Technische Universität Berlin

Fachbereich Informatik

Institut für Wirtschaftsinformatik

MOBILER ZUGANG ZU GESICHERTEN NETZEN – LÖSUNGEN FÜR DIE ZUKUNFT

EVALUATION DES EINSATZES MOBILER ENDGERÄTE IM BMI

PROJEKTBERICHT

(PRESSEVERSION)

Erstellt im Auftrag des Bundesministeriums des Innern

vorgelegt von der

Forschungsgruppe Internet Governance

Berlin, August 2003

Stephan Balszuweit (cand. Inform.)
Thomas Fritsch (cand. Inform.)
Robert Gehring (Diplom-Inform.)
Tilman Kamp (cand. Inform.)
Raphael Leiteritz (Diplom-Inform., Projektleiter)
Bernd Lutterbeck (Prof. für Informationsrecht, Jean Monnet Prof.)
Frank Pallas (cand. Inform.)
Torsten Pehl (cand. Inform.)
Nazan Yildiz (cand. Inform.)

Wichtige Hinweise zu diesem Dokument

1. Dieses Dokument ist die Dokumentation eines Evaluationsprojekt der TU Berlin, Institut für Wirtschaftsinformatik, im Auftrag des Bundesministeriums des Innern zum Thema mobile Endgeräte im behördlichen Einsatz. Basis dieses Dokuments ist wiederum eine allgemeine Studie über Mobiltechnologien, die die TU Berlin im Auftrag des Bundesministeriums des Innern zwischen Mai und Dezember 2002 angefertigt hat („MOB I").

2. Das Executive Summary mit den entscheiderrelevanten Ergebnissen dieses Projekts liegt als separates Dokument vor.

Inhaltsverzeichnis

1 Das Projekt

1.1 Der Projektauftrag

Elektronische Kommunikation über Austausch von E-Mails, Terminen und Aufgaben sowie zur Kontaktverwaltung hat sich zu einem wesentlichen Arbeitsmedium entwickelt. Mit seiner Hilfe können Daten schneller und effizienter ausgetauscht und Entscheidungen auf Grundlage überall verfügbarer Informationen getroffen werden. Elektronische Kommunikation bietet für die Organisation der Arbeit von Behörden und Unternehmen wesentliche Vorteile: Kommunikationswege werden verkürzt, Zeit wird eingespart. Entscheidungen können auch kurzfristig aufgrund aktueller Informationen getroffen werden. Führungskräfte können den unterstellten Bereich rasch und in nachvollziehbarer Art und Weise über aktuelle Entwicklungen und deren Konsequenzen für die tägliche Arbeit unterrichten. Zusatzfunktionen wie der Austausch von Terminen, die Zuweisung von Aufgaben und die Verwaltung von Kontaktinformationen erleichtern die Organisation der Arbeit.

Aufbauend auf den Inhalten des bereits im Sommersemester 2002 durchgeführten Projektes „Mobiles Arbeiten" („MOB I") wurde im Rahmen des Wintersemesters 2002/2003 ein zweites Projekt („MOB II") ebenfalls in Zusammenarbeit mit dem Bundesministerium des Innern (BMI) realisiert. Da „MOB I" als Grundlagenarbeit zu betrachten ist, sollte dieser Bericht zum besseren Verständnis beim Lesen des vorliegenden Dokumentes bereits bekannt sein.

1.1.1 Die Aufgabe

Grundlegende Aufgabe dieses Projektes ist die Untersuchung der voraussichtlichen Konsequenzen eines verstärkten Einsatzes mobiler Endgeräte der Handheldklasse im Zusammenspiel mit Messaging-/Groupwarelösungen, hier insb. Microsoft Exchange. Hierbei steht die Synchronisation bzw. der Abgleich von Daten zwischen dem Groupwareserver und dem mobilen Gerät im Vordergrund. Im Einzelnen sind das:

- E-Mails
- PIM-Daten (Kontakte, Termine, Aufgaben)
- Notizen
- Synchronisation öffentlicher Ordner.

1.1.2 Die Realisierung

Für die Umsetzung des Projektauftrages wurde nach den Vorgaben des Auftraggebers ein Testlabor aufgebaut. Die Synchronisation erfolgte im Labor auf drei unterschiedlichen Wegen:

- Einwahl in das Internet und Verbindung über einen VPN Tunnel zum Labor
- Direkte Einwahl in das Labor mittels RAS
- Direkte Verbindung ins Intranet (z.B. über den Arbeitsplatz).

1.1.3 Das Ergebnis

Im Rahmen des Projektes sollte keine Software entwickelt werden, vielmehr stand der Aspekt der Evaluation verfügbarer Standardsoftware im Hinblick auf die Eignung für das Projektszenario im Vordergrund. Die Auswahl der zu evaluierenden Softwareprodukte erfolgt in Kapitel 3, die Evaluation nebst theoretischer Grundlagen ist in Kapitel 4 zu finden. Endergebnis sollte eine Gesamtempfehlung für ein Referenzsystem sein, das die hier

geschilderten Aufgaben zufriedenstellend erfüllt und beim Auftraggeber, dem Bundesministerium des Innern in dieser Form einsetzbar ist, ohne dessen hohe Sicherheitsanforderungen zu verletzen. Diese Gesamtempfehlung befindet sich in Kapitel 5.

Neben den Ergebnissen der Evaluation sollte die Beschreibung der verwendeten Arbeitsmethodiken ein zweites Produkt des Projektes darstellen. Anhand dieser Ausführungen soll es möglich sein, die Ergebnisse unserer Arbeit nachzuvollziehen und zukünftig Hard- und Softwarekomponenten selbständig zu evaluieren und die so gewonnenen Erkenntnisse mit den hier aufgeführten Ergebnissen zu vergleichen.

1.2 Rahmenbedingungen

Rahmenbedingungen sind Vorgaben seitens des Auftraggebers, wie z. B. Benutzung bestimmter Hard- oder Softwarekomponenten und zeitliche Grenzen, innerhalb derer das Projekt abgeschlossen werden muss.

1.2.1 Zeitliche Rahmenbedingungen

Das Teilprojekt „MOB II" schließt nahtlos an das vorangegangene Projekt „MOB I" an, sollte in der Zeit von Mitte Oktober 2002 bis Mitte Mai 2003 umgesetzt werden und lässt sich zeitlich in drei Abschnitte unterteilen:

- **Vorbereitung:**

  Schwerpunkt der Vorbereitung war eine umfassende Marktanalyse vorhandener Ansätze und Standardsoftware für ähnliche Aufgaben, wie sie auch im Projekt zu bewältigen waren. Auch die Entwicklung eines ersten Evaluationskonzeptes, die Beschaffung benötigter Hardware und Software sowie die genaue Projektplanung fanden in dieser Zeit statt.

- **Evaluation:**

  Nachdem die benötigte Hardware dem Projektteam im Januar 2003 zur Verfügung gestellt worden war, konnte die eigentliche Umsetzung der Evaluation beginnen. Die zweite Phase befasste sich daher hauptsächlich mit der umfangreichen Evaluation der zuvor ausgewählten Produkte (siehe dazu Kapitel 4.2, 4.3 und 4.4). Es fanden jedoch auch der weitere Laboraufbau und eine schrittweise Verfeinerung der Evaluationskonzepte statt.

- **Berichterstellung:**

  Die im Rahmen der Evaluation gesammelten Ergebnisse und Erfahrungen wurden ab Mitte März zu einer Gesamtempfehlung entwickelt, die sich in Kapitel 5 dieses Dokuments findet. Weiterhin wurden die Ergebnisse und Erfahrungen ausführlich dokumentiert. Zudem wurde in Abstimmung mit dem Auftraggeber ein Einblick in die im Projekt eingesetzten Arbeitsmethodiken erarbeitet. Hierauf wird im Kapitel 4.1 eingegangen.

1.2.2 Technische Rahmenbedingungen

Dem Projekt wurden inhaltliche Rahmenbedingungen gesetzt, die insbesondere die Grundlage für die Marktanalyse bildeten und einige Basiskomponenten der Hardware und Software festlegten.

- **Endgeräte:**

  Bei der Wahl der Endgeräte fiel die Entscheidung auf Geräte aus der iPAQ Serie der Firma Hewlett Packard, die zum Zeitpunkt des Projektes zu den leistungsfähigsten ihrer Klasse zählten. Diese boten neben dem anvisierten Betriebssystem PocketPC 2002 auch ausreichend Rechen- und Speicherkapazität, um die gewünschten Eigenschaften realisieren zu können. So bieten die dort verwandten Prozessoren genügend Leistungsreserven, um eine transparente Echtzeitverschlüsselung der Daten im Filesystem des Handhelds zu ermöglichen. Auf die Endgeräte wird in Kapitel 3.2.1 näher eingegangen.

- **Die Laborstruktur:**

  In der Laborstruktur spiegelt sich die in Unternehmen übliche Dreiteilung des Firmennetzes in Intranet, demilitarisierte Zone (DMZ) und Firewallsystem[1] wieder.

- **Das Firewallsystem:**

  Als Firewallsystem kam ein durch das Bundesamt für Sicherheit in der Informationstechnik zertifiziertes deutsches Produkt bestehend aus einem Application Level Gateway (ALG) und Paketfilter (PF) zum Einsatz. Bis zur Bereitstellung eines Testsystems wurden hier zwei Linux-Packetfilter genutzt.

- **Groupware:**

  Der für das Projekt relevante Teil der Infrastruktur des Auftraggebers, der die Bereiche E-Mails, Kontakte und Aufgaben realisiert, beruht im Wesentlichen auf der Groupware Microsoft Exchange. Auf den Arbeitsplatzrechnern im Intranet wird clientseitig Microsoft Outlook eingesetzt. Daher bildete Exchange die grundlegende Groupwarekomponente im Labor.

- **VPN:**

  Die bestehende VPN-Lösung des Auftraggebers wurde ebenfalls berücksichtigt. Diese ermöglicht die Sicherung der Verbindungen mittels personalisierter Zertifikate, welche im Rahmen der Verwaltungs-PKI durch ein zertifiziertes Trustcenter ausgestellt werden.

Neben den genannten grundlegenden technischen Rahmenbedingungen gab es zahlreiche spezielle Vorrausetzungen des Auftraggebers.

[1] Hier bestehend aus einem Application Level Gateway (ALG) und Paketfiler (PF)

1.3 Kategorisierung

Ziel von Diese Projektes war es in erster Linie, eine Empfehlung für ein mögliches Referenzsystem zu erarbeiten, das in der Lage ist, unter den oben vorgestellten Rahmenbedingungen die gestellten Aufgaben der mobilen Synchronisation über die bestehende Infrastruktur zu realisieren. So sollten vor allem mögliche Probleme und Risiken beim praktischen Einsatz von mobilen Endgeräten aufgezeigt und Lösungen für diese Probleme dargelegt werden.

Es wurden vier grundlegende Kategorien als Basis für die gesamte Evaluation definiert:

- **Sicherheit:**

  Von besonderer Bedeutung ist die Sicherheit des Gesamtsystems, da es um den Transfer und die Speicherung hoch sensibler Daten geht. Die Sicherheitsbetrachtungen richten sich neben dem eigentlichen Transfer der Daten auch auf deren Speicherung und Schutz auf den mobilen Endgeräten. Als Beispiel sei hier die mögliche Nutzung eines sicheren Filesystems erwähnt.

- **Administration:**

  Bei der Einführung eines solchen Systems muss sichergestellt werden, dass eine Möglichkeit zur zentralen und effektiven Verwaltung der einzelnen Endgeräte und der darauf verwendeten Software vorhanden ist bzw. geschaffen wird. Auch sollte die notwendige Serverinfrastruktur einen möglichst geringen administrativen Aufwand erfordern.

- **Usability:**

  Die Usability ist ein entscheidender Faktor für die spätere Verwendung eines solchen Systems und die Akzeptanz ihm gegenüber. So sollte der Endnutzer in die Lage versetzt werden, das System ohne größere Schulungsmaßnahmen effektiv, sicher und fehlerfrei zu nutzen.

- **Kosten:**

  Im Hinblick auf die Kosten der Einführung eines Systems zur mobilen Datenverarbeitung besteht die Forderung nach niedrigen und abschätzbaren Kosten für Anschaffung, Wartung und Verbindungen.

Die stetige Verwendung dieser vier Kategorien sowohl bei der Evaluation der einzelnen Komponeten als auch in der abschließenden Bewertung der möglichen Gesamtsysteme ermöglicht es, zwischen verschiedenen Produkten Vergleiche zu ziehen und über eine Gewichtung der vier Kategorien Schwerpunkte zu setzen. Näheres zum Verfahren der Evaluation findet sich in Kapitel 4.1.

2 Systemarchitekturen

Jede Aufgabe, die sich auf die organisierte Kommunikation zwischen verschiedenen Komponenten bezieht, muss eine begriffliche Grundlage beinhalten und das System in seinem Ist-Zustand und seinen angestrebten Soll-Zuständen beschreiben, damit später die Komponenten bestimmt werden können, die noch zu integrieren, zu entfernen oder umzugestalten sind. Dieses Kapitel wird einen Überblick über die im Vorfeld der Evaluation aus architektonischer Sicht zu treffenden Entscheidungen geben.

2.1 Der Ist-Zustand

Das Ziel, eine komplexe Systemarchitektur zu entwickeln, die den in Kapitel 1 gestellten Anforderungen genügt, macht es notwendig, alle beteiligten Komponenten des Ist-Zustandes unter architektonischen Gesichtspunkten zu betrachten. Die Zielsetzung ist hier, ein mobiles Gerät an eine Inhouse-Infrastruktur anzubinden. Dies erfordert, Endgerät und Inhouse-Infrastruktur genauer zu betrachten, um darauf aufbauend ein tragfähiges Konzept für die Anbindung des mobilen Endgerätes zu entwickeln.

2.1.1 Endgerät

Das im Rahmen dieses Projektes vorgegebene Endgerät ist der PDA iPAQ des Hersteller Hewlett-Packard. In seiner abstrakten Struktur entspricht er weitestgehend der PC-Architektur. Er kann daher in ähnlicher Weise aufgegliedert werden nach:

- Hardware
- Betriebssystem
- Applikationen
- Schnittstellen.

Ein vollständiges OSI Schichten Modell des Pocket PC 2002 Systems findet sich im Anhang in Kapitel 7.3.

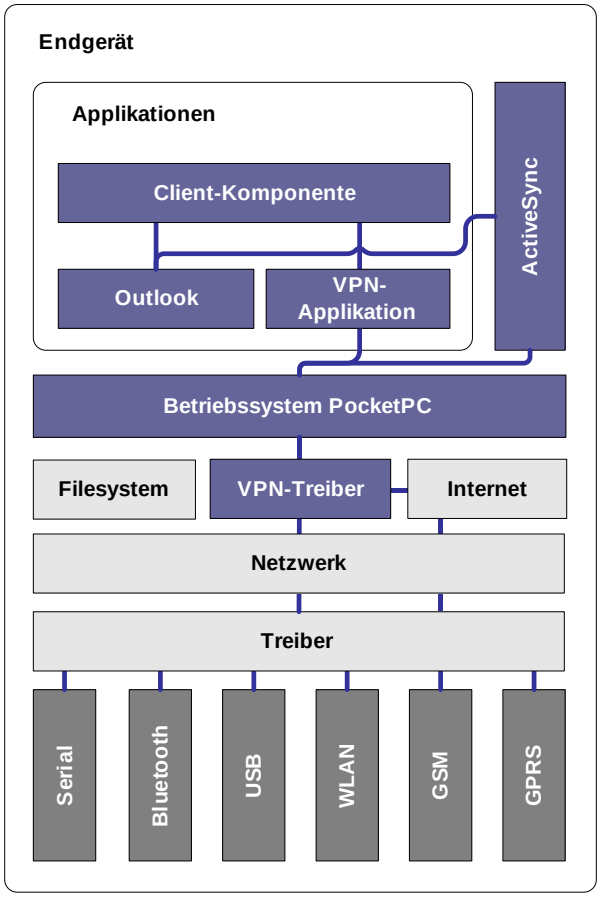

Abbildung 2-1: Schematische Darstellung des Endgerätes

2.1.1.1 Hardware

Der iPAQ besitzt einen ausreichend starken Prozessor und genügend Arbeitsspeicher, um unter seiner Verwendung verschiedenste Sicherheitskomponenten nutzen zu können.

Insbesondere ermöglicht die zur Verfügung stehende Rechenleistung die Nutzung transparenter End-to-End-Verschlüsselung mittels Virtueller Privater Netze (VPN)

2.1.1.2 Betriebssystem

Das hier betrachtete Endgerät ist vom Hersteller mit dem Betriebssystem PocketPC 2002 von Microsoft ausgestattet. Microsoft PocketPC 2002 bietet in Bezug auf gesicherte Kommunikation folgende Vor- und Nachteile:

Vorteile von PocketPC:

- Hoher Verbreitungsgrad und damit Gewährleistung von Drittanbieterunterstützung und Support
- Flexible vollmodulare Struktur (Treiber, API, breite Unterstützung von Netzwerkstandards) und damit Ermöglichung der Migration von Fremdsoftware
- Windows-Look-And-Feel
- Multitaskingfähigkeit

Nachteile von PocketPC:

- Single-User-Betriebssystem
- Kein verschlüsseltes Filesystem
- Kein Open-Source.

2.1.1.3 Applikationen

Auf dem Gerät befindet sich bereits im Auslieferungszustand eine breite Palette von Applikationen. Die hier relevanten Produkte und Produkt-Gruppen sind im Wesentlichen:

ActiveSync

ActiveSync ist der von Microsoft bereitgestellte Synchronisations-Client. Er ist durch sogenannte Module an diverse Applikationen anpassbar. Für PocketOutlook und den reinen Filetransfer existieren bereits Module auf dem Endgerät. ActiveSync wird als vom Hersteller installierte Synchronisationssoftware auch für das Deployment von Software eingesetzt. Ein ActiveSync-Vorgang benötigt als Synchronisations-Gegenstelle einen Companion-PC oder einen Server, der sich wie ein Companion-PC verhält.

Im gebräuchlichsten Szenario dient der Companion-PC in Form eines Notebook oder Desktop-PC als Datenquelle für die Synchronisation. Dieses Szenario kann in einem Firmenumfeld jedoch nicht Anforderungen wie die zentrale Administration erfüllen.

Pocket-Outlook

Pocket-Outlook ist ein auf das Wesentliche reduziertes Outlook. Die Einschränkungen sind vor allem im Bereich Groupware-Funktionalität und E-Mail-Verwaltung zu finden (siehe Evaluation der Synchronisationssoftware in Kapitel 4.3).

PocketWord, PocketExcel und andere Anwendungen

Diese Applikationen stellen die eigentliche Produktivitäts-Umgebung auf dem iPAQ dar. Im Wesentlichen sind alle für die alltägliche Arbeit notwendigen Anwendungen, Viewer und Tools bereits auf dem Gerät vorhanden, wobei jedoch die meisten dieser Applikationen einen im Vergleich zu ihren Desktop-Pendants stark reduzierten Funktionsumfang haben.

2.1.1.4 Schnittstellen

Es werden nun die vom Endgerät unterstützten Schnittstellen für eine mögliche Datenkommunikation mit der Außenwelt erläutert.

WLAN

Die WLAN-Schnittstelle ermöglicht sowohl den direkten netzwerkbasierten Zugriff auf das Inhouse-Netz als auch den Zugriff auf das Internet von einem beliebigen Access-Point aus. Sie ist im mobilen Einsatz nach einer leitungsbasierten Verbindung die schnellste Datenschnittstelle. WLAN kann innerhalb des Hauses auch anstelle einer festen Netzwerkverbindung verwendet werden und verbessert somit die Möglichkeit zu Mobilität auch im Nahbereich.

GSM / GPRS

Der zusätzliche „GSM-Rucksack" ermöglicht den Datentransport durch das Mobilfunk-Netz. Er beherrscht auch GPRS und ist damit geeignet, einen direkten Internet-Provider-Zugriff zur Kommunikation zu nutzen. Die Möglichkeit der GSM-Einwahl kann sowohl zur direkten Einwahl in das Inhouse-Netz als auch zur Einwahl bei einem beliebigen anderen Internet-Provider dienen. Die Möglichkeit, SMS zu empfangen kann später auch durch sog. Push-Dienste (Kommunikationsaufbau vom Intranet zum Endgerät) in Anspruch genommen werden.

USB / Seriell / Bluetooth

Diese Schnittstellen dienen vor allem der Kommunikation mit anderen Endgeräten wie z. B. Clients im Intranet, dem Notebook[2] oder spezieller Peripherie.

2.1.2 Inhouse-Netzwerk

Das hier betrachtete Inhouse-Netzwerk besteht im Wesentlichen aus drei Komponenten:

- Intranet
- Firewall
- Demilitarisierte Zone (DMZ).

Ihr Zusammenspiel ermöglicht die gesicherte Kommunikation aller im Folgenden erläuterten Komponenten miteinander und mit der Außenwelt.

2.1.2.1 Das Intranet

Das Intranet ist der zentrale Bereich des Inhouse-Netzwerkes und Träger aller Applikations- und Verwaltungsdaten. Die gesamte Hausinfrastruktur ist hier eingebettet. In stilisierter Form ist es wie folgt aufgebaut:

[2] Hier im Wesentlichen die Kommunikation mit einem sog. Companion-PC, der seinerseits z. B. wieder eine Netzwerkverbindung nach außen ermöglicht

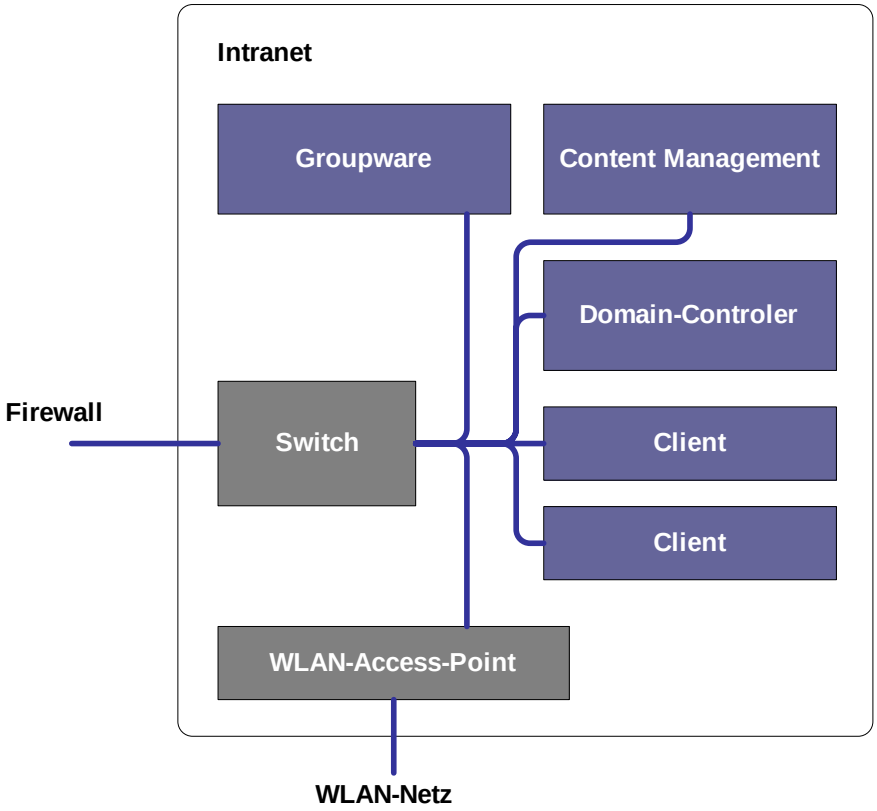

Abbildung 2-2: Das Intranet

Clients

Clients sind die Arbeitsplatzrechner im Inhouse-Bereich, die direkt über das LAN mit der Intranet-Infrastruktur verbunden sind. Alle Clients werden durch die im Intranet eingebetteten Server mit Daten versorgt und verwaltet. Diese Verwaltung gilt es von einem Endgerät aus nutzbar zu machen.

Domain-Controller

Der Domain-Controller steht stellvertretend für alle Intranetsysteme, die die logischen Aufgaben und Backend-Dienste im Intranet wahrnehmen. Sie stellen auch einen nicht unwesentlichen Teil der Funktionalität dar, die es auf ein mobiles Gerät zu übertragen gilt. Solche Systeme sind z.B.:

- Domain-Controller
- DNS
- Backup-System
- Netzwerkdienste-Server.

Content Management System

In Abbildung 2-2 fasst das aufgeführte Content Management System die gesamte Infrastruktur eines solchen Systems zusammen, z. B.:

- Web-Server
- Datenbankserver
- Applikations-Server

Groupware

Die Groupware steht zusammenfassend für alle eingesetzten Groupware-Systeme und deren Sekundärkomponenten. Es ist eine primäre Aufgabe dieses Projektes ihre Dienste von einem mobilen Endgerät aus verfügbar zu machen. Dabei geht es um weit mehr als reinen Mailaustausch – gerade die zentral organisierte Termin-, Kalender- und Adressabstimmung einer Groupware ist im Produktiveinsatz außerhalb des Hauses von hoher Bedeutung.

Switch

Der Switch steht stellvertretend für die verbindende Netzwerkinfrastruktur des Intranets.

2.1.2.2 Die Firewall

Das verwendete Firewall-System ermöglicht es durch seine zweistufige Architektur, eine demilitarisierte Zone (DMZ) vor der Außenwelt zu schützen und vom Intranet zu trennen. Eine schematische Darstellung ihres grundsätzlichen Aufbaus zeigt Abbildung 2-3, die zentralen Elemente der verwendeten Firewall werden anschließend genauer betrachtet.

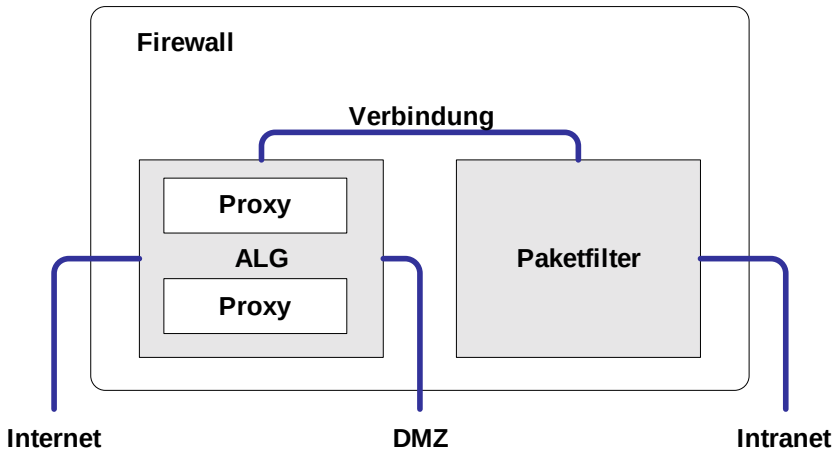

Abbildung 2-3: Die Firewall

Application Level Gateway (ALG)

Der Application Level Gateway stellt eine auf Applikationsebene (OSI-Schicht 7) ablaufende Datenstromkontrolleinheit dar. Er ist durch sog. Proxy-Module (s. u.) in der Lage, Protokolle höherer Kommunikationsschichten zu „verstehen" und entsprechend auf Inhalte hin zu überprüfen. So kann der ALG beispielsweise einen http-Zugriff aus den IP-Paketen rekonstruieren und die im Datenstrom enthaltenen Informationen auf Viren, schädliche Inhalte usw. scannen. Der ALG schirmt die demilitarisierte Zone vom Internet und vom Intranet ab. Ein Zugriff auf Netzwerkebene (OSI-Schicht 3/5) in das Intranet wird dadurch verhindert, dass die Verbindung zwischen dem ALG und dem Paketfilter ein auf Applikationsebene (OSI-Schicht 7) ablaufender Prozess ist.

Proxy-Module

Bei den Proxy-Modulen handelt es sich um einzelne Komponenten des ALG, die jeweils für bestimmte Protokolle höherer Schichten zuständig sind und den betreffenden Daten-

strom einer syntaktischen und semantischen Prüfung unterziehen können. Sie analysieren die Protokollinhalte also z. B. auf illegale Zugriffe und nicht erlaubte Inhalte.

Paketfilter

Der Paketfilter ist eine auf Netzwerkebene (ISO-Schicht 3/5) arbeitende Firewall, die verhindert, dass bestimmte IP-Bereiche und Ports von im Intranet befindlichen Rechnern aus der DMZ heraus angesprochen werden können. Damit haben in der DMZ auftretende „illegale" Datenpakete keine Möglichkeit, beliebige Adressen und/oder Ports des Intranets zu erreichen. Ein nicht explizit zugelassener Zugriff nach außen und damit ein nicht gestatteter Datentransport vom Intranet in eine öffentliche Zone wird auf die gleiche Weise verhindert.

2.1.2.3 Die demilitarisierte Zone (DMZ)

Die demilitarisierte Zone ist ein Bereich, der dazu dient, von außen kommende Zugriffe auf das Intranet entgegenzunehmen und diesen Zugriff mit Hilfe verschiedener Komponenten zu kontrollieren und zu überwachen. Sie ist also ein *per definitionem* unsicherer Bereich, in dem noch keinerlei Nutzdaten zu finden sind.

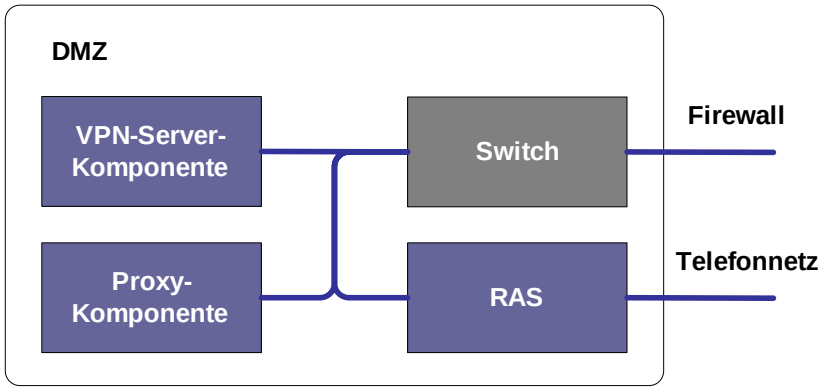

Abbildung 2-4: Die demilitarisierte Zone (DMZ)

VPN-Server-Komponente

Die VPN-Server-Komponente repräsentiert alle VPN-Brückenköpfe in der DMZ. Sie gewährleistet den Aufbau eines sicheren VPN-Tunnels durch ein unsicheres äußeres Netz und leitet den eingehenden Datenverkehr an die entsprechenden Zieladressen weiter.

Proxy-Komponente

Bei der Proxy-Komponente handelt es sich stellvertretend um alle Komponenten der DMZ, die jeweils für bestimmte Datenzugriffe in das Intranet zuständig sind und diese vorverarbeiten und prüfen können. Sie analysieren die Protokollinhalte z. B. auf illegale Zugriffe und nicht erlaubte Inhalte und tätigen ggf., stellvertretend für eine Client-Komponente im Intranet, die Authentifizierung.

RAS

RAS (Remote Access Service) realisiert die telefonische Einwahlmöglichkeit von Endgeräten oder Arbeitsplätzen außerhalb des Intranets in das Intranet. Die RAS-Komponente ermöglicht zusätzlich eine Identifikation des einwählenden Gerätes durch die übertragene Teilnehmernummer. In der Regel wird bei einem RAS-Zugriff durch die RAS-Komponente selbst bereits ein VPN-Tunnel etabliert.

Switch

Der Switch steht wie bei der Komponente Intranet stellvertretend für die verbindende Netzwerkinfrastruktur der DMZ. Er stellt außerdem die Verbindung zur Firewall her.

2.1.2.4 Das gesamte Inhouse-Netzwerk

Zur Zusammenfassung sei hier nochmals die gesamte Struktur des Inhouse-Netzwerkes abgebildet:

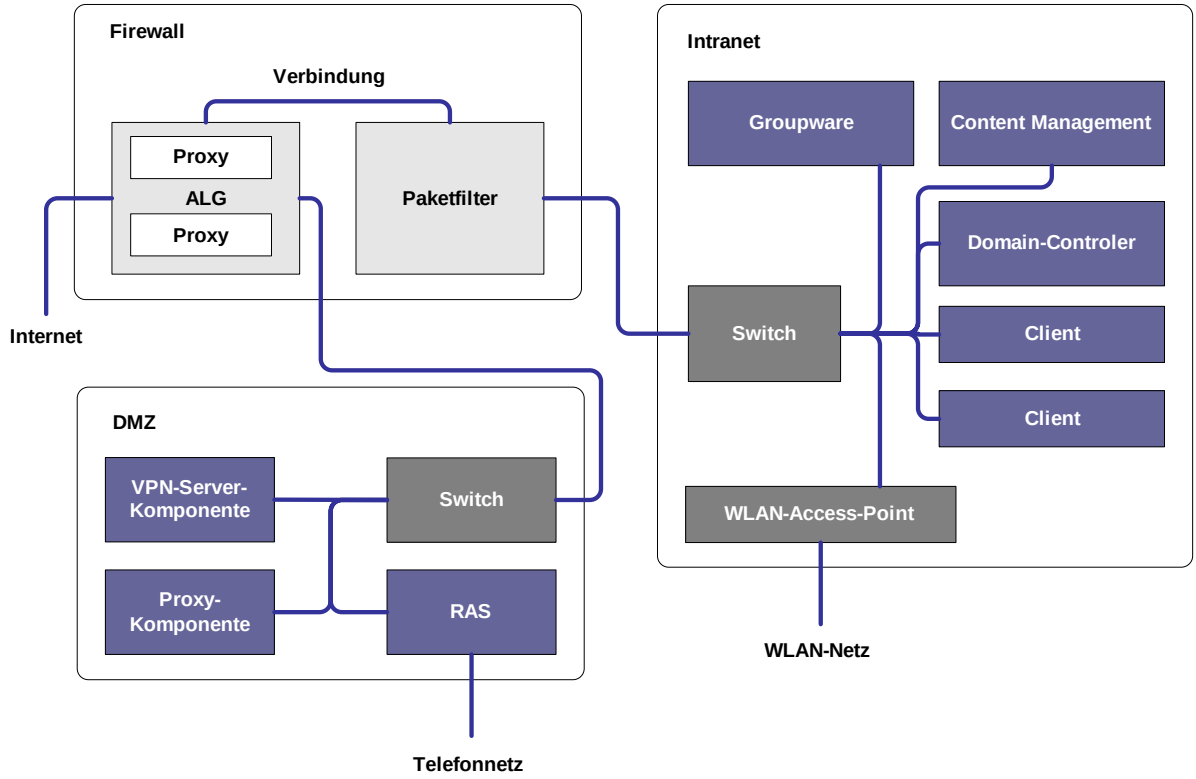

Abbildung 2-5: Die gesamte Infrastruktur des Inhouse-Netzwerkes im Überblick

2.2 Zu integrierende Komponenten

Die Zielsetzung, sowohl eine Administrations- als auch eine Synchronisationskomponente für die Anbindung mobiler Endgeräte an das Intranet zu realisieren, lässt sich wie im Folgenden dargelegt abstrahieren: In beiden Fällen werden im Intranet gehaltene Daten mit einem Endgerät ausgetauscht. Hierzu zählt auch ein Browserzugriff auf ein Content-Management-System im Intranet. Dieser Umstand macht eine generalisierte Betrachtung möglich.

Der Planungsprozess zur Anbindung der Endgeräte an das Intranet lässt sich in drei Stufen unterteilen:

- Die Integration der grundsätzlichen Funktionen (Administration, Synchronisation etc.) in die Infrastruktur
- Die Integration der für den Datentransport notwendigen Elemente in die Infrastruktur
- Die Kombination von Datentransport und Funktion.

Um die Betrachtung der einzubeziehenden Funktionen vereinheitlichen zu können, wird im Folgenden der Begriff der „funktionalen Gruppe" eingeführt:

2.2.1 Funktionale Gruppen

Prozesse wie Administration, Synchronisation und Browserzugriff stellen jeweils eine funktionale Gruppe dar. Unter Berücksichtigung der gegebenen Strukturen (Endgerät, Intranet usw.) und der gesetzten Anforderungen (Sicherheit, Transparenz usw.) lassen sich alle diese funktionalen Gruppen mit Hilfe eines einheitlichen Schemas darstellen:

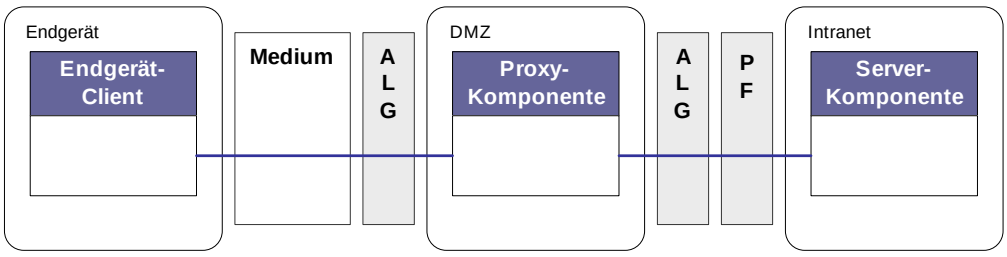

Abbildung 2-6: Schema einer funktionalen Gruppe

Die Endgerät-, Proxy- und Serverkomponenten sind so weit wie möglich für jede funktionale Gruppe in die Architektur zu integrieren.

Die Server-Komponente ist der zentrale Teil jeder funktionalen Gruppe. Sie wird grundsätzlich im Intranet platziert, da sie die Verbindung zur Intranet-Datenbasis darstellt. Das Sicherheitskonzept muss in jedem Fall ein Zugriff auf Gruppen- und Benutzerkonten des Intranets gewährleisten.

Gründe *für* die Platzierung der Server-Komponente im Intranet sind:

- Direkter Zugriff auf die Datenbasis möglich
- Zugriff auf Nutzer- und Gruppenkonten möglich
- Administration in der Regel im Intranet erfolgend
- Konfigurationsdaten der Server-Komponente selbst oft in im Intranet eingebetteten Datenstrukturen gehalten (ActiveDirectory bzw. SQL-Server).

Gründe *gegen* eine Platzierung der Server-Komponente in der DMZ sind gleichzeitig:

- Ein Replizieren der benötigten Intranet-Datenbasis in die DMZ ist aufwendig und fehlerträchtig.
- Die DMZ ist als potentiell unsicher deklariert und sollte daher niemals Nutzdaten beinhalten.
- Gruppen- und Nutzerkonten-Informationen sind sensible Daten, die in einer DMZ einem zu hohen Risiko des Fremdzugriffs ausgesetzt wären.
- Die Konfigurationsdaten der Server-Komponente selbst sind bereits sensible Daten – auch sie sollten nicht in einer DMZ stehen.

Selbst bei einer sehr niedrigen Sicherheitsstufe sollte die Server-Komponente in jedem Fall im gesicherten Intranet angesiedelt werden.

2.2.1.1 Endgerät-Client

Der Endgerät-Client realisiert alle die funktionale Gruppe betreffenden clientseitigen Datenaustauschaufgaben. Er stellt die logische Gegenstelle zur Server-Komponente dar und terminiert die Datenverbindung auf Endgeräte-Seite. In der Regel ist er als Applikation realisiert, die vom Nutzer zum Initiieren des Datenaustausches gestartet wird. Hier muss der Nutzer auch die ggf. notwendigen Login-Angaben machen, die ihm gestatten, mit der Server-Komponente in Verbindung zu treten und den geforderten Dienst in Anspruch zu nehmen.

2.2.1.2 Proxy-Komponente

Die Proxy-Komponente stellt eine Sicherheitsstufe zwischen dem Intranet und der Außenwelt dar. Sie interpretiert den Datenstrom zwischen der Server-Komponente und dem Endgerät-Client, und kann daher bei einem Zugriff diverse sicherheitsrelevante Kontrollen durchführen, bevor Daten in das Intranet hinein- bzw. aus dem Intranet herausgelangen. Sie kann ggf. proprietär codierte oder verschlüsselte Datenströme entschlüsseln und die darin befindlichen Informationen vorab interpretieren. Auch eine Authentifizierung kann auf diese Weise mit akzeptabler Sicherheit ablaufen: Die Komponente entnimmt den eintreffenden Datenpaketen die Login-Informationen und fragt im Intranet (z. B. über LDAP) an, ob der Zugriff gestattet ist. Erst dann wird von Intranet aus die eigentliche Verbindung geöffnet.

2.2.2 Datentransport-Komponenten und ihre Platzierung

2.2.2.1 VPN-Tunnel

Damit eine sichere Datenverbindung vom Endgerät zum Intranet realisiert werden kann, ist es dringend erforderlich, einen VPN-Tunnel zwischen der Proxy-Komponente und dem Endgerät-Client aufzubauen. Die VPN-Server Komponente sollte in der DMZ positioniert werden, um die durch den Tunnel eingehenden Datenpakete an in der DMZ liegende Proxy-Komponenten weiterleiten zu können.

Sollte die Positionierung in der DMZ nicht möglich sein, so ergibt sich neben der niedrigeren Sicherheit dieser Datenverbindung ein weiterer Nachteil: Alle funktionalen Gruppen können sich im Regelfall einen in der DMZ positionierten VPN-Tunnel teilen. Muss jedoch ein weiterer VPN-Tunnel etabliert werden, sinken sowohl die Alltagstauglichkeit als auch die Akzeptanz auf Nutzerseite, da der Nutzer des Endgerätes situationsabhängig jeweils einen anderen Tunnel aufbauen muss.

2.2.2.2 Vollwertiger Proxy in der DMZ

Um eine maximale Sicherheit gewährleisten zu können, bedarf es immer einer Proxy-Komponente in der DMZ, da hier mittels komplexer Analysen verhindert werden kann, dass die Sicherheit des Intranets gefährdende Daten in das Intranet gelangen.

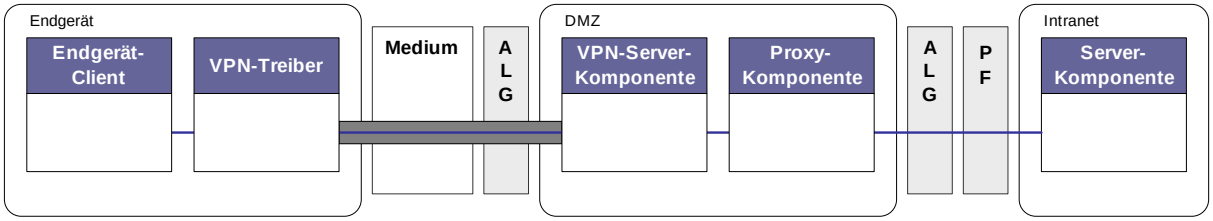

Abbildung 2-7: Sichere Datenaustausch-Variante

Der Ablauf des Zugriffes auf die Groupwaredaten von außen (in der unten stehenden Grafik von links nach rechts) verläuft in folgenden Schritten:

1. Der Endgerät-Client wird durch eine Aktion des Nutzers aufgefordert, sich mit seiner Server-Komponente zu verbinden.
2. Dazu muss der Nutzer bereits eine reguläre IP-Verbindung (z.B. ins Internet über GPRS) etabliert haben.
3. Damit der Client Zugriff auf den Server im Intranet hat, muss über die IP-Verbindung ein VPN-Tunnel in die DMZ bestehen.
4. Der Endgerät-Client schickt nun seine ersten Daten (in der Regel sind das Login-Informationen) an eine Adresse der DMZ – seine Proxy-Komponente.
5. Die Proxy-Komponente analysiert die eingehenden Daten, trennt die Anfrage auf OSI-Schicht 7 und baut ihrerseits eine Verbindung mit der Server-Komponente auf. Es besteht dabei keine direkte Verbindung zwischen Client und Server. Ein zusätzlicher Schutz des Intranets ist der vorgeschaltete Paketfilter.
6. Die Proxy-Komponente versucht nun, sich im Namen des Endgerät-Clients bei der Server-Komponente anzumelden.

7. Stellt die Server-Komponente fest, dass es sich um einen berechtigten Nutzer/Client handelt, so öffnet diese ihrerseits zusätzliche Ports/Transportwege zur Proxy-Komponente.
8. Die Proxy-Komponente steuert nun den Synchronisationsprozess und agiert gegenüber dem Server als Client und gegenüber dem Client als Server.

2.2.2.3 Verlegen der VPN-Server-Komponente in das Intranet

Es kann vorkommen, dass eine funktionale Gruppe keine Proxy-Komponente benötigt oder dass das eingesetzte Software-Paket eine solche nicht zur Verfügung stellt. Eine Möglichkeit ist es dann, die DMZ komplett zu umgehen und das Endgerät direkt mit dem Intranet zu verbinden.

Diese Lösung kann jedoch nur dann sicher sein, wenn die eingesetzte VPN-Software so konfigurierbar ist, dass die VPN-Server-Komponente nur Datenpakete im Intranet freisetzt, die eine bestimmte Zieladresse und einen bestimmten Zielport haben. Anderenfalls würde man riskieren, dass ein Angriff auf das Intranet sehr leicht möglich wird, da im Intranet selbst kaum noch Möglichkeiten bestehen, illegal adressierte Pakete zu identifizieren und abzufangen.

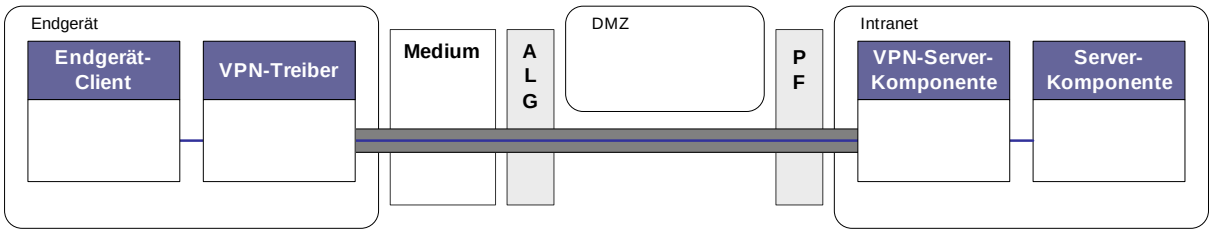

Abbildung 2-8: VPN-Server-Komponente im Intranet

2.2.2.4 Port-Forwarding der Pakete von der VPN-Server-Komponente direkt in das Intranet

Bei Verwendung eines Port-Forwardings durch den ALG bzw. den Paketfilter direkt zur betreffenden Server-Komponente kann die Proxy-Komponente eingespart werden. Allerdings birgt diese Methode Risiken und Nachteile: Sollten die Datenpakete außerhalb des VPN-Tunnels nicht verschlüsselt sein, so können diese innerhalb der DMZ eingesehen werden. Mit einem Port-Forward besteht zudem eine direkte Verbindung in das Intranet, während ein Proxy den Datenverkehr auf OSI-Schicht 7 trennt und so syntaktische und semantische Prüfungen vornehmen kann.

Ein Vorteil gegenüber der Methode, das VPN-Gegenstück in das Intranet zu verlegen, ist der immer noch vorgeschaltete ALG, der die nun nicht mehr „VPN-verpackten" Datenpakete analysieren kann.

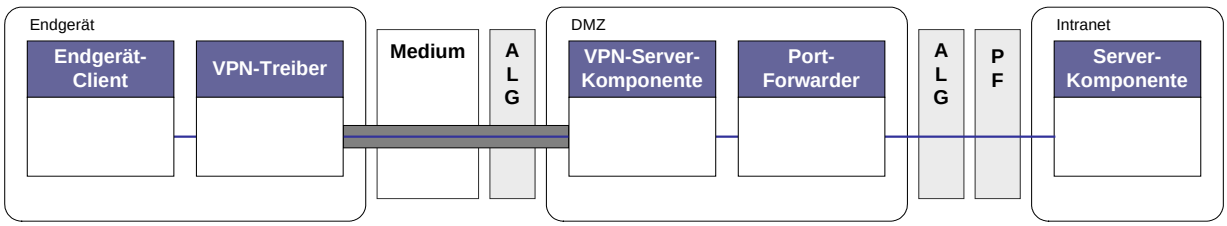

Abbildung 2-9: Port-Forwarding direkt in das Intranet

2.2.2.5 ALG-Proxy-Modul statt DMZ-Proxy-Komponente

Sollte es vorkommen, dass anstatt einer Proxy-Komponente bereits ein spezielles Proxy-Modul für den ALG existiert, so kann dieses die Aufgaben der Proxy-Komponente übernehmen. Dies ist ein analoges Vorgehen zu dem in Kapitel 2.2.2.2 beschriebenen, wobei hier eine Proxy-Komponente durch ein Proxy-Modul ersetzt wird, das gleichwertig ist. Beide Lösungen sind damit gleich sicher.

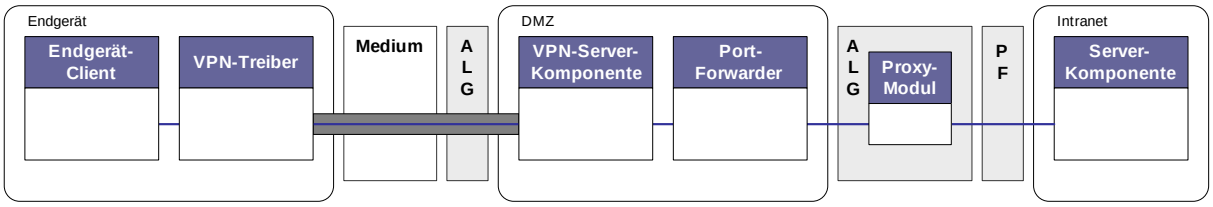

Abbildung 2-10: In das ALG eingebettete Proxy-Komponente

2.3 Vollständiges Szenario

2.3.1 Logischer Aufbau

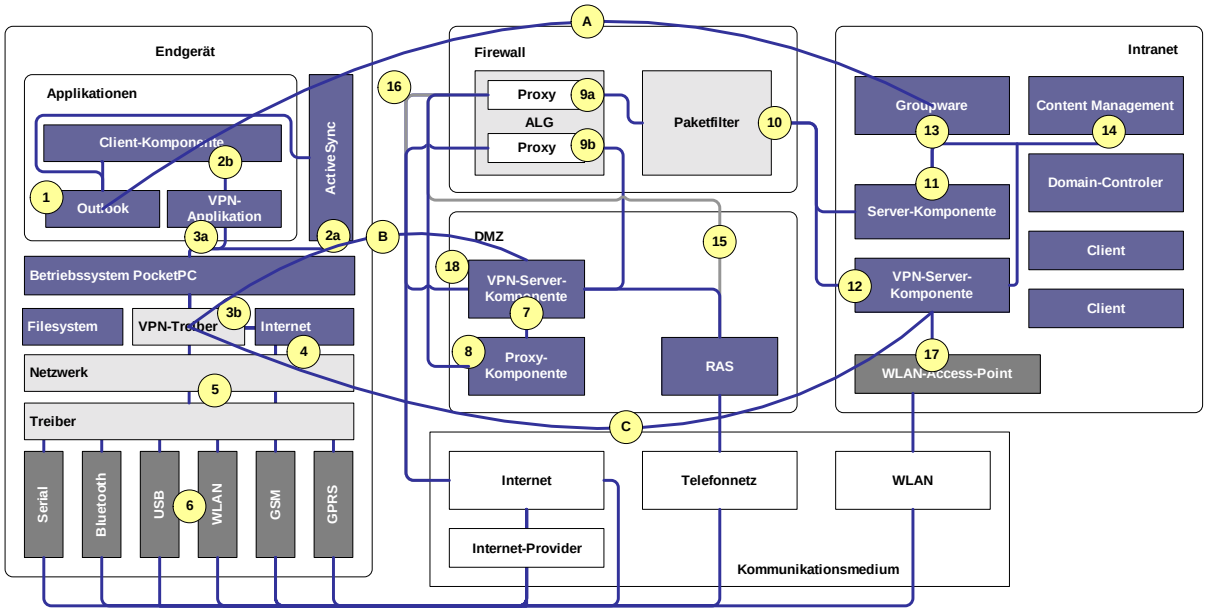

Abbildung 2-11: Vollständiger logischer Zusammenhang aller Komponenten

2.3.2 Ablauf eines vollständigen Datenaustausches

Innerhalb eines dem obigen Konzept entsprechenden Gesamtsystems erfolgt ein Datenaustausch wie im Folgenden beschrieben:

1. Will ein Nutzer den Datenaustauschprozess einer funktionalen Gruppe (hier zwischen Pocket-Outlook (1) und der Groupware (13) – (Linie A)) initiieren, so muss er zunächst einen VPN-Tunnel mittels der VPN-Client-Applikation (3a) aufbauen.
2. Die VPN-Client-Applikation initialisiert den Nutzerangaben (Auswahl zwischen den Tunneln und Name bzw. Passwort) entsprechend den VPN-Client-Treiber (3b).
3. Der VPN-Client-Treiber veranlasst je nach Konfigurationseinstellung des gewählten VPN-Kanals die Endgerät-Netzwerkkomponenten (Betriebssystem, Internet-, Protokoll- bzw. Gerätetreiber (4,5)), eine physikalische Verbindung mit der VPN-Server-Komponente (7 bzw. 12 – Linien B und C) aufzubauen. Die verschiedenen physikalischen Verbindungen werden in Kapitel 1.1.1 aufgeführt.
4. Nach erfolgreicher Authentifizierung des Nutzers an der VPN-Server-Komponente (7 bzw. 12) wird der VPN-Kanal geöffnet.
5. Der Nutzer kann anschließend den eigentlichen Datenaustauschprozess starten, indem er die zuständige Client-Komponente (2a bzw. 2b) aufruft. Diese fordert ihrerseits eine Authentifizierung.
6. Die Kommunikation zwischen der Client-Komponente (2a bzw. 2b) und der Server-Komponente (11) kann in mehreren Varianten erfolgen:
    a. **Vollwertiger Proxy in der DMZ:** Über die vollwertige Proxy-Komponente (8), ein „durchlässiges" Proxy-Modul des ALG (9a) und den Paketfilter (10) wird die Verbindung zur Server-Komponente (11) hergestellt.
    b. **Verlegen der VPN-Server-Komponente in das Intranet:** Von den Zugängen RAS (15) bzw. Internet (16) wird direkt an ein „durchlässiges" Proxy-Modul (9a) des ALG und anschließend durch den Paketfilter zur VPN-

Server-Komponente im Intranet (12) weitergeleitet. Bei WLAN (17) geschieht dies direkt ohne die Firewall.

c. **Port-Forwarding der Pakete von der VPN-Server-Komponente direkt in das Intranet:** Über eine „durchlässiges" Proxy-Modul (9a) des ALG (durch Port-Forwarding (18) bzw. (16) ausgehend von der VPN-Server-Komponente (11)) und den Paketfilter (10) wird eine Verbindung mit der Server-Komponente (11) aufgebaut.

d. **Ein ALG-Proxy-Modul statt einer DMZ-Proxy-Komponente:** Über ein spezielles den Datenstrom analysierendes Proxy-Modul (9a) des ALG (durch Port-Forwarding (18) bzw. (16) ausgehend von der VPN-Server-Komponente (11)) und den Paketfilter (10) wird mit der Server-Komponente (11) verbunden.

7. Die Login-Daten werden nun je nach Variante direkt an die Server-Komponente (11) übertragen oder zunächst von einer Proxykomponente entgegengenommen, die diese prüft und erst anschließend mittels eines gesicherten Kanals an die Server-Komponente (11) weitergibt, welche die endgültige Authentifizierung vornimmt.
8. Der eigentliche Datenaustausch erfolgt zwischen dem Endgerät und dem Inhouse-Netzwerk (hier: zwischen Pocket Outlook (1) und der Groupware (13)).
9. Die Nicht-VPN-Verbindung wird in umgekehrter Reihenfolge wieder abgebaut.
10. Über den noch bestehenden VPN-Kanal können nun weitere funktionale Gruppen betrieben werden (z. B. Browserzugriff auf ein Content-Management-System (14) – weiter mit Schritt 5)
11. Die VPN-Verbindung wird wieder abgebaut.
12. Es können dann weitere funktionale Gruppen betrieben werden, die einen anderen VPN-Kanal benötigen (z. B. Browserzugriff auf ein Content-Management-System (14) – weiter mit Schritt 1).

Dieser Ablauf macht deutlich, dass der Nutzer selbst bei einem simplen Synchronisationsvorgang viel zu beachten hat. Daher sollte in Betracht gezogen werden, auf dem Endgerät eine zentrale Software oder ein Skript zu installieren, mittels derer bzw. dessen diese Aufgaben transparent gestaltet werden können. Es ist in einem solchen Fall jedoch dringend erforderlich, das Filesystem des Endgerätes zu verschlüsseln, da dort Zugriffsdaten (Adressen, Login-Daten, Kennwörter) abgelegt werden müssten. Dies wäre auch dann der Fall, wenn die einzelnen Client-Komponenten bereits die Login-Informationen in sich tragen oder selbst im Dateisystem ablegen würden.

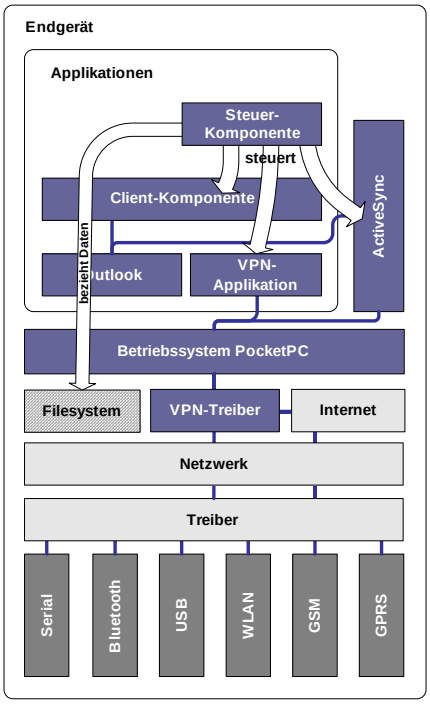

Abbildung 2-12: Endgerät mit einer Steuer-Komponente

2.3.3 Mögliche Verbindungsarten

Die Möglichkeiten einer Verbindung des Endgerätes mit der Infrastruktur ergeben sich aus den vom Gerät unterstützten Schnittstellen (Abbildung 2-13).

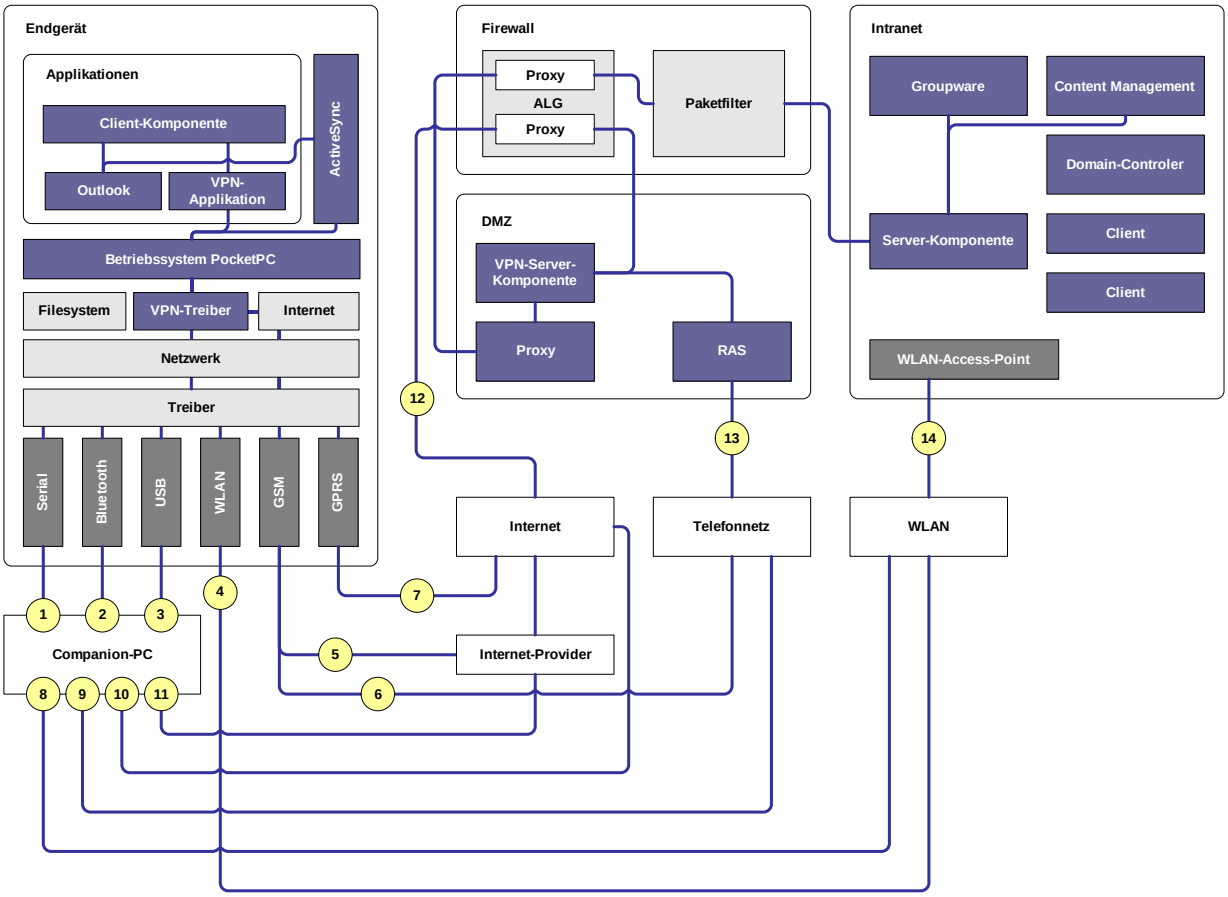

Abbildung 2-13: Die möglichen Verbindungsarten

Durch die Verbindung mit einem Companion-PC über die serielle Schnittstelle (1), Bluetooth (2) bzw. USB (3) kann die Netzwerkverbindung über den Companion-PC realisiert werden.

Es gibt vier grundsätzliche Varianten, eine physikalische Datenfernverbindung zu etablieren:

- Internet-Zugriff über GPRS (7 bzw. 10) und anschließende Verbindung mit dem ALG der Firewall (12)
- Internet-Zugriff durch GSM- bzw. ISDN oder Analog-Einwahl bei einem Internet-Provider (5 bzw. 11) und anschließende Verbindung mit dem ALG der Firewall (12)
- Durch GSM- bzw. ISDN oder Analog-Einwahl (6 bzw. 9) in die DMZ zur RAS-Komponente (13)
- Durch WLAN-Zugriff (4 bzw. 8) auf den Intranet-WLAN-Access-Point (14).

Insgesamt ergeben sich somit 3 x 4 + 1 x 4 = 16 verschiedene mögliche Wege für die Kommunikation vom Endgerät zum Inhouse-Netzwerk.

2.4 Fazit

Zwei grundsätzliche Richtlinien für die Entwicklung einer möglichst sicheren Architektur des Systems lassen sich konstatieren:

- Es sollte angestrebt werden, auf einer Kommunikationsstrecke zwischen Endgerät und Intranet möglichst viele Kontrollstrukturen einzusetzen, mindestens jedoch eine. Alle Kontrollstrukturen sollten auf einer möglichst hohen ISO-Schicht arbeiten, am besten auf der Applikationsschicht (Schicht 7). Standort der Kontrollstrukturen sollte nicht das Intranet selbst sein, sondern die Firewall oder die DMZ.
- Damit die Usability im Einsatz gewährleistet bleibt, ist die Zahl der verschiedenen Verbindungs-Arten (VPN-Tunnel, physische Kommunikationskanäle) gering zu halten.

Diesen Aspekten wird bei den in den Kapiteln 2.2.2.2 und 2.2.2.5 beschriebenen Varianten am besten Rechnung getragen. Sollte für eine funktionale Gruppe weder ein DMZ- noch ein ALG-Proxy verfügbar sein, so ist zumindest ein Aufbau nach Kapitel 2.2.2.4 anzustreben, wobei, wie dort bereits erwähnt, unbedingt auf eine hinreichend starke Verschlüsselung der Nutzdaten zwischen Client und Server zu achten ist. Auf dieser Basis sind die für den Testbetrieb im Labor zu verwendenden Komponenten auszuwählen.

3 Komponentenauswahl

3.1 Software

3.1.1 Administrationssoftware

Mit Administrationssoftware ist hier eine Softwarelösung gemeint, die gezielt der Administration mobiler Endgeräte dient, dabei wird hier nicht zwischen Palm-Endgeräten, Pocket-PCs, Smartphones, Laptops und anderen Geräteklassen unterschieden. Dennoch liegt das Hauptaugenmerk auf der Verwaltung und Administration von PDAs der Pocket-PC-Klasse. Die Möglichkeiten der Integration der anderen Geräteklassen werden ebenfalls untersucht.

3.1.1.1 Extended Connect Server[3]

- Hersteller: Extended Systems
- Version: 3.6
- Homepage: http://www.extendedsystems.de
- Sprache: Englisch
- Preis: siehe Synchronisationssoftware Kapitel 3.1.2.3
- Getestet: ja

Bei der Überprüfung der Synchronisationssoftware (Kapitel 3.1.2) stellte sich heraus, dass der betrachtete Extended Connect auch über ein gewisses Maß administrativer Möglichkeiten verfügt. Diese werden deshalb ebenfalls näher untersucht.

3.1.1.2 XcelleNet Afaria

- Hersteller: XcelleNet
- Version: 4.51
- Homepage: http://www.xcellenet.com
- Sprache: Englisch
- Preis: auf Anfrage, Projektgeschäft

  Serverpreis abhängig von der Anzahl der Clients:
  Bis max. 50 Clients: 5500,- €
  Bis max. 500 Clients: 16.000,- €
  Bei 100 Clients: ca. 7000,-€

  Bei vollem Funktionsumfang des Servers entstehen zusätzliche Kosten in Höhe von 127,- € für jede Clientlizenz.

- Getestet: ja

Die Firma XcelleNet preist ihr Produkt mit einer sehr umfangreichen Feature-Liste nebst Fallstudien an. Dabei werden alle oben genannten Anforderungen (und mehr) abgedeckt. Viel versprechend klingt auch die Möglichkeit zur Verteilung nutzer- bzw. gruppenspezifischer Dateien. Dies findet bei Afaria über so genannte „Channels" statt, die individuell abonniert werden können. Insgesamt scheint einzig diese Software als Lösung in Betracht zu kommen, da nur sie – bei zutreffenden Herstellerangaben – unsere Anforderungen erfüllen kann.

---

[3] Im Folgenden auch als XTND Connect Server bezeichnet.

3.1.2 Synchronisationssoftware

3.1.2.1 Allgemeines

Die Synchronisationssoftware dient dem Abgleich von Inhalten zwischen dem mobilen Endgerät und dem Groupware-Server{ XE "Groupware-Server" }. Als Beispiel für solche Inhalte sei hier das benutzereigene Mailkonto genannt. Im Regelfall werden von einem Groupware-Server jedoch weitere Daten wie Termine, Adressbücher (Kontakte), Aufgabenlisten oder allgemeine Notizen verwaltet, die ebenfalls auf dem mobilen Endgerät abrufbar sein sollen und deshalb ebenfalls synchronisiert werden müssen.

Nicht zuletzt besteht häufig die Notwendigkeit, bestimmte Dateien, unabhängig von ihrem Format oder ihrer Beschaffenheit, mit einem Server zu synchronisieren. Man unterscheidet hierbei zwischen Dateien, die der Allgemeinheit (anderen Benutzern des gleichen Netzes) zugänglich sind, und nutzerspezifischen Dateien, die überall verfügbar sein sollen. Der erste Fall wird oft unter dem Begriff „Öffentliche Ordner" geführt.

Bei der Evaluation der Synchronisationssoftware wird außer Acht gelassen, dass einige der Anforderungen aufgrund von Beschränkungen *auf Endgeräteseite* nicht erfüllt werden können, da dies nicht auf Mängel der Synchronisationssoftware zurückzuführen ist.

3.1.2.2 Mobile Information Server + Internet Security & Acceleration Server

- Hersteller: Microsoft
- Version: 2002 Enterprise (MIS), 2000 (ISA)
- Homepage: http://www.microsoft.com/miserver
  http://www.microsoft.com/ISAServer
- Sprache: Deutsch
- Preis: variables Lizenzmodell, Projektgeschäft
- Getestet: ja

Da Microsoft sowohl für die von uns betrachtete Groupware als auch für das auf den Endgeräten laufende Betriebssystem Pocket PC 2002 verantwortlich ist, lag die Entscheidung nahe, bei diesem Hersteller auch nach einer Lösung für das hier gegebene Szenario zu suchen. Als potentielle Microsoft-Lösung für unsere Aufgabenstellung war der „Microsoft Mobile Information Server (MIS)" verfügbar. Da in unserem Gesamtkonzept eine DMZ nebst Schicht-7-Proxy vorgesehen war, nutzten wir außerdem den „Microsoft Internet Security and Accelaration Server (ISA)". Die Kombination dieser beiden Programme wird vom Hersteller für eine mit dem hier betrachteten Szenario vergleichbare Aufgabenstellung explizit vorgeschlagen. Für beide Produkte steht auf der Microsoft Homepage eine Testversion zur Verfügung.

3.1.2.3 Extended Connect Server

- Hersteller: Extended Systems
- Version: 3.6
- Homepage: http://www.extendedsystems.de
- Sprache: Englisch
- Preis: 20.000,- € zzgl. Kosten für jeden Client gestaffelt nach Anzahl (z.B. 12.500,- € für 100 Clients)
- Getestet: ja

Der Extended Connect Server unterstützt eine Vielzahl von Endgerätetypen und erfüllt laut Herstellerangaben die meisten der oben genannten Anforderungen. Sehr positiv erschien uns die Tatsache, dass das Programm inklusive einer Proxy-Komponente für die Installation in einer DMZ (demilitarisierte Zone) ausgeliefert wird.

Auch von dieser Software stand eine Testversion zur Verfügung. Neben den bereits genannten Punkten bietet der Extended Connect Server zusätzlich ein gewisses Ausmaß administrativer Funktionen, was ihn besonders interessant erscheinen ließ. Nicht zuletzt unterstützt der XTND-Server auch die Groupware Lotus Domino. Dadurch stehen weitere Optionen offen als die ausschließliche Nutzung von Microsoft Produkten.

3.1.2.4 IntelliSync Server

- Hersteller: Pumatech
- Homepage: http://www.pumatech.de
- Sprache: Englisch
- Preis: aus Website nicht ersichtlich, nur auf Anfrage, Projektgeschäft
- Getestet: nein

Die aus der Web-Präsenz des Herstellers von „IntelliSync" verfügbaren Informationen über die Produktpalette beschränkten sich im Wesentlichen auf eine Desktop-Synchronisationslösung. Weitere Einzelheiten waren nur durch Telefonate zu erfahren. Die Möglichkeiten, eine Testversion für unsere Zwecke zu nutzen, waren ebenfalls stark eingeschränkt. In tiefergehenden technischen Gesprächen stellte sich außerdem heraus, dass die Synchronisation öffentlicher Ordner nicht im benötigten Umfang unterstützt wird. Ebenso steht derzeit weder eine Proxy-Komponente zur Verfügung noch ist deren Entwicklung in Planung. Dieses Produkt wurde deshalb nicht in das Testfeld aufgenommen.

3.1.3 Endgerätesoftware

Auch wenn die hier betrachteten Endgeräte bereits bei Auslieferung mit zahlreichen Programmen ausgestattet sind, machen verschiedene insbesondere die Authentifikation und die Datensicherheit betreffende Aspekte die Verwendung zusätzlicher Software unabdingbar. Im Rahmen des Projektes haben wir daher zusätzliche Endgerätesoftware verschiedener Kategorien auf den sinnvollen Einsatz hin evaluiert. Insbesondere betraf dies Software, mittels derer die Sicherheit der Endgeräte gesteigert werden kann. So bietet selbst der Hersteller der Handhelds[4], ebenso wie etablierte große Internetportale[5], umfangreiche Listen mit Empfehlungen für Zusatzsoftware im Bereich der Sicherheit.

3.1.3.1 Sicherheitssoftware

Um hohen Sicherheitsanforderungen Rechnung zu tragen muss insbesondere die Sicherheit der verwendeten mobilen Endgeräte und der dort gelagerten Daten gewährleistet werden. Für Notebooks mit dem Betriebssystem Windows 2000 existieren hierzu etablierte Lösungen aufgrund derer ein hinreichender Schutz sensitiver Daten gewährleistet werden kann. Das Dateisystem von Windows 2000 ist für den Mehrbenutzerbetrieb ausgelegt und stellt somit bereits von Hause aus ein gewisses Maß an Datensicherheit bereit.

Dies verhält sich in Bezug auf die hier betrachteten Geräte anders. Pocket-PCs[6] sind mit dem Betriebssystemkern Windows CE 3.0 ausgestattet, der weder über eine Benutzerverwaltung noch über andere Methoden zum Schutz der gespeicherten Daten verfügt. Alle auf dem Gerät abgelegten Daten befinden sich unverschlüsselt im internen Speicher. Dies hat zur Folge, dass die auf einem entwendeten oder liegen gelassenen Gerät befindlichen Daten in unbefugte Hände gelangen können. Selbst wenn es einem Angreifer nicht gelänge die systemeigene Anmeldeprozedur zu umgehen, kann er das Gerät aufschrauben und sich so physischen Zugriff auf den internen Speicher verschaffen, um diesen dann auszulesen. Die Sicherheit des Dateisystems ist aufgrund des Fehlens jeglicher Schutzmechanismen nicht gegeben und muss unbedingt durch andere Maßnahmen sichergestellt werden[7].

Ziel 1: Erhöhen der Datensicherheit durch Verschlüsselung.

Einen weiteren Sicherheitsmangel stellen bestimmte Eigenschaften der Authentifikation des Benutzers dem System gegenüber dar. Zum einen ermöglicht das Betriebssystem Windows CE 3.0 das komplette Abschalten der Passworteingabe durch den jeweiligen Benutzer, zum anderen ist die Verwendung einer nur vierstelligen, ausschließlich numerischen PIN, problematisch. Da zudem auf dem Eingabefeld lediglich zehn (0...9) verschiedene Eingabefelder noch dazu in numerisch aufsteigend geordneter Position existieren, lässt sich durch einen Beobachter allein durch Betrachtung des Bewegungsablaufes während der Anmeldung leicht herausfinden, welche Ziffern gedrückt werden. Hier würde eine zufällige Anordnung der Zahlenfelder auf dem Display bereits eine deutlich erhöhte Sicherheit gewährleisten. Außerdem verfügt die Standardanmeldung per numerischer PIN für Windows CE 3.0 nicht über ein effektives Verfahren zur Verhinderung von Brute-Force-Angriffen durch simples Ausprobieren aller 10.000 möglichen Ziffernkombinationen. Es existiert zwar eine nach jeder Falscheingabe länger werdende Verzögerung, e, ein Mechanismus zum automatischen Löschen aller auf dem PDA gespeicherten Daten nach einer bestimmten Anzahl falscher Eingaben ist jedoch im Auslieferungszustand des Gerätes nicht verfügbar.

---

[4] Siehe dazu „iPAQ Pocket PC solutions catalog" (SOL 2002).
[5] Z. B. http://www.pocket.at/pocketpc/software.htm [27.03.2003].
[6] Hier Pocket PC 2002.
[7] Siehe dazu auch „Pocket PC 2002 Security" (Herrera 2002).

Eine unsichere und überwindbare Anmeldeprozedur stellt nicht nur eine Gefahr für auf dem Gerät befindliche Daten dar. „Jedes mobile Gerät ist nicht nur selbst durch nicht autorisierten Zugriff gefährdet, sondern stellt auch einen Weg in die Systeme zur Verfügung, mit denen es verbunden ist. Indem er als ein registrierter Benutzer erscheint, kann der unberechtigte Benutzer Daten stehlen oder die Sicherheit des Systems auf andere Weise verletzen." (Dedo 2002, S. 4)

Die Sicherheit der Anmeldeprozedur muss also durch weitergehende Maßnahmen auch erhöht werden, um einen wirksamen Schutz der auf dem Gerät liegenden sensitiven Daten sicherzustellen.

Ziel 2: Erhöhen der Datensicherheit durch verbesserte Anmeldeprozedur.

Auf dem Markt werden diverse Lösungen angeboten, die die Erfüllung der hier definierten Anforderungen an die Endgerätesicherheit für Geräte der Pocket-PC-Klasse gestatten. Sie basieren auf sehr unterschiedlichen Herangehensweisen und unterscheiden sich auch im Funktionsumfang stark. Da diese Programme alle in zentralen Bereichen des Betriebssystems arbeiten, sind sie nicht miteinander kombinierbar – es kann nur immer eine der hier vorgestellten Lösungen auf dem Endgerät aktiv sein.

Einige der verfügbaren Produkte werden im Folgenden kurz beschrieben und die Gründe für deren Aufnahme in Testbetrieb und Evaluation dargelegt. Mittels des in Kapitel 4.1.5 vorgestellten Evaluationskonzeptes ist es außerdem möglich, von uns nicht getestete Software einer Evaluation zu unterziehen.

3.1.3.1.1 PDASecure Premium (Trust Digital)

Das Programm PDASecure Premium verspricht Dateiverschlüsselung ausgewählter Dateien mit wählbaren Algorithmen und Schlüssellängen zwischen 128 und 512 Bit. Die Anmeldeprozedur von Windows CE wird durch eine eigene ersetzt, mittels derer auch Infrarot- und ActiveSync-Verbindungen authentifiziert werden. Weiterhin verspricht der Hersteller Trust Digital zur Verhinderung von Brute-Force-Angriffen Sicherheitsmechanismen für den Fall zu häufiger fehlerhafter Anmeldungen. PDASecure Premium ist nur in englischer Sprache verfügbar. Da diese Lösung sowohl Verschlüsselung als auch den Austausch der Anmeldeprozedur bietet, wurde sie in das Evaluationsfeld aufgenommen.

- Hersteller: Trust Digital
- Version: 1.0
- Website: http://www.trustdigital.com/prod15b.htm
- Sprache: Englisch
- Kosten: 39,95 USD
- Getestet: ja

3.1.3.1.2 FileCrypto - Enterprise Edition (F-Secure)

FileCrypto aus dem Hause F-Secure ist eine bereits mehrfach ausgezeichnete Sicherheitssoftware. Der Hersteller verspricht transparente Echtzeitverschlüsselung sowohl von PIM-Daten und E-Mails als auch von ausgewählten Dateien und Ordnern mittels eines FIPS[8]-zertifizierten Verschlüsselungskerns. Auch FileCrypto ersetzt die systemeigene Anmeldung durch eine eigene. Der Hersteller F-Secure verfügt über lange Erfahrungen im Bereich der Sicherheitssoftware und ist auch in den Bereichen Desktop- und Notebook-

[8] Federal Information Processing Standard 140-1 – Kryptografischer Standard der US-Regierung.

Sicherheit präsent und anerkannt[9]. FileCrypto ist sowohl in deutscher als auch in englischer Sprache erhältlich und wurde ebenfalls in das Testfeld aufgenommen, da sowohl Verschlüsselung als auch Austausch der Anmeldeprozedur zur Verfügung stehen.

- Hersteller: F-Secure
- Version: 2.01
- Website: http://www.f-secure.com/wireless/pocketpc/pocketpc-fc.shtml
- Sprache: Englisch, Deutsch
- Kosten: 76,20 €
- Getestet: ja

3.1.3.1.3 SafeGuard PDA - Personal Edition (Utimaco)

SafeGuard PDA legt einen deutlichen Schwerpunkt auf die Verbesserung der Anmeldeprozedur u. a. durch Handschriftenerkennung und bietet nach Herstellerangaben auch die Option der Verschlüsselung der auf dem PDA befindlichen Daten. Die Software wurde uns vom Hersteller der Administrationssoftware Afaria (siehe Kap. 3.1.1.2) empfohlen. SafeGuard PDA wurde ebenfalls evaluiert.

- Hersteller: Utimaco
- Version: 1.00.1.2
- Website: http://www.utimaco.de
- Sprache: Deutsch
- Kosten: 62,24 €
- Getestet: ja

3.1.3.1.4 movianCrypt (Certicom)

MovianCrypt bietet ebenfalls sowohl Datenverschlüsselung als auch den Austausch der Anmeldeprozedur und die Authentifikation für Infrarot- und ActiveSync-Verbindungen. Auch movianCrypt hat einen FIPS[10]-zertifizierten Verschlüsselungskern und wurde in das Testfeld aufgenommen.

- Hersteller: Certicom
- Version: 1.1
- Website: http://www.certicom.com
- Sprache: Englisch
- Kosten: 50,00 USD, minimal 50 Lizenzen, bei größeren Mengen sukzessive preiswerter
- Getestet: ja

3.1.3.1.5 Pointsec for PocketPC 1.3 (Pointsec)

Obwohl der Hersteller Pointsec bereits die angekündigte Version 2.0 massiv bewirbt, war es uns nicht möglich, zu Evaluationszwecken eine Vorabversion zu erhalten. Deshalb konnte nur die Version 1.3 in unser Testfeld aufgenommen werden. Pointsec wird im Gegensatz zu den anderen beschriebenen Lösungen mit Hardware-Tokens[11] ausgeliefert. Eine weitere Besonderheit an Pointsec ist die Möglichkeit der Integration der Software in den XTND-Server (s. Kap. 3.1.1.1). Dies und die Tatsache, dass auch Pointsec sowohl

---

[9] Zu Pressestimmen siehe auch: http://www.f-secure.com/news/awards/index.shtml [07.04.2003].

[10] Federal Information Processing Standard 140-1 – Kryptografischer Standard der US-Regierung.

Verschlüsselung als auch eine verbesserte Anmeldung bietet, führten zur Aufnahme dieser Software in das Testfeld.

- Hersteller: Pointsec
- Version: 1.3
- Website: http://www.pointsec.com/solutions/solutions_pocketpc.asp
- Sprache: Englisch
- Kosten: 120,00 €, Mindestabnahme: 100 Lizenzen
- Getestet: ja

3.1.3.1.6 PDA Defense Enterprise (Asynchrony)

Auch PDA Defense Enterprise bietet sowohl Verschlüsselung als auch den Austausch der Anmeldeprozedur. Als besonderes Merkmal stellt PDA Defense Enterprise einen Mechanismus bereit, der den jeweiligen Nutzer zwingt, sein Passwort nach einem festgelegten Zeitraum zu ändern. Bereits verwendete Passwörter werden gespeichert, so dass sie nicht nochmals verwendet werden können. Zusätzlich bietet es eine Komponente zur Verwaltung von Sicherheits-Policies.

- Hersteller: Asynchrony
- Version: 3.1.030321
- Website: http://www.pdadefense.com
- Sprache: Englisch
- Kosten: 29,95 USD
- Getestet: ja

3.1.3.1.7 Sign On (CIC)

Sign-On stellt eine Ausnahme unter den hier aufgeführten Lösungen dar. Es bietet keine Funktionen zur Verschlüsselung, sondern ersetzt lediglich die systemeigene Anmeldung durch eine eigene. Nur eines der festgelegten Ziele wird also verfolgt. Die von Sign-On verwendete Anmeldeprozedur basiert jedoch auf Handschriftenerkennung und stellt somit einen biometrischen Zugangsschutz zum PDA dar. Da sich die im Testfeld bereits vertretenen biometrischen Verfahren als mangelhaft und überwindbar erwiesen, wurde Sign-On nachträglich in das Testfeld aufgenommen, obwohl die Software keine Funktionen zur Datenverschlüsselung bietet.

- Hersteller: CIC
- Version: 2.01
- Website: https://secure.cic.com/product_details/signonpocket_details.asp
- Sprache: Englisch
- Kosten: 19,99 USD
- Getestet: ja

---

[11] Vom Erscheinungsbild her mit kleinen Taschenrechnern vergleichbare Geräte, die nach Eingabe einer Zahl aus dieser nach einem für den Benutzer unbekannten Verfahren eine Antwort generieren, mittels derer der Benutzer sich einem Programm gegenüber identifizieren kann (Challenge-Response-Verfahren).

3.1.3.2 Antiviren-Software

Betriebssystem und Software der hier betrachteten PDAs haben mittlerweile einen Leistungsumfang erreicht, in dem es notwendig ist, das System mit einem verlässlichen Virenschutz auszustatten. Es ist auffällig, dass gerade die etablierten Hersteller aus dem Bereich Desktop-Virenschutz derzeit keinen Schutz für Pocket-PCs anbieten.

Dennoch existieren Virenschutzprogramme für Pocket-PCs auf dem Markt, von denen wir hier nur diejenigen aufführen, die direkt auf dem mobilen Gerät installiert werden. Lösungen, die lediglich auf dem Companion-PC installiert werden und bei jedem Synchronisationsvorgang die auf dem PDA befindlichen Daten auf Virenbefall überprüfen, sind für das hier angestrebte Szenario der serverbasierten Synchronisation nicht zweckmäßig und bleiben daher außen vor.

Auf eine Evaluation in Bezug auf die Leistungsfähigkeit/Erkennungsrate wurde generell verzichtet.

3.1.3.2.1 Antivirus for PocketPC (F-Secure)

Antivirus for PocketPC ist, ebenso wie die Sicherheitslösung FileCrypto vom Hersteller F-Secure, eine weit verbreitete Antivirus-Lösung für die Plattform Pocket-PC. Die Software läuft auf dem mobilen Gerät und ist somit in der Lage, schadhafte Dateien zu erkennen, bevor sie aktiv werden. Zumindest der Desktop-Version dieser Software wird eine besonders hohe Virenerkennungsrate bestätigt[12]. Insbesondere die Tatsache, dass bereits eine Sicherheitssoftware aus dem Hause F-Secure in unser Testfeld aufgenommen wurde sowie die bestätigte hohe Erkennungsrate der Desktop-Version ließen uns Antivirus for PocketPC auf den Testgeräten installieren.

- Hersteller: F-Secure
- Version: 1.5
- Website: http://www.f-secure.com/wireless/pocketpc/pocketpc-av.shtml
- Sprache: Englisch
- Kosten: 36,00 USD
- Getestet: ja

3.1.3.2.2 PC-Cillin Wireless (Trend Micro)

Die PDA-Komponente PC-Cillin Wireless ist Bestandteil der Antivirus-Suite PC-Cillin 2003. Auch PC-Cillin Wireless läuft direkt auf dem PDA und kann daher aktiv werden, bevor von einem Virus Schaden verursacht werden kann. Die Verbreitung scheint geringer als jene von Antivirus for PocketPC zu sein. PC-Cillin Wireless stellt kein eigenständiges Produkt dar, sondern ist lediglich als „Beigabe" zu einer Antivirus-Lösung für Desktop-PCs anzusehen. Wir verzichteten deshalb auf eine Evaluation von PC-Cillin.

- Hersteller: Trend Micro
- Website: http://www.trendmicro.com/en/products/desktop/pcc-wireless/evaluate/overview.htm
- Sprache: Englisch, Deutsch
- Kosten: 49,00 €
- Getestet: nein

---

[12] Siehe: http://www.f-secure.com/news/items/news_2003021401.shtml [25.03.2003]. Sowie: http://www.virusbtn.com/vb100/archives/tests.xml?200206 [25.03.2003].

3.1.3.2.3 ETrust Antivirus 7.0 (Computer Associates)

ETrust Antivirus 7.0 stellt eine komplette Antiviren-Suite dar, die Virenschutz vom PDA bis zum Internet-Gateway verspricht. Eine Verwendung dieser Lösung erscheint uns nur im Zusammenspiel mit einer auch auf den verschiedenen Servern genutzten kompletten eTrust-Lösung sinnvoll. Wir entschieden uns deshalb gegen den Testbetrieb von ETrust Antivirus.

- Hersteller: Computer Associates
- Website: http://ca.com
- Sprache: Englisch, Deutsch
- Kosten: 49,00 €
- Getestet: nein

3.1.3.3 Weitere Software

Neben den Bereichen Verschlüsselung/Zugangsschutz und Virenschutz existieren noch weitere, zum Teil sehr umfangreiche Produkte, die die Verwendungsmöglichkeiten für Pocket-PCs zum Teil sehr stark erweitern. Wir haben diese aufgrund des teilweise immensen Aufwands nicht getestet, sie seien jedoch der Vollständigkeit halber an dieser Stelle zumindest erwähnt und kurz beschrieben.

3.1.3.3.1 Mobility (Netmotion)

Die Software Mobility dient dazu, mit mobilen Endgeräten und für den Nutzer transparent und ohne Verbindungsabbruch zwischen verschiedenen Netzen (WLAN, GPRS, GSM, etc.) je nach Verfügbarkeit wechseln zu können. Der Hersteller verspricht also, dass eine Verbindung, die in einem mit WLAN ausgestatteten Zug aufgebaut wurde, auch nach dem Aussteigen nicht abgebrochen, sondern nach Umschalten auf eine GPRS-Verbindung fortgesetzt wird.

Netmotion führt jedoch auf den firmeneigenen Webseiten keine Referenzen auf, so dass es schwer ist, die Alltagstauglichkeit dieser Lösung nachzuvollziehen. Auch war der Hersteller nicht ohne weiteres bereit, uns Preise für diese Lösung mitzuteilen, da die Software offensichtlich nur im Rahmen von Projektverträgen vertrieben wird. Netmotion Mobility wurde von uns nicht getestet.

- Hersteller: Netmotion Wireless
- Website: http://www.netmotionwireless.com
- Sprache: Englisch
- Kosten: unklar
- Getestet: nein

3.1.3.3.2 Trusted Mobility Suite - Enterprise Edition (Trust Digital)

Neben der bereits erwähnten Lösung PDASecure bietet der Hersteller Trust Digital auch die Trusted Mobility Suite an. Die Trusted Mobility Suite baut im Wesentlichen auf dem Trusted Mobility Server auf, mittels dessen ein zentrales Security-Management möglich sein soll. Unsere mehrfachen Nachfragen bezüglich dieses Produktes blieben unbeantwortet. Auch hier wird offensichtlich nur von Projektpreisen ausgegangen und kein definitiver Preis angegeben. Die Mobility Suite blieb ebenfalls ungetestet.

- Hersteller: Trust Digital
- Website: http://www.trustdigital.com
- Sprache: Englisch
- Kosten: unklar
- Getestet: nein

3.1.4 Groupware

In Zusammenarbeit mit dem Auftraggeber wurde als zu untersuchende Groupware Microsoft Exchange festgelegt. Lotus Domino / Notes wurde nicht näher betrachtet.

3.1.4.1 Exchange

Für das Projekt wurde die Version 2000 eingesetzt. So verlangt z. B. der im Rahmen der Synchronisation untersuchte Mobile Information Server ein Active Directory gestütztes System, mit dem erst Exchange 2000 umgehen kann.

Exchange 5.5

- Hersteller: Microsoft
- Website: http://www.microsoft.com/exchange
- Sprache: Deutsch
- Eingesetzt: nein

Exchange 2000

- Hersteller: Microsoft
- Website: http://www.microsoft.com/exchange
- Sprache: Deutsch
- Eingesetzt: Ja

3.1.4.2 Lotus

Das Lotus-Domino / Notes – System ist theoretisch eine Alternative zu Exchange, wurde jedoch noch in der Vorbereitungsphase ausgeschlossen.

- Hersteller: IBM
- Website: http://www.lotus.com
- Sprache: Deutsch
- Eingesetzt: Nein

3.1.5 Netzwerkkomponenten

In den folgenden Unterkapiteln werden die verwendeten Netzwerkkomponenten beschrieben. Im Einzelnen sind dies:

- RAS-Komponenten
- VPN-Verbindungen
- Firewall-Komponenten.

3.1.5.1 RAS

In unserem Testlabor ermöglichen wir nach Vorgaben des Auftraggebers die RAS-Einwahl direkt in die demilitarisierte Zone (DMZ).

Die technische Realisierung der RAS-Einwahl erfolgt in unserem Testlabor über den „Windows RAS- und Routing-Dienst" von Windows 2000. Aus technischen Gründen haben wir

ein Modem an den Rechner angeschlossen. Für die Authentifizierung wird ein lokal eingerichtetes Benutzerkonto benutzt. Der Anschluß einer ISDN-Karte wäre selbstverständlich ebenfalls möglich und würde ein zusätzliches Sicherheitsmerkmal in Form einer Rufnummerauthentifizierung ermöglichen.

3.1.5.2 VPN

Im Rahmen des Projektes kam die vom Auftraggeber vorgegebene VPN-Lösung bestehend aus einem VPN Server und einem VPN Client inklusive Clientmanager zum Einsatz.

3.1.5.3 Firewall

Anfänglich wurden im Testlabor provisorisch zwei Linux-Paketfilter eingesetzt, die die DMZ nach innen und außen schützten. Im weiteren Verlauf des Projekts wurde zusammen mit dem Auftrageber entschieden, auf einen kombinierten ALG- und Paketfilter umzusteigen.

Dieses Firewallsystem hat gegenüber der Linux-Lösung mehrere Vorteile:

- Höherer Schutz durch Application Level Gateway (ALG)
- ALG und Paketfilter als zwei separate Systeme, kombiniert in einem Gehäuse mit einem Administrationsinterface
- Zertifiziert durch das BSI[13] (ITSEC E3 hoch).

Gegenüber der Linux-Lösung stellt dieses Produkt allerdings höhere Anforderungen an die Systemadministration, denn der Application Level Gateway erzwingt, dass die Verbindungen über speziell dafür eingerichtete und konfigurierte Proxies vermittelt werden.

3.1.6 Sonstige Software

3.1.6.1 Betriebssysteme

Als Betriebssystem der Server wurde der Microsoft Windows 2000 Advanced Server mit dem Servicepack 3 eingesetzt. Windows 2000 basiert auf der Microsoft NT-Technologie. Mit umfassenden, bereits eingebauten Diensten, Skalierbarkeit und hoher Leistungsfähigkeit liefert Windows 2000 eine zuverlässige Plattform für Netzwerkanwendungen.

Windows 2000 ist ein Multiuserbetriebssystem. Es ist mehren Personen gleichzeitig über separate Benutzerkonten und Passwörter möglich, dieses System zu nutzen. Eine Weitergabe der hoch sensiblen Passwörter im Bereich der Netzwerkinfrastruktur ist somit nicht notwendig. Ein weiter Vorteil besteht darin, dass Änderungen am System nachvollzogen werden können. Windows 2000 kann über einen gesicherten Zugang auch fernadministriert werden. Dies stellt eine erhebliche Erleichterung im Arbeitsablauf der Administratoren dar. Als Filesystem verwendet Windows 2000 das NTFS (new technology file system). Besonders auf großen Festplatten bringt NTFS Vorteile: Die Dateien werden weitgehend unfragmentiert (d. h. geordnet) gespeichert, deswegen bleibt die Geschwindigkeit auch bei einer Vielzahl von Schreibzugriffen relativ hoch. Die maximale Größe der Partitionen liegt bei vier TeraByte, diese Obergrenze reicht für alle Zwecke auch innerhalb großer

[13] Siehe http://www.genua.de/news/presseinfo/presse/pi_zerti_html [08.04.2003].

und komplexer Systeme aus. NTFS ermöglicht darüber hinaus eine Überwachung aller Dateizugriffe.

Einer der essentiellen Dienste des Windows 2000 Advanced Server ist Active Directory. Es bietet Organisationen einen Directory-Service, der dafür entworfen wurde Informationen über Netzwerkressourcen und Benutzer zentral zu verwalten und zu verteilen. Auch andere Systembestandteile können so auf die zentral verwalteten Benutzerinformationen wie Passwörter und Gruppenzugehörigkeiten zurück greifen.

Zusätzlich zur Bereitstellung eines Directory-Service in einer Windows-Umgebung ist Active Directory dazu vorgesehen, Verzeichnisse zentral zu verwalten.

- Hersteller: Microsoft
- Version: 2000
- Website: http://www.microsoft.de
- Sprache: Deutsch, Englisch

3.1.6.2 ActiveSync

ActiveSync ist die Synchronisationskomponente, die Microsoft als Standard für PocketPC-Handhelds entwickelt hat. Es ist Bestandteil der Grundausstattung der Handhelds und verbindet im Normalfall Microsoft Outlook auf dem Companion-PC mit Pocket Outlook auf dem Handheld und synchronisiert die gewünschten Daten. Die dazu benötigte ActiveSync Komponente für den Companion-PC liegt dem Handheld ebenfalls auf einem Datenträger bei. Für weitergehende Informationen zu ActiveSync siehe auch Kapitel 4.3. Gegen Ende des Projektes aktualisierte Microsoft das Produkt auf die Version Nummer 3.6. Diese Aktualisierung wurde auch im Projekt vorgenommen, da die neue Version einige Verbesserungen brachte.

Soll jedoch über ActiveSync eine Verbindung nicht mehr mit einem Microsoft Outlook, sondern mit einem Exchange Server aufgebaut werden, so reicht das mitgelieferte ActiveSync auf Serverseite nicht mehr aus. Der Mobile Information Server von Microsoft liefert deshalb als Verbindung zwischen Exchange und Handheld das Microsoft Server Active Sync mit.

Als grundlegende Synchronisationskomponente ist Active Sync an vielen zentralen Stellen im Projekt im Einsatz.

- Hersteller: Microsoft
- Version: 3.5/3.6
- Website: http://www.microsoft.de
- Sprache: Deutsch, Englisch

3.2 Hardware

3.2.1 Endgeräte

Im Rahmen des Projektes wurden als beispielhafte Endgeräte der PocketPC Klasse Handhelds von Hewlett Packard (HP) ausgewählt. Zum Einsatz kamen dabei der weit verbreitete iPAQ H3970 und auch der kurz zuvor entwickelte Biometrie iPAQ H5450. Die iPAQ Handhelds Serie stammt ursprünglich vom Hersteller Compaq, der vor wenigen Jahren mit HP fusionierte.

3.2.1.1 iPAQ H3970

Der iPAQ H3970 stellte zum Start des Projektes die modernste Ausstattung und das Spitzenprodukt aus der Reihe der iPAQs dar. Die Standardaustattung des iPAQ H3970 schließt Infrarot und Blutooth ein.

- Hersteller: HP
- Website: http://h71010.www7.hp.com/produkte/handheld
- Sprache: Deutsch
- Kosten: ca. 750,- €[14]

3.2.1.2 iPAQ H5450

Der neue iPAQ H5450 wurde uns, wie oben erwähnt, vor Markteinführung zur Verfügung gestellt. Besonderheit dieses Gerätes ist der thermische Fingerabdruckscanner, der Hoffnung auf eine einfache und zuverlässige Benutzerauthentifikation machte. Außerdem verfügt der H5450 über eine eingebaute W-LAN Karte.

- Hersteller: HP
- Website: http://h71010.www7.hp.com/produkte/handheld
- Sprache: Deutsch
- Kosten: ca. 900,- €[15]

3.2.1.3 Wireless-Pack für GSM/GPRS

Das Wireless-Pack oder auch „Rucksack"-Modul ergänzt den iPAQ um Mobilfunkfähigkeiten. Mit einer entsprechenden SIM-Karte wird es damit möglich, sich über GSM oder GPRS einzuwählen. Diese Fähigkeit ist z. B. wichtig, um eine Verbindung ins Internet aufbauen oder die angestrebte RAS-Einwahl realisieren zu können.

- Hersteller: HP
- Website: http://h71010.www7.hp.com/produkte/handheld
- Sprache: Deutsch
- Kosten: ca. 480,- €[16]

[14] Stand April 2003.
[15] Stand April 2003.
[16] Stand April 2003.

3.2.2 Server

Zur Simulation der serverseitigen Infrastruktur wurden Desktop PCs eingesetzt.

Die Rechner müssen sowohl für die Simulation als auch für den Einsatz in der realen Infrastruktur genügend Kapazitäten aufweisen. Die Kapazitäten müssen in den Bereichen Rechenleistung, Arbeitsspeicher und Festspeicher den Ansprüchen angepasst sein.

Bei der Simulation besteht im Gegensatz zur Realität ein geringerer Bedarf an diesen Kapazitäten, da das Simulationssystem mit wesentlich weniger Nutzern betrieben und somit auch mit geringerem Traffic belastet wird. Die vier Rechner für die Laborsimulation wurden identisch ausgestattet, so mit „Pentium 4" Prozessoren, zwei Netzwerkkarten und zwei Festplatten.

4 Evaluation

Die in den bisherigen Kapiteln beschriebenen Vorgänge dienten der Vorbereitung der Evaluation. Zu Beginn wurden die Aufgaben und Ziele des Projektes definiert, anschließend die möglichen Systemarchitekturen auf ihre Verwendbarkeit hin untersucht und die zu evaluierenden Komponenten identifiziert. Dieses Kapitel beschreibt nun die Evaluation selbst und bildet den Kernteil des Berichtes.

Im ersten Unterkapitel 4.1 wird die Entwicklung des Konzeptes zur Evaluation vorgestellt und ein Einblick in die im Projekt benutzte Arbeitsmethodik gegeben. Danach folgen die drei Abschnitte über die Evaluation der Komponenten

- Administrationssoftware (Kapitel 4.2)
- Synchronisationssoftware (Kapitel 4.3)
- Sicherheitssoftware für Handhelds (Kapitel 4.4).

4.1 Grundlagen

4.1.1 Sicherheitskonzept

Die Arbeit in einem Testlabor bedarf umfangreicher Sicherheitsmaßnahmen, um Schaden durch fehlerhafte Software oder fehlgeschlagene Tests zu vermeiden. Wichtig ist dabei insbesondere der systematische Aufbau der Testkonfigurationen, die nur die wirklich benötigten Komponenten in der dafür nötigen Konfigurationen enthalten. So können Störungen, die nicht auf den Kernbestandteilen des Systems beruhen, vermieden werden bzw. leichter ihrer Ursache zugeordnet werden. Eine Laborkonfiguration erfüllt also genau spezifizierte Aufgaben. Im Testlabor ist zudem die Durchführung unterschiedlicher Testszenarien zu erwarten. Eine Möglichkeit, schnell zwischen verschiedenen Konfigurationen zu wechseln, würde das Arbeiten im Testlabor erheblich erleichtern.

4.1.1.1 Backupstrategie

Zur Sicherung funktionierender Systemkonfigurationen und zum Wiederherstellen einer älteren Konfiguration z. B. bei Datenverlusten wird das Produkt „Norton Ghost 2003“[17] des Herstellers Symantec verwendet. Mittels Norton Ghost kann man ganze Festplatten oder bestimmte Partitionen als Imagedatei sichern. Wird ein solches Image zur Wiederherstellung benutzt, befindet sich die entsprechende Festplatte bzw. Partition danach wieder in exakt dem Zustand wie zum Zeitpunkt der Sicherung. Inzwischen neu hinzugekommene Daten werden bei der Wiederherstellung vernichtet.

Der große Vorteil der Ghost-Lösung besteht in der Möglichkeit, außerhalb des eigentlichen Betriebssystems auf dem entsprechenden Rechner agieren zu können. Mittels einer Bootdiskette, die den Rechner hochfährt und Norten Ghost startet, können völlig unabhängig vom installierten Betriebssystem Backups erstellt werden. Ghost kann sowohl mit Linux als auch Windowspartitionen umgehen. Die Benutzung des Programms wurde im Rahmen des Projekts über eine Reihe von Richtlinien geregelt.

---

[17] Siehe http://www.symantec.de/region/de/product/ghost/pe_produkteigenschaften.html [27.03.2003].

4.1.1.2 Wechsel zwischen Szenarien

Durch die über die Backupstrategie über das gesamte Labor hinweg erfolgte Sicherung jeder einmal erreichten funktionierenden Testkonfiguration besteht die Möglichkeit, jedes gewünschte Szenario wiederherzustellen. Dazu muss die gewünschte Konfiguration nur durch Auswahl der entsprechenden Backups auf den Rechnern mittels Norten Ghost wieder hergestellt werden. So werden zeitraubende Neuinstallationen bei einem Wechsel des Szenarios vermieden, und das Labor kann innerhalb kürzester Zeit in jeden beliebigen vorher gesicherten Zustand zurück gebracht werden.

4.1.1.3 Protokollierung

Jeder Rechner verfügt über ein Rechnerdatenblatt, auf dem die Grundkonfiguration festgehalten wird. Die Vorlage dazu findet sich im Anhang in Kapitel 7.2.1. Die Installation von Software findet nach Möglichkeit in Zweierteams statt. Der Beisitzer protokolliert dabei den Installationsverlauf und die genaue Konfiguration des Programms. Wichtige Ereignisse und Masken werden zudem per Screenshot als Bilddatei auf der Backupplatte in dafür vorgesehenen Verzeichnissen gesichert[18]. Für die Erstellung der Screenshots kommt das Programm ScreenCopy[19] von Smartision zum Einsatz, das als Open Source Software kostenlos verfügbar ist.

[18] Die Benennung der Screenshots erfolgt dabei ebenfalls einer vorgegebenen Systematik.

[19] Siehe http://smartision-sc.sourceforge.net/ [27.03.2003].

4.1.2 Die Basiskonfiguration

Der Ausgangspunkt jedes Testszenarios ist die Basiskonfiguration des Labors. Auf ihr aufbauend werden Zielkonfigurationen für die unterschiedlichen Testszenarien entwickelt. Im Rahmen des in Kapitel 4.1.1 beschriebenen Sicherheitskonzeptes wird diese Grundkonfiguration als Backup gesichert.

4.1.2.1 Der Aufbau

Im Kapitel 2 wurden grundlegende Netztopologien vorgestellt. Grundlage der Netzwerkarchitektur ist dabei die Dreiteilung der Netzstruktur in Firewall, demilitarisierte Zone (DMZ) und Intranet.

In der unsicheren Außenwelt versucht der Client, eine Verbindung zu dem im als sicher angenommenen Intranet positionierten Exchangeserver aufzunehmen, um seine E-Mails, Termine, Aufgaben und Kontakte zu synchronisieren. Dazu muss er das Firewallsystem überwinden und in der DMZ eine Proxykomponente ansprechen. Die Dreiteilung findet sich also auch in der im Labor benutzten Struktur des Labornetzes wieder, zu dem der Client Kontakt aufnimmt.

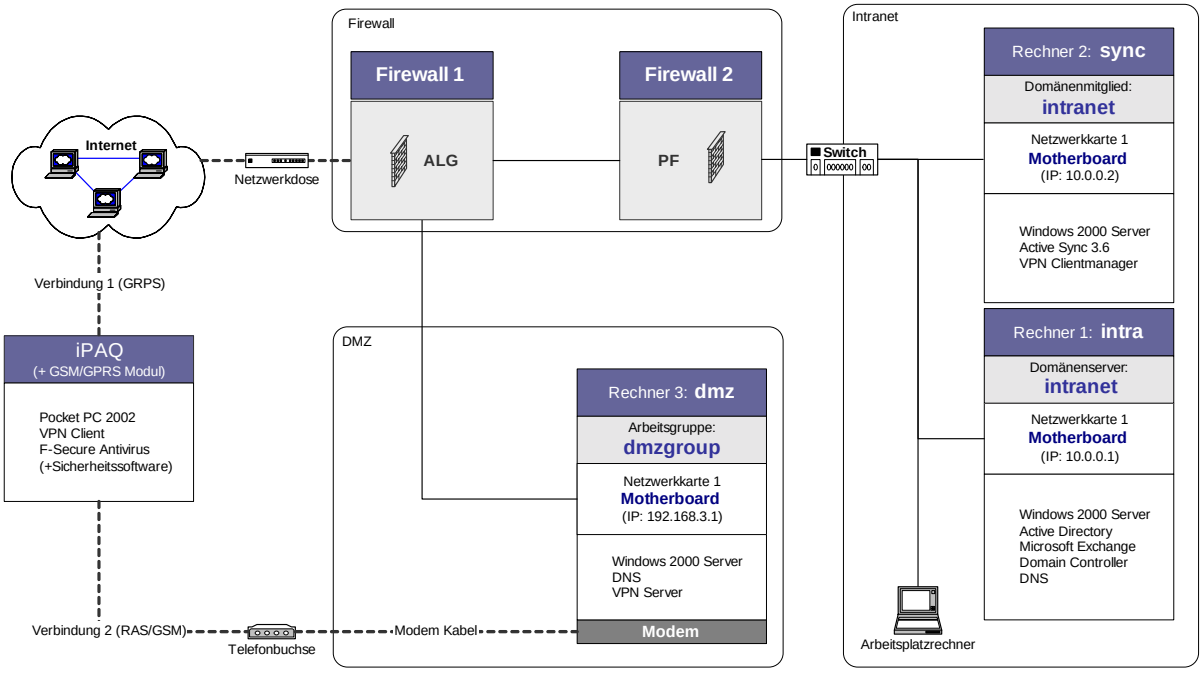

Abbildung 4-1: Labornetzwerk in der Basiskonfiguration

Im Labornetzwerk werden drei Rechner als Server (`dmz`, `sync`, `intra`) und die leihweise zur Verfügung gestellte Firewall verwendet. Das Labor verfügt über einen analogen Telefonanschluss, der über ein 56K V.90 Modem an den Rechner `dmz` angeschlossen ist. Daneben ist der Application Level Gateway) der Firewall mit einer Netzwerkdose des Labors verbunden, der so über das Universitätsnetz Zugang zum Internet hat und auch von außen zu erreichen ist.

4.1.2.2 Softwarekomponenten

4.1.2.2.1 Das Betriebssystem

Auf den 3 Laborservern kommt, wie bereits in Kapitel 3.1.6.1 besprochen, der Microsoft Windows 2000 Advanced Server mit installiertem Service Pack 3 zum Einsatz. Auf dem Rechner `intra` läuft dieser auch als Domainserver und verwaltet das Active Directory. In der demilitarisierten Zone übernimmt der Rechner `dmz` die Aufgabe eines DNS.

4.1.2.2.2 Die Firewall

Die Firewall stellt die Schnittstelle zwischen der Außenwelt und den beiden Labornetzen, der potentiell unsicheren DMZ und dem sicheren Intranet dar.

Folgender Proxy wurde auf dem ALG in der Basiskonfiguration eingerichtet (Im Laufe des Testbetriebes wurden zu Testzwecken noch weitere Proxies benutzt, die später jedoch überflüssig wurden):

Tabelle 4-1: ALG Proxy „Standard VPN"

ALG-Proxy: „Standard VPN“
Daten
Protokoll: UDP Von: Außenwelt (Port 1701) Nach: DMZ (Port 1701)
Beschreibung
Dieser Proxy leitet jede Anfrage aus dem Internet kommend von Port 1701 in die DMZ (Rechner: DMZ) auf Port 1701 weiter .
Zweck
VPN-Strecke von außen über das Internet durch die Firewall in die DMZ, um die Kommunikation der verschiedenen Anwendungen zwischen Client und Proxy zu realisieren (XTND, Afaria, ActiveSync etc.).

4.1.2.2.3 VPN und RAS Konfiguration

Auf dem Rechner `dmz` in der demilitarisierten Zone befindet sich die Serverkomponente der VPN Strecke.

Auf der Clientseite, also dem iPAQ Handheld, müssen der VPN-Client und dessen Verbindungseinstellungen installiert werden. Dies geschieht über das auf dem Rechner `sync` installierte ActiveSync 3.6.

Grundsätzlich werden zwei verschiedene VPN Tunnel benötigt und damit auch zwei verschiedene Verbindungseinstellungen. Beide Tunnel reichen bis zum Rechner `dmz` und umtunneln die Kommunikation der Synchronisations- und Administrationskomponenten mit dem Handheld.

VPN Tunnel aus dem Internet

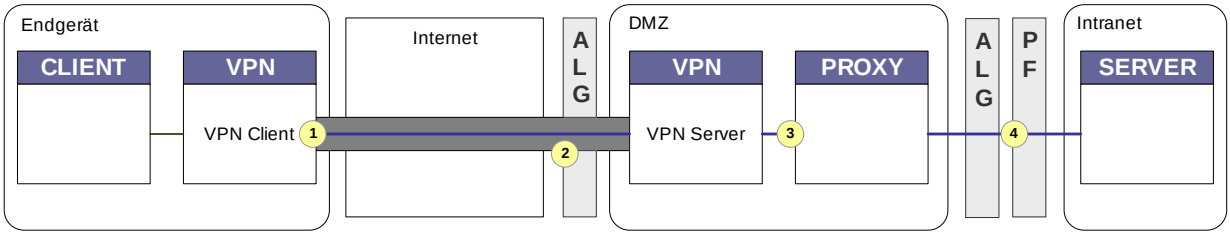

Abbildung 4-2: VPN Tunnel GPRS in DMZ

1. Im ersten Schritt erfolgt, vom Nutzer ausgelöst, bei einem Provider die direkte Einwahl über das GPRS-Netz in das Internet.

2. Über die bestehende Leitung wird der im Internet sichtbare ALG der Firewall angesprochen und ein VPN Tunnel durch das ALG in die DMZ gelegt.

3. Die Pakete des Client[20] auf dem Endgerät gelangen durch den VPN Tunnel in der DMZ zum jeweiligen Proxy.[21]

4. Der Proxy{ XE "Proxy" } trennt die Anfrage auf OSI-Schicht 7 und erzeugt eine neue, sichere[22] Anfrage an den Server[23] im Intranet, die vom Paketfilter als gültig akzeptiert werden muss.

VPN Tunnel über RAS

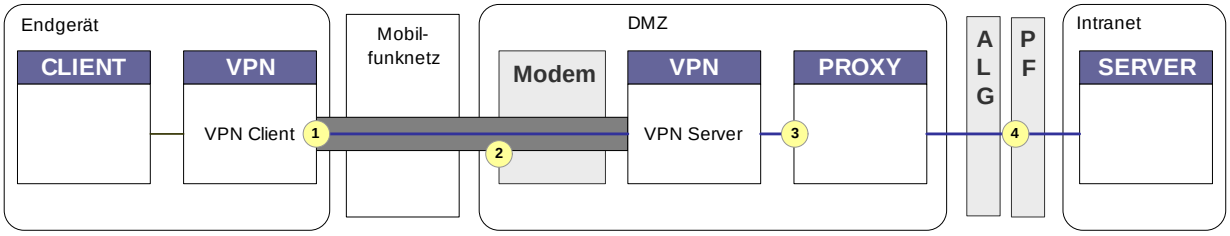

Abbildung 4-3: VPN Tunnel RAS/GSM in DMZ

1. Im ersten Schritt erfolgt, vom Nutzer ausgelöst, die direkte Einwahl über das GSM-Netz in das Modem der DMZ.

2. Über die bestehende Leitung wird ein VPN Tunnel in die DMZ gelegt (Zielrechner ist dabei direkt der Rechner mit dem VPN Server).

3. Die Pakete des Client[24] auf dem Endgerät gelangen durch den VPN Tunnel in der DMZ zum jeweiligen Proxy.[25]

---

[20] Client könnte z. B. der Afaria Client sein. Genauer Client vom Szenario abhängig.
[21] Genauer Proxy z. B. XTND Proxy oder ISA Bestandteil der Evaluation.
[22] möglich wäre hier z. B. eine RSA verschlüsselte Kommunikation über SSL.
[23] Server abhängig vom Evaluationsszenario. Z. B. XTND Connect Server.
[24] Client könnte z. B. der Afaria Client sein. Genauer Client vom Szenario abhängig.
[25] Genauer Proxy z. B. XTND Proxy oder ISA Bestandteil der Evaluation.

4. Der Proxy trennt die Anfrage auf OSI-Schicht 7 und erzeugt eine neue, sichere[26] Anfrage an den Server[27] im Intranet, die vom Paketfilter als gültig akzeptiert werden muss.

4.1.2.2.4 Die Groupware

Die für das Projekt relevante zentrale Groupwarekomponente Exchange befindet sich im Intranet und ist auf dem Rechner `intra,` inklusive einiger Basisdatensätze, in Form einer „virtuellen Firma" mit verschiedenen Mitarbeitergruppen eingerichtet.

4.1.2.2.5 Clientsoftware

Der iPAQ Handheld ist mit den Daten der RAS Verbindung und der GPRS Einwahl konfiguriert. Daneben laufen auf dem Client der VPN Client und das F-Secure Antivirusprogramm.

Die Sicherheitssoftware ist jedoch nicht expliziter Bestandteil der Basiskonfiguration. Da die verschiedenen Produkte hier redundant einsetzbar sind, ist die vorliegende Sicherheitssoftware beliebig. Auf die Themen Endgerätesicherheit und Sicherheitssoftware wird bereits in Kapitel 3.1.3 sowie später in Kapitel 4.4 eingegangen.

[26] Möglich wäre hier z. B. eine RSA verschlüsselte Kommunikation über SSL.
[27] Server abhängig vom Evaluationsszenario. Z. B. XTND Connect Server.

4.1.3 Gegenstand der Evaluation

Im Rahmen der Komponentenauswahl wurden die zu evaluierenden Softwareprodukte identifiziert. Um diese systematisch untersuchen zu können, werden nun, aufbauend auf der Basiskonfiguration aus Kapitel 4.1.2, Zielkonfigurationen definiert. Jede der Zielkonfigurationen ist ein zu evaluierendes Gesamtsystem.

4.1.3.1 Evaluationsbäume

Im ersten Schritt wird ein Evaluationsbaum aufgestellt, um aus ihm die konkreten Laborkonfigurationen ableiten zu können. Eine solche Gesamtkonfiguration setzt sich dabei immer aus einer bestimmten Serverkonfiguration, einer Clientkonfiguration und den verschiedenen Verbindungsarten zusammen. In jeder Laborkonfiguration muss jede der Verbindungsarten möglich sein.

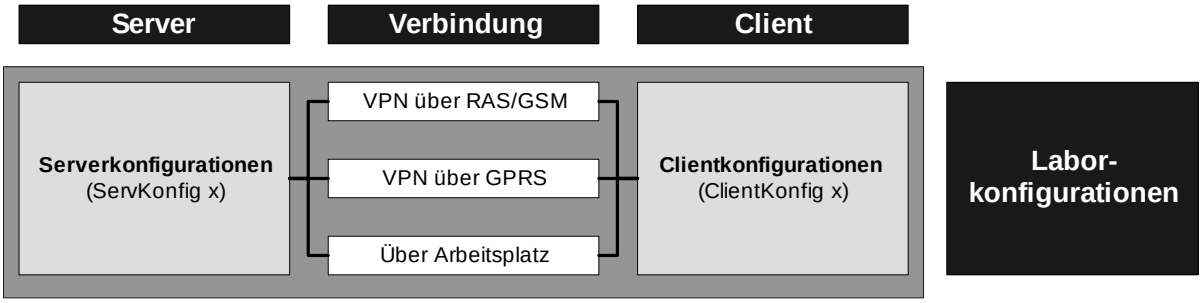

Abbildung 4-4: Evaluationsbaum

Als Verbindungen bleiben dabei zwei VPN Tunnel, entweder über eine direkte RAS Einwahl auf den Rechner dmz oder über das Internet. Diese Verbindungen wurden bereits in der Basiskonfiguration eingerichtet.

4.1.3.1.1 Die Serverseite

Auf der Serverseite unterliegt die exakte Laborkonfiguration in starkem Maße den drei Produktkategorien Groupware, Synchronisation, Administration.

Microsoft Exchange 2000 ist bereits vorkonfiguriert auf dem Rechner intra. Exchange wird implizit im Rahmen der Evaluation der Synchronisation teilweise mitevaluiert, da die für diese ausgewählten Komponenten mit Exchange direkt zusammenarbeiten.

Für die Synchronisation existieren zwei konkurrierende Produkte. Zum einen die reine Microsoft Lösung mittels des Mobile Information Servers (MIS) und des Internet Security and Acceleration Server (ISA). Die Alternative dazu ist zum anderen die Benutzung des XTND Connect Servers. Diese beiden Varianten bilden den Kernbestandteil der Kategorie der Synchronisation.

Zur Administration dient hauptsächlich Afaria. Im Falle des XTND kann jedoch auch die XTND eigene Administrationsschnittstelle benutzt werden. Diese beiden Produkte werden im Rahmen der Administrationsevaluation genau untersucht.

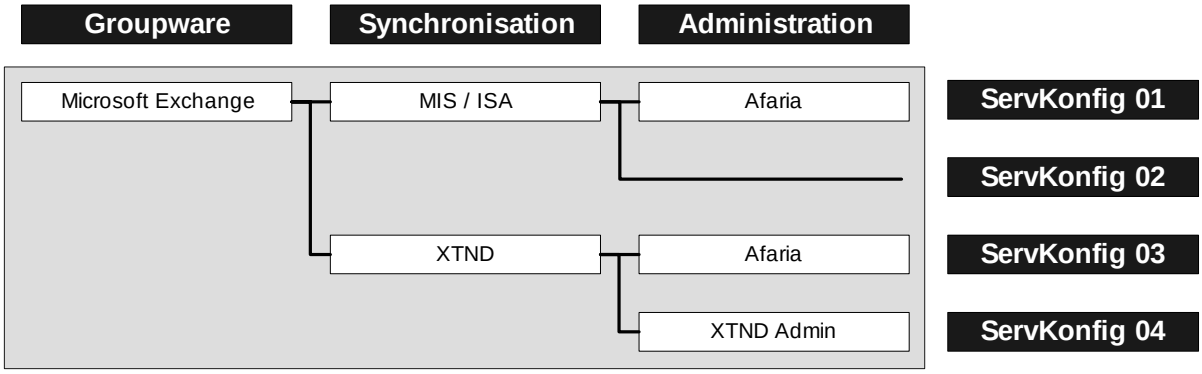

Abbildung 4-5: Evaluationsbaum der Serverseite

Sowohl XTND als auch Afaria umfassen zudem eigene Clientkomponenten, die im Rahmen der jeweiligen Serverkonfiguration zeitgleich auf den Clients installiert werden müssen. Daher hängt die Konfiguration des Handhelds unter anderem auch von der Serverkonfiguration ab[28].

Insgesamt ergibt das vier Serverkonfigurationen, von denen eine völlig ohne Administrationskomponente auskommen muss.

4.1.3.1.2 Die Clientseite

Auf der Clientseite sind neben den beiden gemäß der Basiskonfiguration (siehe Kapitel 4.1.2.2.5) eingerichteten Endgeräten vor allem die Antivirensoftware[29] und die Sicherheitssoftware relevant.

Als Sicherheitssoftware kommen die sieben in Kapitel 3.1.3.1 identifizierten Softwareprodukte in Betracht. Neben dem Einsatz zusätzlicher Sicherheitssoftware müssen auch die Fähigkeiten der Sicherheitskomponenten im Betriebssystem des Handhelds einer Evaluation unterzogen werden.

Um über eine aussagekräftige Vergleichsmöglichkeit zu verfügen, wird der iPAQ h3970 als Referenzgerät festgelegt. Mögliche Kompatibiltätsprobleme aufgrund der Änderungen im neuen iPAQ h5450 sollten damit ausgeschlossen sein. Der h5450 dient hier in erster Linie als Vergleichssystem. Versuchsweise wird dabei jede Sicherheitssoftware auch auf dem neuen Gerät installiert. Sollten Probleme auftreten oder sich Unterschiede im Zusammenspiel ergeben, wird in der Evaluation beim entsprechenden Produkt darauf hingewiesen. Auf das Verfahren zur Evaluation von Endgerätesoftware wird in Kapitel 4.4 noch näher eingegangen.

Die Antivirensoftware ist als Teil der Basiskonfiguration vor der Evaluation bereits auf dem iPAQ installiert worden. Sie wird im Rahmen dieses Projektes keiner gesonderten ausführlichen Untersuchung unterzogen

Somit ergeben sich auf Clientseite insgesamt 16 unterschiedliche Konfigurationen (siehe Abbildung 4-6).

---

[28] Der genaue Einfluss der Konfiguration wird später im Rahmen der Zielkonfigurationen erläutert.

[29] Im Rahmen dieses kommt dabei F-Secure Antivirus for Pocket PC in der Version 1.5 zum Einsatz.

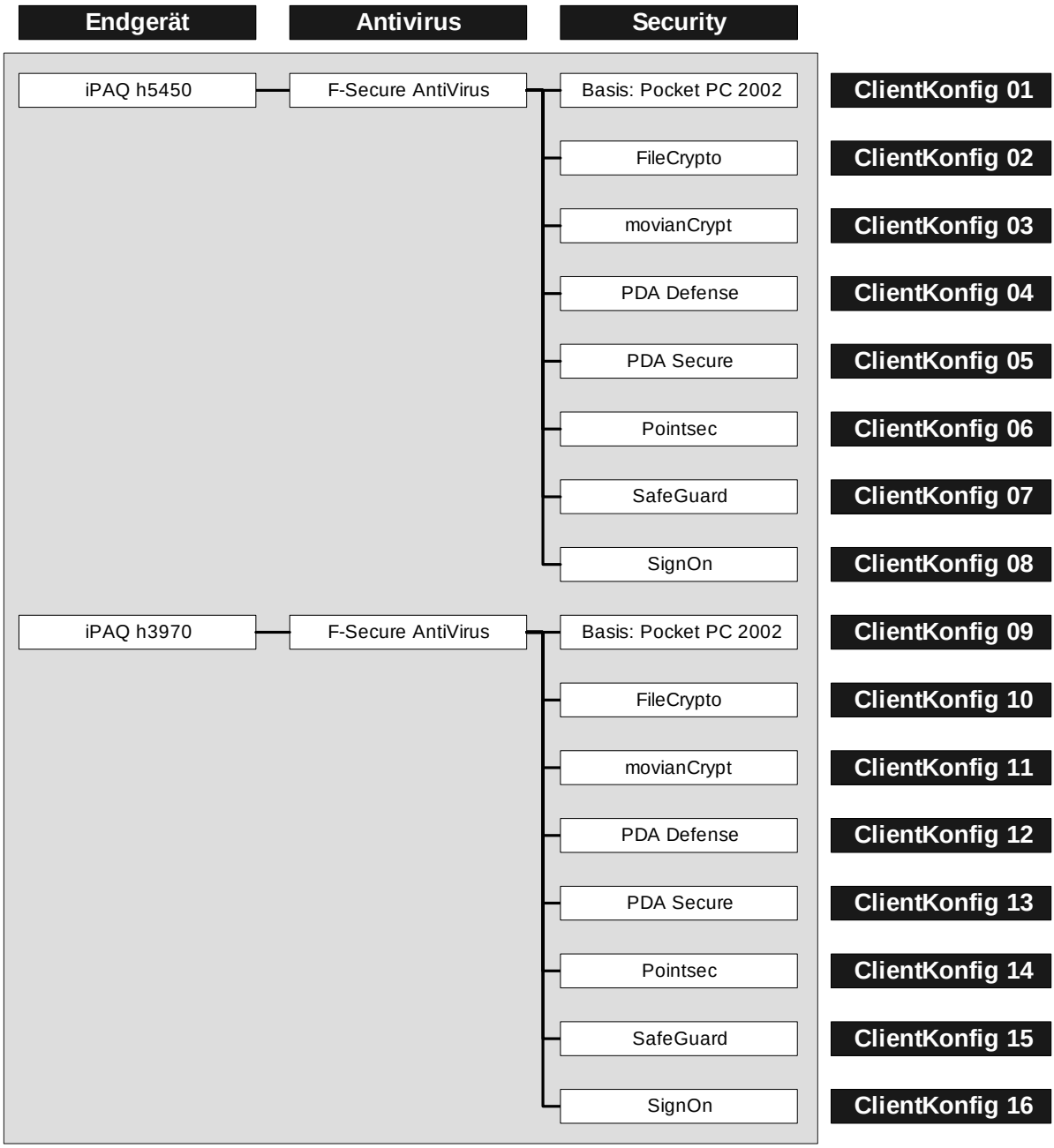

Abbildung 4-6: Evaluationsbaum der Clientseite

4.1.3.1.3 Komplexitätsreduktion

Die zu evaluierenden Softwarekomponenten lassen sich nach ihrer Funktion in drei Gruppen gliedern. Einige übernehmen die Aufgaben der Synchronisationskomponente im Gesamtsystem (MIS/ISA, XTND Connect), andere die Administration (Afaria, XTND Admin) und auf Endgeräteseite sollen Softwarekomponenten die Sicherheit der Handhelds erhöhen (z. B. PDA Secure).

Über den oben aufgestellten Baum wurden vier Server- und 16 Clientkonfigurationen identifiziert. Theoretisch müsste jede Clientkonfiguration mit jeder Serverkonfiguration getestet werden, jeweils für jede der drei Verbindungsarten. So müssten die Testcases

auf insgesamt 192 Testszenarien angewandt werden. Zeitlich war ein solcher Testumfang nicht umsetzbar. Daher wurde der Aufwand an dieser Stelle deutlich reduziert.

Wie bereits oben beschrieben, funktioniert die Sicherheitssoftware auf den Endgeräten relativ unabhängig von den restlichen Komponenten. So können die Sicherheitsprodukte auch in einem getrennten Schritt eigenständig getestet werden (16 Konfigurationen). Die beiden vielversprechendsten Produkte werden dann pro Endgerät in das Gesamtsystem übernommen, wodurch die Zahl der Testszenarien auf 48 reduziert wird, ohne inhaltliche Abstriche vornehmen zu müssen.

Mit Blick auf die für die 48 Szenarien notwendigen Gesamtlaborkonfigurationen kann man die Komplexität weiter verringern. Die Verbindungsarten müssen in jeder Laborkonfiguration jederzeit möglich sein, werden also unabhängig vom Testszenario immer parallel installiert, was zu 16 Laborkonfigurationen (vier ServerKonfigurationen und vier Client-Konfigurationen) führt. Lässt man die Frage nach der konkreten Endgerätesicherheitssoftware offen, verbleiben für das Labor[30] mit zwei eingerichteten Endgeräten[31] vier Zielkonfigurationen.

4.1.3.2 Standorte und Servernamen

Wie aus dem Evaluationsbaum ersichtlich, gibt es verschiedene Verbindungsarten, mit denen der Client (hier der iPAQ Handheld) mit dem Labornetzwerk Kontakt aufnimmt. Dabei lassen sich zwei unterschiedliche Standorte für den iPAQ erkennen:

- mobiler Einsatz

  Mobiler Einsatz bedeutet die Synchronisation über GSM bzw. GPRS von außerhalb des Firmennetzwerkes. Dabei stellt der iPAQ eine Verbindung in die DMZ her und synchronisiert sich über einen der im Kapitel 4.1.2.2.3 vorgestellten VPN Tunnel direkt an der jeweiligen Proxykomponente (siehe Kapitel 2.2) auf dem Rechner `dmz`. Hinter dem Kommunikationspartner verbirgt sich aus Sicht des Client also der transparente Proxy, der die Daten vom Synchronisationsserver erhält.

- Einsatz am Arbeitsplatz

  Am Arbeitsplatz hat der iPAQ bereits eine Verbindung in das Intranet und er befindet sich somit in der sicheren Zone. Dabei ist es egal, ob diese Verbindung über ein Inhouse W-Lan oder die Dockingstation{ XE "Dockingstation" } am Companion{ XE "Companion" }- bzw. Arbeitsplatzrechner hergestellt wird. Der Client synchronisiert sich hier direkt mit dem Synchronisationsserver auf dem Rechner `sync`. Der Client möchte also einen völlig anderen Rechner über dieselbe IP Adresse erreichen.

Mit diesen beiden Standorten entsteht ein Problem für die Auflösung des im Client eingestellten Rechnernamens auf die korrekten IP-Adresse. Eine naheliegende Möglichkeit wäre es, mit verschiedenen standortabhängigen Profilen für die Verbindung auf dem Client zu arbeiten. Dies zieht jedoch ein Usabilityproblem nach sich. Es muss möglichst vermieden werden, dass der Benutzer bei wiederkehrenden Aufgaben wie z. B. der Synchronisation der E-Mails und des Kalenders immer wieder aufs Neue erst das korrekte Profil im Client auswählen muss.

Dieses Problem kann umgangen werden, indem ein „DNS Dummy" eingerichtet wird. Dazu wird im Client anstelle einer festen IP-Adresse ein entsprechender Servername wie

---

[30] Natürlich mit austauschbarer Sicherheitskomponente auf dem Endgerät.
[31] Einmal der iPAQ h3970 und einmal der iPAQ h5450.

beispielsweise „XTND“ bzw. „Afaria“ angegeben, der von den verschiedenen DNS Servern standortabhängig unterschiedlich aufgelöst wird. Ein weiterer Grund für die Verwendung dieser Strategie ist die Tatsache, dass die Angabe fester IP-Adressen im Client ein Sicherheitsrisiko darstellen kann, da diese u. U. von Dritten eingesehen werden können.

Variante 1:

Der Client befindet sich im Intranet. In diesem Fall wird der Rechnername `dmz` zur internen IP des Servers direkt aufgelöst, d. h. die Proxy-Komponente in der DMZ wird nicht benutzt. Dazu muss im Intranet der DNS-Server so eingerichtet werden, dass er den Namen `dmz` in die interne IP des Rechners `sync` umsetzt.

Variante 2:

Der Nutzer ist mobil unterwegs und verbindet den Client entweder per RAS oder über das Internet mit dem Firmennetz. In diesem Fall wird der Rechnername `dmz` zur IP der Proxykomponente aufgelöst. Dieses kann z. B. über den DNS-Server in der DMZ geschehen. Die weitere Kommunikation verläuft regulär über die Proxykomponente.

In beiden Fällen übernimmt der DNS Server die richtige Auflösung, je nach Standort des iPAQ und vermittelt dann an den richtigen Server. Die Proxykomponente in der DMZ ist für den Client transparent. So besteht aus Sicht des Clients bei eingerichtetem „DNS-Dummy“ keinerlei Unterschied zwischen dem Szenario der Arbeitsplatzsynchronisation und der mobilen Synchronisation über RAS/VPN.

4.1.3.3 Zielkonfigurationen

Im Folgenden werden die unterschiedlichen Laborkonfigurationen im Detail diskutiert. Als Endgerät wird dabei ein iPAQ inklusive einer beliebigen Sicherheitssoftware vorausgesetzt.

4.1.3.3.1 Das Afariaproblem

Die Administrationssoftware von Afaria (siehe Kapitel 4.2.3) bietet momentan keine Proxy-Komponente an, die in der DMZ als Schicht-7 Proxy eingesetzt werden könnte. Zugriffe von außen, z. B. über RAS oder das Internet, können also nicht über eine zentrale Proxykomponente nach innen vermittelt und dabei kontrolliert werden.

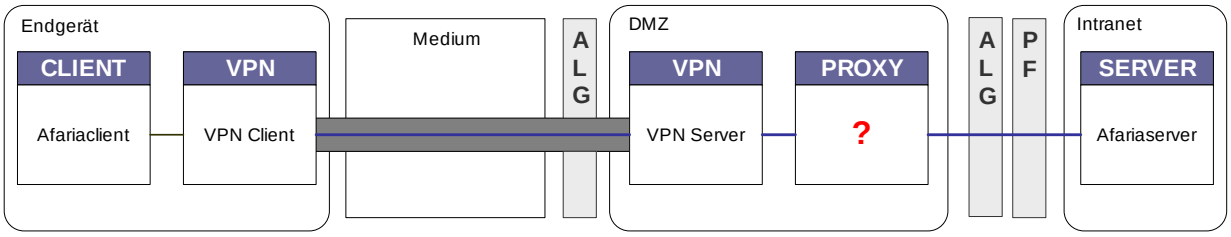

Abbildung 4-7: Das Afariaproblem

Diese Situation schafft zwei Probleme: Auf Sicherheitsebene besteht das Problem, dass ein direkter Kanal von außen an den Afaria-Server geschaltet werden muss, z. B. über eine gesonderte VPN-Verbindung durch die Firewall ins Intranet. Eine Schicht-7-Filterung ist dabei nicht mehr möglich. Mehr zu diesem Problem im Kapitel 4.2.3.

Auf Usability-Seite besteht das Problem, dass mehrere VPN-Verbindungen konfiguriert werden müssen, die je nach gewünschtem Abgleich vom Endbenutzer ausgewählt werden

müssen[32]. Für den Abgleich mit der Synchronisationskomponente muss die „reguläre" VPN-Verbindung in die DMZ aufgebaut und müssen die Daten dort an den Synchronisations-Proxy weiterleitet werden. Für den Afaria-Abgleich muss danach die „direkte" VPN-Verbindung ins Intranet ausgewählt werden.

Diese Situation schafft für den Endbenutzer eine verwirrende Situation, in der er sich jedes Mal aufs Neue Gedanken machen muss, welches Ziel er gerade verfolgt. Für einen kompletten Abgleich müsste eine VPN-Verbindung aufgebaut, wieder getrennt und eine neue aufgebaut werden.

Zur Verbesserung der Usability ist es möglich, einen „Workaround" zu definieren. Die Grundidee besteht darin, eine virtuelle Proxy-Komponente auf TCP-Schicht aufzubauen. Ähnlich wie der Proxy der Synchronisationskomponete wird auf dem Rechner „DMZ" eine Weiterleitung geschaltet, allerdings behelfsweise mittels eines „Port-Forwarders" (Konfiguration: Siehe Kapitel 7.1). Dieser leitet Pakete für die Kommunikation von Afaria[33] zwischen Client und Server ähnlich einem normalen Packetfilter zwischen DMZ (Endpunkt der VPN-Strecke) und dem Intranet hin und her. Da hier insbesondere weder eine semantische noch eine syntaktische Prüfung erfolgt, handelt es sich nicht um einen Schicht-7-Proxy, wie eigentlich von uns gefordert. Der Portforwarder ist unter dem Gesichtspunkt der Sicherheit ähnlich kritisch einzuschätzen wie der direkte VPN Tunnel ins Intranet.

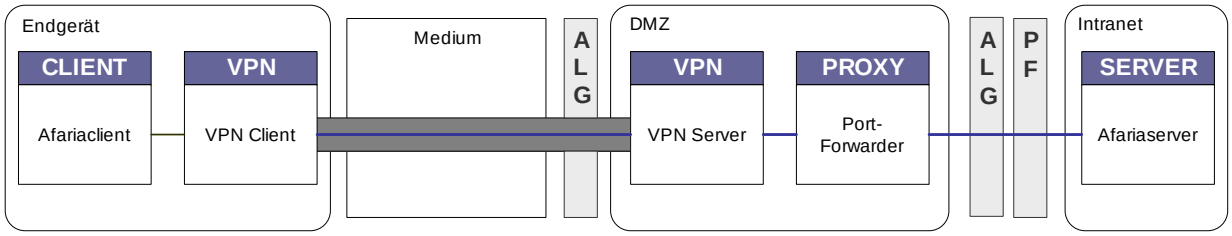

Abbildung 4-8: Afaria mit Port Forwarding

Der Vorteil dieser Lösung besteht darin, dass vom Endbenutzer nur noch eine VPN-Verbindung in die DMZ aufgebaut werden muss. Die VPN-Verbindung in das Intranet ist nicht mehr notwendig, da die Weiterleitung der Afaria-Pakete über den Portforwarder erfolgt. Die einzige VPN-Gegenstelle, die im VPN-Client des Endgeräts angegeben wird, ist das äußere Ende der Firewall (hier also die Internetadresse, über die das Labor zu erreichen ist). Der ALG leitet die Pakete dann in die DMZ weiter, wo wiederum der Portforwarder greift.

Dieser Workaround löst in keiner Weise das grundsätzliche Problem der fehlenden Afaria-Proxykomponente, sondern schafft lediglich Abhilfe für die Bedienungsschwäche auf Endbenutzerseite. Die Sicherheit gegenüber der direkten VPN-Verbindung ins Intranet wird dennoch in geringem Maße erhöht, denn im hier geschilderten Szenario wird außerdem die Firewall inklusive aller Filter- und Protokollierungsregeln benutzt. Auf der anderen Seite schafft ein Portforwarder evtl. durch Buffer overflows o. ä. wieder neue Sicherheitsprobleme.

---

[32] Durch den neuen VPN Tunnel müssten zudem Änderungen im Intranet vorgenommen werden, in dem z. B. ein weiterer VPN Server dort installiert wird.

[33] Also ausschließlich die Encapsulated HTTP Pakete auf dem entsprechenden Afaria Port (per Default auf Port 3007) zwischen Client und Server.

4.1.3.3.2 Szenario MIS / ISA (ServKonfig 1 + 2)

Dieses Szenario entspricht ServKonfig 1+2 und benutzt den Mobile Information Server als Synchronisationskomponente. Die Evaluation dieses Szenarios wird in Kapitel 4.3.2 behandelt.

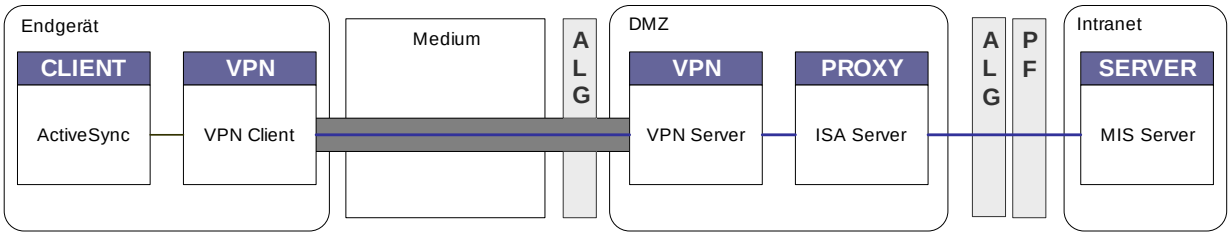

Abbildung 4-9: MIS/ISA Synchronisation

Für die Kommunikation[34] wird das im Betriebssystem des Endgerätes bereits integrierte ActiveSync benutzt. Als Proxykomponente kommt der ISA Server zum Einsatz. Beim Einsatz von Afaria kommt in der Administration zudem oben beschriebenes Afariaproblem zum Tragen[35]. Afaria benötigt außerdem einen eigenen Client auf dem Endgerät, der jedoch gut mit der ActiveSync Synchronisation zusammenarbeitet. So kann bei einer ActiveSync Synchronisation mit dem MIS laut Afariadokumentation im Hintergrund eine automatische Afariasynchronisation laufen.

4.1.3.3.3 Szenario XTND (ServKonfig 3 + 4)

Im Szenario XTND kommt der XTND Connect Server als Synchronisationskomponente zum Einsatz. Bestandteil des XTND Paketes sind dabei eine eigene Proxykomponente und ein Administrationstool (Mehr zur Administration über XTND in Kapitel 4.2.2). Zudem benötigt der XTND Server einen eigenen Client auf dem Endgerät. Die Evaluation dieses Szenarios wird in Kapitel 4.3.3 behandelt.

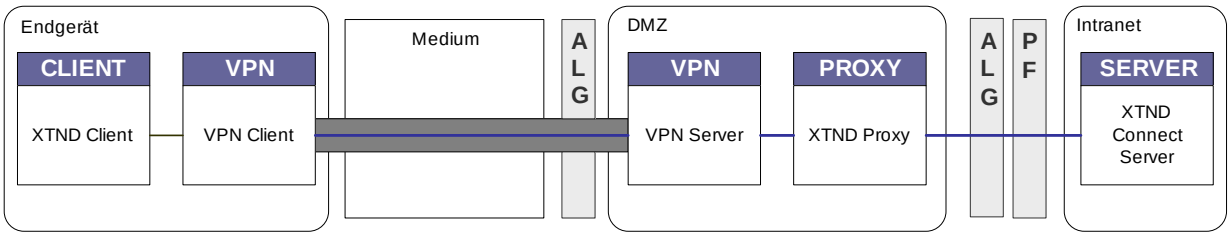

Abbildung 4-10: XTND Synchronisation

[34] Die VPN Strecken über RAS oder Internet wurden bereits in der Basiskonfiguration eingerichtet.

[35] Das wie in Abbildung 4-8 gezeigt, bedingt gelöst werden kann.

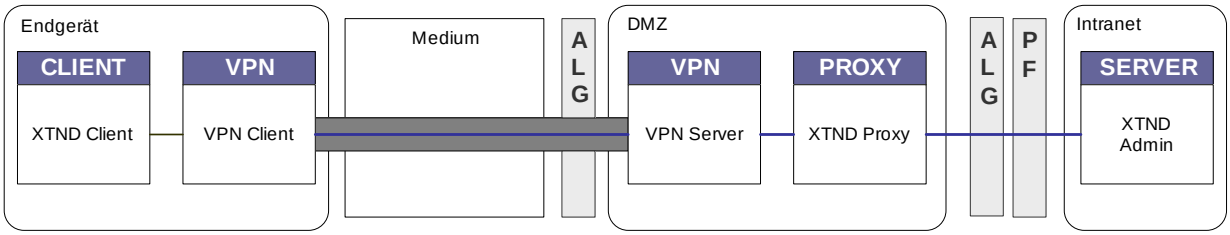

Abbildung 4-11: XTND Administration

Der XTND ist in der Lage über SSL-Verbindungen zu kommunizieren. Sowohl zwischen dem Proxy und dem Server als auch dem Client und dem Proxy wird so bei Bedarf automatisch anstatt der üblichen Verbindung über Port 5001 eine SSL Verbindung über Port 6001 aufgebaut. Dies stellt einen weiteren theoretischen Schutz der nativ von XTND über RSA verschlüsselten Datenkommunikation dar. Folgende Filterregel wird dazu auf dem Paketfilter für den XTND Connect benötigt:

Tabelle 4-2: ALG Proxy „XTND Innen"

ALG-Proxy: „XTND Innen"
Daten
Protokoll: TCP Von: DMZ (Port 6001 für SSL und 5001 ohne SSL) Nach: sync (Port 6001 für SSL und 5001 ohne SSL)
Beschreibung
Diese Regel leitet jede XTND-Anfrage aus der DMZ kommend von Port 6001 in das Intranet (Rechner: SYNC) auf Port 6001 weiter.
Zweck
Von der Proxy-Komponente aus der DMZ kommende Verbindungen an SYNC werden zugelassen.

Kommt nicht die XTND eigene Administrationskomponente zum Einsatz, entsteht auch hier das bekannte Afariaproblem. Da XTND zudem nicht ActiveSync zur Synchronisation benutzt, wird anders als im MIS/ISA Szenario wahrscheinlich ein manuelles Starten des Afariaclients notwendig sein.

4.1.4 Vorbereiten des Labors

Vor der eigentlichen Evaluation muss das Testlabor in die richtige Zielkonfiguration gebracht werden, denn diese ist die grundlegende Vorraussetzung für die Evaluation. Diese Zielkonfiguration muss analog zu Kapitel 4.1.1 gesichert werden, damit sie jederzeit wiederherstellbar ist.

Der systematische Aufbau der Konfiguration im Labor folgte einem abstrakten Stufenplan, der wichtige Zwischenschritte identifizierte und somit einen nachvollziehbaren Aufbau mit überprüfbaren Teilergebnissen ermöglichte. Für die Zielkonfiguration im XTND Szenario ohne Afaria, wie oben beschrieben, stellt sich ein solcher Stufenplan wie folgt dar (Abbildung 4-12). Im Bild sind dabei zur Verdeutlichung der Stufen die letzten beiden Teilschritte im Statusfeld noch mit einem „ToDo" gekennzeichnet, obwohl sie im Projekt vor Evaluation des Szenarios natürlich ebenfalls realisiert wurden.

Phase	Nr.	Stufenziel	Status
Vorraussetzung	01	Labor ist in der Basiskonfiguration	Check
PHASE 1 Basissynchronisation	02	XTND Connect Server und iPAQ Client installiert	Check
	03	Sync. im Intranet direkt am XTND Connect Server	Check
	04	XTND DMZ Proxy installiert und PF konfiguriert	Check
	05	Sync. direkt am XTND DMZ Proxy funktioniert	Check
PHASE 2 Verbindungscheck	06	RAS Dienst funktioniert	Check
	07	VPN über RAS funktioniert	Check
	08	GPRS Einwahl auf iPAQ funktioniert	Check
	09	VPN über GPRS durch ALG in DMZ funktioniert	Check
PHASE 3 Mobile Synchronisation	10	Sync. über RAS auf XTND Proxy funktioniert	Check
	11	Sync. über GPRS auf XTND Proxy funktioniert	Check
	12	XTND Admin ist installiert und konfiguriert	ToDo
	13	Adminsync funktioniert	ToDo

EVALUATION

Abbildung 4-12: Das Stufenkonzept am Beispiel XTND

Der gemeinsame Ausgangspunkt jedes Stufenplans ist die in Kapitel 4.1.2 beschriebene Basiskonfiguration. Dann werden zuerst die Komponenten der Synchronisations-Software installiert und lokal getestet, einerseits direkt im Intranet am Server selbst und bei Schritt 5 andererseits auch in der dmz am Proxy über den Paketfilter der Firewall hindurch ins Intranet. Ein Check der Verbindungsarten gewährleistet eine physische Verbindung sowohl über RAS Einwahl als auch über GRPS in die DMZ. Somit können der Aufbau und die Einrichtung der mobilen Synchronisation und die Aktivierung/Installation der Administrationskomponente erfolgen.

Erst damit befindet sich das Labor komplett in der Zielkonfiguration und ist bereit für die Evaluation.

4.1.5 Das Evaluationskonzept

Neben den bisher erwähnten Konzepten ist auch ein strukturiertes Testverfahren unabdingbar. Ein solches Verfahren muss für den Leser transparent sein und die Möglichkeit bieten, konkurrierende, bisher noch nicht evaluierte Software nachträglich zu testen. Dabei muss die Vergleichbarkeit der Ergebnisse gewährleistet sein.

4.1.5.1 Evaluationsbögen

Ein klassisches und bewährtes Verfahren zur Gewährleistung von Transparenz und Vergleichbarkeit, das wir auch im Rahmen dieses Projektes anwandten, stellt die Verwendung von Evaluationsbögen dar[36]. Auch in diesem Projekt wurden Evaluationsbögen für die verschiedenen Softwarekomponenten entwickelt und anhand ihrer die Tests durchgeführt. Da es nicht sinnvoll ist, für den Test von Synchronisations- und Sicherheitssoftware den gleichen Evaluationsbogen mit den gleichen Bewertungskriterien zu verwenden, wurden drei unterschiedliche, auf die funktionalen Aspekte der jeweiligen Softwarekategorien zugeschnittene Evaluationsbögen entwickelt, d. h. für:

- Synchronisationssoftware
- Administrationssoftware
- Sicherheitssoftware[37]

Der Aufbau der Bögen basiert auf den in Kapitel 1.3 definierten Kategorien Administration, Sicherheit, Usability und Kosten. Darüber hinaus wurden die Evaluationsbögen um spezielle Eigenschaften der jeweils betrachteten Softwarekategorie erweitert.

Unser Ziel bei der Erstellung der Evaluationsbögen war es, neben der bereits erwähnten Transparenz und der Vergleichbarkeit der Ergebnisse sowohl möglichst viele Aspekte der einzelnen Softwarelösungen zu betrachten und zu beurteilen als auch in unseren Augen wichtige Aspekte stärker zu gewichten als weniger wichtige. Der Evaluationsbogen für die Sicherheitssoftware wurde z. B. in verschiedene Kategorien[38] unterteilt, die unterschiedlich stark gewichtet wurden. Die Gewichtung ist hoch (+++), mittel (++) oder gering (+). Dadurch war es möglich, beispielsweise der Authentifikation einen höheren Stellenwert für das Endergebnis beizumessen als dem Kostenfaktor.

Nach der Definierung der verschiedenen Kategorien und deren Gewichtung wurde für jede Kategorie eine möglichst umfassende Sammlung der relevanten Kriterien entwickelt, anhand derer die Tests durchgeführt werden sollten. Dies geschah unter anderem bereits während der Auswahl der zu testenden Komponenten und auf Basis eingehender prospektbasierter Voruntersuchungen.

Zur Bewertung der Kriterien wurde auf zwei unterschiedliche Systeme zurückgegriffen. Zum einen auf eine den bekannten Schulnoten entsprechende sechsstufige Skala (1: sehr gut, 6: ungenügend), zum anderen auf eine boolesche Bewertung (ja/nein) bei Kriterien, die für eine Skalenbewertung wenig geeignet erschienen. Außerdem sind auf den Evaluationsbögen Bemerkungs- beziehungsweise Kommentarfelder vorgesehen, um besondere, durch den Evaluationsbogen sonst nicht abgedeckte Sachverhalte ebenfalls zu erfassen.

---

[36] Zu dem speziellen Aufgabengebiet bzw. Szenarios des Projektes existieren noch keine etablierten darauf angepassten Verfahren zur Evaluation.

[37] Hier nur in Bezug auf die Endgerätesoftware.

[38] Diese Kategorien basieren auf den vier Grundkategorien (Sicherheit, Administration, Usability, Kosten) oder beziehen sich auf besondere Merkmale der jeweiligen Softwarekategorie.

Auf Basis der Beurteilung der einzelnen Kriterien wurde dann, wiederum mittels einer sechsstufigen Skala, die Beurteilung der jeweiligen Kategorie vorgenommen. Das so entwickelte Ergebnis für diese Kategorie floss dann nach entsprechender Gewichtung in das Endergebnis ein.

4.1.5.2 KO-Kriterien

Das bis hier entwickelte Konzept stellt sicher, dass ein hinreichend breites Spektrum von Testfällen existiert, dass die Testergebnisse nachvollziehbar und vergleichbar sind und dass bestimmte Kategorien stärker gewichtet werden als andere. Besonders kritische Punkte bzw. Mindestanforderungen an die Software wurden bisher jedoch nicht explizit beachtet. Hierzu existiert u. a. das Konzept der „Knock-Out-Kriterien" (KO-Kriterien, Ausschlusskriterien).

KO-Kriterien wurden ursprünglich entwickelt, um den Testaufwand umfangreicher Evaluationen zu minimieren. Erfüllt der Untersuchungsgegenstand eines der vor dem Test spezifizierten KO-Kriterien nicht, so könnte der Test sofort abgebrochen und der Evaluationsgegenstand als Ganzes für untauglich befunden werden. Hieraus wird deutlich, dass der Einsatz von KO-Kriterien nur in begrenztem Maß erfolgen darf und dass deren Definition äußerst vorsichtig geschehen muss.

Es wurde auf eine abgewandelte Form der KO-Kriterien zurückgegriffen, bei der nicht die Minimierung des Testaufwandes sondern die außerordentlich hohe Bedeutung der jeweiligen Anforderung im Mittelpunkt steht. Hierbei hat die Nichterfüllung eines KO-Kriteriums zur Folge, dass der Untersuchungsgegenstand (die jeweilige Software) in der entsprechenden Kategorie für untauglich befunden, die Evaluation jedoch entgegen dem eigentlichen Konzept von KO-Kriterien fortgesetzt wird. Wird auf diese Weise ein Produkt in einer Kategorie mit hoher (+++) oder mittlerer (++) Gewichtung für untauglich befunden, so wird auch das gesamte Produkt im Endergebnis für untauglich befunden. Diese Kategorien sind von so essentieller Bedeutung, dass schwerwiegende Schwächen in ihnen nicht tolerierbar sind.

4.1.5.3 Gemeinsamkeiten

Auch wenn sich die zu untersuchenden Softwarekomponenten zu stark unterscheiden, um sie alle anhand derselben Kategorien und Kriterien beurteilen zu können, gibt es Aspekte, die sowohl auf Synchronisations- als auch auf Administrations- und Sicherheitssoftware zutreffen. Insbesondere sind dies die Bewertungskategorien „Kosten" und „Usability". Es war daher unser Ziel, für diese beiden Kategorien Bewertungs- und KO-Kriterien zu definieren, die in allen drei Evaluationsbögen gleichermaßen Verwendung finden konnten.

Für die Bewertungskategorie „Kosten" mußten lediglich Anschaffungskosten sowie laufende Kosten in einer geringen Anzahl konkreter Bewertungskriterien wie „Kosten für Updates", „Kosten für Support-/Wartungsvertrag" etc. betrachten werden[39].

Für die Kategorie „Usability" wurde ein Verfahren benötigt, das es ermöglicht, gleichermaßen Endgeräte- wie auch Serversoftware auf deren Benutzbarkeit und Benutzerfreundlichkeit hin zu untersuchen. Hierbei ist zu beachten, dass bereits durch die unterschiedliche Bildschirmgröße und –auflösung bedingt eine Behandlung des Themas Usability auf einem allgemeingültigen Niveau geschehen muss. Außerdem existiert mit der Norm DIN EN ISO 9241-10 („Grundsätze der Dialoggestaltung")[40] ein rechtlicher Rah-

[39] Kosten für Einführung, Schulung, laufende Betreuung etc. wurden nicht für jede Softwarekategorie betrachtet.

[40] http://www.informatik.uni-stuttgart.de/ifi/ds/Lehre/Softerg/iso9241.pdf [27.03.2003].

men, der auch für die von uns getestete Software relevant ist und auf dessen Einhaltung hin die Software untersucht werden muss.

4.1.5.4 DIN EN ISO 9241-10 und IsoMetrics

Die Norm DIN EN ISO 9241-10 definiert Software-ergonomische Grundsätze der Dialoggestaltung und ist Teil der Norm DIN EN ISO 9241, die 1995 vom europäischen Institut für Normung angenommen wurde. Die DIN EN ISO 9241-10 ist in sieben Teilbereiche gegliedert:

- Aufgabenangemessenheit
- Selbstbeschreibungsfähigkeit
- Steuerbarkeit
- Erwartungskonformität
- Fehlertoleranz
- Individualisierbarkeit
- Lernförderlichkeit.

Die Kategorie „Individualisierbarkeit" haben wir im Rahmen dieser Evaluation nicht betrachtet, da diese hauptsächlich auf Endbenutzersoftware wie z. B. Textverarbeitung abzielt. Bei allen von uns betrachteten Softwarekomponenten handelt es sich jedoch entweder um Serversoftware oder um Software für PDAs. Es erschien wenig sinnvoll, diese Anwendungen daraufhin zu testen, ob Werkzeugleisten oder Menüs an die persönliche Arbeitsweise des jeweiligen Benutzers angepasst werden können. Keine der im Rahmen der Evaluation betrachteten PDA-Software ist individualisierbar .

Darüber hinaus wurde das DIN EN ISO 9241-10-Kategoriensystem um die beiden Kategorien „Sprache" und „Programmexterne Hilfestellungen" erweitert. In der Kategorie „Sprache" wird die Verfügbarkeit der Software in deutscher, englischer sowie in weiteren Sprachen erfasst, die Kategorie „Programmexterne Hilfestellungen" behandelt die Qualität von Benutzer- und Administrationshandbüchern und, soweit bewertbar, die Supportqualität des Herstellers.

Im Rahmen der Norm gilt die folgende Definition für den Begriff „Dialog":

Dialog:

„Eine Interaktion zwischen einem Benutzer und einem Dialogsystem, um ein bestimmtes Ziel zu erreichen." (ISO 1995, S. 5)

Als Dialog und somit als Untersuchungsgegenstand sind hier, entgegen der allgemein gebräuchlichen Verwendung des Wortes Dialog, also nicht nur Mitteilungs- und Eingabefenster zu verstehen, sondern ebenfalls Programm-Hauptfenster, Menüs etc.

All diese Dialogelemente einer jeden Softwarekomponente müssen einer Überprüfung im Hinblick auf die genannten sieben (hier 6+2) Teilbereiche der Norm unterzogen werden.

Um Software auf die Erfüllung der Norm DIN EN ISO 9241-10 hin überprüfen zu können, wurde 1998 an der Universität Osnabrück das Verfahren IsoMetrics entwickelt[41]. Es basiert auf 75, zum Teil redundant ausgelegten Fragen, anhand derer eine Software in den besagten Teilbereichen getestet werden kann. Alle Fragen des Evaluationsbogens erhalten eine gleichartige Skalenbewertung. Der Evaluationsbogen existiert in einer Kurz- und

[41] Siehe http://www.isometrics.uni-osnabrueck.de/ [27.03.2003] (IsoMetrics 2002).

einer Langversion, bei letzterer besteht die Möglichkeit, zu jeder Frage ausführliche Kommentare abzugeben.

Index	Aufgabenangemessenheit	stimmt nicht 1	stimmt wenig 2	stimmt mittelmäßig 3	stimmt ziemlich 4	stimmt sehr 5	Keine Angabe
A1	Die Software zwingt mich, überflüssige Arbeitsschritte durchzuführen.						
A3	Mit der Software kann ich zusammenhängende Arbeitsabläufe vollständig bearbeiten.						
A4	Die Software bietet mir alle Möglichkeiten, die ich für die Bearbeitung meiner Aufgaben benötige.						
A6	Die Software ermöglicht es mir, Daten so einzugeben, wie es von der Aufgabenstellung gefordert wird.						
A7	Die für die Aufgabenbearbeitung notwendigen Informationen befinden sich immer am richtigen Platz auf dem Bildschirm.						
A8	Es müssen zuviele Eingabeschritte für die Bearbeitung mancher Aufgaben durchgeführt werden.						

Abbildung 4-13: Auszug aus IsoMetrics Fragebogen, kurze Version[42]

Wir haben diesen Evaluationsbogen jedoch nicht übernommen, sondern uns vielmehr an ihm orientiert. So konnten wir durch Weglassen der bewusst redundant ausgelegten Fragen, die im ursprünglichen Evaluationsbogen dazu dienen, willkürliche Aussagen zu identifizieren und von der Verwendung auszuschließen, die Anzahl der Fragen pro Bewertungskategorie stark verringern. Die hier entwickelten Evaluationsbögen beinhalten ebenfalls Kommentarfelder, die jedoch nur für die Protokollierung von Auffälligkeiten einer Software verwendet wurden.

Eine weitere Eigenschaft des IsoMetrics-Evaluationsbogens ist die alternierende Skalenausrichtung der einzelnen Fragen. Die Fragen sind so gestellt, dass die qualitative Bewertung „sehr gut" unregelmäßig wechselnd zwischen dem Skalenmaximum („stimmt sehr") und dem Skalenminimum („stimmt nicht") liegt. Eine positive Ausrichtung bei einer Frage bedeutet dabei, dass „sehr gut" und „stimmt sehr" aufeinanderfallen. Dazu entgegengesetzt liegt bei der negativen Ausrichtung das „sehr gut" auf dem Skalenelement „stimmt nicht". Dies liegt in der Tatsache begründet, dass der Fragebogen ursprünglich dafür konzipiert wurde, von vielen verschiedenen Testern ausgefüllt zu werden. So lässt sich die Neigung eines ungeschulten Testers kompensieren, seine Kreuze ungeachtet der konkreten Fragestellung aus Gewohnheit eher rechts bzw. links zu setzen.

Da sich die Auswertung jedoch durch die alternierende Ausrichtung, die für den ursprünglichen Verwendungszweck durchaus sinnvoll ist, umständlicher gestaltet und die ermittelten Rohdaten darüber hinaus weit weniger prägnant sind, haben wir auch hierauf

[42] Entnommen aus „IsoMetrics Kurzform v2.01" (WiHaGe 1997).

verzichtet und unsere Evaluationsfragen so formuliert, dass sie eine einheitliche positive Ausrichtung der Skala aufweisen. Die so entwickelten Bewertungskriterien finden sich in allen von uns verwendeten Evaluationsbögen wieder. Es sei nochmals klargestellt, dass wir mittels dieser Evaluationsbögen **keine** ISO-Zertifizierung durchführen. Wir evaluieren die diversen Softwarekomponenten hier lediglich anhand der durch die ISO-Norm definierten Schwerpunkte.

4.1.5.5 Kategorisierung

Wie oben beschrieben wurden die Softwareprodukte zur Evaluation in drei grundlegende funktionale Kategorien eingeteilt:

1. Synchronisatonsoftware
2. Administrationssoftware
3. Sicherheitssoftware für PocketPC Handhelds.

Für jede Kategorie wurde ein auf die Charakteristik der Softwaresparte zugeschnittener Evaluationsbogen erstellt, der sich wiederum in verschiedene zu untersuchende Kategorien gliedert. Die vier für dieses Projekt grundlegenden Kategorien wurden bereits in Kapitel 1.3 Definiert:

1. Sicherheit
2. Administration
3. Usability
4. Kosten.

Diese Aufteilung spiegelt sich auch in der Kategorisierung der Evaluationsbögen wider, in die jedoch auch neue Aspekte und besondere Merkmale der jeweiligen Gruppe einfliessen. Es folgt daher eine kurze Vorstellung der einzelnen Kategorien für die drei Softwaregruppen. Die Kategorien werden in den jeweiligen Unterkapiteln der Komponentenevaluation (Kapitel 4.2, 4.3 und 4.4) noch ausführlicher dargestellt.

Synchronisationssoftware

Bei der Untersuchung der Synchronisationssoftware steht die eigentliche Funktion besonders stark im Mittelpunkt. Daher wird neben den allgemeinen Kernkategorien eine weitere, unabhängige und rein funktionale Kategorie „Synchronisation" gebildet.

Tabelle 4-3: Kategorisierung Synchronisationssoftware

Gewichtung	Kategorie	Gehört zu:
++	**Administration**	Administration
+	**Besondere Merkmale**	-
+	**Kosten**	Kosten
+++	**Sicherheit**	Sicherheit
+++	**Synchronisation**	-
++	**Usability**	Usability

Administrationssoftware

Zentrale Bedeutung hat hier die Kategorie der Administration. Daher wurde diese Kategorie hier noch feiner unterteilt.

Tabelle 4-4: Kategorisierung Administrationssoftware

Gewichtung	Kategorie	Gehört zu:
+	**Administration allgemein**	Administration
++	**Benutzerverwaltung und Deployment**	Administration
++	**Geräteverwaltung**	Administration
++	**Kommunikationskanäle**	Administration
+	**Kosten**	Kosten
+++	**Remoteanalyse**	Administration
+++	**Sicherheit**	Sicherheit
++	**Softwareverwaltung**	Administration
++	**Usability**	Usability

Sicherheitssoftware (Endgeräte)

Bei der Sicherheitssoftware für die Handheldgeräte spielt natürlich die Sicherheit eine zentrale Rolle. Allerdings können viele Aspekte der Handheldsicherheit bereits von anderen Komponenten wie z.B. der VPN-Software oder gar der Synchronisationssoftware[43] abgedeckt werden. Daher wurden in Kapitel 3.1.3.1 die beiden zentralen Anforderungen an die zu evaluierende Sicherheitssoftware definiert, die sich nun als feinere Untergliederung der Basiskategorie Sicherheit auch auf dem Evaluationsbogen wiederfinden.

Tabelle 4-5: Kategorisierung Sicherheitssoftware (Endgeräte)

Gewichtung	Kategorie	Gehört zu:
++	**Administration**	Administration
+++	**Authentifikation**	Sicherheit
+	**Besondere Merkmale**	-
+++	**Datensicherheit**	Sicherheit
+	**Kosten**	Kosten
++	**Usability**	Usability

4.1.5.6 Flexibilität des Verfahrens

Im Rahmen dieses Projektes wurden während der Evaluation die Bewertungskategorien (Sicherheit, Administration usw.) einer bestimmten Gewichtung für die Gesamtempfehlung unterzogen. Zusätzlich fließen identifizierte KO-Kriterien erst nach Erfassung des kompletten Rohdatensatzes in die Analyse des entsprechenden Evaluationsbogens mit ein. Sie dienen, ähnlich der Gewichtung der Individualisierung, der Bewertung auf die

[43] Der XTND Connect Server z. B. verschlüsselt die Kommunikation zwischen seinem Client und dem Server mittels RSA.

Bedürfnisse des Zielumfeldes. Sollten also grundlegende Änderungen im Zielumfeld stattfinden, die z.B. dem bisher eher als gering eingestuften Kostenfaktor eine signifikant höhere Bedeutung zumessen, so kann die Gewichtung entsprechend angepasst werden. Die konkrete Bewertung der KO-Kriterien, bzw. inwiefern sie tatsächlich zum Ausschluss des evaluierten Softwareproduktes führen, obliegt dabei ebenfalls der Analyse und den Ansprüchen des Analytikers.

Dieses Verfahren ermöglicht es somit, durch z.B. Einführen neuer KO-Kriterien bzw. deren Auslegung und der Verschiebung der Gewichtung, auf veränderte Vorraussetzungen reagieren zu können, ohne den kompletten Rohdatensatz neu zu erheben.

4.1.6 Einblick in die Arbeitsmethodik

Neben einer Evaluationsmethodik wurde für die Durchführung eines Projektes dieser Komplexität auch eine tragfähige Arbeitsmethodik benötigt. Insbesondere die Breite der für das Projekt relevanten Themenkomplexe erzeugte die Notwendigkeit eines strukturierten Arbeitskonzeptes. Zentrale Aspekte waren hierbei:

- Aufgabenstrukturierung und –verteilung
- Kommunikationsmittel und –wege
- Dokumentenmanagement
- Zeitplanung
- Koordination der Labornutzung.

4.1.6.1 Competence Center

Da dieses Projekt Kompetenzen in großer Breite erforderte, wurden „Competence Center" (CCs) gebildet. Ein CC bestand jeweils aus zwei Personen, die als zentrale Ansprechpartner in Bezug auf den durch sie übernommenen Themenkomplex agierten. Die CC-Größe wurde bewusst auf zwei Mitglieder gesetzt, damit zum einen die Erreichbarkeit mindestens eines Mitgliedes in ausreichendem Maße gewährleistet werden konnte und zum anderen für alle drei von uns identifizierten Schwerpunkte (Infrastruktur, Synchronisation und Endgeräte) jeweils ein CC existieren konnte, dessen Mitglieder exklusiv diesem zugeordnet waren.

4.1.6.2 Kommunikation

Für die Kommunikation innerhalb des Projektteams wurden während der Planungsphase Mittel zur synchronen und zur asynchronen Kommunikation adaptiert. Synchrone Kommunikation bezeichnet Kommunikationsformen, bei denen der/ein Gesprächspartner umgehend auf die Äußerungen des jeweils anderen reagiert (z. B. Meetings, Telefon). Im Gegensatz dazu erfolgt bei asynchroner Kommunikation die Reaktion zeitversetzt (z. B. E-Mail)[44]. Beide Kommunikationsformen weisen Vor- und Nachteile auf.

Synchrone Kommunikation hat den Vorteil, dass Antworten schnell gegeben werden können und deshalb der Gedankenaustausch schneller möglich ist. Insbesondere zu Diskussionszwecken und zum Klären grundsätzlicher Fragestellungen ist die synchrone Kommunikation daher als das Mittel der Wahl anzusehen. Dem durch Anwesenheits- bzw. Teilnahmepflicht bedingten kontraproduktiven Effekt synchroner Kommunikation kann durch gezielten Einsatz asynchroner Kommunikationsmittel entgegengewirkt werden.

Wir entschieden uns für ein Mischkonzept aus synchroner und asynchroner Kommunikation. Die von uns genutzten Mittel synchroner Kommunikation waren regelmäßige Treffen und „Instant Messaging"[45] sowie bei Bedarf Telefonate. Die Treffen fanden zweimal wöchentlich statt und dienten hauptsächlich dem Vortragen des aktuellen Arbeitsstatus der einzelnen CCs sowie dem Definieren der folgenden Schritte. Während der weitestgehend getrennt durchgeführten Bearbeitung der verschiedenen Aufgaben durch die CCs kam für Nachfragen aus anderen CCs neben Telefonanrufen auch der Instant Messager ICQ zum Einsatz.

Ergänzend hierzu wurden als asynchrone Kommunikationsmittel eine Mailingliste sowie ein Projektforum genutzt. Die Mailingliste diente primär dazu, von externen Absendern

---

[44] Vgl. „Kommunikation in CSCW-Systemen" (Wolpers 1997).
[45] Wie z. B. die weit verbreiteten Programme ICQ oder AIM.

stammende an ein einzelnes Projektmitglied versandte E-Mails allen anderen Mitgliedern durch Weiterleitung an lediglich eine E-Mail-Adresse zukommen zu lassen. Fragen oder Kommentare, die an alle Projektmitglieder gerichtet waren, wurden nicht über die Mailingliste, sondern mittels eines eigens zu diesem Zweck eingerichteten Projektforums übermittelt.

4.1.6.3 Dokumentenmanagement

Das Projektforum diente neben dem Veröffentlichen von Fragen und projektrelevanten Internet-Adressen (Softwarehersteller, Produktseiten, externe Artikel etc.) auch der CC-übergreifenden Abstimmung sowie als für unsere Zwecke ausreichendes Dokumentenmanagementsystem. U. a. wurden im Forum die folgenden Dokumente von den einzelnen CCs veröffentlicht und jeweils auf dem aktuellen Stand gehalten:

- Teilberichte
- Installationsanweisungen
- Aktuelle Rechnerkonfigurationen
- Protokolle von Treffen und CC-internen Tätigkeiten
- Diskussionsgrundlagen und andere Quelldokumente
- Kontaktadressen und Telefonnummern aller Projektmitglieder.

Um dem asynchronen Charakter der forenbasierten Kommunikation Rechnung zu tragen und dennoch einen aktuellen Kenntnisstand aller Projektmitglieder sicherzustellen, war es notwendig, dass das Forum von jedem Projektmitglied mindestens einmal täglich besucht wurde.

4.1.6.4 Zeitplanung

Ein weiterer wichtiger Punkt der Arbeitsmethodik war eine für alle Projektmitglieder bindende Zeitplanung anhand von Meilensteinen (siehe Kapitel 4.1.4). Fixe Zeitpunkte waren hierbei das festgelegte Datum für das Ende des Projektes sowie zwei Zwischenpräsentationen. Eine Meilensteindefinition bestand aus fest umrissenen Aufgaben, die bis zu einem festgelegten Datum erledigt sein mussten, wobei die einzelnen Aufgaben jeweils den entsprechenden CCs zugeteilt wurden.

4.1.6.5 Koordination der Labornutzung

Auch die Nutzung des uns zur Verfügung stehenden Labors musste so koordiniert werden, dass keine Kollisionen bzw. Doppelbelegungen entstanden. Außerdem musste sichergestellt werden, dass das Labor stets in einem spezifizierten und benutzbaren Zustand vorgefunden wurde. Konnte die Arbeit im Labor von einem CC nicht so zu Ende geführt werden, dass das Labor vollständig lauffähig war, so musste dies im Forum vermerkt werden. Vor Aufnahme der Arbeit durch ein anderes CC wurde dann eine Sicherung des Ist-Zustandes und (gemäß Kapitel 4.1.1) eine Wiederherstellung der letzten lauffähigen Konfiguration durchgeführt.

4.2 Administration

Der nun folgende Abschnitt beschäftigt sich mit der Evaluation der von uns in Kapitel 3.1.1 in den Test aufgenommenen Administrationssoftware für mobile Endgeräte. Hierzu wurden, wie im Evaluationskonzept (Kapitel 4.1.5), zu untersuchende Kategorien identifiziert und anhand dieser die benötigten Evaluationsbögen entwickelt.

4.2.1 Kategorien

4.2.1.1 Die Kategorie Administration allgemein

Unter diese Kategorie fallen alle zu untersuchenden Fragestellungen, die nicht in eine der anderen Kategorien passen.

Systemvoraussetzungen

Welche Voraussetzungen müssen erfüllt sein, damit die Software eingesetzt werden kann? Die Benotung bezieht sich hierbei hauptsächlich auf das Ausmaß der Systemanforderungen. Geringe Mindestanforderungen bewirken eine gute Benotung.

Größe der Client- und Serversoftware

Die Größe der einzelnen Komponenten ist insofern interessant, als dass Ressourcen dafür bereitgestellt werden müssen. Die größere Gewichtung fällt hierbei auf die Client-Software, da man auf der Serverseite von ausreichenden Speicherkapazitäten ausgehen kann.

Geschwindigkeit

In Bezug auf die Geschwindigkeit liegt das Hauptaugenmerk auf der Performance bei gleichzeitiger Konfiguration vieler Endgeräte. Die Evaluation dieses Punktes erwies sich jedoch aufgrund der geringen Anzahl zur Verfügung stehender Endgeräte als in unserem Labor nicht durchführbar und muss gegebenenfalls zu einem späteren Zeitpunkt nachgeholt werden.

4.2.1.2 Die Kategorie Sicherheit

An dieser Stelle sollen einige Punkte aufgeführt werden, die bei der Verwendung von Administrationssoftware von besonderem Interesse sind.

Kennwortverwaltung

Die zentrale Administration und Verwaltung von Passwörtern kann erheblich zur Einhaltung von Sicherheitsrichtlinien dienen. Eine eingehende Betrachtung hierzu befindet sich in Kapitel 4.4 „Endgerätesoftware", da die tatsächlich realisierbaren Administrationsmöglichkeiten in Bezug auf Passwortregeln in starkem Maße von der auf dem Endgerät verwendeten Sicherheitssoftware abhängig sind.

Verschlüsselung des Netzwerkverkehrs

Bei der Administration, Analyse und Fernwartung der mobilen Endgeräte werden generell immer schützenswerte Daten durch das Netzwerk geleitet. Neben Sicherheitsmechanismen, die zusätzlich verwendet werden (z. B. VPN-Tunnel) ist es von zentralem Interesse, ob und wenn ja wie die Administrationssoftware von sich aus den Datenverkehr verschlüsselt (siehe Kapitel 2.2.2.4). Insbesondere ist hier die Stärke des verwendeten Algorithmus von Interesse.

Datensicherheit

Die Datensicherheit soll vor allem dahingehend untersucht werden, ob z. B. bei zentral gelagerten Backups der Administrator die Möglichkeit hat die Backups einzusehen. Dies würde datenschutzrechtliche Komplikationen hervorrufen. Ein weiterer Gesichtspunkt ist der Zugang zur Administrationssoftware selbst.

4.2.1.3 Die Kategorie Kosten

In dieser Kategorie werden die Kosten für die Software aufgeführt. Bei der zu untersuchenden Software handelt es sich um recht große Administrationsserver (im Fall von XTND um einen kombinierten Synchronisations- und Administrationsserver). Neben den Anschaffungskosten muss auch der Aufwand für Wartung und Support berücksichtigt werden. Daneben fallen auch Kosten für die Administration der Software selbst und für Schulungen der Mitarbeiter an.

4.2.1.4 Die Kategorie Benutzerverwaltung und Deployment

Hierbei handelt es sich um ein zentrales Thema bei Administrationssoftware. Es ist von besonderer Bedeutung, ob einzelne Endgeräte differenziert angesprochen werden können und ob es möglich ist, auf Basis von Gruppeneinteilungen bestimmte Standardkonfigurationen über mehrere Geräte hinweg zu verteilen.

Gruppenverwaltbarkeit

In Abhängigkeit von Aufgabengebiet und Sicherheitseinstufung ist es notwendig, das Endgerät unterschiedlich zu konfigurieren. Unterschiedliche Nutzergruppen benötigen mit hoher Wahrscheinlichkeit unterschiedliche, auf ihre Tätigkeiten abgestimmte Umgebungen. Außerdem können erhöhte Sicherheitseinstufungen Passwortregeln mit erhöhter Sicherheit oder das Verhindern des Anlegens von Backups notwendig machen. Es muss also möglich sein, Benutzergruppen effektiv zu verwalten. Auf Windows-Plattformen ist eine Übernahme der Gruppen und Benutzer aus dem Active Directory wünschenswert.

Deployment

Die Verteilung von Konfigurationen auf die Endgeräte bezeichnet man als „Deployment". Bei einer großen Anzahl von Endgeräten, die der organisationsinternen Infrastruktur angepasst werden müssen, ist es aufwendig und deshalb ineffektiv, jedes einzelne Gerät per Hand zu konfigurieren. Es muss also die Möglichkeit geben, eine Standardkonfiguration (gruppen- oder nutzerspezifisch) zu erzeugen und diese möglichst einfach auf eine potentiell hohe Anzahl von Endgeräten zu verteilen. Dabei stellen sich z. B. folgende Fragen: Wie einfach können Konfigurationen erstellt werden? Wie schnell und einfach können diese verteilt werden? Ist für die Installation eine besondere Software nötig? Ist eine besondere Partnerschaft zwischen dem zu konfigurierenden Endgerät und dem installierenden „Companion PC notwendig?

4.2.1.5 Die Kategorie Geräteverwaltung

Um die im Umlauf befindlichen mobilen Endgeräte sinnvoll administrieren zu können, ist es notwendig, eine Möglichkeit zur Abfrage des Bestands und der jeweiligen Konfiguration zu haben. Ebenso kann es erforderlich sein, die Konfigurationen an unterschiedliche Klassen von Endgeräten anzupassen.

Heterogene Endgeräte

Generell ist zu erwarten, dass innerhalb eines Bestandes verschiedene Geräteklassen vorhanden sind. Es muss also möglich sein, neben den hier betrachteten Pocket-PCs auch Gerätetypen wie Palms, Laptops oder Smartphones zu verwalten. Dabei gilt es auch zu

betrachten, wie gut die unterschiedlichen Konfigurationen zu den einzelnen Geräteklassen in Bezug gesetzt werden können.

Bestandsverwaltung

Um in einem Unternehmen die Übersicht über die im Umlauf befindlichen Endgeräte zu behalten, ist eine Bestandsverwaltung unabdingbar. Diese Bestandsverwaltung ist im Idealfall ebenfalls in die Administrationssoftware integriert. Dabei ist insbesondere ein über das simple Auflisten der existierenden Geräte hinausgehendes Verfahren zur flexiblen Reporterstellung wünschenswert. Nur so ist es überhaupt möglich alle Geräte zu identifizieren, auf denen beispielsweise der hochgradig wichtige Sicherheitspatch noch nicht installiert wurde.

4.2.1.6 Die Kategorie Softwareverwaltung

Betriebssystemkontrolle

Viele administrative Aufgaben beziehen sich auf die Gewährleistung der korrekten Einstellungen auf dem Endgerät. Diese Einstellungen können je nach Endgerät mehr oder minder komplex ausfallen. Um also dem Endnutzer diese spezifischen Aufgaben abzunehmen, sollte es möglich sein, über die Administrationssoftware auf die wesentlichen Komponenten des Betriebssystems zuzugreifen.

Softwareabgleich

In vielen Fällen wird für bestimmte Aufgaben spezielle Software benötigt. Sobald andere als die auf dem Endgerät integrierten Programme genutzt werden, ist es wünschenswert, diese zentral verwalten zu können. Dabei stellt sich auch die Frage nach der Fähigkeit der Administrationssoftware zu einer evtl. notwendigen Lizenzverwaltung.

4.2.1.7 Die Kategorie Kommunikationskanäle

Zugangskanäle

Die Kategorie der Kommunikationsmethoden bezieht sich auf die möglichen Verbindungsarten, mittels derer das Endgerät mit dem Administrations-Server Kontakt aufnimmt. Es ist auch von Relevanz, ob für die Installation der Clientsoftware ein Companion-PC notwendig ist.

4.2.1.8 Die Kategorie Remoteanalyse

Hier handelt es sich um zentrale Anforderungen an eine Administrationssoftware. Es ist von signifikanter Bedeutung, dass es möglich ist, aus der Ferne alle Arten von Informationen über den Zustand eines Endgerätes zu erhalten und bei Problemen eingreifen zu können.

Logging

Unter Logging versteht man die Protokollierung verschiedenster Ereignisse. Dazu zählen nicht nur Fehler (s. u.), sondern auch alle Arten von erfolgreich durchgeführten Aktionen wie erfolgreiches Einloggen in das System oder eine reibungslos durchgeführte Synchronisation. Die Einbeziehung von Abfragen zu bestimmten Suchkriterien ist ebenfalls wünschenswert. Zu berücksichtigen ist hierbei, dass es zu daten- und arbeitsschutzrechtlichen Problemen kommen kann, sollte mit dem Logging eine Überwachung der Endbenutzer möglich sein bzw. die Software zu diesen Zwecken missbraucht werden.

Fehlerprotokollierung

Die Fehlerprotokollierung ist ein Teilaspekt des oben erläuterten Loggings. Es muss dem Administrator möglich sein, anhand der Fehlerprotokollierung Fehlerquellen auf dem

Endgerät oder dem Administrationsserver zu lokalisieren. Dies erfordert, dass die protokollierten Meldungen entsprechend aufschlussreich und genau sind. Das Speichern von Fehlerprotokollen kann sowohl auf dem Server als auch auf dem Endgerät sinnvoll sein.

Fehlerbehebung

Die Remote-Fehlerbehebung ist ein weiterer Aspekt einer Administrationssoftware. Endnutzer wie auch Administrator haben ein berechtigtes Interesse daran, dass das Endgerät bei Auftreten eines Problems nicht unbedingt physikalisch dem Administrators übergeben werden muss. Fehlerbehebung und Fehlerprotokollierung gehen natürlich Hand in Hand.

4.2.1.9 Die Kategorie Usability

Die Prinzipien der Usability wurden bereits im Evaluationskonzept (Kapitel 4.1.5.4) ausführlich vorgestellt und finden auch hier ihre Anwendung.

4.2.2 **Extended Connect Server** (ServKonfig 04)

Der Extended Connect Server (weiterhin als XTND-Server bezeichnet) der Firma Extended Systems hat als primäres Aufgabengebiet die Datensynchronisation. Neben dem Synchronisationsmodul, das bei der Evaluation der Synchronisationssoftware genauer untersucht wird, besitzt der XTND-Server ein umfangreiches Administrationsmodul, das an dieser Stelle betrachtet werden soll.

4.2.2.1 **Administration Allgemein** (+)

Tabelle 4-6: XTND Admin – Administration Allgemein

Allgemeines	Bewertung
Systemvoraussetzungen	1
Größe der Komponente	2
Geschwindigkeit	3

Die Hard- und Softwareanforderungen an das System halten sich in Grenzen, die Software ist sogar verhältnismäßig genügsam. Eine kleine Besonderheit ist zu beachten. Bei der Synchronisation muss auf dem gleichen Computer ein aktiviertes Outlook2000 installiert sein, da der Server auf das von Outlook benutzte CDO-Modul zugreift. Dieser Umstand wird durch das Synchronisationsmodul verursacht.

Die Größe der zu installierenden Komponenten ist ebenfalls als verhältnismäßig gering einzuschätzen. Der auf den Endgeräten installierte Client wird in einem Setup verpackt, dessen Größe in unseren Testläufen meist nicht mehr als 5 MB erreichte. Diese resultiert eher aus den durchzuführenden Setup-Aufgaben, denn sowohl der Client als auch der Desktopconnector sind nur wenige hundert Kilobyte groß.

Unter Windows NT ist zu beachten, dass es keine USB-Unterstützung gibt. Dies liegt nicht an der zu installierenden Software, sondern daran, dass es grundsätzlich keine USB-Unterstützung für diese Plattform gibt. Die Installation via USB-Port war erst ab der Version 3.6 möglich.

Über die allgemeine Ausführungsgeschwindigkeit sowohl der Administrations- als auch der Synchronisationsaufgaben können wir in diesem Fall keine fundierten Angaben machen, da es aufgrund der geringen Anzahl zur Verfügung stehender Endgeräte nicht möglich war, einen aussagekräftigen Stresstest durchzuführen.

In Bezug auf die Geschwindigkeit bei der Erstellung administrativer Tasks gibt es Positives und Negatives zu berichten. Das Abrufen von Log-Informationen, Systeminformationen und ähnlichem geht sehr schnell. Das Einrichten neuer Benutzer hingegen ist weniger komfortabel möglich und benötigt unnötig viel Zeit. Hierzu an anderer Stelle mehr (siehe Kapitel 4.2.2.3).

Allgemeines Gesamt	2

4.2.2.2 Sicherheit (+++)

Tabelle 4-7: XTND Admin - Sicherheit

Sicherheit	Bewertung
Kennwortverwaltung	4
Verschlüsselung des Netzwerkverkehrs	2
Datensicherheit	4

Wie bereits in der Kategorienbeschreibung dargelegt, widmet sich dieser Teil der Evaluation ausschließlich der für den administrativen Teil der Software spezifischen Sicherheit.

Die auf den Endgeräten benutzten Passwörter können vom Administrator nicht eingesehen werden. Es besteht zwar die Möglichkeit, ein „Power-On-Passwort" zu erzwingen, in Tests hat sich jedoch herausgestellt, dass dies keinen Einfluss auf die Synchronisation der Groupwaredaten hat. Erst beim Abgleich mit einem persönlichen Ordner greift diese Restriktion, zu diesem Zeitpunkt sind aber E-Mails, Termine etc bereits auf dem neuesten Stand. Dies stellt eine massive Sicherheitslücke dar. Immerhin ist es nicht möglich, die Passwortabfrage abzuschalten oder Passwörter zu speichern.

Die bei der Administration bzw. Synchronisation übertragenen Daten werden mittels des RSA-Algorithmus verschlüsselt. Zu diesem Zweck wird beim ersten Login mit dem Endgerät ein „RSA-Fingerprint" ausgetauscht, der von der Proxy-Komponente generiert wird. Zusätzlich kann bei Bedarf eine SSL-Verschlüsselung zwischen Proxy-Komponente und Server hinzugeschaltet werden. Nach Angaben eines Vertriebsbeauftragten der Firma Extended Systems wurde das RSA-Kryptographie-Modul offiziell von RSA-Security[46] zertifiziert.

Benutzerdaten können zentral auf dem Server abgelegt werden. Dies schließt sowohl Backups als auch persönliche Daten ein. Diese werden jedoch auf dem Server nicht verschlüsselt, es sei denn, es wird ein verschlüsseltes Filesystem[47] benutzt. Das verhindert aber nicht, dass der Administrator Einblick in die Daten des Endbenutzers erhält. Ein solcher Umstand kann jedoch diverse daten- und arbeitsschutzrechtliche Konsequenzen nach sich ziehen.

Positiv ist, dass es möglich ist, differenzierte Backups von Endgeräten zu erstellen. Die Differenzierung auf einen bestimmten Nutzer gestaltet sich dabei jedoch recht umständlich.

Die serverseitigen Konfigurationen können in einer Datei gesichert werden, was einen schnellen Wechsel zwischen unterschiedlichen Einstellungen und schnelle Backups der Serverkonfigurationen ermöglicht. Das Administrationsprogramm ist nicht zusätzlich durch eine Passwortabfrage gesichert. Somit ist ein massiver Eingriff auf die Endgeräte und dessen Daten möglich, sobald ein potentieller Angreifer Zugriff auf einen Administrationsrechner bekommt.

Sicherheit Gesamt	3

4.2.2.3 Kosten

[46] http://www.rsasecurity.com [26.03.2003].
[47] Bei Windows-NT-basierten Systemen ermöglicht dies das Betriebssystem.

Extended Sytems hat ein klar strukturiertes Preismodell. Die Kosten für den Server sind fix (Server Enterprise: 20.000,- €), die Preise für einzelne Clientlizenzen sind nach deren Anzahl gestaffelt (je mehr Clients, desto geringer die Lizenzgebühr pro Client). Da die Administrationskomponente von XTND ein Bestandteil der Synchronisationssoftware ist („Synchronisation Mittels XTND"), wird hier nicht näher darauf eingegangen. Eine Preisliste ist der Komponentenauswahl in Kapitel 3.1.2.3 zu entnehmen.

Kosten Gesamt:	**2**

4.2.2.4 Benutzerverwaltung und Deployment (++)

Tabelle 4-8: XTND Admin – Benutzergruppen und Deployment

Benutzergruppen und Deployment	**Bewertung**
Gruppenverwaltbarkeit	3
Deployment	1

Benutzergruppen können sehr leicht eingerichtet werden. Hierbei besteht völlige Freiheit bei der Namensvergabe. Die Nutzer und Nutzergruppen werden aus dem Active Directory übernommen, allerdings können keine eigenen Benutzer erstellt werden (nur via Active Directory). Für unterschiedliche Gruppen können jeweils unterschiedliche Konfigurationen angelegt werden.

Ebenso besteht die Möglichkeit, nutzer- und gruppenspezifische Dateien zu verteilen. Allerdings ist dafür der Einsatz des Windows-Explorers (oder eines beliebigen anderen Filemanagers) notwendig. Der Administrator muss also die entsprechenden Dateien manuell in ein von der Software angelegtes Verzeichnis kopieren bzw. sie daraus löschen.

Auffällig ist das komplette Fehlen nutzerspezifischer Eingriffsmöglichkeiten. Dies kann sehr lästig sein, wenn bestimmte Einstellungen eben nur für einen spezifischen Nutzer gelten sollen. Es gibt hierfür dann lediglich den Umweg über das Anlegen einer Benutzergruppe mit nur einem Nutzer. Auch gestaltet sich das Umgruppieren wenig komfortabel. Der einzig gangbare Weg besteht darin, einen Nutzer aus einer Gruppe zu entfernen und in eine andere einzutragen. Es ist also kein direkter Transfer möglich. Ebenso gibt es keine Warnungen, wenn ein Benutzer in mehreren Gruppen vertreten ist. Dies ist nicht unbedingt schädlich, kann aber zu Verwirrungen führen.

Die initiale Konfiguration gestaltet sich dank eines gut verständlichen Installationsprogramms recht angenehm. Alle möglichen Einstellungen werden in Dialogen abgefragt. Die so generierte Setup-Datei kann dann z. B. zentral auf einem File-Server abgelegt und von jedem Endbenutzer einer Gruppe ausgeführt werden (natürlich in Verbindung mit einem Desktop-PC). Das erste Setup dauert pro Endgerät ca. 10 Minuten. Hierbei ist es egal, ob das Endgerät via USB oder serieller Schnittstelle mit dem Arbeitsplatzcomputer verbunden ist

Ebenso kann man initial einstellen, ob der Nutzer später die Konfiguration seiner Clientsoftware ändern darf. Nach der Erstinstallation ist dies dann nur noch über so genannte „Profiles" möglich, welche hierzu aber erst aktiviert werden müssen. Dann ist es sogar möglich, unterschiedliche Konfigurationen auf dem Client zu speichern.

Benutzergruppen und Deployment Gesamt	**2**

4.2.2.5 Geräteverwaltung (++)

Tabelle 4-9: XTND Admin Geräteverwaltung

Geräteverwaltung	Bewertung
Heterogene Endgeräteklassen	2
Bestandsverwaltung	5

Es wird ein weites Spektrum an mobilen Endgeräten unterstützt. Hierbei werden alle zurzeit auf dem Markt befindlichen relevanten Systeme abgedeckt. Die Möglichkeiten der Administration wurden allerdings, wie im Projektziel definiert, nur für PocketPC-Systeme untersucht. Die unterschiedlichen Geräteklassen werden innerhalb von XTND-Server strikt voneinander getrennt behandelt. Dabei sind aber bei der Dateiverteilung Verweise auf gleiche Verzeichnisse möglich.

Es können zahlreiche Informationen über die Endgeräte eingeholt werden, z. B. Geräteversionen, eingetragene Benutzer. Leider ist eine sinnvolle Inventarisierung und somit auch eine Momentaufnahme des zu einem bestimmten Zeitpunkt vorhandenen Inventars nicht möglich. Reports können nicht in der von uns gewünschten Flexibilität erzeugt werden, was die Verwaltung weiter erschwert.

Geräteverwaltung Gesamt	3

4.2.2.6 Softwareverwaltung (++)

Tabelle 4-10: XTND Admin - Softwareverwaltung

Softwareverwaltung	Bewertung
Betriebssystemkontrolle	5
Softwareabgleich	4

Die Möglichkeiten des XTND-Servers bzgl. der Betriebssystemkontrolle sind sehr eingeschränkt. Es kann nicht auf systemeigene Einstellungen zugegriffen werden. Der Zugriff auf individuelle Hardwarekomponenten (Modem, Infrarot-Schnittstelle, „Rucksäcke" etc.) ist unmöglich.

Die Anzahl an Optionen bei der Remote-Installation neuer Software hält sich ebenfalls in Grenzen. Aufgespielte Programmpakte können zwar zur Installation angestoßen werden, eine Deinstallation ist aber nicht mehr ohne Weiteres möglich. Es ist auch nicht vorgesehen, dass softwareeigene Einstellungen vorgenommen werden, es sein denn, eine Art „Ini-File" der zu installierenden Software wird zusätzlich überspielt. Dies entzieht sich aber der Kontrolle des XTND-Servers.

Eine Bestandsaufnahme der verwendeten Software gestaltet sich als ebenso unkomfortabel wie bei der Verwaltung der Endgeräte. Es ist nur möglich, sich über Log-Dateien einen Überblick über die installierten Programme zu verschaffen. Eine globale Inventarisierung ist somit faktisch unmöglich. Als Konsequenz ist ebenfalls keinerlei Lizenzverwaltung in den XTND-Server integriert. Es ist also schwer, die Übersicht über die Gesamtheit der genutzten mobilen Endgeräte zu behalten.

Softwareverwaltung Gesamt	4

4.2.2.7 Kommunikationskanäle (++)

Tabelle 4-11: XTND Admin - Kommunikationskanäle

Kommunikationskanäle	Bewertung
Zugangsmethoden	1

Für eine erfolgreiche Kommunikation ist lediglich eine beliebige IP-Verbindung notwendig. Dies kann sowohl über GSM oder GPRS geschehen. Eine Einwahl über einen RAS-Server in die DMZ ist ebenfalls möglich.

Zusätzlich ist auch die Verbindung über den mitgelieferten „DesktopConnector" möglich. Hierbei wird der PDA mittels serieller oder USB Schnittstelle mit einem PC verbunden. Dieser PC stellt dann die Brücke zum Internet dar. So wird eine höhere Übertragungsgeschwindigkeit erzielt, da die am PC vorhandene Bandbreite für den PDA nutzbar ist. Der Umgang mit dem DesktopConnector ist in diesem Zusammenhang sehr einfach. Das Programm hat eine Größe von lediglich 268 Kilobyte und passt somit bequem auf eine Diskette oder einen USB-Stick. Er erfordert kein Setup und kann sofort gestartet werden. Somit ist es möglich ihn überall einzusetzen (Verbindungskabel zum PDA oder eine Infrarotschnittstelle vorausgesetzt).

Zusammenfassend kann gesagt werden, dass eine optimale Mobilität gewährleistet ist, da ein Companion-PC nicht benötigt wird, auch wenn durch diesen eine höhere Performance erzielt werden kann. Dies bezieht sich aber immer auf den laufenden Betrieb. Für die Erstinstallation ist ein DesktopPC notwendig.

Kommunikationskanäle Gesamt	1

4.2.2.8 Remote Analyse (+++)

Tabelle 4-12: XTND Admin – Remote Analyse

Remote Analyse	Bewertung
Logging	3
Fehlerprotokollierung	2
Fehlerbehebung	5

Der XTND-Server verfügt über eine gute Ereignisprotokollierung. Diese Protokolle sind sowohl auf dem Client (direkt nach der Abarbeitung der aktuellen Aufgaben) als auch auf dem Server einsehbar und werden serverseitig auch abgespeichert. Auf dem Client ist lediglich das letzte Protokoll einsehbar. Leider fehlt es an einer Suchfunktion, so dass man den Zeitpunkt des Ereignisses recht genau kennen muss, um eine gesuchte Meldung finden zu können. Die Protokolle sind recht umfangreich. Es wird vermerkt, wer wann welche Aktion ausgelöst hat. Die Protokollierung dient aber primär dazu Synchronisationsaufgaben zu verfolgen.

Die Fehlerprotokollierung ist ebenso umfangreich wie die „normalen" Logs. Die Speicherung ist ebenfalls identisch. Bei Auftreten von Fehlern vermissten wir eine Erklärung, oder zumindest ausführliche Erläuterung der Fehlernummer in der Online-Hilfe. Fehlermeldungen von z. B. Exchange werden durchgereicht und sind somit ebenfalls in den Protokollen einsehbar.

Die Möglichkeiten des XTND-Servers zur Fehlerbehebung sind sehr beschränkt. Es gibt keinen Remote-Desktop oder Vergleichbares. Fehler lassen sich demzufolge nur durch Neuinstallation einzelner Komponenten beheben, sofern es sich um Programme handelt, die nachträglich installiert wurden. Bei Pocket-PC-eigenen Modulen hilft dies nicht.

Remote Analyse Gesamt	**3**

4.2.2.9 Usability (++)

Tabelle 4-13: XTND Admin - Usability

Usability	**Bewertung**
Sprache	
Verfügbar in deutscher Sprache	Nein
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	3
Daten können wie von der Aufgabe gefordert eingegeben werden	2
Informationen und Bedienelemente befinden sich am richtigen Platz	2
Alle benötigten Informationen sind auf dem Bildschirm zu finden	2
Ausgaben sind zweckmäßig und verständlich	3
Wiederholfunktion für wiederkehrende Arbeitsschritte sind verfügbar	2
Selbstbeschreibungsfähigkeit	
Bei Bedarf sind Kontexthilfe oder weitergehende Informationen abrufbar	1
Meldungen sind sofort verständlich	3
Rückmeldungen können einer Ursache eindeutig zugeordnet werden	2
Art und Zusammensetzung geforderter Eingaben sind leicht erkennbar	1
Auswirkungen von Aktionen sind hinreichend ersichtlich	2
Aktuelle Eingabeposition ist eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) ist eindeutig erkennbar	2
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen ist möglich	1
Der aktuelle Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann Abgebrochen werden	n/a
Erwartungskonformität	
Bearbeitungsschritte sind vorhersagbar	4
Die Bearbeitungszeit ist abschätzbar	3
Eine einheitliche Verwendung von Begriffen und Symbolen ist gewährleistet	1

Die Ausführung einer Operation führt zum erwarteten Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	3
Versehentliches Auslösen von Aktionen ist unmöglich oder wird erschwert	3
Bei Fehlern werden zweckmäßige Hinweise zur Ursache und Behebung geliefert.	3
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	2
Erlernbarkeit	
Schnelles Erlernen der Bedienung	4
Intuitive, selbsterklärende Benutzung möglich	4
Nur wenige Detailkenntnisse zur Bedienung nötig	4
Hilfestellung bei Bedarf verfügbar	1
Benutzerhandbuch	
Qualität des Benutzerhandbuchs	3
Verfügbar in deutscher Sprache	Nein
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	Nein
Installations- / Administrationshandbuch	
Qualität des Installations- / Administrationshandbuch	3
Verfügbar in deutscher Sprache	Nein
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	nein
Support	
Qualität des Supports	1

Die hier aufgeführte Tabelle entspricht dem im Kapitel „Evaluationskonzept und Methodik" vorgestellten Konzept. Auf eine differenzierte Kommentierung der einzelnen Punkte wurde an dieser Stelle verzichtet.

Usability Gesamt	**2**

4.2.2.10 Besonderheiten / Ausblick (+)

Der große Kundenstamm (siehe Referenzen auf der Homepage des Herstellers) und die enge Kooperation mit dem Hersteller des Pocket-PC-Betriebssystems Microsoft lassen vermuten, dass dieses Produkt auch in Zukunft weiterentwickelt wird und dementsprechend weiterhin Support zur Verfügung steht.

4.2.2.11 Gesamtbewertung

Tabelle 4-14: XTND - Gesamtwertung

Gesamtwertung	Bewertung
Administration allgemein	2
Sicherheit	3
Administration	3
Usability	2
Kosten	2

XTND bietet in Bezug auf die Administration nur grundlegende Funktionalität und kann nicht mit dem benötigten Funktionsumfang aufwarten. Gravierende Einbußen muss man vor allem bei der Softwareverwaltung und der Betriebssystemkontrolle hinnehmen. Die Administrationskomponente kann man also als durchaus wünschenswerte Erweiterung der Synchronisationssoftware betrachten, aber nicht als ernst zu nehmende Konkurrenz zu Spezialsoftware wie Afaria.

4.2.3 **Xcellenet Afaria** (ServKonfig 01+03)

Das Programm Afaria der Firma Xcellenet ist eine auf alle möglichen Arten der Administration von mobilen Endgeräten ausgerichtete Spezialsoftware. Eine Besonderheit von Afaria ist die interne Strukturierung durch so genannte „Channels". Diese sind aufgabenbezogen und gliedern sich in folgende Bereiche:

- Backup Manager Channels
  - Dienen der Sicherung von Anwendungen und Daten
- Configuration Manager Channels
  - Dienen der Konfiguration der mobilen Endgeräte
- Document Manager Channels
  - Dienen der Verteilung von Dokumenten und Dateien
- Inventory Manager Channels
  - Dienen der Abfrage von Hard- und Softwareausstattung der Endgeräte
- Software Manager Channels
  - Dienen der Verteilung und Installation von Software auf den Endgeräten
- Session Manager Channels
  - Dienen der Automatisierung weitergehender Aufgaben
- Transmitter Listing Manager Channels
  - Dienen der Erstellung von Transmittern

Auf die hier aufgeführten Channels wird im weiteren Verlauf an entsprechender Stelle eingegangen. Der Transmitter Listening Channel wird hierbei außer Acht gelassen.

4.2.3.1 **Administration Allgemein** (+)

Tabelle 4-15: Afaria – Administration Allgemein

Allgemeines	Bewertung
Systemvoraussetzungen[48]	3
Größe der Komponente	2
Geschwindigkeit	3

Die Systemanforderungen von Afaria sind im Vergleich z. B. zum Extended Connect Server als verhältnismäßig hoch zu bewerten. Für den Produktiveinsatz muss zusätzlich eine vollwertige Datenbank (MS SQL Server oder Oracle) — für optimale Performance möglichst auf einem eigenen Server — installiert sein. Für den Laborbetrieb reicht jedoch die reduzierte „Microsoft Database Engine (MSDE aus. Erfreulich wenig Platz nimmt die Clientsoftware auf dem Endgerät in Anspruch. Lediglich 600 Kilobyte fallen hierfür an.

Über die allgemeine Ausführungsgeschwindigkeit der Administrations- und der Synchronisationsaufgaben können wir in diesem Fall keine fundierten Angaben machen, da es mit der geringen Anzahl uns zur Verfügung stehender Endgeräten nicht möglich war, einen aussagekräftigen Stresstest durchzuführen.

---

[48] Siehe: http://www.afaria.com/public/products/afaria/technology.asp [26.03.2003].

Die administrativen Aufgaben gehen innerhalb einer bestehenden Infrastruktur recht schnell. Die initiale Einrichtung nach individuellen Bedürfnissen gestaltet sich allerdings als etwas gewöhnungsbedürftig.

Allgemeines Gesamt	3

4.2.3.2 Sicherheit (+++)

Tabelle 4-16: Afaria - Sicherheit

Sicherheit	Bewertung
Kennwortverwaltung	6
Verschlüsselung des Netzwerkverkehrs	2
Datensicherheit	4

Alle Fragen zum Thema Kennwortverwaltung können einfach beantwortet werden: Es gibt schlichtweg keine. Der Nutzer kann keiner Passwort-Policy unterworfen werden. Es besteht lediglich die Möglichkeit, eine Passwortabfrage zu verlangen, wenn der Endnutzer die Einstellungen des Afaria-Clients auf dem mobilen Gerät verändern möchte. Es kann ihm aber auch untersagt werden, in die Konfiguration einzugreifen. Dies bezieht sich jedoch lediglich auf die Pocket-PC-internen Passwörter. Auf die Verwaltung von Passwörtern und zugehörigen Policies in Bezug auf zusätzliche Endgerätesoftware wird an entsprechender Stelle näher eingegangen.

Laut den Angaben des technischen Supports von Xcellenet wird bei der Datenverschlüsselung zwischen den Endgeräten und dem Server die auf RSA basierende „CryptoAPI"[49] von Microsoft verwendet (der Einsatz der CryptoAPI beschränkt sich auf Win32 und PocketPC Clients). Die reine Datenübertragung findet hierbei mittels des HTTP-Protokolls statt (HTTP-Encapsulation), was es ermöglicht, Webproxies zur erhöhten Sicherheit einzusetzen. Zusätzlich kann über die Sicherheitseinstellungen des Afaria- Transmitters eine SSL-Verbindung hinzugeschaltet werden:

„A Server Certificate, residing on the Server; and the Certificate from the Certificate Authority that signed the Server Certificate, residing on the Client." (AfariaSpec 2003)[50]

Benutzerdaten können zentral auf dem Server abgelegt werden. Dies schließt sowohl Backups als auch persönliche Daten ein. Diese werden aber auch bei Afaria auf dem Server nicht verschlüsselt, es sei denn, es wird ein verschlüsseltes Filesystem[51] benutzt. Auch das verhindert jedoch nicht, dass der Administrator Einblick in die Daten des Endbenutzers erhält, was aus daten- und arbeitsschutzrechtlicher Sicht durchaus unerwünscht sein kann.

Bei der erstmaligen Verbindung eines Endgerätes mit dem Afaria-Server wird jedem Gerät intern eine eindeutige Identifikationsnummer (UID) zugewiesen. Backups werden in einem mit dieser UID bezeichneten Verzeichnis abgelegt, wodurch eine eindeutige Zuordnung gewährleistet ist. Wie bereits erwähnt, geschieht dies allerdings unverschlüsselt und die gesicherten Dateien sind somit vom Administrator einsehbar.

---

[49] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wcesecur/htm/_wcesdk_Using_the_Cryptography_API.asp [26.03.2003].
[50] http://www.xcellenet.com/public/products/afaria/technology.asp [26.03.2003].
[51] Bei Windows-NT-basierten Systemen mit Bordmitteln möglich.

Die serverseitigen Konfigurationen können in einer Datei gesichert werden, was einen schnellen Wechsel zwischen unterschiedlichen Einstellungen und schnelle Backups der Konfigurationen ermöglicht.

Das Administrationsprogramm wird, wie auch bei XTND, nicht zusätzlich durch eine Passwortabfrage gesichert. Somit ist ein Zugriff auf die Endgeräte und deren Daten möglich, sobald Dritten der Zugang zu einem angemeldeten Administrationsrechner zur Verfügung steht.

Leider ist für Afaria keine Proxy-Komponente verfügbar, die sich nahtlos in unsere Topologie eingliedern ließe. Angaben eines Vertriebsmitarbeiters zufolge sei es jedoch möglich, eine entsprechende Komponente auf gezielte Anfrage hin zu entwickeln.

Sicherheit Gesamt	**4**

4.2.3.3 Kosten

Tabelle 4-17: Afaria - Kosten

Kategorie Kosten	**Bewertung**
Einmalige Kosten	
Anschaffungskosten	3
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	3
Schulungsmaßnahmen für die Administration der Software	3
Schulungsmaßnahmen für die Benutzer	2
Aufwand für die initiale Installation und Konfiguration der Komponenten	3
Laufende Kosten	
Administration	3
Zusätzliche Kosten für Support-/Wartungsvertrag	3

Eine detaillierte Kostenabschätzung für die Einführung und den laufenden Betrieb von Afaria gestaltet sich problematisch. Eine genaue Preisliste steht nicht zur Verfügung, da XcelleNet auf das Projektgeschäft setzt. Bei telefonischer Rücksprache ergab sich, dass sich typische Projekte in Größenordnungen von 1000 Clients und mehr bewegen. Neben einer Lizenzgebühr pro Client fällt ebenfalls eine Serverlizenz an. Etwas ungewöhnlich ist dabei die Tatsache, dass die Kosten für die Serverlizenz ebenfalls von der Anzahl der Clients abhängig sind. Um einen Anhaltspunkt für die anfallenden Kosten zu geben, wurden von uns 100 Clients als Grundlage für eine Beispielrechnung angenommen.

- Lizenzgebühr pro Client: 127,- €
- Lizenzgebühr für den Server: 7000,- €

Eine Serverlizenz für bis zu 500 Clients würde ca. 16.000,- € kosten. Außerdem wird vom Hersteller vorgesehen, dass die Installation einer entsprechenden Infrastruktur mit evtl. mehreren Transmittern im Rahmen eines Projektvertrages durch Mitarbeiter von Xcellenet durchgeführt wird.

Ein weiterer Kostenfaktor ist die von Afaria vorausgesetzte Datenbank. Sowohl Oracle als auch MSSQL verursachen zum einen Anschaffungskosten und müssen zum anderen ebenfalls installiert und administriert werden.

Aufgrund der eindeutigen Ausrichtung auf das Projektgeschäft ist eine Abschätzung der Kosten bzgl. Support- und Wartungsverträgen ebenfalls nicht möglich, sondern muss Gegenstand von Verhandlungen sein.

Kosten Gesamt	3

4.2.3.4 Benutzerverwaltung und Deployment (++)

Tabelle 4-18: Afaria – Benutzerverwaltung und Deployment

Benutzergruppen und Deployment	Bewertung
Gruppenverwaltbarkeit	3
Deployment	2

Benutzergruppen können mit Afaria sehr leicht eingerichtet werden. Hierbei besteht völlige Freiheit bei der Namensvergabe. Sehr einfach können auch Nutzer aus dem Active Directory übernommen werden, das Erstellen neuer Benutzer muss auch hier mittels des Active Directories geschehen. Für die unterschiedlichen Gruppen können jeweils unterschiedliche Konfigurationen angelegt werden.

Ebenso besteht die Möglichkeit, nutzer- und gruppenspezifische Dateien zu verteilen. Dies geschieht im Wesentlichen über so genannte „Channels", die vom Endbenutzer abonniert werden. Auf diesem Wege können beliebige Daten und Dateien immer auf dem neuesten Stand gehalten werden. Das Einspielen geänderter Dateien vom Endgerät zum Server hin ist allerdings nicht möglich. Die Channels dienen also nur zur Informationsverteilung und nicht als Groupwareverzeichnis.

Es gibt keine nutzerspezifischen Eingriffsmöglichkeiten in die Betriebssystemeinstellungen. Dies kann nachteilig sein, wenn bestimmte Einstellungen eben nur für einen spezifischen Nutzer gelten sollen. Auf Anfrage bei Xcellenet wurde uns mitgeteilt, dass es sich hierbei um einen grundsätzlichen Design-Fehler in der Software handle, dessen sich der Hersteller bereits bewusst sei. Eine Lösung hierfür sei jedoch in absehbarer Zeit nicht zu erwarten.

Die initiale Konfiguration der Clients gestaltet sich dank eines gut verständlichen Wizards als recht angenehm. Alle möglichen Einstellungen werden in Dialogen abgefragt. Hierbei lässt sich auch festlegen, welche der Einstellungen der Nutzer ändern darf[52]. Die so generierte Setup-Datei kann dann auf einem zentralen File-Server abgelegt und von jedem Endbenutzer einer Gruppe auf seinem eigenen Arbeitsplatz-PC ausgeführt werden. Für die Erstinstallation ist es notwendig, dass ein konfiguriertes „Active Sync" auf dem installierenden Desktop-PC eingerichtet ist und zwischen diesem und dem mobilen Endgerät eine Partnerschaft besteht. Der Afaria-Client wird dann mittels ActiveSync auf dem Endgerät installiert. Ein Installationsprogramm, das, ähnlich wie bei XTND, eine eigene Komponente zur Kommunikation mit dem PDA enthält, ist für Afaria nicht verfügbar.

Benutzergruppen und Deployment Gesamt	3

[52] Hierbei ist es sogar möglich, dem Nutzer jegliche Konfigurationsmöglichkeit zu nehmen.

4.2.3.5 Geräteverwaltung (++)

Tabelle 4-19: Afaria - Geräteverwaltung

Geräteverwaltung	Bewertung
Heterogene Endgeräteklassen	1
Bestandsverwaltung	2

Afaria unterstützt ein breites Spektrum mobiler Endgeräte. Im Gegensatz zu XTND können auch Laptops eingesetzt werden. Die einzelnen Geräteklassen werden in einer Baumstruktur strikt voneinander getrennt.

Für die Inventarisierung der Clients wird der so genannte „Inventory Manager Channel" benutzt. Afaria fragt im Verlauf einer Synchronisation unbemerkt eine Vielzahl von Informationen vom Endgerät ab und speichert diese in der von Afaria genutzten Datenbank. Diese Daten können über diverse Abfragen, die mittels eines Assistenten zusammengestellt werden, eingesehen werden. Im Hintergrund wird hierbei eine SQL-Abfrage generiert. Somit kann sich auf unterschiedlichste Weise Überblick über den Bestand der Endgeräte verschafft werden. Über den gleichen Channel wird auch der Softwarebestand auf den Endgeräten inventarisiert. Afaria nutzt hierfür den DMI 2.0 – Standard (Desktop Management Interface[53]). Jede Hard- und Software, die sich an diesen Standard hält, wird in der Bestandsaufnahme berücksichtigt, andere hingegen nicht. Es gibt einen speziellen DMI-Client, der es ermöglicht, Client-Daten noch detaillierter zu erfassen. Dieser DMI-Clienet muss vom Hersteller des jeweiligen Endgerätes bezogen werden und wurde im Rahmen dieses Projektes nicht berücksichtigt.

Geräteverwaltung Gesamt	2

4.2.3.6 Softwareverwaltung (++)

Tabelle 4-20: Afaria - Softwareverwaltung

Softwareverwaltung	Bewertung
Betriebssystemkontrolle	1
Softwareabgleich	2

Zur Betriebssystemkontrolle und für den Softwareabgleich werden von Afaria zwei unterschiedliche „Channels" benutzt. Zur Konfiguration des Endgerätes wird der „Configuration Manager Channel" verwendet. Dieser ermöglicht es, die wichtigsten Einstellungen für den Endbenutzer vorzunehmen. Zu diesen Einstellungen gehören:

- Verbindungseinstellungen
- Geräteoptionen
- DNS / IP – Einstellungen
- Datenformate
- Netzwerkeinstellungen
- Besitzerdaten.

---

[53] Standardisiert von der DMTF (Distributed Management Task Force), http://www.dmtf.org [20.03.2003].

Der Zugriff auf Hardwarekomponenten ist jedoch recht eingeschränkt. Zusätzliche Module wie z. B. der GSM-Rucksack des iPAQ werden nicht unterstützt. Besondere Einstellungen für beispielsweise Modem oder die Infrarotschnittstelle sucht man ebenfalls vergebens. Dennoch werden die zentralen Aspekte der Konfiguration zufriedenstellend abgedeckt.

Der Bestand installierter Software kann, wie im Punkt „Geräteverwaltung" beschrieben, eingesehen werden. Für die Installation neuer Software steht der „Software Manager Channel" zur Verfügung. Er bietet eine Reihe von Optionen, die es möglich machen, die Installation neuer Software mehr oder weniger umfangreich zu konfigurieren. Dazu gehören Zielverzeichnisse, Setup-Kommentare u. ä. Eine Deinstallation ist leider nicht ohne weiteres möglich, obwohl dieses Feature auf der Afaria-Website propagiert wird[54].

Ein besonderes Feature ist die umfangreiche Scripting-Funktionalität innerhalb eines „Configuration Manager Channels". Hier können in Form von Abfragen und Bedingungen tief greifende Änderungen im System des Endgerätes durchgeführt werden. Diese Änderungen erfolgen durch Zugriff und Manipulation von Registry-Einträgen und erfordert somit tiefgehende Kenntnisse über das PocketPC Betriebssystem. Außerdem birgt dieses Verfahren das Risiko, das Endgerät oder einzelne Softwarekomponenten durch falsche Einträge unbrauchbar zu machen. Anhand von Registry-Einträgen können auch Softwareinstallationen angestoßen werden, die nur unter bestimmten Bedingungen ausgeführt werden.

Afaria kann Pakete des Microsoft System Management Servers (SMS) für die Geräteklasse der Notebooks importieren.[55] In absehbarer Zeit soll der SMS aber um die Möglichkeit zur Verwaltung von PocketPC-Systemen erweitert werden.

Softwareverwaltung Gesamt	2

4.2.3.7 Kommunikationskanäle (++)

Tabelle 4-21: Afaria - Kommunikationskanäle

Kommunikationskanäle	Bewertung
Zugangsmethoden	2

Für die erfolgreiche Verbindung mit dem Afaria-Server ist lediglich eine IP-Verbindung notwendig. Über die unter dem Thema Sicherheit erwähnte HTTP-Encapsulation werden alle benötigten Informationen und Dateien ausgetauscht. Zum Erreichen eines höheren Datendurchsatzes über den Breitband- oder LAN-Anschluss eines DesktopPCs ist der Benutzer auf „Active Sync" angewiesen. Ein „Desktop Connector", wie wir ihn von XTND her kennen, steht für Afaria nicht zur Verfügung.

Kommunikationskanäle Gesamt	2

[54] http://www.xcellenet.com/public/products/afaria/solving_challenges.asp [26.03.2003].
[55] Beziehungsweise für 32-Bit-Windows-Systeme.

4.2.3.8 Remote Analyse (+++)

Tabelle 4-22: Afaria – Remote Analyse

Remote Analyse	Bewertung
Logging	1
Fehlerprotokollierung	2
Fehlerbehebung	3

Afaria verfügt über einen insgesamt sehr mächtigen Logging-Mechanismus. Die Protokolldaten werden, wie auch die Geräte- und Softwaredaten, in der von Afaria benutzten Datenbank abgelegt. Der Zugriff auf diese Protokolle erfolgt auch für das Logging durch das Zusammenstellen potentiell sehr mächtiger Abfragen und lässt demzufolge kaum Wünsche offen. Clientseitig werden die Ereignisprotokolle jedoch nicht gespeichert.

Ähnlich verhält es sich mit der Fehlerprotokollierung. Allerdings vermisst man bei auftretenden Schwierigkeiten Tipps und Ratschläge zur Fehlerbehebung. Die Möglichkeiten zum Beheben auftretender Fehler beschränkt sich weitestgehend auf das Wiederherstellen einer funktionierenden Systemkonfiguration. Es stellt sich zwar die Frage, inwiefern hier weitergehende Funktionen wirklich praktikabel wären, ein Remote-Desktop oder etwas Vergleichbares wäre jedoch in jedem Fall wünschenswert.

Remote Analyse Gesamt	2

4.2.3.9 Usability (++)

Tabelle 4-23: Afaria - Usability

Usabilty	Bewertung
Sprache	
Verfügbar in deutscher Sprache	Nein
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	2
Daten können wie von der Aufgabe gefordert eingegeben werden	2
Informationen und Bedienelemente befinden sich am richtigen Platz	2
Alle benötigten Informationen sind auf dem Bildschirm zu finden	2
Ausgaben sind zweckmäßig und verständlich	2
Wiederholfunktion für wiederkehrende Arbeitsschritte sind verfügbar	2
Selbstbeschreibungsfähigkeit	
Bei Bedarf sind Kontexthilfe oder weitergehende Informationen abrufbar	2
Meldungen sind sofort verständlich	2
Rückmeldungen können einer Ursache eindeutig zugeordnet werden	2
Art und Zusammensetzung geforderter Eingaben sind leicht erkennbar	2

Auswirkungen von Aktionen sind hinreichend ersichtlich	1
Aktuelle Eingabeposition ist eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) ist eindeutig erkennbar	3
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen ist möglich	1
Der aktuelle Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann Abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte sind vorhersagbar	2
Die Bearbeitungszeit ist abschätzbar	2
Eine einheitliche Verwendung von Begriffen und Symbolen ist gewährleistet	2
Die Ausführung einer Operation führt zum erwarteten Ergebnis	2
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen ist unmöglich oder wird erschwert	2
Bei Fehlern werden zweckmäßige Hinweise zur Ursache und Behebung geliefert.	2
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	1
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	1
Nur wenige Detailkenntnisse zur Bedienung nötig	3
Hilfestellung bei Bedarf verfügbar	1
Benutzerhandbuch	
Qualität des Benutzerhandbuchs	3
Verfügbar in deutscher Sprache	Ja
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	Ja
Installations- / Administrationshandbuch	
Qualität des Installations- / Administrationshandbuch	3
Verfügbar in deutscher Sprache	Ja
Verfügbar in englische Sprache	Ja
Verfügbar in weiteren Sprachen	Ja
Support	

Qualität des Supports	2

Die hier aufgeführte Tabelle entspricht dem im Kapitel „Evaluationskonzept und Methodik" vorgestellten Konzept. Auf eine differenzierte Kommentierung der einzelnen Punkte wurde an dieser Stelle verzichtet.

Usability Gesamt	**2**

4.2.3.10 Besonderheiten / Ausblick (+)

Aus den obigen Kapiteln ist ersichtlich geworden, dass die „Channels" bei Afaria eine besondere Rolle einnehmen. Innerhalb des „Document Channels" ist es neben dem Abonnieren des gesamten Channels ebenfalls möglich auszuwählen, welcher Inhalt bzw. welche Dateien auf dem Client zur Verfügung stehen sollen. Dies geschieht mittels Übertragung der Dateinamen und anschließendem Auswählen der gewünschten Dateien. Dieses Verfahren ist unserer Meinung nach sehr gut gelungen und stellt einen guten Kompromiss zwischen Datenverfügbarkeit und Speicherplatzbedarf dar.

Außer im Abonnement können Channels auch im Push-Verfahren verteilt werden. In diesem Fall bekommt der Endnutzer die entsprechenden Inhalte auf jeden Fall zugestellt. Dies erwies sich insbesondere bei „Configuration Channels" und bestimmten „Document Channels" als sehr vorteilhaft.

Ein weiteres interessantes Feature ist die Möglichkeit, den Afaria Client im Hintergrund zu starten und sein GUI (Graphical User Interface) zu verbergen. Somit wird der Endbenutzer nicht mit zusätzlichen Eingabemasken o. ä. konfrontiert. Dieses Verfahren bietet sich jedoch nur bei Nutzung von ActiveSync an, ein automatischer Abgleich nach erfolgreichem Aufbau einer Internetverbindung ist nicht vorgesehen.

Neben der Administrationskonsole auf dem Server stellt Afaria zusätzlich ein Webinterface bereit, das wir aufgrund der uns zur Verfügung gestellten Evaluationslizenz nicht testen konnten.

Im Rahmen letzter Gespräche wurde uns mitgeteilt, dass in Kürze eine neue Version (5.0) veröffentlicht wird. Diese baue komplett auf dem .NET Framework auf und zeichne sich durch das Fehlen der Admin-Konsole aus. Die neue Version würde komplett über ein Web-Frontend bedient.

Der große Kundenstamm (siehe Referenzen auf der Homepage des Herstellers) und die Umstellung auf neue Technologien lassen vermuten, dass dieses Produkt auch in Zukunft weiterentwickelt wird und dementsprechend weiterhin Support zur Verfügung steht.

4.2.3.11 Gesamtbewertung

Tabelle 4-24: Afaria - Gesamtwertung

Gesamtwertung	Bewertung
Administration allgemein	3
Sicherheit	4
Administration	2
Usability	2
Kosten	3

XcelleNets Afaria ist das derzeit einzige uns bekannte Produkt, das den Anforderungen ansatzweise gerecht wird. Zu bedenken ist hierbei, dass sich unsere Bewertung ausschließlich auf den Umgang mit den PocketPCs bezieht. Die Fähigkeiten von Afaria in Bezug auf Palms, Laptops und andere wurde in unserer Betrachtung nicht berücksichtigt.

Neben der Basisfunktionalität rechtfertigen vor allem die ausgezeichneten Logging-Funktionen eine Empfehlung von Afaria. Die Übersicht über den Bestand der mobilen Endgeräte zu bewahren, gestaltet sich ohne entsprechende Software ungleich schwieriger. Auch verschaffen die umfangreichen Scripting-Funktionen Afaria einen großen Leistungsvorsprung gegenüber XTND.

Der relativ hohe Grad der Spezialisierung dieser Software erfordert allerdings ein gewisses Maß an Schulungs- bzw. Einarbeitungszeit. Sofern eine Infrastruktur und entsprechende Vorgehensweisen ausgearbeitet und eingerichtet wurden, sind die administrativen Arbeiten bequem zu leisten. Afaria bietet aufgrund seines höheren Leistungsumfangs weit mehr als nur eine gleichwertige Alternative zu der Administrationskomponente von XTND.

4.3 Synchronisation

Dieser Abschnitt enthält die Evaluationsberichte der in die nähere Auswahl einbezogenen Synchronisationssoftware. Dies ist zum einen die reine Microsoft Lösung mittels des Mobile Information Server (MIS) nebst Internet Security and Acceleration Server (ISA) und zum anderen die Benutzung des XTND Connect Produktes.

Der Evaluationsbaum sieht somit wie folgt aus:

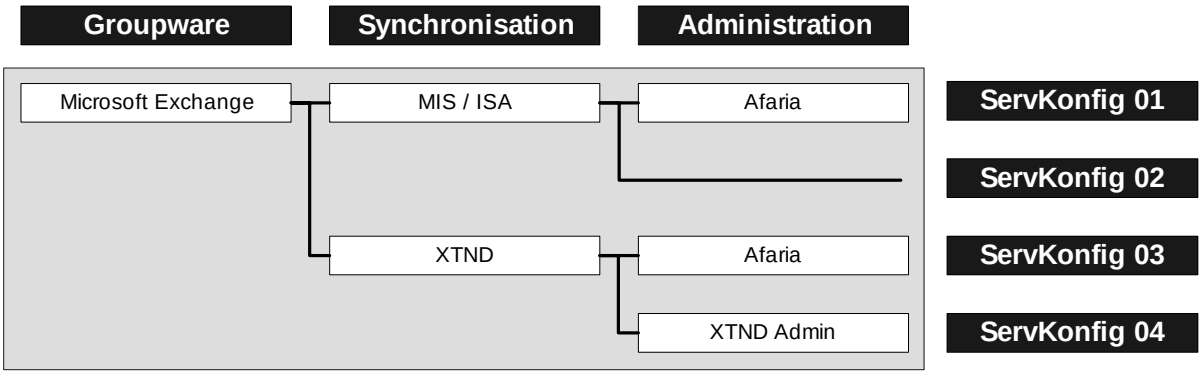

Abbildung 4-14: Evaluationsbaum auf Serverseite

Grundlage für den Aufbau der einzelnen Serverkonfigurationen stellt die Basiskonfiguration dar, wie sie im Kapitel 4.1.2 eingeführt wurde. Bevor wir zur Evaluation der einzelnen Komponenten kommen, werden zunächst die für die Bewertung herangezogenen Kategorien erläutert.

4.3.1 Kategorien

Für die Evaluation der Synchronisationssoftware wurde ebenso wie für die Administration- und die Endgerätesoftware ein Evaluationsbogen entwickelt.

Neben den bereits eingeführten Kategorien Administration, Sicherheit, Usability und Kosten werden zur Bewertung der Synchronisationskomponenten zusätzlich die Kategorien „Synchronisation der einzelnen Elemente" und „Besondere Merkmale" eingeführt. Im Folgenden wird dargestellt, welche Aspekte im Einzelnen unter den Kategorien subsummiert wurden.

4.3.1.1 Die Kategorie Administration (++)

Für einen reibungslosen Ablauf innerhalb des Netzwerks und den effizienten Ressourcen-Einsatz durch zentrales Management spielt die Administrierbarkeit der Synchronisationssoftware eine wichtige Rolle. Die Software sollte Werkzeuge zur Verfügung stellen, die IT-Manager und Administratoren benötigen um Umfang und Art der zu synchronisierenden Daten festlegen und um Sicherheitsrichtlinien umsetzen zu können.

Innerhalb der Kategorie Administration wird zunächst die Installation und Konfiguration der Synchronisationskomponente dargestellt. Hier werden auch Einstellungsmöglichkeiten wie Filterregeln, Kollisionsmanagement, Benutzer- und Rechteverwaltung sowie sonstige Konfigurationsmöglichkeiten untersucht und datenschutzrechtliche Aspekte kurz beleuchtet.

Installation und Konfiguration

Die Installation und Konfiguration der Software sollte sich einfach und transparent gestalten lassen und von einer gute Usability geprägt sein.

Benutzerverwaltung

Der Aspekt Rechteverwaltung behandelt die Abbildung von Gruppen und die Kompatibilität zu Microsoft Exchange bzw. zum Active-Directory-Service.

Logging und Reporting

Geeignete Logmechanismen sind bei der Administration unabdingbar, um beispielsweise Fehlerquellen zu identifizieren. Protokolle und Berichte sollen außerdem Transparenz in den durch die Software ausgeführten Transaktionen schaffen.

Filterregeln

Filterregeln sind wichtig, um die Größe der zu synchronisierenden E-Mails und/oder das Datenvolumen pro Synchronisationsvorgang einschränken zu können. Dies macht zum einen Sinn, da der Speicherplatz auf dem PDA begrenzt ist, zum anderen, da sonst der Synchronisationsprozess viel Zeit und damit beispielsweise bei einer GSM-Verbindung viel Geld kosten würde. Außerdem sollten auch Dateianhänge von E-Mails, die der PDA nicht interpretieren kann, bei der Synchronisation unberücksichtigt bleiben.

Kollisionsmanagement

Unter Kollisionen verstehen wir in diesem Zusammenhang beispielsweise Änderungen ein und desselben Kontaktes, Termines etc. sowohl am PDA als auch im Intranet vom Arbeitsplatzrechner aus ohne zwischenzeitliche Synchronisation. In diesem Zusammenhang wurde untersucht, wie die Synchronisationskomponente mit derartigen Kollisionen umgeht und ob Konfigurationen zum Kollisionsmanagement möglich sind.

Datensicherheit

In diesem Abschnitt soll auf datenschutzrechtliche Aspekte eingegangen werden. Es wird untersucht, ob, wo und welche personenbezogenen Daten bei Benutzung des Endgerätes zur Synchronisation anfallen. Wir wollen an dieser Stelle lediglich darauf aufmerksam machen, dass datenschutzrechtliche Aspekte beim Einsatz der Synchronisationssoftware berücksichtigt werden müssen, empfehlen aber keine konkrete Vorgehensweise, da dies den Rahmen dieses Projektes sprengen würde.

4.3.1.2 Die Kategorie Synchronisation der einzelnen Elemente (+++)

In der Kategorie „Synchronisation der einzelnen Elemente" wird zunächst der Ablauf des Synchronisationsvorgangs erläutert. Anschließend gehen wir auf die Verbindungsarten ein. Danach betrachten wir die zu synchronisierenden Groupware-Daten. Hierzu zählen E-Mails, Termine, Kontakte, Aufgaben, Notizen und Öffentliche Ordner. Schließlich untersuchen wir den Umgang mit möglichen Problemfällen wie Verbindungsabbruch und Speicherplatzmangel.

Da die ständige Verfügbarkeit jeweils aktueller Groupware-Daten der Hauptzweck für den Einsatz der mobilen Endgeräte ist, wird auf die Synchronisation auch bei der Gesamtbewertung viel Wert gelegt.

Ablauf der Synchronisation

In diesem Abschnitt soll als Basis für die folgenden Ausführungen ein Einblick in den Ablauf der Synchronisation und die hierfür notwendigen Schritte gegeben werden. An dieser Stelle findet noch keine Bewertung statt.

Verbindungswege und Profileinstellungen

Der Ablauf des Synchronisationsvorgangs kann je nach gewählter Verbindungsart unterschiedliche Bearbeitungsschritte auf Seiten des Clients mit sich bringen. Dabei sind grundsätzlich folgende Szenarien denkbar:

- Synchronisation am Arbeitsplatzrechner im Intranet
- Synchronisation außerhalb des Intranets über das Internet
    - Kabellos über GPRS (direkte Verbindung mit Internetprovider)
    - Kabelgestützt an einem windows-basierten PC über serielle bzw. USB Docking-Station
- Synchronisation über GSM (RAS-Einwahl).

Durch die Einrichtung eines DNS-Dummys[56], verläuft die Synchronisation am Arbeitsplatzrechner im Intranet für den Benutzer genauso wie eine Synchronisation außerhalb des Intranets über das Internet. In beiden Fällen erfolgt die Verbindung zum Synchronisationsserver kabelgestützt an einem Windows-basierten PC über eine serielle bzw. USB Docking-Station.

Das wohl häufigste Vorgehen zu Datenabgleich und –sicherung von mobilen Endgeräten basiert auf dem Companion[57]-Prinzip. Hierbei hat das mobile Gerät einen immer gleichen Partner-PC, mit dem Abgleich und Sicherung vollzogen werden. Auf diesem Partner-PC wird eigens zu diesem Zweck eine Software (ActiveSync, HotSync o. ä.) installiert, die dann bei Bedarf den Synchronisationsvorgang durchführt.

Die hier betrachteten PDAs aus der Geräteklasse der PocketPCs sind in der Standardinstallation darauf ausgelegt, die auf ihnen abgelegten PIM-Daten wie E-Mails, Kontakte, Termine und Notizen via Active Sync mit einer ActiveSync-Gegenstelle auszutauschen. Allerdings ist auch die Installation anderer Synchronisationssoftware sowohl auf dem Partner-PC als auch auf dem Endgerät möglich.

E-mails

Die Synchronisation von E-Mails ist eine der wichtigsten Funktionen für den sinnvollen Einsatz mobiler Endgeräte. Dateianhänge finden dabei besondere Beachtung, da der Transfer hinsichtlich seines Volumens und der zu übertragenen Dateitypen besondere Anforderungen an das System stellt.

Microsoft Outlook bietet umfangreiche Funktionen zur Verwaltung ein- und ausgehender E-Mails an. Insbesondere besteht die Möglichkeit, E-Mails durch die Einrichtung von Filterregeln innerhalb von Microsoft Outlook automatisch in Unterordner zu verschieben. Mobile Outlook hingegen verfügt in der eingesetzten Version nicht über die Möglichkeit, Unterordner anzulegen oder zu verwalten. Es gilt zu untersuchen, wie die Synchronisationssoftware mit Unterordnern des Posteingangsfaches umgeht.

Außerdem soll untersucht werden, ob Filterregeln für zu synchronisierende E-Mails angegeben werden können und wie ausgefilterte E-Mails behandelt werden.

---

[56] Siehe hierzu Kapitel 4.1.3.2 Standorte und Servernamen.
[57] Engl.: Der Gefährte, der Begleiter.

Termine

Eine weitere Funktion von Microsoft Outlook in Verbindung mit Exchange ist die Terminverwaltung. Hierbei gibt es zwei Teilbereiche, die unterschieden werden müssen. Zum einen die Verwaltung eigener Termine und zum anderen die Verwaltung von Terminen mit anderen Benutzern.

Für letzteres ist es notwendig, dass die an dem Termin beteiligten Personen auch ein Exchangekonto haben. Dann ist es möglich, andere Personen einzuladen, deren Verfügbarkeit im Voraus zu überprüfen und selbst von anderen eingeladen zu werden.

Die Synchronisationssoftware sollte idealerweise alle Funktionen der Terminverwaltung unterstützen.

Kontakte

Innerhalb von Microsoft Outlook und von Microsoft Mobile Outlook können Kontakte verwaltet werden. Microsoft Outlook unterscheidet dabei zwischen persönlichen und öffentlichen Kontakten. Der Unterschied zwischen diesen Kontakten liegt zum einen im Speicherort und zum anderen in deren Verwaltung.

Private Kontakte werden im Verzeichnis des jeweiligen Benutzers abgelegt und können vom Benutzer frei editiert werden. Öffentliche Kontakte sind von allen Nutzern in einem System einzusehen, sie können jedoch nur zentral und von dafür berechtigten Benutzern verwaltet werden.

Die Synchronisationssoftware sollte idealerweise sowohl private als auch öffentliche Kontakte abgleichen können.

Aufgaben

Outlook bietet die Möglichkeit, Aufgaben zu verwalten. Man kann dabei einen Betreff für die Aufgabe und eine textuelle Beschreibung vergeben sowie Daten für Fälligkeit, Beginn und Ende der Aufgabe und einen Erinnerungstermin angeben. Die Angabe einer Priorität und eines Bearbeitungsstatus ist ebenfalls möglich. Microsoft Outlook bietet außerdem die Möglichkeit, Aufgaben anderen Benutzern zuzuordnen.

Notizen

Notizen werden am PDA häufig benutzt, da sie leicht zu handhaben sind und im Vergleich zu Dokumenten im Word-Format wenig Speicherplatz benötigen. Auch diese sollten also synchronisiert werden.

Öffentliche Ordner

Öffentliche Ordner sind Verzeichnisse, die für die zentrale Ablage von Dokumenten und anderen Dateien verwendet und von Exchange verwaltet werden. Obwohl öffentliche Ordner zu den von Exchange verwalteten Groupware-Daten gehören, stellen sie bei der Synchronisation auf iPAQs einen Sonderfall dar.

Öffentliche Ordner enthalten i. d. R. eine Vielzahl von Dateien und Dateitypen, so dass eine vollständige Synchronisation aller Dateien — und damit der Zugriff auf diese Dateien vom iPAQ aus — weder möglich noch sinnvoll erscheint. Der iPAQ hat trotz Erweiterungsmöglichkeiten im Vergleich zu einem gewöhnlichen PC nur einen sehr begrenzten Speicherplatz und kann viele Dateitypen nicht interpretieren. Um trotzdem ein Arbeiten mit den in den öffentlichen Ordnern befindlichen Daten ermöglichen zu können, wäre es an dieser Stelle wünschenswert, eine Liste mit Dateinamen angezeigt zu bekommen, von denen man auf Wunsch einzelne Dateien zum Herunterladen auf den iPAQ markieren kann.

Zusammenfassender Überblick

Alle erläuterten Elemente sollten idealerweise synchronisierbar sein. Insbesondere soll evaluiert werden, in welchem Umfang die gewählte Synchronisationskomponente den Abgleich der einzelnen Elemente unterstützt.

Für jedes der zu synchronisierenden Elemente wurden die beiden Einwahlarten Zugang über RAS und Zugang vom Internet aus getestet. Außerdem wurde die Synchronisation zum einen ausgeführt, nachdem Änderungen am PDA vorgenommen wurden, zum anderen nachdem Änderungen im Intranet vom Arbeitsplatzrechner aus vorgenommen wurden.

Die folgende Grafik veranschaulicht den Testumfang nochmals:

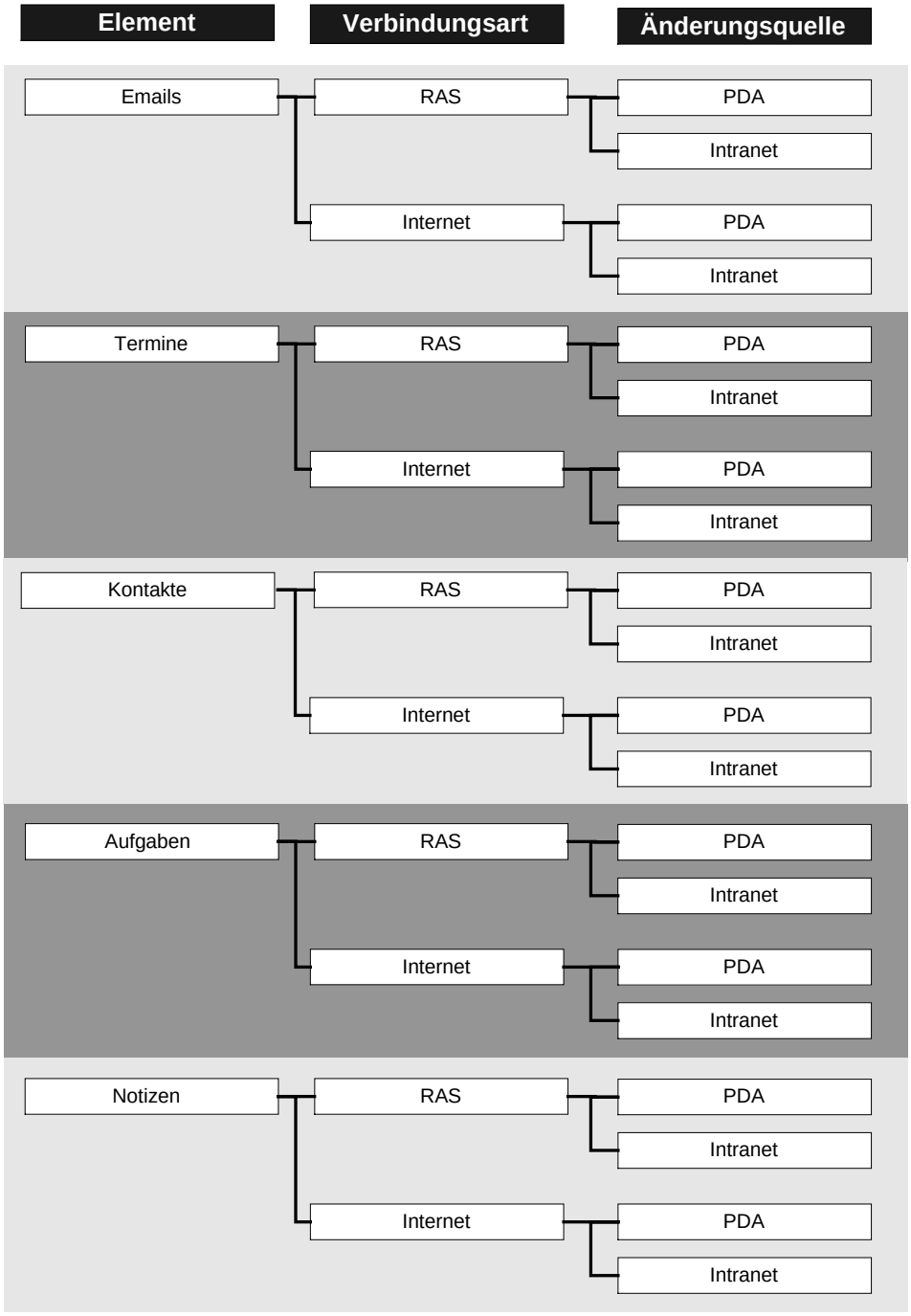

Abbildung 4-15: Synchronisationsszenarien

Umgang mit möglichen Problemfällen

Wie bei jedem System kann es auch bei diesem zu Problemen kommen. Diesen Problemen müssen nicht immer schwerwiegende technische Defekte oder gravierende Bedienungsfehler zu Grunde liegen. Das Hauptaugenmerk soll in diesem Abschnitt auf den „klassischen" bzw. wahrscheinlichen Problemen liegen, da man davon ausgehen kann, dass diese besonders in der Einarbeitungsphase, aber auch in einem späteren Arbeitsbetrieb, häufig auftreten können. Diese Problemfälle müssen bei einer eventuellen Einführung des Systems besondere Beachtung in den hausinternen Schulungen für die Nutzer finden.

Speicherplatzmangel

Durch die technisch bedingte Beschränkung des Speicherplatzes ist es nach einiger Zeit möglich, dass der zur Verfügung stehende Speicher des Endgerätes während eines Synchronisationsvorgangs überschritten wird. Diese Gefahr besteht vor allem, wenn häufig große Dateianhänge wie z. B. Bilder oder Tabellenkalkulationen empfangen und gespeichert werden. Die Auswirkungen eines solchen Ereignisses sollen hier untersucht werden.

Verbindungsabbruch

Ein anderes Problem, das sich nie ganz vermeiden lässt, ist die Unterbrechung der Verbindung des Endgerätes zum Server. Gerade bei Funkverbindungen (WLAN, GSM/GPRS) kann es immer wieder zu einem Verbindungabbruch kommen. Diese Möglichkeit besteht insbesondere dann, wenn sich der Nutzer während des Synchronisationsvorganges bewegt. Dies ist z. B. bei Zugreisen der Fall. Hier soll untersucht werden, wie die Software mit einem solchen Verbindungsabbruch umgeht.

4.3.1.3 Die Kategorie Sicherheit (+++)

Die Möglichkeiten eines Fern-Datenzugriffs über unterschiedliche mobile Endgeräte macht das Problem der Datensicherheit heute außerordentlich komplex. Die Synchronisationskomponente sollte maximale Sicherheit gewährleisten und höchstmöglichen Schutz für alle Unternehmensdaten über den gesamten Verbindungsweg hinweg bieten. Hierzu gehören insbesondere Aspekte wie Verschlüsselungsmechanismen und Art der Authentifizierung am Client. Diese Aspekte werden in der Kategorie Sicherheit untersucht.

Auf der Kategorie Sicherheit liegt auch eine starke Gewichtung bei der Gesamtbewertung.

4.3.1.4 Die Kategorie Usability (++)

Außerdem nahm die Untersuchung der Usability einen hohen Stellenwert ein. Unter Usability von Software versteht man im Allgemeinen, wie gut bzw. schlecht sich eine Anwendung bedienen lässt. Für die Bewertung wird das in Kapitel 4.1.5.4 beschriebene Verfahren angewendet.

Ein weiterer Punkt bei der Bewertung ist die Frage, inwieweit sich die neue Komponente von bekannten Standardanwendungen unterscheidet und somit neue Verwirrungen und Probleme auf Seiten der Benutzer hervorruft. Hingegen erweist sich eine starke Anlehnung an allgemein bekannte Softwareprodukte und deren Bedienkonzepte als sehr positiv.

4.3.1.5 Die Kategorie Kosten (+)

In dieser Kategorie werden die Kosten für die Software soweit wie möglich aufgeführt. Bei der zu untersuchenden Software handelt es sich um große Synchronisationsserver. Neben den reinen Anschaffungskosten müssen noch Kosten für die Wartung und den Support berücksichtigt werden. Daneben fallen Kosten für die Administration der Synchronisationssoftware und für Schulungen der Mitarbeiter an. Dennoch spielen die Kosten bei der Gesamtbewertung eine deutlich geringere Rolle als beispielsweise die Sicherheit.

4.3.1.6 Die Kategorie Besondere Merkmale (+)

Hier werden produktspezifische Merkmale beleuchtet, die innerhalb der anderen Kategorien zwar nicht betrachtet wurden, aber dennoch für eine Bewertung relevant sind. Hierzu gehören beispielsweise externe Referenzen.

4.3.2 Synchronisation mittels MIS und ISA (ServerKonfig 01 und 02)

Die Evaluation der MIS/ISA-Variante wurde vorzeitig abgebrochen. Es wurde festgelegt, den Schwerpunkt des Testbetriebes von einer MIS/ISA Lösung auf eine Lösung mittels XTND zu verlagern, da sich die MIS/ISA Variante als komplex und fehleranfällig erwiesen hat.

MIS/ISA werden an dieser Stelle mit den gesammelten Erfahrungen beschrieben. Dazu werden wir zuerst die Referenzkonzepte vorstellen und anschließend auf die Probleme eingehen, auf die wir beim Versuch einer Lösung mittels MIS/ISA gestoßen sind. Der nächste Abschnitt enthält eine Abschätzung der Fähigkeiten, die zum einen auf den gesammelten Erfahrungen, zum anderen auf Featurelisten des Herstellers und auf Gesprächsergebnissen mit Microsoft-Repräsentanten auf der diesjährigen CeBIT basieren. Schließlich folgt eine Gesamtabschätzung einer Lösung mittels MIS/ISA.

4.3.2.1 Einleitung

Eine Synchronisation von Exchangedaten über ActiveSync auf mobile Endgeräte wie den im Projekt untersuchten iPAQ Handheld kann über den von Microsoft beworbenen „Mobile Information Server“[58] vorgenommen werden. Aufgrund der besonderen Infrastruktur und der hohen Sicherheitsanforderungen wurde bereits in Kapitel 2 erarbeitet, welches Konzept die höchsten Sicherheitsmerkmale mit sich bringt.

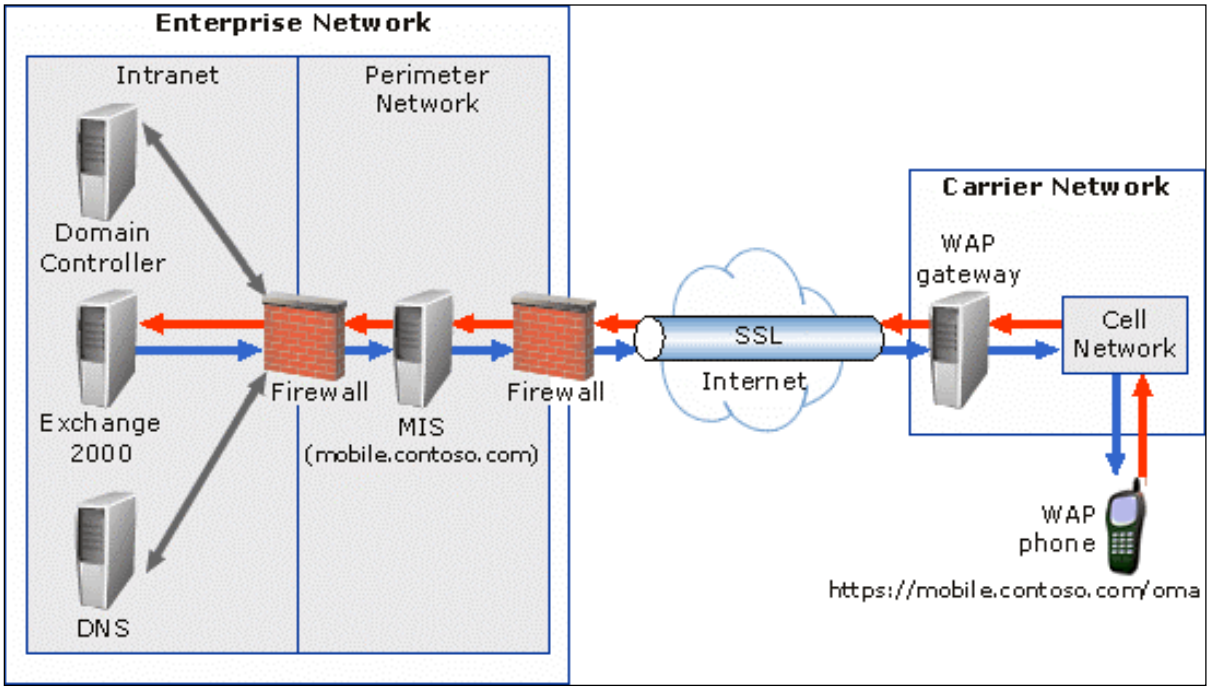

Abbildung 4-16: Standard MIS Deployment

Microsoft stellt unter anderem das Standarddeploymentszenario vor. In diesem Szenario wird der MIS in eine Infrastruktur eingefügt, die über eine DMZ verfügt. Der MIS wird dabei direkt in der DMZ platziert und stellt die Verbindung von der Außenwelt, also dem

[58] Siehe auch: http://www.microsoft.com/miserver/default.asp [12.02.2003].

mobilen iPAQ zum Exchangeserver im Intranet dar. Diese Variante hat jedoch, wie in Kapitel 2 dargelegt, gravierende Sicherheitsmängel.

Zum Aufbau einer unserem Konzept entsprechenden Lösung mit einem in der DMZ platzierten Schicht-7-Proxy existiert ebenfalls eine Referenzempfehlung von Microsoft. Diese sieht die Benutzung des Internet Security & Acceleration Server[59] (ISA Server) als Proxykomponente vor. Dadurch kann der MIS in das Intranet verlagert werden und die Kommunikation zum ISA erfolgt über eine minimale LDAP Verbindung, die bedeutend sicherer ist. Die Kommunikation zwischen MIS und ISA erfolgt über SSL-Verbindungen und setzt daher SSL-Zertifikate für den MIS und ISA voraus. Anders als bei obigem Standarddeploymentszenario werden hierbei nur noch 3 offene Ports in der inneren Firewall benötigt, zudem reichen die Domain und das Active Directory des Intranets tatsächlich nur bis zu dessen logischer Grenze und werden durch die Firewall vollständig geschützt.

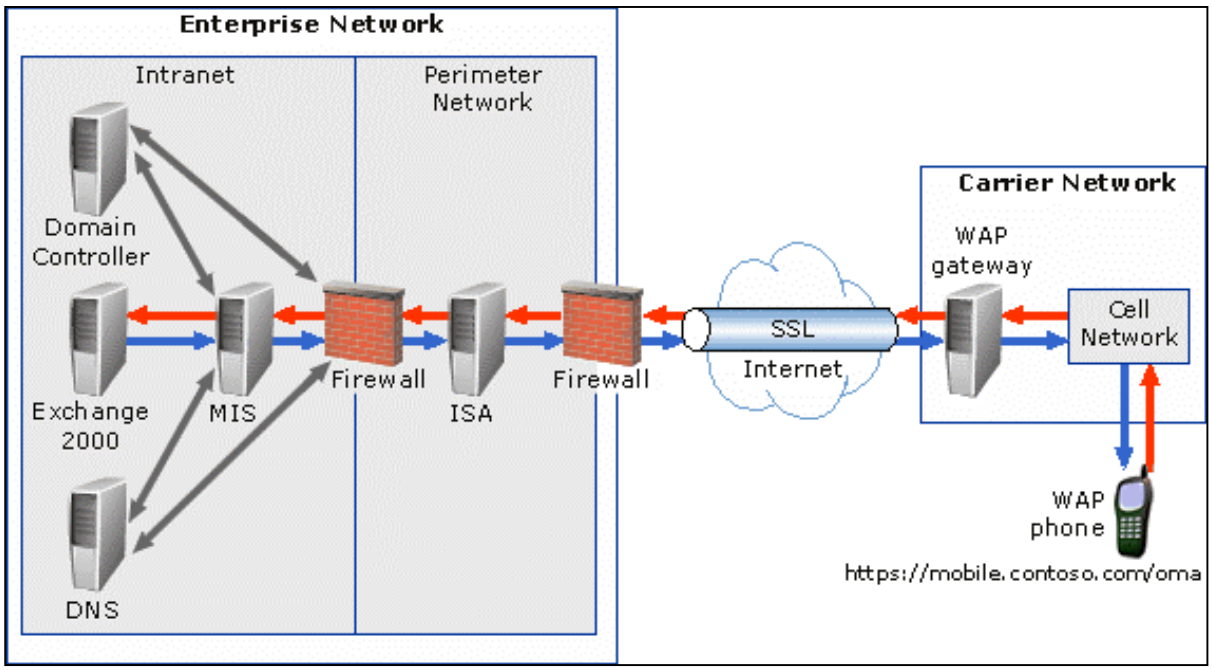

Abbildung 4-17: MIS Deployment mit dem ISA als Gateway

Die Abbildung dieser Infrastruktur auf das Labor wird im Kapitel 4.1.3.3.2 im Netzwerkdiagramm vorgestellt.

[59] Siehe auch: http://www.microsoft.com/isaserver/ [12.03.2003]

4.3.2.2 Aufgetretene Probleme

In diesem Abschnitt stellen wir zunächst ein Konzept zur stufenweisen Realisierung der Zielkonfiguration ServerKonfig 01 (siehe Kapitel 4.1.3.1.1) vor und gehen anschließend auf die aufgetretenen Probleme ein. Die folgende Abbildung zeigt auch den jeweiligen Status zum Zeitpunkt des Abbruchs der Evaluation.

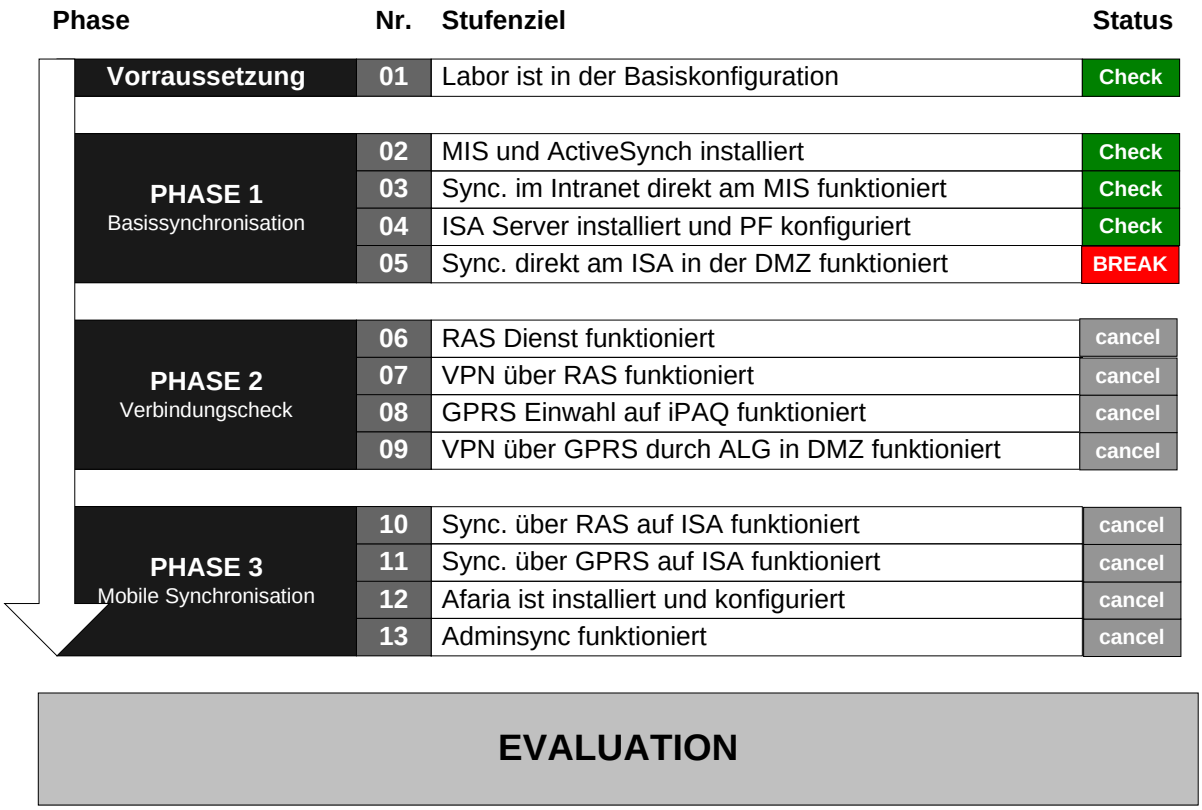

Abbildung 4-18: Stufenkonzept für ServerKonfig 01/02

Bei Installation und Integration des MIS und des ISA Servers haben wir uns weitestgehend an die offiziellen Dokumente von Microsoft gehalten um eine nachvollziehbare und jederzeit transparente Installation der einzelnen Komponenten zu gewährleisten.

Zentrale Hilfestellungen von Microsoft:

1. „ISA Server als Gateway für MIS“ [60] (ISA 2002)
2. „Installation von Microsoft Server Active Sync“ [61].

---

[60] Siehe http://www.microsoft.com/miserver/techinfo/administration/isagateway.asp [10.04.2003].

[61] Dieses Dokument liegt als PDF-Datei (`corpinstall.pdf`) vor und befindet sich auf der CD der Mobile Information Server im Verzeichnis `\<Sprache>\docs`. Alternativ dazu gibt es auch eine HTML-Hilfe-Datei zum Download http://www.microsoft.com/exchange/techinfo/deployment/2000/installactivesync.asp [10.04.2003].

Auf eine detaillierte Installations- und Konfigurationsbeschreibung wird im Rahmen dieses Dokumentes verzichtet. An dieser Stelle sollen lediglich ein Überblick gegeben und die aufgetretenen Probleme belichtet werden.

Das Deployment des Mobile Information Servers lief ohne große Probleme ab. Nachdem wir die notwendigen Konfigurationen am Active-Directory-Service, am Exchange Server etc. vorgenommen hatten, war eine Synchronisation im Intranet durch Kontaktieren des MIS möglich.

Hingegen bereitete die Zusammenarbeit mit dem Internet Security Accelleration Server als Gateway zum MIS enorme Probleme. Der ISA Server ist ein mächtiges Tool, das vor allem umfangreiche Firewall- und Cachefunktionen bietet. Daneben kommt der ISA mit einer eigenen VPN-Lösung und reißt überdies auch noch Routing- und RAS-Funktionen an sich. Wir hatten den ISA jedoch lediglich als Proxykomponente für den MIS vorgesehen, da für Firewall und VPN bereits andere Lösungen existieren. Um den ISA Server als Proxykomponente zu verwenden, müssen der ISA als Firewall konfiguriert und Art und Umfang der Kommunikation zwischen dem MIS und dem ISA und zwischen dem ISA und dem Client umständlich konfiguriert werden. Dazu werden innerhalb des ISA Servers Protokolle und Regeln definiert.

Außerdem ist die Einrichtung von SSL-Zertifikaten sowohl auf dem MIS als auch auf dem ISA notwendig. Zum einen da andernfalls Benutzerdaten zwischen MIS und ISA unverschlüsselt übertragen würden, zum anderen für eine sichere Verbindung zwischen ISA und Client. Hierfür können lokale private Zertifizierungsstellen verwendet werden, wobei es wichtig ist, dass der ISA Server der Zertifizierungsstelle des MIS vertraut. Der ISA muss derart konfiguriert werden, dass er eingehende SSL-Anfragen überbrückt und über eine weitere SSL-Verbindung an den MIS weiterleitet und vice versa.

Bei der Einrichtung der SSL-Verbindung sind wir jedoch auf enorme Probleme gestoßen. Wir konnten vom Endgerät aus zwar eine Verbindung zum ISA Server aufbauen, und dieser leitete auch Datenpakete an den MIS, letztendlich aber scheiterte die Kommunikation zwischen dem MIS und dem ISA Server.

Im Rahmen unserer Recherche zu diesem Problem trafen wir auf eine Vielzahl von Supportanweisungen, Foren sowie Tipps und Tricks zum ISA-Server und speziell auch zu dem Zertifizierungsproblem[62]. Scheinbar ist hier massiver Verbesserungsbedarf vorhanden. Letztendlich waren wir aber, trotz zahlreicher Lösungsversuche, nicht in der Lage, eine erfolgreiche Synchronisation mit dem ISA Server als Proxy durchzuführen.

Der ISA-Server hat sich uns als unüberschaubare Mammutlösung offenbart, die innerhalb der gegebenen Zeit nicht in einen nutzbaren Zustand versetzt werden konnte. Schließlich wurde festgelegt, den Schwerpunkt auf das XTND-Produkt zu verlagern. Im Folgenden werden wir dennoch eine Abschätzung zur MIS/ISA Bewertung der einzelnen Kategorien liefern.

4.3.2.3 Abschätzung der Administrationskosten

Die Administrationskosten für diese Lösung schätzen wir als relativ hoch ein. Da die Installation und Konfiguration außerordentlich komplex ist, gehen wir davon aus, dass diese entweder durch Microsoft-Support-Partner durchgeführt werden muss oder dass intensive Schulungsmaßnahmen für die Administratoren notwendig werden, um den ISA-Server in seiner Komplexität überschauen und sicher konfigurieren zu können.

---

[62] Siehe dazu z. B. in den Foren in http://forums.isaserver.org/ [26.03.2003].

4.3.2.4 Abschätzung des Funktionsumfangs

Der Umfang, in dem der MIS die Synchronisation der einzelnen Elemente unterstützt, wurde nicht im Detail evaluiert. Deswegen beschränken wir uns hier auf die Darstellung der bekannt gewordenen Schwächen einer Synchronisation mittels MIS, die uns Microsoft-Repräsentanten auf der CeBIT 2003 nochmals bestätigten.

Schwächen finden sich in der Verwaltung von E-Mails, Aufgaben, Notizen und öffentlichen Ordnern. Der Mobile Information Server bietet keine Möglichkeit zum Abgleich von Notizen. Auch die Synchronisation öffentlicher Ordner ist nicht vorgesehen. Da der Zugriff auf fremde Kalender nicht möglich ist, sind auch Terminanberaumungen nicht möglich.

Desweiteren kommen Probleme hinzu, die der beschränkte Funktionsumfang von Mobile Outlook verursacht. Innerhalb von Mobile Outlook ist es in der derzeitigen Version nicht möglich, Unterordner im Posteingangsfach anzulegen. Unterordner, die in der vollwertigen Version von Outlook erstellt wurden, werden also auf dem IPAQ nicht mitsynchronisiert.

Auch in Bezug auf die Verwaltung von Aufgaben bietet Mobile Outlook lediglich einen begrenzten Funktionalitätsumfang. So ist eine Zuweisung von Aufgaben an andere Nutzer nicht möglich. Innerhalb des vollwertigen Outlook an andere zugewiesene Aufgaben werden in Mobile Outlook genauso wie eigene Aufgaben dargestellt.

Zukünftig wird der Mobile Information Server in den Exchange Server 2003 integriert werden, bietet allerdings auch dann keine Lösung für diese Probleme.

4.3.2.5 Abschätzung der Sicherheit

Die Kombination des Mobile Information Servers mit dem ISA-Server als Gateway bietet umfangreiche Sicherheitsmechanismen. Die folgende Tabelle zeigt lediglich Sicherheitsaspekte, die evaluiert wurden.

Tabelle 4-25: MIS und ISA - Sicherheit

Kategorie Sicherheit	Bewertung
Kennwortverwaltung	
Kennwort zur Synchronisation verlangt (ja/nein)	Ja
Kennwort durch Administrator einsehbar (ja/nein)	Nein
Power-On-Passwort vorhanden (ja/nein)	Nein
Verschlüsselung des Netzwerkverkehrs	
RSA (ja/nein)	Nein
SSL (ja/nein)	Ja
VPN (ja/nein)	Ja
Sonstige Verschlüsselungsmechanismen (ja/nein)	Nein

Der Internet Security & Acceleration Server (ISA Server) wird als Proxykomponente für die Kommunikation zwischen Außenwelt und MIS in der DMZ eingesetzt. Um die außerordentlich sicherheitskritischen Daten auf dem MIS zu schützen, sollte dieser in das Intranet verlagert werden und die Kommunikation zum ISA über eine minimale LDAP Verbindung erfolgen, die bedeutend sicherer ist. Zudem trennt der ISA die Anfragen logisch auf Anwendungsebene (OSI Schicht 7) und verhindert so jedweden direkten Kontakt von

außen zu Elementen des Intranets. Die Kommunikation erfolgt über SSL-Verbindungen und benötigt daher SSL-Zertifikate für den MIS und ISA. Es werden drei offene Ports in der inneren Firewall benötigt, zudem reichen die Domain und das Active Directory tatsächlich nur bis zur logischen Grenze des Intranets und werden durch die Firewall vollständig geschützt.

Die Integration des MIS in den Exchange Server 2003 wird keinen Einfluss auf die hier erläuterten Sicherheitsmechanismen haben, da der MIS weiterhin im Intranet positioniert sein wird und die Kommunikation nach wie vor über den ISA erfolgt.

4.3.2.6 Gesamtabschätzung zu MIS-ISA

Eine auf einer systematischen und vollständigen Evaluation basierende Gesamtbewertung dieser Synchronisationslösung ist uns zwar nicht möglich, dennoch können wir an dieser Stelle einige wichtige Ergebnisse liefern.

Die Installation und Konfiguration des Systems stellt sich als außerordentlich komplex und fehleranfällig dar. Wie der Name bereits sagt, ist der Internet Security und Acceleration Server nicht als Proxykomponente für den Mobile Information Server entwickelt worden, sondern vereint primär Firewall- und Cache-Funktionalitäten, die umständlich für die Zusammenarbeit mit MIS konfiguriert werden müssen. Insbesondere ist die Einrichtung der notwendigen SSL-Zertifikate und der SSL-Verbindung zwischen dem MIS und dem ISA Server ein heikles Thema, was die zahlreichen Quellen und Postings zu diesem Problem zeigen. Hat man dies alles erreicht, kann man von einer relativ sicheren Datenübertragung zwischen mobilem Endgerät und MIS ausgehen.

Allerdings müssen auch bei dieser Synchronisationslösung einige Abstriche gemacht werden, was die Verwaltung von E-Mails, Terminen, Aufgaben, Notizen und öffentlichen Ordnern betrifft. Diese sind teilweise auf den unzureichenden Funktionsumfang des MIS und teilweise auf die Begrenztheit des Mobile Outlook zurückzuführen.

Bei den E-Mails werden die Unterordner des Posteingangsfaches nicht mitsynchronisiert. Die Synchronisation von Notizen, die aller Voraussicht nach am PDA relativ häufig benutzt werden, ist überhaupt nicht möglich. Ein Abgleich von öffentlichen Ordnern ist nicht vorgesehen. Der Zugriff auf fremde Kalender und eventuelle Terminanberaumungen sind nicht möglich. Aufgaben können nicht anderen Benutzern zugewiesen werden und innerhalb des Intranets am Arbeitsplatzrechner anhand von Outlook an andere Personen zugewiesene Aufgaben werden auf dem iPAQ genauso wie eigene Aufgaben dargestellt und behandelt.

Zukünftig wird der Mobile Information Server integriert in Exchange Server 2003, bietet allerdings auch dann nicht mehr Funktionalität als die jetzige Version.

4.3.3 **Synchronisation mittels XTND** (ServerKonfig 03 und 04)

Dieser Abschnitt enthält die Evaluationsbeschreibung der Synchronisationskomponente XTND Connect Server der Firma Extended Systems. Die Evaluation wurde vollständig anhand des entwickelten Evaluationsbogens durchgeführt.

In der Einleitung geben wir eine Beschreibung der Topologie und der Funktionsweise des XTND Connect Servers. Die darauffolgenden Abschnitte enthalten eine Bewertung gemäß der definierten Kategorien.

4.3.3.1 Einleitung

Mit dem XTND Connect Server lassen sich E-Mails und PIM-Daten zwischen PDAs und den Applikationen Lotus Notes/Domino oder Microsoft Exchange synchronisieren. XTND Connect Server bietet auch Möglichkeiten für einen Datenbankabgleich, auf diese Funktionen werden wir aber nicht näher eingehen.

Die folgende Grafik gibt einen Überblick über die Topologie und den Funktionsumfang.

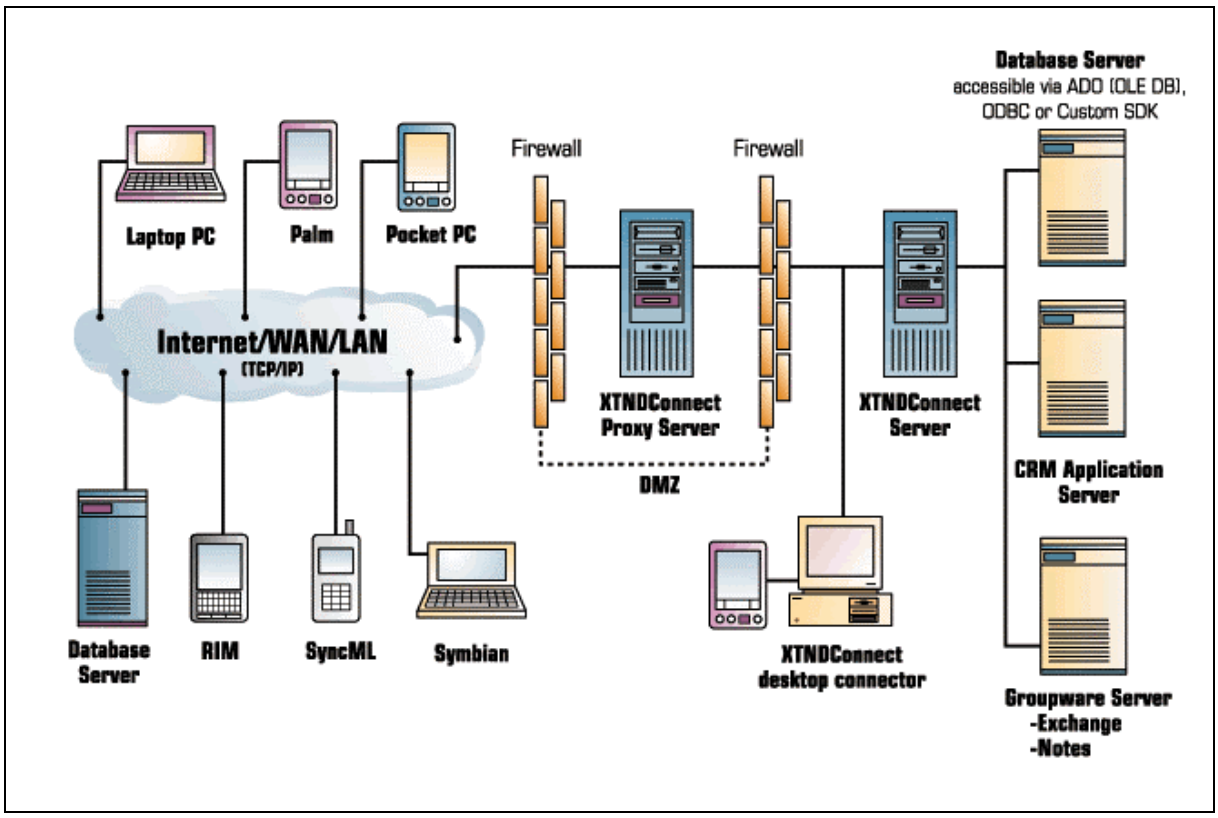

Abbildung 4-19: XTNDConnect Server Deployment

Neben den hier zu untersuchenden iPAQs werden auch eine Vielzahl weiterer Endgeräte unterstützt. Das Produkt ist auch mit einer optional installierbaren Proxy-Komponente ausgestattet, so dass es den in Kapitel 2 definierten Topologieanforderungen entspricht.

Die Abbildung dieser Infrastruktur im Labor wird in Kapitel 4.1.3.3.3 vorgestellt.

4.3.3.2 Kategorie Administration (++)

In diesem Abschnitt wird die Administrierbarkeit der Synchronisationssoftware evaluiert. Die folgende Tabelle gibt einen Überblick über die wichtigsten Aspekte.

Tabelle 4-26: XTND - Administration

Kategorie Administration	Bewertung
Installation und Konfiguration	
Mitgelieferter Guide	2
Installationswizards	2
Installierbarkeit	2
Konfigurierbarkeit	2
Benutzerverwaltung	
Abbildung von Gruppen möglich (ja/nein)	Ja
Active-Directory-kompatibel (ja/nein)	ja
Benotung der Benutzerverwaltung	2
Logging und Reporting	
Logging und Reporting vorhanden (ja/nein)	Ja
Benotung der Log-Funktionen	2
Filterregeln	
Transfer-Volumenbegrenzung pro Synchronisationsvorgang	5
Transfer-Volumenbegrenzung pro E-Mail	2
Dateitypenfilterung	4
Kollisionsmanagement	
Bewertung des Kollisionsmanagements	3
Datensicherheit im Datenschutzrechtlichen Sinne	
Verschlüsselte Ablage der Backups von PDA-Dateien (ja/nein)	Nein
Verschlüsselte Logmeldungen (ja/nein)	Nein
Einschränkungen für die Einsehbarkeit personenbezogener Daten	4

4.3.3.2.1 Installation und Konfiguration

Zur Installation und Konfiguration hielten wir uns an den von XTND bereitgestellten Guide[63]. Das Produkt stellt einen leicht bedienbaren Installationsassistenten zur Verfügung.

Die folgenden XTND Komponenten müssen installiert werden:

- XTNDConnect Server
- XTNDConnect Proxy Server

[63] „Getting Started Guide" (XTNDGuide 2002).

- XTNDClient
- XTNDConnect desktop connector.

XTNDConnect Server

Bevor mit der eigentlichen Installation der XTND-Komponenten begonnen wird, muss sichergestellt werden, dass auf demselben Rechner, auf dem der XTND Connect Server installiert wird, ein Outlook2000 vorhanden ist, da der Server auf das von Outlook bereitgestellte CDO-Modul zugreift.

Für unser Deployment-Szenario installieren wir den XTNDConnect Server und die zugehörigen Groupware-Adapter innerhalb des Intranets. Die Benutzergruppen können entweder bei der Installation oder aber im Nachhinein angelegt werden.

XTNDConnect Proxy Server

Zur Installation der DMZ-Proxy kann ebenfalls der Installationswizard verwendet werden. Die wenigen Angaben, wie zu verwendende Portnummer und IP-Adresse des Rechners, auf dem der XTNDConnect Server läuft, sind schnell gesetzt, so dass sich das Setup des DMZ-Proxies sehr einfach gestaltet.

XTNDClient

Der XTNDClient-Wizard kann von einem beliebigen PC aus betrieben werden. Der Client Deployment Wizard dient zur Erstellung der zur Synchronisierung notwendigen Endgerätesoftware. Der Wizard erstellt dabei eine Setup-Datei, die zur Installation auf dem Client von einem Rechner aus gestartet wird, der mit dem Handheld über einen COM-Port oder USB verbunden ist. Durch das Starten der erstellten Setup-Datei wird die benötigte Clientsoftware auf dem mobilen Endgerät installiert.

Das Setup kann benutzerspezifisch vorkonfiguriert werden, so dass der Benutzer lediglich Benutzerkennung und Passwort eingeben muss und auf eine Konfiguration der zu kontaktierenden Server, der Synchronisationsoptionen etc. verzichten kann. Die notwendige Vorkonfiguration der Verbindungs- und Profileinstellungen bringt zwar mehr Administrationsaufwand, aber auch ein deutliches Plus an Usability auf Seiten des Benutzers, der nicht mehr selbst eingreifen muss und auch nicht versehentlich Einstellungen ändern kann.

XTNDConnect desktop connector

Der XTNDConnect desktop connector dient der Kommunikation zwischen dem Windows-PC und dem über eine serielle bzw. USB-Dockingstation mit dem PC verbundenen iPAQ. Die Komponente ist sehr klein und erfordert weder benutzerspezifische Angaben noch eine Installation und kann somit auch direkt von einem Dateiserver oder gar einer Diskette aus gestartet werden.

4.3.3.2.2 Benutzerverwaltung

Der XTNDConnect Server ist Active-Directory-kompatibel, wodurch beliebige Active-Directory-Gruppen und auch einzelne Benutzer für die Synchronisation übernommen und konfiguriert werden können. Für jede der angelegten Benutzergruppen können getrennte Synchronisationsoptionen angegeben werden.

Eine nützliche Option bildet die Möglichkeit, bestimmte Ordner für die Synchronisation vorzusehen. Je nach Konfiguration werden dann diese Ordner entweder benutzer- oder gruppenspezifisch auf die Endgeräte übertragen.

4.3.3.2.3 Logging und Reporting

Der XTNDConnect Server verfügt über ausreichende Logging-Mechanismen. Logs und Berichte sind zum einen unter Kategorien wie System, Sicherheit und Anwendungen einsehbar und zum anderen nochmals unter den Logstati Fehler, Erfolg, Warnung, Information, Timeout etc. aufgelistet, so dass sich eine gute Übersichtlichkeit ergibt.

4.3.3.2.4 Filterregeln

Der XTNDConnect Server bietet Möglichkeiten, den Umfang der zu synchronisierenden Elemente anzugeben. Dies ist bei E-Mails und Terminen zum einen durch die Angabe von Zeiträumen möglich, zum anderen existiert für E-Mails die Option, die Größe von E-Mails und Dateianhängen zu begrenzen. Je nach Konfiguration werden dann nur die Betreffzeilen der E-Mails synchronisiert, wobei der Benutzer immer die Möglichkeit hat, sich auf Wunsch die gesamte E-Mail im Nachhinein auf sein Endgerät herunterzuladen. Negativ ist, dass sich die Begrenzung des Transfer-Volumens nur auf einzelne E-Mails, aber nicht auf den kompletten Synchronisationsvorgang festlegen lässt.

Bei Dateianhängen von E-Mails besteht zudem die Möglichkeit, bestimmte Dateitypen zu filtern. Die Defaulteinstellung von XTNDConnect Server filtert alle Dateianhänge aus, die nicht mit der standardgemäßen Softwareausstattung von Windows Pocket PC zu öffnen sind. Diese Filterregeln lassen sich auf Seiten des XTNDConnect Servers ändern, dies gestaltet sich allerdings nicht immer intuitiv.

4.3.3.2.5 Kollisionsmanagement

Bei der Konfiguration der Synchronisationsoptionen kann man festlegen, in welche Richtung die Daten synchronisiert werden, also ob geänderte Daten vom PDA zum Intranet oder ob geänderte Daten vom Server zum Endgerät übertragen werden. Insbesondere ist die Angabe von Prioritäten möglich, wie z. B. „Änderungen am Server haben höhere Priorität als Änderungen am Endgerät." Empfehlenswert ist hier die Beibehaltung der Defaulteinstellung, die die Synchronisationsrichtung nach Änderungsdatum festlegt.

4.3.3.2.6 Datensicherheit im datenschutzrechtlichen Sinne

Mit XTNDConnect Server lassen sich Daten nicht nur austauschen, sondern auch sichern. Der Administrator kann konfigurieren, dass bei jeder Synchronisation auch ein Backup des PDA-Speichers auf dem Server erfolgt. Auf diese Weise gehen die Daten bei einem Gerätedefekt nicht verloren. Allerdings erfolgt die Ablage ohne zusätzliche Maßnahmen gänzlich unverschlüsselt, was datenschutzrechtlich sehr bedenklich ist. Eine weitere Quelle personenbezogener Daten stellen die detaillierten Logmeldungen des XTNDConnect Servers dar. Anhand dieser lässt sich leicht nachverfolgen, wann welcher Benutzer welche Daten synchronisiert hat.

4.3.3.3 Kategorie Synchronisation der einzelnen Elemente (+++)

In diesem Abschnitt wird zunächst der Ablauf des Synchronisationsvorgangs beschrieben, anschließend gehen wir detailliert auf die Synchronisation der einzelnen Elemente E-Mails, Termine, Kontakte, Aufgaben und Notizen ein. Des Weiteren folgen Ausführungen zu möglichen Problemfällen wie unerwartetem Verbindungsabbruch oder Speicherplatzmangel auf dem PDA.

Für jedes der zu synchronisierenden Elemente wurden die beiden Einwahlarten Zugang über RAS und Zugang über das Internet getestet. Dabei stellte sich heraus, dass die Einwahlart keinen Einfluss auf den Funktionsumfang bei der Synchronisation hatte. Bei den

Ausführungen zu den einzelnen Elementen werden wir deshalb auf die Unterscheidung nach Verbindungsart verzichten.

4.3.3.3.1 Ablauf des Synchronisationsvorgangs

Nach erfolgreicher Installation des XTND-Clients auf dem Endgerät befindet sich in dem Start-Menu von Windows Pocket PC eine Verknüpfung zum Starten der XTND-Client-Software. Nach Auswahl dieses Menupunktes gelangt der Benutzer zur Bedienoberfläche des XTND-Clients. Hier kann der Benutzer je nach gewünschter bzw. gegebener Kommunikationsinfrastruktur das passende Verbindungsprofil auswählen und den Synchronisationsprozess durch Klick des Buttons „Connect" anstoßen.

Der Benutzer wird aufgefordert, seinen Benutzernamen und sein Passwort einzugeben. Benutzername und Passwort sind identisch mit den im Intranet zur Anmeldung benötigten Benutzerdaten.

Gegenüber dem Exchange-Server verhält sich der XTNDConnect Server wie ein gewöhnlicher Microsoft Outlook Client. Nach Anmeldung mit den relevanten Benutzerdaten (Benutzerkennung und Passwort) hat XTND somit Zugriff auf alle Datensätze des jeweiligen Nutzers innerhalb des Exchange Datenbestandes.

Nach erfolgreicher Anmeldung am XTND-Server wird der Benutzer über den Status des Synchronisationsvorganges informiert. Die Dauer der Synchronisation ist abhängig von dem Datenvolumen und der Verbindungsart.

Ist der Synchronisationsprozess abgeschlossen, erscheint eine nach Kategorien unterteilte Auflistung der soeben synchronisierten Datensätze. Hier wird auch vermerkt, wie viele Datensätze bei der letzten Synchronisation neu hinzugekommen sind, aktualisiert oder gelöscht wurden. Durch Anwahl der einzelnen Kategorien wie „Inbox", „Outbox" etc. hat der Benutzer die Option, sich eine detailliertere Log-Meldung anzeigen zu lassen. Der XTND-Client kann anschließend beendet werden.

In der Standardkonfiguration des Windows Pocket PC findet der Benutzer auf dem Startbildschirm Verknüpfungen zum Posteingang, zu den Terminen sowie zu den Aufgaben. Neben den eigentlichen Verknüpfungen werden hier auch weitere Informationen wie z.B. die Anzahl der neuen E-Mails etc. angezeigt.

4.3.3.3.2 Verbindungswege und Profileinstellungen

Für die Synchronisation ist immer eine Verbindung zum Server nötig, dies kann auf unterschiedlichen Wegen realisiert werden. Die folgende Tabelle zeigt die möglichen Verbindungswege und gibt Aufschluss darüber, welche von XTND unterstützt werden.

Tabelle 4-27: XTND - Verbindungswege

Verbindungswege	
RAS über GSM	Ja
Internet über GPRS	Ja
WLAN	Ja
Serielle Dockingstation an einem Windows PC	Ja
USB Dockingstation an einem Windows PC	Ja

Für dieses Projekt relevant sind dabei die Verbindungswege Zugang über RAS und der Zugang über einen Windows-basierten PC. Auf dem PC muss hierfür der XTND Desktop Connector aktiviert sein, durch die Verwendung des DNS-Dummies spielt es für die Profileinstellungen des Benutzers keine Rolle, ob sich der zur Synchronisation benutzte Windows-PC innerhalb oder außerhalb des Intranets befindet.

Durch die Verwendung von VPN-Tunneln (siehe Kapitel 4.1.2.2.3) sowohl beim Zugang über RAS als auch beim Zugang über das Internet, benötigen wir für den XTNDClient nur ein Profil. Der Benutzer muss zwar, je nachdem, ob er über RAS oder über das Internet synchronisieren will, die passende VPN-Verbindung auswählen, aber der XTNDClient kontaktiert in beiden Fällen den in der DMZ befindlichen XTNDConnect Proxy Server.

4.3.3.3.3 E-Mails

Zunächst wurden die gängigen Grundfunktionalitäten für den E-Mailverkehr getestet. Die folgende Übersicht zeigt den Umfang der Tests.

Tabelle 4-28: XTND - Synchronisation von E-Mails

Synchronisation nach Bearbeitung am Endgerät	
Empfangen von E-Mails ohne Dateianhang	1
Empfangen von E-Mails mit Dateianhang	1
Senden von E-Mails ohne Dateianhang	1
Senden von E-Mails mit Dateianhang	1
Synchronisation nach Bearbeitung im Intranet	
Empfangen von E-Mails ohne Dateianhang	1
Empfangen von E-Mails mit Dateianhang	1
Senden von E-Mails ohne Dateianhang	1
Senden von E-Mails mit Dateianhang	1

Zum Testen der obigen Szenarien wurden E-Mails gesendet und empfangen, die den konfigurierbaren Dateigrößenbeschränkungen[64] entsprachen. Die Dateianhänge, die zum Testen verwendet wurden, befanden sich ebenfalls innerhalb der gesetzten Grenzen für Dateigrößen. Bei der Auswahl der Dateitypen wurde darauf geachtet, dass diese vom PDA interpretiert werden können. Dadurch wurde gewährleistet, dass keinerlei E-Mails oder deren Anhänge durch XTND herausgefiltert wurden. Außerdem wurden keinerlei Unterordner oder Filterregeln innerhalb von Microsoft Outlook am Arbeitsplatzrechner im Intranet für die Ordner Posteingang und Postausgang angelegt.

Das Empfangen und Versenden von E-Mails innerhalb der Ordner Posteingang und Postausgang verläuft sowohl mit als auch ohne die oben spezifizierten Dateianhänge einwandfrei. Neben den Grundfunktionen wie der Synchronisation gesendeter oder empfangener E-Mails wurde auch die Beachtung von Filterregeln getestet – hierunter fällt insbesondere die Synchronisation von Unterordnern, die innerhalb von Outlook im Intranet eingerichtet wurden. Außerdem wurden die Konfigurationsmöglichkeiten für Dateigrößenbeschränkungen und Dateitypenfilterung für den Synchronisationsprozess untersucht.

Synchronisation von Unterordnern

Bei der Synchronisation werden lediglich direkte Inhalte der Ordner Posteingang und Postausgang abgeglichen, Inhalte eventueller Unterordner jedoch nicht. Innerhalb des Intranets manuell in Unterordner verschobene E-Mails werden beim Synchronisieren auf dem PDA als gelöscht markiert und erscheinen im Posteingang des Endgerätes ebenfalls nicht mehr. Hieraus ergeben sich eine Reihe von Problemen beim Einsatz des mobilen Endgerätes.

Benutzer haben also darauf zu achten, welche Filterregeln sie auf ihrem Outlook im Intranet einrichten. E-Mails, die auf den PDA synchronisiert werden sollen, dürfen nicht in Unterordner verschoben werden.

Work-Around 1:

Grundsätzlich bietet der XTNDConnect Server zwar die Möglichkeit an, Unterordner und deren Inhalte mitzusynchronisieren. Dazu müsste man innerhalb der Administrationskomponente des XTND-Servers für jeden Benutzer und jeden zu synchronisierenden Ordner ein eigenes ActionSet[65] erstellen. Aufgrund des daraus resultierenden immensen Administrationsaufwands raten sowohl Extended Systems als auch wir von dieser Verfahrensweise ab[66].

Work-Around 2:

Zum anderen besteht die Möglichkeit, für jeden PDA-Benutzer einen zusätzlichen E-Mail-Account einzurichten, der den Synchronisationsansprüchen entspricht. Im Folgenden werden wir zur besseren Verständlichkeit für diesen E-Mail-Account den Begriff „Mobile-E-Mail-Account" benutzen. Innerhalb des Posteingangsordners dieses Accounts müssten dann sämtliche E-Mails zur Verfügung stehen, die der Benutzer mobil einsehen oder bearbeiten möchte. Auch dieser Work-Around ist allerdings nicht problemfrei. Eine Duplizierung und Verschiebung aller eintreffenden E-Mails in den Mobile-E-Mail-Account würde zu einem unpraktikabel hohen Transfervolumen führen. Es müssen also geeignete Filterregelungen gefunden werden, um die Speicherkapazitäten des PDA nicht zu überschreiten und das Transfervolumen in einem praktikablen Rahmen zu halten.

---

[64] Auf Dateigrößenbeschränkungen und ihre Konfigurationsmöglichkeiten gehen wir unter „Filterregeln" näher ein.

[65] ActionSets sind in der Installationsanleitung des XTNDConnect-Servers erläutert.

[66] Siehe dazu in http://www.extendedsystems.de/ESIde/Support/XTNDConnect+Server/default.htm#Unterordner [26.03.2003].

Für die Einrichtung der Filterregeln sind verschiedene Modelle denkbar. Es gibt die Möglichkeit, nur explizit gewünschte E-Mails in den Mobile-E-Mail-Account zu kopieren und damit zu synchronisieren. Eine Auswahl explizit gewünschter E-Mails lässt sich anhand einer so genannten „White List" realisieren. In dieser White List würden dann z. B. E-Mails von bestimmten Personen, einer bestimmten Priorität oder mit bestimmten Betreffzeilen vermerkt werden. Doch auch bei der White List-Strategie kann es zu Problemen kommen. E-Mails, die nicht den voreingestellten Kriterien entsprechen, werden nicht zur Synchronisation bereitgestellt. Somit kann es bei längerem ausschließlich mobilen Arbeiten zu Verspätungen und Versäumnissen kommen. Eine andere Strategie wäre es, alle E-Mails in den Mobile-E-Mail-Account zu kopieren, die nicht den voreingestellten Parameten entsprechen. Diese Strategie wird auch als „Black List" bezeichnet. Zum Beispiel könnte man so abbonierte und häufig eintreffende E-Mail-Newsletter, private Mails und ähnliches von der Synchronisation ausschließen. Beide dieser beschrieben Strategien erfordern aber ein hohes Maß an Pflege und Wartung um sie auf Dauer effektiv nutzen zu können.

Beachtung von Filterregeln

Filterregeln kann man zum einen in der Administrationskomponente des XTNDConnect-Servers (siehe Kapitel 4.3.3.2) und zum anderen im Client angeben. Auf dem Client erstellte Filterregeln können die auf dem Server erstellten Filterregeln lediglich verschärfen, aber nicht umgehen. Der XTND-Client bietet folgende Sychnchronisationseinstellungen für die Inbox:

- Angabe, ob bei ausgefilterten E-Mails nur
    - der Header der Nachricht + einstellbare Anzahl der Zeichen aus E-Mail-body
    - oder aber die gesamte E-Mail inkl. Anhang zu synchronisieren ist, wobei man noch folgendes einstellen kann:
        - Maximale Zeichen-Anzahl innerhalb des Textes der E-Mail
        - Maximale Größe in KB des Anhangs
- Die Anzahl der Tage, die synchronisiert werden sollen.

Änderungen der Filterregeln wirken sich nicht auf bereits synchronisierte Elemente aus, sondern erst auf die noch zu synchronisierenden. Die Bedienung ist jedoch nicht intuitiv verständlich. Eine Größenbeschränkung auf Zeichenanzahl zum einen und KB zum anderen scheint nicht sinnvoll.

„Ausgefilterte" E-Mails werden dennoch im Posteingang abgelegt, sie werden aber abgeschnitten und innerhalb der E-Mail erscheint die Meldung:

```
*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*

This message has been truncated:

Actual Size (1KB)
```

Ausgefilterte Anhänge bewirken folgende Meldung innerhalb der E-Mail:

```
*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*_*


Filtered Attachments(1):

Dateiname.Typ (50KB)
```

Diese Meldungen erfüllen zwar ihren Zweck, sind aber nicht besonders benutzerfreundlich.

Ausgefilterte E-Mails können nachträglich einschließlich Anhang heruntergeladen werden. Zum Abrufen der ausgefilterten E-Mails ist es notwendig, auf die Startseite zu gehen, den Button unten links, anschließend die Verknüpfung „Filtered E-Mail" auszuwählen, um die ausgefilterten E-Mails auflisten und einzeln herunterladen zu können.

Gesamtbewertung der Synchronisation von E-Mails:	**4**

4.3.3.3.4 Termine

Die folgende Tabelle gibt einen Überblick über den Umfang der durchgeführten Untersuchungen.

Tabelle 4-29: XTND - Synchronisation von Terminen

Synchronisation nach Bearbeitung am Endgerät	
Erstellen von eigenen Terminen	1
Verschieben von eigenen Terminen	1
Löschen von eigenen Terminen	1
Einladungen an Andere versenden	3
Termine mit Anderen verschieben	3
Termine mit Anderen absagen	3
Einladungen erhalten	3
Einladungen annehmen	3
Einladungen ausschlagen	3
Synchronisation nach Bearbeitung im Intranet	
Erstellen von eigenen Terminen	1
Verschieben von eigenen Terminen	1
Löschen von eigenen Terminen	1
Einladungen an Andere versenden	3
Termine mit Anderen verschieben	3
Termine mit Anderen absagen	3
Einladungen erhalten	3
Einladungen annehmen	3
Einladungen ausschlagen	3

Eigene Termine

Das Erstellen, Bearbeiten und Löschen von eigenen Terminen funktioniert problemlos, egal ob die Änderung auf dem PDA oder im Intranet vorgenommen wurde.

Termine mit anderen

In diesem Teilbereich treten Probleme auf. Ein Termin mit mehren Teilnehmern kann zwar vom Endgerät aus anberaumt werden, aber dieser Termin wird den anderen Teilnehmern nur als Text-E-mail übermittelt und muss dann von Hand in die eigenen Termine eingepflegt werden. Auch eine Änderung oder Löschung dieser Termine ist nicht mit der von Outlook gewöhnten Automatisierung möglich.

Das Empfangen von Terminen am Endgerät, die durch andere gesetzt wurden, weist ähnliche Problemen auf. Werden solche Terminen zuerst auf dem PDA empfangen, so werden diese als reine Textmails dargestellt und müssen anschließend manuell in den Terminkalender übernommen werden.

Microsoft Outlook bietet die Möglichkeit, bei entsprechender Berechtigung in fremde Terminkalender Einsicht zu nehmen. Dies ist bei komplexeren Terminplanungen von großem Vorteil, da nicht erst Termine anberaumt werden, die dann aufgrund von Terminüberschneidungen bei anderen Personen verschoben werden müssen. Mobile Outlook bietet nicht die Funktionalität, diese öffentlichen Terminkalender einzusehen.

Gesamtbewertung der Synchronisation von Terminen	3

4.3.3.3.5 Kontakte

Bei der Synchronisation werden die persönlichen und öffentlichen Kontakte unterschiedlich behandelt.

Persönliche Kontakte

Bei der Evaluation der Synchronisation der persönlichen Kontakte wurden folgende Szenarien unterschieden:

Tabelle 4-30: XTND - Synchronisation von persönlichen Kontakten

Synchronisation nach Bearbeitung am Endgerät	
Kontakte erstellen	1
Kontakte bearbeiten	1
Kontakte ergänzen	1
Kontakte löschen	1
Synchronisation nach Bearbeitung im Intranet	
Kontakte erstellen	1
Kontakte bearbeiten	1
Kontakte ergänzen	1
Kontakte löschen	1

Die Synchronisation von eigenen Kontakten funktionierte unabhängig vom Bearbeitungsort ohne Probleme. Beachtung sollten hier wiederum die Unterschiede von Microsoft Outlook und Mobile Outlook finden. Nicht alle vordefinierten Textfelder von Microsoft Outlook sind unter derselben Bezeichnung in der Mobilversion zu finden, andere Felder sind gar nicht vorhanden.

Öffentliche Kontakte

Beim Arbeiten im Intranet ist mittels Microsoft Outlook die Einsicht bzw. die Verwaltung von öffentlichen Kontakten möglich, sofern der jeweilige Benutzer die dementsprechenden Zugriffsrechte besitzt. Mobile Outlook hingegen kann nicht zwischen privaten und öffentlichen Kontakten unterscheiden. Bei der Synchronisation der Kontaktdatensätze mittels XTND werden momentan lediglich die persönlichen Kontakte abgeglichen.

Diese Vorgehensweise ist unbefriedigend, da öffentliche Kontaktordner in Organisationen ab einer gewissen Größenordnung eine immense Rolle spielen. Eine Synchronisation aller öffentlichen Kontakte scheint nicht sinnvoll, da dies die Speicherkapazitäten eines PDA übersteigen könnte.

Wünschenswert hingegen wäre die Möglichkeit, sich bestimmte Kontakte aus dem öffentlichen Kontaktordner „on the fly" herunterladen zu können. Dies könnte beispielsweise dadurch geschehen, dass beim Anstoß des Synchronisationsvorgangs lediglich eine Liste der zur Verfügung stehenden Kontakte übertragen wird, aus der man sich anhand der Namen den benötigten Kontaktdatensatz herunterladen und lokal auf dem PDA speichern kann.

Gespräche mit Mitarbeitern der Firma Extended Systems stellten eine Lösung dieses Problems in Aussicht. In künftigen Versionen von XTND soll die Angabe von beliebigen Kontaktordnern für die Synchronisation möglich sein. Allerdings ist auch hierbei zu beachten, dass voraussichtlich die gesamten Datensätze übertragen werden und nicht wie oben beschrieben eine Liste optional herunterladbarer Kontakte.

Anzumerken ist in diesem Zusammenhang, dass derzeit auch keine andere Synchronisationssoftware die Funktionalitäten zum optionalen Synchronisieren von durch den Endbenutzer ausgewählten Kontakten unterstützt.

Abhilfe kann derzeit nur durch das Kopieren der benötigten Kontakte aus den öffentlichen Ordnern in den persönlichen Kontakte-Ordner geschaffen werden. Allerdings ist auch dieser Work-Around unbefriedigend. Zentral ausgeführte Aktualisierungen von öffentlichen Kontakten werden nicht automatisch mit den persönlichen Kontakten abgeglichen. Die zentrale Administration und Aktualisierung sind somit nicht mehr möglich. Damit wird der eigentliche Sinn von öffentlichen Kontakten untergraben.

Gesamtbewertung der Synchronisation von Kontakten	**4**

4.3.3.3.6 Aufgaben

Tabelle 4-31: XTND Synchronisation von Aufgaben

Synchronisation nach Bearbeitung am Endgerät	
Eigene Aufgaben erstellen	1
Eigene Aufgaben bearbeiten	1
Eigene Aufgaben löschen	1
Aufgaben an Andere senden/ zuweisen	--[67]
Aufgaben an Andere bearbeiten	--
Aufgaben an Andere löschen	--
Aufgaben von Anderen erhalten und annehmen	3
Aufgaben erhalten und ablehnen	3
Synchronisation nach Bearbeitung im Intranet	

[67] Wird von Pocket Outlook nicht unterstützt.

Eigene Aufgaben erstellen	1
Eigene Aufgaben bearbeiten	1
Eigene Aufgaben löschen	1
Aufgaben an Andere senden/ zuweisen	--
Aufgaben an Andere bearbeiten	--
Aufgaben an Andere löschen	--
Aufgaben von Anderen erhalten und annehmen	1
Aufgaben erhalten und ablehnen	1

Eigene Aufgaben

Die Synchronisation der eigenen Aufgaben verlief im Testbetrieb, unabhängig davon, ob die Bearbeitung im Intranet oder am PDA stattfand, einwandfrei.

Aufgaben an Andere zuweisen oder Augabenanforderungen empfangen

Schwierigkeiten verursachte das Zuordnen von Aufgaben an Andere. Microsoft Outlook bietet die Möglichkeit an, Aufgaben an Personen aus den zugänglichen Kontakten zuzuweisen. In diesem Fall bekommt die Person, der die Aufgabe zugeordnet wurde, eine E-Mail mit einem Attachment, das von Outlook als Aufgabenzuweisung interpretiert wird. Die empfangende Person kann dann die Aufgabe annehmen oder ablehnen. Wird die Aufgabe angenommen, so wird diese automatisch in die eigenen Aufgaben übernommen und es werden Termine im Kalender für Fälligkeitsdatum und Erinnerungsdatum etc. gesetzt. Lehnt der Empfänger die Aufgabenanforderung ab, so wird der zuweisende Benutzer per E-Mail benachrichtigt und der kann die Aufgabe neu oder anderweitig vergeben.

Diese Funktionalität steht in Mobile Outlook nicht zur Verfügung. Mit Mobile Outlook ist eine Zuweisung von Aufgaben an andere Personen nicht möglich. Weiterhin kann Mobile Outlook nicht zwischen eigenen Aufgaben und anderen Benutzern zugewiesenen Aufgaben unterscheiden. So tauchen Aufgaben, die vom Intranet aus an andere Personen oder Personengruppen zugewiesen wurden, in Mobile Outlook als eigene Aufgaben auf.

Aufgabenanfragen von Anderen werden von Mobile Outlook als gewöhnliche E-Mails behandelt, es erfolgt also insbesondere kein Eintrag im eigenen Kalender für etwaige Erinnerungs- oder Fälligkeitstermine der Aufgabe. Dies wird verursacht, da bei Aufgabenanfragen das MS-Outlook-Aufgaben-Objekt als Anhang der E-Mail verschickt wird. Diesen Anhang erkennt Mobile Outlook nicht.

Die Synchronisation der bereits im Intranet von anderen zugewiesenen und übernommenen Aufgaben funktioniert wiederum einwandfrei, da schon im Intranet diese als eigene Aufgabe behandelt werden und sämtliche mit der Aufgabe verbundenen Termine gesetzt sind.

Gesamtbewertung der Synchronisation von Aufgaben	**3**

4.3.3.3.7 Notizen

Tabelle 4-32: XTND - Synchronisation von Notizen

Synchronisation nach Bearbeitung am Endgerät	

Notizen erstellen	1
Notizen bearbeiten	1
Notizen löschen	1
Synchronisation nach Bearbeitung im Intranet	
Notizen erstellen	1
Notizen bearbeiten	1
Notizen löschen	1

Die Evaluation der einzelnen Szenarien ergab keinerlei Probleme oder Unstimmigkeiten bei der Synchronisation von Notizen.

Gesamtbewertung der Synchronisation von Notizen	**1**

4.3.3.3.8 Öffentliche Ordner

XTNDConnect Server bietet in der eingesetzten Version keine direkte Möglichkeit, öffentliche Ordner zu synchronisieren. Wie bereits im Einführungskapitel erläutert ist die Synchronisation der öffentlichen Ordner ohnehin wegen dem begrenzten Speicherplatz der PDAs nicht sinnvoll.

Work-Around:

Man kann innerhalb des XTNDConnect Servers bestimmte Ordner für die Synchronisation angeben. Je nach Konfiguration werden diese Ordner dann entweder benutzer- oder gruppenspezifisch auf die Endgeräte übertragen. Zu beachten ist hierbei, dass die Dateien innerhalb dieser Ordner vom PDA interpretierbar sein sollten. Ein Nachteil dieses Work-Arounds ist, dass bei Anstoß einer Synchronisation der Ordner komplett übertragen wird und der Benutzer nicht die Möglichkeit hat, sich optional einzelne Dateien herunterzuladen.

Gesamtbewertung der Synchronisation öffentlicher Ordner	**4**

4.3.3.3.9 Umgang mit möglichen Problemfällen

Hier wurde der Umgang mit Speicherplatzmangel auf dem PDA und der Umgang mit einem Verbindungsabbruch während einer Synchronisation untersucht.

Speicherplatzmangel

Im Test wurde der Speicherplatzmangel bewusst herbeigeführt. Beim letzten und entscheidenden Synchronisationsvorgang wurde die Kapazitätsgrenze des Endgerätes überschritten und der Synchronisationsvorgang ohne Fehlermeldung abgebrochen.

Der Pocket PC besitzt eine dynamische Speicherverwaltung, die den gesamten Speicher des Gerätes je nach Bedarf als Arbeits- oder Datenspeicher nutzt. Diese Speicherverwaltung kann es aber nicht verhindern, dass durch einen letzten und entscheidenden Downloadvorgang die Speicherkapazität des PDAs überschritten werden kann. Im Gegenteil kommt es erst durch die dynamische Speicherverwaltung zu schwerwiegenden Funktionsstörungen, da der gesamte Speicher für die Daten verwendet wird und somit kaum noch Arbeitsspeicher zur Verfügung steht.

Ein weiterer anschließender Synchronisationsversuch scheiterte daran, dass sich die Oberfläche von XTND zwar noch aufrufen ließ, ein Betätigen des Connect-Button aber ohne

Folgen blieb. Auch hier blieb uns das Endgerät eine Fehlermeldung schuldig, die auf das bestehende Problem hätte hinweisen können.

Erst das Löschen sämtlicher Nutzdaten und ein Softreset brachten das Gerät wieder in einen arbeitsfähigen Zustand, dann ließ sich der XTND Client wieder starten. Ein erneuter Synchronisationsversuch schlug aber wiederum fehl. Jetzt erst wurde eine Fehlermeldung angezeigt: „Server Connection Lost". Erst die Anmeldung mit einem anderen Benutzernamen brachte das System wieder in einen voll funktionsfähigen Zustand.

Verbindungsabbruch

Auch dieses Problem wurde von uns bewusst herbeigeführt. Hierzu wurde während eines laufenden Synchronisationsvorganges per RAS das Modem auf der Serverseite ausgeschaltet. Daraufhin wurde eine Fehlermeldung auf dem Endgerät angezeigt, die den Benutzer über die verlorene Verbindung informierte. Gleichzeitig führte der Verbindungsabbruch aber zu einen Absturz des Endgerätes. Auch hier half wiederum nur ein Softreset.

Gesamtbewertung des Umgangs mit Problemfällen	5

4.3.3.4 Kategorie Sicherheit (+++)

Tabelle 4-33: XTND - Sicherheit

Kategorie Sicherheit	Bewertung
Kennwortverwaltung	
Kennwort zur Synchronisation verlangt (ja/nein)	Ja
Kennwort durch Administrator einsehbar (ja/nein)	Nein
Power-On-Passwort vorhanden (ja/nein)	Ja[68]
Verschlüsselung des Netzwerkverkehrs	
RSA (ja/nein)	Ja
SSL (ja/nein)	Ja
VPN (ja/nein)	Ja
Sonstige Verschlüsselungsmechanismen (ja/nein)	Nein

Die Sicherheitsfunktionen des XTNDConnect Servers sind bis auf einige Schwächen in der Kennwortverwaltung positiv zu bewerten. Die Software sollte nur dann den Zugriff auf den Server freigeben, wenn die kennwortgeschützte Einschaltsperre (Power-on-Passwort) auf dem PDA aktiviert ist. In Tests hat sich aber herausgestellt, dass dies keinen Einfluss auf die Synchronisation der Groupware-Daten hat. Erst beim Abgleich mit einem persönlichen Ordner greift diese Restriktion, zu diesem Zeitpunkt sind aber E-Mails, Termine etc. bereits auf dem neuesten Stand. Dies stellt eine massive Sicherheitslücke dar, die durch geeignete Endgerätesoftware abgefangen werden muss.

Die eigentliche Authentifizierung der User erfolgt auf zwei Ebenen. Wir sprechen also von einer Two-Tier-Authentifizierung, wobei die erste Ebene durch Windows NT/2000/XP und die zweite durch Microsoft Exchange beziehungsweise Lotus Notes definiert wird. Die Authentifizierung auf erster Ebene ist Active Directory kompatibel.

[68] Funktioniert nur begrenzt, Details befinden sich in der textuellen Beschreibung.

Immerhin ist es nicht möglich, die Passwortabfrage für die eigentliche Authentifikation abzuschalten. Theoretisch besteht die Möglichkeit, das Passwort zu speichern, hierfür ist eine Checkbox auf der Oberfläche der Client-Software vorgesehen. Der Administrator kann bei der Konfiguration der Client-Software allerdings die Möglichkeit zur Speicherung von Passwörtern unterbinden. Die Checkbox ist dann zwar weiterhin vorhanden, kann vom Benutzer aber nicht aktiviert werden.

Eine eklatante Sicherheitslücke hat sich dennoch bei Eingabe des Passwortes ergeben. Nach mehrmaliger Eingabe des Passwortes kam es auch hier diverse Male dazu, dass Wortvorschläge erschienen. Dies ist eigentlich ein Feature, das vom Betriebssystem PocketPC2002 zur Verfügung gestellt wird, aber zur Unterstützung bei der Eingabe von Texten gedacht ist. Zu den Einstellungen der Wortvorschläge gibt es betriebssystemeigene Optionen, die aber von der Synchronisationssoftware nicht beeinflusst werden können.

Während der Verbindung zwischen Server und PDA arbeitet das System mit einer Kombination aus symmetrischer und asymmetrischer Verschlüsselung. Beim Verbindungsaufbau erfolgt der Keyaustausch mit asymmetrischer ECC-Verschlüsselung (Elliptic Curve Cryptography). Die zu übertragenden Daten werden symmetrisch durch RC4-Algorithmen verschlüsselt. Der RC4-Algorithmus ist ein Verschlüsselungsverfahren von RSA Data Security Inc. und arbeitet mit einem geheimen Schlüssel und einer variablen Schlüssellänge. Desweiteren besteht die Möglichkeit, eine zusätzliche SSL-Schicht über die RSA-verschlüsselten Daten zu legen. Sollte dies immer noch als unzulänglich erscheinen, so lässt sich all dies nochmals über einen VPN-Tunnel absichern.

Gesamtbewertung Sicherheit:	**2**

4.3.3.5 Kategorie Usability (++)

Tabelle 4-34: XTND - Usability

Kategorie Usability	**Bewertung**
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	nein
Verfügbar in englischer Sprache (ja/nein)	ja
Verfügbar in weiteren Sprachen (ja/nein)	nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	2
Daten können wie von der Aufgabe gefordert eingegeben werden	2
Informationen und Bedienelemente befinden sich am richtigen Platz	3
Alle benötigten Informationen sind auf dem Bildschirm zu finden	3
Ausgaben sind zweckmäßig und verständlich	3
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	2
Selbstbeschreibungsfähigkeit	

Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	4
Meldungen sind sofort verständlich	3
Rückmeldungen können einer Ursache eindeutig zugeordnet werden	3-4
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	2
Auswirkungen von Aktionen hinreichend ersichtlich	2
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	3
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	3
Aktueller Bearbeitungsschritt kann unterbrochen werden	2
Ein laufender Vorgang kann abgebrochen werden	2
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	2
Bearbeitungszeit abschätzbar	4
Einheitliche Verwendung von Begriffen und Symbolen	2
Die Ausführung einer Operation führt zu erwarteten Ergebnis	2
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	2
Eingaben werden auf syntaktische Korrektheit geprüft	3
Versehentliches Auslösen von Aktionen unmöglich	1
Bei Fehlern zweckmäßige Hinweise zur Ursache und Behebung	4
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	4
Erlernbarkeit	
Schnelles Erlernen der Bedienung	2
Intuitive, selbsterklärende Benutzung möglich	2
Nur wenige Detailkenntnisse zur Bedienung nötig	2
Hilfestellung bei Bedarf verfügbar	4

Zu bemängeln ist beim XTND-Produkt, dass sowohl die Server- als auch die Clientkomponenten lediglich in englischer Sprache vorhanden sind.

Die Bedienung gestaltet sich recht einfach. Die Konfigurationen können von der Administration definiert werden. Durch geeignete Vorkehrungen wie der Einrichtung eines DNS-Dummies und dem Einsatz der VPN-Verbindung ist nur ein einziges Verbindungsprofil notwendig, womit ein Auswählen des geeigneten Profils entfällt.

Auch die Synchronisationsoptionen wie Dateigrößenbeschränkungen bei der Übertragung von E-Mails oder der zu synchronisierende Zeitraum bei E-Mails, Terminen und Aufgaben etc. sollten bereits vom Administrator vorgenommen werden, da dies sich auf dem XTNDClient für den Endnutzer als nicht intuitiv und kompliziert darstellt.

Zum Starten der Synchronisation ist lediglich ein Betätigen des Connect-Button mit anschließender Passworteingabe notwendig. Die daraufhin folgende Logseite gibt direkt nach dem Synchronisationsvorgang Informationen über die synchronisierten Elemente aus. Die Logmeldungen sind allerdings nicht sehr benutzerfreundlich gestaltet und geben beispielsweise auch keinen Aufschluss über ausgefilterte E-Mails.

Überhaupt gestaltet sich der Umgang mit ausgefilterten E-Mails etwas umständlich und nicht intuitiv. Dass eine E-Mail nicht oder aufgrund von Dateigrößenbeschränkungen in Form von Filterregeln unvollständig übertragen wurde, erfährt man nur durch einen Blick in die E-Mail selbst, an deren Ende die Meldung „Truncated Message" auftaucht oder durch einen Blick in die Liste der ausgefilterten E-Mails[69].

Zu bemängeln ist weiterhin, dass zum Teil bei verschiedenen Ereignissen die gleiche Fehlermeldung ausgegeben wird, z. B. „Authentication Failed" bei Fehlanmeldung und bei Speicherüberlastung des PDAs, die damit nicht eindeutig einer Fehlerquelle zugeordnet werden können. Außerdem entbehren die Fehlermeldungen zweckmäßige Hinweisen zur Fehlerbehebung.

Auch die Art der Rückmeldung (Fehler/Warnung/Information etc.) wird nicht kategorisiert. Dies wäre beispielsweise durch geeigneten Farbeinsatz oder durch ein vorangestelltes „Warning" realisierbar.

Irritierend ist, dass die Option „Save Passwort" noch immer erscheint aber nicht aktivierbar ist, wenn dies beim Setup durch den Administrator unterbunden wurde. Die Anzeige dieser Option könnte jedoch in diesem Fall gänzlich entfallen, um den Benutzer nicht zu verwirren.

Die Synchronisation einzelner E-Mails und Dateien kann problemlos unterbrochen werden, wenn sich beispielsweise herausstellt, dass der Vorgang sonst zu lange dauern würde. Negativ ist jedoch, dass nicht schon bei Anstoß der Synchronisation über das zu erwartende Transfervolumen informiert wird.

Gravierende Mängel weist die Fehlerrobustheit auf. Vor allem bei einem unerwarteten Verbindungsabbruch oder bei Speicherplatzmangel auf dem PDA sind die Auswirkungen für den Benutzer unzumutbar. So führt beides zu Systemabstürzen des PDAs, der letztendlich nur durch einen Softreset oder noch drastischere Maßnahmen behoben werden kann. Eine Warnung, dass nicht genug Speicherplatz für die zu synchronisierenden Daten vorhanden ist, fehlt vollends.

Die Erlernbarkeit ist als gut zu beurteilen, wenn die Möglichkeiten zur Vorkonfiguration ausgeschöpft werden. Eine Einführung über den Umgang mit ausgefilterten E-Mails und insbesondere das Aufzeigen der Möglichkeit des Softresets sind allerdings unabdingbar.

Gesamtbewertung Usability:	**3**

4.3.3.6 Kategorie Kosten (+)

Tabelle 4-35: XTND - Kosten

Kategorie Kosten	**Bewertung**
Einmalige Kosten	

[69] Zum Abrufen der ausgefilterten E-Mails ist es notwendig, auf die Startseite zu gehen, den Button unten links und anschließend die Verknüpfung „Filtered email" auszuwählen, um die ausgefilterten E-Mails auflisten und einzeln herunterladen zu können.

Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Schulungsmaßnahmen für die Administration der Software	1
Schulungsmaßnahmen für die Benutzer	2
Aufwand für die initiale Installation und Konfiguration der Komponenten	2
Laufende Kosten	
Administration	2
Zusätzliche Kosten für Support-/Wartungsvertrag	2

Die Kosten sind stark abhängig vom Umfang, in dem auf benutzerspezifische Wünsche bezüglich der Synchronisationsoptionen eingegangen wird. Je weniger benutzerspezifische Einstellungen verwaltet werden, umso geringer ist der Administrationsaufwand und somit die Kosten. Die Einstellungen können schon bei der initialen Installation oder aber erst später bei laufendem Betrieb vorgenommen werden.

Gesamtbewertung Kosten:	**2**

4.3.3.7 Kategorie Besondere Merkmale (+)

Tabelle 4-36: XTND - Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Herstellerangaben	2
Externe Referenzen/Erfahrungsberichte	1
Zukünftig zu erwartende Funktionalitätserweiterungen	3
Erwartungen Zukunftssicherheit	2
Weitere wichtige Eigenschaften	2

Die Ergebnisse in dieser Kategorie decken sich größtenteils mit den Herstellerangaben. Zwar ist die Synchronisation von E-Mails, Kalender, Kontakten, Aufgaben und Notizen nur bedingt möglich, aber dies ist auf die Beschränkungen von Pocket PC und Pocket Outlook zurückzuführen. Zu bemängeln ist an dieser Stelle lediglich die Unausgereiftheit des Power-On-Passworts, was aber hier nicht weiter ins Gewicht fällt, da in jedem Fall zusätzliche Sicherheitssoftware verwendet wird.

Auf der offiziellen Webseite von XTND sind eine Reihe von Wirtschaftsgrößen wie British Airways und Reuters Ltd. vertreten, die Empfehlungen für das Produkt abgeben. Außerdem wird das Produkt bereits im Bundeskanzleramt verwendet. Das Bundeskanzleramt berichtete uns gegenüber von durchweg positiven Erfahrungen mit diesem Produkt.

An Funktionalitätserweiterungen stellt XTND eine Lösung zur Synchronisation von öffentlichen Kontakten und Ordnern in Aussicht.

Die Zukunft des Produktes ist natürlich abhängig vom Weiterbestehen der Firma Extended Systems. Viele große Kunden aus verschiedenen Wirtschaftsbereichen und weitgefächerten Branchen lassen ein plötzliches und gravierendes Schrumpfen des Kundenstamms unwahrscheinlich erscheinen. Da diese Kunden den XTNDConnect Server verwenden, ist davon auszugehen, dass die Weiterentwicklung und der Support von Exten-

ded Systems auch weiterhin gewährleistet sein werden. Das Produkt ist auch nach eventueller Migration zum Lotus Domino Server einsatzfähig.

Eine weitere wichtige Eigenschaft stellt die Möglichkeit dar, ausgewählte Ordner für einzelne Benutzer und auch für bestimmte Benutzergruppen zu synchronisieren. Außerdem gilt es zu beachten, dass zur Synchronisation ausschließlich der Connect-Client benutzt werden darf und nicht wie allgemein üblich das Pocket-PC-eigene ActiveSync. Bei Nichteinhaltung dieser Auflage kann es zu Inkonsistenzen bei den zu synchronisierenden Inhalten — wenn nicht sogar zu Datenverlust — kommen.

Gesamtbewertung der besonderen Merkmale:	1

4.3.3.8 Gesamtbewertung für XTND

Tabelle 4-37: Gesamtbewertung Synchronisation über XTND

	Gesamtbewertung	Note
++	Kategorie Administration	2
+++	Kategorie Synchronisation der einzelnen Elemente	3
+	Kategorie Kosten	2
+++	Kategorie Sicherheit	2
++	Kategorie Usability	3
+	Kategorie Besondere Merkmale	1

Das Produkt ist sehr transparent, überschaubar und gut konfigurierbar. Die Sicherheitsmechanismen sind überzeugend, müssen aber durch geeignete Sicherheitssoftware auf dem Endgerät unterstützt werden, da das Power-On-Passwort nicht den diesem Projekt zu Grunde liegenden Sicherheitsanforderungen gerecht wird.

Die Beschränkungen im Funktionsumfang lassen sich größtenteils auf die Begrenztheit des Pocket PC zurückführen und beeinflussen auch die Usability negativ. Die Möglichkeit, ausgewählte Ordner für die Synchronisation zu konfigurieren, stellt eine sinnvolle Alternative zur Synchronisation von öffentlichen Ordnern dar.

Das Produkt hält die Option einer Migration zu Lotus Domino offen, zudem mindert man durch Einsatz von XTND die Abhängigkeit von Microsoft.

Lobend zu erwähnen ist an dieser Stelle auch der Support der Firma, der beeindruckend schnell und hilfsbereit erfolgte. Wir haben sowohl mit dem Produkt als auch der Firma Extended Systems gute Erfahrungen gemacht und können die positiven Berichte des Bundeskanzleramts vollkommen bestätigen.

4.3.4 Gesamtfazit zur Synchronisationssoftware

Eine Synchronisationslösung, die allen in der Aufgabenstellung des Projektes definierten Ansprüchen genügt, gibt es derzeit nicht. Dies wird durch den begrenzten Speicherplatz auf den untersuchten Endgeräten als auch den begrenzten Funktionsumfang des Pocket PC Betriebssystems und des Mobile Outlook verursacht.

Das größte Manko ist, dass die Inhalte von Unterordnern des Posteingangsfaches sowie öffentliche Ordner und öffentliche Kontakte nur über Umwege und zumeist nur unbefriedigend synchronisiert werden.

Die XTND-Lösung weist im Vergleich zur Microsoft-Lösung folgende Vorteile auf:

- Der XTNDConnect Server unterstützt den Abgleich von Notizen, während der MIS dazu nicht fähig ist.
- Die XTND-Lösung ist wesentlich transparenter und dadurch auch sicherer, da der ISA-Server über eine Vielzahl von zusätzlichen Features wie VPN, Routing, RAS, Firewall- und Cachefunktionalitäten verfügt. All diese Funktionalitäten sind für die Proxy-Komponente der Synchronisationsoftware jedoch überflüssig, wenn sie durch den Einsatz anderer, bewährter Produkte abgedeckt werden.
- Für den Betrieb und die Konfiguration des XTNDConnect Servers sind im Gegensatz zu der MIS/ISA-Lösung geringere Schulungsmaßnahmen notwendig. Der Support der Firma Extended Systems stellte hilfsbereit und schnell Lösungen für aufgetretenen Probleme bereit.

4.4 Endgerätesoftware

In diesem Kapitel erfolgt die Evaluation der Clientseite. Den Evaluationsbaum zeigt Abbildung 4-20. Untersucht werden im Rahmen der Komponentenevaluation insbesondere die Fähigkeiten verschiedener Softwarelösungen für die iPAQ Handhelds zur Steigerung der Sicherheit (siehe Komponentenauswahl in Kapitel 3.1.3.1). Als feste Antiviruskomponente kommt dabei F-Secure Antivirus zum Einsatz, das hier jedoch nicht getrennt untersucht wird, da es bereits Teil der Basiskonfiguration (siehe Kapitel 4.1.2) ist. Als Referenzsystem für die Evaluation gilt der iPAQ h3970 in seiner Basiskonfiguration. So wird verhindert, dass Kompatibilitätsprobleme, die den Softwareprodukten nicht anzulasten sind, die Bewertung verfälschen, da der h5940 erst im April 2003 auf den Markt gekommen ist. Auf aufgetretene Probleme wird jedoch bei den entsprechenden Produkten hingewiesen.

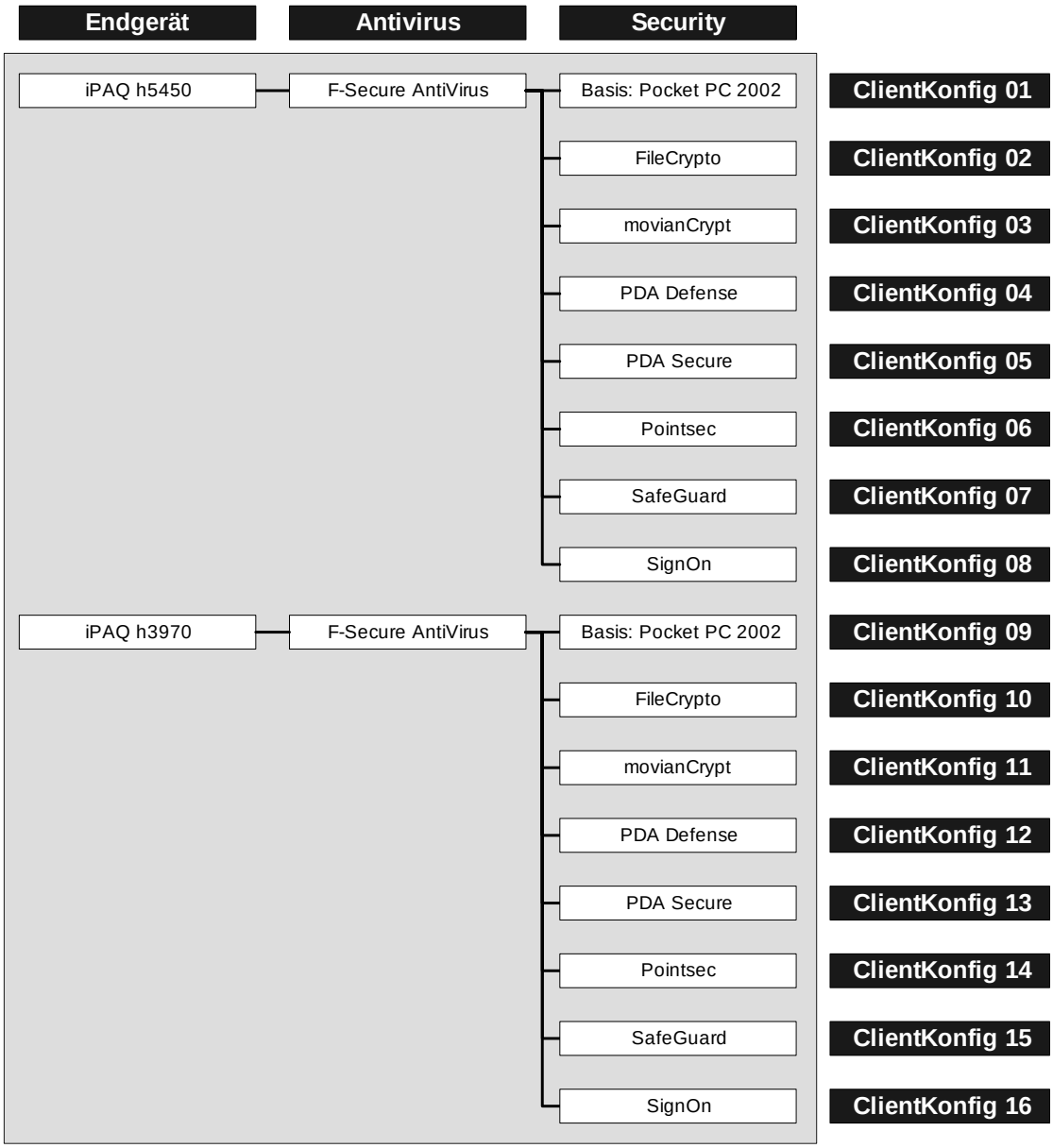

Abbildung 4-20: Evaluationsbaum der Clientseite (2)

4.4.1 Kategorien

Wie in Kapitel 4.1.5.5 beschrieben, sind zur Evaluation der Sicherheitslösungen für Endgeräte die identifizierten Anforderungen kategorisiert. Grundsätzlich wurden im Rahmen der Komponentenauswahl (Kapitel 3.1.3.1) zwei Kernziele für die Nutzung zusätzlicher Software entwickelt:

- Erhöhen der Datensicherheit durch Verschlüsselung
- Erhöhen der Datensicherheit durch verbesserte Anmeldeprozedur

Die Möglichkeit zur Verschlüsselung wurde hierbei als zwingend notwendig erachtet, da der auf verlorenen oder entwendeten Geräten befindliche Datenbestand sonst nicht in ausreichender Weise vor dem Zugriff unbefugter Dritter geschützt ist. Ein Austausch der Anmeldeprozedur ist ebenfalls unbedingt erforderlich, um die im Gerät gespeicherten Daten zu sichern. Eine Lösung, bei der das Dateisystem zwar verschlüsselt wird, die Benutzerauthentifikation jedoch als unsicher zu bewerten ist, erscheint ebensowenig sinnvoll wie der umgekehrte Fall. Es gilt hier das Prinzip des schwächsten Gliedes einer Kette. Austausch der Authentifikation und Verschlüsselung des Gerätes sind nur dann sinnvoll, wenn beide gemeinsam in sich ergänzender Weise Verwendung finden. Die ersten beiden zu betrachtenden Kategorien für die hier untersuchten Softwarekomponenten zur Erhöhung der Endgerätesicherheit sind deshalb:

- Authentifikation
- Datensicherheit.

Neben diesen beiden für die Endgerätesoftware zentralen Aspekten sind die bereits in Kapitel 4.1.5.5 definierten, für dieses Projekt grundlegenden Kategorien zu betrachten:

- Administration
- Usability
- Kosten.

Die ebenfalls in Kapitel Kapitel 4.1.5.5 definierte Basiskategorie „Sicherheit" fließt in die Untersuchung der Kategorien „Authentifikation" und „Datensicherheit" ein. Außerdem wurde eine Kategorie benötigt, um auch Eigenschaften der jeweiligen Software bewerten zu können, die entweder nur für einzelne Lösungen relevant sind oder nicht einer der übrigen Kategorien zugeordnet werden konnten: Die Kategorie

- Besondere Merkmale.

Im Folgenden werden die einzelnen Kategorien und die zugehörigen Evaluationskriterien vorgestellt. Die innerhalb der einzelnen Kategorien definierten KO-Kriterien (siehe Kapitel 4.1.5.2) sind gesondert hervorgehoben.

4.4.1.1 Die Kategorie Administration

Eine Software ist nur dann wirklich für den Einsatz in größeren Organisationen geeignet, wenn sie Möglichkeiten zu zentralen Administration bietet. Relevant für Endgerätesoftware sind insbesondere die Möglichkeiten der Administration von

- Verschlüsselungs-Policies für geräteinternen und –externen Speicher
- PIN-/Passwort-Policies
- Policies für sicherheitsrelevante Einstellungen.

Weitere wichtige Administrationsaspekte sind:

- Verteilung von Updates der Sicherheitssoftware
- Verteilung von Updates anderer Software
- Zentrales Key-Management
- Zentrale Schlüsselerstellung
- Profilverwaltung.

Mittels dieser Methoden ist es insbesondere möglich, Sicherheitsrichtlinien über die gesamte Organisationseinheit hinweg effektiv umzusetzen und so ein klar definiertes Mindestmaß an Sicherheit zu gewährleisten, das im Idealfall vom Nutzer nicht unterschritten werden kann. Ein Policy-Konzept sollte es ermöglichen festzulegen, dass der Benutzer eine Passwortlänge von mindestens sechs Zeichen unter Verwendung von Buchstaben und Ziffern verwenden muss.

Einige in das Testfeld aufgenommene Produkte verfügen über eigene Komponenten zur Administration o. g. Aspekte. Um eine integrierte Produktivumgebung zu ermöglichen, betrachteten wir außerdem, welche Möglichkeiten die jeweilige Software für ein Zusammenspiel mit den in diesem Projekt untersuchten Administrationskomponenten Afaria und XTND bietet:.

- Zusammenarbeit mit Afaria und
- Zusammenarbeit mit XTND.

Die Benotung dieser beiden Kriterien bezieht sich auf die Möglichkeiten, die jeweilige Software durch von den Managementlösungen bereitgestellte Verfahren zu administrieren. Dies kann beispielsweise durch die von Afaria bzw. XTND geleistete Verteilung von Konfigurationsdateien geschehen. Je besser ein solches Verfahren in die gesamte Umgebung integriert werden kann, desto besser fällt die Bewertung für diese Kriterien aus. Werden von der Software beispielsweise die für eine Installation auf den Clients benötigten Dateien (.cab) explizit bereitgestellt, so dass ein Deployment der Software mittels der jeweiligen Administrationslösung in praktikabler Weise möglich ist, so lautet die Bewertung für das entsprechende Kriterium „ausreichend".

Weitergehende Möglichkeiten wie die Verteilung von Konfigurationsdateien, anhand derer applikationsspezifische Einstellungen wie Policies etc. möglich sind, führen zu einer entsprechend besseren Bewertung. Als „sehr gut" gilt ein Zusammenspiel, bei dem alle oder nahezu alle sicherheitsrelevanten Einstellungen der Software über Konfigurationsdateien konfigurierbar sind und diese sich problemlos verteilen lassen. Auch die Bereitstellung grafischer Tools zur Policy-Bearbeitung und Generierung der Konfigurationsdateien direkt in die entsprechenden Verzeichnisse der Management-Software wurden entsprechend positiv bewertet. Negative Auswirkungen auf die Beurteilung dieser beiden Kriterien hat es, wenn das Zusammenspiel mit der Administrationslösung umständlich ist. Da die Administration im Gegensatz zu Authentifikation und Verschlüsselung an dieser Stelle lediglich Sekundärziel ist, wurde diese Kategorie nur mit mittlerer Gewichtung (++) betrachtet.

Tabelle 4-38: KO-Kriterien Administration

KO-Kriterien
Administration
keine

4.4.1.2 Die Kategorie Authentifikation

Anhand dieser Kategorie untersuchten wir die von der jeweiligen Software gebotenen Authentifikationsmöglichkeiten des Nutzers am Gerät. Insbesondere unterscheiden wir hier zwischen den Standardverfahren

- PIN
- Erweiterte PIN
- Passwort / Passphrase
- Sicheres Passwort / Passphrase

und den biometrischen Verfahren

- Thermischer Fingerabdruckscanner
- Handschrifterkennung.

PIN, Passwort und sicheres Passwort sind etablierte Zugangsverfahren, die in vielen Bereichen Verwendung finden. Eine PIN ist im Regelfall vierstellig und numerisch, ein Passwort kann aus Buchstaben und Ziffern bestehen und ein Sicheres Passwort beinhaltet gezwungenermaßen sowohl Buchstaben als auch Ziffern. Im Idealfall ist auch die Verwendung von Sonderzeichen Pflicht.

In Bezug auf Authentifikation ist es nicht nur wichtig zu betrachten, wie, sondern auch wann eine Authentifikation des Nutzers am Gerät geschieht. Selbst der beste Authentifikationsmechanismus ist wenig sinnvoll, wenn die Anmeldung nicht zumindest beim Einschalten des Gerätes erfolgen muss. Zwei Arten von Authentifikationszeitpunkten werden unterschieden:

- Gerätebezogene Authentifikationszeitpunkte (Beim Einschalten, in regelmäßigen Abständen, nach Inaktivität, Abschaltung nach Inaktivität)
- Verbindungsbezogene Authentifikationszeitpunkte (Synchronisationsvorgang, Infrarot, Bluetooth, WLAN, GSM/GPRS).

Außerdem betrachteten wir eventuell vorhandene Sicherheitsmechanismen für

- die Freischaltung des Gerätes bei verlorenem/vergessenem Passwort (durch den Nutzer, durch den Administrator)
- die Sicherung des Gerätes bei falscher Passworteingabe und gegen Brute-Force-Attacken.

Als Schutz gegen Brute-Force- und andere Attacken sind innerhalb des Testfeldes verschiedene Mechanismen verfügbar. Diese sind:

- Softlock: Das Gerät sperrt sich nach einer bestimmten Anzahl von Fehlversuchen. Der Zähler kann durch Aus- und Einschalten zurückgesetzt werden.
- Sicherer Softlock: Das Gerät sperrt sich nach einer bestimmten Anzahl von Fehlversuchen. Der Zähler kann durch Aus- und Einschalten **nicht** zurückgesetzt werden.
- Hardlock: Das Gerät sperrt sich nach einer bestimmten Anzahl von Fehlversuchen und führt einen echten Hardreset durch, wobei das Gerät auf den Auslieferungszustand zurückgesetzt und alle Daten aus dem RAM gelöscht werden.

- Wipe: Das Gerät sperrt sich nach einer bestimmten Anzahl von Fehlversuchen und löscht den gesamten Speicher des Gerätes inklusive aller installierter Anwendungen durch sicheres Löschen.
- Verzögerung: Die Wartezeit zwischen zwei möglichen Passworteingaben erhöht sich bei Falscheingaben sukzessive.
- Sperrung. Freischaltung nur mit Masterkey möglich: Das Gerät sperrt sich und akzeptiert keine Passworteingabe mehr. Die Freischaltung ist nur mittels einer SuperPIN / eines Masterpassworts möglich.

Außerdem bewerteten wir in dieser Kategorie die

- Einflussmöglichkeiten des Benutzers auf die Authentifikation
- Die Sicherheit der Authentifikation durch geringe Rückmeldungen.

Eine gute Sicherheitssoftware sollte die Deinstallation oder Deaktivierung (z. B. aus Bequemlichkeitsgründen) durch den jeweiligen Benutzer unterbinden, um jederzeit einen Schutz der auf dem Gerät befindlichen Daten zu gewährleisten. Da die Authentifikation eine zentrale sicherheitsrelevante Kategorie darstellt, wird diese Kategorie mit einer starken (+++) Gewichtung versehen.

Tabelle 4-39: KO-Kriterien Authentifikation

KO-Kriterien
Authentifikation
Keine Möglichkeit, Authentifikation beim Einschalten des Gerätes zu erzwingen
Keine Authentifikation beim Ändern der Einstellungen
Kein Schutzmechanismus gegen Brute-Force-Attacken
Beurteilung 5 oder 6 bei „Sicherheit der Authentifikation durch geringe Einflussmöglichkeiten des Benutzers“
Beurteilung 5 oder 6 bei „Sicherheit der Authentifikation durch geringe Rückmeldungen“

4.4.1.3 Die Kategorie Kosten

In der Kategorie Kosten werden auch hier die in Kapitel 4.1.5.3 verwendeten Unterkategorien gebildet:

- Einmalige Kosten (Beschaffung, zusätzliche Kosten wegen besonderer Hardwareanforderungen) und
- Laufende Kosten (zu erwartende Kosten für Updates etc., zusätzliche Kosten für längere Verbindungsdauer, zusätzliche Kosten für Support- oder Wartungsverträge)

Die Kategorie Kosten wird als schwach (+) gewichtet.

Tabelle 4-40: KO-Kriterien Kosten

KO-Kriterien
Kosten
Keine

4.4.1.4 Die Kategorie Datensicherheit

Der neben der Authentifikation zweite zentrale Aspekt bei der Beachtung der Endgerätesoftware ist die Datensicherheit und damit einhergehend die Verschlüsselung. Wie bereits in Kapitel 3.1.3.1 dargelegt, kann der Authentifikationsmechanismus einer Software relativ leicht durch Aufschrauben des Gerätes und Ausbau des geräteinternen Speichers umgangen werden. Befinden sich unverschlüsselte Daten im Speicher, so sind diese auch ohne Kenntnis des Anmeldepasswortes les- und nutzbar. Insbesondere untersuchten wir die Software daher auf Verfügbarkeit der Verschlüsselungsalgorithmen

- RC4
- Rijndael/AES
- Toofish
- Blowfish
- TEA
- XOR

sowie die angebotenen Gegenstände der Verschlüsselung

- Kompletter PDA
- PIM-Daten
- E-Mail
- Externe Speichermedien
- Manuell Ausgewählte Dateien oder Verzeichnisse
- Backup-Dateien
- E-Mail-Anhänge.

Die erwähnten Algorithmen wurden bereits im Projekt „MOB I" (MOB I, Kapitel 8.3.1) genauer betrachtet[70]. Ein Algorithmus galt dort nur dann als vorhanden, wenn die verwendete Schlüssellänge mindestens 128 Bit betrug. In Bezug auf die Gegenstände der Verschlüsselung legten wir hier besonderen Wert auf die Verschlüsselung von PIM-Daten sowie die Möglichkeit, weitere verschlüsselte Dateien auf dem PDA ablegen zu können.

Außerdem erfassten wir weitere sicherheitsrelevante Aspekte der jeweiligen Software:

- Zertifizierter kryptographischer Kern der Software
- Sicheres Löschen von Dateien möglich
- Schutz vor unbefugter Deinstallation
- Datenkompression bei Verschlüsselung
- Erstellen verschlüsselter selbstextrahierender Dateien.

Insbesondere der Zertifizierung des kryptographischen Kerns widmeten wir besondere Aufmerksamkeit, da ein Großteil der Angriffe auf Kryptographiesoftware auf dem Ausnutzen von Implementierungsfehlern wie Buffer-Overflows basiert. Ein zertifizierter Verschlüsselungskern stellt hier ein gewisses Maß an Sicherheit dar. Zertifizierungen werden beispielsweise nach dem US-Amerikanischen FIPS[71] durchgeführt. Ein kryptographischer

---

[70] Zum dort nicht erwähnten Algorithmus TEA („Tiny Encryption Algorithm") siehe auch „Related-Key Cryptanalysis of TEA" (KSW 1997, Seite 8).

[71] Siehe Fips 140-2 „Security Requirements for Cryptographic Modules" (FIPS 2001).

Kern galt für uns auch dann als zertifiziert, wenn er nicht vom Hersteller selbst, sondern von einer vertrauenswürdigen dritten Instanz wie Beispielsweise RSA Security implementiert wurde.

Da die Sicherheit ein zentraler Aspekt sowohl bei diesem Projekt als auch bei der hier betrachteten Software an sich ist, wurde diese Kategorie von uns mit einer starken (+++) Gewichtung versehen.

Tabelle 4-41: KO-Kriterien Datensicherheit

KO-Kriterien
Datensicherheit
Weder AES (128 Bit) noch vergleichbar starker Algorithmus unterstützt
Keine Möglichkeit PIM-Daten zu verschlüsseln
Keine Möglichkeit verschlüsselte Dateien abzulegen

4.4.1.5 Die Kategorie Usability

Auch die Usability der Endgerätesoftware untersuchten wir anhand der bereits in den Kapiteln 4.1.5.3 und 4.1.5.4 entwickelten Vorgehensweise. Die Unterkategorien sind:

- Sprache
- Aufgabenangemessenheit
- Selbstbeschreibungsfähigkeit
- Steuerbarkeit
- Erwartungskonformität
- Fehlerrobustheit
- Erlernbarkeit
- Programmexterne Hilfestellungen.

Die Usability wurde von uns aus arbeitswissenschaftlichen Gründen sowie im Hinblick auf eine möglichst hohe zu erreichende Akzeptanz der Sicherheitssoftware bei den Nutzern mit der Gewichtung „mittel" (++) versehen.

Tabelle 4-42: KO-Kriterien Usability

KO-Kriterien
Usability
Programm weder in deutscher noch in englischer Sprache verfügbar
Bewertung 5 oder 6 für das Kriterium „Abstürze/Systemfehler" der Kategorie „Fehlerrobustheit"
Bewertung 5 oder 6 für das Kriterium „Qualität des Supports" der Kategorie „Programmexterne Hilfestellungen"

4.4.1.6 Die Kategorie Besondere Merkmale

Wiederum erfassten wir auch weitere, besondere Merkmale und Eigenschaften der jeweiligen Software. Dies waren:

- Erfahrungen
    - Deckung der Testergebnisse mit den Prospekten
    - externe Referenzen und Erfahrungsberichte
- Erwartungen an die Zukunft
    - zu erwartende Funktionalitätserweiterungen
    - Erwartungen in die Zukunftssicherheit.

Aufgrund des lediglich ergänzenden Charakters dieser Kategorie ist auch hier die Gewichtung „schwach" (+) adäquat.

Tabelle 4-43: KO-Kriterien Besondere Merkmale

KO-Kriterien
Besondere Merkmale
Bewertung 5 oder 6 für das Kriterium „Externe Referenzen und Erfahrungsberichte"

4.4.2 Gesamtwertung und Überblick

Tabelle 4-44: Gesamtübersicht Komponentenevaluation Endgerätesoftware

Client 1[72]	-	01	02	03	04	05	06	07	08
Client 2[73]	09	-	10	11	12	13	14	15	16
	Basis H3970	Basis H5450	File Crypto	Movian Crypt	PDA Def.	PDA Sec.	Point Sec	Safe Guard	Sign On
Admin.	5	5	1	5	1	6	-	6	5
Authen.	6	6	2	6	2	6	-	2	6
Kosten	1	2	2	2	2	2	-	2	2
Security	6	6	3	3	3	6	-	6	6
Usability	4	6	4	2	6	3	-	2	4
Sonstiges	6	6	2	2	3	2	-	3	4
Gesamt	**6**	**6**	**3**	**6**	**6**	**6**	**-**	**6**	**6**
KO	**5**	**6**	**0**	**1**	**1**	**2**	**-**	**1**	**5**

Aufgrund der umfangreichen Evaluation für das gesamte Testfeld der Endgerätesoftware wird an dieser Stelle eine Zusammenfassung der anschließend ausführlich beschriebenen Ergebnisse gegeben.

[72] ClientKonfig im Evaluationsbaum in Bezug auf den neuen iPAQ H5450.
[73] ClientKonfig im Evaluationsbaum mit dem Referenzsystem (iPAQ H3970).

Insgesamt zeigt sich ein ernüchterndes Bild. Der Fingerabdruckscanner des iPAQ h5450 erwies sich als unsicher, was von einer Benutzung des neuen Gerätes dringend abraten lässt, und der Großteil der Drittanbieter für Pocket PC Sicherheitssoftware war nicht in der Lage, die bekannten Probleme von Windows CE 3.0 zu beheben. Diese ist daher für den Einsatz in einem Hochsicherheitsumfeld nicht verwendbar. Die Mehrzahl der Software erhält die schlechtest mögliche Gesamtwertung Sechs. Die wenigen Ausnahmen weisen jedoch, insbesondere in Bezug auf den „Aufschraubschutz", der in keinem Fall ausreichend war, ebenfalls Schwachpunkte auf.

Eine weitere Enttäuschung waren die Biometriemechanismen. Wie erwähnt konnte der im Vorfeld vielfach beworbene Fingerabdruckscanner des h5450 im Labor mehrmals gebrochen werden. Auch SafeGuard vom deutschen Hersteller Utimaco, das mit einem Biometriemodul zur Handschriftenerkennung ausgestattet ist, erwies sich im Labor als unsicher. Die Handschriftenerkennung von SignOn versagte zwar nicht vollends, dafür erwies sich diese Software in anderen Bereichen als untauglich.

MovianCrypt zeigte trotz guter Ansätze insgesamt doch deutliche Schwächen bei Administration und Authentifikation und überzeugte auch in der Frage der Sicherheit nicht. Insbesondere die mangelnden Administrationsmöglichkeiten sowie die Tatsache, dass die Software von einem Nutzer deinstalliert und somit außer Kraft gesetzt werden kann, hatte auch für movianCrypt eine „ungenügende" Bewertung zur Folge. Sollte die Software in folgenden Versionen um ein brauchbares Administrationsverfahren und die Einschränkung der Nutzerrechte erweitert werden, wäre sie eine Alternative zu der hier präferierten Lösung.

PDA Defense weist erstaunliche konzeptionelle Stärken auf und erfüllt nahezu alle von uns gestellten Anforderungen. Ebenso überzeugte der zugehörige Policy-Editor, mittels dessen die Administration der Software in sehr komfortabler Form möglich ist. Leider war es uns jedoch nicht möglich, die Software auch nur annähernd stabil zu benutzen. Regelmäßig auftretende Abstürze machten das Endgerät geradezu unbrauchbar. Die restlichen Evaluationsergebnisse lassen jedoch darauf schließen, dass PDA Defense für den Fall, dass diese Probleme behoben werden, durchaus dem Produktiveinsatz auch in großen Unternehmen und Verwaltungen gewachsen ist.

PDASecure Premium bietet weder Möglichkeiten zum Schutz der PIM-Daten noch verhindert die Software erfolgreich die komplette Außerkraftsetzung durch den jeweiligen Benutzer. Außerdem lässt sich PDASecure Premium nicht zentral administrieren. Für diese Zwecke bietet der Hersteller Trust Digital die Software Mobility Suite inklusive eines Policy Editors an, die jedoch aus den in Kapitel 3.1.3.3.2 genannten Gründen nicht evaluiert werden konnte. Der Hersteller schien schlichtweg nicht an einer Evaluation dieser Software durch uns interessiert zu sein.

Das bereits für PDA Defense Gesagte trifft zu großen Teilen auch für PointSec zu: Konzeptionelle Stärken und einzelne gute Ansätze sind vorhanden, im Gegensatz zu PDA Defense war es uns jedoch nicht möglich, die uns zur Verfügung gestellte Version 1.3 tatsächlich zu testen. Insbesondere die mittlerweile aktuelle Version 2.0 erscheint uns jedoch durchaus betrachtenswert. Sollte diese Version halten, was versprochen wird, wäre ihr Einsatz durchaus in Erwägung zu ziehen. Dennoch sei angemerkt, dass das zu der von uns getesteten Version gehörige Handbuch teilweise inkonsistent ist und viele Fragen offen lässt, was das Vertrauen in den Hersteller mindert.

Die Software SafeGuard PDA ist ebenso wie PDASecure nicht in der Lage, PIM-Daten zu verschlüsseln und somit für die Benutzung nicht geeignet. Viele von uns ausdrücklich geforderte Funktionalitäten, insbesondere im Bereich der Administration, werden auf der Website des Herstellers zwar beworben, bleiben jedoch einer „Enterprise-Edition" vorbehalten, deren Ankündigung seit nunmehr mindestens sechs Monaten keine Veröffentlichung folgte. Nach Ende der Evaluationsphase wurde die Version 2.0 der Software veröffentlicht, die jedoch ebenfalls nicht getestet werden konnte. Eine nachträgliche Betrach-

tung sowohl dieser als auch der Enterprise-Version ist jedoch ausdrücklich zu empfehlen, da uns insbesondere das Bedien- und Authentifikationskonzept der Software überzeugte, auch wenn es uns gelang, mittels des Authentifikationsverfahrens der Handschriftenerkennung unberechtigten Zugriff auf den PDA zu bekommen.

Sign-On stellt in diesem Testfeld eine Besonderheit dar. Die Software erhebt gar nicht erst den Anspruch, neben dem Austausch der Authentifikation andere sicherheitsrelevante Funktionen wie die Dateiverschlüsselung zu bieten und hatte daher von Anfang an keine Aussichten, im Rahmen der Evaluation als empfehlenswert erachtet zu werden. Im Gegensatz zu SafeGuard PDA gelang es uns hier jedoch nicht, das Verfahren zur Handschriftenerkennung zu brechen. Offensichtlich sind also in diesem Bereich weitaus bessere Leistungen möglich, als SafeGuard PDA sie erbringt

Der meistversprechende Kandidat des Feldes bleibt letztendlich FileCrypto. In der Frage der Administration glänzt er mit den umfangreichsten Möglichkeiten und er arbeitet auch gut mit den hier betrachteten Administrationstools zusammen. Jedoch muss FileCrypto mittels manuell zu bearbeitender Konfigurationsdateien verwaltet werden, deren Möglichkeiten allerdings außerordentlich groß sind. Die Authentifikation gehört zu den besten im Testfeld. Wirkliche Schwächen weist die Software lediglich im Bereich der Usability auf. Von den hier getesteten Lösungen zur Erhöhung der Endgerätesicherheit können wir lediglich FileCrypto tatsächlich für den Einsatz in großen und größeren Unternehmen und Verwaltungen empfehlen.

4.4.3 iPAQ H3970 Standard (ClientKonfig 09)

Um eine nachvollziehbare Bewertung des gesamten Testfeldes durchführen zu können, haben wir zuerst die ab Werk installierte Software des iPAQ H3970 anhand der gleichen Bewertungskriterien wie das restliche Evaluationsfeld getestet.

Der iPAQ h3970 läuft unter der Produktversion 2.5 und basiert auf dem Windows CE 3.0 Betriebssystem[74]. Wie im Kapitel 3.1.3 beschrieben, weist dieses Betriebssystem grundlegende Schwächen im Sicherheitskonzept auf, deren Auswirkungen hier durch eine gezielte Evaluation der integrierten Sicherheitsfeatures näher untersucht werden sollen, um insbesondere eine Referenz für die in Kapitel 3.1.3.1 ausgewählten Softwareprodukte zu erhalten.

4.4.3.1 Kategorie Administration (++)

Tabelle 4-45: iPAQ H3970 - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	5
Zusammenarbeit mit Afaria	4

Von Hause aus bietet der iPAQ H3970 in Bezug auf die Administration sicherheitsrelevanter Aspekte keinerlei Funktionalität. Im Lieferumfang ist lediglich das für die Kommunikation mit dem Companion-PC gedachte ActiveSync 3.5 enthalten, das keinerlei Möglichkeiten bereitstellt, serverseitig eine zentrale Administration zu realisieren. Der Companion PC ist der Rechner, an dem die mitgelieferte Dockingstation angeschlossen ist. Dieser Rechner geht über ActiveSync mit dem Handheld eine feste Partnerschaft ein. Ein zentrales Deployment von Updates, Keymanagement oder gar eine zentrale Schlüsselerstellung über einen Administrationsserver sind somit über die Standardausstattung nicht umsetzbar.

Durch die fehlende Benutzer- und Rechteverwaltung ist der Benutzer in der Lage, alle Einstellungen des PDAs zu ändern, also z. B. auch das Passwort zu deaktivieren. Mit Betriebssystemmitteln lassen sich die Benutzerrechte nicht einschränken. Somit sind auch Vorschriften in Form einer Policy zur Verschlüsselung oder Authentifizierung hinfällig, da es allein im Ermessen des Benutzers liegt, ob er diesen folgt.

[74] Genauer: Microsoft Windows CE 3.0.11171 (Build 11178).

Managementlösungen wie die im Rahmen dieses Projektes untersuchten Produkte XTND Connect oder Afaria wurden eigentlich für diese Grundkonfiguration des iPAQ entwickelt, wiesen jedoch in der Praxis bei den entsprechenden Eigenschaften Mängel auf. HP liefert mit dem iPAQ h3970 auf der beiliegenden Software-CD sogar den Client zum Afariaserver kostenlos mit. Ohne den entsprechenden Server, der kostenlos lediglich als eingeschränkte Testversion verfügbar ist, hat dieser Client jedoch keinen praktischen Nutzen für den Anwender.

So muss sich bei der Grundausstattung die Gesamtbewertung in dieser Kategorie auf die Möglichkeiten externer Produkte beziehen, das völlige Fehlen der zentraler Administration auszugleichen. Dies erwies sich jedoch bei der Evaluation der entsprechenden Produkte (siehe Kapitel 4.2) als „mangelhaft" hinsichtlich der hier untersuchten Kriterien.

Gesamtbewertung Administration:	**5**

4.4.3.2 Kategorie Authentifikation (+++)

Tabelle 4-46: iPAQ H3970 - Authentifikation

Kategorie Authentifikation	**Bewertung**
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Nein
Sicheres Passwort / Passphrase (ja/nein)	Ja
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	-
Bei falscher Eingabe: Softlock (ja/nein)	Nein

Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Ja
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	6
Sicherheit der Authentifikation durch geringe Rückmeldung	4

Tabelle 4-47: iPAQ H3970 – Authentifikation KO

Anzahl KO

Authentifikation

Bewertung von 5 oder 6 bei Einflussmöglichkeiten durch Benutzer

Der iPAQ h3970 verfügt in der Standardaustattung sowohl über eine vierstellige PIN, die jedoch in verwirrender Weise als „Kennwort" bezeichnet wird, als auch über ein komplexes alphanumerisches Passwort, bei dem die Benutzung von Sonderzeichen, Buchstaben und Zahlen genauso wie eine Mindestlänge von 7 Zeichen erzwungen wird.

Ein PowerOn Passwort ist auf einem Umweg möglich, indem bei der Kennworteinstellung im entsprechenden Dialogfeld das Zeitintervall für die Aktivierung der Passworteingabe auf 0 Minuten gesetzt wird. Über einen noch umständlicheren Workaround kann sogar die Abschaltung nach Inaktivität simuliert werden, indem bei eingeschaltetem PowerOn Passwort im Dialog zur Stromversorgung die entsprechenden Felder[75] auf das gewünschte Intervall gesetzt werden. Die Möglichkeiten der Authentifizierung sind vom Benutzer völlig frei beeinflussbar, können also auch deaktiviert werden, was nicht verhindert werden kann. Das völlige Fehlen von Sicherungsmechanismen verstärkt den negativen Eindruck. Lediglich ein in der Dokumentation missverständlich erklärter Verzögerungsmechanismus, der auch nicht weiter beeinflussbar ist, erzeugt in der Praxis nach 10 Falscheingaben eines Passworts eine spürbare Verzögerung, die bei jedem weiteren Versuch länger wird. Eine unendliche Anzahl an Fehlversuchen ist jedoch auch hier möglich.

Das Betriebssystem besitzt sogar ein schwerwiegendes Sicherheitsproblem. Die Erinnerungsfunktion für Termine und Aufgaben ist auch ohne gültige Anmeldung aktiv. So sind Termine und Aufgaben inklusive ihres möglicherweise vertraulichen Inhaltes vor der Authentifizierung sichtbar und somit einem Angreifer gegenüber offen einsehbar.

Zudem sind die Rückmeldungen an den Benutzer bei der Authentifikation eher negativ einzuschätzen. Kritikpunkte im Einzelnen sind hier, dass Passwörter zwar im Regelfall[76] maskiert werden, auf eine Stelle des Passwortes aber auch genau ein Maskierungszeichen fällt und ein Beobachter somit zumindest auf die Länge des verwendeten Passwortes schließen kann. Nicht reproduzierbar sprang in einigen Fällen sogar die integrierte Wortvervollständigung mit konkreten Vorschlägen an.

[75] Dialogfelder: „Bei Akkubetrieb" und „Bei externer Stromversorgung" ausschalten nach Inaktivität.

[76] Nur beim Festlegen einer neuen PIN wird diese als Klartext angezeigt.

Die Grundfunktionalität ist somit nicht ausreichend. Gerade die Möglichkeit des Benutzers, den gesamten Mechanismus beliebig zu beeinflussen[77], verhindert eine bessere Gesamtbewertung als „ungenügend".

Gesamtbewertung Authentifikation:	6

4.4.3.3 Kategorie Kosten (+)

Tabelle 4-48: iPAQ H3970 - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	1
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	1
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Bei den Kosten zeigt die Standardausstattung des iPAQ h3970 ihre Stärken. Neben den Kosten für den iPAQ h3970, der in dieser Studie das günstigere der zwei untersuchten Endgeräte ist, fallen keine weiteren Kosten für die Sicherheitskomponenten an, da sie in das Betriebssystem integriert sind. Die zusätzlichen Kosten bilden dabei ebenfalls das Minimum im Feld der Testkandidaten.

Gesamtbewertung Kosten:	1

4.4.3.4 Kategorie Datensicherheit (+++)

Tabelle 4-49: iPAQ H3970 - Datensicherheit

Kategorie Sicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Nein
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein

[77] Was auch eines der KO-Kriterien ist.

Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Nein
E-Mail (ja/nein)	Nein
Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Nein
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	(Ja)

Tabelle 4-50: iPAQ H3970 – Datensicherheit KO

Anzahl KO
Sicherheit

Kein AES oder vergleichbar starker Algorithmus

Keine Möglichkeit PIM-Daten zu verschlüsseln

Keine Möglichkeit verschlüsselte Dateien / Ordner abzulegen

Das völlige Fehlen eines Dateisystemschutzes lässt jede weitere Diskussion in dieser Kategorie überflüssig erscheinen. Der Speicher des iPAQ h3970 und mit ihm alle sensiblen Daten können so von einem Angreifer, der in den physischen Besitz des Gerätes gelangt ist, ohne großen Aufwand ausgelesen werden. Zudem greifen hier 3 der definierten KO-Kriterien, so dass diese zentrale Kategorie mit „ungenügend" bewertet werden muss. Selbst das „Ja" für den Schutz vor unbefugter Deinstallation kann hier nicht positiv bewertet werden, denn es handelt sich um einen Betriebsystembestandteil, der nicht deinstalliert werden kann. Jedoch ist jederzeit das Überschreiben mit einem anderen Sicherheitsprodukt möglich.

Gesamtbewertung Sicherheit:	6

4.4.3.5 Kategorie Usability (++)

Tabelle 4-51: iPAQ H3970 – Usability 1

Kategorie Usability	Bewertung
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Ja
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Ja
Aufgabenangemessenheit	

Software ist zielgerichtet ohne überflüssige Arbeitsschritte	4
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	1
Alle benötigten Informationen sind auf dem Bildschirm zu finden	3
Ausgaben sind zweckmäßig und verständlich	2
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	1
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	5
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	2
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	2
Auswirkungen von Aktionen hinreichend ersichtlich	2
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	1
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	4
Aktueller Bearbeitungsschritt kann unterbrochen werden	4
Ein laufender Vorgang kann abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	3
Bearbeitungszeit abschätzbar	2
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwarteten Ergebnis	2
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen unmöglich	2
Bei Fehlern zweckmäßige Hinweise zu Ursache und Behebung	1
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	2
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	2
Nur wenige Detailkenntnisse zur Bedienung nötig	1
Hilfestellung bei Bedarf verfügbar	5

Tabelle 4-52: iPAQ H3970 – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	4
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Ja
Qualität des Administrationshandbuches	-
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	-
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	-
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	-
Qualität des Supports (soweit bewertbar)	2

Bei der Usability gibt es einige ungewöhnliche Probleme. Wünscht der User einen Softlock, muss er an völlig verschiedenen Stellen und Masken Einstellungen vornehmen, die erst im Zusammenspiel den Softlock bzw. das Ausschalten nach Inaktivität „simulieren". Der Begriff „Kennwort" wird zum einen benutzt, um die im üblichen Sprachgebrauch als „PIN" bezeichnete 4-stellige Zahlenkombination zur Authentifizierung zu bezeichnen, zum anderen jedoch wird von einem „starken Kennwort" gesprochen, wenn ein alphanumerisches Passwort zur Authentifikation gemeint ist, das aus mindestens 7 Zeichen gemischt aus Zahlen, Sonderzeichen und Buchstaben in Groß-/Kleinschreibung bestehen muss. Dies erfährt der Benutzer jedoch erst, wenn er versucht, ein den Anforderungen ungenügendes Passwort als neues Passwort festzulegen. Ein Hilfebutton fehlt ebenso wie ein Abbruchbutton. Der Verzögerungsmechanismus bei der Authentifikation ist zudem an keiner Stelle dokumentiert. Er wird nicht wie bei anderen Produkten z. B. durch einen immer langsamer laufenden Statusbalken für die Wartezeit zwischen zwei Versuchen optisch veranschaulicht, was die Abschätzung der verbleibenden Zeit ermöglichen und den Eindruck vermeiden würde, das Gerät sei abgestürzt.

Einige, eigentlich inzwischen veraltete Rückmeldungen wie z. B. der Fehler einer falschen Passwortzusammensetzung tauchten erneut auf, nachdem das Gerät reaktiviert wurde, solange im Hintergrund der Bildschirm für die Kennworteinstellungen offen bleibt. Systemabstürze traten im Laborbetrieb in nicht regelmäßigen Abständen mehrmals auf. Massive Schwierigkeiten bereitete die Inbetriebnahme des GSM/GPRS Wireless expansion pack. Ein Aufstecken auf den iPAQ in seiner Standardausstattung ließ das komplette System zusammenbrechen. Nur ein echter Hardwarereset (dann wieder ohne GSM/GPRS Modul) konnte dem abhelfen. Hier war ein sehr umständlich durchzuführendes Firmwareupdate sowohl des iPAQ als auch des Expansion Pack notwendig. Die mitgelieferte Dokumentation in Papierform ist auf den unerfahrenen Benutzer zugeschnitten, der Step-by-Step Anleitungen benötigt. Detailinformationen zur Bedienung finden sich hier ebensowenig wie eine genaue Dokumentation der jeweiligen Sicherheitsfeatures. Leider ist in dieser Beziehung die Dokumentation auf der ebenfalls mitgelieferten CD ähnlich zurückhaltend und sie kann daher nur mit schlechten Noten bewertet werden. Sehr gut hingegen ist die Homepage des Herstellers[78], die mit vielen weiteren nützlichen Informationen aufwartet. Bei den Telefonaten mit dem Support wurde dieser gute Eindruck noch verstärkt. Aufgrund der genannten Inkonsistenten lautet die Bewertung dennoch „genügend".

Gesamtbewertung Usability:	**4**

4.4.3.6 Kategorie Besondere Merkmale (+)

[78] http://www.hp.com/country/us/eng/prodserv/handheld.html [26.03.2003]

Tabelle 4-53: iPAQ H3970 – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	1
Externe Referenzen/Erfahrungsberichte	6
Zukünftig zu erwartende Funktionalitätserweiterungen	2
Erwartungen Zukunftssicherheit	2

Tabelle 4-54: iPAQ H3970 – Besondere Merkmale KO

Anzahl KO
Besondere Merkmale
Bewertung von 5 oder schlechter bei externen Referenzen

Mit dem iPAQ erhält der Homeuser ein einfach zu bedienendes System, das seinen Ansprüchen auch im Bereich der Sicherheit durchaus genügt. Leider erfüllt er jedoch in keinster Weise weitergehende Ansprüche und so urteilt auch die Fachpresse skeptisch[79] über die Sicherheit des Pocket PC 2002 Betriebssystems auf dem iPAQ h3970. Selbst Microsoft weist auf Lücken im Bereich der Sicherheit hin[80].

Microsoft arbeitet intensiv an neuen Versionen des Systems. So wird Pocket PC 2003 mit dem Codenamen „Ozone" bereits auf dem Windows CE .NET 4.1 Kern aufbauen[81]. Die iPAQ Produktreihe von HP zählt zu den erfolgreichsten in der PocketPC Klasse, vor zwei Jahren waren über zwei Millionen Handhelds verkauft[82]. Ein Ende der Entwicklung ist nicht zu erwarten und so wird der iPAQ mit PocketPC in Zukunft vermutlich einen steigenden Marktanteil erobern. Daher besteht auch die berechtigte Hoffnung, dass zumindest ein Teil der Mängel im Sicherheitsbereich im Laufe der Zeit behoben werden.

Gesamtbewertung Besondere Merkmale:	6

[79] z. B.: „Pocket PC 2002 Security" (Herrera 2002).
[80] Vergleiche dazu insbesondere Douglas Dedo: „Pocket PC-Sicherheit" (Dedo 2002).
[81] Mehr dazu in http://www.heise.de/newsticker/data/jk-01.04.03-001/ [15.04.2003].
[82] siehe: http://www.golem.de/0204/19445.html [15.04.2003].

4.4.3.7 Gesamtbewertung

Tabelle 4-55: iPAQ H3970 – Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	5
+++	Kategorie Authentifikation	1	6
+	Kategorie Kosten	-	1
+++	Kategorie Sicherheit	3	6
++	Kategorie Usability	-	4
+	Kategorie Besondere Merkmale	1	6
	KO-Kriterien gesamt	**5**	

Der Standard iPAQ versagt gleich in mehreren Kategorien. Ohne Zusatzsoftware oder grundlegende Änderungen bleibt der iPAQ h3970 ungeeignet für den Einsatz. So zeigt er gravierende Schwächen gerade im Bereich der untersuchten Authentifikation und Datensicherheit. Im Bereich der administrativen Möglichkeiten arbeitet das System zwar prinzipiell mit den ausgewählten Managmentprodukten (siehe auch Kapitel 4.2) zusammen, es zeigt jedoch auch dort Mängel. Als Gesamtbewertung kann deshalb nur ein „ungenügend" vergeben werden.

Gesamtbewertung iPAQ h3970:	6

4.4.4 iPAQ H5450 Standard (ClientKonfig 01)

Das zweite Basisgerät im Testfeld ist der iPAQ h5450. Untersucht wurde die von HP vor offiziellem Verkaufsstart im Rahmen des Projektes erhaltene Testversion, die jedoch laut Angaben von HP der späteren Verkaufsversion entspricht. Der iPAQ h5450 basiert auf demselben Betriebssystem wie der h3970[83], läuft jedoch unter der Produktversion 3.0

Damit unterliegt er weitestgehend den gleichen Problemen und Beschränkungen wie der h3970. Es wird hier deshalb verstärkt auf die Unterschiede zwischen den beiden Geräten eingegangen.

4.4.4.1 Kategorie Administration (++)

Tabelle 4-56: iPAQ H5450 - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	5
Zusammenarbeit mit Afaria	5

Die Unterschiede zum iPAQ h3970 im Bereich der Administration sind minimal. Der h5450 führt jedoch u. a. einen neuen Authentifikationsmechanismus ein. Die Zusammenarbeit mit den Administrationslösungen wie Afaria und XTND sollte deshalb – insbesondere aufgrund der gerade erst erfolgten Markteinführung des Gerätes – einer gewissen Vorsicht unterliegen. Speziell die Konfiguration des neuen thermischen Fingerabdruckscanners und generelle Veränderungen im System führen hier derzeit noch zu Inkompatibilitäten, die eine Abstufung um eine Note auch bei Afaria nach sich ziehen. Es bleibt zu klären, inwiefern dies in kommenden Versionen der Administrationslösungen verbessert wird.

Gesamtbewertung Administration:	5

[83] Microsoft Windows CE 3.0.11171 (Build 11178).

4.4.4.2 Kategorie Authentifikation (+++)

Tabelle 4-57: iPAQ H5450 - Authentifikation

Kategorie Authentifikation	Bewertung
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Nein
Sicheres Passwort / Passphrase (ja/nein)	Ja
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	5
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	-
Bei falscher Eingabe: Softlock (ja/nein)	Ja
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Nein
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	6
Sicherheit der Authentifikation durch geringe Rückmeldung	4

Tabelle 4-58: iPAQ H5450 – Authentifikation KO

Anzahl KO
Authentifikation
Bewertung von 5 oder 6 bei Einflussmöglichkeiten durch Benutzer

Der Authentifikationsmechanismus wurde im Bereich Sicherheit weitgehenden Änderungen unterzogen. Sowohl Passwort als auch PIN[84] werden nach wie vor verwendet. Neu hinzugekommen ist die Möglichkeit, einen thermischen Fingerabdruckscanner[85] zur Benutzeranmeldung zu wählen. Zum ersten Mal sind zudem logische Verknüpfungen der verschiedenen Methoden möglich. Im Einzelnen sind die ODER Verknüpfungen „PIN oder Fingerabdruck", „Passwort oder Fingerabdruck" und die UND Verknüpfungen „PIN und Fingerabdruck", „Passwort und Fingerabdruck" auswählbar. Daneben kann jede Methode einzeln angewählt werden. Gerade die UND-Verknüpfung, in der zwei Authentifizierungshürden vom Nutzer genommen werden müssen, erhöht die Sicherheit in erfreulichem Maße. Ein Angreifer müsste auf diese Art z. B. den Fingerabdruck fälschen können und die PIN bzw. das Passwort kennen.

Der Fingerabdruckscanner

Der thermische Fingerabdruckscanner gilt zumindest in der Theorie als sicherer im Vergleich zu den optischen Modellen, da er nicht nur zwischen hell/dunkel, sondern auch zwischen warm/kalt unterscheidet[86]. Ein abgeschnittener Finger z. B. ist nicht nutzbar. Die Methode des Anhauchens wird ebenfalls verhindert, denn es handelt sich nicht um ein Scanfeld, auf das der Finger gelegt wird, sondern über einen dünnen Scanstreifen, über den der Finger gezogen werden muss. Die Sicherheit der Authentifikation hängt somit in großem Maße von der Sicherheit des Scanners ab, davon abgesehen unterscheidet sich der iPAQ in seinen Methoden kaum vom iPAQ h3970.

Der Fingerabdruckscanner bedarf einer gewissen Gewöhnung, bis man gute Muster mit dem dünnen Scanstreifen erzielt. Empfohlen wird die Benutzung des Zeigefingers. In der Praxis erwies sich jedoch der Daumen zumindest beim Training als einfacher zu verwenden.

Zu Beginn wurde der Scanner einer unsystematischen Untersuchung unterzogen. Dabei gelang es, mehrere Muster zweier unterschiedlicher Personen in einem kleinen Personenkreis zu brechen. Anfangs erfolgten die Tests mit niedriger Sicherheitsstufe. Selbst ein Umstellen auf die höchste Stufe und mehrmaliges Anfertigen neuer Muster brachten keine sichtbare Verbesserung. Nach anfänglichen sechs Brechungen durch mehrere unterschiedliche Personen stellte sich eine scheinbar sichere Phase ein, in der neue Muster nicht mehr gebrochen werden konnten. Ein längerer Test mit zufällig ausgewählten Testpersonen (z. B. in einem Zug unter grellem Kunstlicht) erreichte später, diesmal sowohl bei Mustern von Daumen als auch beiden Zeigefingern derselben Person, weitere fünf Brechungen.

Diese katastrophalen Ergebnisse ließen einen systematischen Test angeraten sein. Dazu wurde der iPAQ unter den drei Variablen Licht, Temperatur, Finger mit unterschiedlichen Mustern in der höchsten Sicherheitsstufe untersucht. Die Muster wurden von der Person geliefert, die im Vorfeld die meisten gelungenen Brechungen verzeichnen musste. In den insgesamt sieben Testdatensätzen von Personen sowohl aus dem Projekt als auch von projektfremden Personen gelang es jedoch nur noch in einem Fall, den Fingerabdruckscanner zu täuschen. Es konnte leider keine Ursache für die Unzuverlässlichkeit des

[84] Die nun endlich auch tatsächlich als „PIN" bezeichnet wird.
[85] Die Software dazu stammt ist von Cogent Systems und lautet „BioSwipe" (iPAQ Version 3.2) http://www.cogentsystems.com [05.04.2003].
[86] Siehe dazu „Biometrische Zugangskontrollen auf die Probe gestellt" (Ziegler 2002).

Scanners ermittelt werden. Ein Defekt des Gerätes scheint unwahrscheinlich, denn die Tests wurden über die beiden verfügbaren Endgeräte vom Typ H5450 verteilt, genauso wie verschiedene Muster von mehreren Personen zum Einsatz kamen und der systematische Test zudem ausschließlich unter der höchsten Scanstufe durchgeführt wurde. Bei grellem Kunstlicht schien der Scanstreifen selbst bei dem richtigen Finger Schwierigkeiten zu haben, das Muster korrekt zu scannen. So hatte selbst der autorisierte Benutzer massive Schwierigkeiten, Zugang zum Gerät zu erhalten.

Die schlechten Ergebnisse machen den Scanner selbst für den Normalbetrieb völlig unbrauchbar, was die gesamte Authentifikation des H5450 in Frage stellt.

Weitere Analyse der Authentifikation

Die Abschaltung nach Inaktivität funktioniert genauso umständlich wie das PowerON Passwort nach wie vor durch Einstellen eines Intervalls von 0 Minuten. Das Anspringen der Wortvervollständigung wurde beim iPAQ h5450 nicht beobachtet. Das Passwordmasking wird jedoch genauso gehandhabt. Der Zugriff auf Termine und Aufgaben vor der eigentlichen Authentifikation besteht ebenfalls unverändert. Die Möglichkeiten der Benutzerauthentifizierung sind vom Benutzer wieder frei beeinflussbar, können also nach wie vor auch deaktiviert werden.

Die beim iPAQ noch vorhandene und unklar dokumentierte Verzögerung bei Falscheingaben ist weggefallen. Der iPAQ h5450 verlangt das Einstellen einer maximalen Anzahl von Anmeldeversuchen. Nach dieser Anzahl von Versuchen erscheint ein Fenster mit einem Hinweis und den Optionen „Vollständiger Reset" und „Fortfahren". Ein Klick auf „Fortfahren" gibt dem Benutzer wieder die eingestellte Anzahl Versuche, was den Mechanismus ad absurdum führt. Immerhin lässt sich der Zähler über die Fehlversuche weder durch Ausschalten noch durch einen Softreset löschen. Ein Klick auf „Vollständiger Reset" führt zu mehreren neuen Hinweisfenstern, deren letztes die Aufforderung an den Benutzer enthält, den Hardwarereset selbst durchzuführen und zu näheren Erläuterungen im Benutzerhandbuch nachzulesen. Die Wertung lautet deshalb wieder „ungenügend". Tendenziell erscheint das Ergebnis jedoch sogar noch gefährlicher als beim iPAQ h3970, suggeriert doch der Fingerabdruckscanner bei einem durchschnittlichen Benutzer erhöhte Sicherheit, was zu sorglosem Umgang mit wichtigen Daten führen kann.

Gesamtbewertung Authentifikation:	**6**

4.4.4.3 Kategorie Kosten (+)

Tabelle 4-59: iPAQ H5450 - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	1
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	3
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	1
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Die Anschaffungskosten für die Sicherheitssoftware des iPAQ h5450 sind wie beim iPAQ h3970 bereits mit dem Kaufpreis des Handhelds abgeglichen. Die Biometriesoftware basiert jedoch auf dem thermischen Fingerabdruckscanner, der im Vergleich zum h3970 zu einem Aufpreis von rund 100-150 Euro[87] führt. Daher erreicht der iPAQ h5450 hier insgesamt nur eine Gesamtbewertung von „gut".

Gesamtbewertung Kosten:	2

4.4.4.4 Kategorie Datensicherheit (+++)

Tabelle 4-60: iPAQ H5450 - Datensicherheit

Kategorie Sicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Nein
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Nein
E-Mail (ja/nein)	Nein
Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Nein
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	(Ja)

Tabelle 4-61: iPAQ H5450 – Datensicherheit KO

Anzahl KO
Sicherheit
Kein AES oder vergleichbar starker Algorithmus
Keine Möglichkeit PIM-Daten zu verschlüsseln
Keine Möglichkeit verschlüsselte Dateien / Ordner abzulegen

[87] Stand März 2003

Keinerlei Verbesserungen gab es auf dem Gebiet der Verschlüsselung und Sicherheit. Der iPAQ h5450 versagt hier ebenso wie der iPAQ h3970. Ohne zusätzliche Verschlüsselungssoftware, die auch eine sichere und transparente Echtzeitverschlüsselung des Filessystems realisiert, kann keiner der iPAQs in seiner Basisausstattung empfohlen werden.

Gesamtbewertung Sicherheit:	**6**

4.4.4.5 Kategorie Usability (++)

Tabelle 4-62: iPAQ H5450 – Usability 1

Kategorie Usability	**Bewertung**
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Ja
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Ja
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	5
Daten können wie von der Aufgabe gefordert eingegeben werden	2
Informationen und Bedienelemente befinden sich am richtigen Platz	1
Alle benötigten Informationen sind auf dem Bildschirm zu finden	3
Ausgaben sind zweckmäßig und verständlich	1
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	1
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	5
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	2
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	1
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	5
Aktueller Bearbeitungsschritt kann unterbrochen werden	4
Ein laufender Vorgang kann abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	4
Bearbeitungszeit abschätzbar	1
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwarteten Ergebnis	1

Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen unmöglich	2
Bei Fehlern zweckmäßige Hinweise zur Ursache und Behebung	1
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	5
Erlernbarkeit	
Schnelles Erlernen der Bedienung	3
Intuitive, selbsterklärende Benutzung möglich	3
Nur wenige Detailkenntnisse zur Bedienung nötig	1
Hilfestellung bei Bedarf verfügbar	5

Tabelle 4-63: iPAQ H5450 – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	3
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Ja
Qualität des Administrationshandbuches	-
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	-
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	-
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	-
Qualität des Supports (soweit bewertbar)	2

Tabelle 4-64: iPAQ H5450 – Usability KO

Anzahl KO
usabilità

Bewertung von 5 oder schlechter bei Auftreten von Abstürzen und Systemfehler

Die Abschaltung nach Inaktivität muss genauso umständlich wie beim iPAQ h3970 vorgenommen werden. Weitere bereits vom kleineren Modell bekannte Ungereimtheiten wie beispielsweise das Fehlen von Abbruchmöglichkeiten existieren ebenfalls noch. Dafür wird die PIN endlich auch als solche und nicht mehr mit dem irritierenden Begriff „Passwort" bezeichnet und es fällt auch in vielen anderen Details auf, das die gesamte Bedienung aufmerksam überarbeitet wurde.

Leider macht die Software für den Fingerabdruckscanner[88] den guten Eindruck wieder zunichte. Eine zusätzliche PIN-Eingabe wird erzwungen, wenn man eigentlich nur den Fingerabdruck ändern will. Die Software stürzte im Testbetrieb häufig ab und blieb kommentarlos hängen. Selbst ein Ein- und Ausschalten änderte nichts an dem Zustand. Nur

[88] „Bioswipe" (iPAQ v3.2) von Cogent Systems, siehe http://www.cogentsystems.com [07.04.2003]

ein Softreset konnte das System wieder reaktivieren. Auch die Dokumentation der 3 verfügbaren Sicherheitsstufen für die Scansoftware[89] lässt zu wünschen übrig. Es ist unklar, inwiefern die Sicherheitsstufen Auswirkungen auf die Genauigkeit des Scannens haben. Im Testbetrieb ließ sich kein Unterschied feststellen. Zudem ist der iPAQ h5450 spürbar langsamer und zäher in der Reaktionszeit. Das Arbeiten mit verschiedenen Dialogfenstern ist so noch anstrengender als beim iPAQ h3970. Die Qualität des Bildschirmes hat ebenfalls deutlich abgenommen. Dies ist jedoch möglicherweise auf das Testmodell zurückzuführen, da die vorliegende Version exklusiv von HP vor Markteinführung zur Verfügung gestellt wurde. Als Bewertung kann somit nur ein „ungenügend" vergeben werden.

Gesamtbewertung Usability:	6

4.4.4.6 Kategorie Besondere Merkmale (+)

Tabelle 4-65: iPAQ H5450 – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	5
Externe Referenzen/Erfahrungsberichte	5
Zukünftig zu erwartende Funktionalitätserweiterungen	2
Erwartungen Zukunftssicherheit	2

Tabelle 4-66: iPAQ H5450 – Besondere Merkmale KO

Anzahl KO
Besondere Merkmale
Bewertung von 5 oder schlechter bei externen Referenzen

Noch existieren keinerlei Erfahrungsberichte oder Testergebnisse unabhängiger Quelle zum neuen iPAQ h5450. Praktische Erfahrungen zum Fingerabdruckscanner außerhalb unseres Labors sind somit auch Mangelware. In Newsgroups tauchen jedoch in jüngster Zeit verstärkt Meldungen über Probleme mit dem Fingerabdruck auf. Die im Labor aufgetretene Unzuverlässlichkeit scheint also kein Einzelfall zu sein. Die in den Prospekten durch den Scanner als besonders hoch angegebene Sicherheit existiert in der Praxis nicht. Der Fingerabdruckscanner suggeriert eine besonders hohe Sicherheit, die er nicht bietet und verleitet dazu, besonders sensible Daten auf dem iPAQ zu speichern und fördert weiterhin eine gewisse Sorglosigkeit im Umgang mit dem Gerät.

Der iPAQ h5450 stellt eine direkte Fortentwicklung des ebenfalls hier getesteten iPAQ h3970 dar. Fehler in der Scansoftware für den Fingerabdruckscanner werden hoffentlich im Laufe der Zeit behoben werden. Sonstige Sicherheitslücken gehen wie beim iPAQ h3970 hauptsächlich auf den Windows CE 3.0 Kern des Betriebssystems zurück. Im momentanen Stadium bleibt somit nur ein „ungenügend" als Bewertung in dieser Kategorie.

Gesamtbewertung Besondere Merkmale:	6

4.4.4.7 Gesamtbewertung

[89] Gut verstecktes Feld „Optionen" mit den Einstellungen der Sicherheitsstufen „normal", „hoch", „sehr hoch".

Tabelle 4-67: iPAQ H5450 - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	5
+++	Kategorie Authentifikation	1	6
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	3	6
++	Kategorie Usability	1	6
+	Kategorie Besondere Merkmale	1	6
	KO-Kriterien gesamt	**6**	

In vielen Bereichen ist der iPAQ h5450 dem iPAQ h3970 ähnlich. Er verursacht geringfügig höhere Kosten und versagt genauso wie der h3970 völlig in der Kategorie Sicherheit. Trotz in Ansätzen besserer Usability, senkt der Fingerabdruckscanner die Wertung deutlich. Er erweist sich als grundlegende Schwäche des Gerätes.

Im Labor konnte der Fingerabdruckscanner in insgesamt 12 Fällen gebrochen werden, selbst unter der höchsten Sicherheitsstufe. Daher ist von einem Einsatz des Scanners, der eine höhere Sicherheit suggeriert, dringend abzuraten. Lässt man den Fingerabdruckscanner jedoch in der Kategorie Authentifikation weg, hat man von der Sicherheit her einen dem kleineren iPAQ h3970 vergleichbaren Mechanismus. Man muss jedoch sicherstellen, dass der Scanner von den Nutzern tatsächlich nicht wieder reaktiviert werden kann.

Insgesamt ist das Versagen in den Kernkategorien Authentifikation und Sicherheit genauso wie beim iPAQ h3970 ausschlaggebend für die Gesamtwertung. Ohne zusätzliche Software, die die massiven Probleme an diesen Stellen behebt, ist ein Einsatz des iPAQ h5450 in höchstem Maße gefährlich, insbesondere in einem Hochsicherheitsumfeld. Der iPAQ h5450 versagt sogar bei sechs KO-Kriterien, was die höchste Anzahl im gesamten Testfeld darstellt.

Gesamtbewertung iPAQ h5450:	6

4.4.5 **FileCrypto** (ClientKonfig 02 + 10)

FileCrypto stammt vom Hersteller F-Secure. Dieser Hersteller liefert auch die für dieses Projekt eingesetzte Endgeräteantivirenlösung und hat in seiner Produktpalette auch die Verschlüsselungssoftware FileCrypto für Windows CE 3.0 Systeme. Im Rahmen dieser Evaluation wurde die Enterpriseversion von FileCrypto mit der laufenden Versionsnummer 2.01 (Build 9) getestet.

Die Stärke des Produktes liegt laut Prospekten in der transparenten Echtzeitverschlüsssselung des Filesystems über den AES Algorithmus. Daneben bietet FileCrypto aber auch einen Authentifikationsmechanismus. Eine überschneidende Installation mit anderen Sicherheitslösungen ist daher unmöglich und der Hersteller rät auch davon ab.

Auf dem iPAQ h5450 konnte FileCrypto nicht zum Funktionieren gebracht werden. Hier hat das Programm insbesondere massive Probleme den Authentifikationsmechanismus richtig zu überschreiben. Die folgende Evaluation bezieht sich daher vollständig auf den iPAQ h3970. Es ist zu erwarten, das nach Markteinführung des h5450 eine neue Version von FileCrypto diese Probleme behebt.

4.4.5.1 **Kategorie Administration** (++)

Tabelle 4-68: FileCrypto - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Ja
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Ja
Vorschriften für PIN/Passwort (ja/nein)	Ja
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Ja
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Ja[90]
Zentrale Schlüsselerstellung (ja/nein)	Ja[91]
Profilverwaltung (ja/nein)	Nein[92]
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	2
Zusammenarbeit mit Afaria	2

Es gibt zwei Zusatztools[93] für Handhelds von F-Secure („Key Manager" und „Handheld Manager"), die Administrationsaufgaben übernehmen. Der Handheld Manager dient der Verteilung aktueller Virussignaturen für die Antiviruslösung auf den Handhelds. Der Key

[90] Nur über erhältliches Zusatzprogramm „Key Manager" von F-Secure.
[91] Nur über erhältliches Zusatzprogramm „Key Manager" von F-Secure.
[92] Könnte aber über die Verwaltung der INI-Files für Benutzergruppen simuliert werden.
[93] Siehe dazu: http://www.f-secure.com/wireless/management.shtml [07.04.2003].

Manager wiederum ist auf die hier betrachtete Sicherheitslösung FileCrypto abgestimmt. Er erzeugt ein Installationspackage und zugehörige Schlüssel und Passwörter. Diese Packages sind explizit dafür gedacht, über Admistrationslösungen wie XTND und Afaria verteilt zu werden. Die beiden Tools konnten leider im Rahmen des Testes nicht evaluiert werden.

Der Mechanismus dahinter wurde jedoch überprüft und erscheint sehr vielversprechend. Ohne Key Manager muss der Nutzer per Hand einen Schlüssel auf dem Handheld erzeugen. Selbst dort kann er jedoch über ein INI File eine „Prekonfiguration" vornehmen und diese inklusive der CAB Datei für die Installation von einer externen Administrationslösung auf den iPAQ schieben lassen. Diese Möglichkeit wird von FileCrypto explizit vorgesehen und dient der zentralen Administration. Das INI-File[94] kann in jedem beliebigen Texteditor verändert werden.

Produkteigene Administrationslösungen, die darüber hinausgehen, bietet FileCrypto nicht. Der Weg über den Texteditor erscheint zwar recht umständlich[95], bietet aber vielfältige Möglichkeiten und arbeitet gut mit den vorhandenen Administrationslösungen zusammen. Die Rechte des Benutzers können hierbei gezielt eingeschränkt werden.

Eine Profilverwaltung wäre über eine gruppen- bzw. benutzerspezifische Verwaltung der INI-Dateien realisierbar. Die Installationspakete und Updates können problemlos über Afaria oder XTND verteilt werden. Insgesamt verdient dieses Konzept deshalb ein „sehr gut", auch wenn die Usability nicht optimal ist.

Gesamtbewertung Administration:	**1**

4.4.5.2 Kategorie Authentifikation (+++)

Tabelle 4-69: FileCrypto - Authentifikation

Kategorie Authentifikation	**Bewertung**
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Ja
Sicheres Passwort / Passphrase (ja/nein)	Ja
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein

[94] Eigentlich 2 INI-Files: „prodset.ini" für die Installation auf dem Handheld und „settings.ini" für die Sicherheitspolicy.

[95] Es ist nicht bekannt inwieweit der „Key Manager" von F-Secure auch als Oberfläche für die Erzeugung der INI-Files dient.

Abschaltung nach Inaktivität (ja/nein)	Ja[96]
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	2[97]
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	2[98]
Bei falscher Eingabe: Softlock (ja/nein)	Nein
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Ja
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Nein
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Ja
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	2
Sicherheit der Authentifikation durch geringe Rückmeldung	2

FileCrypto kennt verschiedene Sicherheitsebenen mit unterschiedlichen Arten der Authentifikation. Im einfachsten Modus, dem Sperrmodus, genügt eine 4-stellige PIN[99] zur Entriegelung des Gerätes. Im Sperrmodus ist die transparente Ver- und Entschlüsselung des Filesystems weiterhin aktiv. Das Filesystem liegt also unverschlüsselt im Speicher. Diese Phase wird genutzt, um schnelles Reaktivieren nach einer kurzen Phase des Nichtbenutzens zu ermöglichen, denn das Verschlüsseln bzw. Entschlüsseln des Filesystems und das dazu notwendige Laden des FileCrypto Treibers benötigt eine gewisse Zeit. Im verschlüsselten Zustand, also bei entladenem FileCrypto Treiber und verschlüsseltem Dateisystem, kommt die nächsthöhere Stufe zur Reaktivierung zum Einsatz. Dazu dient eine Passphrase. Je nach eingestellter Policy kann die Passphrase ein normales Passwort aus mind. 8 einfachen Buchstaben sein oder eine max. 40-stellige Phrase bestehend aus Sonderzeichen, Zahlen und Groß-/Kleinschreibung[100]. Sollte der Benutzer sowohl die PIN

[96] Wie bei den Konkurrenten nur über den Weg zu den Energieoptionen, hier aber mit einem im FileCrypto eingebetteten direkten und dokumentierten Knopf.

[97] Dazu dient der Masterkey in nicht zentral administrierten Umgebungen. Dieser ist vergleichbar mit einem „sicheren Passwort".

[98] Dazu dient der in zentral administrierten Umgebungen vom Administrator mittels „Key Manager" erstellte Masterkey. Dieser ist mit einem „sicheren Passwort" vergleichbar.

[99] Bestehend aus normalen Zahlen, kann die PIN jedoch auf bis zu 8 Zeichen verlängert werden oder völlig deaktiviert werden.

[100] Die genauen Vorschriften für die Zusammensetzung der Passphrase und die Länge sind wieder über die INI-Files einstellbar bzw. erzwingbar.

als auch die Passphrase vergessen haben, greift die 3. Stufe der Authentifikation. Bei Installation wird ein 32-stelliger Schlüssel erzeugt, bestehend aus 8 4er-Gruppen gemischt aus Buchstaben und Zahlen. In einem zentral administrierten Umfeld kann vom Administrator für den User nicht einsehbar vor Installation dieser Schlüssel mittels Keymanager erzeugt werden. Andernfalls erzeugt man den Schlüssel als User selbst bei der Installation der FileCrypto Software auf dem Handheld. Dieser Masterkey dient dann dem Freischalten des verschlüsselten Gerätes, sollte das Passwort verloren gegangen sein[101]. Als weitere Authentifikationsmöglichkeit kann schließlich der Administrator für den Benutzer nicht einsehbar in einem zentral administrierten Umfeld eine Passphrase[102] für die Deinstallation festlegen.

Gerade im Zusammenspiel mit der Administration zeigt sich die ganze Stärke der Authentifikation von FileCrypto. Der bei der Basiskonfiguration umständlich über die Stromversorgung eingestellte automatische Logout nach Inaktivität muss bei FileCrypto zwar immer noch über diesen Umweg erstellt werden, aber direkt im FileCrypto Dialog existiert ein direkter Link in die korrekte Untermaske der Stromversorgung. Insgesamt bietet FileCrypto hier die Grundanforderungen eines PowerOn Passwortes und einer Abschaltung nach Inaktivität. Weitergehende Ansprüche werden nicht unterstützt.

Beim Passwortmasking liefert FileCrypto wie der Großteil des Testfeldes den üblichen Standard: Eine Passwortstelle wird mit einem Zeichen maskiert. Ausfälle, wie das Anspringen der Wortvervollständigung, waren nicht zu beobachten. Die Einschränkungen der Möglichkeiten des Benutzers sind bei normaler Installation genauso schlecht wie bei der Basiskonfiguration. Der Benutzer könnte die Authenfikation sogar vollständig deaktivieren oder FileCrypto deinstallieren. Betrachtet man aber den programminternen Mechanismus der INI-Files, kann der Administrator die Rechte bis auf ein absolutes Minimum reduzieren. Sogar die Zusammensetzung der Passwörter kann vorgeschrieben werden. Da dies eine von F-Secure fest vorgesehene und dokumentierte Möglichkeit ist, wird von einem gut vorkonfigurierten INI-File ausgegangen und eine gute Note vergeben.

Das bereits beschriebene Problem von Windows CE mit der Erinnerungsfunktion von Terminen und Aufgaben kennt F-Secure und im Handbuch wird explizit darauf hingewiesen. Völlig verhindern kann FileCrypto dies nicht, jedoch ist bei aktivierter Verschlüsselung der PIN-Daten immerhin nur noch der Titel der Aufgabe oder des Termins einsehbar. F-Secure empfiehlt hier, über eine Sicherheitspolicy den Mitarbeitern zu verbieten, in Terminen zu schützende Angaben zu machen.

Eine sehr gute Bewertung verhindert vor allem der immer noch vorhandene Terminbug. Auch die vorhandenen Sicherheitsmechanismen könnten in Details besser ausfallen. Neben dem Sperren des Gerätes mit einem Masterkey wären insbesondere Mechanismen wie ein Hardlock oder gar ein Wipe wünschenswert. Somit lautet die Bewertung „gut".

Gesamtbewertung Authentifikation:	**2**

[101] Im nicht zentral verwalteten Umfeld kennt der User selbst den Masterkey und kann sein Gerät selber freischalten. Andernfalls muss der Administrator Zugang zum Handheld bekommen, um mit dem nur ihm bekannten Masterkey das Gerät zu entsperren.

[102] Wieder bestehend aus 6-40 Zeichen.

4.4.5.3 Kategorie Kosten (+)

Tabelle 4-70: FileCrypto - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	3
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Die Anschaffungskosten für FileCrypto sind gering. Eine Lizenz der FileCrypto Enterprise Edition kostet 76,20 EUR. Da es sich bei dem für FileCrypto erhältlichen Key Manager um eine in zentral administrierten Umgebungen unabdingbare Zusatzsoftware handelt, sollte hier mit weiteren Kosten gerechnet werden, die zu einer Bewertung der Anschaffungskosten mit „befriedigend" führen. Insgesamt bewegen sich die Kosten jedoch in den üblichen Dimensionen. Die Gesamtbewertung der Kategorie Kosten lautet deshalb „gut".

Gesamtbewertung Kosten:	2

4.4.5.4 Kategorie Datemsicherheit (+++)

Tabelle 4-71: FileCrypto - Datensicherheit

Kategorie Sicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Ja
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Ja
E-Mail (ja/nein)	Ja
Externe Speichermedien (ja/nein)	Ja
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Ja
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein

Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Ja
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	Ja[103]

FileCrypto basiert auf einem FIPS-zertifizierten AES Kryptographiekern[104], der für eine transparente Echtzeitverschlüsselung sorgt. Mittels FileCrypto können sichere Ordner angelegt werden[105] und PIM Daten sowie E-Mails verschlüsselt werden. Leider kann FileCrypto nicht den kompletten PDA sichern. Selbst im gesperrten (verschlüsselten) Zustand ist für einen professionellen Angreifer somit ein Zugriff auf unsichere Ordner theoretisch möglich.

Der FileCrypto Treiber muss erst geladen werden, um mit den sicheren Ordnern arbeiten zu können. Andernfalls verbleiben sie mit AES verschlüsselt geschützt im Filesystem. Zum Starten des Treibers ist eine gültige Authentifikation wie weiter oben beschrieben notwendig. Im Testbetrieb konnten keinerlei Probleme mit der Ver- und Entschlüsselung festgestellt werden. Nur die Titel für Aufgaben und Termine sind weiterhin unverschlüsselt auslesbar. Insgesamt lautet die Bewertung der Sicherheit deshalb „befriedigend" und damit besser als bei den meisten Konkurrenten. Vor allem der Komplettschutz für das Filesystem wird auch hier vermisst.

Gesamtbewertung Sicherheit:	3

4.4.5.5 Kategorie Usability (++)

Tabelle 4-72: FileCrypto – Usability 1

Kategorie Usability	Bewertung
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Ja
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	1
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	2
Alle benötigten Informationen sind auf dem Bildschirm zu finden	2
Ausgaben sind zweckmäßig und verständlich	2
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	1
Selbstbeschreibungsfähigkeit	

[103] Administrator kann extra Passphrase aus 6-40 Zeichen festlegen, die für die Deinstallation benötigt wird.
[104] Basierend auf einer festen Schlüssellänge von 128 Bit.
[105] Sei es im internen Speicher oder auf externen Speicherkarten.

Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	5
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	2
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	1
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	1
Aktueller Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann abgebrochen werden	2
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	1
Bearbeitungszeit abschätzbar	2
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwarteten Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	2
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen unmöglich	1
Bei Fehlern zweckmäßige Hinweise zur Ursache und Behebung	1
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	4
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	1
Nur wenige Detailkenntnisse zur Bedienung nötig	1
Hilfestellung bei Bedarf verfügbar	5

Tabelle 4-73: FileCrypto – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	1
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Administrationshandbuches	2
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	Ja
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	Ja

Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Supports (soweit bewertbar)	3

FileCrypto ist nur in deutscher und englischer Sprache verfügbar. Der KeyManager, der hier aus Zeitgründen nicht mit evaluiert wurde, ist sogar nur in Englisch verfügbar. Bei der Bedienung zeigt sich ein in weiten Teilen vorbildliches Konzept. Dies wird besonders am in das Programm integrierten Knopf für den Zugriff auf die Stromversorgungseinstellungen deutlich. FileCrypto legt keine extra Programmgruppe an, sondern ist, wie vom Nutzer gewohnt, unter dem üblichen Kennwortdialog zu finden. Die Dokumentation, die Administrations- und Benutzerhandbuch vereint, geht detailliert auch auf spezielle Themen ein und erläutert z. B. jede Konfigurationsmöglichkeit über die INI-Dateien und ausführlich den Verschlüsselungsmechanismus. Hier vermisst man dann jedoch ein Tool, das eine komfortablere Bearbeitung der INI-Dateien ermöglicht als ein gewöhnlicher Texteditor wie Notepad.

Das Laden und Entladen des FileCrypto Treibers nimmt einige Zeit in Anspruch und verursacht somit eine kleine Wartezeit. Eine Kontexthilfe existiert nicht. Ein schwerer Fehler tritt zudem reproduzierbar immer dann auf, wenn der Speicher sehr knapp wird. Im Labor stürzte in diesen Fällen das Sperren des Dateisystems irreparabel ab. Hier half nur ein echter Hardwarereset, womit auch alle Daten auf dem iPAQ verloren waren. Immerhin kann diesem Problem in der Praxis durch eine ausreichende Speicheraustattung begegnet werden. In der Regel sollte dieser Fehler dann nicht auftreten.

In der Summe zeigt sich ein durchdachtes Bedienkonzept, aufgrund dessen FileCrypto trotz gewisser Schwächen (Wartezeiten, umständlich zu bedienende Administration) und dem Fehler bei knappem Speicher mit „genügend" bewertet werden kann.

Gesamtbewertung Usability:	**4**

4.4.5.6 Kategorie Besondere Merkmale (+)

Tabelle 4-74: FileCrypto – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	2
Externe Referenzen/Erfahrungsberichte	2
Zukünftig zu erwartende Funktionalitätserweiterungen	2
Erwartungen Zukunftssicherheit	2

Die einzige schwerer wiegende Schwäche von FileCrypto ist, dass es nicht den kompletten PDA verschlüsseln kann. F-Secure ist einer der größten Hersteller für Sicherheitssoftware für PocketPC und es steht somit zu erwarten, dass auch in Zukunft regelmäßig neue Versionen herauskommen, die z. B. die in diesem Projekt beobachteten Probleme mit dem neuen iPAQ h5450 beheben. Externe Stimmen zum Produkt sind insgesamt sehr positiv. FileCrypto wurde z. B. von der renommierten Fachzeitschrift Pocket PC Magazine zur besten Sicherheitssoftware im Jahr 2002 gekürt[106].

Gesamtbewertung Besondere Merkmale:	**2**

[106] Für weitere Pressestimmen siehe: http://www.f-secure.com/news/awards/index.shtml [07.04.2003].

4.4.5.7 Gesamtbewertung

Tabelle 4-75: FileCrypto - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	1
+++	Kategorie Authentifikation	-	2
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	-	3
++	Kategorie Usability	-	4
+	Kategorie Besondere Merkmale	-	2
	KO-Kriterien gesamt	**0**	

FileCrypto wurde zu Recht ausgezeichnet. Die zentralen Kategorien Authentifikation und Sicherheit erreichten die besten Noten in unserem Testfeld. Trotzdem bleibt zu sagen, dass gerade im Punkt „Aufschraubschutz" noch Mängel bestehen, die in einem Umfeld mit hohen Sicherheitsansprüchen bedenklich sind. Die Usability fällt durch einige kleine Unannehmlichkeiten etwas aus dem Rahmen, Gesamtbewertung lautet dennoch „befriedigend".

Die schweren Probleme mit dem neuen iPAQ h5450 werden hoffentlich bald der Vergangenheit angehören. Bis dann sollte auf jeden Fall der ältere iPAQ h3970 eingesetzt werden.

Gesamtbewertung FileCrypto:	3

4.4.6 **movianCrypt** (ClientKonfig 03 + 11)

Im Rahmen der Komponentenauswahl war movianCrypt ursprünglich hauptsächlich wegen der vom gleichen Hersteller stammenden VPN-Software movianVPN interessant. Das von uns erhoffte gute Zusammenspiel zwischen diesen beiden Anwendungen konnten wir jedoch nicht testen, da im Laborbetrieb die vom Auftraggeber vorgegebene VPN-Lösung bzw. wurde. Somit beschränkten wir uns auf die Evaluation von movianCrypt in der Version 1.1 (Build 0132) als alleinstehende Endgerätesoftware. Die Tatsache, dass der Hersteller Certicom eine Breite Palette sicherheitsrelevanter Software auch für PDAs vertreibt, machte Hoffnung auf ein sicherheitstechnisch durchdachtes Gesamtkonzept.

4.4.6.1 **Kategorie Administration** (++)

Tabelle 4-76: movianCrpyt - Administration

Kategorie Administration	**Bewertung**
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	5
Zusammenarbeit mit Afaria	5

MovianCrypt bietet keine programmeigenen Administrationsmöglichkeiten. Dennoch kann zumindest die Installation von movianCrypt mittels separat verfügbarer Installationsdateien über Administrationslösungen bewerkstelligt werden. Zu weitergehenden Administrationsmöglichkeiten, beispielsweise zu übertragende Konfigurationsdateien, sagt die Dokumentation nichts. Das Programm movianCrypt wurde deshalb in Bezug auf Administrationsmöglichkeiten mit „mangelhaft" bewertet.

Gesamtbewertung Administration:	**5**

4.4.6.2 Kategorie Authentifikation (+++)

Tabelle 4-77: movianCrpyt - Authentifikation

Kategorie Authentifikation	Bewertung
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Ja
Sicheres Passwort / Passphrase (ja/nein)	Nein
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja[107]
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	-
Bei falscher Eingabe: Softlock (ja/nein)	Nein
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Ja
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Ja
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	6
Sicherheit der Authentifikation durch geringe Rückmeldung	2

[107] Nur mit Windows CE Energieoptionen.

Tabelle 4-78: movianCrpyt – Authentifikation KO

Anzahl KO
Authentifikation
Bewertung von 5 oder 6 bei Einflussmöglichkeiten durch Benutzer

Auch bei movianCrypt lässt sich eine PIN-Authentifikation durch Eingabe eines numerischen Passwortes umsetzen. Das Abschalten nach Inaktivität erfolgt auch bei movianCrypt mittels der Windows CE-eigenen Energieoptionen.

movianCrypt unterstützt keine separate Authentifikation von Verbindungen. Außerdem schützen weder Hardlock noch Wipe das Gerät vor Brute-Force-Angriffen. Die einzige Möglichkeit hierzu bietet der Mechanismus, der das Gerät nach zu häufiger Falscheingabe des Passworts für eine konfigurierbare Zeitspanne sperrt. Dies stellt einen Mittelweg zwischen sicherem Softlock und Verzögerung und somit nur einen mäßigen Schutz vor Brute-Force-Attacken dar. Hinzu kommt, dass ein einmal angemeldeter Benutzer die Sicherungsmechanismen durch Deinstallation komplett deaktivieren kann und dass auch movianCrypt die Erinnerung an fällige Termine vor einer gültigen Anmeldung nicht verhindert.

Der vorhandene Minimalschutz vor Brute-Force-Attacken kann deshalb die Bewertung „ungenügend" nicht verhindern.

Gesamtbewertung Authentifikation:	6

4.4.6.3 Kategorie Kosten (+)

Tabelle 4-79: movianCrpyt - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Neben den als gering zu betrachtenden reinen Anschaffungskosten von 50,00 USD sind für movianCrypt keine über die eventuelle Umstellung auf neuere Versionen hinausgehenden Kosten zu erwarten. Daher bewerten wir movianCrypt in Bezug auf die Kosten mit „gut".

Gesamtbewertung Kosten:	2

4.4.6.4 Kategorie Datensicherheit (+++)

Tabelle 4-80: movianCrpyt - Datensicherheit

Kategorie Datensicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Ja
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Ja
E-Mail (ja/nein)	Ja[108]
Externe Speichermedien (ja/nein)	Ja
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Ja
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Ja
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	Nein

Das Produkt movianCrypt bietet alle für den praktischen Betrieb notwendigen Verschlüsselungsfunktionen. Die Verschlüsselung erfolgt mit einem FIPS-zertifizierten Verschlüsselungskern nach dem von uns präferierten Algorithmus AES (128 Bit) sowohl für PIM-Daten als auch für E-Mails. Außerdem besteht die Möglichkeit der Benutzung von sicheren Ordnern zum geschützten Ablegen sensitiver Dokumente auf dem PDA. Ebenfalls können externe Speichermedien verschlüsselt werden. Die Tatsache, dass neben AES kein weiterer Verschlüsselungsalgorithmus verfügbar ist, wiegt an dieser Stelle nicht schwer, da AES von uns als hinreichend sicher erachtet wurde. Insbesondere aufgrund der Möglichkeit, sowohl PIM-Daten als auch E-Mails und ganze Datenverzeichnisse gesichert abzulegen, erhielt movianCrypt in der Kategorie Sicherheit die Bewertung „befriedigend". Für eine „gute" oder gar „sehr gute" Bewertung fehlt neben der Verschlüsselung des ganzen PDAs vor allen Dingen der Schutz vor unbefugter Deinstallation von Seiten des Nutzers. Anzumerken ist, dass der Hersteller Certicom empfiehlt, die „Save Contacts" Option von Windows CE bei der Verwendung von Verschlüsselungssoftware generell abzuschalten, da andernfalls die Kontaktdaten unverschlüsselt im ROM des PDAs gehalten werden und somit nicht geschützt sind.

Gesamtbewertung Datensicherheit:	3

[108] nur Inbox.

4.4.6.5 Kategorie Usability (++)

Tabelle 4-81: movianCrpyt – Usability 1

Kategorie Usability	Bewertung
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Nein
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	1
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	2
Alle benötigten Informationen sind auf dem Bildschirm zu finden	1
Ausgaben sind zweckmäßig und verständlich	1
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	-
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	6
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	1
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	2
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	1
Aktueller Bearbeitungsschritt kann unterbrochen werden	3
Ein laufender Vorgang kann abgebrochen werden	4
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	2
Bearbeitungszeit abschätzbar	2
Einheitliche Verwendung von Begriffen und Symbolen	2
Die Ausführung einer Operation führt zu erwarteten Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	-[109]
Versehentliches Auslösen von Aktionen unmöglich	1

[109] Keine Möglichkeit, syntaktisch falsche Dinge einzugeben.

Bei Fehlern zweckmäßige Hinweise zu Ursache und Behebung	3
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	1
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	2
Nur wenige Detailkenntnisse zur Bedienung nötig	2
Hilfestellung bei Bedarf verfügbar	6

Tabelle 4-82: movianCrpyt – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	2
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Administrationshandbuches	2
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Supports (soweit bewertbar)	-

Die Usability von movianCrypt ist bis auf das Fehlen von Kontexthilfe und anderen Hilfestellungen gut. Die Tatsache, dass keine Kontexthilfe aus dem Programm heraus verfügbar ist, kann der Hersteller Certicom durch eine hohe Selbstbeschreibungsfähigkeit des Programms und die guten Handbücher nahezu ausgleichen. Als weiterer Nachteil ist anzusehen, dass laufende Vorgänge und Arbeitsschritte nicht abgebrochen werden können.

Die gute Dokumentation sowie die überzeugende Selbstbeschreibungsfähigkeit von movianCrypt führen zur Bewertung der Usability des Programms mit „gut".

Gesamtbewertung Usability:	**2**

4.4.6.6 Kategorie Besondere Merkmale (+)

Tabelle 4-83: movianCrpyt – Besondere Merkmale

Kategorie Besondere Merkmale	**Bewertung**
Deckung der Testergebnisse mit Prospekten	2
Externe Referenzen/Erfahrungsberichte	2
Zukünftig zu erwartende Funktionalitätserweiterungen	3
Erwartungen Zukunftssicherheit	2

Abgesehen von dem Versprechen, den gesamten PDA zu sichern, deckten sich unsere Ergebnisse mit den Angaben aus den Prospekten des Herstellers. Certicom kann auf Kunden wie zum Beispiel das US-Verteidigungsministerium, Cisco und DaimlerChrysler ver-

weisen[110]. In Bezug auf zukünftig zu erwartende Funktionalitätserweiterungen von movianCrypt war wenig zu erfahren. Die Tatsache, dass Certicom über eine Fülle von Partnern und Lizenznehmern verfügt, ließ uns jedoch auch eine gute Zukunftssicherheit erwarten und das Produkt movianCrypt in der Kategorie Besondere Merkmale mit „gut" bewerten.

Gesamtbewertung Besondere Merkmale:	2

4.4.6.7 Gesamtbewertung

Tabelle 4-84: movianCrpyt - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	5
+++	Kategorie Authentifikation	1	6
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	-	3
++	Kategorie Usability	-	2
+	Kategorie Besondere Merkmale	-	2
	KO-Kriterien gesamt	**1**	

Lediglich die stark begrenzten Administrationsmöglichkeiten sowie das problematische Authentifikationsverfahren verhinderten die „gute" Gesamtbewertung von movianCrypt. Würde das Produkt über einen brauchbaren Deinstallationsschutz verfügen und dem Benutzer nicht das Deaktivieren der Sicherungsmechanismen gestatten, wäre die Bewertung in der Kategorie Authentifikation sicherlich deutlich besser ausfallen.

Mit einer Möglichkeit, movianCrypt zumindest dateibasiert (durch Übermitteln von Konfigurationsdateien) zu administrieren und einem Deinstallationsschutz würde auch die Gesamtbewertung besser als „ungenügend" ausfallen.

Gesamtbewertung movianCrypt:	6

[110] vergleiche: http://www.fcw.com/supplements/Fedlist/2002/fed-10com-09-16-02.asp [26.03.2003] und http://www.certicom.com/about/index.html [26.03.2003].

4.4.7 PDA Defense (ClientKonfig 04 + 12)

Die Software PDA Defense des Herstellers Asynchrony stellt im Rahmen dieses Evaluationsfeldes eine Ausnahme dar. Die als Hersteller auftretende Firma Asynchrony ist lediglich als Vermarkter von Projekten einer Entwicklergemeinde zu verstehen. Unter dem Dach von Asynchrony führen Entwickler, die nicht vertraglich gebunden sind, die verschiedensten Projekte durch, die dann nach Projektabschluss, zumeist als Shareware, von Asynchrony vertrieben werden.

Umso erstaunlicher sind die versprochenen Fähigkeiten der Software PDA Defense, die von dateibasierter Policy-Administration (mittels eines mitgelieferten Policy-Editors) über ein Challenge-Response-Verfahren zur Freischaltung eines gesperrten PDAs bis hin zum Schutz von einzelnen Applikationen reichen.

Leider war es uns jedoch nicht möglich, PDA Defense in für den Produktiveinsatz geeigneter Weise zu nutzen. Abstürze waren im Laufe der Evaluation an der Tagesordnung, nicht einmal das Passwort konnte auf verlässliche Art und Weise geändert werden und das Programm musste regelmäßig manuell aus dem Speicher entfernt werden.

Dennoch gelang es uns, auch PDA Defense anhand unseres Evaluationsbogens zu evaluieren. Dabei ist zu beachten, dass die häufigen Abstürze nicht in die Bewertung jeder einzelnen Kategorie einflossen.

4.4.7.1 Kategorie Administration (++)

Tabelle 4-85: PDA Defense - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Ja
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Ja
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Ja
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Ja
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	1
Zusammenarbeit mit Afaria	1

Über den mitgelieferten Policy Editor können gruppenbasiert Mindestanforderungen sowohl an die von den Benutzern verwendeten Passwörter als auch für sicherheitsrelevante Einstellungen und Verschlüsselung definiert werden, die der jeweilige Benutzer nicht unterschreiten kann. Ist ein solches Policy-Set erstellt, kann daraus eine Policy-Datei er-

zeugt und beim nächsten Synchronisationsvorgang auf den PDA übertragen werden, wo die Vorschriften dann aktiv werden.

So lässt sich im Policy-Editor eine minimale Passwortlänge zwischen 4 und 15 Zeichen sowie die Vorschrift, dass neben Buchstaben auch Ziffern im Passwort vorhanden sein müssen, einstellen. Das Vorschreiben der Verwendung von Sonderzeichen ist nicht möglich. Außerdem kann im Policy Editor definiert werden, welche Datenbanken (Kontakte, E-Mail) verschlüsselt werden sollen und wie oft die Benutzer die Passwörter wechseln müssen. Auch sicherheitsrelevante Einstellungen wie das automatische Sperren des Gerätes nach einer definierten Zeitspanne oder die erzwungene Anmeldung nach Einschalten des Gerätes lassen sich im Policy-Editor festlegen.

Vorschriften können gruppen- beziehungsweise profilbasiert angelegt werden, wobei die Policy-Dateien dann in den Gruppennamen entsprechend bezeichneten Verzeichnissen abgelegt werden. Dadurch ließe sich sogar realisieren, dass die Policy-Dateien genau in das einer Gruppe entsprechende Afaria-Verzeichnis zur Dateiverteilung hineingeneriert und somit beim nächsten Synchronisationsvorgang automatisch sofort verteilt werden.

Für den Fall, dass keine Managementsoftware wie Afaria oder das XTND-Management verwendet wird, lassen sich diese Dateien auch über ein lokales ActiveSync auf die PDAs bringen. Das somit einzige von PDA Defense nicht erfüllte Kriterium in der Kategorie Administration sind Vorschriften zur Verschlüsselung externer Medien. Dennoch rechtfertigten insbesondere die gute Bedienoberfläche und die Fähigkeiten des Policy Editors eine „sehr gute" Bewertung[111] in der Kategorie Administration.

Gesamtbewertung Administration:	**1**

4.4.7.2 Kategorie Authentifikation (+++)

Tabelle 4-86: PDA Defense - Authentifikation

Kategorie Authentifikation	**Bewertung**
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Ja
Sicheres Passwort / Passphrase (ja/nein)	Ja
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein

[111] Mithin die einzige des gesamten Testfeldes, umso mehr bedauerten wir die häufigen Abstürze

Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	1[112]
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	3[113]
Bei falscher Eingabe: Softlock (ja/nein)	Nein
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Ja
Bei falscher Eingabe: Verzögerung (ja/nein)	Nein
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	2
Sicherheit der Authentifikation durch geringe Rückmeldung	2

PDA Defense bietet lediglich die Anmeldung über ein Passwort an, das bei entsprechend konfigurierten Policies sowohl aus Buchstaben als auch aus Ziffern bestehen muss. Die Mindestlänge kann ebenfalls über die Policies festgelegt werden. Durch Verwendung eines vierstelligen rein numerischen Passworts ist dies auch als PIN verwendbar. Allerdings nutzt PDA Defense dieses Passwort nur, um das Gerät beim Anschalten zu sichern. Die Verbindungsaufnahme wird nicht verhindert. Mittels der Policies ist es auch möglich, dem Benutzer Konfigurationen des Programms außer dem Einstellen seines Passwortes zu verbieten.

Nachteilig ist, dass bei PDA Defense als minimaler Zeitraum zwischen Abschalten und Absichern des Gerätes eine Minute einstellbar ist. Ein sofortiges Sichern nach dem Abschalten ist offensichtlich nicht möglich. Allerdings ist nach der Installation im Startmenü von Windows CE ein Eintrag vorhanden, mittels dessen es möglich ist, den PDA unverzüglich zu sichern. Schaltet man diesen danach ab, so ergibt sich das gewünschte Verhalten. Warum die Option zum sofortigen Sichern nicht verfügbar ist, bleibt allerdings offen.
Ebenfalls in den Policies einstellbar sind Vorschriften zum Schutz vor Brute-Force-Angriffen. So lässt sich festlegen, dass nach 5 fehlgeschlagenen Anmeldeversuchen alle PIM-Datenbanken sowie das Dokumentenverzeichnis gelöscht werden sollen. Hat der Benutzer sein Passwort verloren oder vergessen, so bietet PDA Defense ein Challenge-

[112] In Form eines Challenge-Response-Verfahren, wobei die Response mit einem sicheren Passwort incl. Sonderzeichen vergleichbar ist.
[113] Frei wählbares Passwort.

Response-Verfahren[114] zur Freischaltung an, bei dem das Programm eine Zahl ausgibt, mittels derer der Administrator einen für den Zeitraum von 60 Minuten gültigen, aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen bestehenden Freischaltschlüssel generieren kann. Bei Verwendung dieser Option ist sicherzustellen, dass unbefugte Personen auf keinen Fall einen solchen Freischaltschlüssel erhalten. Es stellt sich somit die Frage der Authentifikation des Nutzers dem Administrator gegenüber, die an dieser Stelle jedoch nicht behandelt werden soll.

PDA Defense wirbt damit, auch den Start einzelner Applikationen an eine gesonderte Passworteingabe binden zu können. Der Versuch, diese Funktion zu benutzen verursachte jedoch in jedem Fall den einzig eindeutig reproduzierbaren Absturz von PDA Defense.

Da die Systeminstabilität nicht in die Bewertung der einzelnen Kategorien einfließt, kann aufgrund des durchdachten Verfahrens bei verlorenem oder vergessenem Passwort und des Deinstallationsschutzes die Bewertung „gut" abgegeben werden. Zu einer besseren Bewertung wären Funktionen zur Sicherung von Verbindungen sowie flexiblere Einstellungsmöglichkeiten für den Sicherungszeitpunkt und das Verhalten bei Falscheingabe notwendig gewesen.

Gesamtbewertung Authentifikation:	**3**

4.4.7.3 Kategorie Kosten (+)

Tabelle 4-87: PDA Defense - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Die Anschaffungskosten für PDA Secure sind mit 29,95 USD moderat, es fallen keine zusätzlichen Hardwarekosten an und auch die Kosten für den Umstieg auf spätere Folgeversionen dürften gering sein. Somit bekommt auch PDA Defense hier die Bewertung „gut".

Gesamtbewertung Kosten:	**2**

[114] Mehr zu Challenge Response Verfahren in „Identifikation durch Challenge-Response-Verfahren" (Sans 2000).

4.4.7.4 Kategorie Datensicherheit (+++)

Tabelle 4-88: PDA Defense - Datensicherheit

Kategorie Datensicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Nein
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Ja[115]
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Ja
E-Mail (ja/nein)	Ja
Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Ja
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Ja[116]
Schutz vor unbefugter Deinstallation (ja/nein)	Ja

Auch PDA Defense verschlüsselt PIM-Daten, E-Mail und manuell ausgewählte Verzeichnisse. Es ist das einzige Programm im Testfeld, das nicht die Verwendung des AES-Verschlüsselungsalgorithmus ermöglicht. Dafür bietet PDA Defense jedoch den Blowfish-Algorithmus mit einer Schlüssellänge von 128 oder 512 Bit sowie ein eigenes, nicht näher erläutertes Verschlüsselungsverfahren an.

Ein Benutzer kann die Software nicht deinstallieren, da hierzu das Nicht-Setzen des Passwortes erforderlich ist. Dies sollte im Regelfall mittels der gestaltbaren Policies verhindert und nur bei anstehender Deinstallation durch den Administrator explizit zugelassen werden.

Da die Verfügbarkeit eines 512-bittigen Blowfish-Algorithmus einem 128-Bit-AES zumindest gleichwertig ist und sowohl PIM-Daten als auch E-Mails und gesonderte Ordner verschlüsselt werden können, geben wir hier die Bewertung „befriedigend" ab.

Gesamtbewertung Datensicherheit:	3

[115] 128 oder 512 Bit
[116] Nur im Rahmen eines Wipes.

4.4.7.5 Kategorie Usability (++)

Tabelle 4-89: PDA Defense – Usability 1

Kategorie Usability	Bewertung
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Nein
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	2
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	4
Alle benötigten Informationen sind auf dem Bildschirm zu finden	4
Ausgaben sind zweckmäßig und verständlich	3
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	-
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	6
Meldungen sind sofort verständlich	2
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	2
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	3
Auswirkungen von Aktionen hinreichend ersichtlich	2
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	3
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	1
Aktueller Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	2
Bearbeitungszeit abschätzbar	2
Einheitliche Verwendung von Begriffen und Symbolen	2
Die Ausführung einer Operation führt zu erwarteten Ergebnis	2
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	2
Versehentliches Auslösen von Aktionen unmöglich	2
Bei Fehlern zweckmäßige Hinweise zu Ursache und Behebung	1
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	6

Erlernbarkeit	
Schnelles Erlernen der Bedienung	3
Intuitive, selbsterklärende Benutzung möglich	3
Nur wenige Detailkenntnisse zur Bedienung nötig	2
Hilfestellung bei Bedarf verfügbar	6

Tabelle 4-90: PDA Defense – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	2
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Administrationshandbuches	2
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Supports (soweit bewertbar)	-

Tabelle 4-91: PDA Defense – Usability KO

Anzahl KO
Usability

Benotung „ungenügend" bei Abstürze/Systemfehler

Neben dem bereits in der Einleitung erwähnten bis zur Unbenutzbarkeit häufigen Auftreten von Abstürzen erscheinen in der Oberfläche auch große Mengen von abgeschnittenen und dadurch nicht vollständig lesbaren Texten.

Z. B. muss man, um das Passwort zu ändern, auf ein Dialogelement tippen, dass wie ein inaktives Ausgabefeld aussieht, nicht jedoch wie ein Button. Noch dazu ist der darauf befindliche Text „ssword is assigned. Tap to change passwo" am Anfang und Ende abgeschnitten. Auf der Eingabemaske für das neue Passwort befinden sich ein „Cancel" und ein „Clear" Button, ein „OK" Button fehlt jedoch. Hierzu muss der „OK" Button der Maske (nach Windows CE-Standard in der Titelzeile) verwendet werden.

Außerdem ist die Art und Zusammensetzung eines neu einzugebenen Passwortes nicht ersichtlich. Weder die minimale Länge noch die an eine Policy gebundene Zusammensetzung sind erkennbar. Erst nach Eingabe eines nicht der Policy entsprechenden Passwortes wird der Benutzer darauf aufmerksam gemacht.

Hinzu kommt, dass das Programm ausdrückliche Warnungen nicht als Warnungen sondern als Fragen markiert. Die Oberfläche des Programms ist oftmals verwirrend oder lässt Dinge unerklärt. Die Handbücher sowohl für PDA Defense als auch für das Management-Tool Policy Editor sind ganz im Gegensatz dazu gut.

Würde hier nicht das KO-Kriterium erfüllt, könnten wir PDA Defense in Bezug auf die Usability mit „befriedigend" beurteilen. Da jedoch die Abstürze derart häufig auftraten,

dass ein sinnvolles Arbeiten mit PDA Defense unmöglich war, lautet die Beurteilung „ungenügend".

Gesamtbewertung Usability:	6

4.4.7.6 Kategorie Besondere Merkmale (+)

Tabelle 4-92: PDA Defense – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	2
Externe Referenzen/Erfahrungsberichte	2
Zukünftig zu erwartende Funktionalitätserweiterungen	3
Erwartungen Zukunftssicherheit	3

Die Kategorien „Zukunftssicherheit" und „Funktionalitätserweiterungen" werden mit „befriedigend" beurteilt, da Asynchrony sich selbst nicht als Softwarehersteller im eigentlichen Sinne Versteht:

„Asynchrony.com is a unique virtual community for software programmers, designers, writers, project managers and testers. Members share ideas with each other and form teams to collaborate on software projects. Asynchrony markets the finished software and gives the lion's share of revenues to the team members who created the software." (Asynchrony 2003)

Unsere Erwartungen diesbezüglich sind daher sehr vorsichtig. PDA Defense wurde bereits ausgezeichnet, allerdings beziehen sich diese Auszeichnungen offensichtlich auf die Palm OS Version[117].

Gesamtbewertung Besondere Merkmale:	3

4.4.7.7 Gesamtbewertung

Tabelle 4-93: PDA Defense - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	1
+++	Kategorie Authentifikation	-	2
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	-	3
++	Kategorie Usability	1	6
+	Kategorie Besondere Merkmale	-	3
	KO-Kriterien gesamt	**1**	

Trotz der zahlreich aufgetretenen Abstürze ist es uns gelungen, das Programm PDA De-

[117] Z. B. Test von PDA Defense in SC Online Magazin vom November 2002 (SCMag 2002).

fense dem Evaluationsbogen entsprechend zu testen. Das zugrunde liegende Konzept sowie die Administrationsmöglichkeiten mittels des beiliegenden Policy Editors überzeugen. Ohne das Absturzproblem wäre die Kategorie Usability mit „befriedigend" bewertet worden.

Für den Fall, dass das Programm in Zukunft stabil funktioniert, käme es durchaus für eine „gute" bis „befriedigende" Wertung und die Verwendung in Betracht. Im derzeitigen Stadium ist es jedoch aufgrund der massiven Stabilitätsprobleme unbrauchbar.

Gesamtbewertung PDA Defense:	**6**

4.4.8 **PDASecure Premium** (ClientKonfig 05 + 13)

Die Sicherheitslösung PDASecure Premium war ursprünglich nur für das Betriebssystem Palm OS verfügbar. In diesem Markt genießt sie eine sehr hohe Popularität und wurde mit diversen Preisen ausgezeichnet[118]. Mittlerweile existiert ebenfalls eine Version für PDAs nach dem PocketPC 2002–Standard, die jedoch nur einen eingeschränkten Funktionsumfang bietet. Diese haben wir hier in der Version 1.0 getestet.

4.4.8.1 **Kategorie Administration** (++)

Tabelle 4-94: PDA Secure - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	6
Zusammenarbeit mit Afaria	6

Die PocketPC–Version von PDASecure Premium bietet im Betrieb ohne die vom Testbetrieb ausgeschlossene Mobility Suite des gleichen Herstellers (Kapitel 3.1.3) keinerlei Möglichkeit zur Administration. Auch die Administration der Sicherheitslösung mittels Afaria oder XTND war nicht möglich. Daher konnten wir hier nur die Bewertung „ungenügend" abgeben

Gesamtbewertung Administration:	Note 6

[118] Vergleiche: http://www.trustdigital.com/med10.htm [26.03.2003].

4.4.8.2 Kategorie Authentifikation (+++)

Tabelle 4-95: PDA Secure - Authentifikation

Kategorie Authentifikation	Bewertung
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	m. Einschr.
Passwort / Passphrase (ja/nein)	Ja
Sicheres Passwort / Passphrase (ja/nein)	Nein
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	-
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja[119]
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Ja
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Ja
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	-
Bei falscher Eingabe: Softlock (ja/nein)	Ja
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	Ja
Bei falscher Eingabe: Wipe (ja/nein)	Ja
Bei falscher Eingabe: Verzögerung (ja/nein)	Ja
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	6
Sicherheit der Authentifikation durch geringe Rückmeldung	2

[119] Nur mit Windows CE Energieoptionen.

Tabelle 4-96: PDA Secure – Authentifikation KO

Anzahl KO
Authentifikation
Bewertung von 5 oder 6 bei Einflussmöglichkeiten durch Benutzer

PDASecure Premium bietet zwar kein explizit vorgesehenes Anmeldeverfahren mittels numerischer PIN oder erweiterter PIN, aber ein Passwort, das aus einer beliebigen Anzahl beliebiger alphanumerischer Zeichen bestehen darf. Es sind somit auch numerische Passwörter erlaubt, die aus 4 Ziffern bestehen, wodurch auch eine PIN-basierte Anmeldung möglich ist. Außerdem bietet PDASecure Premium die Möglichkeit, eine solche numerische PIN nicht mittels systemeigener Methoden (Bildschirmtastatur, Handschrifterkennung, etc.) eingeben zu lassen, sondern statt dessen ein programmeigenes Verfahren zur Eingabe von Ziffern zu nutzen. PDASecure Premium blendet hierzu zusätzlich zu der Windows CE-eigenen Bildschirmtastatur unterhalb der Eingabezeile für das Passwort zehn auf dem Gerät verfügbare Programmsymbole ein, die mit den Ziffern 0-9 beschriftet werden. Dieses Verfahren stellt zwar keine erweiterte PIN im Sinne dieser Evaluation dar, bietet aber dennoch ein alternatives Eingabeverfahren, was von uns grundsätzlich begrüßt wird. In diesem Fall ist jedoch der dadurch erzielte Mehrwert gleich Null, da die Anordnung der Symbole nicht wechselnd ist (die 0 ist stets oben links platziert) und somit das Ausspionieren durch Verfolgen von Bewegungsabläufen nicht verhindert wird.

Außerdem existiert keine Mindestlänge für Passwörter, was aus sicherheitstechnischer Sicht äußerst bedenklich ist.

In Bezug auf die möglichen Authentifikationszeitpunkte unterscheidet sich die Pocket PC-Version von PDASecure Premium stark von der am Markt etablierten Palm OS-Version. So wird zwar auf den Webseiten des Herstellers massiv damit geworben, dass PDASecure Premium in den zwei unterschiedlichen Modi *Global* und *Local* betrieben werden könne. Im globalen Modus würde der gesamte PDA geschützt, im lokalen Modus einzelne Applikationen. Die Pocket PC-Version kennt jedoch lediglich den globalen Modus, so dass, ist ein Benutzer angemeldet, auch bei Benutzung von PDASecure beliebige Applikationen gestartet werden können, was auf der Website des Herstellers an keiner Stelle erwähnt wird. Die Abschaltung nach Inaktivität ist auch mit PDASecure Premium nur auf dem bereits für die Standardausstattung dargelegten Umweg über die Energieoptionen möglich und auch PDASecure Premium verhindert nicht das Aufpoppen fälliger Termine, ohne dass der Benutzer angemeldet ist. Vielmehr aktiviert sich das Gerät, wie auch ohne zusätzliche Sicherheitssoftware üblich, bei Fälligkeit, um den Termin anzuzeigen.

Das neben den zulässigen einstelligen Passwörtern größte Manko von PDASecure Premium ist die Tatsache, dass ein angemeldeter Benutzer die Applikation mit dem Windows-CE-eigenen Standardverfahren zur Programmdeinstallation vom System zwar nicht vollständig, aber teilweise entfernen kann. Dabei wird die Deinstallation nicht abgeschlossen und der PDA muss einem Softreset unterzogen werden. Bis auf den weiterhin vorhandenen und manuell zu entfernenden Ordner im Dateisystem ist danach das Programm PDASecure nicht mehr auf dem Gerät aktiv. Der hierdurch entstehende Status kommt einer Deaktivierung der gesamten durch die Software bereitgestellten zusätzlichen Funktionalität gleich.

PDASecure Premium bietet auch die Optionen, nach zu häufiger Eingabe eines falschen Passworts einen Wipe oder einen Hardlock durchzuführen. Weder der Hardlock noch der Wipe funktionierte im Labor problemlos. Zwar aktivierte sich der Hardlock vorschriftsgemäß nach zu häufiger Falscheingabe des Passwortes und das Gerät wurde auf den Auslieferungszustand zurückgesetzt, doch der Zähler für die Fehlversuche ließ sich durch Durchführen eines Softresets wieder auf 0 zurücksetzen. Die Wipe-Funktion von PDASe-

cure Premium konnte noch weniger überzeugen. Sie hinterließ das Gerät in einem undefinierten Zustand mit offensichtlich fehlenden Schriftarten diverser Fehlermeldungen auf dem Schirm. Nach einem manuell durchgeführten Hard-Reset konnte der PDA, dann im Auslieferungszustand wie nach einem gewöhnlichen Hard-Reset, sogar wieder in Betrieb genommen werden. Dies führte neben dem nicht vorhandenen Deinstallationsschutz zu der Bewertung „ungenügend".

Gesamtbewertung Authentifikation:	**6**

4.4.8.3 Kategorie Kosten (+)

Tabelle 4-97: PDA Secure - Kosten

Kategorie Kosten	**Bewertung**
Einmalige Kosten	
Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Neben den als gering zu bezeichnenden Anschaffungskosten in Höhe von 39,95 USD fanden wir keine Anhaltspunkte für weitergehende Kosten. Lediglich die Aktualisierung der Software durch eventuell neu angebotene Versionen kann unter Umständen zusätzliche laufende Kosten verursachen. Daher sind die durch Benutzung von PDASecure Premium entstehenden Kosten als „gut" zu bewerten.

Gesamtbewertung Kosten:	**2**

4.4.8.4 Kategorie Datensicherheit (+++)

Tabelle 4-98: PDA Secure - Datensicherheit

Kategorie Datensicherheit	**Bewertung**
Kryptografische Algorithmen	
RC4 (ja/nein)	Ja
Rjindael / AES (ja/nein)	Ja
Toofish (ja/nein)	Ja
Blowfish (ja/nein)	Ja
TEA (ja/nein)	Ja
XOR (ja/nein)	Ja
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein

PIM-Daten (ja/nein)	Nein
E-Mail (ja/nein)	Nein
Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Ja
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	Nein

Tabelle 4-99: PDA Secure – Datensicherheit KO

Anzahl KO
Datensicherheit
Keine Möglichkeit PIM-Daten zu verschlüsseln

Auch wenn PDASecure Premium eine überwältigende Anzahl von Verschlüsselungsalgorithmen anbietet, scheitert diese Sicherheitslösung dennoch an dem definierten KO-Kriterium der nicht möglichen Verschlüsselung von PIM-Daten. PDASecure Premium ermöglicht lediglich die Verschlüsselung manuell ausgewählter Verzeichnisse, was zur Folge hat, dass insbesondere Kontakt- und Termindaten unverschlüsselt im Speicher des Gerätes liegen. Die beste und sicherste Authentifizierungsmethode kann leicht durch Aufschrauben des Gerätes umgangen werden und wird somit ohne Verschlüsselung der sensitiven Daten sinnlos.

Deswegen kann die Gesamtbewertung nur „ungenügend" lauten.

Gesamtbewertung Datensicherheit:	**6**

4.4.8.5 Kategorie Usability (++)

Tabelle 4-100: PDA Secure – Usability 1

Kategorie Usability	**Bewertung**
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Nein
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	2
Daten können wie von der Aufgabe gefordert eingegeben werden	2
Informationen und Bedienelemente befinden sich am richtigen Platz	3
Alle benötigten Informationen sind auf dem Bildschirm zu finden	2

Ausgaben sind zweckmäßig und verständlich	1
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	-
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	6
Meldungen sind sofort verständlich	1
Rückmeldungen können einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	1
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	3
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	2
Aktueller Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann abgebrochen werden	6
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	1
Bearbeitungszeit abschätzbar	3
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwarteten Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	3
Eingaben werden auf syntaktische Korrektheit geprüft	3
Versehentliches Auslösen von Aktionen unmöglich	2
Bei Fehlern zweckmäßige Hinweise zu Ursache und Behebung	3
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	4
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	2
Nur wenige Detailkenntnisse zur Bedienung nötig	2
Hilfestellung bei Bedarf verfügbar	6

Tabelle 4-101: PDA Secure – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	4
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein

Qualität des Administrationshandbuches	-
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	-
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	-
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	-
Qualität des Supports (soweit bewertbar)	-

PDASecure Premium hinterlässt in Bezug auf die Usability gemischte Eindrücke. Der als gut zu bezeichnenden Gestaltung der Benutzerinteraktion steht die grundsätzliche Nichtverfügbarkeit von Kontexthilfen oder anders gearteten Hilfestellungen gegenüber. Diese grundsätzliche Schwäche setzt sich auch in der Qualität der nur in englischer Sprache verfügbaren Benutzerhandbuchs fort. Es wirkt marktschreierisch, unorganisiert und technisch schlecht umgesetzt. Die Tatsache, dass sich verschiedene Textfelder bis zur Unleserlichkeit überschneiden ist ebenfalls von großem Nachteil.

Einer „guten" Bewertung steht außerdem entgegen, dass die Art der Rückmeldung nicht immer eindeutig erkennbar ist und dass die Deinstallation des Programms, wie bereits im Text zur Kategorie Authentifikation beschrieben, nicht vollständig durchgeführt werden konnte und somit ein manuelles Entfernen einiger zum Programm gehörender Dateien notwendig war.

PDASecure Premium wurde deshalb von uns in dieser Kategorie mit der Note „befriedigend" bewertet.

Gesamtbewertung Usability:	**3**

4.4.8.6 Kategorie Besondere Merkmale (+)

Tabelle 4-102: PDA Secure – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	4
Externe Referenzen/Erfahrungsberichte	3
Zukünftig zu erwartende Funktionalitätserweiterungen	2
Erwartungen Zukunftssicherheit	2

Wie bereits erwähnt decken sich die Fähigkeiten der Pocket PC-Version von PDASecure Premium nur teilweise mit den Angaben des Herstellers. Insbesondere ist hier lediglich der globale Modus verfügbar, worauf vom Hersteller vorab nicht hingewiesen wird.

Die verfügbaren Referenzen und Auszeichnungen zu diesem Programm beziehen sich auf die Palm OS-Version, lassen jedoch hoffen, dass der Hersteller seine auf dem Gebiet der Palm-Sicherheit erworbene Kompetenz und Marktpräsenz in Zukunft auch in die offensichtlich noch relativ neue Version für PocketPCs einfließen lässt. Da dies in unseren Augen weitaus schwerer wiegt als die Tatsache, dass das Produkt nicht alle im Prospekt aufgeführten Eigenschaften bereitstellt, entschlossen wir uns zu der Bewertung „gut".

Gesamtbewertung Besondere Merkmale:	**2**

4.4.8.7 Gesamtbewertung

Tabelle 4-103: PDA Secure - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	6
+++	Kategorie Authentifikation	1	6
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	1	6
++	Kategorie Usability	-	3
+	Kategorie Besondere Merkmale	-	2
	KO-Kriterien gesamt	**2**	

PDASecure Premium wurde in zwei Kategorien für völlig untauglich befunden. Da dies noch dazu die stark gewichteten Kategorien Sicherheit und Authentifikation sind, ist, entsprechend unserem Evaluationskonzept, die Gesamtbewertung „untauglich" bzw. „ungenügend" zu vergeben.

Auch wenn diese Bewertung sich nicht zwingend aus den aufgestellten KO-Kriterien ergeben hätte, wäre die Software insbesondere aufgrund des Authentifikationskonzeptes und der mangelnden Verschlüsselung von PIM-Daten und E-Mails lediglich als bedingt empfehlenswert zu bezeichnen.

Gesamtbewertung PDASecure Premium:	6

4.4.9 **Pointsec for PocketPC** (ClientKonfig 06 + 14)

Der Hersteller „Pointsec Mobile Technologies AB" [120] bezeichnet sich als „leading distributor of enterprise IT security solutions in the Nordic region" (Pointsec 2003). Das Flaggschiff der Produktlinie ist die Sicherheitslösung Pointsec, die in das Testfeld aufgenommen wurde. Der Hersteller stellte uns dabei die schon ältere Version 1.3 zur Evaluation zur Verfügung. In der Phase der Evaluation traten massive Probleme mit der Software auf, die auf keine eindeutige Ursache zurückzuführen waren, jedoch eine Evaluation unmöglich machten. Eine Kontaktaufnahme mit dem Hersteller bestätigte schließlich den Verdacht. Die uns nach Deutschland zugeschickte Version des Clients könne nicht mit dem deutschen Windows CE umgehen, wurde uns *nach* erfolgter Bezahlung und Lieferung mitgeteilt.

Pointsec für PocketPC ist als Sicherheitsprodukt speziell für große Unternehmen gedacht und wird nicht an Consumer vertrieben. Pointsec wirbt insbesondere mit den umfangreichen Administrationsmöglichkeiten der Software. Daher wurde entschieden, es im Rahmen des Berichtes zumindest vorzustellen, auch wenn eine Wertung mangels praktischer Evaluation entfallen muss.

4.4.9.1 **Kategorie Administration** (++)

Im Lieferumfang enthalten sind ein Administrationstool und einige Hardwaretoken. Diese Hardwaretoken ähneln kleinen Taschenrechnern und sind mit einer vierstelligen PIN gesichert. Jedes Token ist in der Lage, aus einer sogenannten Challenge[121] eine nur für dieses Token gültige Response[122] zu errechnen.

Bei der Installation des kleinen Administrationstools, wird vom Administrator ein Fingerprint vergeben. Dieser, so die Anleitung, wird benutzt, um diese Installation von Pointsec „unique to the Company organization" (Pointsec 2002, Seite 8) zu machen. Leider bleibt unklar, was genau „unique" hier bedeutet und wie dieser Mechanismus funktioniert[123]. Außerdem müssen mit dem Fingerprint mindestens zwei[124] Token registriert werden. Mit Hilfe der Token[125] kann der Administrator später im laufenden Betrieb zu der vom Administrationsprogramm ausgegebenen Challenge eine gültige Response errechnen, um z. B. das Tool starten zu können. Die genaue Auswirkung der Anzahl Token bleibt mangels praktischer Evaluation und ungenügender Dokumentation ebenfalls unklar.

Das Konzept von der Pointsec Administration basiert auf dem Generieren von Installationspaketen inklusive einer zugehörigen Sicherheitspolicy. Diese können, vom Programm fest vorgesehen, mit dem XTND Connect Server verteilt werden. Pointsec wirbt an dieser Stelle mit der guten Zusammenarbeit. Im Prinzip lassen sich so die Benutzerrechte und alle wichtigen Einstellungen gezielt erzwingen. Die Fähigkeiten sind dabei ähnlich gut, wie beim ebenfalls im Test untersuchten FileCrypto, nur dass hier eine Oberfläche für die Erstellung der Installationspakete angeboten wird, die mit einem recht komplizierten und leider zu undurchsichtigen Tokenkonzept arbeitet.

---

[120] Internetpräsenz unter http://www.pointsec.com [10.04.2003].
[121] Eine 8-stellige Zahl.
[122] Die 8-stellige Response besteht dabei aus Buchstaben und Zahlen.
[123] Ein Umstand, der der mangelhaften Dokumentation geschuldet bleibt.
[124] Maximal jedoch bis zu 50.
[125] Im Testbetrieb wurden zwei Hardwaretoken der Firma Secure Computing aus New Brighton mit der Programmierung für die Pointsec Sicherheitssoftware geliefert.

4.4.9.2 Kategorie Authentifikation (+++)

Die Authentifikation basiert auf der produkteigenen PicturePIN. Diese PIN Eingabe ist eine sichere PIN wählbarer Länge[126] im Sinne der Definition in Kapitel 4.4.1. Die Symbolsets sind individualisierbar und erscheinen bei geforderter Authentifikation in zufälliger Anordnung auf dem Bildschirm. Alternativ gibt es auch einfachere Mechanismen wie eine QuickPIN oder alphanumerische Passwörter. Kernbestandteil ist aber die PicturePIN. Ein PowerON Passwort ist damit ebenfalls möglich.

Sollte das Passwort einmal verloren gehen oder eine vordefinierte Anzahl an Fehlversuchen überschritten werden, bietet Pointsec einen recht ungewöhnlichen Mechanismus an, um das Gerät zu entsperren. Dazu benutzt Pointsec eine Remote Help Funktion, die ein Challenge und Response Verfahren zwischen Administrator und Benutzer verwendet, um den Nutzeraccount freizuschalten. Dazu wird keinerlei Netzwerkverbindung benötigt.

Auf dem Bildschirm des PDA erscheint dazu eine Challenge. Zusammen mit dem Gerätenamen muss der Nutzer diese Challenge z. B. über Telefon an den Administrator übermitteln. Der Administrator erzeugt dazu mittels des Administrationsprogramms, eines spezifischen Unlockcodes und der übermittelten Daten eine Response. Diese Response[127] wird z. B. wieder telefonisch an den Nutzer übermittelt, der sie eingibt und damit das Gerät entsperrt. Leider bietet Pointsec nicht die Möglichkeit eines Wipes oder echten Hardwarereset im Falle einer bestimmten Anzahl von Fehlversuchen an.

Dank der guten Administrationsmöglichkeiten hat zudem der Benutzer bei entsprechender Sicherheitspolicy kaum Einflussmöglichkeiten auf die Einstellungen von Pointsec und kann somit z. B. auch nicht die Authentifikation deaktivieren. Einzigartig im Testfeld ist die Möglichkeit, bei Aufnahme einer ActiveSync Verbindung eine erneute Benutzerauthentifikation am PDA zu verlangen.

Unklar bleibt, ob Pointsec erfolgreich den Terminbug verhindert. Pointsec zeigt jedoch in der Theorie gute Ansätze und Ideen. In der vorliegenden Version stören insbesondere fehlende Sicherungsmechanismen. Insgesamt reicht es in dieser Kategorie trotzdem zum Spitzenfeld der Testkandidaten.

4.4.9.3 Kategorie Kosten (+)

Anders als bei den übrigen hier vorgestellten Sicherheitslösungen wird PointSec nicht direkt über z. B. Internetshops vertrieben. Pointsec verkauft sein Produkt vielmehr über einen Rahmenvertrag direkt an das entsprechende Unternehmen. Die Kosten fallen deutlich höher aus als bei den anderen Produkten im Testfeld. So verlangt Pointsec 120 Euro für eine Lizenz und eine Mindestabnahme von 100 Lizenzen. Unter einem Preis von 12.000 Euro ist somit Pointsec nicht verfügbar. Die teuersten Produkte im restlichen Feld kommen ungefähr auf die Hälfte dieses Preises und verlangen keine Mindestmenge an Lizenzen.

Eine weitere Hürde stellt die Vorraussetzung von Pointsec dar, mindestens zwei autorisierte und von Pointsec eingewiesene Administratoren im Unternehmen zu haben. Pointsec bietet dazu Seminare an, in denen Unternehmen ausgewählte Mitarbeiter zertifizieren lassen können, was ebenfalls nicht kostenlos ist.

---

[126] Zwischen 4 und 13 Stellen.
[127] Eine 16 stellige Zahlenfolge.

Insgesamt bildet Pointsec im Testfeld die Spitze im Bereich Kosten. Es bleibt zu überlegen, ob die höheren Anschaffungskosten die Vorteile gegenüber der Konkurrenz rechtfertigen.

4.4.9.4 Kategorie Datensicherheit (+++)

Im Bereich Verschlüsselung scheint PointSec for Pocket PC 1.3 in keiner Weise den Ansprüchen gerecht zu werden. Pointsec bietet zwar eine sichere Verschlüsselung über AES mit 128 Bit Schlüssellänge, allerdings beschränkt sich die Verschlüsselung auf Compact Flash (CF) Speicherkarten. Diese werden komplett verschlüsselt und über die CardID sogar mit einer eigenen Authentifikation in Form einer extra PicturePIN versehen. Möglichkeiten, das Filesystem des iPAQ, PIM Daten oder E-Mails zu verschlüsseln, bestehen jedoch nicht, was dieser Kategorie in der derzeitigen Form bei einer Wertung ein „ungenügend" bringen würde.

Einige positive Details wie die Erzeugung einer Zufallszahl mittels vom Benutzer gezeichneter wahlloser Linien bei der Erstinstallation des PDA-Clients werden im Handbuch zwar aufgeführt, aber nicht ausreichend dokumentiert.

4.4.9.5 Kategorie Usability (++)

Zur Usability kann nicht viel gesagt werden, da, wie in der Einleitung auf Seite 176 beschrieben, eine praktische Evaluation des Produktes nicht möglich war. Im Lieferumfang enthalten waren ein Ordner mit der Dokumentation getrennt in Benutzer- und Administrationshandbuch, eine CD mit der Software, zwei Hardwaretoken, eine Diskette mit den TokenPINs und dem Evaluationskey.

Das Administrationstool scheint durchdacht und in der Bedienung durchweg logisch zu sein. Der Client konnte mangels Installationsmöglichkeit nicht getestet werden.

Massive Probleme traten jedoch aufgrund der mangelhaften Dokumentation auf, die eindeutig die schlechteste Dokumentation des Testfeldes ist. Fehlende Informationen und Hinweise an entsprechenden Stellen verhindern selbst bei schrittweisem Abarbeiten der Installationsanweisungen eine erfolgreiche Installation. Die Dokumentation ist in eine Benutzer- und eine Administratordokumentation getrennt, die jedoch beide oberflächlich bleiben und viele Lücken aufweisen. Die mitgelieferte Dokumentation trägt den Titel „Pointsec for Pocket PC 1.1" anstatt des erwarteten 1.3. Erst auf der CD findet man eine inhaltlich identische Dokumentation mit der richtigen Versionsnummer und neuen und farbigen Screenshots.

Der Support hinterlässt ebenfalls einen zwiespältigen Eindruck. So wollte man uns im Rahmen des Projektes keine aktuelle Version[128] zuschicken und verschwieg uns bei der alten Version die Inkompatibilität mit dem deutschen Betriebssystem, obwohl im Rahmen der groben Projektbeschreibung das deutsche Windows CE als Basis der Endgeräte angegeben wurde. Es bleibt unklar, wo hier Missverständnisse aufgetreten sind.

[128] Z. B. die brandneue Version 2.0 von Pointsec für PocketPC.

4.4.9.6 Kategorie Besondere Merkmale (+)

Die Zukunft von Pointsec scheint gesichert. Die neue Version 2.0 verspricht massive Verbesserungen, insbesondere auch volle Kompatibilität mit dem deutschen Windows CE. Anfang April 2003 wurde eine deutsche Niederlassung in Düsseldorf gegründet. So bleibt auch zu hoffen, dass bald eine deutschsprachige Version erscheint.

Die neue Version Pointsec for PocketPC 2.0 verspricht insbesondere Verbesserungen im Bereich der Verschlüsselung, dem von uns am meisten kritisierten Bereich. So soll dann eine über den AES realisierte transparente Echtzeitverschlüsselung von PIM Daten, E-Mails und ausgewählten sicheren Verzeichnissen möglich sein. Die uns zugeschickte Version 1.3 verfügt noch nicht über diese Features.

4.4.9.7 Gesamteinschätzung

In der uns vorliegenden Version 1.3 zeigt Pointsec bereits sehr gute Ansätze. Insbesondere die Authentifikation könnte mit dem in dieser Evaluation am besten benoteten FileCrypto mithalten und ihn eventuell sogar übertreffen. Das Administrationskonzept scheint durchdacht und bietet eine Oberfläche zur Erstellung der Policies, die bei FileCrypto vermisst wurde. Die Software versagt jedoch völlig in der Kategorie Sicherheit. Die Datenblätter der neuen Version 2.0 scheinen hier zumindest ein FileCrypto nahekommendes Niveau zu bieten. Der Bereich der Usability ist äußerst mangelhaft. Auch fehlende Referenzen für die PocketPC Software lassen hier zur Vorsicht raten. Ob das Potential die Mehrkosten rechtfertigt bleibt unklar.

Dennoch sollte für ein Folgeprojekt die Möglichkeit offen gehalten werden, die aktuelle Version von Pointsec einer praktischen Evaluation zu unterziehen. Pointsec scheint ein großes Potential zu besitzen und speziell auf das Enterpriseszenario zugeschnitten zu sein. Wenn es hält, was es auf dem Papier verspricht, könnte es einen Spitzenplatz[129] im Testfeld belegen.

[129] Allerdings nur in der Version 2.0.

4.4.10 SafeGuard PDA (ClientKonfig 07 + 15)

Als einzige der von uns getesteten Sicherheitslösungen für PocketPCs verfügt SafeGuard PDA über eine Zertifizierung mit dem „Designed for Microsoft Windows Pocket PC"-Logo. Wie bereits im Kapitel Komponentenauswahl (3.1.3.1.3) beschrieben, weist die Software eine deutliche Verbesserung der Anmeldeprozedur auf. SafeGuard PDA bietet in der von uns getesteten Version 1.00.1.2 einige teilweise hochinteressante und in unseren Augen wünschenswerte Alternativen zur Standardanmeldung wie die Symbol PIN oder die Anmeldung via biometrischer Handschriftenerkennung. Der Deutsche Hersteller Utimaco verfügt über umfangreiche Referenzen und Auszeichnungen, die sich jedoch alle auf die Desktop-Applikationen (Festplattenverschlüsselung, PKI) aus der SafeGuard-Familie beziehen.

4.4.10.1 Kategorie Administration (++)

Tabelle 4-104: SafeGuard - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	6
Zusammenarbeit mit Afaria	6

Auf der Website zum Produkt SafeGuard PDA wird massiv mit den Möglichkeiten zur zentralen Administration geworben, die allerdings nur in der Enterprise-Version enthalten sind. Diese war zum Testzeitpunkt noch nicht verfügbar. Wir hätten somit nur die Administrationsmöglichkeiten der Standardversion beurteilen können, mussten aber feststellen, dass es gar keine gibt. Auch fanden wir keine Möglichkeit einer dateibasierten Administration, weshalb die zentrale Administration mittels XTND oder Afaria ebenfalls nicht möglich war. Die von uns getestete Version von SafeGuard PDA wurde in der Kategorie Administration deshalb mit „ungenügend" bewertet.

Offen bleibt hierbei, inwiefern dieses Ergebnis auch für die angekündigte Enterprise-Version gelten würde. Es wird auf jeden Fall empfohlen, diese bei Verfügbarkeit zu evaluieren.

Gesamtbewertung Administration:	6

4.4.10.2 Kategorie Authentifikation (+++)

Tabelle 4-105: SafeGuard - Authentifikation

Kategorie Authentifikation	Bewertung
Art der Authentifikation	
PIN (ja/nein)	Nein
Erweiterte PIN (ja/nein)	Ja
Passwort / Passphrase (ja/nein)	Ja
Sicheres Passwort / Passphrase (ja/nein)	Nein
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	6
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja[130]
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Ja
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	3
Bei falscher Eingabe: Softlock (ja/nein)	Nein
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	s. Text
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Ja
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	4
Sicherheit der Authentifikation durch geringe Rückmeldung	2

[130] Mittels Windows CE Energieoptionen.

Die Software SafeGuard PDA verfügt über die wählbare Authentifizierungsart der erweiterten PIN. Der Hersteller Utimaco verwendet hierzu eine Sequenz von Symbolen (Hund, Blume, Haus etc.), die bei jedem Anmeldevorgang in unterschiedlicher Anordnung auf dem Anmeldebildschirm positioniert sind. Eine Anmeldesequenz kann aus 4-8 Symbolen bestehen. Zum einen hat die wechselnde Anordnung der Symbole gegenüber einer klassischen PIN-Eingabe den immensen Vorteil, dass ein potentieller Angreifer nicht bereits aufgrund der Bewegungen des Benutzers die tatsächliche Zugangs-PIN ausspähen kann. Zum anderen wird dem Benutzer durch die symbolbasierte Anmeldung das Merken seiner Anmeldesequenz erleichtert, da dieser sich beispielsweise eine eigene „Geschichte" ausdenken kann, die die zur Anmeldung notwendigen Symbole in einen kausalen Zusammenhang setzt und dann beim Anmelden lediglich „erzählt" werden muss.

Neben der Authentifizierung mittels Symbolsequenz ermöglicht SafeGuard PDA auch die Anmeldung durch handschriftliche Eingabe eines Wortes. Hierbei wird neben dem tatsächlichen Aussehen des geschriebenen Wortes auch der Schreibrhythmus ausgewertet. Ein potentieller Angreifer muss somit nicht nur das zu verwendende Wort kennen und die Handschrift des rechtmäßigen Besitzers nachbilden, sondern außerdem in der Lage sein, dessen Schreibrhythmus nachzuahmen. Das Erkennungsverfahren ist hierbei nach Aussagen von Utimaco nicht zertifiziert sondern eine Eigenentwicklung. Man war auch nicht bereit, uns die dahinter stehende Technologie genauer zu erläutern. Wir mussten feststellen, dass die Zugangsmethode „Handschrift" von SafeGuard PDA im Laborbetrieb einmal nicht reproduzierbar versagte und auch einer unbefugten Person die Anmeldung ermöglichte. Die Qualität dieses Authentifikationsverfahrens ist somit deutlich in Frage gestellt.

Neben den beiden erweiterten Authentifizierungsmöglichkeiten ist auch bei SafeGuardPDA die Anmeldung mit einem Passwort (4 - 32 Zeichen, beliebige Zusammensetzung) möglich. Außerdem wird bei der Installation von SafeGuard PDA ein Masterpasswort vergeben, mit dem ein durch ein vergessenes Passwort unbrauchbar gewordener PDA dennoch wieder freigeschaltet werden kann. Das Master-Passwort ist weiterhin auch zur Deinstallation der Software notwendig, wodurch dem Benutzer die Möglichkeit genommen wird, die Sicherheitsfunktionen komplett zu deaktivieren. Hierbei zeigten sich jedoch im Testbetrieb starke Unterschiede zwischen der Installation auf einem iPAQ h3970 und dem Modell h5450.

So akzeptierte das Programm auf einem iPAQ h5450 das einstellige Master-Passwort „a", auf einem h3970 war dagegen ein zumindest vierstelliges Master-Passwort erforderlich. Auch hier wurde jedoch das Master-Passwort „aaaa" akzeptiert. Diesem Umstand ließe sich durch die konsequente Umsetzung einer Passwort-Policy bei der Vergabe der Master-Passwörter durch die Administratoren begegnen.

Weitaus fragwürdiger erschien uns die angebotene Hardlock-Funktion. Wurden das Gerät auf dem h3970 noch erwartungsgemäß in den Auslieferungszustand zurückgesetzt und alle Daten im RAM gelöscht, wurde auf dem h5450 die Hardlock-Funktion aktiviert, nachdem eine unzulässige Anzahl falscher Anmeldeversuche durchgeführt worden war, das Gerät jedoch nicht wie erwartet in Auslieferungszustand zurückgesetzt, sondern lediglich die Software SafeGuard PDA deinstalliert.

Alle anderen auf dem PDA befindlichen Daten (PIM, Mail, etc.) befanden sich weiterhin, nun jedoch völlig ungeschützt, im RAM und waren für einen potentiellen Angreifer problemlos lesbar.

Insbesondere die Flexibilität der Anmeldeprozedur von SafeGuard PDA erschien uns durchaus dem typischen Einsatz von PDAs angemessen und das Anmeldeverfahren über Symbolsequenzen wirkt sehr durchdacht. Auch die mögliche Freischaltung des Gerätes mittels eines Masterpasswortes ist möglich, sollte im Produktiveinsatz jedoch nur unter Beachtung gesonderter Passwort-Policys genutzt werden. Die Abschaltung nach Inaktivität ist zwar möglich, muss aber mittels der Windows CE-eigenen Energieoptionen erfol-

gen, die vom Benutzer manipuliert und somit außer Kraft gesetzt werden können. Auch SafeGuard verhindert nicht das Erscheinen von Terminen vor der eigentlichen Anmeldung. Aufgrund der besonders guten Anmeldeprozedur entschieden wir uns im Falle der Verwendung auf dem iPAQ h3970 zu der Gesamtbewertung „gut". Wir raten jedoch eindeutig von der Verwendung der Anmeldung mittels Handschrifterkennung ab.

Gesamtbewertung Authentifikation:	**2**

4.4.10.3 Kategorie Kosten (+)

Tabelle 4-106: SafeGuard - Kosten

Kategorie Kosten	**Bewertung**
Einmalige Kosten	
Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Die reinen Anschaffungskosten sind mit 62,25 € auch für SafeGuard PDA als gering zu bezeichnen. Bis auf die Kosten für eventuell zu verwendende neue Versionen sind keine weiteren laufenden Kosten zu erwarten, deshalb wird SafeGuard PDA in der Kategorie Kosten mit „gut" bewertet.

Gesamtbewertung Kosten:	**2**

4.4.10.4 Kategorie Datensicherheit (+++)

Tabelle 4-107: SafeGuard - Datensicherheit

Kategorie Datensicherheit	**Bewertung**
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Ja
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Nein
E-Mail (ja/nein)	Nein

Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Ja
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Ja
Schutz vor unbefugter Deinstallation (ja/nein)	Ja

Tabelle 4-108: SafeGuard – Datensicherheit KO

Anzahl KO
Datensicherheit
Keine Möglichkeit PIM-Daten zu verschlüsseln

Das eigentliche Programm SafeGuard PDA führt keine Verschlüsselung von auf dem PDA befindlichen Daten durch. Im Lieferumfang der Software befindet sich auch das dafür benötigte Zusatzmodul PrivateCrypto, dessen Fähigkeiten sich jedoch auf das manuelle (für den Benutzer nicht transparente) Verschlüsseln ausgewählter Dateien nach dem AES-Algorithmus mit einer Schlüssellänge von 128 Bit beschränken. Es werden weder PIM Daten noch Mails oder gar der komplette PDA verschlüsselt, weshalb das Programm SafeGuard PDA für die von uns zu untersuchenden Zwecke nicht verwendbar ist. Ein sicheres Löschen von Dateien ist nur im Rahmen der Ver- bzw. Entschlüsselung möglich. Zudem wird eine eigene Implementierung des Verschlüsselungskerns verwendet, die nicht zertifiziert ist.

Da weder SafeGuard PDA noch das zugehörige Modul PrivateCrypto eine Möglichkeit bietet, die hochsensitiven PIM-Daten zu verschlüsseln, wird das entsprechende KO-Kriterium erfüllt. Die Sicherheit von SafeGuard PDA war somit als „ungenügend" zu bewerten.

Gesamtbewertung Datensicherheit:	**6**

4.4.10.5 Kategorie Usability (++)

Tabelle 4-109: SafeGuard – Usability 1

Kategorie Usability	**Bewertung**
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Ja
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Ja
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	1
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	1
Alle benötigten Informationen sind auf dem Bildschirm zu finden	3

Ausgaben sind zweckmäßig und verständlich	1
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	1
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	6
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	3
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	1
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	1
Aktueller Bearbeitungsschritt kann unterbrochen werden	1
Ein laufender Vorgang kann abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	1
Bearbeitungszeit abschätzbar	1
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwartetem Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	3
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen unmöglich	3
Bei Fehlern zweckmäßige Hinweise zur Ursache und Behebung	3
Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	2
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	1
Nur wenige Detailkenntnisse zur Bedienung nötig	1
Hilfestellung bei Bedarf verfügbar	6

Tabelle 4-110: SafeGuard – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	2
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Ja

Qualität des Administrationshandbuches	-
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	-
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	-
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	-
Qualität des Supports (soweit bewertbar)	-

Die Usability von SafeGuard PDA ist insgesamt überzeugend. Bis auf die auch hier vollständig fehlende Kontexthilfe existierten keine groben Unstimmigkeiten in der Benutzerinteraktion. Zu bemängeln ist lediglich, dass bei der Eingabe von Passwort und Master-Passwort keine Angaben zur erforderlichen Zusammensetzung oder Mindestlänge gemacht werden und dass auch bei Eingabe eines zu kurzen Passwortes kein Hinweis auf die Mindestlänge erfolgt. Außerdem wird vor der letztmaligen Möglichkeit der Passworteingabe vor einem Hardlock nicht davor gewarnt, dass bei Falscheingabe alle Daten verloren gehen.

Außerdem ist SafeGuard PDA mit dem h5450 inkompatibel. Auf dem h3970 funktioniert SafeGuard PDA erwartungsgemäß, doch auf dem h5450 erscheint, unabhängig von den gewählten Einstellungen, nach dem Einschalten grundsätzlich die Aufforderung zur Eingabe eines Passwortes. Es ist somit auf dem h5450 nicht möglich, die erweiterten Anmeldeprozeduren von SafeGuard PDA zu nutzen.

Gesamtbewertung Usability:	**2**

4.4.10.6 Kategorie Besondere Merkmale (+)

Tabelle 4-111: SafeGuard – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	3
Externe Referenzen/Erfahrungsberichte	3
Zukünftig zu erwartende Funktionalitätserweiterungen	2
Erwartungen Zukunftssicherheit	2

Zu SafeGuard PDA waren, im Gegensatz zu den anderen Lösungen des Herstellers Utimaco, keine externen Erfahrungsberichte oder Referenzen verfügbar. Die zum Testzeitpunkt bereits seit mindestens sechs Monaten angekündigte Enterprise-Version der Software lässt, ebenso wie die Ankündigung der Version 2.0, vermuten, dass der Hersteller an der Weiterentwicklung und Pflege von SafeGuard PDA arbeitet und dies auch in Zukunft tun wird, weist aber auf Probleme bei der Entwicklung oder zu frühzeitige Ankündigung hin. Dies ließ uns in dieser Kategorie eine nur „befriedigende" Bewertung abgeben.

Gesamtbewertung Besondere Merkmale:	**3**

4.4.10.7 Gesamtbewertung

Tabelle 4-112: SafeGuard - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	6
+++	Kategorie Authentifikation	-	2
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	1	6
++	Kategorie Usability	-	2
+	Kategorie Besondere Merkmale	-	3
	KO-Kriterien gesamt	**1**	

Da die Software SafeGuard PDA keine Möglichkeit bietet, PIM-Daten zu verschlüsseln, mussten wir in der als wichtig (+++) eingestuften Kategorie „Sicherheit" die Bewertung „ungenügend" abgeben, weshalb die Software auch in der Gesamtbewertung für untauglich befunden wird. Die ebenfalls „ungenügende" Bewertung in der Kategorie Administration bestätigt dies.

Für den Fall, dass der Hersteller die Software in Zukunft in diesen beiden Punkten entscheidend verbessert, wäre SafeGuard PDA durchaus zu empfehlen. Sowohl das Bedienkonzept als auch die erweiterte Anmeldemöglichkeit mittels Symbolsequenz überzeugten, die Anmeldung über Handschrifterkennung trotz des gelungenen Konzeptes hingegen leider nicht.

Aufgrund der genannten Schwächen insbesondere im Sicherheitsbereich lautet die Bewertung beim derzeitigen Stand der Software „ungenügend".

Gesamtbewertung SafeGuard PDA:	6

4.4.11 Sign On (ClientKonfig 08 + 16)

Da es sich bei SignOn um eine reine Authentifikationssoftware handelt, erfüllt sie prinzipiell nicht die Anforderungen an eine Sicherheitssoftware gemäß dieser Evaluation. Im Laufe der Evaluation des Testfeldes wurden jedoch massive Probleme bei den biometrischen Verfahren und allgemeine Schwächen der Authentifikationsmechanismen der Sicherheitslösungen offenbar. Deshalb wurde entschieden, SignOn in der aktuellen Version 2.01 als Alternative zu den bisher zum Einsatz gekommenen Biometrieansätzen vorzustellen, da es ebenfalls auf einem biometrischen Verfahren zur Handschriftenerkennung basiert.

4.4.11.1 Kategorie Administration (++)

Tabelle 4-113: SignOn - Administration

Kategorie Administration	Bewertung
Produkteigene Administrationsmöglichkeiten	
Vorschriften zur Verschlüsselung (ja/nein)	Nein
Vorschriften zur Verschlüsselung externer Medien (ja/nein)	Nein
Vorschriften für PIN/Passwort (ja/nein)	Nein
Vorschriften für sicherheitsrelevante Einstellungen (ja/nein)	Nein
Zentrale Verteilung von Updates (Sicherheitssoftware) (ja/nein)	Nein
Zentrale Verteilung von Updates (alle) (ja/nein)	Nein
Zentrales Key-Management (ja/nein)	Nein
Zentrale Schlüsselerstellung (ja/nein)	Nein
Profilverwaltung (ja/nein)	Nein
Integrationsmöglichkeiten mit externen Administrationslösungen	
Zusammenarbeit mit XTND	5
Zusammenarbeit mit Afaria	5

Produkteigene Möglichkeiten der Administration sind in dem kompakten SignOn nicht vorgesehen und der Ablauf der Zusammenarbeit mit Afaria sowie XTND ist unklar. Bei genauerer Recherche konnten 3 versteckte .CAB Dateien im Ordner auf dem Companion PC identifiziert werden[131]. Hierbei könnte es sich um z. B. über Afaria verteilbare Installationspakete handeln. Leider ist an keiner Stelle dokumentiert, welchen Inhalt diese 3 Pakete haben und wann genau welche Datei benutzt werden soll. Einflussmöglichkeiten auf die Policy oder Konfiguration des Programms konnten überhaupt nicht gefunden werden. Nur das Vorhandensein der Installationspakete verhindert eine schlechtere Wertung als „mangelhaft".

Gesamtbewertung Administration:	5

[131] Sign-On for Pocket PC.PPC300_2577.cab, Sign-On for Pocket PC.PPC300_4000.cab, Sign-On for Pocket PC.PPC300_10003.cab.

4.4.11.2 Kategorie Authentifikation (+++)

Tabelle 4-114: SignOn - Authentifikation

Kategorie Authentifikation	Bewertung
Art der Authentifikation	
PIN (ja/nein)	Ja
Erweiterte PIN (ja/nein)	Nein
Passwort / Passphrase (ja/nein)	Nein
Sicheres Passwort / Passphrase (ja/nein)	Nein
Falls vorhanden, Qualität biometrisches Verfahren Handschrifterkennung	2
Falls vorhanden, Qualität biometrisches Verfahren Fingerabdruckscanner	-
Zeitpunkt der Authentifikation	
Bei Einschalten des Gerätes (ja/nein)	Ja
In regelmäßigen Intervallen (ja/nein)	Nein
Nach Inaktivität (ja/nein)	Nein
Abschaltung nach Inaktivität (ja/nein)	Ja[132]
Bei Herstellen einer Active-Sync-Verbindung (ja/nein)	Nein
Bei Herstellen einer Infrarot-Verbindung (ja/nein)	Nein
Bei Herstellen einer Bluetooth-Verbindung (ja/nein)	Nein
Bei Herstellen einer WLAN-Verbindung (ja/nein)	Nein
Bei Herstellen einer GSM/GPRS-Verbindung (ja/nein)	Nein
Bei Start von Applikationen (ja/nein)	Nein
Beim Ändern der Einstellungen (ja/nein)	Nein
Sicherungsmechanismen	
Bei verlorenem/vergessenem Passwort: Freischaltung durch User	-
Bei verlorenem/vergessenem Passwort: Freischaltung durch Administrator	-
Bei falscher Eingabe: Softlock (ja/nein)	Nein
Bei falscher Eingabe: Sicherer Softlock (ja/nein)	Nein
Bei falscher Eingabe: Hardlock (ja/nein)	Nein
Bei falscher Eingabe: Wipe (ja/nein)	Nein
Bei falscher Eingabe: Verzögerung (ja/nein)	Nein
Bei falscher Eingabe: Sperrung. Freischaltung durch Masterkey oder ähnliches nötig (ja/nein)	Nein
Sonstiges	
Sicherheit durch geringe Einflussmöglichkeiten des Benutzers	6
Sicherheit der Authentifikation durch geringe Rückmeldung	3

[132] Nur mit Windows CE Energieoptionen.

Tabelle 4-115: SignOn – Authentifikation KO

Anzahl KO
Authentifikation
Bewertung von 5 oder 6 bei Einflussmöglichkeiten durch Benutzer
Keine erneute Authentifikation beim Ändern der Passworteinstellungen

Die Authentifikation über die biometrische Signatur bildet das Kernstück von SignOn. Die Handschriftenerkennung hat einwandfrei gearbeitet. Im Labor wurde kein Fall des Versagens beobachtet. Neben der biometrischen Signatur bietet SignOn eine 4-stellige PIN an. Diese kann nur in Verbindung mit der Signatur als zusätzliches bzw. alternatives Mittel verwendet werden[133]. Es gibt keinerlei Sicherungsmechanismen wie z. B. eine Verzögerung oder einen Masterkey, und SignOn kann komplett vom Benutzer deaktiviert werden. In diesem Zusammenhang ist es besonders kritisch, dass beim Ändern der Einstellungen zur Authentifikation keine erneute Authentifikation stattfindet. Es werden also zwei KO-Kriterien erfüllt, obwohl SignON in Werbeprospekten gerade im Bereich Authentifikation seine Stärken haben soll. Insgesamt kann nur ein „ungenügend" vergeben werden.

Gesamtbewertung Authentifikation:	6

4.4.11.3 Kategorie Kosten (+)

Tabelle 4-116: SignOn - Kosten

Kategorie Kosten	Bewertung
Einmalige Kosten	
Anschaffungskosten	2
Zusätzliche Kosten wg. besonderer Hardwareanforderungen	1
Laufende Kosten	
Zu erwartende Kosten für Updates etc.	2
Zusätzliche Kosten für längere Verbindungsdauer	1
Zusätzliche Kosten für Support-/Wartungsvertrag	1

Preislich bewegt sich die getestete SignOn Version mit 19,99 USD im unteren Feld der Testkandidaten. Damit ist hier die Note „gut" berechtigt.

Gesamtbewertung Kosten:	2

[133] Über logische AND und OR Verknüpfungen ähnlich den Möglichkeiten beim iPAQ h5450.

4.4.11.4 Kategorie Datensicherheit (+++)

Tabelle 4-117: SignOn - Datensicherheit

Kategorie Sicherheit	Bewertung
Kryptografische Algorithmen	
RC4 (ja/nein)	Nein
Rjindael / AES (ja/nein)	Nein
Toofish (ja/nein)	Nein
Blowfish (ja/nein)	Nein
TEA (ja/nein)	Nein
XOR (ja/nein)	Nein
Gegenstand der Verschlüsselung	
Kompletter PDA (ja/nein)	Nein
PIM-Daten (ja/nein)	Nein
E-Mail (ja/nein)	Nein
Externe Speichermedien (ja/nein)	Nein
Manuell ausgewählte Dateien/Verzeichnisse (ja/nein)	Nein
Backup-Dateien (ja/nein)	Nein
E-Mail-Anhänge (ja/nein)	Nein
Sonstige Sicherheitsaspekte	
FIPS 140-1 Zertifikat (ja/nein)	Nein
Sicheres Löschen von Dateien (ja/nein)	Nein
Schutz vor unbefugter Deinstallation (ja/nein)	Nein

Tabelle 4-118: SignOn – Datensicherheit KO

Anzahl KO
Sicherheit
Kein AES oder vergleichbar starker Algorithmus
Keine Möglichkeit PIM-Daten zu verschlüsseln
Keine Möglichkeit verschlüsselte Dateien abzulegen

Wie eingangs erwähnt ist SignOn ein reines Authentifikationsprodukt. Abseits der biometrischen Signatur gibt es keinerlei Sicherheitsfeatures. Damit versagt SignOn in der Kategorie Datensicherheit völlig.

Gesamtbewertung Sicherheit:	6

4.4.11.5 Kategorie Usability (++)

Tabelle 4-119: SignOn – Usability 1

Kategorie Usability	Bewertung
Sprache	
Verfügbar in deutscher Sprache (ja/nein)	Nein
Verfügbar in englischer Sprache (ja/nein)	Ja
Verfügbar in weiteren Sprachen (ja/nein)	Nein
Aufgabenangemessenheit	
Software ist zielgerichtet ohne überflüssige Arbeitsschritte	2
Daten können wie von der Aufgabe gefordert eingegeben werden	1
Informationen und Bedienelemente befinden sich am richtigen Platz	3
Alle benötigten Informationen sind auf dem Bildschirm zu finden	3
Ausgaben sind zweckmäßig und verständlich	1
Wiederholfunktion für wiederkehrende Arbeitsschritte verfügbar	1
Selbstbeschreibungsfähigkeit	
Bei Bedarf Kontexthilfe oder weitergehende Informationen abrufbar	5
Meldungen sind sofort verständlich	1
Rückmeldungen könne einer Ursache eindeutig zugeordnet werden	1
Art und Zusammensetzung geforderter Eingaben leicht erkennbar	2
Auswirkungen von Aktionen hinreichend ersichtlich	1
Aktuelle Eingabeposition eindeutig hervorgehoben	1
Art der Rückmeldung (Fehler/Warnung/etc.) eindeutig erkennbar	1
Steuerbarkeit	
Leichter Wechsel zwischen verschiedenen Bearbeitungsbildschirmen	2
Aktueller Bearbeitungsschritt kann unterbrochen werden	2
Ein laufender Vorgang kann abgebrochen werden	1
Erwartungskonformität	
Bearbeitungsschritte vorhersagbar	2
Bearbeitungszeit abschätzbar	1
Einheitliche Verwendung von Begriffen und Symbolen	1
Die Ausführung einer Operation führt zu erwarteten Ergebnis	1
Fehlerrobustheit	
Sicherheitsabfrage vor Durchführung kritischer Operationen	1
Eingaben werden auf syntaktische Korrektheit geprüft	1
Versehentliches Auslösen von Aktionen unmöglich	1
Bei Fehlern zweckmäßige Hinweise zu Ursache und Behebung	1

Im Testbetrieb kein Auftreten von Abstürzen oder Systemfehlern	1
Erlernbarkeit	
Schnelles Erlernen der Bedienung	1
Intuitive, selbsterklärende Benutzung möglich	1
Nur wenige Detailkenntnisse zur Bedienung nötig	1
Hilfestellung bei Bedarf verfügbar	5

Tabelle 4-120: SignOn – Usability 2

Programmexterne Hilfestellungen	
Qualität des Benutzerhandbuches	5
Benutzerhandbuch verfügbar in deutscher Sprache (ja/nein)	Nein
Benutzerhandbuch verfügbar in englischer Sprache (ja/nein)	Ja
Benutzerhandbuch verfügbar in weiteren Sprachen (ja/nein)	Nein
Qualität des Administrationshandbuches	-
Administrationshandbuch verfügbar in deutscher Sprache (ja/nein)	-
Administrationshandbuch verfügbar in englischer Sprache (ja/nein)	-
Administrationshandbuch verfügbar in weiteren Sprachen (ja/nein)	-
Qualität des Supports (soweit bewertbar)	3

Aufgrund der Kompaktheit des Programmes fällt auch die Usability in weiten Teilen zufriedenstellend aus. Neben FileCrypto ist SignOn das einzige Programm im Testfeld, das den Eintrag „Kennwort" in der Systemsteuerung auf dem Handheld wirklich ersetzt. Statt jedoch wie FileCrypto hinter „Kennwort" das eigene Konfigurationsprogramm zu setzen, löscht SignOn den Eintrag komplett und legt stattdessen einen neuen Eintrag unter eigenem Namen an die Stelle. Genauso erfreulich ist die einschaltbare Statusmeldung nach erfolgreichem Login, die über in der Zwischenzeit stattgefundene fehlgeschlagene Loginversuche berichtet. So wird schnell deutlich, wenn Unbefugte (erfolglos) versucht haben, sich anzumelden. Andere Details in der Usability lassen jedoch insgesamt einen zwiespältigen Eindruck entstehen: Buttons, die sich nicht an den erwarteten Stellen befinden oder Felder die scheinbar aktiviert sind, beim Anklicken jedoch nicht reagieren.

Das Handbuch ist nicht mehr als eine Minimalinstallationsanleitung, die zudem ein sehr unübersichtliches Layout aufweist und viele Informationen vermissen lässt.

Die der Signaturanalyse zugrunde liegende Technologie scheint zudem nicht von einer unabhängigen Stelle zertifiziert worden zu sein. Zumindest finden sich in der Dokumentation keinerlei Hinweise darauf. So bleibt insgesamt nur ein „ausreichend" als Bewertung.

Gesamtbewertung Usability:	**4**

4.4.11.6 Kategorie Besondere Merkmale (+)

Tabelle 4-121: SignOn – Besondere Merkmale

Kategorie Besondere Merkmale	Bewertung
Deckung der Testergebnisse mit Prospekten	3
Externe Referenzen/Erfahrungsberichte	4
Zukünftig zu erwartende Funktionalitätserweiterungen	4
Erwartungen Zukunftssicherheit	4

Externe Referenzen sind spärlich. Die auf der Homepage des Herstellers aufgeführten Pressehinweise beschränken sich auf andere Produkte als die PocketPC Variante und verzeichnen keinerlei Awards oder euphorisch klingende Zitate aus Tests, wie sie bei anderen Herstellern zu Marketingzwecken weit verbreitet sind. Es ist unklar, wie stark sich SignOn auf dem PocketPC verbreiten wird. Demzufolge sind Zukunftssicherheit und Weiterentwicklung des Produktes skeptisch zu betrachten. Die angebliche Stärke von SignOn, die Benutzerauthentifikation, wurde sehr schlecht umgesetzt, obwohl das biometrische Verfahren an sich zu funktionieren scheint. Insgesamt reicht es deshalb nur zu einem „ausreichend".

Gesamtbewertung Besondere Merkmale:	4

4.4.11.7 Gesamtbewertung

Tabelle 4-122: SignOn - Gesamtwertung

	Gesamtbewertung	KO	Note
++	Kategorie Administration	-	5
+++	Kategorie Authentifikation	2	6
+	Kategorie Kosten	-	2
+++	Kategorie Sicherheit	3	6
++	Kategorie Usability	-	4
+	Kategorie Besondere Merkmale	-	4
	KO-Kriterien gesamt	**5**	

SignOn ist selbst in der Kernkompetenz des Programmes sehr mangelhaft. Zwar scheint die biometrische Authentifikation zu funktionieren, abseits dessen bietet die Software jedoch absolut nichts an. Sie versagt mangels Sicherheitsmechanismen auch bei den restlichen Authentifikationskriterien, es gibt keinerlei Administrationsschnittstellen und Datensicherheit sowie Verschlüsselung sind der Software fremd. Selbst in der Usability gibt es einige schwerwiegende Schwächen. Insgesamt muss insbesondere aufgrund der Bedeutung der Kriterien Authentifikation und Sicherheit ein „ungenügend" ausgesprochen werden.

Gesamtbewertung Sign On:	6

5 Empfehlung

In diesem Abschnitt betrachten wir das Gesamtsystem, das aus unserer Sicht bei der Verwendung von PocketPC Handhelds zum Einsatz kommen sollte.

Dabei wird versucht, das System sinnvoll und so weit wie möglich auf die vorgegebene Infrastruktur des Auftraggebers abzustimmen. Beispielsweise entfällt bei dieser Betrachtung die Möglichkeit einer direkten Einwahl in die DMZ über einen RAS-Dienst. Die folgenden Grafik gibt einen Überblick über das Gesamtsystem.

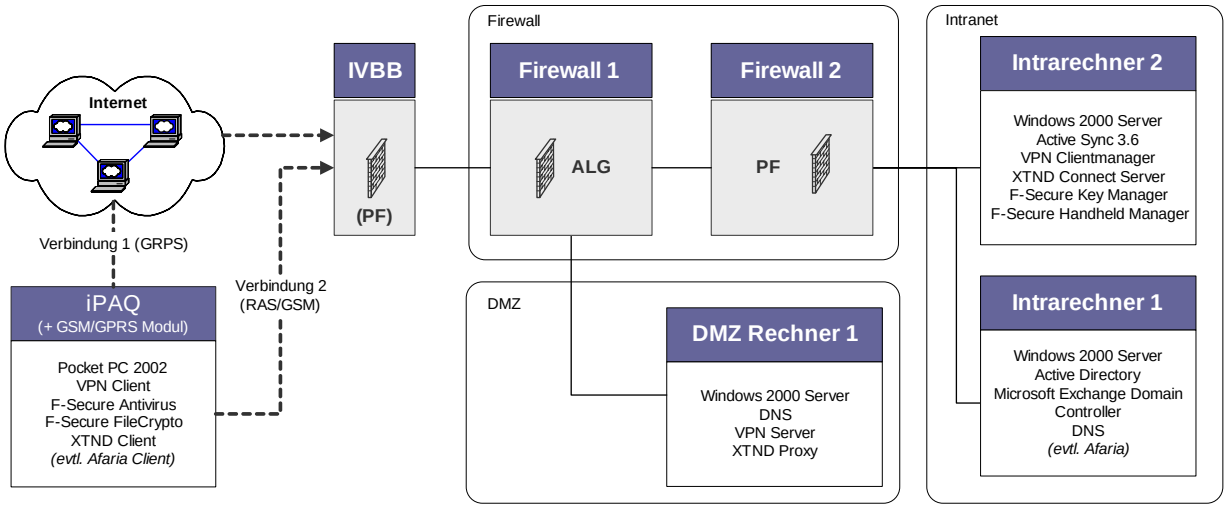

Abbildung 5-1: Gesamtsystem

Als Synchronisationskomponente wird XTND verwendet.

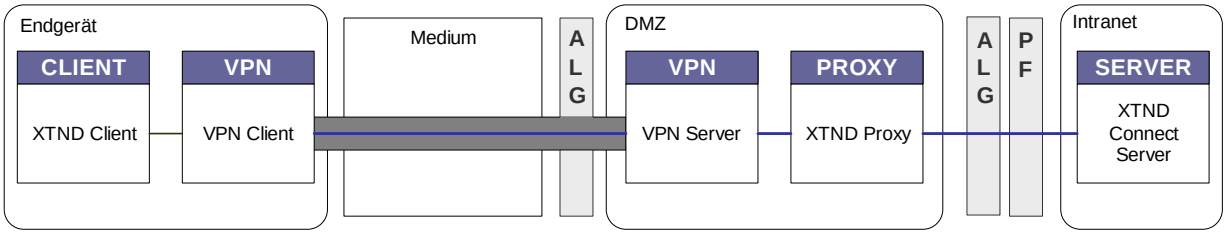

Abbildung 5-2: Synchronisationskomponente

Die Administration der Endgeräte kann mit XTND allein oder aber durch den Einsatz von Afaria bewerkstelligt werden. Hier gilt es zu entscheiden, ob die erweiterten Administrationsfunktionen von Afaria trotz fehlender Proxykomponente in Anspruch genommen werden sollen.

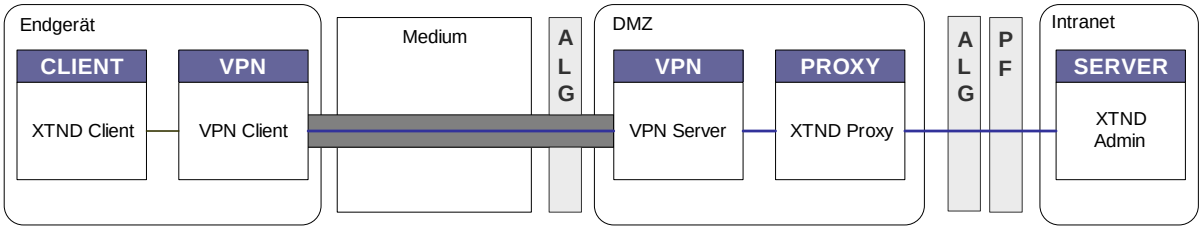

Abbildung 5-3: Administrationsvariante 1: XTND

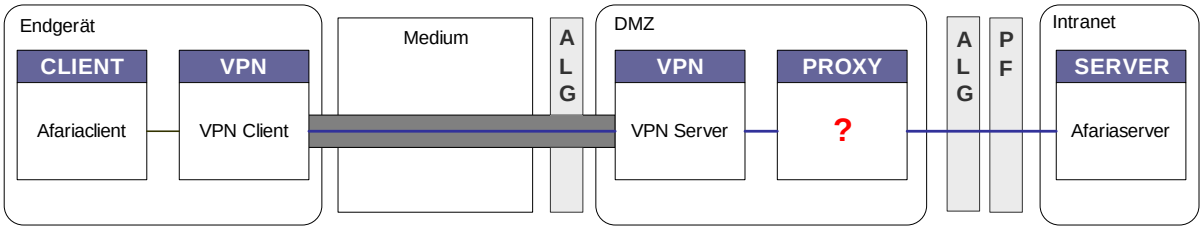

Abbildung 5-4: Aministrationsvariante 2: Afaria – ABER: „Das Afariaproblem"

Für den Einsatz der RAS Einwahl über den Informationsverbund Berlin-Bonn (IVBB) sollte dieses Szenario ebenfalls Bestand haben, da sich an der Systematik in der DMZ und dem Intranet nichts ändern würde. Eventuell wird jedoch eine zweite VPN Konfiguration nötig, die dann vom Benutzer manuell auf dem VPN Client (Handheld) vor Synchronisation anwählen muss.

5.1 Die Komponenten

Hier eine Darstellung der verwendeten Komponenten und der notwendigen Konfigurationen:

5.1.1 Endgerät

Als Endgeräte werden iPAQs der Version h3970 verwendet. Zusätzlich sind diese Geräte mit einem GPRS/GSM-Jacket ausgestattet. Folgende Softwarepakete werden auf den Endgeräten eingesetzt:

- PocketPC 2002

  Das PocketPC-Betriebsystem muss so eingerichtet werden, dass in Zusammenarbeit mit dem GPRS/GSM-Jacket oder einem Companion-PC eine Internetverbindung bzw. eine RAS-Einwahl möglich ist.

- VPN Client

  Der VPN Client wurde nach Vorgaben des Auftraggebers ausgewählt und entsprechend konfiguriert

- F-Secure Antivirus

  F-Secure Antivirus ist als Standard installiert und wird in regelmäßigen Abständen via Administrationssoftware mit aktuellen Virensignaturen, die vom Handheld Manager bereitgestellt werden, versorgt.

- F-Secure Filecrypto

  F-Secure Filecrypto kann bis in kleinste Details konfiguriert werden. Folgende Einstellungen werden empfohlen:

  - Alle Dateien, die der Software zugänglich sind, mit höchster Sicherheit verschlüsseln
  - Nutzung von Passphrases um Brute-Force-Attacken zu unterbinden
  - Bei längerer Inaktivität des Gerätes im eingeschalteten Zustand die Dateien verschlüsseln und einen erneuten Login fordern
  - Bei mehrfacher Eingabe eines falschen Passwortes einen Wipe auslösen

- XTND-Client

  Der von uns etablierte VPN-Tunnel endet in der DMZ. Innerhalb der DMZ ist der XTND-Proxy installiert. Der Client ist so zu konfigurieren, dass er am Ende des VPN-Tunnels den XTND-Proxy findet und eine Verbindung mit diesem herstellen kann. Zusätzlich sollte verhindert werden, dass der Endbenutzer das einzugebende Passwort, das zur Anmeldung erforderlich ist, speichern kann.

- Afaria-Client

  Wie bei dem XTND-Client endet die VPN-Verbindung in der DMZ. Von dort aus wird die Anfrage des Afaria-Clients in das Intranet weitergeleitet. Der Afaria-Client darf zum einen nicht in den „Invisible Mode" geschaltet werden, was das Erscheinen des Clients bei einer Verbindung via ActiveSync unterbindet, und es darf nicht zugelassen werden, dass das Login-Passwort gespeichert wird. Außerdem sollte für den Benutzer ein Default Channel bzw. Channel-Set eingestellt werden.

5.1.2 Informationsverbund Berlin-Bonn (IVBB)

Der IVBB müsste entweder einen VPN-Tunnel-Aufbau durch sämtliche eigenen Sicherheitsstrukturen hindurch ermöglichen oder selbst den VPN-Server stellen, dann wären weitere Maßnahmen erforderlich. Vom IVBB aus müsste dann eine sichere Verbindung bis in die DMZ des BMI aufgebaut werden. In unserer Betrachtung wird der IVBB in Abstimmung mit dem Auftraggeber jedoch wie ein gewöhnlicher Internet-Provider behandelt und demzufolge keiner gesonderten Untersuchung unterzogen.

5.1.3 Firewall

Die einzelnen Komponenten der Firewall sind entsprechend unseres Gesamtsystems wie folgt anzupassen.

- ALG

  Der Application Level Gateway (ALG) ist so zu konfigurieren, dass er eingehende VPN-Verbindungen auf den entsprechenden Port in die DMZ weiterleitet. Das in der DMZ liegende Gegenstück auf diesem Port ist der VPN-Server. Auf dem ALG müssen Proxies derart konfiguriert werden, dass ein Datentransport von der DMZ ins Intranet für die Applikationen XTND und Afaria möglich ist.

- Paketfilter

  Am Paketfilter müssen die für XTND und Afaria eingerichteten Ports geöffnet werden.

5.1.4 DMZ

Die in der demilitarisierten Zone notwendigen Komponenten und Einstellungen sind:

- DNS

  Der DNS in der DMZ muss den im Client eingetragenen Servernamen zu der IP-Adresse der XTNDConnect Proxy Komponente bzw. zur IP-Adresse des Afaria-Servers im Intranet auflösen. Dies ist für den im Abschnitt „Standorte und Servernamen" eingeführten DNS-Dummy notwendig.

- Portforwarder

  In der DMZ muss ein Port-forwarding realisiert werden, da zur Steigerung der Usability nur ein einziger in der DMZ endender VPN-Tunnel verwendet wird. Der Portforwarder leitet dabei Datenpakete, die an den Afaria-Server gerichtet sind mangels eigener Proxykomponente direkt in das Intranet weiter.

- VPN-Server

  Der VPN-Server muss derart konfiguriert werden, dass er von den Clients eingehende Verbindungen authentifiziert und akzeptiert und Antworten des Servers wieder über den VPN-Tunnel zum Client liefert.

- XTND-Proxy

  Der XTND-Proxy wird auf einem Rechner innerhalb der DMZ installiert. Der Proxy muss eine Verbindung zum XTND-Server herstellen können. Dazu muss ein Port im Paketfilter der Firewall geöffnet werden. Um die Sicherheit so weit wie möglich zu erhöhen, sollte die SSL-Verbindung zwischen DMZ und Server aktiviert werden.

5.1.5 Intranet

Innerhalb des Intranets sind zusätzliche Server und einige Konfigurationen notwendig.

- Active Directory

  Das Active Directory steht hier stellvertretend für eine zentrale Nutzerverwaltung im Intranet. Wichtig ist an dieser Stelle, dass für den XTND Server ein Konto eingerichtet wird, das mit administrativen Rechten für Exchange ausgestattet ist. Außerdem ist es sinnvoll, eine Gruppe für alle mobilen Nutzer zu definieren, um wenigstens eine differenzierte Vergabe von Rechten realisieren zu können.

- Microsoft Exchange

  Zwar sind Szenarien für den mobilen Zugriff in der Grundkonfiguration von Exchange bereits realisierbar, dennoch empfehlen wir Exchange für den Zugriff von mobilen Nutzern speziell zu konfigurieren. Exchange stellt hierfür zahlreiche Mechanismen wie Rechteverwaltung, verschiedene Exchange-Domänen, Replikation etc. zur Verfügung. Eine tiefgehende Betrachtung dieser Mechanismen konnte innerhalb dieses Projektes nicht durchgeführt werden.

- DNS

  Der DNS im Intranet sollte derart konfiguriert werden, dass er den im Client angegebenen Servernamen (z. B. „XTND" bzw. „Afaria") zu dem jeweiligen Server im Intranet auflöst.

- ActiveSync

  ActiveSync wird benötigt, um zumindest die Clientsoftware der Administrationssoftware auf dem PDA zu installieren. Eventuell ist hier eine Speicherkarten-Lösung mit Duplikation einer Referenzinstallation besser für den täglichen Einsatz geeignet.

- (VPN-Clientmanager)

  Ein im Rahmen der betrachteten VPN-Lösung zur Verfügung gestellter Clientmanager könnte im Intranet das Aufspielen der VPN Clients realisieren. Hier steht zu überlegen, ob eine Speicherkarten-Lösung mit Duplikation einer Referenzinstallation besser für den täglichen Einsatz geeignet ist.

- Extended Connect Server

  Der XTND-Server muss innerhalb des Intranet installiert werden. Er nimmt die Verbindungsanfragen der Endgeräte über den in der DMZ installierten Proxy entgegen. Die Anfragen werden entsprechend aufbereitet und an den MS Exchange Server weitergeleitet. Der XTND-Server muss Zugriff auf das Active Directory haben, damit eine Authentifikation der Endbenutzer möglich ist (second tier). Der XTNDConnect Server verhält sich dabei gegenüber dem Exchange-Server wie ein gewöhnlicher Outlook-Client. Damit der XTNDConnect Server die notwendigen CDO-Objekte nutzen kann, muss auf dem Rechner, auf dem der XTNDConnect Server läuft, Microsoft Outlook installiert und mindestens einmal in Verbindung mit dem Exchange-Server genutzt worden sein.

  XTND läuft als Windows-Dienst und muss unter einem Benutzerkonto mit Domänen-Administrationsrechten laufen.

- Afaria Server

  Der Afaria Server wird in Verbindung mit einer Datenbank benutzt. Während zu Evaluationszwecken der MSDE benutzt wurde, ist für den produktiven Einsatz eine MS-SQL oder eine Oracle Datenbank nötig. Afaria benötigt Zugang zum Active Di-

rectory, um Benutzer authentifizieren zu können. Der Server ist als Windows-Dienst realisiert und benötigt lediglich ein gültiges Benutzerkonto unter dem er läuft.

- F-Secure Key Manager

  Der Key Manager ist für die hier betrachtete Sicherheitslösung FileCrypto vorgesehen. Er erzeugt ein Installationspackage und zugehörige Schlüssel und Passwörter. Diese Packages sind expilizit dafür ausgelegt, über Admistrationslösungen wie XTND und Afaria verteilt zu werden.

- F-Secure Handheld Manager

  Der Handheld-Manager ist eines von zwei Zusatztools von F-Secure. Im Intranet aktualisiert er die Virensignaturen für das Antivirusprogramm (verteilbar sind diese dann über eine Administrationssoftware). Der Handheld Manager sollte so konfiguriert sein, dass er Zugriff auf das Internet hat und die jeweils aktuellen Signaturen in einem von Afaria bzw. XTND aus zugänglichen Ordner ablegt.

5.2 Betrachtung des Funktionalitätsumfangs

In diesem Abschnitt erfolgt eine Beschreibung des Funktionalitätsumfangs der empfohlenen Lösung bezüglich Synchronisation und Administration durch XTND oder Afaria.

5.2.1 Umfang der Synchronisation

Bei der Synchronisation der von Exchange verwalteten Groupware-Daten ist zu beachten, dass der verfügbare Messaging-Client Pocket Outlook gegenüber dem regulären Outlook erhebliche Einschränkungen aufweist und nicht den gewohnten Leistungsumfang von Outlook in Kombination mit dem zentralen Exchange-System bietet.

- E-Mails

  Bei der Synchronisation von E-Mails werden per Default lediglich direkte Inhalte des Posteingangsordners synchronisiert. Die Synchronisation von Unterordnern kann zwar konfiguriert werden, bedarf aber eines enormen Aufwandes, so dass selbst die Firma Extended Systems davon abrät. Um alle E-Mails, also auch jene in den Unterordnern des Posteingangsfaches, synchronisieren zu können, muss man zusätzliche E-Mail-Accounts speziell für die mobile Synchronisation einrichten. Innerhalb dieser E-Mail-Accounts dürfen dann keine Unterordner angelegt werden, sondern alle E-Mails müssen direkt im Posteingangsordner abgelegt sein. Es ist also keine Abbildung der Organisations- und Ablagestruktur am Arbeitsplatzrechner im Intranet auf dem iPAQ möglich.

- Termine

  Die Terminverwaltung ist bis auf wenige Einschränkungen gut einsetzbar und bietet nahezu alle Funktionen, die das vollwertige Outlook am Arbeitsplatzrechner zur Verfügung stellt. Lediglich wenn man erweiterte Dienste wie die Terminanberaumungen oder Zugriff auf fremde Kalender benutzen möchte, stößt man auf Grenzen.

- Kontakte

  Per Default werden nur die persönlichen Kontakte synchronisiert. Man kann mittels XTND auch öffentliche Kontakteordner zur Synchronisation freigeben. Da nur vollständige Ordner abgeglichen werden können und nicht gezielt einzelne Kontakte, ist von der Synchronisation des gesamten Kontaktbestandes abzuraten, da dies den Speicher auf dem PDA übersteigen würde. Benutzer können entweder Kontakte, die sie auf dem iPAQ verfügbar haben wollen, in ihre persönlichen Kontakte kopieren oder aber es werden durch die Administratoren spezielle Kontakteordner für die Synchronisation erstellt.

- Aufgaben

  Bei der Verwaltung von Aufgaben besteht die hauptsächliche Einschränkung darin, dass PocketOutlook nicht zwischen eigenen Aufgaben und Aufgaben, die an andere zugewiesen wurden, unterscheiden kann. Beide Arten von Aufgaben werden gleich dargestellt und behandelt.

- Notizen

  Die Synchronisation von Notizen funktioniert einwandfrei.

- Öffentliche Ordner

  Die Synchronisation von öffentlichen Ordnern ist aufgrund des begrenzten Speichers auf den Endgeräten und der Unfähigkeit, alle Dateitypen zu interpretieren, nur begrenzt sinnvoll. Stattdessen sollte man für einzelne Benutzer oder Benut-

zergruppen administrationsseitig Ordner einrichten, die ausgewählte Dokumente aus den öffentlichen Ordnern enthalten.

5.2.2 Funktionsumfang der Endgeräteadministration

Als Administrationslösung stellen sich zwei Möglichkeiten: die Administration nur mittels XTND oder unter zusätzlichem Einsatz von Afaria.

An dieser Stelle ist es nicht notwendig, den gesamten Funktionalitätsumfang von XTND oder Afaria zu dokumentieren. Es wird ein Überblick über die Möglichkeiten gegeben.

Afaria erfüllt die Ansprüche an eine Administrationskomponente besser als XTND. Afaria ermöglicht u. a. ein dezidierteres Logging, eine genauere Bestandsaufnahme der vorhandenen Endgeräte und Systeminformationen.

Durch eine eigene Scriptsprache ist bei Afaria eine SQL-ähnliche Abfrage möglich. Anhand verschiedener Abfragekriterien kann man einen guten Überblick über die Informationen zu den sich im Umlauf befindlichen Endgeräte gewinnen, von Besitzerinformationen bis hin zu installierter Software.

Durch die vorgefertigten Dialoge von Afaria lassen sich die wichtigsten Betriebssystemeinstellungen wie Verbindungs-, DNS/IP- und Netzwerkkonfigurationen der Endgeräte bequem remote konfigurieren.

Die Verteilung von Dokumenten und Inhalten kann mit Afaria besser und differenzierter erfolgen als mit XTND.

Auch Softwarepakete lassen sich mit Afaria besser vorkonfigurieren und verteilen als mit XTND. Hierbei können Pakete über mehrere Sessions verteilt überspielt werden, so dass die einzelnen Verbindungszeiten vom Endbenutzer kürzer gestaltet werden können.

Beide Administrationslösungen bieten die Möglichkeit, differenzierte Backups der Endgeräte zentral anzulegen.

Aufgrund des umfassenderen Funktionsumfangs zur Verwaltung und Administration, empfehlen wir ab einer Anzahl von 100 Endgeräten den Einsatz von Afaria.

5.3 Betrachtung der Sicherheit

Im Folgenden wird das von uns entwickelte Gesamtsystem auf seine Sicherheitseigenschaften hin untersucht. In der Betrachtung gehen wir von einer Variante mit dem Einsatz von Afaria als Managementkomponente aus. Falls aus Sicherheitsgründen aufgrund der fehlenden Proxy-Komponente auf den Einsatz von Afaria verzichtet wird, entfallen die entsprechenden Bedrohungsszenarien.

Für die Untersuchung der Bedrohungsszenarien haben wir die Darstellung als „Angriffsbaum" („attack tree") gewählt. Diese Methode geht auf den Sicherheitsexperten Bruce Schneier zurück, der diese Methode entwickelt hat (Schneier 1999). Der entwickelte Angriffsbaum befindet sich im Anhang in Kapitel 7.4.

Attack trees ermöglichen es, Angriffsszenarien auf IT-Systeme systematisch darzustellen und sich dadurch einen umfassenden Überblick über die Sicherheit eines Systems zu verschaffen. Wissenschaftler an der TU München haben die Methodik der attack trees aufgegriffen und diese auf mobile Systeme übertragen (Baumgarten 2001).

Der hier benutzte attack tree erhebt dabei allerdings weder den Anspruch auf Vollständigkeit noch strukturelle Korrektheit. Wir haben mit dem Ziel, die aus unserer Sicht bedeutendsten Bedrohungen zu identifizieren, einen bewusst pragmatischen Ansatz gewählt. Andere wichtige Bedrohungen sind in unserer Analyse nicht berücksichtigt, beispielsweise das „social engineering", die Beeinflussung des Endgerätebenutzers zur Preisgabe von sensiblen Daten.

Zusammengefasst stellen aus unserer Sicht folgende Bedrohungsszenarien die größten Risiken für den Einsatz des Gesamtsystems dar. In den Klammern wurde dabei jeweils eine Einordnung in die Struktur des Grundschutzhandbuchs des BSI vorgenommen.

- Verlust/Diebstahl des Endgeräts (Ebene IT-Systeme und übergreifende Aspekte)
- Manipulation der Software und Hardware (Ebene IT-Systeme)
- Bedrohung durch Trojaner und Viren (Ebene IT-Systeme und übergreifende Aspekte)
- Unzureichende Identifikation des Benutzers und des Gerätes (Ebene Übergreifende Aspekte)
- Angriffe auf Kommunikationsverbindungen (Ebene Netze).

5.3.1 Endgerät

5.3.1.1 Operating System (OS)

Bedrohung: Sniffer, Trojaner und Viren können auf unterschiedlichste Weise das Betriebssystem infiltrieren, beispielsweise durch Mail-Anhänge oder durch den Endbenutzer leichtsinnig nachinstallierte Software. Sniffer und Trojaner dienen vor allem dazu, Informationen auf dem Endgerät oder, bei Übertragung, Daten und/oder Passwörter aus dem Firmennetz auszuspionieren. Viren haben hingegen meist einen zerstörerischen Charakter und versuchen in der Regel, Daten bzw. das System unbrauchbar zu machen.

Maßnahme Technik: Solche Bedrohungen kann man in vielen Fällen mit Virenscannern und Portblockern abwehren. Dazu ist es vor allem notwendig, in regelmäßigen Abständen aktuelle Virensignaturen für den Virenscanner zu beschaffen.

Maßnahme Policy: Um eine Infizierung zu vermeiden, müssen Endbenutzer für das Thema sensibilisiert werden. Dazu gehört z. B. das Prinzip, dass Mail-Anhänge von unbekannten Absendern nicht geöffnet werden. Ebenso sollte es unterbunden werden, dass

Endbenutzer eigenmächtig Software auf dem Gerät installieren, auch wenn das breite Angebot an, unter Umständen auch kostenfreier, Software im Internet dazu verleitet.

5.3.1.2 Hardware

Bedrohung: Wenn ein Endgerät durch Verlust oder Diebstahl in die Hände eines potentiellen Angreifers gerät, kann dieser durch Aufschrauben des Gerätes und Auslesen des Speicherinhaltes an sensible Daten und Passwörter gelangen. Wir gehen hier davon aus, dass das Gerät via Power-On-Password geschützt ist.

Maßnahme Technik: Um solche Angriffe und Bedrohungen abzuwehren ist es notwendig, die Inhalte des Gerätes bei der Speicherung zu verschlüsseln. Hierzu wurde geeignete Software vorgestellt.

Maßnahme Policy: Die Benutzer sollten die Geräte nicht unbeaufsichtigt liegen lassen und bei Transport möglichst dicht am Körper tragen.

5.3.1.3 Authentifizierung

5.3.1.3.1 Beobachtung der Person

Bedrohung: Beobachtung des Benutzers während des Umgangs mit dem Gerät kann Dritten Passwörter und Inhalte preisgeben.

Maßnahme Policy: Endbenutzer müssen für diese Problematik sensibilisiert werden.

5.3.1.3.2 Biometrie umgehen

Bedrohung: Es ist möglich, die biometrischen Authentifikationsmechanismen zu umgehen und zu täuschen, so dass die Gefahr eines Zugriffs auf das Endgerät und dadurch die Erlangung von Nutzdaten und/oder Kennwörtern besteht.

Maßnahme Technik: Um dies zu verhindern, sollte Zusatzsoftware eingesetzt werden. Die Authentifizierung anhand von Biometriemerkmalen sollte um Passwörter/PINs oder Smartcards erweitert werden.

Maßnahme Policy: Die Benutzer sollten darauf aufmerksam gemacht werden, dass die derzeitigen biometrischen Authentifizierungsverfahren noch unsicher sind und dass die Verwendung von zusätzlichen Sicherheitsmaßnahmen notwendig ist.

5.3.1.4 Applikation

5.3.1.4.1 Ausnutzen von Bugs

Bedrohung: Bugs in Applikationen (z. B. PocketOutlook, Synchronisationssoftware usw.) werden häufig ausgenutzt, um Nutzdaten und/oder Kennwörter zu erlangen.

Maßnahme Technik: Regelmäßige Updates/Wartung durch das IT-Management (evtl. mit Hilfe der Administrationskomponente) und Wartungsverträge mit Herstellern helfen dieses Risiko zu verringern.

5.3.1.4.2 Extraktion von Kennwörtern aus dem Filesystem

Bedrohung: Viele Applikationen erfordern das Eingeben von Kennwörtern. Allerdings ist nicht immer sichergestellt, dass diese Kennwörter mit ausreichend sicheren Verfahren verschlüsselt abgelegt werden. Unter Umständen kann ein Angreifer durch einen direkten Zugriff auf die relevanten Dateien die Kennwörter extrahieren oder entschlüsseln.

Maßnahme Technik: Wir empfehlen den Einsatz von Zusatzsoftware zur Verschlüsselung des Dateisystems.

Maßnahme Policy: Mitarbeiter sollten verpflichtet werden, Kennwörter nicht abzuspeichern.

5.3.2 Netzwerke

5.3.2.1 Öffentlich

Öffentliche Netze werden z. B. auf Messen, in Hotels und bei der Einwahl über unabhängige ISP genutzt. Ein weiteres wichtiges „öffentliches Netz" stellen die eingebauten Nahverkehrsnetze Bluetooth und WLAN dar, die unter Umständen von Dritten aktiv angesprochen werden können.

Bedrohung: Insbesondere in öffentlichen Netzwerken ist es möglich, durch Abhören/Verfälschen der Verbindung Nutzdaten und/oder Kennwörter zu erlangen. Diese Gefahr besteht zum einen bei der Einwahl zum Internet-Provider über GPRS und GSM, zum anderen durch Nahbereichsfunktechnologien wie Bluetooth und WLAN.

Maßnahme Technik: Dem kann durch Einsatz von Firewalls[134], starke VPN-Verschlüsselung und die Sperrung aller unnötigen Client-Ports durch die VPN-Software entgegengewirkt werden.

Maßnahme Policy: Um die Risiken in öffentlichen Netzten zu minimieren, sollten die Mitarbeiter dazu angehalten werden, Bluetooth und WLAN abzuschalten.

5.3.2.2 Nicht-öffentlich

Unter nicht-öffentlichen Netzwerken betrachten wir hier das Intranet, den im Rahmen dieses Projektes relevanten IVBB und die DMZ. Hier besteht die Gefahr des Missbrauchs des Endgeräts durch einen unbefugten Dritten. Dann sind nicht nur die Daten auf dem Endgerät gefährdet, sondern auch das firmeneigene Netzwerk.

Für die nachfolgenden Punkte raten wir insgesamt zur Entwicklung eines Notfall-Plans für gestohlene Endgeräte inkl. Änderung von Kennwörtern, Sperrung von Einwahlports, Auswertung von Logfiles etc. innerhalb einer Policy.

---

[134] Derzeit nicht verfügbar.

5.3.2.2.1 Intranet

Bedrohung: Das Intranet kann, z. B. durch die Einschleusung von Viren, Trojanern etc., angegriffen werden.

Maßnahme Technik: Wir empfehlen den Einsatz von Content-Scanning, Firewalls und VPN-Gegenstellen speziell für die Anbindung der Endgeräte.

5.3.2.2.2 IVBB

Bedrohung: Durch kompromittierte Endgeräte sind Angriffe auf das IVBB-Netzwerk möglich.

Maßnahme Technik: Auch hier ist der Einsatz von speziellen Firewalls/VPN-Gegenstellen im IVBB speziell für die Anbindung der Endgeräte sinnvoll.

5.3.2.2.3 DMZ

Bedrohung: Die DMZ kann durch ein kompromittiertes Endgerät angegriffen werden.

Maßnahme Technik: Wir empfehlen die Protokollierung sämtlicher Zugriffe der Endgeräte auf die DMZ und die Analyse ungewöhnlichen Verhaltens durch Intrusion Detection Algorithmen.

5.3.3 Arbeitsplatz

Auch der Arbeitsplatzrechner ist ein potenzielles Einfallstor für Bedrohungsszenarien.

5.3.3.1 Endgerät

Bedrohung: Eine Bedrohung ergibt sich durch die Verwendung von Rechnern, die nicht den verwendeten Sicherheitsrichtlinien unterworfen sind. Hier besteht die Gefahr einer Infektion durch Viren, den Einfall von Trojanern und von Sniffer-Lauschangriffen.

Maßnahme Policy: Um eine Infektion des Endgerätes durch ungeschützte Rechner zu verhindern, sollte der Arbeitsplatzrechner der einzige Companion-PC des PDA sein.

5.3.4 Administrations-Software

5.3.4.1 Endgeräte

Bedrohung: Eine Infektion der Endgeräte durch ein Fehlverhalten oder einen Missbrauch der Administrationskomponente ist nicht gänzlich ausgeschlossen. Da die Administrationskomponente ein zentrales Element in der Verwaltung aller Endgeräte darstellt, kann ein Angriff Auswirkungen auf alle im Einsatz befindlichen Endgeräte haben.

Maßnahme Technik: Ein besonderer Schutz des Administrationsservers, ähnlich dem Schutz anderer sicherheitskritischer Infrastrukturen, ist sinnvoll.

5.3.4.2 Intranet

Bedrohung: Eine Bedrohung ergibt sich auch durch das Einschleusen von bösartigem Code durch ein kompromittiertes Endgerät in das Intranet. Denkbar ist z. B., dass ein Angreifer Trojaner oder mit Makroviren verseuchte Word-Dokumente auf dem Endgerät ablegt, so dass diese bei einer Synchronisation durch Afaria mit öffentlichen Ordnern abgeglichen werden. Im nächsten Schritt könnten Mitarbeiter auf diese Dateien zugreifen und den schadhaften Code aktivieren.

Maßnahme Technik: Dieser Gefahr kann durch zentrales Content-Scanning am Afaria-Rechner und entsprechende Virenscanner am Endgerät begegnet werden.

Maßnahme Policy: Grundsätzlich gilt es, einen Transfer von Dateien vom Endgerät in das Intranet weitestgehend zu vermeiden. Außerdem sollten die Mitarbeiter für die Bedrohung durch Trojaner und ähnliches sensibilisiert werden. Vom Endgerät in das Intranet transferierte Dateien dürfen nicht ohne genaues Wissen über ihren Inhalt geöffnet oder gar ausgeführt werden.

5.3.4.3 Mitarbeiter

Bedrohung: Hier sind datenschutzrechtliche Aspekte zu berücksichtigen. Die Administrationskomponente ermöglicht den Zugriff auf personenbezogene Daten. Anhand dieser Daten ist die Erstellung von Bewegungs- und Aktivitätsprofilen denkbar. Datensicherungen können zweckentfremdet werden, indem sie zur Extraktion von Nutzdaten und/oder Kennwörtern benutzt werden. Insbesondere besteht die Gefahr der Umgehung von Sicherheitsrichtlinien durch die IT-Systemadministratoren, da diese Zugriff auf vertrauliche Daten auf den Endgeräten erhalten.

Maßnahme Policy: Die zu entwickelnde Policy für die Administrationskomponente muss möglichst restriktiv sein und die personenbezogenen Daten müssen besonders geschützt werden.

5.4 Betrachtung der Usability

Die Usability des vorgeschlagenen Gesamtsystems für den Endbenutzer schätzen wir als mittelmäßig bis schlecht ein. Einschränkungen im Bereich der Usability ergeben sich durch die begrenzte Eignung des iPAQ, die generell unzureichenden Funktionalitäten der Synchronisationssoftware und die zusätzlichen Bedienschritte, die der Einsatz von zusätzlichen Sicherheitsmechanismen mit sich bringt. Den Einsatz der untersuchten Endgeräte muss man aufgrund dieser Schwächen gründlich abwägen.

Trotz Erweiterungsmöglichkeiten der Speicherkapazität anhand externer Speichermodule ist der auf dem iPAQ verfügbare Speicherplatz schnell ausgeschöpft und bedarf er eines umsichtigen Umgangs seitens des Benutzers.

Mitarbeiter werden die vom Arbeitsplatzrechner gewohnten Funktionalitäten der Office-Werkzeuge nicht vorfinden. Die auf dem iPAQ verfügbaren Office-Tools wie Pocket Word, Pocket Excel und Pocket Outlook verfügen lediglich über Basisfunktionen. Der Browser ist aufgrund der geringen Displaygröße und der eingeschränkten Darstellung nur für gelegentlichen Einsatz geeignet. Die Texteingabe per Stift ist gewöhnungsbedürftig, beim Einsatz einer externen Tastatur leidet die Mobilität und damit die Akzeptanz auf Endbenutzerseite.

Für die untersuchten Endgeräte wird damit geworben, dass sie klein, handlich und mobil einsetzbar sind. Will man den iPAQ aber tatsächlich mobil, also unabhängig von einem Arbeitsplatz-PC und einem Cradle (Basisstation), nutzen, ist ein sogenanntes „Rucksack"-Modul[135] notwendig, das GSM/GPRS-Funktionen nachrüstet. Durch dieses Rucksack-Modul erlangt der iPAQ etwa das doppelte seines ursprünglichen Volumens und auch Gewichts.

Bei der Verwendung via GSM bzw. GPRS ist aufgrund einer geringen Bandbreite mit verhältnismäßig langen Übertragungszeiten zu rechnen, was die Akzeptanz beim Endbenutzer negativ beeinflusst.

Sicherheitsansprüche konkurrieren in starkem Maße mit Ansprüchen an die Usability. So sind für die zusätzliche Endgerätesoftware, die Verwendung von VPN-Tunneln, den Anstoß des Synchronisationsvorgangs und gegebenenfalls die Verwendung von Afaria Verbindungseinstellungen und Kennworteingaben notwendig.

Die Bedienschritte werden dabei durch den Einsatz des DNS-Dummies im Intranet und den Einsatz des Portforwarders in der DMZ soweit wie möglich reduziert. So ist nur ein einziges XTND-Profil notwendig, unabhängig davon, ob sich der Benutzer über RAS, über GPRS oder am Arbeitsplatzrechner im Intranet verbindet.

Durch Einsatz des Portforwarders ist nur ein einziger VPN-Tunnel notwendig, so dass der Benutzer nicht jedes Mal aufs Neue den passenden Tunnel auswählen muss. Beim Kontaktieren des XTND- oder Afaria-Servers über einen Arbeitsplatzrechner im Intranet kann und muss auf die Verwendung des VPN-Clients gänzlich verzichtet werden.

Folgende Bedienschritte seitens des Benutzers ergeben sich mit dem empfohlenen System für eine Synchronisation und einen Systemupdate mittels Afaria außerhalb des Intranets:

Power-On-Passwort

---

[135] Fachbegriff: Jacket.

Passwort für Endgerätesoftware

Herstellen der physikalischen Verbindung

VPN Client:

1. Aktivierung des VPN-Treibers
2. Starten des VPN-Clients
3. Auswählen eines Telefonbucheintrags
4. Start des Verbindungsaufbaus

XTND:

1. XTND-Client starten
2. Anstoss des Synchronisationsvorgangs
3. Eingabe des Passworts (identisch mit dem Exchange-Passwort)

Afaria:

1. Afaria-Client starten
2. Verbindung mit dem Afaria-Server initialisieren
3. Passwort eingeben.

Trotz der eingeführten Maßnahmen zur Steigerung der Usability bedarf es also immer noch zahlreicher Bedienschritte und eines beachtlichen Zeitaufwandes.

Wie bereits im Zusammenhang mit dem Funktionalitätsumfang der Synchronisation beschrieben, gibt es in der Verwaltung der Groupware-Daten mittels Pocket Outlook und der Sychnchronisationssoftware XTND erhebliche Einschränkungen.

Eines der Hauptmankos ist hierbei die Tatsache, dass Unterordner des Posteingangsfaches nicht mitsynchronisiert werden. Würde dem Benutzer ein spezieller E-Mail-Account für die Synchronisation auf dem iPAQ eingerichtet, so hätte er keine Möglichkeit zur Strukturierung des Posteingangsfaches und damit auch nicht die am Arbeitsplatz gewohnte Ablage- und Organisationsstruktur, so dass eine gezielte Suche nach bestimmten E-Mails umständlich und zeitaufwendig sein könnte.

Das gelegentliche Verfassen von E-Mails am PDA ist ein zweckmäßiges Anwendungsszenario. Hierbei wäre es natürlich wünschenswert, sowohl die persönlichen, als auch die öffentlichen Kontakte zur Verfügung zu haben. Da aber nur komplette Ordner zur Synchronisation freigegeben werden können, wird der Speicherplatz auf dem PDA nicht ausreichen, um sämtliche Kontaktdaten zu erfassen. Auch hier muss der Benutzer also entscheiden, welche der öffentlichen Kontakte er auf seinem PDA abgleichen möchte und diese selbst entweder in seine persönlichen Kontakte oder in einen durch die Administration für die zur Synchronisation freigegebenen Ordner verschieben.

Aufgrund des begrenzten Speichers auf den iPAQs ist die Synchronisation von öffentlichen Ordnern mitsamt ihrer kompletten Inhalte nicht sinnvoll. Auch hier gilt es genau abzuwägen, welche Dokumente auf dem iPAQ verfügbar sein sollen und diese in die zur Synchronisation freigegebenen Ordner zu verschieben.

Die Terminverwaltung am iPAQ ist ausreichend, solange man nicht erweiterte Funktionen wie Terminanberaumungen oder Zugriff auf fremde Kalender in Anspruch nehmen will.

Einfluss auf die Usability hat natürlich auch die gewählte Administrationslösung. So erfordert der Einsatz von Afaria zusätzliche Bedienschritte durch den Benutzer, um System- und Softwareupdates durchführen zu können. Setzt man Afaria hingegen nicht ein, so wird es nicht zu vermeiden sein, dass die erforderlichen administrativen Maßnahmen am Endgerät direkt beim Administrator vor Ort durchgeführt werden müssen und die Vorteile der Remote-Administration verloren gehen.

Insbesondere die unzureichende Usability macht die Betrachtung alternativer Lösungen sinnvoll.

5.5 Betrachtung der Administration

Die Integration mobiler Endgeräte in eine bestehende Infrastruktur ist mit einem erheblichen administrativen Aufwand verbunden. Je nach Anzahl der zu betreuenden Clients, kann der Zeitaufwand schnell zu groß werden, als dass diese Arbeit von der bestehenden Zahl an Administratoren nebenbei erledigt werden könnte. Zusätzlich zu den Aufgaben, die sich ausschließlich auf Konfiguration und Inhaltsverteilung für die Endgeräte beziehen, müssen auch Maßnahmen für die Einbindung in die Infrastruktur geplant werden. Zu berücksichtigen sind dabei unterschiedliche Bereiche des Firmennetzes.

In der DMZ ist es erforderlich, verschiedene Einstellungen anzupassen. Neben der neu zu installierenden Software (XTND-Proxy) müssen auch bestehende Dienste modifiziert werden. Zum einen ist es erforderlich, einen in der DMZ positionierten VPN-Server entsprechend anzupassen, so dass aufgebaute Verbindungen Anfragen an den XTND-Proxy stellen können. Der Proxy wiederum muss die Anfrage weiterleiten, dazu muss er die Firewall zum Intranet überwinden können. Also ist es notwendig, einen Port im Packetfilter der Firewall zu öffnen (für XTND per Default Port 5001 bzw. 6001 bei SSL-Verbindung zwischen Proxy und Server).

Bei der Verwendung der Afaria Administrationssoftware müssen zusätzlich ein Port geöffnet und eine Portforwarding-Regel definiert werden, damit die Anfrage des Afaria-Clients den Server erreichen kann. Die Option, einen zweiten VPN-Tunnel direkt in das Intranet zu legen, wurde aus Gründen der Usability verworfen, da hierfür der alte Tunnel aufgelöst werden und ein neuer etabliert werden müsste. Zudem würde eine solche Konfiguration die Sicherheitsmechanismen der Firewall komplett außer Kraft setzen. Diese „Schwachstelle" ließe sich elegant lösen, wenn eine der Infrastruktur entsprechende Proxy-Komponente entwickelt würde.

Während die XTND-Komponente ihre Datenspeicherung selbst durchführt und verwaltet, ist Afaria auf eine externe Datenbank angewiesen, die nach Möglichkeit auf einem eigenen Server liegen sollte. Auch wenn Afaria die benötigten Datenbankstrukturen anlegt und weitere Eingriffe seitens des Datenbankadministrators nicht zwingend erforderlich sind, fallen im laufenden Betrieb Wartungsarbeiten an.

Sofern Afaria als Administrationssoftware eingesetzt wird, kann es bei einer größeren Anzahl von mobilen Endgeräten sein, dass ein einzelner Server mit den Aufgaben überfordert ist. Als Folge daraus können/müssen die administrativen Aufgaben von mehreren Servern übernommen werden. Das Einrichten solcher Serverfarmen erfordert deutlich mehr Arbeit und die Koordination der zu verwaltenden Inhalte und Konfigurationen.

Bei der Verwendung von XTND für die Synchronisation ist zu beachten, dass diese nicht nur von außen, sondern auch vom Arbeitsplatz aus möglich sein soll. Hier kommt der Konflikt zwischen dem XTND-Client und Active Sync zum tragen. Aus administrativer Sicht muss berücksichtigt werden, dass jeder einzelne Arbeitsplatz, auf dem Active Sync läuft, so vorkonfiguriert wird, dass er nicht in Konflikt mit dem XTND-Client gerät, dass also keine Synchronisation über Active Sync stattfindet. Vor allem sollte in diesem Fall auch darauf geachtet werden, dass der Endnutzer die Synchronisation via Active Sync nicht nachträglich, absichtlich oder versehentlich, wieder aktivieren kann. Dies erfordert zum einen eine strikte Policy für die Mitarbeiter (siehe nichttechnische Maßnahmen) und zum anderen eine ständige Kontrolle durch die Administratoren.

5.5.1 Inhalte und Konfigurationen

Sowohl mit Afaria als auch mit XTND ist es möglich, Software auf den Endgeräten remote zu installieren. Die Optionsvielfalt weist aber je nach verwendeter Administrationskomponente erhebliche Unterschiede auf. Während man mit XTND lediglich installationsfähige Dateien überträgt und das entsprechende Setup anstößt, hat man mit Afaria wesentlich

mehr Eingriffsmöglichkeiten zur Verfügung. Bei der Verteilung von Software, die ggf. auch im Nachhinein Anpassungen erfordert, ist man mehr oder minder auf die Afaria-Software angewiesen, da diese gegenüber XTND mehr Möglichkeiten zur individuellen Anpassung bietet.

Sowohl unter Afaria als auch unter XTND ist eine Software-Distribution mit einem gewissen Aufwand verbunden. Es müssen die zu installierenden Softwarekomponenten, Lizenzen oder allgemein die Software- und Gerätebestände verwaltet und gewartet werden. Auch hier ist der Einsatz von Afaria ab etwa 100 Endgeräten zu empfehlen, da es sonst schwer fallen dürfte bzw. entsprechend Mehraufwand bedeuten würde, Überblick über die mobilen Endgeräte zu behalten oder sie zu inventarisieren.

Zur Verteilung von Dokumenten für bestimmte Benutzergruppen ist sowohl XTND als auch Afaria geeignet. Während Afaria lediglich dazu konzipiert wurde Dokumente zugänglich zu machen, benutzt XTND die Benutzer- bzw. Gruppen-spezifischen Verzeichnisse auch zur Synchronisation, d. h. Dateien können optional auch auf den Server hochgeladen werden.

Bezüglich der Verteilung und der reinen Downloads ist Afaria flexibler, da zunächst nur die Namen der zur Verfügung stehenden Dateien übertragen werden und der Benutzer daraufhin eine Auswahl treffen kann, welche Daten er auf seinem Endgerät benötigt, während bei XTND lediglich eine volle Synchronisation des entsprechenden Verzeichnisses möglich ist.

Hinzu kommt, dass durch das Prinzip der Document-Channels von Afaria beliebige Dateien auf dem Server zur Distribution freigegeben werden können, auch für unterschiedliche Gruppen und Channels, d. h. die zu verteilende Datei muss nur einmal auf dem Server bereit liegen. Bei XTND hingegen kann es dazu kommen, dass bestimmte Dateien, die für unterschiedliche Nutzer oder Gruppen bereit gestellt werden sollen, auf dem Server doppelt auftauchen, da diese zur Verteilung in die entsprechenden Unterverzeichnisse kopiert werden müssen. Dies erschwert zum einen den Überblick und stellt zum anderen eine Speicherplatzverschwendung auf dem Server dar. Dasselbe gilt für die zu verteilende Software.

5.5.2 Benutzerverwaltung

Die Benutzerverwaltung und auch die Gruppenverwaltung gestalten sich sowohl unter Afaria als auch unter XTND gewöhnungsbedürftig. Das Ansprechen eines individuellen Endnutzers ist unter beiden Komponenten nicht direkt möglich. XTND verfügt zwar noch über eigene Verzeichnisstrukturen, in denen ein bestimmter Benutzer seine individuellen Dateien ablegen bzw. synchronisieren kann, über die Administration können aber nur gruppenweite Einstellungen vorgenommen bzw. Profile angelegt werden.

Bei Afaria ist eine Individualisierung lediglich über das Abonnieren unterschiedlicher Channels bzw. Channel-Sets möglich. Diese müssen dazu aber namentlich bekannt sein, was für den Endbenutzer eine unnötige Belastung darstellt. Er müsste sich also in jedem Fall mit einem Administrator in Verbindung setzen, um einen spezifischen, für ihn angepassten Channel zu erhalten. Dies bedeutet zudem auch für den zuständigen Administrator zusätzliche Arbeit.

Positiv zu bewerten ist die Tatsache, dass Benutzerinformationen aus dem vorhandenen Active Directory übernommen werden können. Somit müssen diese Daten nicht nachträglich per Hand eingepflegt werden. Hier hört die ActiveDirectory-Unterstützung aber auch schon wieder auf, da bei Hinzukommen neuer Benutzer die entsprechenden Informationen per Hand kopiert bzw. übernommen werden müssen. Die nicht vorhandene Vollintegration in das Active Directory hat zur Folge, dass eine doppelte Administration notwendig ist und diese dadurch insgesamt aufwendiger wird.

5.6 Betrachtung Kosten

Die Kosten eines Systems zum mobilen Arbeiten spielen eine nicht zu vernachlässigende Rolle bei der Einführung. Vor der Einführung muss eine Abwägung zwischen den entstehenden Kosten und dem gewonnenen Nutzen getroffen werden. Die hier genannten Preise sind lediglich als Anhaltspunkte zu verstehen, da es sich in der Regel um Einzelpreise laut Preisliste der Hersteller handelt. Die Preise können durch Abnahme größerer Posten eventuell gesenkt werden. Im Folgenden führen wir die Serverhardware als zusätzlichen Kostenfaktor nicht explizit auf, da wir davon ausgehen, dass diese bereits vorhanden und weiter nutzbar ist.

- Kosten für die Einführung des Systems:

  Hardware, Software, Kosten für Entwicklung der Policy, Schulung Mitarbeiter, Schulung Administratoren, ggf. Support für Einrichtung, Sicherheitscheck

- Kosten für den laufenden Betrieb:

  Administrationskosten für laufenden Betrieb, Kosten für Support und Wartungsverträge, Verbindungsgebühren[136]

5.6.1 Kosten für die Einführung des Systems

Tabelle 5-1: Kosten – Einführung Gesamtsystem

Hardware		
Modell	**Hersteller**	**Preis**[137]
IPAQ 3970	HP	748,20 €
GSM/GPRS Rucksack	HP	479,01 €
Software		
Softwarekomponente	**Hersteller**	**Preis**[138]
XTND Connect Server	Extended Systems	20.000,-- €
XTND Client [139]	Extended Systems	125,-- €
Afaria Server [140]	XcelleNet	ca. 7000,-- €
Afaria Client	XcelleNet	127,-- €
FileCrypto	F-Secure	76,20 €
Antivirus For Pocket PC	F-Secure	36,-- €
VPN Lösung [141]	Nicht verf.	Nicht verf.

Bei den Kosten der Software muss zwischen der Server- und Clientsoftware unterschieden werden, da für eine Abschätzung der gesamten Softwarekosten die Zahl der Endgeräte und der somit zu erwerbenden Lizenzen entscheidend ist.

---

[136] Eine genauere Untersuchung nach TCO-Massstäben wäre noch erforderlich.
[137] Kosten für jeweils ein Gerät.
[138] Kosten für jeweils eine Lizenz.
[139] Kosten pro Client bei einer Abnahme von 100 – 490 Clients.
[140] Kosten bei einer Installation für 100 Clients.
[141] Es wurde die bereits beim Auftraggeber im Einsatz befindliche VPN Lösung benutzt.

5.6.2 Kosten für den laufenden Betrieb

Die laufenden Kosten sollten bei der Entscheidung für oder gegen ein derartiges System nicht unterschätzt werden. Neben notwendigen kostenpflichtigen Updates der Systemkomponenten fallen besonders die Kosten für den laufenden Betrieb ins Gewicht. Dazu zählen in erster Linie die anfallenden Gebühren für Funkverbindungen via GSM oder GPRS.

Die Tarife hierfür variieren sehr stark je nach Vertrag mit dem jeweiligen Netzbetreiber und Standort. Diese Kosten können besonders beim Arbeiten im Ausland stark ansteigen, da der Benutzer hier im Allgemeinen auf einen Roamingpartner seines Netzbetreibers angewiesen ist.

Weitere laufende Kosten entstehen durch Wartungsverträge. Laut Angaben der IT-Abteilung des Bundeskanzleramtes kann man z. B. für XTND von einer jährlichen Höhe von ca. 10% der ursprünglichen Lizenzkosten ausgehen.

5.7 Empfohlene nichttechnische Maßnahmen

5.7.1 Sicherheits-/Datenschutzpolicy

Beim Einsatz der beschriebenen Endgeräte und der notwendigen Zusatzkomponenten entstehen eine Reihe von Problemen, die nicht allein mit technischen Maßnahmen gelöst werden können. Beispiele hierfür sind im Kapitel 5.3 zu finden. Probleme bestehen zum einen hinsichtlich der Sicherheit, zum anderen aufgrund datenschutzrechtlicher Aspekte.

Die Entwicklung einer Policy war nicht Gegenstand dieses Projekts, wir empfehlen dennoch dringend, die Einführung eines Gesamtsystems für mobile Endgeräte mit der Implementierung einer Sicherheits- und Datenschutzpolicy zu begleiten.

Betroffene dieser Policy sind dabei u. a. die Anwender der mobilen Endgeräte, die IT-Administratoren, Notfall-Teams, Mitarbeiter im Support und Mitarbeiter im Bereich Datensicherheit/Datenschutz.

Die Entwicklung einer Policy kann aus unserer Sicht in folgenden Schritten erfolgen:

1. Identifikation der zu regelnden Bereiche:
    - Ermittlung des bestehenden und des erwarteten Sicherheitsniveaus
    - Ermittlung notwendiger Sicherheitsmaßnahmen
    - Verlustmeldung, Eskalationsstrategie bei Verletzung der Sicherheits-/Datenschutzpolicy
    - Ermittlung der Randbedingungen für geschäftliche und private Nutzung privater und/oder dienstlicher PDAs
    - Erlaubte Anwendungen (Standards, Genehmigungsmechanismen für zusätzliche bzw. alternative Anwendungen)
    - Kontrollen, Auditierung der Einhaltung festgelegter Maßnahmen
    - Identifikation und Analyse datenschutzkritischer Vorgänge durch zentrale Administrationskomponente (z. B. Nutzerprofile, Zugriff auf Datensicherungen)
    - Ermittlung des Integrationsbedarfs in Bezug auf die bestehende Sicherheits-/Datenschutzpolicy
2. Konzeptuelle Integration mit der existierenden Sicherheits-/Datenschutzpolicy für den IT-Bereich
3. Implementation.

5.7.2 Schulung

Die Mitarbeiter sollten vor dem Einsatz der mobilen Endgeräte gründlich geschult werden. Neben der Benutzung und Konfiguration sollte besonderes Augenmerk auf die entwickelte Policy gelegt werden. Dies gilt sowohl für Endbenutzer als auch für Administratoren.

5.8 Fazit

Insgesamt kann man sagen, dass der Bereich des mobilen Arbeitens unter Benutzung von PocketPC-Systemen noch in den Anfängen der Entwicklung steckt. Für persönliche Informationen, Notizen, Kontakte und das gelegentliche Betrachten eines Dokuments ist der Einsatz solcher Systeme durchaus gerechtfertigt und sinnvoll. Anders verhält es sich aber, wenn es darum geht, mittels eines PDAs einen mobilen Arbeitsplatz zu schaffen.

Durchaus brauchbar ist der Datenabgleich am Arbeitsplatz in Verbindung mit zusätzlicher Sicherheitssoftware auf dem Endgerät (vor allem im Bezug auf Authentifikation und Datenverschlüsselung). Sobald man aber Daten mobil aktualisieren will, stößt man auf Hindernisse. Zu einer wirklich umfangreichen Infrastruktur, die aufgebaut und verwaltet werden muss, kommen Probleme bei der Nutzbarkeit und Sicherheit.

Bei einer Verbindung über das Internet müssen diverse Sicherheitsaspekte berücksichtigt werden. Zum einen gilt es das Endgerät so gut wie möglich abzusichern, zum anderen bedeutet eine hinreichende Absicherung immer eine Gefährdung der Usability. Nicht zuletzt müssen die Übertragungswege und der Zugriff auf Daten im Intranet bestmöglich geschützt werden. Ebenso muss durch den Einsatz von Antivirensoftware verhindert werden, dass schädliche Dateien ihren Weg in das Firmennetzwerk finden. Letzter Punkt gilt allerdings auch für die ausschließliche Verwendung am Arbeitsplatz.

Selbst wenn man eine entsprechende Infrastruktur etabliert hat und die Synchronisation der Daten technisch möglich ist (zumindest weitestgehend), ist eine komplette Synchronisationssession einschließlich einer administrativen Verbindung mit einer hohen Zahl von Arbeitsschritten verbunden. Dies dürfte die Akzeptanz der Geräte bei den Mitarbeitern stark vermindern.

Ein wirklich effektives Arbeiten ist auf diesen Geräten aufgrund ihrer Größe und der eingeschränkten Leistungsfähigkeit (sowohl die Softwarekomponenten als auch die Rechengeschwindigkeit des Gerätes selbst betreffend) weder möglich, noch ist es zu empfehlen. Dies resultiert u. a. auch daraus, dass Worddokumente für die Darstellung auf dem iPAQ teilweise in ein entsprechendes Format umgewandelt werden und hierbei diverse Formatierungen verloren gehen. Es ist also nicht zu empfehlen ein Dokument, das man am Arbeitsplatz begonnen hat, unterwegs auf dem PDA weiterzubearbeiten, da es später wieder komplett neu formatiert werden muss. Deshalb ist ein solches Gerätes lediglich als ausgefeilter Document-Viewer nutzbar. Durchaus sinnvoll ist die Nutzung wenn es um persönliche Informationen geht. Eigene Kontakte, Notizen, Sprachmemos, eigene Termine und evtl. das Verfassen einer kurzen Mail sind relativ einfach erlern- und durchführbar. Setzt man den Nutzen zu dem notwendigen Aufwand in Relation, so ist der Enterprise-Einsatz mehr als nur fraglich.

Die Verteilung von wichtigen Daten und Dateien verursacht einen hohen Aufwand für die Administratoren im Hintergrund, sowohl die Logistik betreffend als auch die dafür notwendigen Arbeitsschritte und Kosten.

Der zentrale Einsatz solcher Geräte ist außerdem an ein massives datenschutzrechtliches Problem gekoppelt. So werden z. B. Backups und persönliche Dateien zentral auf einem Server abgelegt. Diese Dateien sind zum einen nicht verschlüsselt, was bedeutet, dass Administratoren Einsicht in die evtl. sensiblen oder/und persönlichen Inhalte der Endbenutzer nehmen können. Zum anderen ist das teils sehr detaillierte Logging von Ereignissen dahingehend missbrauchbar, dass Arbeitszeiten und –methoden der Endnutzer rekonstruierbar sind. Ebenfalls ist nachvollziehbar, wann welche Information einer Benutzergruppe bzw. einem Benutzer zugänglich und verfügbar war.

Der Einsatz mobiler Endgeräte in Verbindung mit einer mobilen Synchronisation ist nicht zu empfehlen. Bei ausschließlicher Verwendung in Zusammenhang mit dem eigenen Arbeitsplatz und den erwähnten zusätzlichen Sicherheitsvorkehrungen auf den Endgeräten kann dem Einsatz jedoch zugestimmt werden.

5.9 Alternativen

Es gibt eine Reihe von alternativen Entwicklungen sowohl im Bereich Hardware als auch bei der Software. Bei der Software sind erste Linux-Systeme auf Basis der iPAQ-Plattform verfügbar. Im Hardwarebereich könnten die neuen leistungsfähigen Palm-Handhelds eine Alternative darstellen. Hinzu kommen andere Systeme mit vorinstalliertem mobilem Linux.

Wir empfehlen, diese Alternativsysteme in Zukunft anhand der in diesem Evaluationsprojekt erarbeiteten Kriterien und identifizierten Probleme zu untersuchen.

Viele der aufgedeckten Schwächen sowohl im Bereich des Funktionsumfangs als auch im Bereich der Usability könnten sich durch den Einsatz von immer kompakter werdenden Subnotebooks beheben lassen, da auf diesen Geräten ein vollwertiges Windows-System installiert ist. Das vollwertige Windows-System ist im Gegensatz zum Pocket-PC Betriebssystem eine erprobte Plattform. Es besitzt einen erheblich höheren Leistungsumfang und die gewohnten Funktionalitäten der am Arbeitsplatzrechner befindlichen Office-Tools. Für Notebooks bestehen bereits etablierte Administrationskonzepte, die für Subnotebooks nahezu uneingeschränkt übernommen werden könnten.

Die Kosten der modernen Subnotebooks können dabei mit denen der iPAQs einschließlich der benötigten Jackets durchaus konkurrieren. Die Ausmaße betragen bei vielen Modellen ungefähr die doppelte Grundfläche des iPAQs bei gleicher, wenn nicht sogar geringerer Höhe. Die Vorteile des größeren Displays und einer vollwertigen Tastatur sind ebenfalls nicht von der Hand zu weisen.

In Anbetracht der Vorteile, die der Einsatz von Mini-/Subnotebooks gegenüber dem Einsatz von iPAQs mit sich bringen würde, empfehlen wir für ein mobiles Arbeiten auf langfristige Sicht den Einsatz von Subnotebooks.

Da die Möglichkeit zur Stifteingabe auch einen Anreiz für den Einsatz von iPAQs darstellt, kann man auch sogenannte Tablet-PCs in Erwägung ziehen, da diese ebenfalls eine Eingabe per Stift bei einer erheblich genaueren Schrifterkennung unterstützen.

Produktbeispiele Subnotebooks:

- Sony Vaio SRX51P/A

  http://www.vaio.sony-europe.com/ger/products/notebooks/srx51p_frames_top.html [2.5.2003]

- JVC Notebook MP-XP

  http://www.jvc-europe.com/JvcCons/deu.html [2.5.2003]

- Panasonic CF-R1 oder CF-T1

  http://www.panasonic.de [2.5.2003]

- Toshiba Libretto L5

  http://www.golem.de/0204/19550.html [2.5.2003]

  http://www.dynamism.com/libretto/index.shtml [2.5.2003]

Produktbeispiele Tablet-PCs:

- TravelMate C100 Serie

http://www.acer.de [2.5.2003]

- Toshiba Portégé 3500 Serie
  http://www.toshiba.de [2.5.2003]
- Fujitsu-Siemens Stylistic ST4000 Tablet PC
  http://www.fujitsu-siemens.de [2.5.2003]

  http://www.fujitsu-siemens.de/rl/produkte/index.html [2.5.2003] --> pensysteme
- HP Compaq TC1000 Tablet PC
  http://h40050.www4.hp.com/eu/euro_jump/tabletpc/de/ [2.5.2003]
- Viewsonic V1100 Tablet PC
  http://www.viewsoniceurope.com/DE/Products/Mobile_and_Wireless/V1100.htm [2.5.2003]
- Pacebook tablet pc
  http://www.paceblade.com/ [2.5.2003].

5.10 Offene Probleme

An dieser Stelle möchten wir auf offene Punkte verweisen, die in diesem Projekt nicht geklärt werden konnten, die aber aus unserer Sicht für eine zukünftige Evaluation des Einsatzes mobiler Endgeräte von Bedeutung sind.

5.10.1 Sicherheitsanalyse

Ein wichtiger Schwerpunkt im Rahmen dieses Projekts war die Untersuchung der Sicherheit der verwendeten Komponenten. Unsere Evaluation ersetzt jedoch keine dedizierte Sicherheitsanalyse. Beispielsweise konnte in diesem Projekt keine Quellcodeanalyse der verwendeten Software durchgeführt werden. Auch mussten wir an einigen Stellen auf Aussagen der Hersteller vertrauen und konnten keine Detailanalyse durchführen, so zum Beispiel in der Frage der verwendeten Kryptoalgorithmen und der von den Anbietern fremdlizensierten Sicherheitskomponenten.

Außerdem würden wir es begrüßen, wenn die in diesem Projekt erarbeiteten Aussagen einer kritischen Begutachtung unter Einbeziehung Dritter unterzogen würden. Die beteiligten Parteien sollten sich über die jeweiligen Erfahrungen im Bereich der mobilen Endgeräte austauschen und gemeinsame Schlussfolgerungen ziehen.

5.10.2 Entwicklung einer Administrationskomponente

Derzeit ist keine Administrationskomponente verfügbar, die sowohl den Ansprüchen an den Funktionalitätsumfang als auch den Sicherheitsanforderungen genügt. Afaria bietet zwar gute Administrationsmöglichkeiten, verfügt aber nicht über eine Proxy-Komponente in der DMZ. Das Produkt XTND hat gute Sicherheitsmechanismen, stellt aber nicht genügend Funktionalität zur Administration der Endgeräte zur Verfügung.

5.10.3 Untersuchung der Skriptingfähigkeit auf dem Endgerät

Ein kritischer Faktor ist für uns die schlechte Bedienbarkeit auf Endgeräteseite (siehe Kapitel 4.4). Problematisch sind insbesondere die mehrfache Eingabe von Kennwörtern und die schlechte Integration der Endgerätesoftware.

Ein Ansatz ist die Untersuchung der Skriptingfähigkeiten der jeweiligen Applikationen und des Betriebssystems. Das Ziel wäre dabei, mehrere „Batch-Dateien" für die Automatisierung verschiedener Aufgaben („Austausch von E-Mails", „Afaria-Synchronisation") zu erstellen, um die Anzahl der Bedienschritte pro Aufgabe zu minimieren. Kritisch dabei ist allerdings insbesondere die Kennwortspeicherung. Trotz der Automatisierung von Aufgaben muss sichergestellt werden, dass die Kennwörter ihre Sicherheitsfunktionen weiterhin erfüllen.

5.10.4 Engere Anbindung der Endgeräte an das Intranet

Bei der Anbindung der Endgeräte haben wir uns in diesem Projekt auf die Synchronisation mit MS Exchange beschränkt. Für die Zukunft ist aber auch ein weitergehender Zugriff denkbar, z. B. auf das Intranet-Portal, entweder auf eine elektronische Akte oder direkt auf das Dateisystem.

Dieser Zugriff erfordert, in Abhängigkeit vom jeweiligen Endgerätesystem, u. U. eine Aufbereitung der übermittelten Daten, da auf dem Endgeräte nicht jede Datei in jeder Form dargestellt werden kann. Lösung könnte ein zentrales CMS-System sein, dass Daten für bestimmte Zielplattformen automatisch aufbereitet.

6 Ausblick

In diesem Abschnitt wird auf die in der nächsten Zeit zu erwartenden bzw. von Herstellern angekündigten Neuerungen eingegangen.

6.1 SafeGuard PDA 2.0 Enterprise Edition

Nach Abschluss der Evaluationsphase erreichte uns eine Beta-Version[142] der lange angekündigten Enterprise Edition von SafeGuard PDA. Diese haben wir nicht einer vollständigen Evaluation[143] unterzogen, wir möchten aber an dieser Stelle zumindest einen ersten Eindruck der Software vermitteln.

In dem uns zur Verfügung gestellten Paket befinden sich neben den eigentlichen Installationsdateien für Administrations- und Client-Software[144] eine deutschsprachige Anleitung für die Personal Edition von SafeGuard PDA 2.0[145], eine deutschsprachige Anleitung für erste Schritte in der Enterprise Edition 2.0 sowie eine vollständige Anleitung zur Enterprise Edition 2.0 in englischer Sprache. Außerdem existiert eine Textdatei (lismich.txt) mit letzten Hinweisen zur jeweiligen Version.

Der größte Unterschied der Client-Software zu der von uns untersuchten Version scheint die Unterstützung von Smartphones nach dem Pocket PC 2002 Phone Edition Standard zu sein. In der Datei liesmich.txt steht hierzu der folgende Absatz:

„Auf Pocket PC Telefonen erlaubt SafeGuard® PDA einige Telefonnummern als „Notrufnummern“ zu konfigurieren, die ohne Authentisierung am PDA gewählt werden können. Diese Funktionen werden automatisch verfügbar, wenn SafeGuard® PDA das Vorhandensein eines GSM Chips im Pocket PC erkennt.“

Auch soll es dem Benutzer eines solchen Smartphones möglich sein, eingehende Anrufe ohne vorherige Authentifikation anzunehmen.

Wir werden nun anhand ausgewählter für Endgerätesoftware aufgestellter Kategorien kurz auf den zu erwartenden Funktionsumfang der Enterprise Edition eingehen. Dies ist jedoch *kein* Ersatz für eine vollwertige Evaluation im Sinne dieses Berichtes. Wir wollen lediglich darlegen, weshalb wir eine gesonderte Evaluation von SafeGuard PDA Enterprise Edition 2.0 *ausdrücklich* empfehlen.

6.1.1 Administration

Erhielt die Personal Edition 1.0 in dieser Kategorie noch die Benotung „ungenügend", so scheint der Hersteller Utimaco gerade im Bereich der zentralen Administration von SafeGuard PDA umfangreiche Funktionalitätserweiterungen implementiert zu haben. Die Software ist laut Dokumentation nun sowohl über ein Snap-In in die Microsoft Management Konsole und das Active Directory als auch über Software von Drittherstellern administrierbar. Neben der Installation der Client-Software auf den mobilen Endgeräten soll auch deren Konfiguration in der von uns präferierten Form verschlüsselter Konfigurationsdateien möglich sein.

---

[142] Genauer: SafeGuard PDA Enterprise Edition 2.00.0.14 Beta.
[143] im Gegensatz zur Personal Edition 1.0 die in Kapitel 4.4.10 näher vorgestellt wird.
[144] Jeweils im Microsoft-Installer-Format .msi.
[145] Innerhalb der Anleitung wird deutlich, dass sie sowohl auf die Personal als auch auf die Enterprise Edition eingeht.

Die von uns evaluierten Administrationslösungen XTND und Afaria werden in der Dokumentation explizit genannt, die Installation und Administration mittels Afaria wird sogar eingehend erklärt und selbst ein Importskript für Afaria soll laut Dokumentation in der vollwertigen Version enthalten sein.

Die zentral administrierbaren Einstellungen sind:

- Passwort-, Symbol-PIN- und Signatur-Policies (Mindestlänge, Gültigkeitsdauer, Umfang der History gegen nochmalige Verwendung bereits abgelaufener Passwörter etc.)
- Zwingende, vom Nutzer nicht abschaltbare Verwendung einer Power-On-Authentifikation
- Zwingende, vom Nutzer nicht abschaltbare Authentifikation bei ActiveSync
- Bei Bedarf keine Authentifikation nach dem Einschalten, wenn Gerät nur kurz (konfigurierbare Zeitdauer) ausgeschaltet war
- Aktion nach konfigurierbarer Anzahl fehlerhafter Anmeldungen
    - Abspielen eines Alarmtons
    - Hardlock.

Die auch in der Version 2.0 enthaltenen Module PrivateDisk und PrivateCrypto lassen sich auf die gleiche Art und Weise konfigurieren. Die Tatsache, dass für keine dieser drei Applikationen Einstellungen in Bezug auf die Verschlüsselung von PIM-Daten und E-Mails möglich sind, verursacht jedoch ernsthafte Bedenken.

6.1.2 Authentifikation

Die Möglichkeiten zur Authentifikation des Benutzers am Gerät unterscheiden sich unserem ersten Eindruck nach nicht von denen der von uns getesteten Version. Es stehen weiterhin die Verfahren Passwort, Symbol-PIN und Handschriftenerkennung zur Verfügung. Inwiefern der Hersteller bei der Qualität der Handschriftenerkennung nachgebessert hat, muss im Rahmen einer tiefer gehenden Evaluation geklärt werden.

Ließ sich bei der Anmeldung per Symbol-PIN in der von uns getesteten Version lediglich zwischen zwei verschiedenen Symbolsätzen wählen, so ist es in der Version 2.0 möglich, eigene Symbolsets zu definieren und diese anstelle der mitgelieferten zu verwenden. Es sei dahingestellt, ob hierdurch ein tatsächlicher Vorteil entsteht. In jedem Fall ist es besser als in der von uns getesteten Version 1.0 möglich, die Applikation an die Corporate-Identity anzupassen.

In der Enterprise Version ist auch der von uns stark bemängelte Punkt des Masterpassworts überarbeitet worden. SafeGuard PDA bietet nunmehr ein Challenge-Response-Verfahren zur Freischaltung durch Administratoren an, was der noch in der Version 1.0 verwendeten Methode des nahezu frei wählbaren Masterpasswortes in unseren Augen überlegen ist.

6.1.3 Datensicherheit

Dokumentation und ein Minimaltest der Software lassen vermuten, dass auch die Version 2.0, noch dazu in der explizit für große Organisationen vorgesehenen Enterprise Edition, keine Möglichkeit zur Verschlüsselung von PIM-Daten oder E-Mails bietet. Weder existiert hierzu ein Konfigurationsdialog, noch findet sich in der Dokumentation ein Hinweis darauf. Auch eine Verschlüsselung des gesamten PDAs findet an keiner Stelle Erwähnung.

Es ist deshalb zu vermuten, dass sich die Funktionen von SafeGuard PDA 2.0 in Bezug auf die Datensicherheit nicht oder nur minimal von denen der von uns getesteten Version 1.0 unterscheiden.

6.1.4 Zusammenfassung

Gerade hinsichtlich der zentralen Administration halten mit der Enterprise Edition 2.0 viele Funktionen Einzug in SafeGuard PDA, die wir noch in der Personal Edition 1.0 vermissten. Einer der zwei wichtigsten Kritikpunkte an dieser Software entfällt somit. Im Hinblick auf die Datensicherheit konnte uns dieser kurze Einblick jedoch nicht überzeugen. Sollte sich im Rahmen einer vollständigen Evaluation zeigen, dass die Software auch die Verschlüsselung von PIM-Daten und E-Mails oder gar die Verschlüsselung des gesamten PDAs leistet, so wäre SafeGuard PDA Enterprise Edition durchaus als Alternative zu der hier empfohlenen Sicherheitssoftware zu betrachten.

6.2 Pointsec for PocketPC 2.0

Wie bereits in der Evaluation zu Pointsec for PocketPC (siehe Kapitel 4.4.9) ausgeführt, halten auch hier mit der derzeit aktuellen Version Neuerungen Einzug, die wir in der von uns evaluierten Version vermissten. Wir empfehlen dringend eine eingehende Evaluation der aktuellen Pointsec for PocketPC Version.

6.3 PocketPC 2003

Laut Heise-Newsticker soll auch das Betriebssystem PocketPC 2003 noch innerhalb des Jahres 2003 verfügbar sein[146]. Dann sollen zum ersten Mal die in den hier untersuchten Geräten verwendeten XScale-Prozessoren nativ unterstützt werden, was positive Auswirkungen auf die Ausführungsgeschwindigkeit (insbesondere bei Ver- und Entschlüsselung) erwarten lässt. Kern dieses Betriebssystems soll nicht mehr Windows CE 3.0, sondern Windows CE .NET 4.1 sein.

Darüber hinaus gehende Erweiterungen werden voraussichtlich nicht tief greifend sein, sondern vielmehr der Produktpflege und Fehlerbeseitigung dienen[147]. PocketPC 2003 soll zwar abwärtskompatibel sein und somit auch PocketPC 2002-Applikationen ausführen können, da aber insbesondere die hier betrachtete Sicherheitssoftware stark in das Betriebssystem eingreift, empfehlen wir, vor der Verwendung dieses neuen Betriebssystems unbedingt das Zusammenspiel mit *allen* hier betrachteten Lösungen intensiv zu testen.

Welche Bedeutung dem .NET-Framework innerhalb des Betriebssystems zukommen wird lässt sich derzeit nicht hinlänglich abschätzen.

6.4 Microsoft Compact .NET Framework[148]

Das „Compact .NET Framework" von Microsoft ermöglicht es, plattformunabhängige Software für PDAs zu entwickeln. Das neue PocketPC (Windows CE .NET 4.1) beinhaltet bereits im Auslieferungszustand die notwendigen Komponenten, um alle auf dem Framework basierenden Applikationen ausführen zu können.

Für Entwickler mit Erfahrungen auf dem vollwertigen „.NET Framework" ist das Compact-Framework durch seine sehr enge Verwandtschaft sowohl im Bezug auf die Entwicklungsumgebung als auch im Bezug auf die verwendeten Systematiken sehr schnell beherrschbar. Damit will Microsoft gewährleisten, dass viele Softwareproduzenten bereits nach kurzer Einarbeitungszeit Applikationen für PDAs anbieten können.

So sind in näherer Zukunft möglicherweise viele Softwareneuerungen für PDAs zu erwarten. Beispielsweise ist Afaria in der neuen Version bereits mit .NET umgesetzt worden.

---

[146] Siehe http://www.heise.de/mobil/newsticker/data/jk-01.04.03-001/ [02.04.2003].
[147] vgl.:http://www.brighthand.com/article/First_Pocket_PC_2003_Details_Surface [02.04.2003].
[148] http://msdn.microsoft.com/vstudio/device/compact.aspx [03.05.2003].

6.5 Microsoft Exchange 2003 mit Mobile Information Server[149]

Microsoft führt den Mobile Information Server (MIS) in Zukunft nicht als eigenständiges Produkt weiter, sondern integriert dessen Funktionalitäten vollständig in den Exchange 2003 Server.

Nach Aussagen von Microsoft (Gespräch mit einem Microsoft-Repräsentanten auf der CeBit) wird aber weiterhin nicht die Möglichkeit zur Synchronisation von Notizen bestehen.

6.6 Microsoft Outlook 2003[150]

Microsoft Outlook 2003 ermöglicht in Zukunft im Betriebsmodus „Unternehmen oder Arbeitsgruppen" (volle Integration in eine Exchange-Domäne - i. d. R. innerhalb eines Intranets) ein Trennen der Verbindung zum Server. Outlook sorgt dann dafür, dass alle bisher abgerufenen Daten (Kontakte, Mails usw.) lokal gecached werden und erst beim Anfordern lokal nicht verfügbarer Daten nach einer erneuten Verbindung mit dem Server gefragt wird. Wird Outlook daraufhin wieder mit dem Server verbunden, sorgt ein intelligenter Synchronisationsmechanismus dafür, dass die Datenintegrität bewahrt wird.

So wäre man mittels eines Subnotebooks mit einem Outlook 2003 mobil in der Lage, ohne dauerhafte Verbindung zum Exchange-Server mit einem vollwertig in einer Exchange-Domäne lokalisierten Profil zu arbeiten.

6.7 XcelleNet

Laut der Aussage eines Vertriebsmitarbeiters von XcelleNet wird die nächste Version von Afaria einerseits das „Microsoft .NET Framework" nutzen, was eine fast vollständige Neuentwicklung zur Folge hat, und andererseits das Betriebssystem SymbianOS unterstützen. Weitere Änderungen dürften sich hauptsächlich auf die Produktpflege beschränken. Ob mit dem komplett neu entwickelten Programm eine Verbesserung der Nutzer- und Gruppenverwaltung realisiert werden wird, konnten wir nicht in Erfahrung bringen.

6.8 Extended-Systems (XTND)

„RSA Security's BSAFE Crypto-C Micro Edition"[151]

Der XTNDConnect Server ist laut Extended-Systems in Zukunft mit der Software „RSA Security's BSAFE Crypto-C Micro Edition" ausgestattet, die es ermöglicht, dem „FIPS 140-2 Level I"-Sicherheitsstandard zu entsprechen. Die „Federal Information Processing Standards" – kurz FIPS – werden vom „National Institute of Standards Technology" (NIST) definiert und sollen insbesondere den Sicherheitsansprüchen von Regierungen und Banken genügen.

„Real Time"[152]

Das „XTNDConnect Real Time"-Zusatzpaket zum XTNDConnect Server ermöglicht den direkten Live-Zugriff auf Daten im Intranet über einen Browser.

---

[149] http://www.microsoft.com/exchange/evaluation/ti/whatsnew.asp [03.05.2003].
[150] http://www.microsoft.com/exchange/evaluation/ti/whatsnew.asp [03.05.2003].
[151] http://www.extendedsystems.com/ESI/Company+Info/News+-+Events/PressDetail.htm?newsID=20030318 [03.05.2003].
[152] http://www.extendedsystems.com/ESI/Company+Info/News+-+Events/PressDetail.htm?newsID=200303031 [03.05.2003].

Die von XTND angegebenen Features sind:

- Unterstützung von Microsoft Exchange und Lotus Notes
- Bidirektionaler E-Mail-Zugriff in Echtzeit mit der Unterstützung von Attachments, Unterordnern und üblichen Groupware-Funktionalitäten
- Zugriff auf die persönlichen und öffentlichen Adressbücher von Exchange und Notes
- Die Unterstützung von SSL, RADIUS und Secure ID Authentifikation sowie end-to-end 128-Bit-Verschlüsselung und FIPS-Konformität
- Der Server-basierte Ansatz mache bei gleicher Sicherheit die Administrierbarkeit so einfach wie bei Desktop-Computern.

Aufgrund der Notwendigkeit einer stehenden Verbindung mit dem Intranet eignet sich „Real Time" vor allem für ein Inhouse-Szenario (z. B. über WLAN).

7 Anhang

7.1 Konfiguration eines Port-Forwarders

Der Portforwarder dient in unserem Testaufbau als Ersatz für eine Proxy-Komponente von Afaria. Der Portforwarder wird anstelle der Proxy-Komponente auf dem Rechner DMZ installiert und konfiguriert. Die Funktion des Portforwarders besteht darin, den Datenstrom von Afaria auf TCP-Ebene (Schicht vier) kommend aus dem Internet entgegenzunehmen und ins Intranet weiterzuleiten. Dabei findet allerdings keine Inspektion des Datenstroms statt, so daß keine Sicherheitsmaßnahmen wirksam werden.

Tabelle 7-1: Afaria – Der Portforwarder

TCP-Forwarder: „Afaria von außen ins Intranet“
Daten
(I) Erster Schritt Protokoll: TCP Von: Außenwelt Nach: DMZ (Port 3007) (II) Zweiter Schritt Von: DMZ Nach: Afaria-Server im Intranet (Port 3007)
Beschreibung
Der Datenstrom der Afaria-Clients wird von der Komponente entgegengenommen und 1:1 auf Schicht vier an den Afaria-Server im Intranet weitergeleitet. Die Rückantwort wird ebenfalls weitergeleitet.
Zweck
Die TCP-Forwarding-Komponente ersetzt provisorisch die fehlende Afaria-Proxy-Komponente.

Die Konfiguration selber kann mit dem „Internet Sharing Connection Wizard“ vorgenommen werden. Eine genaue Anleitung ist im Internet zu finden.[153]

[153] http://www.informit.com/isapi/product_id~%7B3BD59E20-8ADA-4E5A-891E-7D9C76E2E628%7D/content/index.asp [25.04.2002].

7.2 Musterdatenblätter und Evaluationsbögen

7.2.1 Rechnerdatenblatt

Hier das Muster für die Rechnerblätter, wie sie im Testlabor zur Erfassung der Basisdaten eingesetzt wurden.

Rechnername	Rechnername
Domaine	Domaine
IP-Adresse (MB)	IP-Adresse (MB)
DNS (MB)	DNS (MB)
IP-Adresse (RT)	IP-Adresse (RT)
DNS (RT)	DNS (RT)
Laufwerk	Laufwerk
Installierte Software	Installierte Software
Daten	Daten

7.2.2 Fingerabdrucktest

Das leere Muster eines Testdatensatzes, wie er im Rahmen der Evaluation des Fingerabdruckscanners eingesetzt wurde:

Tabelle 7-2: Musterdatenblatt Fingerabdrucktest

Nr:	Muster von:	Tester:	Datum:	Uhrzeit:

Temperatur	**Licht**	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**
Daumen rechts											
Warm	Helles Kunstlicht										
Warm	Tageslicht										
Warm	Schwaches Licht										
normal	Helles Kunstlicht										
Normal	Tageslicht										
Normal	Schwaches Licht										
Kalt	Helles Kunstlicht										
Kalt	Tageslicht										
Kalt	Schwaches Licht										
Zeigefinger links											
Warm	Helles Kunstlicht										
Warm	Tageslicht										
Warm	Schwaches Licht										
normal	Helles Kunstlicht										
normal	Tageslicht										
normal	Schwaches Licht										
Kalt	Helles Kunstlicht										
Kalt	Tageslicht										
Kalt	Schwaches Licht										

7.3 OSI Modell – Pocket PC 2002

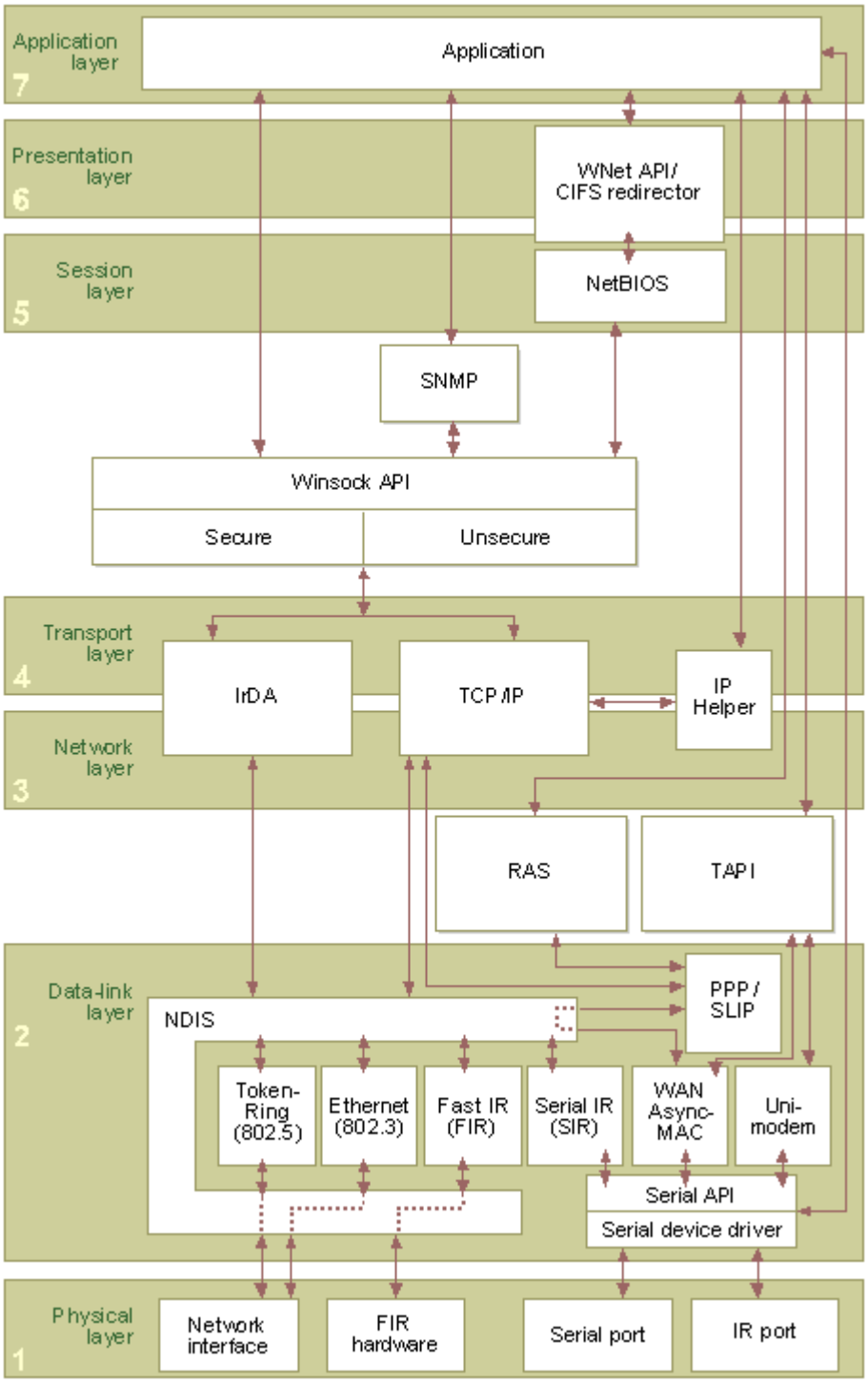

Abbildung 7-1: vollständiges OSI-Schichtenmodell von Microsoft-PocketPC

7.4 Bedrohungsszenarien

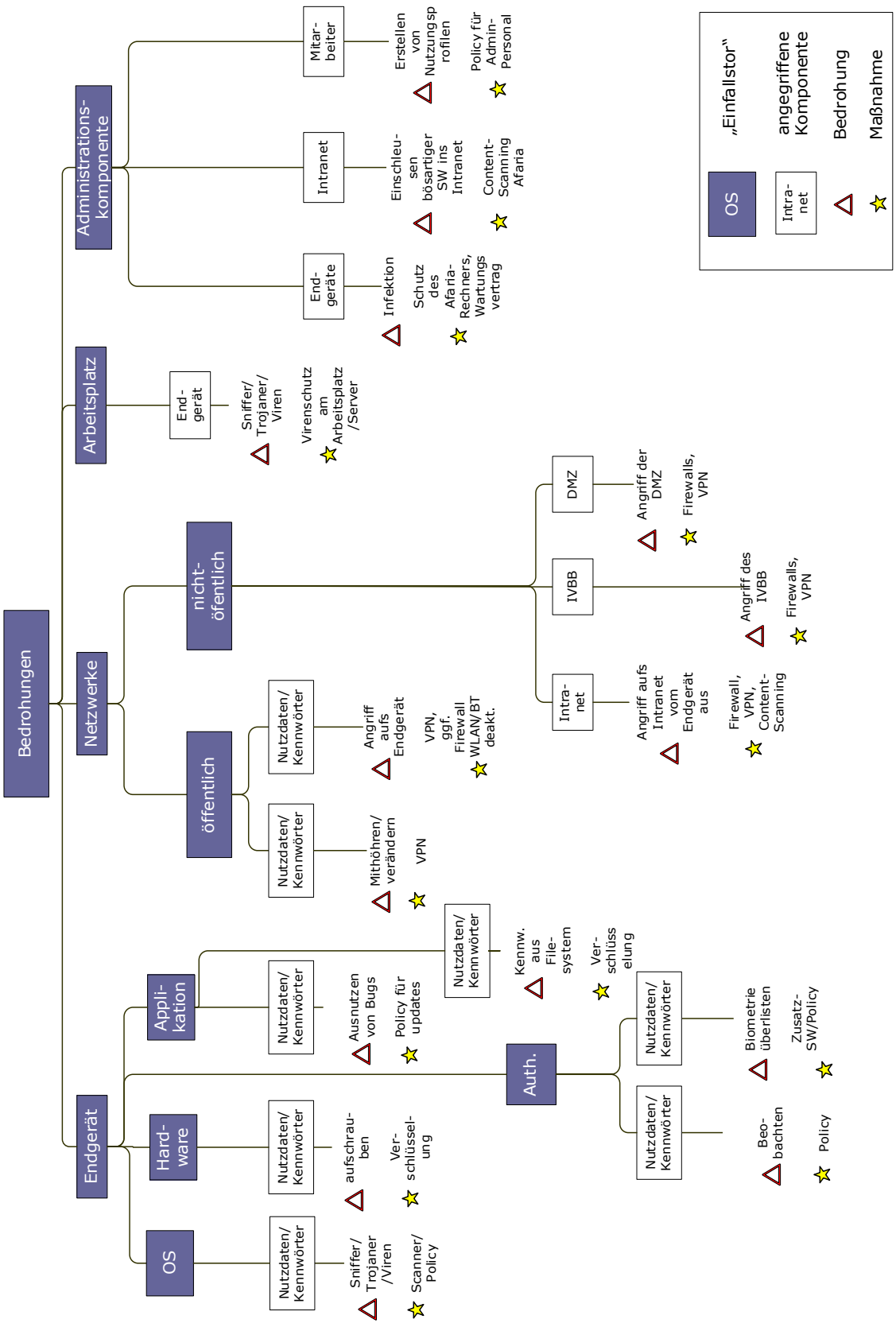

Abbildung 7-2: Attack-Tree

7.5 Projektplanung

Hier ein Überblick über die Zeitplanung im Rahmen des Projektes „MOB II" im Wintersemester 2002/2003 inklusive wichtiger zentraler Meilensteine. Stand der Planung: Mitte März. Der Endbericht wurden im Zeitraum von 15.04. bis 15.05. fertiggestellt.

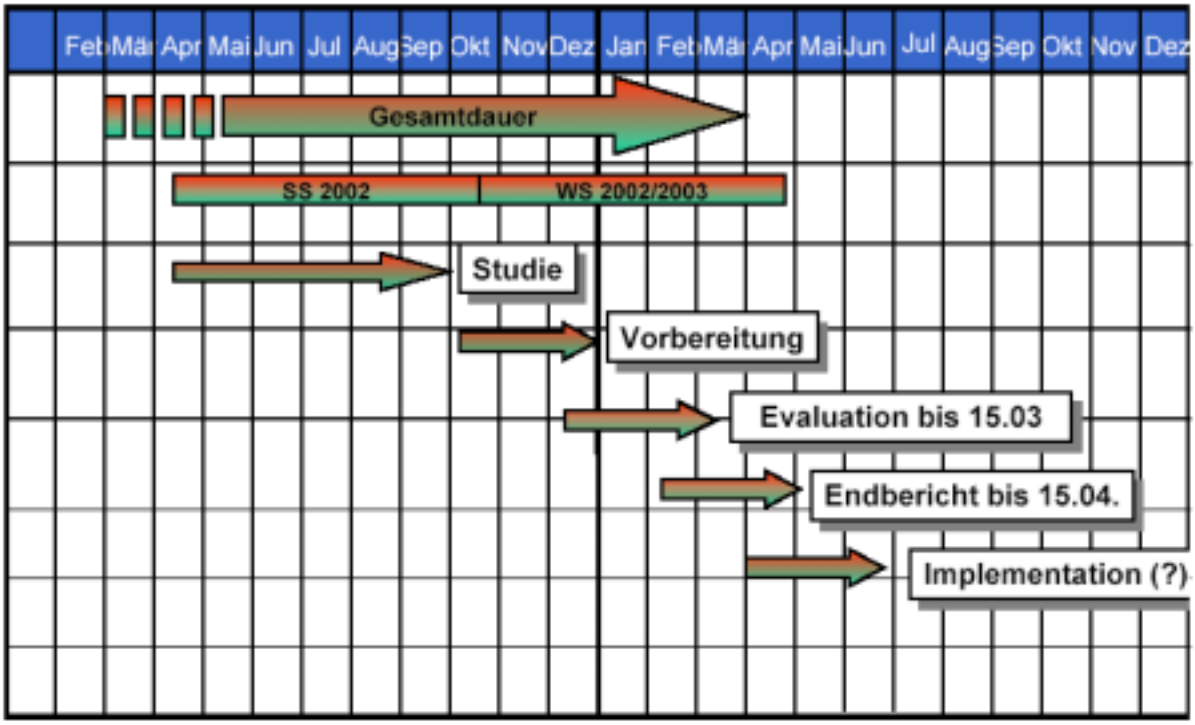

Abbildung 7-3: Zeitplanung

7.6 Quellenverzeichnis

Asynchrony 2003
About Asynchrony
http://www.asynchrony.com/welcome.jsp [26.03.2003]

AfariaSpec 2003
XcelleNet's Afaria 5.0 - Technical specifications
http://www.xcellenet.com/public/products/afaria/technology.asp [26.03.2003]

Baumgarten 2001:
Uwe Baumgarten, Claudia Eckert: Mobil und trotzdem sicher?
In: It + ti – Informationstechnik und Technische Informatik,
Oldenbourg Verlag (2001), Nr. 5, S. 254f.
http://www.sec.informatik.tu-darmstadt.de/de/publikationen/Papers/it+ti.pdf

Dedo 2002
Douglas Dedo: Pocket PC-Sicherheit
Engl. Originaltitel: Pocket PC Security
In: Microsoft Technet
http://technet.microsoft.at/includes/file.asp?ID=3244 [26.03.2003]

FIPS 2001
Von: United States Of America – Department Of Commerce
FIPS 140-2 „Security Requirements for Cryptographic Modules" (Mai 2001)
In: Federal Information Processing Standards Publications
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [26.03.2003]

GeNUA 2002
BSI zertifiziert erstmals Firewall nach „ITSEC E3 hoch"
In: GeNUA Pressemeldungen
http://www.genua.de/news/presseinfo/presse/pi_zerti_html [26.03.2003]

Herrera 2002
Chris De Herrera: Pocket PC 2002 Security (Version 1.01)
In: CE-Windows Net (Mai 2002)
http://www.cewindows.net/reviews/pocketpc2002security.htm [26.03.2003]

ISA 2002
Microsoft Whitepaper - „Using Internet Security and Acceleration Server as a Gateway for Mobile Information Server 2002"
In: Microsoft Technet
http://www.microsoft.com/miserver/techinfo/administration/isagateway.asp
[26.03.2003]

ISO 1995
DIN EN ISO 9241-10
Europäisches Institut für Normung
Deutsche Fassung vom 09.02.1995

IsoMetrics 2002
Iso Metrics - Development of a software usability instrument
In: Netz der Universität Osnabrück
http://www.isometrics.uni-osnabrueck.de/ [26.03.2003]

KSW 1997
John Kelsey, Bruce Schneider, David Wagner: „Related-Key Cryptanalysis" (1997)
In: International Conference on Information and Communications Security in Beijing
http://www.cs.berkeley.edu/~daw/papers/keysched-icisc97.ps [26.03.2003]

MOB-I 2002
Prof. Dr. iur. Bernd Lutterbeck: „Mobiler Zugang zu gesicherten Netzen"
Forschungsgruppe Internet Governance, Technische Universität Berlin

OSIM 2001
Jon Christiansen (März 2001):
„Microsoft Windows CE 3.0 - Open Systems Interconnection Model"
In: MSDN-Library
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnce30/html/ceevalguide.asp [10.03.2003]

Pointsec 2002
Pointsec for Pocket PC 1.3
Administrator Guide 2. Edition November 2002

Pointsec 2003
Pointsec Mobile Technologies—Who We Are
http://www.pointsec.com/company/company.asp [26.03.2003]

Sans 2000
Oda Sans: „Identikation durch Challenge-Response-Verfahren" (August 2000)
http://www.fernuni-hagen.de/NT/kurse/sem_2000/sans_challange.pdf [26.03.2003]

Schneier 1999:
Bruce Schneier: Attack trees
In: Dr. Dobb's Journal December (1999)
http://www.counterpane.com/attacktrees-ddj-ft.html

SCMag 2002
Test von PDA Defense für Palm OS
In: SC Online Magazin (November 2002)
http://www.scmagazine.com/scmagazine/2002_11/test_01/20.html [26.03.2003]

SOL 2002
iPAQ Pocket PC solutions catalog
In: Hewlett Packard (HP) – HP Invent
http://h20022.www2.hp.com/busprod/pocketpc/solutions/featured/?lsidebarLayId=824
[26.03.2003]

SOFT 2002
Pocket PC – Software
In: pocket.at – Die Plattform für Pocket PCs
http://www.pocket.at/pocketpc/software.htm [26.03.2003]

WiHaGe 1997
Fragebogen zur Evaluation von graphischen Benutzungsschnittstellen
Heinz Willumeit, K.C. Hamborg, G. Gediga: IsoMetrics Kurzform (v2.01)
http://www.isometrics.uni-osnabrueck.de/boegen/www/Isometrs.ps [26.03.2003]

Wolpers 1997
M. Wolpers: Kommunikation in CSCW-Systemen (1997)

In: Repository-gestützte Gruppenarbeit im World Wide Web
http://www.kbs.uni-hannover.de/Arbeiten/Diplomarbeiten/97/wolpers/node10.html
[26.03.2003]

XTNDGuide 2002
XTNDConnect Server Groupware Edition Version 3.5 - Getting Started Guide
http://www.extendedsystems.com/ESI/Service+Support/XTNDConnect+Server/Documentation/default.htm

Ziegler 2002
Peter-Michael Ziegler: „Biometrische Zugangskontrollen auf die Probe gestellt"
In: C't 11/2002, Seite 114

7.7 Abbildungsverzeichnis

7.8 Tabellenverzeichnis

7.9 Glossar

A

Access-Point

Zentraler Zugangspunkt zu drahtlosen Netzwerke.

Active Directory

Skalierbarer, hierarchischer Verzeichnisdienst zur zentralen Verwaltung aller für das Netzwerk relevanter Daten.

ActiveSync

Synchronisationssoftware von Microsoft. ActiveSync ist fester Bestandteil von PocketPC.

Administration

Verwaltung von IT-Systemen.

Administrationskomponente

Software zur Verwaltung von Soft- und Hardwarekomponenten.

Application Level Gateway (ALG)

Filtertyp bei Firewalls. Dieser Filtertyp arbeitet auf der Anwendungsschicht (OSI-Schicht sieben). Hierbei werden die Daten auf ihre syntaktische und evtl. inhaltliche Korrektheit beim Passieren der Firewall überprüft.

API

Application Programming Interface. Schnittstelle zur Programmierung von Anwendungsprogrammen. Sie stellt Programmierern eine genormte Schnittstelle zur Verfügung, über die auf Dienste des Betriebssystems zugegriffen werden kann.

Applikationsebene

Ebene des OSI-Schichtenmodels, auf der die eigentlichen Anwendungen arbeiten.

Applikations-Server

Rechner, auf dem zentrale Anwendungsprogramme im Netzwerk laufen, z.B. Microsoft Exchange.

Arbeitsplatzrechner

Siehe Desktop-PC.

Arbeitsspeicher

Flüchtiger Speicher im System, der alle im Augenblick benötigten Daten zwischenspeichert und für das System zur Verfügung stellt. Die Größe des Arbeitsspeichers ist entscheidend für die Leistungsfähigkeit eines Systems.

Authentifikation

Die Authentifikation eines Objekts (z.B. Benutzer oder Gerät) ist die Feststellung ihrer Identität aufgrund festgelegter, charakterisierender Merkmale. Kann u.a. durch Passwort-Eingabe, Schlüsseldatei oder Biometrie erfolgen.

B

Benutzerkonto

Hier werden alle Daten eines Benutzers abgespeichert, z.B. Benutzername, Passwort, E-Mailadresse etc.

Biometrie

Die Biometrie steht für die Technik der Erkennung einer Person anhand persönlicher Charakteristika. Der Begriff Biometrie stammt aus dem Griechischen und bildet sich aus den Wörtern „bios" für Leben und „metron" für Maß. Danach ist die Biometrie die Wissenschaft der Körpermessung an Lebewesen. Mit der Biometrie werden physiologische oder verhaltenstypische Charakteristiken des Anwenders zur Authentizität herangezogen. Die Vorteil: Biometrische Merkmale können normalerweise weder vergessen, weitergeben, erspäht oder gestohlen werden.

Bluetooth

Kurzstreckenfunktechnologie („Personal Area Network – PAN") zur Anbindung von Peripheriegeräten per Funk ohne direkten Sichtkontakt zwischen den einzelnen Geräten, siehe „MOB1".

Browserzugriff

Abruf von Webseiten von einem Server über ein Netzwerk mittels eines Browsers.

C

CDO-Modul

Collaboration Data Objets, Schnittstelle für die vereinfachte Anbindung von Messaging-Diensten.

Client-Software / Client-Komponente

Auf dem Endgerät des Benutzers installierte Programme, die ihn befähigen, gemäß seiner Zugangsrechte Daten abzurufen und zu bearbeiten. Erfordert eine serverseitige Gegenstelle.

Companion

Der Rechner, mit dem eine AktiveSync Partnerschaft zu einem Handheld besteht.

Compaq

Hersteller von Computern und Handhelds. Fusionierte Ende 2002 mit HP.

Content Management System

Software zum Verwalten von Inhalten auf Webserver, z.B. im Inter- oder Intranet.

D

Datenbankserver

Zentralrechner, der eine große Menge eingegebener oder automatisch generierter Daten nach einem Ordnungsprinzip verwaltet und bereitstellt.

Demilitarisierte Zone (DMZ)

Eine DMZ ist ein Zwischennetz, das aus Sicherheitsgründen zwischen dem Intranet und dem Internet platziert wird. Sie stellt ein eigenes Netz dar, in dem die Sicherheitsanforderungen geringer als im eigentlichen Intranet sind. Sie wird zu beiden Seiten mit Firewalls abgesichert.

Deployment

Inbetriebnahme einer größeren Anzahl von IT-Systemen in einer Organisation, u.U. mit einer zuvor definierten einheitlichen Konfiguration.

Desktopconnector

Programm der Firma ExtendedSystems für die Synchronisation eines Endgerätes in Verbindung mit einem Desktop-PC. Hierfür wird dieses Programm auf dem Desktop-PC installiert.

Desktop-PC

Arbeitsplatzrechner

DNS-Dummy

Service, der es ermöglicht, Domain-Name-Service-Anfragen innerhalb eines Netzwerkes umzuleiten.

Dockingstation

Hardwaremäßige Schnittstelle zum Verbinden von Endgeräten wie z.B. Handhelds mit einem Desktopcomputer.

Domain-Controller

Ein Domain-Controller ist die zentrale Managementinstanz für ein Microsoft-Netzwerk („Domäne").

E

Endgerät

Siehe Handheld.

Endgerät-Client

Softwarekomponente einer Server-Client-Kombination, die auf dem Endgerät installiert ist und mit der dazugehörigen Serverkomponente zusammenarbeitet.

Extended Systems

Anbieter von Synchronisationssoftware.

F

Features

Leistungsmerkmale von technischen Produkten im Soft- und Hardwarebereich.

Firewall-System

Schutzsystem zur Trennung unterschiedlicher Computernetze. Eine Firewall soll den unautorisierten Zugriff von einem auf das andere Netz unterbinden.

Funktionale Gruppe

Gruppe von verschieden Softwarekomponenten, die zusammen eine bestimmte Funktionalität realisieren.

G

Gateway

Bezeichnung für eine Verbindungs- bzw. Übertragungsstelle zwischen zwei verschiedenen Netzwerken.

GPRS (General Packet Radio System)

Mobilfunkstandard, mit dem sich Daten mit einer Geschwindigkeit von bis zu 115 kbps übertragen lassen; eignet sich auch für den mobilen Zugriff auf das Internet. GPRS basiert auf GSM-Technik, benutzt aber bei der Übertragung das Internet-Protokoll. GPRS ermöglicht die Abrechnung nach übertragener Datenmenge.

Groupware

Software für die Zusammenarbeit von Arbeitsgruppen, Firmen, Institutionen. Diese Software ermöglicht es, Daten auszutauschen und gemeinsam zu nutzen bzw. zu bearbeiten.

Groupware-Server

Auf diesem Server sind die zentralen Komponenten der jeweiligen Groupware installiert und die dazugehörigen Datensätze gespeichert.

Gruppenkonto

Fasst mehrere Benutzerkonten mit denselben Zugriffsrechten zusammen. Vorteil ist, dass Änderungen, die alle Personen einer Gruppen betreffen, effizient durchgeführt werden können.

GSM (Global System for Mobile Communication)

Standard im Mobilfunkbereich. Weltweit (außer USA) verbreitet. Alle deutschen Mobilfunknetze bauen auf diesem Standard auf. Ermöglicht einen Datentransfer von maximal 9,6 kBps.

GSM-Rucksack

Zusatzhardware für iPAQs. Ermöglicht es, mit dem iPAQ GSM und GPRS Verbindungen aufzubauen. Neben dem Datenaustausch wird auch das Telefonieren mit dem iPAQ möglich.

H

Handheld

Handhelds sind mobile Endgeräte, die die ungefähre Größe der Handfläche haben und mit nur einer Hand bedient werden. Die Dateneingabe erfolgt über wenige Tasten und über den Touchscreen mittels eines speziellen Stiftes.

Hewlett Packard

IT-Anbieter, 2002 mit Compaq fusioniert.

http-Zugriff

Siehe: Browserzugriff.

I

Imagedatei

Datei, die den gesamten Inhalt eines Datenträgers zwecks Datensicherung beinhaltet und später wieder zurückgespielt kann.

Infrarot, IrDA-Schnittstelle

Die Infrarotschnittstelle stellt eine drahtlose Verbindung zwischen zwei Geräte her. Die Geräte müssen dabei unmittelbaren „Sichtkontakt" zueinander haben.

Internet Security Acceleration Server (ISA)

Proxy-Komponente von Microsoft für die Synchronisation mittels MIS, daneben noch umfangreiche andere Funktionen wie VPN, Firewall, RAS u.a.

Internet-Provider

Ein Provider stellt einen Zugang zum Internet bereit.

Intranet

Unternehmens- oder verwaltungsinternes Netzwerk, zu dem man nur von bestimmten Rechnern und mittels einer Benutzerkennung Zugang erhält. Basiert auf ähnlichen Technologien wie das Internet.

iPAQ

Handheld von HP, siehe: Handheld.

IP-Bereich

Ist eine vorgegebene Menge von an IP-Adressen, die in einem Netzwerk genutzt werden kann, z.B.:10.xxx.xxx.xxx oder 192.168.xxx.xxx

IP-Paket

Datenpaket, das an eine bestimmte IP-Adresse gerichtet ist.

K

kryptographische Stärke

Beschreibt die Qualität einer Verschlüsselung und seiner Algorithmen.

L

LDAP

Lightweight Directory Access Protocol ist ein Protokoll, welches für den Zugriff auf Informationssammlungen entworfen wurde, angelehnt an das X.500-Dateisystem.

Logging

Automatisches Aufzeichnen von Daten. Die dabei entstehenden Log-Dateien speichern anfallende Daten, z.B. wann, wo und wie lange sich welcher Nutzer an einem System angemeldet hat.

Login

Unter Login versteht man die Anmeldung eines Clients an einem Server. Zu einem Login gehört in der Regel eine Benutzerkennung und ein Passwort.

Lotus Domino

Groupwareanwendung der Firma IBM. Sie bietet ähnliche Funktionen wie Microsoft Exchange an. Der dazugehörige Client ist Lotus Notes.

M

Microsoft PocketPC

Betriebssystem für Handhelds. Es ist ein Single-User-Ssytem.

Microsoft Windows 2000 Advanced Server

Betriebssystem auf NT-Basis für Serveranwendungen.

Mobile Information Server (MIS)

Synchronisationsserver der Firma Microsoft, dient der Anbindung mobiler Endgeräte u.a. an MS Exchange.

Mobile Outlook

Ist der von Microsoft bereitgestellte Mailclient für PocketPC. Mobile Outlook ist fester Bestandteil von PocketPC.

Mobilfunk-Netz

Siehe GSM.

Microsoft Database Engine (MSDE)

Datenbanksoftware der Firma Microsoft.

N

Netztopologie

Systematische Struktur des Netzwerkes in seinen einzelnen Schichten.

Netzwerkarchitektur

Systematischer Aufbau der Hard- und Software eines Netzwerkes mit Clients, Servern, drahtgebundener oder drahtloser Anbindung.

Norton Ghost 2003

Software der Firma Symantec zum Erstellen von Image-Dateien kompletter Betriebssysteme.

O

Öffentliche Ordner

Öffentliche Ordner werden in einem Netzwerk allen berechtigten Nutzern zur Verfügung gestellt und zentral gespeichert und administriert. Sie können Daten aller Art enthalten.

on the fly

Aufgaben, die automatisch und im Hintergrund erledigt werden, z.B. Aktualisierung von Daten.

Outlook

Microsoft Outlook ist ein Groupware-Client. Mit Outlook können E-Mails, Termine, Aufgaben, Kontakte und Notizen verwaltet werde.

P

Pager-Nachrichten

Kurze Textnachrichten, die ähnlich einer SMS versandt und empfangen werden können.

Paketfilter

Filtertyp bei Firewalls. Er lässt nur Pakete durch, die vorgegeben Kritieren (z.B. Quell-IP, Ziel-IP, Portadressen) entsprechen. So können unerwünschte Pakte abgeblockt werden. Für diesen Filter müssen Regeln erstellt werden.

Partnerschaft

Siehe Companion.

PDA

Personal Digital Assistant, siehe Handheld.

PocketExcel

Tabellenkalkulationsprogramm der Firma Microsoft auf dem PocketPC Betriebssystem. Es gehört zur Grundausstattung von Pocket-PC.

PocketOutlook

Mail- und Groupwareclient auf dem PocketPC Betriebssystem. Es gehört zum Grundausstattung von PocketPCs.

PocketPC

Siehe Microsoft PocketPC.

PocketWord

Textverarbeitungsprogramm der Firma Microsoft auf dem PocketPC Betriebssystem. Es gehört zum Grundausstattung von Pocket-PC. Diese Word-Version kann allerdings keine regulären Word-Dateien bearbeiten, diese müssen zuvor umgewandelt werden.

Policy

Nichttechnisches Regelwerk zur Benutzung von Systemen. Richtet sich z. B. an Administratoren und Endnutzer und reguliert u.a. Nutzungsbedingungen, Umgang mit privaten Daten, Nachinstallation von Software uvam.

Port

Ist die allgemeine Bezeichnung von Übergabestellen von Daten oder Adressen. Ports im TCP-Protokoll sind die Schnittstellen zwischen Schicht vier und den Anwendungen. Als Port werden allerdings auch Schnittstellen zwischen Peripheriegeräten bezeichnet.

Port-Forwarding

Das Empfangen uind weiterleiten von Datenpaketen an eine andere Adressen gemäss vorgegebener Regeln. Damit können Zielsysteme vom Absender der Pakete abgeschirmt werden.

Power-on-Passwort

Ist ein Passwort, das unmittelbar nach dem Einschalten eines Gerätes abgefragt wird und ohne dass man keinen Zugriff auf das Gerät erhält.

proprietär

Unter proprietärer Software versteht man Software die auf firmeneigenen, nicht offengelegten Technologien und Standards basiert. Bekanntestes Beispiel sind die Produkte der Firma Microsoft.

Protokoll

Protokolle legen grundsätzlich Verfahrensweisen und Standards fest. Nur auf Basis von Protokollen ist eine Kommunikation der verschiedenen Komponenten im System möglich. Sie kommen zwischen verschieden Rechnerkomponenten, Programmen, Computern oder Netzwerken zum Einsatz. Beispiele: TCP/IP, GSM, GPRS etc.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzwerken. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netzwerk weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten. Der Einsatz von Proxys kann somit die Sicherheit in Netzwerken erhöhen.

Prozessor

Der Prozessor oder auch CPU ist die zentrale Recheneinheit jedes Computers.

Push-Dienst

Hierunter versteht man Dienste, die von einer zentralen Stelle initiiert werden und keine Einflussnahme des Endnutzers notwendig ist.

R

Remote Access Service (RAS)

Technologie zum Zugriff auf Daten und Netzwerkstrukturen über eine beliebige Distanz. Der Weg zwischen dem Endgerät wird über das Telefonnetz ermöglicht. Man benötigt einen RAS-Client, der in der Lage ist eine Telefonverbindung aufzubauen und einen RAS-Server, der sowohl an das Telefonnetz, als auch an das Zielnetzwerk angebunden ist. Wird nun eine Verbindung vom Endgerät aus initialisiert, so nimmt der RAS-Server dieses „Telefonat" an und stellt somit über das Telefonnetz eine Verbindung zum Zielnetzwerk her.

Rechnerdatenblatt

Rechnerdatenblätter wurden im Rahmen diese Projektes angelegt um immer den jeweiligen Ist-Zustand der einzelnen Rechner zu dokumentieren und für alle Beteiligten übersichtlich zu gestalten. Sie enthalten Angaben zu Partitionen, installierter Software und Einstellungen der Netzwerkkarten.

remote

„aus der Ferne"

Remote-Desktop

Programm, das es ermöglicht, über eine Netzwerkverbindung Zugriff und Kontrolle über einen anderen Rechner zu erlangen. Dies bietet Administratoren die Möglichkeit, ihre Aufgaben wahrzunehmen ohne selber persönlich anwesend zu sein.

Replikation

Das exakte Kopieren von Datensätzen an einen anderen Speicherort.

S

Schnittstellen

Schnittstellen sind Verbindungsstellen zwischen verschiedenen Hard- oder Softwarekomponenten. Man unterscheidet zwischen Hardware-, Software-, Netzwerk- und Benutzer-Schnittstellen.

ScreenCopy

Programm zum Erstellen von Screenshoots. Dies Programm ist in der Lage das Erstellen, Benennen und Abspeichern weitestgehend zu automatisieren.

Service

Ist ein Programm, das auf einem Server hin Hintergrund läuft und automatisch gestartet wird.

Service Pack

Sammlung von Updates verschiedener Programmbestandteile. Servicepacks werden in unregelmäßiger Folge vom Hersteller bereitgestellt, um aufgetretene Fehler zu beheben.

Sicherheitskomponenten

Softwarebestandteile, die eine Verbesserung der System- und Programmsicherheit ermöglichen sollen. Sie bieten unter anderen die Möglichkeit zusätzlicher Verschlüsselungen und Passwörter an.

Single-User-Betriebssystem

Betriebssystem, das nur für die Nutzung durch einen Anwender gedacht ist. Z.B. Windows 98 und Pocket PC. Diesen Betriebssystemen fehlen verschiede Möglichkeiten in der Zugriffssteuerung auf die einzelnen Bestandteile und Daten des Systems.

Skript

Eine Art von kleinem Programm, das eine automatisierte Abarbeitung verschiedener Arbeitsschritte ermöglicht.

SMS

Short Message Service. Standart zum Versenden und Empfangen von Textnachrichten auf Mobiltelefonen. Die Länge ist auf 160 Zeichen beschränkt.

SQL-Server

Server zur Verwaltung von Datenbanken. SQL Server bieten einheitliche Schnittstellen, die eine Anbindung an andere Softwareprodukte ermöglichen.

SSL-Verschlüsselung

Secure Socket Layer. Sichere Übertragungsmethode, bei der über einen Schlüssel und eine darin enthaltene Prüfsumme eine sichere Identifikation des Servers und eien Überprüfung des Inhaltes möglich wird.

Switch

Gerät zum Verbinden mehrer Computer auf Netzwerkebene.

Synchronisation

Ist der Abgleich von Datensätzen zwischen verschieden Speicherplätzen, z.B. Server und Endgerät.

Synchronisations-Client

Softwarekomponente, die die Synchronisation auf Seiten des Endgerätes ermöglicht.

Synchronisationskomponente

Softwarekomponente, die die Synchronisation zwischen Geräten ermöglicht.

Systemarchitektur

Grundlegender Aufbau und Struktur von Systemen und Netzwerken

T

Tasks

Aufgaben, die im Rahmen von automatisierten Vorgängen vorgegeben und abgearbeitet werden.

Thermischer Fingerabdruckscanner

Gerät zum Abtasten des Fingerabdruckes auf Wärmebasis. Hierbei wird das Muster des Fingerabdruckes nicht optisch, sondern über minimale Temperaturunterschiede in der Oberfläche der Fingerkuppe ermitteln.

Transparent

Ist ein System transparent, so ist seine Funktionsweise einfach nachvollziehbar.

U

USB

Univarsal Serial Bus. Multifunktionale Schnittstelle an PCs zum Anschluss verschiedenster Peripheriegeräte. Die Schnittstelle ist „hotcutable", das heißt, Geräte können im laufenden Betrieb angeschlossen und abgezogen werden, ohne dass ein Systemneustart erforderlich ist. Wird von allen gängigen Betriebssystemen außer NT unterstützt.

USB-Stick

Mobiler, nicht flüchtiger Speicher, der direkt an die USB-Schnittstelle angeschlossen wird. USB-Sticks gibt es bis zu einer Kapazität von 1 GB.

V

Verbindungsart

Verschiedene technische Lösungen für den Austausch von Daten zwischen Rechnern, entweder drahtgebunden oder drahtlos.

VPN

Technologie, um einen abgesicherten Kanal (Tunnel) zwischen Netzwerken aufzubauen.

VPN-Komponenten

Für VPN-Verbindungen sind ein VPN-Server mit einer Schnittstelle zum Internet und ein VPN-Client notwendig.

VPN-Tunnel

Sichere Verbindung zwischen VPN-Server und Client, über den das lokale Netzwerk vom mobilen Endgerät erreicht werden kann.

W

Webproxies

Stellvertreter, der http-Zugriffe zwischenspeichert und Anfragen weiterleitet. Erhöht die Sicherheit.

Web-Server

Server, der Inhalte von Webseiten in Netzwerken bereitstellt. Webserver gibt es in Internet, aber auch im Intranet. Ihre Inhalte werde mittels eines Browsers abgerufen.

WLAN

Standard zur kabellosen Netzwerkverbindung. Siehe auch MOB1

Work around

Work around bezeichnet die Umgehung eines Problems. Work-Arounds stellen im Allgemeine keine perfekte, aber eine durchaus praktikable Lösung eines Probleme dar.

X

XTND

Siehe Extended Systems.

XTND Client

Synchronisationskomponente von der Firma XTND, die auf dem Handheld installiert ist.

XTND Connect Desktop Connector

Siehe Desktop Connector.

XTND Connect Proxy Server

Proxy-Komponente des xTND-Systems, die den Datenaustausch zwischen Intranet und dem Endgerät über die DMZ realisiert.

XTND Connect Server

Synchronisationskomponente, die die jeweiligen Groupware-Daten aus der Groupware-Anwendung heraus für die Synchronisation bereitstellt.