INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Konzept für eine PKI im internationalen Umfeld

Akos Regi

Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering

Betreuer: Ralf König
Dr. Harald Rölle

Abgabetermin: 13. März 2006

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Konzept für eine PKI im internationalen Umfeld

Akos Regi

Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering

Betreuer: Ralf König
Dr. Harald Rölle

Abgabetermin: 13. März 2006

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den 13. März 2006

.....

(Unterschrift des Kandidaten)

Zusammenfassung

Das Ziel dieser Diplomarbeit war die Untersuchung der Möglichkeiten für den Einsatz einer PKI in internationalem Umfeld und Entwurf eines Konzepts. Da in den meisten Unternehmen bereits einige Strukturen und Prozesse vorhanden sind, mussten diese auch beachtet und untersucht werden. Ziel ist natürlich die Sicherung der Prozesse und bei Möglichkeit auch eine Vereinfachung und Konsolidierung der Ressourcen. Schwierigkeiten bereiten in einem internationalen Unternehmen nicht nur die Größe, sondern auch die Verteilung der Standorte und Abteilungen.

Inhaltsverzeichnis

1 Einleitung **1**
- 1.1 Motivation . . . 1
- 1.2 Aufgabenstellung . . . 2
- 1.3 Gliederung . . . 2

2 Anwendungsfälle und Prozesse **3**
- 2.1 IT Sicherheit im allgemeinen . . . 3
- 2.2 IT Prozesse in einem Unternehmen . . . 4
- 2.3 Definition von grundlegenden Anwendungsfällen . . . 5
  - 2.3.1 Verschlüsselung . . . 6
  - 2.3.2 Digitale Signatur . . . 7
  - 2.3.3 Authentifizierung . . . 10

3 Ist-Stand: vorhandene Anwendungsfälle **11**
- 3.1 Emailverschlüsselung . . . 12
  - 3.1.1 Bemerkung zu den Verschlüsselungsstandards . . . 12
  - 3.1.2 Bemerkung zu den Cryptomaterialien . . . 14
  - 3.1.3 Umfeld der Emailverschlüsselung . . . 14
  - 3.1.4 Bestellung von PGP Schlüsselpaaren . . . 20
  - 3.1.5 Das Bestellformular für PGP Schlüsselpaare . . . 22
  - 3.1.6 Authentifizierung und Autorisierung der Bestellung . . . 23
  - 3.1.7 Generierung des PGP Schlüsselpaares . . . 24
  - 3.1.8 Verteilung von generierten PGP Schlüsselpaaren . . . 26
  - 3.1.9 Importvorgang eines PGP Schlüsselpaares . . . 26
  - 3.1.10 Veröffentlichung des öffentlichen PGP Schlüssels . . . 28
  - 3.1.11 Verwendung der Emailverschlüsselung mit PGP Schlüssel . . . 29
  - 3.1.12 Wiederbereitstellung von PGP Schlüsselpaaren . . . 31
  - 3.1.13 Widerruf von PGP Schlüsseln . . . 31
  - 3.1.14 Emailverschlüsselung mit Geschäftspartnern . . . 32
  - 3.1.15 Lebenszyklus . . . 32
  - 3.1.16 Zusammenfassung und Bewertung . . . 33
- 3.2 Emailsignatur . . . 35
  - 3.2.1 Verwendung der Emailsignatur . . . 36
- 3.3 Dateiverschlüsselung . . . 36
  - 3.3.1 Verwendung der Dateiverschlüsselung . . . 36
  - 3.3.2 Verwendung der Verzeichnisverschlüsselung . . . 36
- 3.4 Dateisignatur . . . 40
  - 3.4.1 Verwendung der Dateisignatur . . . 40

3.5 Code-Signatur 41
3.5.1 Bestellung 42
3.5.2 Verwendung 43
3.5.3 Bewertung 43
3.6 Dokumentensignatur 43
3.6.1 Bestellung 44
3.6.2 Verwendung 44
3.7 Benutzerauthentifikation 44
3.7.1 Bestellung des Authentifizierungszertifikates 44
3.7.2 Verteilung des Authentifizierungszertifikates 44
3.7.3 Import des Authentifizierungszertifikates 45
3.7.4 Verwendung des Authentifizierungszertifikates 45
3.7.5 Widerruf des Authentifizierungszertifikates 45
3.7.6 Wiederbereitstellung des Authentifizierungszertifikates 45
3.7.7 Bewertung 45
3.8 Sonstige Anwendungsfälle 46
3.8.1 VPN-Authentifizierung 46
3.8.2 WEB-Serverauthentifizierung 47
3.8.3 Emailverschlüsselung mittels S/MIME 47
3.8.4 Bewertung der sonstigen Anwendungsfälle 47

4 Anforderungen **48**
4.1 Anforderungen an die Emailverschlüsselung 48
4.1.1 Organisatorische Anforderungen 48
4.1.2 Technische Anforderungen an die Emailverschlüsselung . . . 53
4.1.3 Gewährleistung der Interoperabilität 56
4.2 Anforderungen an die Emailsignatur 57
4.2.1 Organisatorische Anforderungen 57
4.2.2 Technische Anforderungen 58
4.2.3 Anforderungen an das Signaturmaterial 59
4.3 Anforderungen an die Dateiverschlüsselung 59
4.4 Anforderungen an die Benutzerauthentifizierung 60
4.4.1 Organisatorische Anforderungen 60
4.4.2 Technische Anforderungen 60
4.5 Zusammenfassung der Anforderungen 60

5 Umsetzungsmöglichkeiten **65**
5.1 Umsetzungsmöglichkeiten im Allgemeinen 65
5.1.1 Die ausgelagerte Lösung 65
5.1.2 Die verteilte Lösung 68
5.1.3 Die eigene Lösung 69
5.2 PKI im Allgemeinen 70
5.2.1 Unterschied zwischen PGP und X.509 PKI 71
5.2.2 Standardkomponenten 71
5.2.3 Andere in der Fachliteratur erwähnten Einheiten 75
5.3 Certificate Lifecycle Management 75
5.3.1 Initialisierungsphase 76
5.3.2 Verwendungsphase 78
5.3.3 Vernichtungsphase 78
5.4 Eigene Lösung: Möglichkeiten für die E-Mail-Verschlüsselung 80

5.4.1 Organisatorische Prozesse 80
5.4.2 Technische Strukturen 86
5.5 Umsetzungsmöglichkeiten für die Emailsignatur 94
5.5.1 Wahl des Cryptomaterials 94
5.6 Umsetzungsmöglichkeiten für die Benutzerauthentifizierung 94
5.6.1 Organisatorische Prozesse 94
5.6.2 Technische Strukturen 95
5.7 Umsetzungsmöglichkeiten für die Dateiverschlüsselung 95
5.7.1 Organisatorische Prozesse 96
5.7.2 Technische Strukturen 96
5.8 Umsetzungsmöglichkeiten für die Dateisignatur 100
5.9 Umsetzungsmöglichkeiten für die Dokumentensignatur 100
5.10 Umsetzungsmöglichkeit für Serverprodukte 101
5.10.1 Microsoft CA 101
5.10.2 OpenCA 101
5.10.3 PGP Enterprise CA 102
5.10.4 Neuentwicklung der CA Software 102
5.10.5 Vergleich der Produkte 102
5.11 Vertrauensmodell 104
5.11.1 Definition von Vertrauen 104
5.11.2 Verschiede Vertrauensmodelle: 105
5.12 Informationsrepräsentation 109
5.12.1 Informationsrepräsentation in der Struktur 109
5.12.2 Informationsrepräsentation im Objekt 109
5.12.3 Informationsrepräsentation in einer Datenbasis 109
5.12.4 Bewertung der Möglichkeiten für die Informationsrepräsentation 109

6 Konzepte **111**
6.1 Berechtigungskonzept 111
6.1.1 Rollen in der PKI 111
6.1.2 Berechtigungen 112
6.2 Organisatorisches Prozesskonzept 114
6.2.1 Registration des Mitarbeiters 114
6.2.2 Authentifizierung des Mitarbeiters 115
6.2.3 Autorisierung der Bestellung 115
6.2.4 Schlüssel- bzw. Zertifikatsgenerierung 116
6.2.5 Auslieferung von Schlüsselmaterialien 116
6.2.6 Veröffentlichung der Schlüsselmaterialien 117
6.2.7 Sicherung von Schlüsselmaterial (Backup) 117
6.2.8 Import von Schlüsselmaterial 117
6.2.9 Ablauf von Schlüsselmaterial 117
6.2.10 Widerruf von Schlüsselmaterial 118
6.3 Technisches Prozesskonzept 118
6.4 Konzept für die Emailverschlüsselung 120
6.4.1 Konzept für die Bestellung von Cryptomaterial für Emailverschlüsselung 120
6.4.2 Konzept für die Verwendung von Cryptomaterial für Emailverschlüsselung 121
6.4.3 Wiederbereitstellung von Schlüsselmaterial 121
6.4.4 Bereitstellung von Schlüsselmaterial (escrow) 122

6.4.5 Ablauf und Widerruf von Cryptomaterial für Emailverschlüsselung . . . 122
6.4.6 Technisches Konzept für die Emailverschlüsselung . . . 122
6.5 Konzept für die Emailsignatur . . . 126
6.5.1 Organisationskonzept für die Bestellung von Cryptomaterial für Email-signatur . . . 126
6.5.2 Technisches Konzept für die Emailsignatur . . . 126
6.6 Konzept für die Benutzerauthentifizierung . . . 128
6.6.1 Organisatorisches Konzept für die Benutzerauthentifizierung . 129
6.6.2 Technisches Konzept für die Benutzerauthentifizierung . . . 130
6.7 PKI Strukturkonzept . . . 132
6.7.1 PKI Architektur . . . 132
6.7.2 Struktur für die Registrationsstelle . . . 132
6.7.3 Struktur für die Zertifikatsstelle . . . 133
6.7.4 Zertifikatsbasis . . . 134
6.7.5 Endeinheiten . . . 135
6.7.6 Wahl der CA Software . . . 136

7 Migration **137**
7.1 Serverseitige Migration . . . 137
7.1.1 Einrichtung der Wurzel CA . . . 137
7.1.2 Einrichtung der ausstellenden CA . . . 137
7.1.3 Einrichtung von Schutzmechanismen . . . 138
7.1.4 Einrichtung des neuen Keyservers . . . 139
7.2 Clientseitige Migration . . . 139
7.2.1 Einrichtung von Testclients . . . 140
7.2.2 Pilotphase . . . 140
7.2.3 Vorbereitung der neuen Clientsoftware zur automatisierten Softwareverteilung . . . 140
7.2.4 Verteilung der neuen Clientsoftware . . . 142
7.2.5 Verteilung der CA Zertifikate . . . 142

8 Zusammenfassung und Ausblick **144**
8.1 Ausblick . . . 144

A Anforderungen an die Verschlüsselungsverfahren **145**
A.1 Shannon'sche Kriterien: . . . 145

B Anhang B: PGP Standards **147**

C Eigenschaften der Authentifizierungszertifikate **151**

D Beispiel für eine Unternehmenspolicy **153**

Abbildungsverzeichnis

2.1 Anwendungsfälle für Authentifizierung 10

3.1 Einfachster Fall für die Emailverschlüsselung 16
3.2 Komplexer Fall für die Emailverschlüsselung 17
3.3 PGP Schlüssellebenszyklus 18
3.4 Outlook mit der Verschlüsselungssoftware 19
3.5 Anwendungsfall Emailverschlüsselung 20
3.6 Ablauf des Bestellvorganges 21
3.7 Datenfluss der Mitarbeiterdaten 24
3.8 Ändern des Initialpasswortes 28
3.9 Funktionsweise der Emailverschlüsselung 30
3.10 Setzen des Pfades zu der Containerdatei 37
3.11 Eigenschaften der Verschlüsselung von der Containerdatei 38
3.12 Verschlüsselungsschlüssel der Containerdatei 38
3.13 Benennung des lokalen Datenträgers und Wahl des Dateisystems . . . 39
3.14 Zuweisung eines Laufwerksbuchstaben 39
3.15 Dateiverschlüsselung mit CryptoEx File 39
3.16 Dateiverschlüsselung mit CryptoEx File 40
3.17 Dateisignatur mit CryptoEx File 41
3.18 Sicherheitsebenen der Office Anwendungen 42
3.19 Anzeigefenster von Digitaler Signatur 43

5.1 Funktionsschema einer PKI im allgemeinen (Quelle:[SSX02]) 71
5.2 Lifecycle Management 76
5.3 Erste Umsetzungsmöglichkeit für den Bestellprozess 83
5.4 Erste Umsetzungsmöglichkeit für den Zertifikatswiderruf 84
5.5 Erste Umsetzungsmöglichkeit für die Zertifikatswiederbereitstellung . 84
5.6 Zweite Umsetzungsmöglichkeit für den Bestellprozess 85
5.7 Funktionsweise der Proxylösung bei Ciphire Mail (Quelle:Ciphire Mail) 87
5.8 Hierarchisches Vertrauensmodell: Single CA 105
5.9 Oligarchie von CAs 106
5.10 Hierarchisches Vertrauensmodell: Top-Down 107

6.1 Benutzerauthentifizierung bei der Bestellung 119
6.2 Generierung, Auslieferung und Veröffentlichung von Schlüsselmaterial 119
6.3 Mögliche Netzwerkstruktur für eine PKI 132

Tabellenverzeichnis

2.1 Signaturarten und deren Vergleich (Quelle:[BSK02]) 9

3.1 Berechtigungsmatrix für PGP Schlüsselbestellungen 22
3.2 Bestellformular für PGP Schlüsselpaar 23
3.3 Eigenschaften von PGP Schlüsselpaar 25
3.4 Bedeutung der Vertrauensbezeichnungen bei PGP 29
3.5 Wiederbereitstellung von PGP Schlüsselpaaren 31

4.1 Berechtigungsmatrix für PGP Schlüsselbestellungen 49
4.2 Möglichkeiten verschiedener Standards 53
4.3 Empfohlene Schlüssellänge für asymmetrische Schlüssel (Quelle: [SCHB01]) 54
4.4 Anforderung an die Schlüssel und Zertifikate für Emailverschlüsselung 62
4.5 Anforderung an das Benutzerauthentifizierungszertifikat 63
4.6 Anforderung an die Schlüssel- und Zertifikate 64

5.1 Vergleich der verschiedenen Ansätze für Registrationsstellen 82
5.2 Produktvergleich der clientseitige Lösungen für die Emailverschlüsselung 90
5.3 Vergleich verschiedener Lösungen zur Emailverschlüsselung 93
5.4 Vergleich verschiedener Clientsoftware 99
5.5 Vergleichsmatrix der CA Produkte 103
5.6 Zusammenfassung und Bewertung der Möglichkeiten für die Informationsrepräsentation 110

6.1 Eigenschaften des neuen PGP Schlüsselpaares 124
6.2 Beschaffenheit des X.509 Zertifikats für die Emailverschlüsselung . . 125
6.3 Eigenschaften des neuen PGP Schlüsselpaares 128
6.4 Beschaffenheit des X.509 Zertifikats für die Emailsignatur 129
6.5 Beschaffenheit des X.509 Benutzerauthentifizierungszertifikats 131

Kapitel 1

Einleitung

Diese Diplomarbeit wurde in dem Bereich der IT Sicherheit an dem Lehrstuhl für Systemnahe Programmierung an der Ludwig Maximilians Universität München (**L**udwig **M**aximilians **U**niversität) erstellt. Diese Diplomarbeit beschäftigt sich mit dem Konzept zum Aufbau einer PKI im internationalen Umfeld. Die Diplomarbeit wurde bei einem Unternehmen erstellt.

1.1 Motivation

Mit der Entwicklung der Informationstechnologie verbreitete sich die Informationsdigitalisierung, weshalb die Anzahl der digitalisierten Informationen in der letzten Zeit stark gestiegen ist. Vor ein paar Jahren wurde sogar der Ruf nach einem papierlosen Büro aus diesem Grund immer lauter. Analysten sagten sogar damals, dass das papierlose Büro in der näheren Zukunft verwirklicht wird. Wie wir wissen, kam es nicht dazu. Ein papierloses Büro setzt nämlich voraus, dass berechtigte Personen jeder Zeit ein beliebiges Dokument in authentischer Form vorlegen und bei Bedarf ausdrucken können. Dazu gehört natürlich auch die Überprüfung der Authentizität des Dokuments. Dies benötigt aber auch die Speicherung der Dokumente in authentischer Form und bei Bedarf sogar in verschlüsselter Form. Im heutigen Wirtschaftsleben gewinnt der Besitz und zeitgerechte Zugriff auf Informationen immer mehr an Bedeutung. Parallel zu der immer stärkeren Technologisierung der eingesetzten Ressourcen steigen allerdings auch die damit verbundenen Risiken, gerade in Hinblick auf die Informationssicherheit. Das Handling dieser Risiken und der sachgemäße Umgang mit vertraulichen Informationen stellen einen wesentlichen Faktor für die Wettbewerbsfähigkeit eines Unternehmens dar, da die Geheimdienste den Emailverkehr abhören und wichtige geschäftliche Informationen an die heimische Wirtschaft verkaufen und zur Verfügung stellen. ([Wri98b, Wri98a, SH98b, stw97, Hag96, Hag97, Ebe98, CCC99])

Diese Diplomarbeit befasst sich mit dem Entwurf eines Konzeptes für eine Public-Key-Infrastruktur (**P**ublic **K**ey **I**nfrastructure = PKI) in einem verteilten Umfeld. Ziel ist die Erstellung eines Konzeptes anhand der Anforderungen. Nach Untersuchung vorhandener Lösungen und nach der Vorstellung der Lösungsmöglichkeiten sollen die Konzepte anhand der Anforderungen erstellt werden.

1.2 Aufgabenstellung

Im Rahmen dieser Diplomarbeit wird untersucht, welche Prozesse in einem Unternehmen vorhanden sind, wie man diese mit technisch verbessern und absichern kann. Dies alles soll unter Beachtung der vorhandenen verteilten Infrastruktur geschehen. Die Infrastruktur besteht aus 100 weltweit verteilten Standortorten in 30 Ländern. Diese Infrastruktur wird von 6000 Mitarbeitern täglich rund um die Uhr benutzt.
Es gibt zwar eine Infrastruktur und einige Prozesse, die die Aufgaben einer PKI teilweise behandeln, diese müssen aber auch untersucht werden, ob und wie sich diese vorhandenen Prozesse zu einer PKI, die den Anforderungen entspricht, ausbauen lassen, oder ob neue Prozesse und Strukturen geschaffen werden müssen. Die Ziele sind die Absicherung der Prozesse mit Hilfe einer PKI in einer verteilten Umgebung. Verteilt heißt hier nicht nur, dass es mehrere Client bzw. Server gibt, sondern die Client und Server verteilt an verschiedenen Orten in verschiedenen Ländern mit verschiedenen Gesetzen und Infrastruktur vorliegen. In dieser Diplomarbeit wird auch untersucht, ob diese verteilte Struktur eine Auswirkung auf das Konzept einer PKI hat. Falls eine Auswirkung feststellbar ist, wird die Auswirkung auf die einzelnen Komponente einer PKI gezeigt.

1.3 Gliederung

Zuerst werden einige grundlegende Anwendungsfälle definiert. Die vorhandenen Prozesse werden in diese grundlegende Aufteilung eingeordnet, soweit es möglich ist. So werden eventuelle Defizite und Unsicherheiten deutlich. Ausgehend aus der Bewertung der vorhandenen Lösungen, wir ein Anforderungskatalog erstellt. Als nächstes wird ein allgemeiner Lösungsansatz beschrieben. Anhand des Anforderungskataloges und der Bewertung der der vorhandenen Lösungen wird versucht, ein realisierbares Konzept mit eventuellen Kompromissen erstellt zu werden.

Kapitel 2

Anwendungsfälle und Prozesse

Sicherheitsaktivitäten im Unternehmen haben im Sinne der Sicherstellung der einwandfreien Funktion IT-technischer Einrichtungen und Abläufe die Zielsetzung, einerseits die Verfügbarkeit von Servern, Netzwerken und Anwendungen als auch andererseits den Schutz von Daten gegen unberechtigten Zugriff und Manipulation zu gewährleisten.
Durch die zunehmende Digitalisierung und Vernetzung ergibt sich eine rasante Zunahme des Gefährdungspotentials von geschäftskritischen Daten, Anwendungen und Netzen. Im Zuge dieser Überlegungen ergibt sich die Notwendigkeit einer Überprüfung der bisherigen Lösungen und - wo notwendig und sinnvoll - einer Integration vorhandener bzw. neuer Prozesse und Lösungen im gesamten Unternehmen. All dies sind Aufgaben der IT Sicherheit, die im nächsten Abschnitt kurz beschrieben werden.

2.1 IT Sicherheit im allgemeinen

Der Bereich der IT Sicherheit ist ein breites Gebiet. Ziel der IT Sicherheit ist Vertraulichkeit, Verfügbarkeit und Integrität [BSI 04] zu gewährleisten. Diese Ziele sind in Standards (z. B. [OSI7498-2]) und Empfehlungen [OSI7498-2] festgelegt.

Unter Vertraulichkeit versteht man Schutz vor unbefugter Kenntnisnahme.

Integrität bedeutet Schutz vor Veränderung der Daten.

Verfügbarkeit beinhaltet Schutz der Ressourcen gegenüber Angriffen, die die Nutzbarkeit der Ressource beeinträchtigen.

Die Erstellung einer Sicherheitsrisikoanalyse bzw. Risikomanagement wird ebenfalls als Aufgabe der IT Sicherheit verstanden. Die Unternehmen werden durch verschiedene Gesetze (siehe [BSI 04, Seite 8]) zur Erstellung eines IT (Sicherheits-) Risikomanagement verpflichtet. Dabei geht es um einen umfassenden organisatorischen Plan und Maßnahmenkatalog. [HOBII] Diese dienen als Grundlage zur Berechnung des operationellen Risikos, das zur Berechnung des erforderlichen Eigenkapitals im Rahmen von Basel II (http://www.basel-ii.info) herangezogen wird.
In dieser Diplomarbeit werden natürlich nicht alle Themen der IT Sicherheit behandelt. Das Thema wird auf die Erstellung eines Konzepts für eine PKI (**P**ublic **K**ey

Infratstucture) eingeschränkt. Eine PKI ist ein Hilfsmittel für die Unterstützung der Absicherung kritischer Unternehmensprozesse.

2.2 IT Prozesse in einem Unternehmen

Es zeigt sich in der Praxis, dass bei einer umfassenden Sicherheitslösung sowohl für die äußere als auch für die innere Sicherheit Maßnahmen gesetzt werden müssen. Absolute Sicherheit kann mit reinen technischen Systemen grundsätzlich nicht erreicht werden. Die zunehmende Abhängigkeit der Geschäftsprozesse von Informations- und Kommunikationswegen verlangt Schutzmaßnahmen zur Gewährleistung der optimalen Informationssicherheit des Unternehmens. Aus der technologischen Entwicklung ergibt sich die Notwendigkeit einer unternehmensweiten Sicherheitsstrategie. Das langfristige Ziel eines optimal umgesetzten Sicherheitsmanagements ist die Integration von Sicherheit in alle Bereiche des Unternehmens. Um dieses Ziel zu erreichen gilt es die folgenden Punkte im Auge zu behalten:

- Sicherheit muss als unabdingbare Notwendigkeit ins Bewusstsein der Mitarbeiter und Führungskräfte übernommen werden.
- Es muss eine gelebte Sicherheit im Unternehmen geben. Jeder Einzelne soll aktiv zur Unternehmenssicherheit beitragen.
- Gelebte Sicherheit ist Voraussetzung für die Wettbewerbsfähigkeit des Unternehmens.
- Sicherheit ist ein Prozess, der die Arbeit möglichst wenig beeinträchtigen soll.
- Angemessene Unterstützung von Software und Hardware zur Informationssicherheit sollen transparent für den Anwender die Geschäftsprozesse des Unternehmens schützen.

Es gibt im Unternehmen Prozesse die bereits in elektronischer Form ablaufen, aber noch nicht in gesicherter Umgebung. Ziel der Untersuchung ist diese Prozesse sicher(er) zu gestalten. Wenn der bisherige Aufwand sich bei einigen Prozessen sogar minimieren lässt und die Prozesse sich eventuell auch noch konsolidieren lassen, bedeutet dies natürlich einen zusätzlichen Bonus, von den Kosten ganz zu schweigen.
Was das in der Praxis bedeuten könnte, wird an den folgenden Beispielen gezeigt.

1. Bei den mittelständischen Unternehmen ist es inzwischen üblich die Reisekostenabrechnung über das Intranet zu erledigen. Diese und ggf. auch andere Intranetseiten benötigen eine sichere Verbindung. Die Sicherung solcher Seiten geschieht mittels HTTPS Protokoll. Zur Verwendung des HTTPS Protokolls benötigt der Webserver ein von einer CA unterschriebenes Zertifikat.
2. Es gibt Intranetseiten und Intranetapplikationen die eine Anmeldung erfordern. Eine Anmeldung ist nach der herkömmlichen Login und Passwortmethode nicht mehr zeitgemäß und nicht sicher genug. Eine Lösung bietet hier die zertifikatsbasierte Anmeldung. Sie erfordert aber nicht nur ein Zertifikat sondern auch eine serverseitige Infrastruktur, deren Komplexität von der Aufwändigkeit der Zertifikatsprüfung abhängig ist.

3. Es gibt Mitarbeiter die viel unterwegs sind. Sie müssen auch über das Internet auf das Unternehmensnetzwerk zugreifen können. Der Zugriff soll aber in sicherer Umgebung erfolgen. Eine VPN (**V**irtual **P**rivate **N**etwork - virtuelles privates Netzwerk) Verbindung ermöglicht den sicheren Zugriff auf das Firmennetzwerk. Je nach Konfiguration benötigt eine VPN Infrastruktur unter anderem auch Zertifikate.

4. Es gibt aber auch Informationen die nicht nur von außen geschützt transferiert werden müssen, sonder auch authentisch. Dazu verwendet man in der Regel eine Dokumentensignatur. Falls das Dokument eine E-Mail ist, soll überlegt werden, ob ein Unterschied zwischen E-Mail- und Dokumentensignatur gemacht werden muss. Die Dokumentensignatur erfordert auch Cryptomaterial.

5. Es ist heutzutage auch erforderlich, dass bestimmte Informationen in verschlüsselter Form verteilt werden. Dabei soll ebenfalls geprüft werden, ob es einen Unterschied zwischen Dokumenten- und E-Mailverschlüsselung gibt. Alle gängigen Emailverschlüsselungsstandards arbeiten mit schlüsselbasierten Algorithmen.

Zu all diesen Prozessen benötigt man Verschlüsselungsmaterial, das natürlich auch verwaltet werden muss. Die Komplexität und Schwierigkeit der Verwaltung wächst mit ansteigender Anzahl der Mitarbeiter und mit derer örtlicher Verteilung. Dazu benötigt man in der Regel eine Technik, besser gesagt eine Infrastruktur. Diese Infrastruktur wird in der Fachliteratur PKI (**P**ublic **K**ey **I**nfrastructure) genannt. Das Betreiben einer PKI benötigt ebenfalls Prozesse und Vorschriften. Diese Prozesse und Vorschriften entstehen aus den Anforderungen des Unternehmens.
Um aber die Unternehmensprozesse zu sichern, müssen diese beschrieben werden. Durch die Prozessbeschreibung werden die Schwachstellen eines Prozesses erkennbar. Demnach gibt es zwei Klassen von Prozessen:

die ursprünglichen Prozesse, die man versucht abzusichern

die neuen Prozesse, die durch diese Absicherung und Einführung neuer Technik entstehen.

Durch die Beschreibung und Aufdeckung der Schwachstellen vorhandener Prozesse und aus den Anforderungen entstehen die neuen Prozesse. Um aber diese neuen Prozesse definieren zu können, was notwendig ist, muss man auch die ursprünglichen Prozesse gut kennen und beschreiben zu können.
Die Prozesse können Anwendungsfällen zugeordnet werden. Deshalb wird zuerst auf die Anwendungsfälle eingegangen.

2.3 Definition von grundlegenden Anwendungsfällen

Die grundlegenden Anwendungsfälle lassen sich aus den Zielen der IT Sicherheit (vgl. Abschnitt 2.1) ableiten. Demnach können die folgenden grundlegenden Anwendungsfälle definiert werden:

- Verschlüsselung
- Digitale Signatur
- Authentifizierung

Die meisten Anwendungsfälle lassen sich in dieses Schema einordnen. Weil diese grundlegenden Anwendungsfälle als Ausgangspunkt dienen, werden diese in den folgenden Abschnitten vorgestellt.

2.3.1 Verschlüsselung

Bei der Verschlüsselung handelt es sich um sichere Kodierung mit Hilfe eines Verschlüsselungsverfahrens von im Klartext vorliegender Information, die sich nicht ohne weiteres Dekodieren lässt. Die Kodierung soll so gewählt werden, dass der Aufwand für die Dekodierung möglichst hoch ausfällt. Die Kodierung soll aber immer und ohne Informationsverlust von berechtigten Personen dekodierbar sein.

Einteilung der Verschlüsselungsverfahren

Nachdem die Kriterien für Verschlüsselungsverfahren bekannt sind, muss die Klassifizierung der Verfahren bekannt gemacht werden, damit die Grundlage für die Schlüsselproblematik ersichtlich wird. Bisher wurde noch nicht über Schlüssel gesprochen. Was genau ein Schlüssel ist, wird nach der Definition von asymmetrischem Verschlüsselungsverfahren offensichtlich.

Schlüssellose Verfahren erfordern keinen kryptographischen Schlüssel. Wichtige Vertreter dieser Gruppe sind die so genannten Hashfunktionen. Hashfunktionen bilden große Datenmengen auf vergleichsweise kleine Datensätze einer festen vorgegebenen Länge ab. Der Hashwert einer Nachricht ist eine für die jeweilige Nachricht charakteristische Prüfsumme. Hashfunktionen werden im Zusammenhang mit der Erstellung elektronischer (oder digitaler) Signaturen verwendet. Anstatt eine lange Nachricht zu signieren, wird der im Allgemeinen viel kürzere Hashwert der Nachricht signiert.

Symmetrische Verfahren - secret key cryptography verwenden denselben Schlüssel zum Verschlüsseln und zum späteren Entschlüsseln der Nachricht. (Manchmal sind Ver- und Entschlüsselungsschlüssel auch verschieden; es ist dann aber möglich den einen von ihnen leicht aus dem anderen zu berechnen.) Symmetrische Chiffrierverfahren werden auch konventionelle Chiffrierverfahren genannt. Die Sicherheit dieser Verfahren beruht auf der Geheimhaltung des Verschlüsselungsschlüssels. Die Kommunikationspartner müssen den Schlüssel geheim halten und auf gesichertem Weg austauschen. Die Authentizität der Information hängt von der Geheimhaltung des Schlüssels ab.

Asymmetrische Verfahren - public key cryptography verwenden zum Ver- und Entschlüsseln verschiedene Schlüssel. Jeder Teilnehmer besitzt einen (geheim zu haltenden) vertraulichen Schlüssel (Private Key) und einen nicht geheimen öffentlichen Schlüssel. Aus dem vertraulichen Schlüssel kann der öffentliche berechnet werden, aus dem öffentlichen aber nicht der vertrauliche. Wendet man beide Schlüssel nacheinander (in beliebiger Reihenfolge) auf eine beliebige Nachricht an, so erhält man stets wieder die ursprüngliche Nachricht. Asymmetrische Chiffrierverfahren werden auch Chiffrierverfahren mit öffentlichen Schlüsseln genannt. Bei diesem Verfahren, da der öffentliche Schlüssel frei zugänglich ist, kann die Authentizität der verschlüsselt übertragenen Information nur mit Hilfe einer Signatur gewährleistet werden.

2.3.2 Digitale Signatur

In der Einführung wurde über das papierlose Büro geschrieben. Demnach kann es notwendig sein, dass die Authentizität eines Dokuments gewährleistet sein muss. Die Authentizität ist durch digitale Signatur zu erreichen. Die digitale Signatur wird oft mit der einegnhändigen Unterschrift verglichen.
Bei einem Vertragsabschluss wird der Vertrag in der Regel in der Anwesenheit des Vertragspartners oder eines Notars unterschrieben.

Klassifizierung der Signaturen

Bei der digitalen Signatur ist dagegen die Anwesenheit des Geschäftspartners bzw. eines Notars nicht erforderlich, weil die Authentizität des Dokuments die digitale Signatur gewährleistet. Die Authentizität des Dokuments kann anhand der Prüfung der digitalen Signatur des Dokuments festgestellt werden. Die digitalen Signaturen werden aber in mehrere Klassen geteilt. Diese Signaturklassen sind:

- Normale oder einfache Signatur
- Fortgeschrittene Signatur
- Qualifizierte Signatur

Diese Klassifizierung bedeutet aber auch, dass sie die Verbindlichkeit der verschiedenen Signaturen unterschiedlich ist. Bei der einfachen Signatur handelt es sich um eine Signatur, mit deren Hifle nur die Integrität nicht aber die Authentizität eines Dokuments festgestellt werden kann. Die Verwendung der anderen beiden digitalen Signaturen wird gesetzlich geregelt. Es gibt auch neben dem deutschen Signaturgesetz ein europäisches Gesetz [EUSIG99], das auch die Verwendung der digitalen Signatur regelt. Im deutschen Signaturgesetz (SigG) und in der Verordnung zum Signaturgesetz (SigV) werden die elektronischen Signaturen selbst und insbesondere die Anforderungen an elektronische Signaturen und Zertifizierungsdienstanbieter (ZDA) definiert. Die Rahmenbedingungen jedoch, wann welche elektronische Signatur verwendet werden kann oder muss, werden nicht im Signaturgesetz definiert, sondern beruhen im wesentlichen auf dem Bürgerlichen Gesetzbuch (BGB) und anderen Gesetzen sowie Rechts- und Verwaltungsverordnungen. Weitere Informationen befinden sich auf der Seite der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (vormals Regulierungsbehörde für Telekommunikation und Post) [BEGTPE].
Die verschiedenen Signaturklassen mit der Beschreibung der Rechstwirkung sind in der Tabelle 2.1 dargestellt.

Das Ziel einer digitalen Signatur ist, einige wesentliche Eigenschaften der handschriftlichen Unterschrift in elektronischer Form zu realisieren. Solange die Verbindlichkeit der Unterschrift in die digitale Signatur realisierbar ist, beinhaltet die digitale Signatur das Schriftbild (Schriftführung und Druckstellen) in der Regel nicht. Das grundlegende Konzept ist hier das eines Signaturschemas. Jeder Teilnehmer eines Benutzerkreises, der in der Lage sein soll, Dokumente elektronisch zu signieren, verfügt über eine eigene Signaturfunktion und eine Verifikationsfunktion. Dabei ist die Signaturfunktion geheim, also nur seinem Besitzer bekannt.
Die Verifikationsfunktionen sind aber öffentlich zugänglich. Eine wichtige Eigenschaft

von Signaturschemata ist, dass es rechnerisch unmöglich sein muss aus der Verifikationsfunktion eines Teilnehmers auf dessen Signaturfunktion zu schließen. Ein Teilnehmer signiert eine Nachricht, indem er seine Signaturfunktion auf die Nachricht anwendet. Das Ergebnis ist die elektronische Signatur.

Funktionsweise der digitalen Signatur

Jedes asymmetrische Chiffrierverfahren kann Grundlage eines Signaturschemas sein. Die Signaturfunktion eines bestimmten Teilnehmers entspricht dabei der Verschlüsselung mit dem vertraulichen Schlüssel dieses Teilnehmers. Die Verifikationsfunktion entspricht der Anwendung des asymmetrischen Verfahrens mit dem öffentlichen Schlüssel des Teilnehmers.
Wenn der Teilnehmer A einen Text m signieren will, dann verschlüsselt er m mit seinem vertraulichen Schlüssel. Das Ergebnis dieser Verschlüsselung ist die elektronische Signatur von m. Andere Benutzer überprüfen die elektronische Signatur des Teilnehmers A, indem sie darauf den öffentlichen Schlüssel von A anwenden (und hierbei m erhalten).
Da asymmetrische Kryptosysteme relativ langsam sind, wäre das Digitale Signieren langer Dokumente auf die oben beschriebene Weise zeitraubend. Außerdem hat die oben beschriebene Methode den Nachteil, dass die Signatur ungefähr so groß ist wie der zu signierende Text; man möchte aber eine kurze Signatur fester Länge haben.
Beide Probleme werden durch Anwendung kryptographischer Hashfunktionen bereinigt. Zur Signaturerzeugung wird das Dokument m zunächst durch eine (öffentlich zugängliche) Hashfunktion h auf einen Wert h(m) fester Länge komprimiert. Danach wird dieser Hashwert h(m) der Signaturfunktion unterworfen. Das unterzeichnete Dokument besteht dann aus dem geordneten Paar (m, h(m)).
In den letzten Jahren wurden von vielen Staaten die gesetzlichen Grundlagen zur rechtlichen Anerkennung elektronischer Signaturen auf der Basis kryptographischer Algorithmen geschaffen. Gerade der Bereich der elektronischen Signaturerstellung sollte mit besonderer Sorgfalt betrachtet und die nötige Sensibilität erzeugt werden, schon allein um nicht in rechtliche Schwierigkeiten zu geraten. Eine wesentliche Voraussetzung für die gesetzliche Haftung eines Trustcenters bei Unterschriftenmissbrauch ist, dass tatsächlich nur der rechtmäßige Signator einen PIN/Passwort-geschützten Zugang zu den Signaturerstellungsdaten (wie den vertraulichen Schlüssel) hat. Der Signator ist gesetzlich verpflichtet, seine Signaturerstellungsdaten geheim zu halten.

Signatur	Beschreibung	Rechtswirkung
Qualifizierte Signatur mit Akkreditierung	Sicherheit der Zertifizierungsstelle wird von von der Bundesnetzagentur* überprüft; (= nachgewiesene technische Sicherheit); mindestens 30jährige Überprüfbarkeit der Signatur.	U. U. Voraussetzung für bestimmte Verwaltungsverfahren.
Qualifizierte Signatur	Sichere Signaturerstellungseinheit durch hardwarebasierte Lösungen (Chipkarte); von Zertifizierungsstellen gewährleistet, die ihren Betrieb bei der Bundesnetzagentur* angemeldet haben.	Erfüllt die Schriftformerfordernisse im Privat- und öffentlichen Recht; erhöhter Beweiswert.
Fortgeschrittene Signatur	Hard- und software -basierte Lösung (z. B. PGP, S/MIME). Signatur kann ausschließlich einem Inhaber zugeordnet werden. Das Zertifikat wird von einer offiziellen Stelle bestätigt.	Steht im Privatrecht der rechtsgeschäftlichen Schriftform gleich (§ 127 Abs. 3 BGB); erhöhter Beweiswert.
Einfache Signatur	Beliebige Unterschrift; ermöglicht keine Authentifizierung	Formlose Rechtsgeschäfte; formfreie Verfahrenshandlungen.

Tabelle 2.1: Signaturarten und deren Vergleich (Quelle:[BSK02])

*) – früher Regulierungsbehörde für Telekommunikation und Post heute Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (http://www.bundesnetzagentur.de/enid/2.html)

2.3.3 Authentifizierung

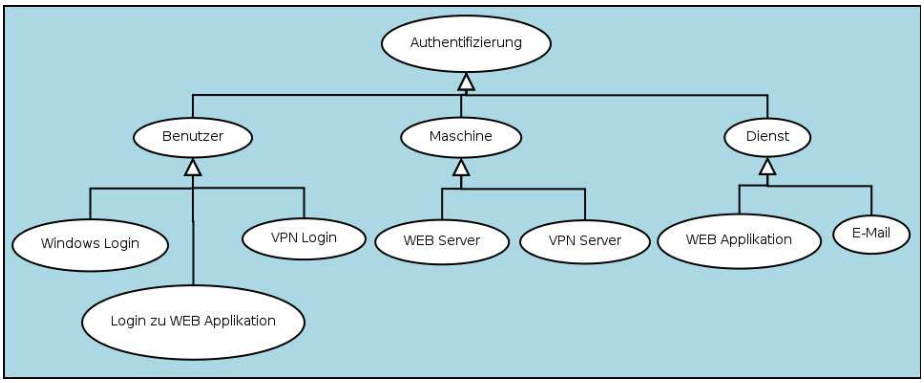

Abbildung 2.1: Anwendungsfälle für Authentifizierung

Der englische Ausdruck für Authentifizierung ist authentication. Dieser Begriff deckt aber sowohl Authentisierung als auch Authentifizierung. Deshalb wir für jedern dieser Begriffe eine Definition angegeben:

Die Authentifizierung bedeutet in der Regel die Überprüfung der Identität an Hand eines bestimmten Merkmals.

Als Authentisierung bezeichnet man den Nachweis einer Identität.

Nähere Informationen zu den aktuellen Authentifizierungslösungen befinen sich in [SM05].
Die Authentifizierung ist einer der grundlegenden Prozesse für jeden Benutzer in einer verteilten Umgebung. Die Authentifizierung ist ein Teil der Zugriffskontrollsysteme:

1. Identifikation des Benutzers anhand der Loginname, unter der Annahme, dass der Benutzer seinen Loginnamen nicht an weitere Person verraten hat.
2. Authentifizierung des Benutzers anhand eines Passwortes, unter der Annahme, dass der Benutzer sein Passwort nicht weitergegeben hat.
3. Autorisierung des Benutzers mit Hilfe einer Datenbasis (in der Regel ein Verzeichnisdienst)
4. Accounting mit Hilfe der Sicherheitsprotokoll zum Auditzwecken

Bei der Authentifizierung handelt es sich um Identitätsmanagement. Eine Registrationsstelle übernimmt in der Regel diese Aufgabe (vgl. Abschnitt 5.2.2). Dieser Prozess setzt natürlich eine vorherige Registration der Benutzer voraus.

Kapitel 3

Ist-Stand: vorhandene Anwendungsfälle

Es gibt bereits einige Anwendungsfälle in betrachtetem Unternehmen für:

1. Email-Verschlüsselung
2. Email-Signatur
3. Datei-Verschlüsselung
4. Datei-Signatur
5. Code-Signatur
6. Dokumentensignatur
7. Benutzerauthentifikation
8. VPN Authentifizierung
9. SSL Serverzertifikat für Webserver

Diese Anwendungsfälle behandeln mehrere grundlegende Anwendungsfälle (siehe Abschnitt 2.3) und sichern einige Unternehmensprozesse. Diese werden in den kommenden Abschnitten beschrieben.
Das wichtigste Objekt bezüglich Verschlüsselung und Signatur ist das Dokument. Man versteht unter einem Dokument eine Datei, die mit Hilfe einer Anwendung geöffnet werden kann und enthält menschenlesbare Informationen. Wenn so ein Objekt (Dokument) verschlüsselt werden sollte, könnte man im Prinzip die Verschlüsselung über Dateiverschlüsselung, da jedes Dokument eine Datei ist, behandeln. Dabei würden aber die Benutzbarkeit und Konformität enorm benachteiligt werden. Deshalb differenziert man zwischen Dokumenten und behandelt die Dokumente nicht auf Ebene des Filesystems, sondern auf Applikationsebene. Da aber nicht jede Applikation jede Dokumentenart öffnen kann, muss zwischen verschiedenen Dokumentumarten differenziert werden. Solange es für die Emailverschlüsselung und Emailsignatur mehrere Lösungen gibt, werden Officedokumente (Word, Excel etc.) nur ungenügend unterstützt. Da die meisten (größeren) mittelständischen Unternehmen Microsoft Produkte einsetzen, bieten diese die Grundlage für die Untersuchung dieser Diplomarbeit.

Für die Fälle 1 - 4 werden die Verschlüsselungsmaterialien durch die bei dem Unternehmen eingesetzte PGP Software generiert. Für die anderen Fälle, da diese mittels PGP Material nicht behandelt werden können, wird das Cryptomaterial bei einem externen TrustCenter (kommerzieller Betreiber einer akkreditieren PKI) zugekauft. Der wichtigste Anwendungsfall ist die Emailverschlüsselung, weshalb dieser in dem nächsten Abschnitt näher beschrieben wird.

3.1 Emailverschlüsselung

Durch die Emailverschlüsselung wird eines der wichtigsten Kommunikationsmittel gesichert. In einem Unternehmen ist die Emailverschlüsselung neben dem Telefon das wichtigste Kommunikationsmedium. Weil sich ein Telefongespräch nur mit hohem Aufwand verschlüsseln lässt, da es spezielle Hardware (Telefon) benötigt, lässt sich die Emailverschlüsselung mit relativ wenig Aufwand betreiben. Der Aufwand steigt aber mit zunehmender Anzahl der Beteiligten. In diesem Abschnitt wird die Emailverschlüsselung und deren Realisierung in einem mittelständischen Unternehmen vorgestellt.
Es gibt heute verschiedene Möglichkeiten und Standards zur Umsetzung der Emailverschlüsselung (siehe Bemerkung 3.1.1). Aus den mehreren Standards haben bis heute eigentlich nur zwei überlebt.

3.1.1 Bemerkung zu den Verschlüsselungsstandards

Für Verschlüsselung gibt es zwei miteinander inkompatible und konkurrierende Standards:
PGP und S/MIME.

S/MIME ist eine Erweiterung der MIME Spezifikation um die Funktionen Verschlüsselung und Signatur. S/MIME arbeitet mit X.509 Zertifikaten als Cryptomaterial, die von einer hierarchisch organisierte Zertifikatsstelle (CA – **C**ertificate **A**uthority) ausgestellt werden. Für die Richtigkeit des Zertifikats haftet die ausstellende Stelle. Die Zertifikate beinhalten den Schlüssel, mit dem die Verschlüsselung bzw. Signatur vollzogen wird. In dem Abschnitt 5.2.2 wird dies ausführlicher behandelt. S/MIME wurde in mehreren standardisierten RFCs (S/MIME wird im Wesentlichen in der RFCs 3369 , 3370, 2633 und 2632 beschrieben. Sie finden eine detaillierte Liste unter: http://www.imc.org/ietf-smime/index.html) (**R**equest **F**or **C**omments), die von IETF (**I**nternet **E**ngineering **T**ask **F**orce – Vereinigung von Entwicklern zur Entwicklung des Internets) und IESG (**I**nternet **E**ngineering **S**teering **G**roup – zuständig für das Management der IETF Arbeitsgruppen) definiert und veröffentlicht wurden.

PGP steht für die Abkürzung **P**rietty **G**ood **P**rivacy. Es muss aber erwähnt werden, dass PGP sowohl für ein Emailverschlüsselungsalgorithmus, für eine Firma (PGP Deutschland AG http://www.pgp.de bzw. PGP Corp. http://www.pgp.com), für Schlüsselmaterial (PGP Schlüssel) und als auch für mehrere Standards openPGP [RFC2440] bzw. PGP steht. (Sie finden ein Überblick im Anhang B.)
PGP wurde von Phil Zimmermann entwickelt und erschien zum ersten Mal in

Jahre 1991 als frei erhältliche Software. PGP verfolgt den Ansatz des gegenseitigen Vertrauens. Aus diesem Grund benötigt PGP keine Infratsruktur. Zur besseren Schlüsselverteilung wurde aber der Ansatz des Keyservers entwickelt. Ein Keyserver ist eine zentrale Stelle, die zur Speicherung öffentlicher Schlüsseln dient.
Obwohl PGP auf den Ansatz des gegenseitigen Vertrauens basiert, kann damit auch eine hierarchische Struktur aufgebaut werden.
Bei der Benennung PGP handelt es sich um Schlüssel, Protokoll und Produkt.
Das Produkt wird von PGP Corporation (http://www.pgp.com/de/products/index.html) und direkt von P. Zimmermann (http://www.philzimmermann.com/EN/findpgp/index.html) vertrieben. Das Protokoll hat verschiedene Versionen, die teilweise inkompatibel zu einander sind.
Folgende Ausdrucksweise hat sich inzwischen etabliert:

OpenPGP für den Standard OpenPGP

PGP für eine Datei

PGP Schlüssel für OpenPGP öffentliches Cryptomaterial

PGP Schlüsselpaar für OpenPGP Cryptomaterial (privater und öffentlicher Teil)

PGP Schlüsselring Containerdatei für OpenPGP Schlüssel

PGP öffentlicher Schlüsselring Containerdatei für OpenPGP Schlüssel (.pkr Datei)

PGP privater Schlüsselring Containerdatei für OpenPGP Schlüsselpaare (.skr Datei)

PGP arbeitet ebenfalls mit Verschlüsselungsmaterial. Bei PGP wird das Verschlüsselungsmaterial Schlüssel bzw. Schlüsselpaar genannt. Das Schlüsselpaar besteht aus einem privaten und aus einem öffentlichen Schlüssel. Der private Schlüssel wird zum Entschlüsseln verwendet und muss sicher aufbewahrt werden. Mit dem öffentlichen Schlüssel wird verschlüsselt. Der öffentliche Schlüssel soll auf sicherem Kanal dem Kommunikationspartner zur Verfügung gestellt werden.

Einen Lösungsansatz bieten die so genannten Keyserver. Ein Keyserver speichert und stellt die öffentlichen Schlüssel der Kommunikationspartner den Kommunikationspartnern zur Verfügung. Je nach Konfiguration ist es möglich, dass der Kommunikationspartner seinen eigenen öffentlichen Schlüssel auf den Keyserver lädt. Das ist meistens nur bei den öffentlichen Keyservern erlaubt.
Um einem Schlüssel zu vertrauen, muss man ihn signieren. An dem Schlüssel angehängte Signatur, wird auch Zertifikat genannt.
Die Einheit, die zur Speicherung der Schlüssel dient, wird Schlüsselring genannt. Dabei unterscheidet man zwischen privaten und öffentlichen Schlüsselringen. Der öffentliche Schlüsselring kann nur öffentlichen Schlüssel aufnehmen. Falls man ein PGP Schlüsselpaar darin zu speichern versucht, wird nur der öffentlicher Teil des Schlüsselpaares gespeichert. Manchmal wird auch die Bezeichnung Store verwendet. Unter dieser Bezeichnung versteht man sowohl die Schlüsselringe an sich, als auch die Schlüsselringdateien. Diese Bezeichnung stammt von einigen Softwareherstellern und ist zum Schlüsselring synonym.

PEM steht für Privacy Enhanced Message. Dieser dritter bisher nicht erwähnter Standard liget seit 1993 als RFC (RFC 1421) vor. PEM wird heute nur in wenigen Bereichen eingesetzt. Das PEM Nachrichtenformat basiert auf 7-Bit Text-Nachrichten, während die anderen Formate auch Binärdaten als Anhang zulassen. Zu erwähnen sind im Zusammenhang mit PEM insbesondere die Bemühungen, PEM in Deutschland über das MailTrusT Projekt der TeleTrusT durchzusetzen. Das Projekt hat sich aber neuerdings in Richtung S/MIME geöffnet. PEM hat sich auch international kaum durchgesetzt und wird daher hier nicht näher betrachtet.

MTT ist die Abkürzung für den inzwischen nicht mehr weiterentwickelter Standard MailTrustT (MTT) von TeleTrusT Deutschland (http://www.teletrust.de/). Dabei handelt es sich sicherlich um ein recht gut spezifiziertes und durchdachtes System. Genauso wie S/MIME arbeitet MTT auf der Basis von X.509-Zertifikaten. Die Spezifikationen sind noch frei verfügbar. Dieser Standard wird nicht von vielen Unternehmen eingesetzt und wird auch nicht weiterentwickelt.

3.1.2 Bemerkung zu den Cryptomaterialien

Es gibt verschiedene Arten von Cryptomaterialien, wobei jedes Cryptomaterial einen öffentlichen Teil und einen privaten Teil hat. Mit dem öffentlichen wird verschlüsselt mit dem privaten entschlüsselt. Bei OpenPGP wird das Cryptomaterial Schlüssel genannt. Bei OpenPGP werden die zwei Teile zusammen Schlüsselring genannt.
Es muss zwischen verschiedenen Zertifikaten differenziert werden:

- X.509 Zertifikat
- Simple Public Key Infrastructure (SPKI) Zertifikat
- Attribut Zertifikat

Bei diesen Zertifikaten wird keine andere Bezeichnung für den privaten bzw. für den öffentlichen Teil verwendet. Bei dem öffentlichen Teil kann man das Wort öffentlich hinzufügen, z. B. X.509 öffentliches Zertifikat.
Es werden auch bei OpenPGP Zertifikate verwendet. Diese werden aber nur im Sinne einer Signatur von OpenPGP Schlüsseln verwendet.

3.1.3 Umfeld der Emailverschlüsselung

Das Umfeld der Emailverschlüsselung lässt sich in drei Bereiche teilen:

- Die Beteiligten
- Die Verschlüsselungssoftware
- Funktionsweise der Software

Im folgenden werden diese Bereiche, die Hintergrundinformationen für den Anwendungsfall Emailverschlüsselung liefern und das Umfeld, in dem die Emailverschlüsselung abläuft, beschrieben.

Die Beteiligten

An der Emailverschlüsselung nehmen die Mitarbeiter teil, die für sich einen Emailverschlüsselungsschlüssel bestellt haben. Bei einem mittelständischen Unternehmen kann man ungefähr mit 2000 bis 10000 Benutzer rechnen. Die Emailverschlüsselung steht jedem Mitarbeiter offen. Jeder Mitarbeiter, der an der Emailverschlüsselung teilnehmen möchte, muss sich nur einen Schlüssel bestellen.
Die Emailverschlüsselung wird vor allem für die interne Kommunikation verwendet. Die Kommunikation läuft in vielen Ländern zwischen hundert Standorten ab. Da die Kommunikation teilweise über gemietete Netze und zum Teil in Ländern mit großem wirtschaftlichen Interesse an vertraulichen ausländischen Industrieinformationen abläuft, musste bei dem betrachteten Unternehmen vor einigen Jahren eine Lösung zur Emailverschlüsselung gefunden werden.

Damals war der Standard S/MIME (S/Mime steht für **S**ecure **M**ultipurose **I**nternet **M**ail **E**xtension), was die Unterstützung von den Softwareprodukten angeht, noch nicht ausgereift. Dieser Emailverschlüsselungsstandard war damals nicht sehr verbreitet, obwohl S/MIME zu jener Zeit auch schon spezifiziert war. Die geringe Verbreitung von S/MIME lässt sich auf hohen Preise für X.509 Zertifikate für die Emailverschlüsselung zurückführen.
Damals wurde PGP entwickelt und befand sich auf dem Weg von der Nischenlösung zu einer anerkannten Lösung für die Emailverschlüsselung. Der Standard PGP hatte schon damals einen großen Kreis von Sympathisanten und Anwendern. Es existierte damals eine funktionierende Lösung für Email- und Dateiverschlüsselung bzw. Signatur auf PGP basis.
Weil das Unternehmen aber kundenorientiert arbeitet und viele Kunden PGP basierte Emailverschlüsselung eingesetzt haben, wurde für den Einsatz von PGP entschieden, und eine bis heute einsatzfähige und funktionierende Lösung erarbeitet. Die Entwicklung und Verbreitung beider Standards konnte nicht vorhergesehen werden. Es gibt aber immer noch viele Geschäftspartner, die mit PGP Verschlüsselung kommunizieren.

Die Kommunikationszenarien

Es gibt mehrere Kommunikationsszenarien, wobei man zwischen unternehmensinterner Verschlüsselung (geschlossene Gruppe) und Verschlüsselung an Geschäftspartner (offene Gruppe) differenzieren muss. Diese Differenzierung ist erforderlich, weil die Konfigurationen bei der geschlossenen Gruppe auf der Senderseite und auf der Empfängerseite gleich sind. Das wird durch die Standardclients gewährleistet. Man muss sich dagegen bei einer offenen Gruppe auf die Interoperabilität verschiedener Software verlassen. Die Interoperabilität wird durch die Einhaltung der Standards erreicht.
Eine weitere Unterscheidung kann nach der Anzahl der Empfänger gemacht werden. Da stellt sich die Frage, ob es einen Unterschied macht, wieviele Personen in der Empfängerliste stehen. Wenn man aber auch die Möglichkeit in Betracht zieht, dass ein Empfänger aus der Empfängerliste keinen (öffentlichen) Schlüssel zur Emailverschlüsselung hat, und dass dieser Fall auch behandelt werden muss, dann macht diese Betrachtung auch einen Sinn.
Demnach sind folgende Szenarien durchaus denkbar und realistisch.

Der Mitarbeiter sendet eine verschlüsselte Email an

- einen Mitarbeiter (siehe Abbildung 3.1)
- mehrere Mitarbeiter
- einen Geschäftspartner
- mehrere Geschäftspartner
- einen Geschäftspartner und an einen Mitarbeiter
- einen Geschäftspartner und an mehrere Mitarbeiter
- mehrere Geschäftspartner und an einen Mitarbeiter
- mehrere Geschäftspartner und an mehrere Mitarbeiter (siehe Abbildung 3.2)

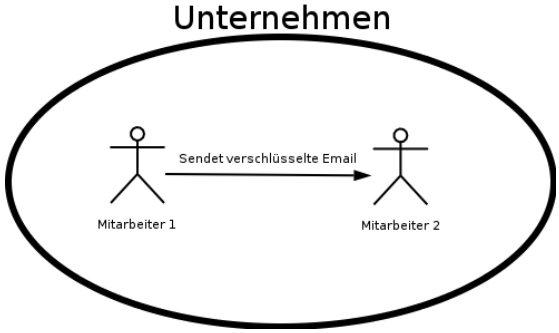

Abbildung 3.1: Einfachster Fall für die Emailverschlüsselung

Bei diesen Szenarien wurde nicht beachtet, ob alle Empfänger einen Schlüssel haben. Die Emailverschlüsselungssoftware muss diesen Fall abfangen und eine Benutzerinteraktion von dem Absender verlangen. Man könnte es zwar umgehen und als Firmenpolicy ausgeben, wenn ein Absender keinen Emailverschlüsselungsschlüssel hat, soll er die Information unverschlüsselt erhalten. Dies bedeutet aber eine Verletzung des Gedanken und Zwecks der Emailverschlüsselung.

Die Verschlüsselungssoftware

Warum PGP als Verschlüsselungsstandard zum Einsatz kam, wurde bereits beschrieben. Nach dem diese Entscheidung fiel, musste eine geeignete Software gefunden werden.

Da das Unternehmen Microsoft Produkte einsetzt, wird Software von Drittherstellern zu der Verwendung von der PGP-Verschlüsselung benötigt. Bei der Produktwahl wurden verschiedene Produkte miteinander verglichen. Wichtig war bei der Wahl, dass ein europäisches Produkt zum Einsatz kommen soll. Zu jener Zeit konnte nicht mit Sicherheit festgestellt werden, ob ein amerikanisches Produkt eventuell eine Hintertür hat oder nicht. Deshalb fiel die Entscheidung auf das Produkt *CryptoEx Outlook* von der Firma Glück & Kanja AG. Diese Software hat andere Geschwisterprodukte mit denen Dateiverschlüsselung und -Signatur bzw. Verzeichnisverschlüsselung möglich ist.

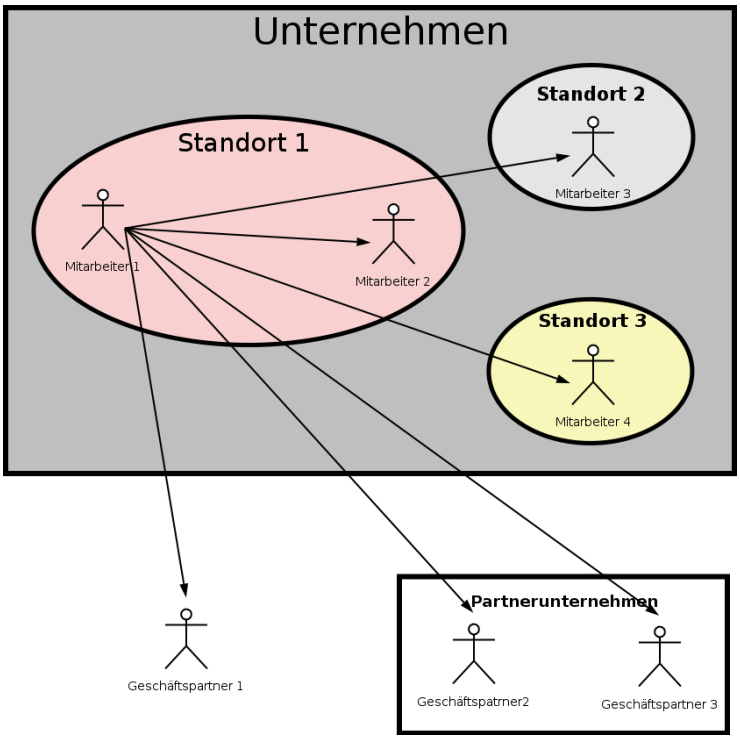

Abbildung 3.2: Komplexer Fall für die Emailverschlüsselung

CryptoEx Outlook bietet zwar Unterstützung für S/MIME, da sich aber die Benutzung und zentrale Verwaltung von S/MIME Schlüsseln (tatsächlich sind es X.509 Zertifikate) recht schwierig erwies, wurde auf S/MIME vorerst verzichtet.
CryptoEx Outlook müsste installiert werden, da das Unternehmen aber sog. Standardclients einsetzt, auf denen eine Basisinstallation von Software installiert wird, muss der Anwender nur ein PGP Schlüsselpaar bestellen.

Der Anwendungsfall Emailverschlüsselung besteht aus folgenden Teilprozessen:

1. Bestellung
2. Authentifizierung und Autorisierung
3. Generierung
4. Verteilung und Veröffentlichung
5. Import und Verwendung

Wenn man diese Prozesse als Ablauf betrachtet, wird die Ähnlichkeit mit dem Schlüssellebenszyklus (vgl. Abschnitt 3.1.15) deutlich. Es ist demnach möglich anhand des Anwendungsfalls für Emailverschlüsselung den Schlüssellebenszyklus im Detail anzusehen und nachzuvollziehen.
Der Anwendungsfall Emailverschlüsselung ist genau genommen ein Zyklus. Er beginnt mit der Bestellung und endet mit dem Widerruf des Schlüsselpaares. Eine Über-

sicht verschafft die Abbildung 3.3. Die einzelnen Schritte werden in den folgenden Abschnitten beschrieben.

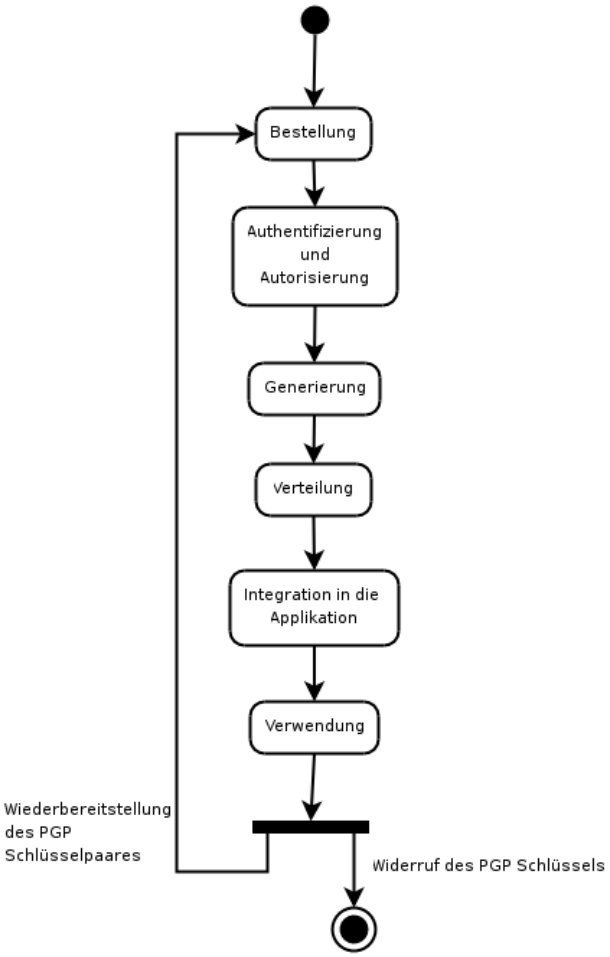

Abbildung 3.3: PGP Schlüssellebenszyklus

Wenn ein Mitarbeiter eine Email verschlüsseln möchte, muss er im Prinzip zweierlei Unterlagen haben: die Verschlüsselungssoftware und ein PGP Schlüsselpaar. Jeder Mitarbeiter arbeitet mit einem Standardclient, worauf ein vorinstalliertes Windows XP mit unternehmensspezifischen Einstellungen und mit vorinstallierter Softwarebasis läuft. Diese vorinstallierte Softwarebasis beinhaltet auch die Software für Emailverschlüsselung. Das Unternehmen verwendet Microsoft Outlook, wobei die Outlook-eigene Verschlüsselung deaktiviert wird.
Ein Standardclient ist bei einem Unternehmen mit mehrere Tausend Mitarbeiter zwingend erforderlich. Der Standardclient bedeutet nicht nur eine Standardinstallation, sondern auch die regelmäßige und zentral gesteuerte Verteilung der Softwareaktualisierungen bzw. den Austausch von Softwareprodukten.
Früher konnten die Mitarbeiter mit Hilfe der Email-Verschlüsselungssoftware PGP

Schlüssel selber generieren, was aber auf eine zentrale Verwaltung der Verschlüsselungsschlüssel aus Gründen, die im Abschnitt 3.1.7 genannt wird, umgestellt wurde. Die dazu benötigten Einstellungen in der Verschlüsselungssoftware wurden per SMS (System Management Server- Werkzeug zur automatisierten Softwareverteilung von Microsoft
http://www.microsoft.com/smserver/) an allen Standardclients vorgenommen. Diese geänderten Einstellungen erlauben den Mitarbeitern eine Schlüsselgenerierung nicht.

Die vorkonfigurierte Verschlüsselungssoftware hat bereits:

einen dateibasierten Standardstore, der aus einem öffentlichen und privaten Schlüsselring besteht. Dieser Store beinhaltet den öffentlichen Schlüssel der Sicherheitsabteilung.

einen dateibasierten Store der Geschäftspartner, der nur aus einem öffentlichen Schlüsselring besteht. Dieser Store hält die Schlüssel der Geschäftspartner und wird über die zentrale Softwareverteilung verteilt und bei Änderung ersetzt.

einen HTTP Store, der zur Abfrage des unternehmenseigenen Keyservers, der auch über das Internet erreichbar ist, dient.

Die Verschlüsselungssoftware ist so konfiguriert, dass jeder Benutzer, der berechtigt ist sich an dem Rechner anzumelden und ein Profil an diesem Rechner hat, eigenen Standardstore hat und auf die von anderen Benutzern keinen Zugriff hat. Alle diese Einstellungen dienen zur erleichterten Verwendung der Emailverschlüsselung. Wenn also ein Mitarbeiter die Emailverschlüsselung verwenden möchte, dann muss er nur zuerst ein PGP Schlüsselpaar bestellen.

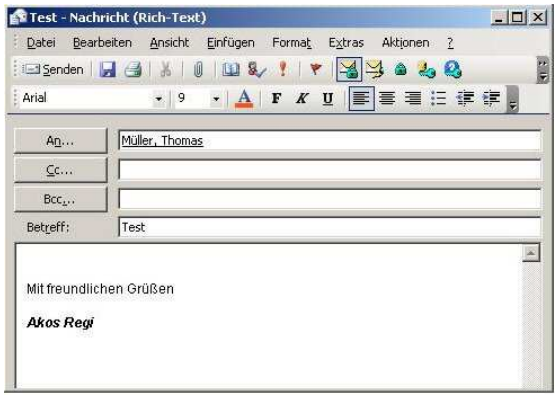

Abbildung 3.4: Outlook mit der Verschlüsselungssoftware

Funktionsweise der Software

Falls der Mitarbeiter also kein PGP Schlüsselpaar hat und versucht trotzdem eine verschlüsselte Email zu schreiben, wobei er auf eine spezielle aber unverwechselbare Ikone in der Ikonenleiste klickt, erhält er eine Meldung, da die Verschlüsselungssoftware *CryptoEx Outlook* so eingestellt ist, dass die gesendete Email mit zwei Schlüsseln, sowohl mit dem Empfängerschlüssel als auch mit dem Absenderschlüssel, verschlüsselt

wird. In dem Fall sucht die Software ein PGP Schlüsselpaar, findet aber keines. (Vergleiche mit dem Schritt eins in der Abbildung 3.5.) Diese Einstellung ist eine sinnvolle Einstellung aber keine notwendige. Die Verschlüsselungssoftware sucht nach PGP Schlüsseln auf dem unternehmenseigenen Keyserver anhand der Emailadresse des Empfängers.
Die Abbildung 3.5 zeigt den ganzen Vorgang. Es konnten zwar nicht alle Einzelheiten dargestellt werden, diese werden aber in den folgenden Abschnitten behandelt.

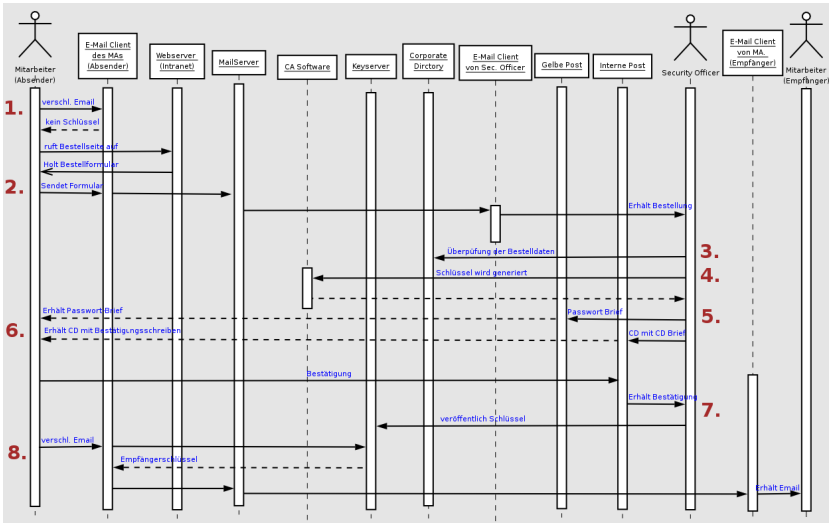

Abbildung 3.5: Anwendungsfall Emailverschlüsselung

3.1.4 Bestellung von PGP Schlüsselpaaren

Für die Emailverschlüsselung benötigt man Schlüsselmaterial. Der Anwender muss nur ein PGP Schlüsselpaar bestellen, damit er in der Lage ist, Emails zu verschlüsseln. Dazu ruft der Mitarbeiter die Intranetseite der Sicherheitsabteilung auf, um von dort das Bestellformular (siehe Abschnitt 3.1.5) zu holen.
Der Bestellvorgang wird in der Abbildung 3.6 dargestellt.

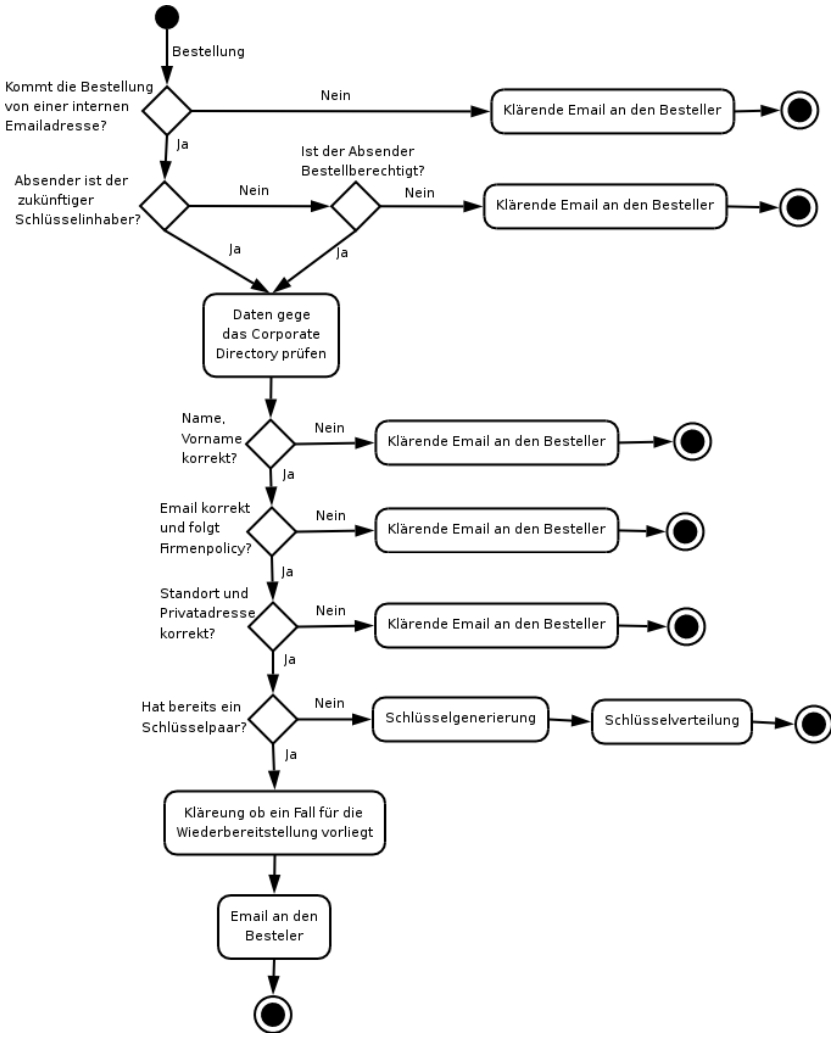

Abbildung 3.6: Ablauf des Bestellvorganges

In der Regel bestellt jeder Mitarbeiter für sich selber den Verschlüsselungsschlüssel. Es gibt aber zwei Ausnahmen:

Eine Sekretärin darf für ihren direkten Vorgesetzten bestellen. Dies muss aber auch aus den Einträgen im Corporate Directory hervorgehen.

Eine LRA (Local Registration Authority - lokale Registrationsstelle), die im Unternehmen Aufgaben der lokalen Sicherheitsadministration an einem Standort übernimmt, kann für seine Kollegen Schlüssel bestellen. Pro Standort gibt es ein LRA. Die LRA wird durch die Sicherheitsabteilung nach Prüfung des- oder derjenigen ernannt. Dieser ist eine von den zentralen Sicherheitsadministratoren bekannte und für vertrauenswürdig gehaltene Person. Die LRA erhält nach der Ernennung eine eigene Emailadresse und einen Verschlüsselungsschlüssel für diese Emailadresse. Die LRA kennt sich mit den organisatorischen und technischen Aspekten der Emailverschlüsselung aus.

Besteller	Empfänger			
	anderer Mitarbeiter	andere Sekretärin	anderer Vorgesetzter	andere LRA
Mitarbeiter	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt
Sekretärin	Nicht berechtigt	Nicht berechtigt	berechtigt	Nicht berechtigt
Vorgesetzter	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt
LRA	berechtigt	berechtigt	berechtigt	Nicht berechtigt
Sicherheitsabteilung	berechtigt	berechtigt	berechtigt	berechtigt

Tabelle 3.1: Berechtigungsmatrix für PGP Schlüsselbestellungen

3.1.5 Das Bestellformular für PGP Schlüsselpaare

Das Bestellformular für PGP Schlüsselpaare ist nur über das Intranet erhältlich und beinhaltet folgende Felder, die mit den Daten des zukünftigen Schlüsselinhabers gefüllt werden müssen.

- Name
- Vorname
- Abteilung
- Standort
- Privatadresse - Postleitzahl
- Privatadresse - Ort
- Privatadresse - Straße und Hausnummer

Das Bestellformular ist eine Exceltabelle und kein HTML Formular. Es wurde für die Exceltabelle entschieden, da man mit Hilfe der Exceltabelle für mehrere Mitarbeiter PGP Schlüssel bestellen kann, ohne die gleichen Daten mehrmals eintippen zu müssen. Diese von den Mitarbeitern freiwillig angegebenen Daten sind erforderlich, weil die CD mit dem PGP Schlüsselpaar und das zugehörige Initialpasswort auf getrennten Wegen zum Schlüsselinhaber kommen sollen. Das ausgefüllte Formular (siehe Tabelle

Name	Vorname	Abteilung	Privatadresse			
			PLZ	Ort	Straße	Hausnummer

Tabelle 3.2: Bestellformular für PGP Schlüsselpaar

3.2 wird an die im Formular genannte Emailadresse der Sicherheitsabteilung gesendet werden. Schritt zwei in der Abbildung 3.5.

3.1.6 Authentifizierung und Autorisierung der Bestellung

Die Sicherheitsabteilung erhält die Email mit dem ausgefüllten Formular und überprüft die Angaben. (Schritt drei in der Abbildung 3.5.) Die Absenderemailadresse muss eine unternehmenseigene Emailadresse sein. Der Absender muss im Corporate Directory einen Eintrag haben. Die Einträge in das Corporate Directory kommen aus dem Active Directory. Das Active Directory wird wiederum mit Daten aus dem Personalverfahren versorgt. Die Daten des Personalverfahrens werden zum größten Teil während der Einstellung von Mitarbeitern erfasst.
In der Regel ist der Absender auch der Besteller und somit auch der zukünftiger Schlüsselinhaber. Die Daten in dem Formular werden gegen das Corporate Directory geprüft. Geprüft werden, ob die angegebenen Namen und Abteilungsbezeichnung richtig sind. Falls nicht, wird der Antrag nicht angenommen und an den Absender zurückgeschickt. Bei externen Mitarbeitern werden die Daten gegen das globale Adressbuch geprüft. Falls die Daten korrekt sind, werden diese mit Datumsangabe und Kürzel des Administrators in die interne Datenbasis übernommen. In der Datenbasis werden die Daten mit Datumsangaben zu dem Antrag, zu der Schlüsselgenerierung und zu der Veröffentlichung des öffentlichen Schlüssels auf dem Keyserver. Ein Kürzel des Mitarbeiters der Sicherheitsabteilung sowie die Passwörter der Schlüssel werden ebenfalls in der

Datenbasis geführt. Die Datenbasis wird regelmäßig gesichert.
Die Privatadresse der Mitarbeiter wird nach 3 Monaten aus der Datenbasis gelöscht.
Bei dem Antrag wird ebenfalls überprüft, ob der Mitarbeiter bereits einen aktiven Schlüssel besitzt. Es kann nämlich vorkommen, dass der Mitarbeiter ein neues Schlüsselpaar bestellt, obwohl es nicht erforderlich wäre. In so einem Fall wird nachgefragt, ob das Passwort bzw. CD mit Schlüsselmaterial noch vorliegen. Dies wäre aber eine Wiederbereitstellung, die in dem Abschnitt 3.1.12 behandelt wird.

Bemerkung 3.1.1 *Es sind Daten aller Mitarbeiter in dem Personalverfahren gespeichert. Aus dem Personalverfahren wird auch das Active Directory mit gefilterten Daten versorgt. Gefiltert heißt hier, das nicht alle Daten eines Mitarbeiters das Personalverfahren verlassen, sondern nur eine kleine Teilmenge. Das globale Adressbuch, das über Microsoft Outlook erreichbar ist, wird Daten aller Mitarbeiter aus dem Acitve Directory versehen. Das Corporate Directory wird mit den Daten der Angestellten aus dem Active Directory versorgt. Der Datenfluss wird anhand in der Abbildung 3.7 visualisiert.*

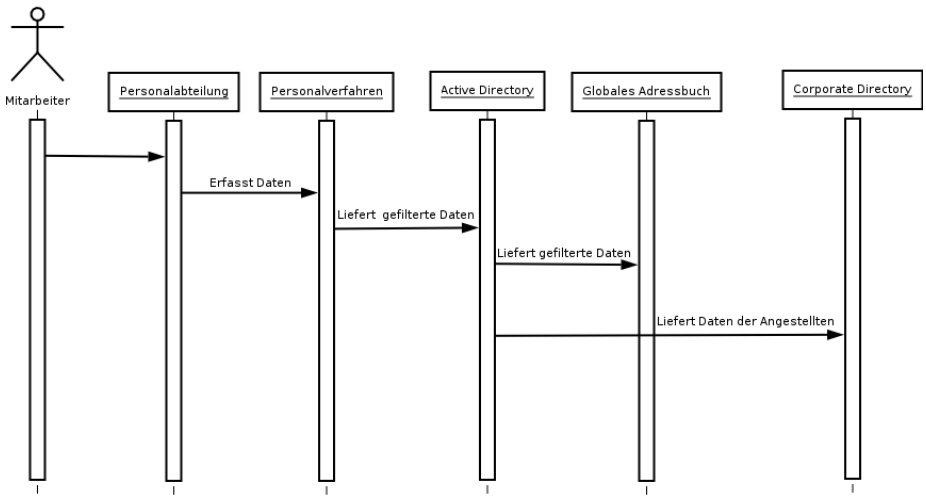

Abbildung 3.7: Datenfluss der Mitarbeiterdaten

3.1.7 Generierung des PGP Schlüsselpaares

Die Schlüsselgenerierung erfolgt bei den meisten mittelständischen Unternehmen zentral. Es hat sich an den Anrufen bei der Hotline für Unterstützung für die Emailverschlüsselung bemerkbar gemacht, dass die Mitarbeiter nicht in der Lage waren, den früher selber generierten Schlüssel zu sichern und sicher aufzubewahren. Aus dieser Erfahrung heraus, entstand der Prozess für die zentralisierte Verwaltung von Verschlüsselungsmaterial. Ein weiterer Grund ist, dass Unternehmen zu der Aushändigung von verschlüsselten Unterlagen von der Staatsanwaltschaft mit dazu erforderlicher Beschluß aufgefordert werden können. Dies erfordert eine zentrale Sicherung der Verschlüsselungsmaterialien. Das zentral verwaltete Crypromaterial wird natürlich auch regelmäßig gesichert und auf sicherem offline Ort aufbewahrt.

Die Generierung des Verschlüsselungsmaterials erfolgt mit Hilfe von *CryptoEx Outlook*. Der Hersteller von *CryptoEx Outlook* , Glück & Kanja AG wurde inzwischen von PGP Deutschland AG aufgekauft [H57134]. (Die Generierung entspricht dem Schritt vier in der Abbildung 3.5.) Die Daten für das Schlüsselpaar werden aus der internen

Schlüsseleigenschaften	
Anzeigename	[Name],[Vorname]
Emailadresse	[Vorname].[Nachname]@[UD*].[TLD**]
Schlüsselalgoritmus	RSA Algorithmus
Schlüssellänge	1024 bit
Format	.pgp binäre Datei mit privatem Schlüssel

Tabelle 3.3: Eigenschaften von PGP Schlüsselpaar

*) – Unternehmensdomain **) –Top Level Domain

Datenbasis der Sicherheitsabteilung übernommen. Die Generierung erfolgte zuerst manuell, später wurde ein Skript zur Erleichterung erstellt. Das Skript benötigt eine CSV (Comma Separated Value) Datei, die das Initialpasswort (kommt aus der internen Datenbasis) den Vornamen, den Nachnamen und die Emailadresse der Mitarbeiter beinhaltet. Diese Datei wird dem Skript übergeben. Da die Emailadresse nicht in dem Bestellformular eingetragen wird, muss der Sicherheitsadministrator die Emailadresse des Schlüsselinhabers aus dem Corporate Directory aussuchen. Dabei muss er bei Namensgleichheit darauf achten, dass die richtige Emailadresse in die CSV Datei eingetragen wird. Es gibt zwar eine Firmenpolicy, wie die Emailadressen anhand des Mitarbeiternames gebildet werden sollen. Diese Policy wird aber nicht immer befolgt. Das Skript prüft noch mal die Emailadresse, ob der Domainenteil und Topleveldomainteil der Emailadresse korrekt ist, da nur unternehmenseigene Emailadressen akzeptiert werden. Die generierten PGP Schlüsselpaare verwenden den RSA Algorithmus mit 1024 Bit Schlüssellänge. Das Schlüsselpaar der Sicherheitsabteilung und der LRAs hat ein Schlüssellänge von 2048 Bit. Das Schlüsselpaar folgt laut Softwarehersteller dem OpenPGP Standard. Die Tabelle 3.3 zeigt die Schlüsseleigenschaften.
Da bei den größeren mittelständischen Unternehmen die organisatorischen Prozesse nicht immer so greifen, wie es erwünscht wäre, wurde früher die Lebensdauer der Schlüsselpaare auf zwei Jahre begrenzt. Dies führte jedoch zu dem Problem, dass manche Schlüssel am Wochenende oder an den Feiertagen ungültig wurden. Der Sicherheitsadministrator musste jede Woche alle Schlüssel auf Ablaufdatum prüfen. Da

dies bei ca. 2000 Schlüsseln einen nicht geringen Aufwand verursacht hat, wurde diese zeitliche Begrenzung der Schlüssel abgeschafft.
Nachdem die Schlüssel per Skript generiert worden sind, fordert das Skript den Administrator auf, der Reihe nach für jeden Schlüssel eine CD Rohling in den CD Brenner einzulegen, da die generierten Schlüssel auf CD ausgeliefert werden. Der Eintrag in der internen Datenbasis wird mit dem Datum der Generierung ergänzt.

3.1.8 Verteilung von generierten PGP Schlüsselpaaren

Die CD, auf der die PGP Schlüsselpaare gebrannt wurden, und das Bestätigungsschreiben werden per firmeninterner Post an den Schlüsselinhaber (vgl. mit Abschnitt Bestellung), an die in dem Antragsformular angegebene und überprüfte Standortadresse geschickt. Das ist der Schritt fünf in der Abbildung 3.5.
Falls es sich bei der Bestellung um eine eilige Bestellung von einer LRA (vgl. mit Abschnitt Bestellung) handelt, dann werden sowohl das Schlüsselpaar als auch das Initialpasswort an die LRA in getrennten aber jeweils verschlüsselten Emails zugeschickt. Die LRA muss diese beiden Materialien auf sicherem (persönlich) Weg dem Schlüsselinhaber überreichen. Aus dem Grund ist es besonders wichtig, dass die LRA eine Vertrauensperson ist, der sich mit den technischen und organisatorischen Aspekten der Emailverschlüsselung gut auskennt.
Das Bestätigungsschreiben muss von dem Anwender nach erfolgreichem Schlüsselimport unterschrieben an die Sicherheitsabteilung zurückgeschickt werden, damit der Schlüssel aktiviert (siehe Abschnitt Aktivierung) wird.
Der Schlüsselinhaber findet Hinweise auf eine Importanleitung im Intranet auf dem Bestätigungsschreiben.
Das Passwort wird gedruckt und an die in dem Antragsformular angegebene Privatadresse per deutsche Post geschickt. Die beiden Informationen müssen auf getrennten Wegen zum Schlüsselinhaber gelangen, damit der Abfang beider Informationen möglichst erschwert wird[LP03].
Nachdem diese Briefe (oder ggf. Emails) auf den Weg gebracht wurden, wird das aktuelle Tagesdatum des Versands in die interne Datenbasis eingetragen.

3.1.9 Importvorgang eines PGP Schlüsselpaares

Der Mitarbeiter muss nur das eigene PGP Schlüsselpaar importieren, da alles andere bereits eingestellt ist. Wenn der Schlüsselinhaber alle Unterlagen zur Emailverschlüsselung erhalten hat, kann er anhand der Importanleitung, die im Intranet verfügbar ist, das Schlüsselpaar importieren. Der Schritt 6 in der Abbildung 3.5 entspricht sowohl dem Importvorgang als auch dem Versenden des Bestätigungsschreibens (siehe Abschnitt 3.1.10).
Als erstes muss dazu die Verschlüsselungssoftware *Start* $\Rightarrow$ *Programme* $\Rightarrow$ *CryptoEx* $\Rightarrow$ *Certificate Manager* gestartet werden. Der *CryptoEx Certificate Manager* hat per Voreinstellung drei Stores:

Standard Store dient zur Verwaltung des benutzereigenen Schlüsselpaares.

Unternehmensstore dient zur Abfrage des unternehmenseigenen PGP Keyservers.

BP Store beinhaltet die Schlüssel der Geschäftspartner, die von der Sicherheitsabteilung zertifiziert sind.

Die Reihenfolge der Stores ist nicht optimal, weshalb der Schlüsselinhaber die Reihenfolge zuerst ändern muss.
Um das Schlüsselpaar zu importieren, muss zuerst die CD mit dem Schlüsselpaar eingelegt und dann der *Standard Store* mit der rechten Maustaste angeklickt werden. Aus dem Kontextmenü muss dann *Import* ausgewählt werden. Daraufhin erscheint ein Windows Dateiöffnen Dialogfenster, in dem der Dateityp auf *All Files* geändert werden muss. Nachdem das Schlüsselpaar auf der CD ausgewählt und *Öffnen* angeklickt wurde, erscheint das Dialogfenster worin die zu importierenden Schlüssel ausgewählt werden können.
Eine Datei kann ja mehrere Schlüssel bzw. Schlüsselpaare enthalten. Nach dem das zu importierende Schlüsselpaar ausgewählt und zu der Liste der importierenden Schlüsseln hinzugefügt wurde, wird der Import des Schlüsselpaars mit einem Klick auf den *OK* Knopf bestätigt und durchgeführt.
Als nächstes muss das Initialpasswort geändert werden. Dazu klickt man mit der rechten Maustaste auf das Schlüsselpaar, das mit einer Ikone von zwei Schlüsseln angedeutet wird, und wählt aus dem Kontextmenü *Properties*. In dem neuen Fenster werden die Schlüsseleigenschaften angezeigt. In diesem Fenster soll das Register *Secret Key Options* (siehe Abbildung 3.8) gewählt werden. Jetzt kann der Schlüsselinhaber unter *Old Password* das Initialpasswort aus dem Passwortbrief eingeben. In das Feld *New Password* wird das neue persönliche Passwort eingegeben. Jetzt muss vorsichtig vorgegangen werden, da jetzt zuerst auf *Apply* geklickt werden muss, damit die Meldung über das Ergebnis der Passwortänderung kommt. Falls jetzt auf *OK* geklickt wird, fragt die Software nur, ob das Passwort geändert werden soll, gibt aber über das Ergebnis der Änderung keine Rückmeldung. In so einem Fall kann es schon vorkommen, wenn sich der Schlüsselinhaber vertippt hat, dass das Passwort nicht geändert wird. Falls die Meldung über die erfolgreiche Änderung des Passwortes kam, muss der Schlüsselinhaber den Schlüssel der Sicherheitsabteilung signieren. Dazu muss der Schlüsselinhaber den Schlüssel der Sicherheitsabteilung mit der rechten Maustaste anklicken und aus dem Kontextmenü *Properties* wählen. Das neue Fenster sieht anders aus, als bei einem Schlüsselpaar. In dem Fenster soll der Register *UserIDs and Certificates* gewählt werden. In dieser Ansicht muss der Knopf *Certify UserID ...* zum Signieren angeklickt werden. Der Schlüsselinhaber muss den Schlüssel der Sicherheitsabteilung als Metaintroducer anerkennen. Dieser Schritt dient dazu, dass jeder Schlüssel, der mit dem Schlüssel der Sicherheitsabteilung signiert wurde, automatisch als vertrauenswürdig anerkannt wird. Im nächsten Schritt muss der Schlüsselinhaber mit der Eingabe seines persönlichen Passwortes die Signatur vollziehen. Mit diesem Schritt wird aus einem einfachen Schlüssel eine Vertrauensinstanz. Das heißt, dass mit dem Signieren dieses Schlüssels wird jedem Schlüssel vertraut, der die Signatur dieses Schlüssels hat. Danach wird in dem Eigenschaftenfenster des Schlüssels der Sicherheitsabteilung das Zertifikat des Schlüsselinhabers angezeigt. Nach diesem Vorgang werden alle Schlüssel in dem *Standard Store* als gültig (mit der Farbe grün) markiert. Mit diesem Schritt wird es gewährleistet, dass der Schlüsselinhaber nicht jeden Empfängerschlüssel als vertrauenswürdig anerkennen muss, da jeder öffentlicher Schlüssel mit dem Schlüssel der Sicherheitsabteilung, den der Schlüsselinhaber als vertrauenswürdig anerkannt hat, signiert wurde.

Bemerkung 3.1.2 *Ein PGP Schlüssel ist gültig, wenn er*

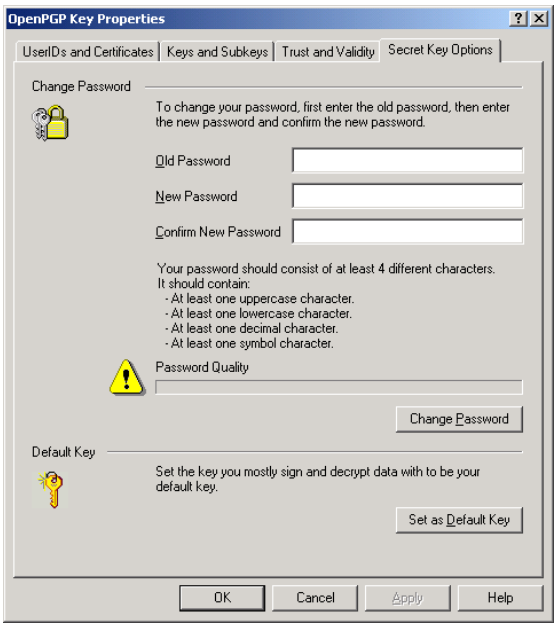

Abbildung 3.8: Ändern des Initialpasswortes

- *vom Inhaber des Schlüsselpaares zertifiziert (unterschrieben) wurde, oder*
- *von genügend anderen Personen unterschrieben (zertifiziert) wurde, denen der Inhaber des Schlüsselpaares traut.*

Ein Schlüssel, der in einem Store als nicht gültig gekennzeichnet ist, wird von PGP nur mit Vorbehalt verwendet:

- *Schlüsselzertifikate, die mit diesem Schlüssel erzeugt wurden, werden nicht beachtet.*
- *Wird eine Unterschrift geprüft, die mit diesem Schlüssel erzeugt wurde, wird eine Warnung ausgegeben, dass nicht garantiert ist, dass dieser Schlüssel zu der angegebenen Person gehört.*

Vertrauen in die Schlüssel
Jeder Schlüssel ist in genau einer Vertrauenstufe. Hat ein Schlüssel einen anderen Schlüssel signiert, wird anhand der Vertrauensstufe bestimmt, ob der signierte Schlüssel als gültig anerkannt wird.

3.1.10 Veröffentlichung des öffentlichen PGP Schlüssels

Obwohl der Schlüssel generiert und an den Inhaber geschickt wurde, kann er nach erfolgreichem Schlüsselimport verschlüsselte und signierte Emails nur versenden. Der Schlüsselinhaber kann aber solange keine verschlüsselte Email empfangen, bis er den erfolgreichen Import nicht mit dem Zurücksenden des unterschriebenen Bestätigungsschreibens bestätigt. Dieser Schritt gewährt eine zusätzliche Sicherheit, dass der Schlüsselinhaber alle Materialien, die zur Verwendung der Emailverschlüsselung erforderlich

bei PGP 2.x.x	bei PGP 5.x	Bedeutung
undefiniert (undefined)	untrusted	Unterschriften mit diesem Schlüssel werden ignoriert.
teilweise (marginal)	marginal	Es müssen mindestens 2 solche Schlüssel einen dritten Schlüssel signieren, damit dieser (der dritte Schlüssel) als gültig anerkannt wird.
voll (complete)	complete	Es muss mindestens 1 solcher Schlüssel einen anderen Schlüssel signieren, damit dieser (der andere Schlüssel) als gültig anerkannt wird.
absolut (ultimate)	ultimate	Zu diesem Schlüssel besitzt man auch den geheimen Schlüssel. Jeder Schlüssel, der mit diesem Schlüssel signiert wird, ist sofort als gültig anerkannt.

Tabelle 3.4: Bedeutung der Vertrauensbezeichnungen bei PGP

ist, erhalten hat. Nachdem das Bestätigungsschreiben bei der Sicherheitsabteilung eingetroffen ist (Schritt sieben in der Abbildung 3.5.), wird der öffentlicher PGP Schlüssel der Schlüsselinhaber mit dem PGP Schlüssel der Sicherheitsabteilung von dem Sicherheitsadministrator signiert und in den dafür vorgesehenen Store (Keyserver) der Verschlüsselungssoftware kopiert. Der Store des Keyservers wird offline in der Sicherheitsabteilung von dem Sicherheitsadministrator verwaltet und nach Aktualisierung auf dem Keyserver kopiert, d.h. die Datei auf dem Keyserver ersetzt. Dieser Store muss auf den Server, auf dem der unternehmenseigene Keyserver läuft, kopiert werden. Dazu wird die Anwendung Microsoft Frontpage benötigt. Der Sicherheitsadministrator meldet sich auf dem Server, worauf der *CryptoEx Keyserver* der Firma Glück & Kanja läuft, an. Nach erfolgreicher Anmeldung muss in das Verzeichnis *stores* gewechselt werden und mittels Drag-and-Drop die Storedatei hinkopieren.

3.1.11 Verwendung der Emailverschlüsselung mit PGP Schlüssel

Nach dem erfolgreichen Import und Zurücksenden des unterschriebenen Bestätigungsschreiben. Kann der Schlüsselinhaber eine Email verfassen und mit Anklicken der Iko-

ne 3.4 kann der Schlüsselinhaber die verfasste Email als verschlüsselt senden (Schritt acht in der Abbildung 3.5). Der Schlüsselinhaber wird über den Verschlüsselungsvorgang visuell informiert. Wie die Emailverschlüsselung abläuft zeigt das UML Diagramm 3.9. Falls der Empfänger keinen gültigen Schlüssel auf dem Keyserver hat, bekommt der Absender eine Meldung darüber. Nach dem Versenden der Email, wird sie in dem Outlook Ordner *Gesendete Objekte* abgelegt und da die Email sowohl an den Empfänger als auch an den Absender (mit zwei Schlüsseln) verschlüsselt wurde, kann der Schlüsselinhaber (sowohl der Absender als auch der Empfänger) die versendete Email nach Eingabe des persönlichen Passwortes lesen.
Falls der Absender eine Email an eine Empfängerliste verschlüsseln möchte, muss er genauso vorgehen, wie bei einem einzigen Empfänger. Die Empfängerliste wird von Microsoft Outlook automatisch aufgelöst. Die Verschlüsselungssoftware holt die öffentlichen Schlüssel im Hintergrund und verschlüsselt die Email. Problematisch wird es nur dann, wenn mindestens einer der Empfänger keinen öffentlichen Schlüssel hat. Dabei spielt es keine Rolle, ob der Empfänger ein Geschäftspartner oder ein Mitarbeiter ist. Wenn dieser Fall eintritt, erhält der Absender die Meldung wie im Abschnitt *Funktionsweise der Software* berschrieben ist. In diesem Fall kann der Absender entweder den Empfänger ohne Schlüssel aus der Liste der Empfänger entfernen oder einen Drittschlüssel diesem Absender zuordnen.

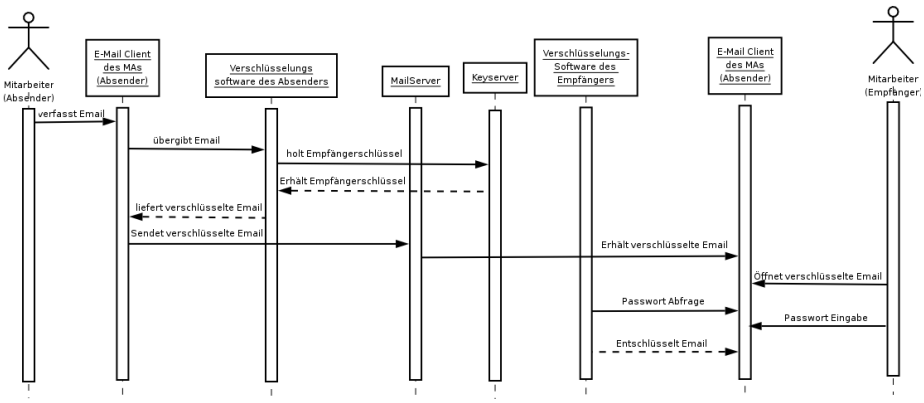

Abbildung 3.9: Funktionsweise der Emailverschlüsselung

Die erste Vorgehensweise wäre eigentlich die richtige. Nachdem der Empfänger ohne Schlüssel entfernt wurde, kann die Email verschlüsselt gesendet werden. Der Absender sollte dann den Empfänger ohne Schlüssel anschreiben, dass er sich ein PGP Schlüssel bestellen soll, damit er auch die vertrauliche und verschlüsselte Informationen erhält. Die zweite Vorgehensweise wird zwar meistens gewählt, führt leider zu unentschlüsselbaren Emails, weil Schlüssel und Emailadresse stimmen nicht überein. Auch wenn der Empfänger später einen Schlüssel hat, kann er die Email nicht entschlüsseln. In diesem Fall wendet er sich an die Hotline, die ihm erklärt was schief gegangen ist.
Diese zweite Möglichkeit wird für den Fall offen gehalten, wenn ein kleines Unternehmen für alle seine Emailadressen den selben Schlüssel verwendet.

3.1.12 Wiederbereitstellung von PGP Schlüsselpaaren

Die Authentifizierung und Autorisierung erfolgt wie im Abschnitt 3.1.6.
Es gibt verschiedene Möglichkeiten, wie es zu einer Wiederbereitstellung kommen kann. Entweder bestellt der Schlüsselinhaber ein neues PGP Schlüsselpaar oder er fordert eine Wiederbereitstellung des Initialpasswortes oder des PGP Schlüsselpaares mit der Angabe auf dem Bestellformular. Eine Wiederbereitstellung des Initialpasswortes bzw. des PGP Schlüsslepaares ist nur dann möglich, wenn eine der beiden vorhanden ist (siehe Tabelle 3.5). Das Initialpasswort wird per deutsche Post, die CD mit dem Bestätigungsschreiben per unternehmensinterner Post zugestellt. Wenn der Schlüsselinhaber weder die CD mit dem PGP Schlüsselpaar, noch das Initialpasswort mehr hat, dann ist keine Wiederbereitstellung möglich. In so einem Fall kann der Schlüsselinhaber, falls er noch verschlüsseltes Material vorliegen hat, das widerrufene PGP Schlüsselpaar zugeschickt bekommen. Wenn der Schlüsselinhaber ein neues PGP Schlüsselpaar benötigt und die Daten in dem Formular korrekt sind, kann mit dem Bestellvorgang begonnen werden. Falls die Daten nicht korrekt oder unvollständig sind, wird der Schlüsselinhaber gebeten die Daten zu korrigieren.

Initialpasswort	CD mit PGP Schlüsselpaar	
	vorhanden	verloren
vorhanden	keine Wiederbereitstellung nötig	Wiederbereitstellung möglich
verloren	Wiederbereitstellung möglich	keine Wiederbereitstellung möglich

Tabelle 3.5: Wiederbereitstellung von PGP Schlüsselpaaren

3.1.13 Widerruf von PGP Schlüsseln

Ein Fall für den Widerruf eines PGP Schlüsselpaares liegt es vor, wenn der Schlüsselinhaber weder die CD mit dem PGP Schlüsselpaar noch das Schreiben mit dem Initialpasswort mehr besitzt (vgl. Abschnitt 3.1.12). Ein anderer Grund für den Widerruf liegt vor, wenn der Mitarbeiter ungewollt oder nicht im Frieden aus dem Unternehmen ausgeschieden ist.
Bei dem Widerruf muss der Sicherheitsadministrator die Sicherung des Schlüssels wieder in einen der dafür geeigneten Store der Verschlüsselungssoftware einspielen und das Schlüsselpaar mit Eingabe des Initialpasswortes des zu widerrufenden Schlüsselpaares aus der Datenbasis der Sicherheitsabteilung, widerrufen. Das widerrufene PGP Schlüsselpaar wird ähnlich wie im Abschnitt 3.1.10 in zwei Stores der Verschlüsselungssoftware ersetzt werden. Der Sicherheitsadministrator muss danach den Store auf

dem Server, auf dem der Keyserver läuft, aktualisieren. Dieses muss im Fall von Widerrufen eines PGP Schlüsselpaares schnell passieren.

3.1.14 Emailverschlüsselung mit Geschäftspartnern

Bisher wurde nur eine geschlossene Anwendergruppe betrachtet. Die Mitglieder dieser Gruppe können interoperabel miteinander kommunizieren, da sie alle dieselbe Infrastruktur und Konfiguration verwenden. Da die meisten Unternehmen mit Geschäftspartnern kommunizieren, muss der Kreis erweitert werden. Bei der Kommunikation über Emailverschlüsselung zwischen Mitarbeiter und Geschäftspartner kommt es zu einem wichtigen Punkt, wie die öffentlichen Schlüssel der Geschäftspartner zu dem Mitarbeiter gelangen. Wenn der Mitarbeiter den öffentlichen Schlüssel des Geschäftspartners hat, muss dieser u. U. noch verifiziert werden. Nach der Verifikation muss dem Schlüssel auch vertraut werden, damit die Emailverschlüsselung funktioniert. Dabei muss zwischen PGP und S/MIME Emailverschlüsselung unterschieden werden. Da die S/MIME Emailverschlüsselung bisher von dem Unternehmen nicht unterstützt wurde, wird dies nicht ausführlich behandelt. Bei der Anwendung von S/MIME Emailverschlüsselung wurden die Mitarbeiter gebeten, ein S/MIME Zertifikat (X.509 Zertifikat für Emailverschlüsselung) von dem Geschäftspartner zu holen oder, wenn es nicht möglich war, extern bei einem Trustcenter zu kaufen.
Bei der Emailverschlüsselung mit PGP muss der Mitarbeiter den öffentlichen Schlüssel des Geschäftpartners entweder auf sicherem Weg erhalten oder über einen unsicheren Kanal. In der jetzigen Softwarekonfiguration der Verschlüsselungssoftware ist kein Keyserver von Geschäftspartnern vorhanden. Deshalb muss der Mitarbeiter den Schlüssel des Geschäftspartners über die Webseite des Geschäftspartners oder auf sonstige Wege (Email, Datenträger etc.) besorgen. Wenn der Schlüssel des Geschäftspartner über einen unsicheren Kanal erhalten wurde, muss die Authentizität des Schlüssels durch Vergleich des Hashwertes (PGP-Fingerprint) über einen vertrauenswürdigen (authentischen) Kanal, z.B. ein Telefonat, mit dem Schlüsselinhaber abgeglichen werden. Mit dem Vergleich des Fingerprints wird eine evtl. Verfälschung des Schlüssels (man in the middle attack, siehe dazu http://www.it-administrator.de/lexikon/man-in-the-middle-attack.html) erkannt, da ein Dritter bei der Übertragung des Schlüssels über einen unsicheren Kanal den Schlüssel abfangen und mit einem verfälschten austauschen kann.
Nachdem der Mitarbeiter den Schlüssel des Geschäftpartners verifiziert hat, fehlt noch das Vertrauen in den Schlüssel, damit er verwendet werden kann. Dazu muss der Mitarbeiter den verifizierten öffentlichen Schlüssel des Geschäftspartners an die Sicherheitsabteilung schicken. Die Sicherheitsabteilung signiert mit normaler Signatur den öffentlichen Schlüssel des Geschäftspartners und veröffentlicht ihn in dem Geschäftspartner Store, der automatisch verteilt wird. Somit haben mehrere Mitarbeiter Zugriff auf den Schlüssel des Geschäftspartners.

3.1.15 Lebenszyklus

Die Abschnitte 3.1.4 bis 6.2.10 beschreiben den Lebenszyklus eines PGP Schlüssels. Der Schlüssel entsteht bei der Generierung auf Anfrage und wird nach Verwendung und eventueller Wiederbereitstellung irgendwann widerrufen. Mit dem Widerrufen des Schlüssels beendet dies den Lebenszyklus.

3.1.16 Zusammenfassung und Bewertung

Dieser Anwendungsfall ist inzwischen erprobt. Obwohl viele Mitarbeiter sich damit auskennen, kommt es immer wieder zu Problemen verschiedener Art, die folgend beschrieben werden.

Kritik 3.1.1 *Es gibt immer wieder Mitarbeiter die das PGP Schlüsselpaar per Email oder Telefon bestellen möchten. Sie müssen auf die Seiten der Emailverschlüsselung im Intranet verwiesen werden.*

Kritik 3.1.2 *Der Sicherheitsadministrator übernimmt auch Aufgaben der Registrationsstelle (vgl. 5.2.2), die sich im Prinzip leicht automatisieren lassen würden, da alle Daten in elektronischer Form vorliegen.*

Kritik 3.1.3 *Das Bestellformular (Exceltabelle) wird oft falsch ausgefüllt, da das Bestellformular an manchen Stellen missverständlich ist:*

1. *oft wird nicht angegeben, was der Mitarbeiter genau anfordern möchte:*
   (a) *ein neues Schlüsselpaar für Email- und Dateiverschlüsselung*
   (b) *ein neues Schlüsselpaar für Email- und Dateiverschlüsselung, weil eine Änderung der Emailadresse vorliegt*
   (c) *ein neues Schlüsselpaar für Email- und Dateiverschlüsselung, weil das vorhandene Schlüsselpaar abgelaufen ist*
2. *Statt der Privatadresse wird oft die Standortadresse eingetragen.*

Kritik 3.1.4 *Der Sicherheitsadministrator muss die von dem Mitarbeiter angegebenen Daten aus dem Bestellformular in die Datenbasis der Sicherheitsabteilung kopieren. Dabei oder vor der Generierung muss der Sicherheitsadministrator die Daten auf Richtigkeit überprüfen.*

Kritik 3.1.5 *Es besteht die Möglichkeit, dass die Daten aus der Datenbasis der Sicherheitsabteilung in die CSV Datei vor der Generierung falsch kopiert werden, oder die Emailadresse aus dem Corporate Directory falsch übernommen wird. Da die externen Mitarbeiter keinen Eintrag im Corporate Directory haben, muss der Sicherheitsadministrator aus dem Globalen Adressbuch die Emailadresse nachschauen und weil von dort kein Kopieren möglich ist, in die CSV Datei manuell eintragen. Bei dem manuellen Eintragen und bei dem Kopieren der Emailadresse können Fehler gemacht werden.*

Kritik 3.1.6 *Falls der Sicherheitsadministrator vor der Generierung vergisst zu überprüfen, ob der Mitarbeiter bereits ein gültiges Schlüsselpaar hat, kann es vorkommen, dass Mitarbeiter zwei gültige Schlüsselpaare haben. Es kann auch als Folgefehler auftreten, dass der Mitarbeiter zwei gültige öffentliche Schlüssel auf dem Keyserver hat.*

Kritik 3.1.7 *Nach der Generierung müssen die Schlüsselpaare auf CDs gebrannt werden, die mit dem Bestätigungsschreiben zusammen an den Schlüsselinhaber geschickt werden. Es kann vorkommen, dass der Empfänger des Bestätigungsschreibens nicht zu dem Schlüsselinhaber, dessen Schlüssel auf die CD gebrannt wurden, passt.*

Kritik 3.1.8 *Falls der Mitarbeiter die Importanleitung nicht aufmerksam genung durchliest, kommt es vor, dass der Mitarbeiter sein Schlüsselpaar nicht in den Standardstore, der als einziger Store auch Schlüsselpaare aufnehmen kann, sondern in den Geschäftspartnerstore importiert, wodurch aus dem Schlüsselpaar ein öffentlicher Schlüssel im falschen Store wird, weshalb die Verschlüsselung nicht funktionieren kann.*

Kritik 3.1.9 *Falls der Schlüsselinhaber vergisst das Initialpasswort zu ändern, wird das Schreiben mit dem Initialpasswort höchstwahrscheinlich in der Nähe des Rechners (z.B. unter der Tastatur) gut aufbewahrt.*

Kritik 3.1.10 *Wenn der Schlüssel der Sicherheitsabteilung nicht oder nicht als Metaintroducer anerkannt wird, funktioniert die Verschlüsselung nicht, da die öffentlichen Schlüssel von dem Keyserver nicht als vertrauenswürdig von der Verschlüsselungssoftware gewertet werden.*

Kritik 3.1.11 *Vor der Veröffentlichung der öffentlichen Schlüssel müssen diese von der Sicherheitsabteilung mit dem Schlüssel der Sicherheitsabteilung signiert werden. Falls der Sicherheitsadministrator vergisst zu tun, wird der öffentlicher Schlüssel vergessen wurde zu signieren, von der Verschlüsselungssoftware als nicht vertrauenswürdig gewertet.*

Kritik 3.1.12 *Es kann ebenfalls vorkommen, dass der Sicherheitsadministrator den signierten öffentlichen Schlüssel in den Store zu kopieren vergisst, der auf dem Keyserver kopiert wird.*

Kritik 3.1.13 *Wenn der Sicherheitsadministrator vergisst den Schlüsselring auf den Keyserver zu erneuern, können sogar mehrere Schlüssel auf dem Keyserver fehlen.*

Kritik 3.1.14 *Wenn ein Mitarbeiter nicht im Frieden aus dem Unternehmen ausscheidet und die Kündigung eines Mitarbeiters die Sicherheitsabteilung nicht erreicht, bleibt ein Schlüssel auf dem Keyserver unbeabsichtigt stehen.*

Kritik 3.1.15 *Wenn der Sicherheitsadministrator vergisst den Schlüssel zu widerrufen, obwohl es bekannt wurde, dass der Schlüsselinhaber das Schlüsselpaar samt Datenträger und Passwortbrief verloren hat.*

Kritik 3.1.16 *Wenn der Schlüsselinhaber eine Email verfasst, die verschlüsselt versendet werden sollte, aber der Empfänger keinen öffentlichen Schlüssel auf dem Keyserver hat, meldet die Verschlüsselungssoftware, dass kein zu der Emailadresse passenden Schlüssel gefunden werden konnte. Da der Schlüsselinhaber die Email unbedingt versenden will, und da die Verschlüsselungssoftware an dieser Stelle die Möglichkeit der Auswahl eines PGP Schlüssel anbietet , der nicht zu der Emailadresse passt, wird eine Email generiert, die vom Empfänger nicht entschlüsselt werden kann.*

Kritik 3.1.17 *Diese Schlüsselverwaltung funktioniert in dem jetzigen Umfang (ca. 2000 aktive Schlüssel), lässt sich aber nur bedingt skalieren, was aber für die Zukunft wichtig wäre.*

Kritik 3.1.18 *Das Problem bei dieser Schlüsselverwaltung liegt in ihrer Natur, da das Schlüsselmaterial auf einem Rechner und in gesicherter Form vorliegt. Dies erfordert einen Zugriff auf diesen Rechner.*

Kritik 3.1.19 *Da die Lebensdauer der PGP Schlüssel nicht eingeschränkt ist, bedeutet dies ein Risiko und Sicherheitsdefizit, die mit anderen Prozessen und regelmäßiger Überprüfung der Schlüssel teilweise abgedeckt wurde.*

Kritik 3.1.20 *Ein Nachteil dieses Anwendungsfalls, dass er nur den Standard PGP unterstützt und für den Standard S/MIME keine Lösung anbietet. Heutzutage die Unterstützung beider Standards erforderlich, da einige sehr enge und bedeutende Geschäftspartner S/MIME verwenden.*

Kritik 3.1.21 *Es gibt leider Mitarbeiter, die nicht den offiziellen Weg für die Bereitstellung von Geschäftspartnerschlüsseln gehen. Dabei können zwei verschiedene Szenarien auftreten:*

1. *Wenn der Mitarbeiter den Schlüssel des Geschäftspartners in den Standard Store (mit dem eigenen Schlüsselpaar) importiert und signiert, kann es bei einer Neuinstallation zu einem Kommunikationsproblem kommen, weil der Schlüssel des Geschäftspartners nicht mehr von CryptoEx gefunden wird, es sei denn, dass der Mitarbeiter den Standard Store vorher gesichert hat.*

2. *Wenn der Mitarbeiter den Schlüssel des Geschäftspartners in den Store der Geschäftspartner kopiert hat, wird dieser bei einer Aktualisierung verloren gehen, da der Store der Geschäftspartner bei einer Aktualisierung über die zentrale Softwareverteilung überschrieben wird, wobei es zu einem Kommunikationsproblem kommen kann, weil der Schlüssel des Geschäftspartners nicht mehr von CryptoEx Outlook gefunden wird.*

3. *Einige Mitarbeiter, die sich mit der Emailverschlüsselung und mit CryptoEx Outlook gut auskennen legen einen weiteren Store an, wohin sie verschiedene Schlüssel ablegen. Dieses Vorgehen wird von der Sicherheitsabteilung nicht unterstützt und es wird davon abgeraten.*

3.2 Emailsignatur

Für die Emailsignatur wurde in dem Unternehmen eingesetzt. Die Signatur wurde aber nur zur Überprüfung der Integrität der Email verwendet, obwohl an eine qualifizierte oder fortgeschrittene Signatur gestellte Anforderungen und Auflagen in den Gesetzen klar definiert sind (vgl. Abschnitt 2.3.2), deren Einhaltung aber nicht einfach ist. Deshalb wurde darauf vorerst verzichtet.
Für die Emailsignatur wird dasselbe Schlüsselpaar und dieselbe Software *CryptoEx Outlook* verwendet wie zur Emailverschlüsselung. Der Anwender, um die Emailsignatur zu verwenden, benötigt nur ein PGP Schlüsselpaar. Falls der Mitarbeiter noch kein PGP Schlüsselpaar hat und versucht eine Email zu signieren, kommt eine Fehlermeldung, dass die Verschlüsselungssoftware kein PGP Schlüsselpaar gefunden hat. Wenn der Mitarbeiter kein PGP Schüsselpaar hat, muss er eines bestellen. Der Vorgang läuft genauso ab, wie im Abschnitt 3.1.

3.2.1 Verwendung der Emailsignatur

Die Verwendung des PGP Schlüsselpaares ist einfach: der Schlüsselinhaber muss auf eine Ikone in der Outlook-Ikonenleiste klicken. Nach dem der Schlüsselinhaber auf *Senden* klickt, wird der Schlüsselinhaber aufgefordert sein persönliches Passwort einzugeben. Mit der Eingabe des Passwortes signiert der Schlüsselinhaber die Email. Die Verwendung der Emailsignatur mit der Emailverschlüsselung zusammen ist auch möglich. Der Empfänger erhält über eine Meldung, wenn er eine signierte Email erhält. Die Meldung zeigt das Ergebnis der Signaturüberprüfung.

Kritik 3.2.1 *Die Emailsignatur ist zwar funktionsfähig, entspricht dem Stand der Technik aber nicht. In der Regel ist eine Entkoppelung des Signaturschlüssels von den Verschlüsselungsschlüssel wünschenswert.*

3.3 Dateiverschlüsselung

Bei der Dateiverschlüsselung muss zwischen Datei- und Verzeichnisverschlüsselung differenziert werden. Die Datei- und Verzeichnisverschlüsselung werden auch mit Hilfe von PGP Schlüsselpaar und mit Hilfe von *CryptoEx File* (Dateiverschlüsselung) und von *CryptoEx Volume* (Verzeichnisverschlüsselung) bewerkstelligt. Beide arbeiten schlüsselbasiert und greifen auf denselben Schlüsselspeicher, wie die Software *CryptoEx Outlook* für die Emailverschlüsselung und -Signatur zu. Aus diesem Grund benötigt der Anwender kein neues Schlüsselmaterial. Die Schlüsselbestellung läuft genauso ab wie die Bestellung für die Emailverschlüsselung (siehe Abschnitte 3.1.4 bis 6.2.10).

3.3.1 Verwendung der Dateiverschlüsselung

Wenn der Schlüsselinhaber mit der rechten Maustaste auf eine beliebige Datei klickt, kann er aus dem Kontextmenü unter *CryptoEx* den Eintrag *Verschlüsselung* auswählen. In dem erscheinenden Fenster kann der Anwender den Store und einen Schlüssel aus dem ausgewählten Store auswählen. Der Schlüsselinhaber kann mehrere Schlüssel auswählen. Der eigene Schlüssel wird automatisch ausgewählt. Es gibt auch die Möglichkeit nach der erfolgreichen Kodierung die ursprüngliche Datei zu löschen.

3.3.2 Verwendung der Verzeichnisverschlüsselung

Die Verzeichnisverschlüsselung wurde bisher nicht zentral verteilt, sondern von einer Gruppe von Pilotanwendern getestet. Die Software *CryptoEx Volume* arbeitet schlüsselbasiert und verwendet denselben Schlüsselspeicher wie die Emailverschlüsselungssoftware *CryptoEx Outlook* . Aus diesem Grund benötigt der Anwender kein neues Schlüsselmaterial. Die Schlüsselbestellung läuft genauso ab wie die Bestellung für die Emailverschlüsselung (siehe Abschnitte 3.1.4 bis 6.2.10).

Bestellung der Software für Verzeichnisverschlüsselung

Jeder Anwender dieser Gruppe musste eine Email an die Sicherheitsabteilung verfassen. Als Antwort erhielten sie eine Email mit dem Verweis auf die Installationsdateien, einen PowerPoint Foliensatz als Hilfe zur Verwendung sowie der Berechtigung die Software installieren zu dürfen. Zum Einsatz kam die Software *CryptoEx Volume* . Diese greift auf den Schlüsselstore der Emailverschlüsselungssoftware zu, deshalb war kein erneuerter Schlüsselimport nötig.

Installation und Einrichtung der Verzeichnisverschlüsselung

Die Installation erfolgt über ein Installationsskript. Nach der Installation öffenet sich ein Assistent, mit dessen Hilfe die Containerdatei angelegt werden kann. Zuerst muss der Pfad zu der zukünftigen Containerdatei Bild 3.10 gesetzt werden. Im zweiten Schritt

Abbildung 3.10: Setzen des Pfades zu der Containerdatei

(Bild 3.11) lässt sich die Größe und Schlüssellänge für die Verschlüsselung für die Containerdatei auswählen. Beide Werte werden vorgeschlagen. Die Schlüssellänge lässt sich nicht ändern. Dieser Wert wurde während der Installation festgelegt. Als nächstes muss der Anwender die Schlüssel für die Verschlüsselung (Bild 3.12) auswählen. Per Voreinstellung ist kein Schlüssel bzw. Schlüsselpaar ausgewählt. Dadurch soll gewährleistet werden, dass der Anwender bewusst Schlüssel zur Verschlüsselung auswählt.
Die Abbildung 3.12 zeigt das Fenster, in dem auf den Knopf *OpenPGP* geklickt werden muss. In dem neuen Fenster kann man die Schlüssel für die Verschlüsselung auswählen. Dabei muss darauf geachtet werden, dass die Anwendung auch die Wahl eines öffentlichen Schlüssels (Fremdschlüssels) zulässt. Falls der Anwender sein eigenes Schlüsselpaar nicht auswählt, kann die angelegte Containerdatei nicht verwenden. Im nächsten Schritt (Abbildung 3.13) kann dem zukünftigen Laufwerk ein Name gegeben werden. (Die Containerdatei wird als lokaler Datenträger in das Windows Dateisystem eingehängt.)
Das verwendete Filesystem kann ebenfalls hier gewählt werden. In dem PowerPoint Foliensatz zur Einführung (siehe voriger Abschnitt) wird dem Anwender geraten NTFS als Filesystem wegen der Möglichkeit der Rechteverwaltung zu wählen. Danach lässt

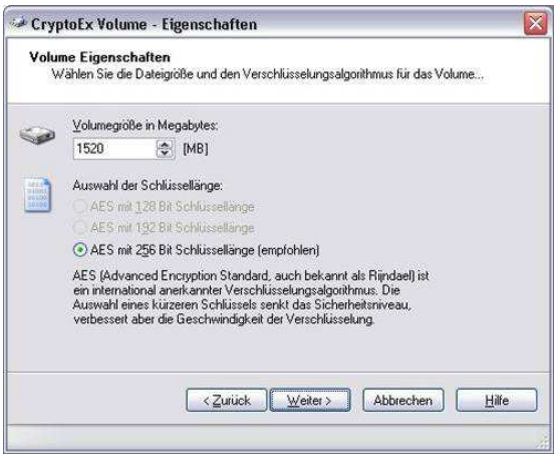

Abbildung 3.11: Eigenschaften der Verschlüsselung von der Containerdatei

Abbildung 3.12: Verschlüsselungsschlüssel der Containerdatei

sich ein Laufwerksbuchstabe des lokalen Datenträgers (eingehängte Containerdatei) zuordnen. Hier (siehe Abbildung 3.14) kann man auch die Option wählen, ob das automatisches Einhängen nach einem Login erfolgen soll oder nicht. Falls diese Option gewählt wird, erscheint nach dem Login ein Fenster zur Passworteingabe. Nach der Zusammenfassung, die in einem eigenen Fenster angezeigt wird, wird der zukünftige lokale Datenträger mit dem gewählten Dateisystem formatiert. Zum Schluss wird der Einhängepunkt (mount points) des lokalen Datenträgers angezeigt.
Man kann auch die Containerdatei manuell einhängen. Dies kann mit Hilfe des *CryptoEx Volume Managers* vorgenommen werden. Nach dem Start öffnet sich ein Fenster, in dem alle dem Manager bekannte Containerdateien (Abbildung 3.15) gelistet angezeigt werden. Die in der Listenanzeige gewählte Containerdatei kann über *Volumes* $\Rightarrow$ *Volume Verbinden* (siehe Abbildung 3.16) nach der Passworteingabe in das Dateisystem eingehängt werden.
Die eingehängte Containerdatei wird im Windows Explorer als ein neuer lokaler Datenträger angezeigt. Man kann mit diesem lokalen Datenträger genauso arbeiten, wie

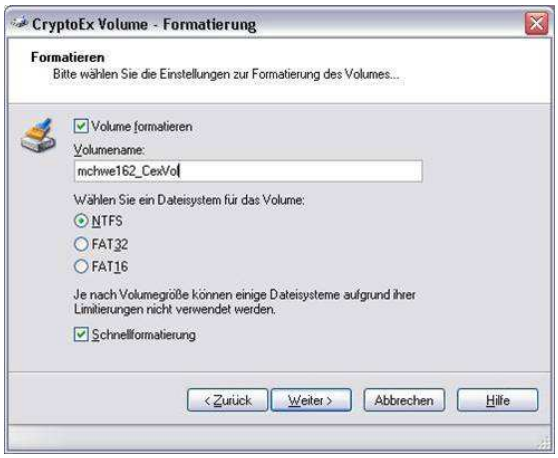

Abbildung 3.13: Benennung des lokalen Datenträgers und Wahl des Dateisystems

Abbildung 3.14: Zuweisung eines Laufwerksbuchstaben

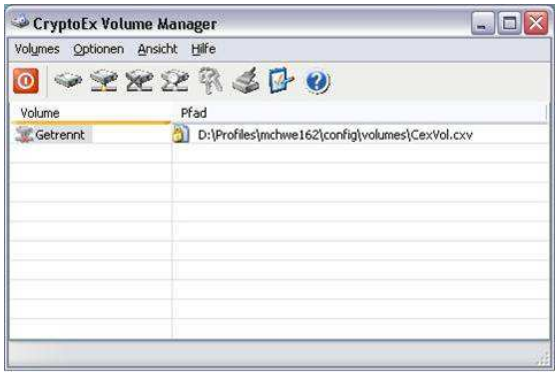

Abbildung 3.15: Dateiverschlüsselung mit CryptoEx File

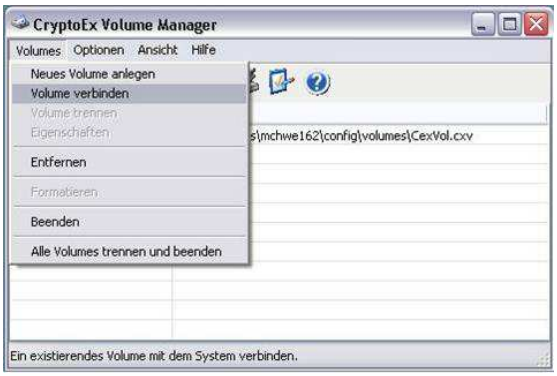

Abbildung 3.16: Dateiverschlüsselung mit CryptoEx File

mit einem herkömmlichen lokalen Datenträger. Nach Angabe des Herstellers erfolgt die Entschlüsselung stets im Hauptspeicher und es werden keinerlei temporäre Dateien angelegt.
Aus Rückmeldungen ist bekannt, dass verschiedene Windows Anwendungen temporäre Dateien schreiben und zum Teil hinterlassen. Diese temporären Dateien sind natürlich unverschlüsselt und bedeuten ein Sicherheitsrisiko. Aus dem Grund wurde den Anwendern geraten, das Verzeichnis der temporären Dateien (*D: \temp*) regelmäßig zu löschen.
Ebenfalls aus Rückmeldungen kam hervor, dass dieses Produkt bei der Verwaltung (vor allem beim Schreiben) von vielen kleinen Dateien an ihre Grenzen stößt. Das macht sich an dem Performance bemerkbar.

3.4 Dateisignatur

Die Dateisignatur wird auch mit Hilfe von *CryptoEx File* und PGP Schlüsselpaar bewerkstelligt. Die Software greift auf denselben Schlüsselspeicher, wie die Software für die Emailverschlüsselung und -Signatur, zurück. Deshalb benötigt der Anwender kein neues Schlüsselmaterial. Die Schlüsselbestellung läuft genauso ab wie die Bestellung für die Emailverschlüsselung (siehe Abschnitte 3.1.4 bis 6.2.10). Das Cryptomaterial wird genauso angefordert und erhalten wie es in dem Abschnitt 3.1 beschrieben wurde. Die Zusatzsoftware zur Dateisignatur stammt von dem selben Hersteller und kann auf dessen Schlüsselspeicher zugreifen und somit mit dem Cryptomaterial des Anwenders die Datei signieren.

3.4.1 Verwendung der Dateisignatur

Wenn der Schlüsselinhaber mit der rechten Maustaste auf eine beliebige Datei klickt, kann er aus dem Kontextmenü unter *CryptoEx* den Eintrag *Signatur* auswählen. In dem erscheinenden Fenster kann der Anwender den Store und einen Schlüssel aus dem ausgewählten Store auswählen. Die Verwendung der Dateisignatur ist wie die digitalen Signaturen nur mit Hilfe eines Schlüsselpaares möglich. Der Schlüsselinhaber

Abbildung 3.17: Dateisignatur mit CryptoEx File

kann den Store und ein Schlüsselpaar aus dem selektierten Store auswählen. Nach der Eingabe des Passwortes wird die Datei signiert.

3.5 Code-Signatur

Bei den bisherigen Anwendungsfällen wurde stets PGP Cryptomaterial verwendet. Bei den kommenden werden X.509 Zertifikate gebraucht. Da X.509 nicht von PGP Software generiert werden kann, müssen diese extern zugekauft werden.
Bei der Code-Signatur geht es um das Signieren einer Anwendung. Die Signatur soll gewährleisten, dass die Anwendung aus vertraulicher Quelle stammt und keine bösartigen Absichten hat. Mit dieser Lösung soll eine zusätzliche Hilfe bei der Unterscheidung zwischen bösartigen und vertraulichen Anwendungen erleichtert werden. Verschiedene Anwendungen können signiert werden:

JAVA Code, besser gesagt JAR (**J**ava **AR**chive) Dateien. JAR Dateien sind mit Hilfe einer Laufzeitumgebung (JRE - Java Runtime Environment) lauffähig. Die Signatur von JAR Dateien werden nicht näher betrachtet. Weiter Informationen zur JAR Signatur befinden sich unter [SJS02, SKT02, MFSJ99].

VBA Code - bei VBA (**V**isual **B**asic for **A**pplication) handelt sich um Markos, die in einer Microsoft Office Anwendung laufen. Die Microsoft Office Anwendungen haben einen eingebauten Sicherheitsmechanismus, der vier verschiedene Sicherheitsebenen kennt. Mit diesen vier Stufen lässt sich die Ausführung von Makros steuern (siehe Abbildung 3.18). Falls ein Makro signiert ist, kommt keine Sicherheitswarnung, falls das Zertifikat, mit dem der Makro signiert wurde, dem System als Vertrauenswürdig bekannt ist.

Treiber - bei Treibern handelt es sich meistens um Bibliotheken (DLL - **D**ynamic **L**ink **L**ibrary) bzw. ausführbare Dateien (EXE). Falls ein Anwender versucht einen Treiber zu installieren, kommt eine Meldung über die Signatureigenschaften und eine Frage, ob der Anwender dem Zertifikat vertraut und den Treiber installieren

möchte. Dieser Ansatz kommt verstärkt in dem neuen Microsoft Betriebssystem Windows Vista zum Einsatz. [MSV06]

Abbildung 3.18: Sicherheitsebenen der Office Anwendungen

3.5.1 Bestellung

Das Problem der Codesignatur kann mit PGP Schlüsselmaterial nicht gelöst werden. Die Code-Signatur benötigt anderes Cryptomaterial als PGP liefern kann. Das Cryptomaterial (X.509 Zertifikat) muss im Zertifikatsspeicher von Microsofts Betriebsystem vorhanden sein, um VBA Code signieren zu können. Für die Verifikation muss das Rootzertifikat des Code-Signaturzertifkats auf jedem Client in dem Zertifikatsspeicher des Betriebsystems vorhanden sein. Dies lässt sich mittels SMS bzw. Policy an alle Clients verteilen.
Da CryptoEx das benötigte Cryptomaterial nicht liefern kann, musste ein geeignetes Cryptomaterial beschafft werden. Es wurde bei einem externen Trustcenter durch die Sicherheitsabteilung bestellt. Der Entwickler fordert über seinen Vorgesetzten bei der Sicherheitsabteilung ein Codesignatur Zertifikat an. Die Daten des Entwicklers (Name und Abteilung) werden mit den Daten des Corporate Directory vergleichen. Bei der Überprüfung wird auch die Abteilung untersucht, ob diese Abteilung auch für Entwicklung zuständig ist.
Die Sicherheitsabteilung sendet eine Verpflichtungserklärung an den Entwickler, in der er sich zur vertraulichen Verwendung des Cryptomaterials verpflichtet. Nachdem diese unterschriebene Erklärung in der Sicherheitsabteilung eintrifft, wird zu der Codesignatur benötigtes Cryptomaterial dem Entwickler zugeschickt.

3.5.2 Verwendung

Der Entwickler muss das Zertifikat in das Zertifikatsstore des Betriebsystems importieren. Falls er ein Makro signieren will, kann er dies in der entsprechenden Anwendung tun. Über den Weg *Extras* ⇒ *Makro* ⇒ *Visual Basic Editor* wird zuerst der Visual Basic Editor geöffnet. Mit Hilfe dieses Editors können Makros erstellt und signiert werden. Ob ein VBA Makro signiert ist, kann man über *Extras* ⇒ *Digitale Signatur* anzeigen lassen. In diesem Fenster (vgl. Abbildung 3.19) kann man auch die Makrozertfizierung vornehmen. Wenn man auf *Wählen* klickt, dann öffnet sich der Zertifikatsspeicher des angemeldeten Benutzers. In diesem Anziegefenster lässt sich ein Zertifikat anzeigen und auswählen. Nach dem ein Zertifikat ausgewählt wurde, kann man das Makro speichern. Es gibt auch eine ausführliche Beschreibung von Microsoft ([MSCS02]) zur VBA Code-Signatur.

Abbildung 3.19: Anzeigefenster von Digitaler Signatur

3.5.3 Bewertung

Kritik 3.5.1 *Es gibt nur ein Zertifikat, das von mehreren Entwicklern verwendet wird. Falls ein Entwickler das Zertifikat missbraucht muss bei dem TrustCenter das Sperren des Zertifkats und ein neues Zertifikat angefordert werden. Dies verursacht wiederum weitere Kosten und evtl. Imageschaden.*

Kritik 3.5.2 *Da nur ein Codesignaturzertifikat verteilt wird, ist die Steuerung der Gültigkeit sehr stark eingeengt. Wenn der Rückruf eines Zertifikates im Prinzip genügen würde, müssen in der Praxis alle zurückgerufen werden.*

3.6 Dokumentensignatur

Die Dokumentensignatur wurde bisher bei dem Unternehmen nicht oft benötigt. Die Dokumentensignatur wird bisher mit Hilfe von Adobe Acrobat gelöst.
Es gibt zwar auch andere Lösungen (z.B. GEVA von Datev EV), diese wurde bisher bei dem Unternehmen aus Kostengründen nicht aufwendig getestet und in Betracht gezogen.

3.6.1 Bestellung

Die Bestellung und Verwaltung wurde bei der bisher geringen Anzahl der Dokumentensignaturzertifikate bei der jeweiligen Abteilung geführt. Die Sicherheitsabteilung bietet ihre Unterstützung nur zur Verwendung.

3.6.2 Verwendung

Die Erstellung der digitalen Signatur ist nur mit Adode Acrobat und mit einem geeigneten X.509 Zertifikat möglich.
Die Softwarehersteller bietet zu der Überprüfung einer Signatur nur unausreichende Unterstützung. Die Software Acrobat Reader kann zwar auf den Zertifikatsstore des Betriebsystems zugreifen, das ist aber in der Standardsoftwareinstallation nicht eingestellt. Stattdessen verwendet die Software einen eigenen Zertifikatsstore, worin sich nur wenige (eigentlich nur von Adobe selber) öffentliche Zertifikate befinden, was zu einer erfolgreichen Validierung nötig wäre. Weitere Informationen bietet dazu der Hersteller unter: http://www.adobe.de/products/acrobat/signature.html

3.7 Benutzerauthentifikation

Das Zertifikat zur Benutzerauthentifikation wird zur zertifikatsbasierten Anmeldung für eine Intranetapplikation benötigt. Bisher war eine Anmeldung über Login und Passwort auch möglich. Diese wurde vor einiger Zeit auf die zertifikatsbasierte Anmeldung umgestellt. Diese Anmeldungsart gewährleistet eine höhere Sicherheit.

3.7.1 Bestellung des Authentifizierungszertifikates

Die Zertifikatsbestellung läuft über die Personalabteilung. Der Personalabteilung ist bekannt, wer auf diese Intranetapplikation einen Zugriff benötigt. Zu der zertifikatsbasierten Anmeldung erforderliches Cryptomaterial kann *CryptoEx* nicht liefern, deshalb wurden die Zertifikate für diesen Zweck bei dem Geschäftspartner bestellt, der auch die Intranetapplikation wartet und eine eigene interne PKI betreibt. Die Zertifikatsbestellung kommt von der Personalabteilung und wird an die Sicherheitsabteilung übergeben. Die Sicherheitsabteilung kann in Einzelfällen entweder über eine Webapplikation oder über eine Batch-Schnitstelle bestellen.

3.7.2 Verteilung des Authentifizierungszertifikates

Nach erfolgreicher Bestellung erhält der Zertifikatseigentümer eine PIN Email mit der Import-PIN. Das Zertifikat wird an die Sicherheitsabteilung in verschlüsselter Email geliefert. Die Sicherheitsabteilung sendet das Zertifikat in einer verschlüsselten Email an den Zertifikatsinhaber. Falls der Zertifikatsinhaber keine Emailverschlüsselung (keinen PGP Schlüssel) hat, wird das Zertifikat auf eine CD gebrannt und per unternehmensinterner Hauspost an den Zertifikatsinhaber geschickt.

3.7.3 Import des Authentifizierungszertifikates

Dem Zertifikatsinhaber wird ein Intranetlink auf die Importanleitung gemeinsam mit dem Zertifikat in der verschlüsselten Email geschickt. Der Zertifikatsinhaber soll anhand dieser Anleitung das Zertifikat ohne Probleme importieren können, da die Anleitung einfach gehalten ist und mit vielen Bildern versehen ist.
Der Zertifikatsinhaber soll zuerst die verschlüsselte Email mit der Eingabe des persönlichen Passwortes öffnen und dann die Zertifikatsanlage speichern. Dieser Schritt ist wichtig, da die sofortige (on-the-fly) Anhangentschlüsselung aus Performancegründen abgeschaltet ist. Die Emailanlage wird erst beim Speichern entschlüsselt.
Nach dem der Zertifikatsinhaber das Zertifikat gespeichert hat, kann er die Zertifikatsdatei mit einem Doppelklick öffnen. Danach meldet sich der Zertifikatsimport-Assistent und fragt nach der Import-PIN. Sie muss aus der PIN-Email geholt werden. Nach der PIN-Eingabe, kann der Zertifikatsinhaber wählen, ob er für die Zertifikatsverwendung noch eine zusätzliche Sicherheit (Passwortschutz) vergeben möchte. Die Sicherheitsabteilung empfiehlt es nicht zu tun, da der Zertifikatsinhaber sich noch ein zusätzliches Passwort merken müsste. Nach dem letzten Schritt kommt eine Meldung über den Erfolg des Importvorganges.

3.7.4 Verwendung des Authentifizierungszertifikates

Die Benutzerauthentifikation wird bei der Anmeldung zu einer Intranetapplikation verwendet. Bei der Anmeldung handelt es sich um eine zertifikatsbasierte Benutzeranmeldung. Dazu wird ein X.509 Zertifikat mit speziellem Inhalt im Subject-Feld. Das Zertifikat wird bei einem Partnerunternehmen, das auch die Intranetapplikation wartet, ausgestellt.
Im Anhang C finden Sie die Eigenschaften der Authentifizierungszertifikaten, wie sie von dem OpenSource Werkzeug OpenSSL (http://www.opensssl.org) gelistet werden.

3.7.5 Widerruf des Authentifizierungszertifikates

Bei dem Verlust des Zertifikats lässt der Sicherheitsadministrator über die Webapplikation das Zertifikat sperren und bei Bedarf ein neues Zertifikat für den Mitarbeiter bestellen.

3.7.6 Wiederbereitstellung des Authentifizierungszertifikates

Falls der Mitarbeiter die PIN-Email gelöscht oder nicht erhalten hat, kann eine Wiederbereitstellung von dem zentralen Sicherheitsadministrator über die Webapplikation angefordert werden.

3.7.7 Bewertung

Kritik 3.7.1 *Jede Anforderung sei es Zertifikatsbestellung oder Zertifikatswiderruf wird dem Unternehmen in Rechnung gestellt. Je mehr Mitarbeiter unausreichend mit der*

PIN-Email umgehen, desto mehr Kosten werden verursacht. Dies führt zu nicht kalkulierbaren Kosten, was bei jedem Unternehmen im Prinzip zu vermeiden ist. Mit einer eigenen PKI lassen sich diese Kosten enorm senken. Die eigene PKI schafft Unabhängigkeit.

Kritik 3.7.2 *Es kommt sehr oft vor, dass Mitarbeiter die PIN Email löschen, da sie sie nicht für wichtig halten. Da die PIN-Email nicht über die Sicherheitsabteilung geht, ist sie nicht wiederherstellbar.*

Kritik 3.7.3 *Da die PIN-Email von einem engen Geschäftspartner kommt, der nicht bereit ist, eine angepasste Email an das Unternehmen zu erstellen und diese PIN-Email Hinweise auf den Importvorgang bzw. einen Intranetlink auf eine Importanleitung beinhaltet, kommt es oft vor, dass Mitarbeiter die falsche, in der Email genannte Importanleitung verwenden. Mit einer eigenen PKI kann dieser Fehler behoben werden.*

Kritik 3.7.4 *Viele Mitarbeiter machen einen Fehler, in dem sie auf die Anlage klicken und so versuchen sie zu öffnen. Da meldet das Betriebsystem einen Fehler während des Importvorgangs, weil das Zertifikat in verschlüsselter Form dem Betriebsystem übergeben wurde.*

Kritik 3.7.5 *Jede Bestellung, Wiederbereitstellung, Widerruf und Neubestellung gehen nur über die Sicherheitsabteilung. Die Sicherheitsabteilung leitet diese Anfragen weiter, die dann nach einiger Zeit bearbeitet werden. Diese Zeitverzögerung und der Zusatzaufwand würden sich mit einer eigenen PKI minimieren.*

3.8 Sonstige Anwendungsfälle

Diese Prozesse funktionieren gut, erfordern aber einen nicht zu unterschätzenden Administrationsaufwand. Außerdem bieten diese vorhandenen firmeninternen Vorgänge keine Lösung für folgende Fälle:

- VPN-Authentifizierung
- WEB-Serverauthentifizierung
- S/MIME Verschlüsselung

Diese Anwendungsfälle erfordern ein X.509 Zertifikat. Dieses Zertifikat kann von PGP Software nicht generiert werden. Die benötigten Cryptomaterialien wurden zu diesem Zwecken bisher extern zugekauft.

3.8.1 VPN-Authentifizierung

Hierbei muss man zwischen VPN-Server und VPN-Client unterscheiden. Das Zertifikat für VPN Server wurde bisher direkt bei einem Trust-Center bestellt. Eine reine zertifikatsbasierte basierte VPN Client Authentifizierung wurde in Verbindung mit einem RSA Token realisiert. An einer gegenseitigen zertifikatsbasierten Lösung für Authentifizierung im VPN Bereich wird gearbeitet. Zu einer gegenseitigen zertifikatsbasierten Authentifizierung werden auch mehrere X.509 Zertifikate benötigt.

3.8.2 WEB-Serverauthentifizierung

Die Webserver-Zertifikate wurden bisher direkt bei einem Trust-Center bestellt.

3.8.3 Emailverschlüsselung mittels S/MIME

Der andere Standard für Emailverschlüsselung ist am Anfang dieses Kapitels der bereits erwähnte S/MIME. Dieser Standard baut auf X.509 Zertifikat auf. Da ein PGP Software kein X.509 Zertifikat liefern kann, wurde die Emailverschlüsselung über S/MIME bei dem Unternehmen bisher nicht verwendet. Wenn ein Mitarbeiter unbedingt S/MIME Emailverschlüsselung nutzen musste, musste er das dazu benötigte X.509 Zertifikat entweder von dem externen Geschäftspartner mit der er kommunizieren muss, oder von einem TrustCenter holen.

3.8.4 Bewertung der sonstigen Anwendungsfälle

Kritik 3.8.1 *Diese Zertifikate werden extern bei einem TrustCenter gekauft. Falls ein Server neukonfiguriert oder neuinstalliert wird, muss in der Regel das Zertifikat ausgetauscht werden. Diese Zertifikate verursachen Kosten.*

Mit einer eigenen PKI lassen sich die Kosten für die Zertifikate, die in den Abschnitten 3.8.1, 3.8.2 und 3.8.3 vorgestellt wurden, erheblich reduzieren.

Kapitel 4

Anforderungen

Alle im vorherigen Kapitel (Kapitel 3) erwähnten Anwendungsfälle verwenden zertifikatsbasierte bzw. schlüsselbasierte Verschlüsselung und Signatur. Wenn man es genau nimmt, dann muss man eher von Schlüsseln reden, da die vorhandenen Lösungen auf PGP basieren. In der PGP Terminologie gibt es auch Schlüssel und Zertifikate. Diese werden aber anders als im Umfeld von X.509 Zertifikaten verwendet (siehe dazu 3.1.1).
Ziel ist möglichst viele der Anwendungsfälle aus dem vorherigen Kapitel durch eine unternehmensinterne Lösung abzudecken. Es ist für das Unternehmen von großer Bedeutung, dass die Lösungen für alle Anwendungsfälle aus einer Hand, d.h. von einem Softwarehersteller kommen.

4.1 Anforderungen an die Emailverschlüsselung

An die Emailverschlüsselung gestellte Anforderungen können in zwei Aspekte, in organisatorische und technische eingeteilt werden.

4.1.1 Organisatorische Anforderungen

Bei den organisatorischen Anforderungen geht es vor allem um Berechtigung, Autorisierung und Ablauf des Anwedungfalles, wie es erwünscht wäre. Als Ausgangspunkt dienen die Abschnitte Zusammenfassung und Bewertung (Abschnitt 3.1.16). Bei den Anforderungen soll aber nicht nur auf die Probleme, die in der Bewertung erkannt wurden, eingegangen, sondern es sollen auch zukunftsfähige und optimierte Prozesse erzielt werden.

Zuerst muss definiert werden, wer an der Emailverschlüsselung teilnehmen darf und soll. In erster Linie sollen alle Mitarbeiter an der Emailverschlüsselung teilnehmen. Sie sollen das Cryptomaterial nicht zwangsweise erhalten, sondern bei Bedarf anfordern. D.h. wenn ein Mitarbeiter Emails verschlüsseln möchte, aber kein Cryptomaterial hat, soll er zuerst eins bewusst bestellen. Dadurch soll auch die Sensibilität bezüglich der (Email)Verschlüsselung gestärkt werden.

Organisatorische Anforderung 4.1.1 *Jeder Mitarbeiter der einen gültigen Eintrag im globalen Adressbuch hat, ist berechtigt Cryptomaterial zu bestellen. Es ist erwünscht, dass jeder Mitarbeiter ohne Ausnahme für sich selber Cryptomaterial für Emailverschlüsselung bestellt. Demnach vereinfacht sich die Berechtigungsmatrix (siehe Tabelle 4.1).*

Organisatorische Anforderung 4.1.2 *Der zentrale Sicherheitsadministrator soll aber weiterhin für andere Mitarbeiter bestellen, aber nur bestellen dürfen, und nicht wie bisher generieren können. Ob unter solchen Umständen ein lokaler Sicherheitsadministrator erforderlich ist, soll noch geklärt werden. Der Sicherheitsadministrator soll aber nur im Ausnahmefällen Cryptomaterial bestellen können. So ein Ausnahmefall wäre zum Beispiel die Bestellung eines Cryptomaterials für eine Funktionskennung, die ggf. von mehreren Mitarbeitern zeitlich disjunkt aber gemeinsam genutzt werden soll.*

Besteller	Empfänger			
	anderer Mitarbeiter	andere Sekretärin	anderer Vorgesetzter	andere LRA
Mitarbeiter	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt
Sekretärin	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt
Vorgesetzter	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt	Nicht berechtigt
LRA	berechtigt	berechtigt	berechtigt	Nicht berechtigt
zentraler Sicherheits-administrator	berechtigt	berechtigt	berechtigt	berechtigt

Tabelle 4.1: Berechtigungsmatrix für PGP Schlüsselbestellungen

Der erste Schritt ist meistens die Bestellung. Bei der Betrachtung der Abbildung 3.5 fällt sicherlich auf, dass der Bestellprozess der aufwendigste ist. Der optimale Ablauf der vorhandenen Bestellung besteht aus 4 Schritten, die aber eine erfolgreiche Generierung und Verteilung nicht garantieren. Es kommt öfters vor, dass eine Bestellung wegen falscher Daten zurückgeschickt werden muss oder ein Fehler bei der Generierung dem Sicherheitsadminstrator unterläuft.

Bei der aktuellen Bestellung von PGP Schlüsselpaaren (vgl. Abschnitt 3.1.4) musste bisher vieles manuell erledigt werden. Nicht nur der Besteller und zukünftige Schlüsselinhaber, sondern auch der Sicherheitsadministrator. Dies sollte weitgehend automatisiert werden, da mit wachsender Anzahl der Schlüssel die Verwaltungs- und Generierungsaufwand stark anwächst und somit das Zeitintervall zwischen Bestellung und Verteilung groß ist.

Organisatorische Anforderung 4.1.3 *Der Bestellprozess soll so aufgebaut werden, dass der Anwender nur wenige Auswahlmöglichkeiten hat und möglichst wenige Daten selber eingeben muss, damit dieser Punkt als potentielle Fehlerquelle vom Anfang an eliminiert werden kann. Die Bestellung und die Benutzerauthentifikation bzw. Benutzerautorisierung soll über das Intranet erfolgen, da viele Daten über das Intranet erreichbar sind.*

Organisatorische Anforderung 4.1.4 *Die Daten für die Schlüsselgenerierung sollen automatisch aus vorhandenen Datenbeständen geholt werden. Dabei müssen die Firmenvorschriften und Datenschutzgesetze beachtet werden. Aus diesem Grund muss der neue Prozess möglichst wenige personenbezogene Daten (z.B. Privatadresse), die später gelöscht werden müssten, speichern.*

Organisatorische Anforderung 4.1.5 *Die Schlüsselgenerierung selber muss automatisch erfolgen, damit dem Sicherheitsadministrator kein Fehler unterlaufen kann und der Generierungsprozess nicht beeinflusst werden kann. Damit soll auch gewährleistet werden, dass der zentrale Sicherheitsadministrator nur im Notfall an das Schlüsselmaterial eines Mitarbeiters herankommen kann. Dies könnte bei einer Aufforderung höherer Gewalt (z.B. Staatsanwaltschaft) nötig sein.*

Organisatorische Anforderung 4.1.6 *Bei der Generierung soll eine Existenz-Überprüfung von vorhandenen Schlüsseln des Bestellers ebenfalls automatisiert erfolgen, damit verlorene Schlüsselmaterialien bei Bestellung automatisiert zurückgerufen werden können oder eine Wiederbereitstellung erfolgen kann, ohne dass ein Mitarbeiter mehrere gültigen Schlüssel auf dem Online Keystore haben könnte. Dabei soll unterschieden werden, ob eine Wiederbereitstellung möglich und erwüscht ist oder neues Schlüsselmaterial generiert werden soll.*

Organisatorische Anforderung 4.1.7 *Bei der Generierung muss automatisch eine zentrale Sicherheitskopie des Cryptomaterials angefertigt werden, das nicht ohne weiteres aus dem System extrahiert werden kann und darf. Der Schlüsselinhaber soll aber jederzeit und bei Bedarf eine Wiederbereitstellung des gesicherten Cryptomaterials nach ausreichender Authentifikation und Autorisierung anfordern können.*

Der größte Teil des Anwendungfalles für Emailverschlüsselung besteht aus dem Bestellvorgang und der Aktivierung des Schlüsselpaares. Dieser Teil des Anwendungsfalles ist stark optimierungsbedürftig.

Organisatorische Anforderung 4.1.8 *Die Verteilung des Cryptomaterials soll auf elektronischem Weg aber in abgesicherter Umgebung erfolgen. Der Schlüsselinhaber soll über den Vorgang informiert werden. Dem Schlüsselinhaber soll nur wenig Interaktionsmöglichkeit eingeräumt werden.*

Durch die Umstellung der Verteilung soll die Wartezeit zwischen Bestellung und Aktivierung erheblich verkürzt werden. Zurzeit können bis zu 4 Wochen vergehen, bis der Schlüssel auf den Keyserver kommt und damit für andere nutzbar wird.

Organisatorische Anforderung 4.1.9 *Durch die automatisierte Verteilung sollen Passwortbrief und Datenträger entfallen. Diese sind ebenfalls potentielle Gefahrenquelle, da der Schlüsselinhaber diese zwei Materialien getrennt aber sicher aufbewahren soll.*

Organisatorische Anforderung 4.1.10 *Der Schlüsselinhaber soll jederzeit in der Lage sein, sein Passwort zurückzusetzten. Dazu muss natürlich ein Workflow erarbeitet werden, wie es gelöst werden kann. Dies ist stark von dem Importvorgang abhängig, da wenn das Cryptomaterial nicht als Datei auf dem Rechner des Schlüsselinhabers abgelegt wird, kann das Passwort nur in Verbindung mit einer Wiederbereitstellung zu Stande kommen. Es muss eine Lösung zur Registration gefunden werden, da nur registrierte und bekannte Anwender Cryptomaterial bestellen und erhalten dürfen.*

Der Import von Cryptomaterial soll ebenfalls vereinfacht werden. Der vorhandene Importvorgang ist für die meisten Mitarbeiter nicht einfach zu bewerkstelligen und hat einige Kleinigkeiten, deren Nichtbeachtung potentielle Fehlerquelle sind, und als solche zu einer Beeinträchtigung der Funktionalität führen. Durch die automatisierte Verteilung sollen auch eventuelle Fehler während des Importvorganges minimiert werden. Da der Datenträger und Passwortbrief entfallen sollen, muss der Importvorgang umgestaltet werden.

Organisatorische Anforderung 4.1.11 *Der neue Importvorgang soll aber sicher ablaufen. Zum Import soll weiterhin ein Importpasswort verwendet werden.*

Organisatorische Anforderung 4.1.12 *Das Importpasswort soll auf getrenntem aber sicherem Weg zum Schlüsselbesteller geleitet werden. Es wäre von Vorteil, wenn das Cryptomaterial nicht auf dem Rechner des Schlüsselinhabers zwischengespeichert wird, sondern sofort in die entsprechende Applikation nach Abfrage und Eingabe des Importpasswortes importiert wäre.*

Organisatorische Anforderung 4.1.13 *Die Veröffentlichung und Aktivierung der öffentlichen Schlüssel muss ebenfalls automatisiert werden. Die Veröffentlichung der öffentlichen Cryptomaterialien soll auch automatisch erfolgen. Dabei sollen Repositories gewählt und ggf. eingerichtet werden, die sowohl firmenintern als auch von den Geschäftspartnern erreichbar sind. Falls mehrere Repositories erforderlich sind, müssen die Daten der Repositories automatisiert konsistent und aktuell gehalten werden.*

Zentrale Frage bei der Wiederbereitstellung ist, ob der Schlüssel eventuell in fremde Hände geraten sein kann, oder der Mitarbeiter nur einen neuen Rechner oder eine Neuinstallation auf dem bisherigen Rechner erhalten hat.

Organisatorische Anforderung 4.1.14 *Eine Wiederbereitstellung soll für den Schlüsselinhaber schnell und unkompliziert erfolgen. Der Benutzer soll selber in der Lage sein, eine Wiederbereitstellung anzufordern und durchzuführen. Dabei soll eine Authentifizierung des Schlüsselinhabers erfolgen. Weitere Schutzmechanismen wären sinnvoll.*

Organisatorische Anforderung 4.1.15 *Weiter oben wurde schon der Importvorgang angesprochen. Wichtig wäre bei der Wahl der Clientsoftware, dass das Cryptomaterial in einem geschützen Cryptospeicher gehalten wird. Jeder Benutzer soll eine eigene Cryptospeicher für das Cryptomaterial haben und soll auf die Cryptospeicher eines anderen Benutzers nicht zugreifen bzw. nicht in die Clientsoftware einbinden können. Es soll weiterhin gewährleistet werden, dass das Cryptomaterial nicht aus der Cryptospeicher extrahiert werden kann. Wenn ein Schlüsselinhaber seine Cryptomaterial transferiern will, soll die ganze Cryptospeicher kopiert werden.*

Organisatorische Anforderung 4.1.16 *Das Widerrufen eines Schlüssels soll schnell und mit wenig Aufwand erfolgen können. Nur der zentrale Sicherheitsadministrator soll in der Lage sein, ein Cryptomaterial eines Schlüsselinhabers widerrufen zu können. Der Sicherheitsadministrator soll dies auf Anforderung des Vorgesetzten des jeweiligen Schlüsselinhabers bzw. auf Anforderung der Personalabteilung durchführen können. Die Aktualisierung der Stores der öffentlichen Cryptomaterialien sollen automatisch und ohne zusätzlichen Eingriff des Sicherheitsadministrators und ohne große zeitliche Verzögerung erfolgen. Im Notfall soll dies binnen ein paar Stunden erfolgen.*

Organisatorische Anforderung 4.1.17 *Da eine Lösung für offene Gruppen angestrebt ist, soll eine Schnittstelle für Geschäftspartner definiert werden. In der vorhandenen reinen PGP Lösung gibt es eine Schnittstelle nach außen. Die interne und äussere Schnittstellen (PGP Keyserver) sind über standardisierte Verfahren abzufragen. Da die Forderung nach der Unterstützung des S/MIME Standards besteht, muss diese Schnittstelle erweitert werden. Die dazugehörige Infrastruktur wird später angesprochen.*

Organisatorische Anforderung 4.1.18 *Die neue Lösung soll mit der vorhandenen zusammenarbeiten können, da der eventuell erforderliche Austausch der Clientsoftware bei einer Unternehmensgröße von mehreren Tausend Mitarbeitern ein paar Monate in Anspruch nimmt und während dieser Zeit die problemlose Verschlüsselung weiterhin gewährleistet werden muss. Die Umstellung der Clients erfolgt Schrittweise, z.B. nach Standorten.*

Organisatorische Anforderung 4.1.19 *Die Schlüsselverwaltung soll möglichst unabhängig von einem Rechnerzugriff erfolgen. D.h. die Schlüsselverwaltung soll über ein Interface ablaufen, das keine Anmeldung an einem speziellen Rechner erfordert. Der Sicherheitsadministrator soll von jedem beliebigen Ort innerhalb des Firmennetzes sicher und schnell auf die erforderlichen Daten und Verwaltungstools zugreifen können.*

Organisatorische Anforderung 4.1.20 *Die vorhandenen und zukünftige Lösungen müssen zusammenarbeiten, da nicht alle Clients auf einmal umgestellt werden können. Es soll aber eine Lösung erarbeitet werden, wobei die neue Lösung serverseitig sowohl mit den neuen als auch mit den vorhandenen Clients zusammenarbeiten soll.*

Organisatorische Anforderung 4.1.21 *Die neue Lösung soll nicht viel Umstelllungsaufwand von der jetzigen auf die neue Lösung für die Mitarbeiter verursachen. Eine (aufwendige) Schulung der Mitarbeiter zur Verwendung der neuen Lösung soll nicht erfolgen. Als Hilfe soll ein Foliensatz ausreichen können.*

4.1.2 Technische Anforderungen an die Emailverschlüsselung

Es müssen möglichst alle der erwähnten Anwendungsfälle mit der unternehmenseigenen Infrastruktur abgedeckt werden. Die technischen Anforderungen lassen sich in zwei Aspekte einteilen: Standards und Infrastruktur. Bei den Standards geht es um PGP und S/MIME. Bei der Infrastruktur handelt es sich um den Aufbau der Technik, mit deren Hilfe das Verschlüsselungsmaterial verwaltet, verteilt und verwendet wird.

Technische Anforderung 4.1.1 *Bei der Emailverschlüsselung sollen beide Standards openPGP und S/MIME unterstützt werden.*

Theoretisch würde ein Cryptomaterial ausreichen, wenn man aber alle Details beachtet, dann stößt man af verschiedene Probleme. So wie für ein Cryptomaterial für Verschlüsselung in der Regel eine Sicherheitskopie (Backup) erforderlich ist, darf in der Regel für Cryptomaterial für Authentifizierung und Signatur keine angelegt werden. Ein weiteres Problem ist, dass PGP für Authentifizierung keine Lösung bietet. Eine Zusammenfassung der Möglichkeiten verschiedener Standards zeigt die Tabelle 4.2. Detaillierte Informationen sind dazu in [BRA97] zu finden.

	PGP	X.509
Verschlüsselung	möglich und erwünscht	möglich und erwünscht
Signatur	möglich und erwünscht	möglich und erwünscht
Authentifizierung	nicht möglich	möglich und erwünscht

Tabelle 4.2: Möglichkeiten verschiedener Standards

Technische Anforderung 4.1.2 *Es muss wieder ein Ablaufdatum des Schlüsselmaterials, der als Notbremse dienen soll, ermöglicht werden. Das Ablaufdatum soll gewährleisten, dass auch Cryptomaterial durch das Ablaufen ungültig wird, falls eine Kündigung bzw. Ausscheidung die Sicherheitsabteilung nicht erreicht. Die Anforderung an das Cryptomaterial beinhaltet die Tabelle 4.4. Die Cryptomaterialien sollen möglichts nicht nur personifiziert werden, sondern möglichst nur in Verbindung mit einer Domainkennung verwendet werden.*

Technische Anforderung 4.1.3 *Was die Schlüssellänge angeht, wird eine Mindestlänge von 1024 Bit von den verschiedenen Fachliteraturen empfohlen. Deshalb soll bei der Emailverschlüsselung eine Schlüssellänge von mindestens 1024 Bit verwendet werden.*

Die Schlüssellänge wird seit einiger Zeit in der Fachliteratur [LeVe 01, ECRYPT, SCHB01] diskutiert. Die Meinungen gehen bezüglich der Schlüssellänge auseinander. Es werden verschiedene Empfehlungen in der Fachliteratur angegeben. Heutzutage sollte aber mindestens eine Schlüssellänge von 1024 bit verwendet werden, weil

inzwischen sogar 512-Bit-RSA-Schlüssel gebrochen worden sind.
(http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa155.html) Weitere Ausführung zu diesem Thema befindet sich im [CKLW00, Seite 48, 4.8.3 Schlüssellängen] Die Tabelle 4.3 zeigt eine Liste empfohlener Schlüssellänge. Die Schlüssellänge in der Tabelle 4.3 bezieht sich auf die Mindestanforderung.

Jahr	Empfohlene Schlüssellänge
1995	1280
2000	1280
2005	1536
2010	1536
2015	2040

Tabelle 4.3: Empfohlene Schlüssellänge für asymmetrische Schlüssel (Quelle: [SCHB01])

Als Algorithmus wird RSA aus Gründen der guten und verbreiteten Unterstützung und guter Performance gewählt. [SCHB01, Wie98] Bei dem PGP Schlüssel muss RSA Algorithmus aus Kompabilitätsgründen zu älteren PGP Versionen gewählt werden. [CKLW00, Seite 47, 4.8.1 Welche Algorithmen sollen unterstützt werden?]

Die Integration von Mitarbeiter Login bzw. GID soll nicht erfolgen, da diese Informationen aus Sicherheitsgründen nicht nach außen publiziert werden sollen.
Als Laufzeit sollen 2 Jahre gewählt werden. Diese Zeit ist ein guter Kompromiss zwischen Sicherheit und Konformität. Wenn der Bestellvorgang einfach gestaltet werden kann, wäre eine Laufzeit von einem Jahr auch denkbar.

Technische Anforderung 4.1.4 *Die Bestellung des Cryptomaterial soll übers Intranet erfolgen. Die Bestellung soll in gesicherten Umgebung ablaufen, d.h. sie soll über eine HTTPS Seite erfolgen. Das dazu benötigte Serverzertifikat soll von der eingesetzten CA ausgestellt werden. Damit es keine Sicherheitswarnung gibt, muss das Rootzertifikat und das Ausstellerzertifikat an die Clients verteilt und als vertrauenswürdig gesetzt werden.*

Technische Anforderung 4.1.5 *Da die Möglichkeit der Benutzerüberprüfung mittels Microsoft integrated Authentication gelöst werden kann, ist eine Benutzerauthentifikation mit der zusätzlichen Abfrage des globalen Adressbuches mit Hilfe des LDAP Protokolls erwünscht. Da durch die Abfrage des globalen Adressbuches mittels LDAP*

auch die Benutzerdaten abgefragt werden können, wodurch eine einfache Autorisierung ebenfalls technisch lösbar ist, sollte dies auch eingesetzt werden.

In den organisatorischen Anforderungen wurde erwähnt, dass jeder der einen gültigen Eintrag im globalen Adressbuch hat, berechtigt ist, Cryptomaterial anzufordern. Weil eine autorisierte Onlinebestellung mit den beschriebenen technischen Möglichkeiten möglich ist, soll die Bestellung unter Anwendung dieser Möglichkeiten erfolgen. Dadurch können manuelle Eingaben und die daraus resultierenden Fehler eliminiert werden.

Technische Anforderung 4.1.6 *Der Besteller soll aber bestätigen, dass die angezeigten Daten, die im Hintergrund aus dem globalen Adressbuch geholt wurden, korrekt und zutreffend sind. Nach der Bestätigung soll der Besteller das Cryptomaterial und Importpasswort auf getrennten aber sicheren Wegen erhalten.*

Da bisher für Emailverschlüsselung und Emailsignatur dasselbe Cryptomaterial genommen wurde, kam das PGP Schlüsselpaar auf CD gebrannt mit der unternehmensinternen Hauspost und der CD Brief mit der gelben Post.

Technische Anforderung 4.1.7 *Die Verteilung soll auch wie im Anwendungsfall für Emailverschlüsselung, auf Verteilung übers Intranet umgestellt werden. Die Verteilung soll in gesicherter Umgebung (HTTPS) geschehen. Die Zieladresse, wo das Zertifikat erhältlich ist, soll nur einmal und nach erfolgreicher Autorisierung und Authentifizierung aufgerufen werden können. Wie die Zieladresse zu dem Besteller gelangt, ist noch zu klären. Da ein vollautomatisierter Import von Cryptomaterial nicht erwünscht ist, da dem Anwender nichts unterschoben werden soll, muss dem Besteller ein Importpasswort bzw. eine Import-PIN mitgeteilt werden. Das Importpasswort muss dem Besteller auf sicherem Weg mitgeteilt werden.*

Wenn die Mitarbeiter nur untereinander die Emailverschlüsselung nutzen, spricht man von einer geschlossenen Gruppe. Eine Lösung dafür wäre einfacher, da sie nur eine firmeninterne Lösung und Infrastruktur erfordert. Da aber ein mittelständisches Unternehmen meistens mit Geschäftspartnern kommuniziert, müssen die Geschäftspartner in den Anwendungsfall für Emailverschlüselung miteinbezogen werden. Dabei ist die entscheidende Frage, wer für die Geschäftspartner das Cryptomaterial zur Verfügung stellt. In unserem Fall sollen die Geschäftspartner selber Cryptomaterial besorgen. Sie werden aus Haftungsgründen nicht mit Cryptomaterial versorgt werden.
In userem Fall wird, davon ausgegangen, dass der Geschäftspartner Cryptomaterial hat und es auch verwenden kann.

Technische Anforderung 4.1.8 *In dem Fall muss die unternehmensinterne Infrastruktur mit speziellen Schnittstellen versehen werden, die von den Geschäftspartnern benutzt werden kann. Somit wäre die Öffnung der geschlossnenen Gruppe gemacht. Die offene Gruppe stellt weitergehende Anforderungen an die Infrastruktur die gut überlegt und geplant werden müssen. Bei einer reinen PGP Infrastruktur benötigt man nur einen PGP Keyserver von außen erreichbar machen. Da aber die Forderung der Unterstützung des S/MIME Standards besteht, der auch andere Infrastruktur benötigt, muss zusätzliche Infrastruktur geschaffen werden, die sowohl von den Mitarbeitern als auch von den Geschäftspartnern benutzt werden kann.*

Technische Anforderung 4.1.9 *Ziel ist es die Infrastruktur so aufzubauen, dass sie möglichst beide Standards unterstüzt und für beide Benutzergruppen auf verschiedene Weise verwendbar ist. Auf der Serverseite benötigt man eine Struktur oder einen Server, die oder der die Cryptomaterialien liefert. Auf der Clientseite soll eine Software zur Verwendung kommen, die mit beiden Cryptomaterialien arbeiten kann. Dabei soll es keinen Unterschied machen, welches Cryptomaterial zur Verschlüsselung verwendet werden wird. Die Clientsoftware soll automatisch die Infrastruktur nach Empfängerschlüssel suchen, den Schlüssel der Empfängeradresse zuordnen und die entsprechende Email generieren können.*

Technische Anforderung 4.1.10 *Bei der Emailverschlüsselung soll die zu verschlüsselnde Email mit mehreren Empfängern an alle Empfänger und an den Absender verschlüsselt werden. Wenn es bei der Verschlüsselung verschiedene Standards zum Einsatz kommen, sollen zwei Emails, eine mit PGP und eine mit S/MIME generiert werden. Der Hintergrund ist, dass bei dem Unternehmen Empfängerlisten verwendet werden. Diese Empfängerlisten machen keinen Unterschied, ob der Empfänger einen öffentlichen Schlüssel hat oder nicht bzw. was für einen Schlüssel der Empfänger hat.*

Technische Anforderung 4.1.11 *Die zum Einsatz kommende Clientsoftware soll die vorhandenen verschlüsselten Materialien weiterhin entschlüsseln können und die vorhandenen Schlüsselmaterialien sollen ebenfalls weiter genutzt werden können. Da die ganze vorhandene Infrastruktur aus Microsoft Produkten besteht, soll die angestrebte Lösung entweder auf Microsoft Produkten basieren oder zumindest in Microsoft Produktumfeld integrierbar sein und mit Microsoft Produkten zusammenarbeiten.*

Technische Anforderung 4.1.12 *Eine Unterstützung für das nächste Microsoftbetriebssystem soll vom Hersteller zugesichert sein.*

4.1.3 Gewährleistung der Interoperabilität

Bei der Interoperabilität handelt es sich um die Fähigkeit der Zusammenarbeit von verschiedenen Systemen bzw. Techniken. Dazu ist in der Regel die Verwendung gemeinsamer Standards notwendig. Diese Voraussetzung ist bei einer Lösung für eine geschlossene Gruppe gegeben.
Bei der Interoperabilität für offene Gruppen geht es um die Fähigkeit unabhängiger, heterogener Systeme, die möglichst nahtlos zusammen arbeiten sollen, um Informationen auf effiziente und verwertbare Art und Weise auszutauschen bzw. dem Benutzer zur Verfügung zu stellen, ohne dass dazu gesonderte Absprachen zwischen den Systemen notwendig sind. Die Interoperabilität muss also auf Anwendungsebene garantiert werden. Deshalb ist die Interoperabilität zu gewährleisten zwischen:

dem alten und neuen System, d.h. vorhandene verschlüsselte Materialien sollen weiterhin gelesen werden und vorhandenes Schlüsselmaterial soll mit dem neuen System ebenfalls verwendet werden können

der neuen und der alten Clientsoftware d.h. vorhandene verschlüsselte Materialien sollen weiterhin gelesen werden und vorhandenes Schlüsselmaterial soll mit dem neuen System ebenfalls verwendet werden können

der alten und der neuen Serveranwedung d.h. sie müssen mit den vorhandenen Verschlüsselungsmaterialien arbeiten können

der neuen Clientanwendung mit den Verschlüsselungsmaterialien der vorhandenen Geschäftspartner d.h. die Emailverschlüsselung soll mit dem Verschlüsselungsmaterial der Geschäftspartner weiterhin funktionieren. Dabei soll überlegt werden, ob eine neue Lösung für Anerkennung der PGP Schlüssel der Geschäftspartner erforderlich ist.

der Infrastruktur der Geschäftspartner und der eigenen Infrastruktur, d.h. im Fall von PGP Verschlüsselung kann das Unternehmen auf den PGP Keyserver des Geschäftspartners und umgekehrt zugreifen. Im Fall von S/MIME Verschlüsselung müssen die Zertifikate bzw. die Zertifikatssperrlisten erreichbar sein. Dies erfordert spezielle Netzeinstellungen.

Einbindung vorhandener Strukturen

Die Einbindung vorhandener Infrastruktur ist erforderlich, da einige Datenbasen jedem größeren Unternehmen bereits existieren. Die Anzahl dieser Datenbasen soll nicht noch vergrößert werden, da die meisten benötigten Daten in mindestens einer der Datenbasen auffindbar sind.
Als zentrale Informationsquelle kann das Active Direcoty genommen werden. Das bietet sich sogar wegen der standardisierten LDAP Schnittstelle an.
Die ganze Emailinfrastruktur basiert auf Microsoft Produkten, die nicht (einfach) austauschbar sind, weshalb die neue Lösung unbedingt mit Microsoft Produkten zusammenarbeiten soll. Dabei ist sowohl an Mailserver (Exchange Server) als auch an die Mailclients (Outlook) gedacht. Es ist aus heutiger Sicht wichtig, dass die Lösung auch die zukünftigen Microsoft Produkte unterstützen wird.

4.2 Anforderungen an die Emailsignatur

Die Emailsignatur wurde bisher auf PGP-Basis gelöst. Nun soll eine zeitgemäße Lösung für die Unterstützung beider Standards gefunden werden.

4.2.1 Organisatorische Anforderungen

Organisatorische Anforderung 4.2.1 *Im Prinzip soll jeder, der an der Emailverschlüsselung teilnimmt, auch Emailsignatur nutzen können. D.h. jeder darf und kann nur für sich ein Signaturzertifkat bestellen. Ein Signaturzertifikat soll nicht wiederherstellungsfähig sein, d.h. eine zentrale Sicherung der Signaturzertifikate ist nicht erwünscht. Wenn ein Mitarbeiter eine Wiederbereitstellung des eigenen Signaturzertifikats anfordert, soll ein neues Zertifikat mit neuem Schlüssel ausgestellt werden. Eine Entkoppelung von dem Schlüsselmaterial der Emailverschlüsselung ist an dieser Stelle erwünscht.*

Organisatorische Anforderung 4.2.2 *Es soll nun sowohl PGP als auch S/MIME Emailsignatur möglich sein.*

Anforderungen an die Generierung von Cryptomaterial zur Emailsignatur

Organisatorische Anforderung 4.2.3 *Die Generierung von Signaturzertifikaten soll ohne manuellen Eingriff passieren. Der Anwender soll keine Daten angeben müssen.*

Der Sicherheitsadministrator soll auf den Generierungsprozess keinen Einfluss nehmen können.

Organisatorische Anforderung 4.2.4 *Die Benutzerauthentifikation und Autorisierung soll automatisch nach dem Motto geschehen: wer in dem globalen Adressbuch einen gültigen und vollständigen Eintrag hat, darf bestellen.*

Anforderungen an die Verteilung von Cryptomaterial zur Emailsignatur

Da bisher kein separater Signaturschlüssel vorhanden war, ist die Verteilung eines Signaturschlüssels eine neue Anforderung.

Organisatorische Anforderung 4.2.5 *Die Verteilung von Signaturzertifikaten soll möglichst ohne manuellen Eingriff passieren. Die Passwort- oder PIN-Eingabe läßt sich in der Regel nicht umgehen. Es soll aber dem Anwender die Möglichkeit des Zertifikatsexports verwehrt werden.*

Organisatorische Anforderung 4.2.6 *Die Verteilung des Signaturschlüssels bzw. Zertifikats soll ohne Datenträger, aber in sicherer Umgebung erfolgen.*

4.2.2 Technische Anforderungen

Im Signaturgesetz (SigG) und in der Verordnung zum Signaturgesetz (SigV) werden die elektronischen Signaturen selbst und insbesondere die Anforderungen an elektronische Signaturen und Zertifizierungsdienstanbieter (ZDA) definiert. Die Rahmenbedingungen jedoch, wann welche elektronische Signatur verwendet werden kann oder muss, werden nicht im Signaturgesetz definiert, sondern beruhen im wesentlichen auf dem Bürgerlichen Gesetzbuch (BGB) und anderen Gesetzen sowie Rechts- und Verwaltungsverordnungen. Eine ausführlichere Beschreibung der digitalen Signatur steht im Abschnitt 2.3.2. Deshalb werden weder die Auflagen noch die Gültigkeit der digitalen Signatur hier beschrieben. Wie man es schon dort sehen konnte, sind die Auflagen zur verwendung von rechtsgültigen Signaturen streng und mit hohen Kosten verbunden, weshalb darauf vorerst verzichtet wird.

Technische Anforderung 4.2.1 *Für die Emailsignatur soll keine qualifizierte Signatur verwendet werden, da es strenge Auflagen zu erfüllen sind.*

Weitere Details können aus [SLES05] entnommen werden.

Weil für eine qualifizierte Signatur strenge Auflagen gelten, soll eine qualifizierte Signatur zuerst nicht zum Einsatz kommen. Bisher wurde die Emailsignatur auf reiner PGP Basis gelöst, d.h. für die Emailverschlüsselung und für die Emailsignatur wurde dasselbe Cryptomaterial genommen.

Technische Anforderung 4.2.2 *Nun soll in der Zukunft sowohl X.509 als auch PGP Signatur möglich sein.*

In den Fachliteratur werden verschiedene Anforderungen an ein Signaturzertifikat gestellt, die nicht außer Acht gelassen werden dürfen.

Technische Anforderung 4.2.3 *Eine zentrale Sicherung der Signaturzertifikate ist nicht erwünscht.*

4.2.3 Anforderungen an das Signaturmaterial

Die Eigenschaften eines PGP Schlüssels in Hinsicht auf die Verwendung lassen sich nicht einstellen. Dagegen lässt sich ein Signaturzertifikat auf X.509 Standard basierend genau definieren, wofür es eingesetzt werden kann.

Technische Anforderung 4.2.4 *Das Zertifikat soll folgende Informationen beinhalten:*

1. *Mitarbeitername (Vor- und Nachname)*
2. *Mitarbeiter Emailadresse*
3. *Unternehmensname*

Technische Anforderungen an die Verteilung

Da bisher für Emailverschlüsselung und Emailsignatur dasselbe Cryptomaterial genommen wurde, kam das PGP Schlüsselpaar auf CD gebrannt mit der unternehmensinternen Hauspost und der CD Brief mit der gelben Post.

Technische Anforderung 4.2.5 *Die Verteilung soll auch wie im Anwendungsfall für Emailverschlüsselung, auf Verteilung über Intranet umgestellt werden. Die Verteilung soll in gesicherter Umgebung (HTTPS) geschehen. Die Zieladresse, wo das Zertifikat erhältlich ist, soll nur einmal und nach erfolgreicher Autorisierung und Authentifizeirung aufgerufen werden können.*

4.3 Anforderungen an die Dateiverschlüsselung

Bisher wurde dasselbe Schlüsselmaterial für die Dateiverschlüsselung wie für die Emailverschlüsselung verwendet. Diese hat sich bewehrt, weshalb die neue Lösung auch mit demselben Schlüsselmaterial arbeiten soll. Deshalb gelten die Anforderungen der Emailverschlüsselung auch für das Schlüsselmaterial der Dateiverschlüsselung. Es gibt ein paar zusätzliche Anforderungen, die hier definiert werden:

Organisatorische Anforderung 4.3.1 *Die Dateiverschlüsselung muss schlüsselbasiert erfolgen, damit eine Wiederherstellung jederzeit möglich ist, falls die verschlüsselte Datei selber nicht beschädigt ist.*

Organisatorische Anforderung 4.3.2 *Falls der Verschlüsselungsschlüssel verloren geht, soll dieser mit der Wiederbereitstellung wieder beschaffen werden können.*

Organisatorische Anforderung 4.3.3 *Zur Dateiverschlüsselung soll dasselbe Cryptomaterial wie es zur Emailverschlüsselung verwendet wird, benutzt werden.*

Technische Anforderung 4.3.1 *Die neue Software soll denselben Schlüsselspeicher verwenden wie die Software für die Emailverschlüsselung, damit der Anwender sein Schlüsselmaterial nicht nochmal importieren muss.*

4.4 Anforderungen an die Benutzerauthentifizierung

4.4.1 Organisatorische Anforderungen

Organisatorische Anforderung 4.4.1 *In der Regel soll jeder Mitarbeiter berechtigt sein, sich ein Authentifizierungszertifikat zu bestellen. Es muss aber zwischen Mitarbeiter, der direkt bei dem Unternehmen angestellt sind, und den externen Mitarbeitern, die über ein Geschäftspartner bei dem Unternehmen tätig sind, differenziert werden.*

Organisatorische Anforderung 4.4.2 *Nur Mitarbeiter (d.h. Angestellten) des Unternehmens sollen für sich ein Authentifizierungszertifikat bestellen zu können.*

4.4.2 Technische Anforderungen

Die technische Anforderungen ergeben sich aus den Eigenschaften der zurzeit eingesetzten Zertifikaten und aus der Möglichkeiten der X.509 Standard [RFC2459].

Technische Anforderung 4.4.1 *Die genaue Vorgaben für ein Benutzauthetifikationszertifikat beinhaltet die Tabelle 4.5.*

Organisatorische Anforderung 4.4.3 *Mit dem Zertifikat der eigenen PKI soll die zertifikatsbasierte Anmeldung zu den Intranetapplikationen funktionieren. Es soll auf dem Client ausser dem Zertifikat nichts geändert werden. Falls es dennoch erforderlich wäre, soll die Änderung mittels SMS und Windows Policy gesetzt werden können.*

4.5 Zusammenfassung der Anforderungen

Wenn für jeden grundlegenden Anwendungsfall zwei Cryptomaterialien (ein für PGP und ein für X.509) erwünscht sind, müssen die Schlüsselinhaber nach der Tabelle 4.2 mit 5 verschiedenen Cryptomaterialien arbeiten. Obwohl die Software heutzutage einige Erleichterung bietet, müssen die Schlüsselinhaber die Cryptomaterialien und deren Zweck kennen. Aus diesem Grund versucht man so viele Anwendungsfälle wie möglich und sinnvoll mit einem Crytpomaterial abzudecken. Aus dieser Überlegung ergibt sich, dass für Authentifizierung und Signatur ein X.509 Zertifikat und für Emailverschlüsselung ein PGP Schlüssel und ein X.509-S/MIME Zertifikat verwendet werden sollte. Heutzutage müssen die meisten mittelständischen Unternehmen sowohl PGP als auch S/MIME unterstützen können. Einige Geschäftspartner verwenden S/MIME, einige andere wiederum PGP. Sowohl PGP als auch S/MIME benötigen eine Infrastruktur. Eine Infrastruktur für die PGP Lösung ist bereits vorhanden. Die Infrastruktur ist funktionsfähig, aber auf lange Sicht nicht zukunftsfähig. Es muss zwar auch der PGP Standard unterstützt werden, es muss aber untersucht werden, ob und wie die

vorhandene Infrastruktur in eine neue überführt oder integriert werden kann. Die Anforderungen an die Schlüsselmaterialien sind in der Tabelle 4.6 zusammengefasst.

Anforderung	Verschlüsselung	
	PGP	X.509 (S/MIME)
Backup / Recovery	erforderlich	erforderlich
Schlüssellänge	empfohlen mind. 1024 bit	empfohlen mind. 1024 bit
Schlüsselalgorithmus	RSA	RSA
Integration von Mitarbeiternamen	möglich und erwünscht	möglich und erwünscht
Integration von Emailadresse des Mitarbeiters	möglich und erwünscht	möglich und erwünscht
Integration von Mitarbeiter Logon-Name	nicht möglich und nicht erwünscht	möglich aber nicht erwünscht
Integration von Mitarbeiter GID	nicht möglich und nicht erwünscht	möglich aber nicht erwünscht
Schlüssel- bzw Zertifikatslebensdauer	empfohlen 2 Jahre	empfohlen 2 Jahre

Tabelle 4.4: Anforderung an die Schlüssel und Zertifikate für Emailverschlüsselung

X.509 Authentifizierungszertifikat	
Schlüssellänge	1024 Bit
Schlüsselalgoritmus	RSA
Zertifikatsverwendungszweck (Key Usage)	Key Encipherment Data Encipherment
erweiterter Zertifikatsverwendungszweck (Extended Key Usage)	Client Authentication
Subject	O = [Name des Unternehmens] CN = [Mitarbeitername] Email = [Emailadresse des Mitarbeiters] 1.3.6.1.4.1.1201.1.1.2.2.75 = [ID des Mitarbeiters]
Subject Alternativ Name (SAN)	Unified Principal Name (UPN) [Mitarbeitername]@[Unternehmens-Domäne]
Lebensdauer	1 Jahr

Tabelle 4.5: Anforderung an das Benutzerauthentifizierungszertifikat

	Verschlüsselung	Signatur	Authentifizierung
Backup/Recovery	erforderlich	nicht erwünscht	nicht erwünscht
Schlüssellänge	empfohlen mind. 1024 bit	empfohlen mind. 1024 bit	empfohlen mind. 1024 bit
Schlüsselalgorithmus	RSA	RSA	RSA
Schlüssel- bzw. Zertifikatstyp	PGP und X.509 möglich und erwünscht	PGP und X.509 möglich, erwünscht ist X.509	X.509 möglich und erwünscht
Integration von Mitarbeitername	möglich und erwünscht	möglich und erwünscht	möglich und erwünscht
Integration von Mitarbeiter-Emailadresse	möglich und erwünscht	möglich und erwünscht	möglich aber nicht erwünscht
Integration von Mitarbeiter Logon-Name	nicht möglich und nicht erwünscht	nicht erforderlich	möglich und erwünscht
Integration von Mitarbeiter ID	nicht möglich und nicht erwünscht	nicht erforderlich	möglich und erwünscht
Schlüssel- bzw. Zertifikats-Lebensdauer	empfohlen 2 Jahre	empfohlen 1 Jahr	empfohlen 1 Jahr

Tabelle 4.6: Anforderung an die Schlüssel- und Zertifikate

Kapitel 5

Umsetzungsmöglichkeiten

In Abschnitt 3 wurden die vorhandenen Anwendungsfälle beschrieben. Weil die vorhandene Lösung nicht zufriedenstellend ist, wird nach neuen Möglichkeiten gesucht. Die neue Lösung soll die beschriebene Anwendungsfälle abdecken. Im diesem Kapitel werden zuerst die allgemeine Ansätze erläutert, dann wird auf die Möglichkeiten für die Anwendungsfälle eingegangen.

5.1 Umsetzungsmöglichkeiten im Allgemeinen

Es gibt die drei grundlegende Möglichkeiten, die unterschiedliche Kosten verursachen:

- Ausgelagerte Lösung (Out-Sourced-Solution)
- Die verteilte Lösung
- Eigene Lösung (In-House-Solution)

Obwohl die erste Lösung meistens als zu teuerer und die zweite Lösung als Ideal angesehen wird, entpuppt sich eine ausgelagerte Lösung auf langer Sicht oft teuerer als eine eigene. Der dritte Ansatz erfordert eine lange und genaue Planungsphase, damit die Schnittstellen und Zuständigkeiten geklärt und definiert werden.

5.1.1 Die ausgelagerte Lösung

Bei der ausgelagerten Lösung können PKI Dienste abonniert oder nur Cryptomaterial bestellt werden. Die letztere Möglichkeit kann aber auch als Dienst gesehen werden. In dem Fall wird ein CA Dienst benutzt. Es ist aber egal welche Variante genutzt wird, ein Datenaustausch muss auf jeden Fall stattfinden. Welche Daten ausgetauscht werden müssen, hängt von dem Dienstleister, dessen Verwaltung und dessen Cryptomaterial ab. In jedem Cryptomaterial können und sollen in der Regel personbezogene Daten gespeichert werden. Falls es sich bei dem Cryptomaterial um ein Material für Server oder Service handelt, ist es nicht erforderlich, ergibt aber durchaus einen Sinn, eine Emailadresse in das Cryptomaterial zu integrieren.
Bei diesem Ansatz gibt es zwei verschiedene Realisierungen:

Push-Model: bei diesem Modell liefert das Unternehmen dem Dienstleister die Daten, die die Grundlage für die Verwaltung und Erstellung von Cryptomaterialien dienen. Bei dieser Variante kann man auch von Bestellung sprechen, weil der Dienstanbieter nur durch Aufforderung aktiv wird.

Pull-Model bei diesem Modell holt regelmäßig der Dienstanbieter die Daten von einem vereinbarten Ort in vereinbarten Zeitintervallen.

Abgesehen von diesen Realisierungsmöglichkeiten können serverseitige Teile einer PKI abonniert werden. Welche CA Dienste im welchem Umfang abonniert werden können, hängt von dem Dienstanbieter ab. Dienste wie Zertifikatsdienst, Registrationsdienst, Verzeichnisdienst (Veröffentlichung der öffentlichen Zertifikate) und Veröffentlichung der Sperrlisten (CRL - **C**ertificate **R**evocation **L**ist) sind die Basisdienste. Andere Dienste sind aber auch möglich. Obwohl diese Elemente einer PKI sind, liefern sie aber nur die serverseitige Lösung. Eine PKI wird erst durch die Endeinheiten (End-Entities) zu einem Ganzen. Die Endeinheiten müssen in die Betrachtung miteinbezogen werden. Man kann höchstens auf die mit den Endeinheiten mitgelieferten Lösungen ausweichen. D. h. im Fall der Emailverschlüsselung bedeutet dies die Verwendung der Microsoft Outlook internen S/MIME Verschlüsselung. Bei der Verwendung von PGP ist man auf eine Zusatzsoftware angewiesen. Der Vorteil der ausgelagerten Lösung ist, dass keine serverseitige Hardware und Software erforderlich ist. Als Fazit kann man folgendes feststellen:
Eine Art Voll-PKI auf Dienstbasis ist bisher nicht bekannt. Das heißt nicht, dass es unmöglich wäre. Eine Möglichkeit wäre der Einsatz von Webapplikationen. Nach diesem Ansatz würde die gesamte Software auf Webservice basierend genutzt. Dabei würde aber die ganze Applikationsumgebung auf dem Server ablaufen. Die Betrachtung dieses Ansatzes wäre an dieser Stelle zu umfangreich, weshalb darauf verzichtet wird.
Die ausgelagerte Lösung erfordert eine genaue Definition der Dienstzugangpunkte (Service Access Point). Der Dienstanbieter benötigt Daten um das angefordertes Cryptomaterial erzeugen zu können. Der Dienstnehmer möchte die erzeugten Materialien auch erhalten. Diese beiden Schritte erfordern einen gegenseitigen Datenaustausch. Dabei soll auch geregelt werden, ob die Bestellungen direkt zum Dienstanbieter gesendet werden, oder ob sie zuerst autorisiert werden müssen. Diese Aufgabe könnte ein intelligenter Proxy übernehmen. Dieser Proxy könnte die nicht berechtigten Bestellungen ausfiltern und die autorisierten an den Dienstanbieter weiterleiten.
Die Listenführung der Bestellungen ist in dem meisten Unternehmen für statistische und interne Abrechnungszwecke erforderlich. Diese Aufgabe könnte der Proxy auch übernehmen.
Die Verfügbarkeit des abonnierten PKI Dienstes muss auch geregelt werden. Dies erfordert aber nicht nur eine prozentuelle Zusicherung, sondern die Regelung des maximalen Ausfalls im Stück. Diese Problematik führt auch zu der Problematik der Performance, wie viele Anforderungen innerhalb eines bestimmten Zeitraumes gestellt werden können.
Zuletzt, aber nicht zu vernachlässigen sind die Sicherheitsfragen. Die Dienstnutzung soll in sicherer Umgebung erfolgen. Bei der Dienstnutzung geht es nicht nur um die Ausstellung von Schlüsselmaterialien, sondern auch um die Prüfung der ausgestellten Materialien bzw. um die Führung eines Verzeichnisdienstes, um die öffentlichen Materialien verfügbar zu machen.
Aus Interoperabilitätsgründen muss die vorhandene Infrastruktur weiter betrieben werden. Nach diesem Ansatz müsste diese vorhandene Infrastruktur auch ausgelagert wer-

den oder ein entsprecheder Dienst abonniert werden. Das würde eine nicht zu unterschätzende Änderung der Client- und Netzwerklandschaft mit sich bringen. Alle Clients müssen umkonfiguriert und die entsprechende Wege im Netzwerk müssen zu dem Dienstanbieter bidirektional geschaltet werden. Unter Umständen muss sogar neue Clientsoftware eingesetzt werden, wobei auf die Interoperabilität geachtet werden muss.
Zu diesen Anforderungen kommt noch die Unterstützung der Benutzer hinzu. Das muss zusätzlich eingerichtet und kommuniziert werden, damit die Benutzer wissen, an wen sie sich im Problemfall wenden können.
Es müssen unter anderem folgende Fragen geklärt und geregelt werden:

- Auf welche Informationen und über welche Wege darf der Dienstanbieter zugreifen?
- Welche Informationen dürfen dem Dienstanbieter geliefert werden?
- Wer darf die abonnierten Dienste administrieren?
- Über welche Wege erfolgt die Dienstadministration?
- Welches Material soll der Dienstanbieter liefern?
- In welcher Form soll das Material geliefert werden?
- An wen soll der Dienstanbieter liefern?
- Welche Verfügbarkeit wird von dem Dienstanbieter garantiert?
- Wer ist im Notfall zu benachrichtigen?
- Wer ist im Notfall handlungsberechtigt?

Diese Lösung ist für mittelständische und große Unternehmen langfristig kostspieliger. Es gibt inzwischen erste Praxisbeispiele, welche Kosten einzelnen Unternehmen bei der Einführung einer Public-Key-Infrastruktur entstanden sind: Über einen Zeitraum von fünf Jahren kommen bei 5 000 Nutzern gut 100 Dollar pro User [Mac98] zusammen. Andere Studien nennen zwischen 200 000 und 0,8 Millionen Euro [NC98] für die gleiche Anzahl von Zertifizierungen und den gleichen Zeitraum. Es muss dabei aber auch erwähnt werden, dass es bei dieser Lösung meistens um akkreditierte Dienste handelt.

Vorteile dieser Lösung:

+ Niedrige Startkosten
+ Keine Serverhardware notwendig
+ Keine Serversoftware notwendig
+ Akkreditierte Dienste
+ Kein Hardware- und Softwaresupport nötig
+ Je nach Anforderungen schneller Dienststart
+ Profitierung guter Kenntnisse des Dienstanbieters

Nachteile dieser Lösung:

- Schnittstellen müssen klar definiert werden

- Externer Zugriff bei Bestellung notwendig
  - Pull-Modell: Der Dienstanbieter holt sich die Daten regelmäßig vom Unternehmen (von einem bestimmten Ort)
  - Push-Modell: Der Dienstnutzer sendet die Daten dem Dienstanbieter
- Bestellvorgang muss sicher und komplett neu gestaltet werden
- Einige der Mitarbeiterdaten (mind. Name, Email etc.) müssen weitergegeben werden
- Je nach Konfiguration und Anforderung eine Zwischenstelle erforderlich
- Nicht kalkulierbare Kosten (die Kosten stehen in Relation zu der Anzahl der Mitarbeiter und Zertifikate)
- In der Regel werden nur X.509 Zertifikate unterstützt
- Unterstützung der Benutzer muss weiterhin gewährleistet werden
- Abhängigkeit von einem Dienstanbieter
- Wechsel des Dienstanbieters ist sehr schwierig
- Keine Gewährleistung der Kontinuität
- Freischaltung der Wege zum Dienstanbieter im Netzwerk erforderlich

Da das Unternehmen die sicherheitsrelevanten Lösungen nicht auslagern will, wird diese Variante nicht näher betrachtet.

5.1.2 Die verteilte Lösung

Bei dieser verteilten Lösung werden die Ansätze aus dem Abschnitt 5.1.1 übernommen und erweitert. Bei diesem Ansatz werden nur Teile einer PKI ausgelagert, z. B. die Generierung des Cryptomaterials. Das Problem bei diesem Ansatz ist die Verwaltung bzw. die Zusammenarbeit beider Lösungen. Dieser Ansatz erfordert entweder ein spezielles Verwaltungswerkzeug oder die zwei Lösungen werden separat verwaltet, was den Verwaltungsaufwand erhöht. Bei der verteilten Lösung gibt es auch mehrere Möglichkeiten. Manche Dienstleister erlauben, dass ein berechtigter Administrator für das Unternehmen über eine Verwaltungsoberfläche die Materialien des Unternehmens verwaltet. Manche Dienstleister generieren Cryptomaterialien anhand der erhaltenen Daten. In so einem Fall müssen die Daten für den Dienstleister in der Regel aufbereitet werden. Es ist im Prinzip egal wie die Materialien verwaltet werden, weil die verteilte Lösung in der Regel zusätzlichen Aufwand bedeutet.
Anhand der verschiedenen Anwendungsfälle aus Kapitel 3 wird ersichtlich, dass dieser Ansatz sich im Einsatz befindet. Weil der Dienstanbieter nicht zufriedenstellend und zuverlässig arbeitet und weil das Unternehmen über die technische Infrastruktur verfügt, wurde entschieden eine eigene Lösung zu erarbeiten.

Bewertung der verteilten Lösung:

+ Profitierung guter Kenntnisse des Dienstanbieters

+ Gewährleistung der Kontinuität
- Höhere Kosten als für die ausgelagerte Lösung
- Je nach Konfiguration und Anforderung ist eine Zwischenstelle erforderlich
- Hohe Administrationsaufwand durch die verteilten Dienste
- Unterstützung der Benutzer muss weiterhin gewährleistet werden
- Abhängigkeit von einem Dienstanbieter
- Ständige Kosten
- Wechsel des Dienstanbieters sehr schwierig

Weil die zentrale Verwaltung der Schlüssel bei diesem Ansatz schwierig bis nicht möglich ist, wird auf die nähere Betrachtung diesen Ansatzes verzichtet.

5.1.3 Die eigene Lösung

Wie bereits erwähnt, verfügt das Unternehmen über technische Strukturen und über eine eigene aber nicht zeitgemäße Lösung. Es muss eine Lösung für die Verwaltung und Weiterverwendbarkeit vorhandener Cryptomaterialien und verschlüsselter Materialien gefunden werden. Das übernimmt kein Dienstanbieter, weshalb nach einer eigenen Lösung gesucht wurde.
Es gibt immerhin weitere Lösungskategorien für die eigene Lösung: die Insellösung und der traditionelle PKI Ansatz.

Insellösung

Bei der Insellösung handelt es sich um eine Lösung, die nur einen Bereich (Anwendungsfall) abdeckt. Um aber alle Anwendnungsfälle abdecken zu können, muss eine Sammlung der Insellösungen erarbeitet werden. Die Zusammenarbeit mehrerer Inseln ist nicht einfach zu koordinieren, da diese Lösungem in der Regel als allein stehende Lösungen entwickelt wurden. Ein Beispiel für eine Insel(lösung) ist z.B. das Emailverschlüsselungs-Gateway.

Bewertung der Insellösung:

+ Gewährleistung der Kontinuität
+ Niedrige Folgekosten
+ Keine Abhängigkeit von einem Dienstanbieter
- Hohe Anfangskosten für Hardware, Software und Aneignung der Kenntnisse
- In der Regel lange Planungsphase
- Beratung in der Planungsphase in der Regel erforderlich
- Unterstützung der Benutzer muss weiterhin gewährleistet werden

- Zusammenarbeit mehrerer Produkte muss koordiniert werden, evtl. Anpassung der Software erforderlich

Traditioneller PKI Ansatz

Diese Lösung baut auf einer Server-Client Infrastruktur auf, wobei die Clients und die Server zwangsläufig nahtlos zusammenarbeiten. Bei diesem Ansatz muss zwischen PGP und X.509 PKI Infratsruktur differenziert werden. Während PGP keine aufwendige Infrastruktur benötigt, kann bei der X.509 PKI auf eine Infrastruktur nicht verzichtet werden. Das wurde im Abschnitt 3.1.1 beschrieben. Ein kurzes Vergleich befindet sich auch im Abschnitt 5.2.1.

Bewertung des traditionelles PKI Ansatzes

+ Gewährleistung der Kontinuität
+ Keine Zwischenstelle erforderlich
+ Niedrige folge Kosten
+ Keine Abhängigkeit von einem Dienstanbieter
- Hohe Anfangskosten (für Hardware, Software und Aneignung der Kenntnisse)
- In der Regel lange Planungsphase
- Beratung in der Planungsphase in der Regel erforderlich
- Unterstützung der Benutzer muss weiterhin gewährleistet werden

Da die gesuchte Lösung auf einer PKI aufbaut, soll zuerst eine PKI Infrastruktur im allgemeinen vorgestellt werden, um danach auf die einzelne Komponenten und Aufgaben Bezug nehmen zu können. Der nächste Abschnitt soll als eine Einführung in die PKI betrachtet werden. Obwohl der Trend zur Zeit stark dienstorientiert ist, muss untersucht werden, ob ein Dienstabonement als Lösung in Frage kommen kann. Zuerst soll aber die PKI an sich vorgestellt werden.

5.2 PKI im Allgemeinen

Bei einer PKI handelt es sich,wie schon die Bezeichnung sagt, um eine Infrastruktur. Eine PKI bildet eine Hilfsstruktur zu einer Public Key Cryptography. Mit Public Key Cryptography bezeichnet man ein Verschlüsselungsverfahren, das auf asymmetrischer Verschlüsselung basiert, und als solches ein Schlüsselpaar (öffentlicher Schlüssel und privater Schlüssel) verwendet.
Die Motivation zur Entwicklung einer PKI ist die automatisierte Schlüsselveröffentlichung, da die Verschlüsselung nur dann erwartungsgemäß funktioniert, wenn die Schlüssel auf einer zentralen vertraulichen Stelle abgelegt werden. Die Kommunikationspartner können die benötigten öffentlichen Schlüssel von dieser Stelle holen. Diese zentrale Stelle sorgt für die Aktualität der Schlüssel. Die Schlüsselvalidierung soll mit Hilfe dieser zentralen Komponente automatisiert erfolgen. Was die einzelnen Komponente einer PKI sind und wie sie zusammenarbeiten, werden im Weiteren beschrieben.

5.2.1 Unterschied zwischen PGP und X.509 PKI

Der Ansatz von PGP lehnt jede Art von zentraler Verwaltungsstelle ab. Der Ansatz von PGP basiert auf gegenseitigem Vertrauen. (Vergleiche mit Abschnitt 5.11.2) Im Prinzip funktioniert die PGP Verschlüsselung auch ohne zentrale Komponente abgesehen von dem Emailserver. Um aber die Schlüsselverteilung zu vereinfachen, wurde im PGP Bereich der so genannte Keyserver entwickelt, der als einzige zentrale Stelle in einer PGP PKI vorhanden ist. Der Keyserver speichert die öffentlichen Schlüssel und kann meistens übers Webinterface oder mit Hilfe einer PGP Software abgefragt werden. Die PGP Schlüssel könnnen auch in Verzeichnisdiensten gespeichert werden. Ein Verzeichnisdienst lässt sich mit Hilfe des LDAP Protokolls abfragen.
Die X.509 PKI Infratrsuktur ist etwas komplexer, weil sie mehrere Komponenten benötigt, die im nächsten Abschnitt beschrieben werden.

5.2.2 Standardkomponenten

Es gibt mehrere Ansätze aus welchen Komponenten eine PKI besteht. In dieser Diplomarbeit wird der Ansatz, den auch Abbildung 5.1 zeigt, verwendet. Die Abbildung wurde aus dem Opensource PKI Buch [SSX02] entnommen. Die Abbildung folgt dem Standard und den Empfehlungen der PKIX (http://www.ietf.org/html.charters/pkix-charter.html).

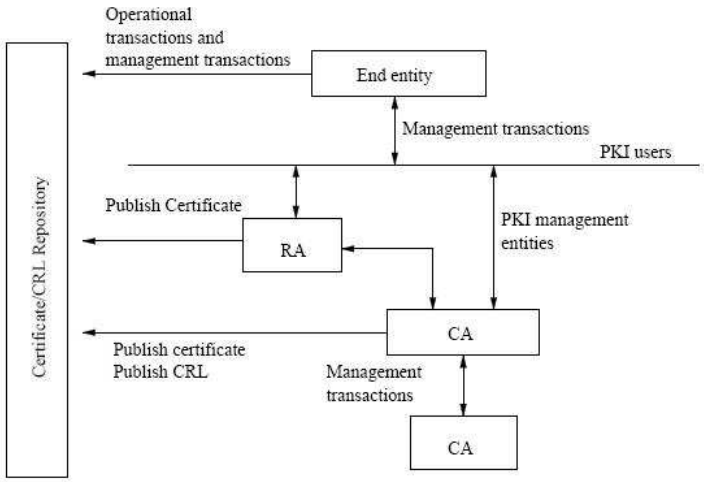

Abbildung 5.1: Funktionsschema einer PKI im allgemeinen (Quelle:[SSX02])

Endeinheit

Für Endeinheit wird in der Fachliteratur oft der englische Begriff End-Entity verwendet. Endeinheiten sind die Zertifikatsnehmer. Ein Zertifikatsnehmer kann ein Router, Server, Prozess oder ähnliches sein, vorausgesetzt, dass es anhand eines Eintrages im Zertifikatssubjekt identifiziert werden können.

Zertifizierungsstelle

In der Fachliteratur wird die Zertifizierungsstelle oft Certificate Autority, kurz CA genannt. Öffentliche Schlüssel werden in der Form von öffentlichen Zertifikaten verteilt. Die CA bildet das Grundgerüst einer PKI, denn sie ist die einzige Komponente einer PKI, die öffentliche Zertifikate signieren oder ggf. Zertifikate erstellen kann.
Die CA ist ebenfalls für das Erstellen einer CRL (**C**ertificate **R**evocation **L**ist - Zertifikats-Sperrliste) verantwortlich. Eine Zertifizierungsstelle (CA) stellt digitale Bestätigungen (Zertifikate) aus. In ihnen bestätigt die Zertifizierungsstelle mit ihrer digitalen Signatur die Bindung eines bestimmten Public Keys (und damit implizit auch des zugehörigen Private-Keys) an eine Person, Institution oder Instanz (die beispielsweise auch ein Rechner sein kann), die in dem Zertifikat namentlich benannt wird. Die Zertifizierungsstelle bietet damit also einen Dienst ganz ähnlich einer notariellen Beglaubigung dafür, dass ein bestimmter Public Key und eine bestimmte Person zusammengehören. Es wird dadurch eine Reduktion der Komplexität möglich: statt vieler individueller Public Keys muss nur noch der öffentliche Schlüssel der Zertifizierungsstelle authentisch verteilt werden. Liegt er einer Person vor, kann diese mit seiner Hilfe die digitalen Unterschriften der Zertifizierungsstelle unter jedem der von ihr ausgestellten Zertifikate überprüfen und sich damit der Echtheit und Unverfälschtheit aller von ihr ausgestellten Zertifikate vergewissern. Stimmt die Unterschrift, dann kann aus dem betreffenden Zertifikat der öffentliche Schlüssel der darin genannten Person abgelesen werden. Allerdings muss man dafür dem Aussteller des Zertifikates, also der betreffenden CA, dahingehend vertrauen, dass sie immer korrekt zertifiziert und keine falschen Bestätigungen ausstellt. Sehr wichtig für die Arbeit einer Zertifizierungsstelle ist also ihre Glaubwürdigkeit bei möglichst vielen Nutzern. Nur wenn die Anwender bereit sind, sich auf die Bestätigung eines fremden öffentlichen Schlüssels durch die betreffende CA zu verlassen, hat diese eine Arbeitsgrundlage. Also muss es im Interesse der Zertifizierungsstelle sein, alles zu tun, um sich ihre entsprechende Reputation zu erhalten oder eine solche gegebenenfalls auch erst zu erarbeiten. Im einzelnen lässt sich der Vorgang der Public-Key-Zertifizierung durch eine Zertifizierungsstelle in die folgenden Teilschritte gliedern:

- Erzeugung eines Schlüsselpaares (beim Zertifikatnehmer, in der Registrierungs- oder Zertifizierungsstelle)
- Registrierung und Identifizierung des Zertifikatnehmers direkt bei der CA oder in einer Außenstelle von ihr (Registrierungsstelle, Registration Authority, RA), gegebenenfalls erfolgt dort auch die Übergabe einer Kopie des öffentlichen Schlüssels vom Zertifikatnehmer an die CA / RA
- gegebenenfalls: Übermittlung der Daten aus dem Zertifizierungsantrag von der RA an die Zertifizierungsstelle Zertifizierung des Schlüssels (sofern alle Voraussetzungen dafür wie Schlüssellänge, eindeutiger Name des Schlüsselinhabers usw., erfüllt sind)
- Aushändigung oder Übermittlung des Zertifikates an den Schlüsselinhaber
- Veröffentlichung des Zertifikates durch die Zertifizierungsstelle mittels geeigneter Verzeichnis- oder Verteildienste.

Hinzu kommen können später noch Dienste wie die Re-Zertifizierung eines Schlüssels, wenn ein bereits erteiltes Zertifikat abzulaufen droht, oder auch die Sperrung des Zertifikates, wenn entsprechende Gründe dafür vorliegen. Nicht jede Zertifizierungsstelle muss alle diese Tätigkeitsfelder abdecken; es ist gut möglich, dass sich manche Stellen auf einen Teil dieser Aufgaben beschränken und sie andere Teilaufgaben, beispielsweise den Betrieb eines Verzeichnisdienstes, an Partnerunternehmen oder andere Anbieter delegieren. Die Zertifizierung von Schlüsseln als zentraler Tätigkeitsbereich einer Zertifizierungsstelle wird allerdings immer dazugehören. Einrichtungen, die nicht nur Zertifizierungsdienste anbieten, sondern die beispielsweise zusätzlich auch Schlüssel für Nutzer generieren, Sicherungskopien vertraulicher Schlüssel verwahren oder Zeitstempeldienste offerieren, werden häufig auch als Trustcenter oder auch als Trusted Third Party (TTP), also als ein „vertrauenswürdiger Dritter“ bezeichnet. Ihnen muss, im Unterschied zu einer reinen Zertifizierungsstelle, auch der Zertifikatnehmer, also derjenige – dessen Schlüssel zertifiziert wird – Vertrauen entgegenbringen, denn er muss sich darauf verlassen, dass das Trustcenter wie zugesichert nach der Schlüsselerzeugung und -aushändigung alle Spuren des vertraulichen Schlüssels vernichtet bzw. dass das Trustcenter die hinterlegte Sicherheitskopie des vertraulichen Schlüssels auch wirklich geheimhält. Um eine internationale Akzeptanz der Zertifikate zu erreichen, ist an ein Signieren des Root-Zertifikates der internen PKI durch eine international namhafte Zertifizierungsstelle (sogenanntes Root-Signing) zu denken (z.B. VeriSign, GlobalSign, ...). Damit wäre der gesicherte Nachrichtenaustausch mit externen Partnern problemloser möglich.

Registrationsstelle – RA - Registration Authority

Die (lokale) Registrierungsstelle ([L]RA) nimmt eine Schlüsselrolle in einer PKI ein. Diese Stelle haftet für die Richtigkeit der ausgestellten elektronischen Daten. Werden hier falsche Angaben registriert, so entspricht das einer fehlerhaften Personaldatenfeststellung die zur Ausgabe eines falschen Personalausweises führt. Zertifizierungshierarchien sehen zumeist vor, dass von den Zertifizierungsstellen mehrere Registrierungsstellen (RAs) betrieben werden können, um für die Nutzer den Weg zur Zertifizierungsstelle zu verkürzen. Zertifizierungswillige können ihren Zertifizierungsantrag statt bei der CA bei einer der RAs stellen, die dann auch gleich die Identitätsprüfung vornimmt. Bei der Entscheidung für oder gegen dezentrale Registrierungsstellen sollte abgewogen werden zwischen den Vorteilen durch die Nähe zum Benutzer und die leichtere Erreichbarkeit (Reisekosten) dieser Außenstellen der CA und den Nachteilen, die sich durch eine zu starke Aufsplittung ergeben (Mehrfacharbeit, Hardware-Ressourcen in der RA, Kommunikationskosten, ...). Der Mehraufwand zusätzlicher Registrierungsstellen sollte jedenfalls vom Management monitär bewertet werden. Potentielle RA-Standorte sind Außenstellen, die sehr weit von der Zentrale entfernt liegen, so dass es den dort Beschäftigten nicht zugemutet werden soll, für eine Zertifizierung einen längeren Anfahrtsweg oder eine längere Abwesenheit vom Arbeitsplatz in Kauf nehmen zu müssen. Eine gute Alternative zu fixen Registrierungsstellen sind mobile Registrierungsstellen, die zu verschiedenen Zeitpunkten (periodisch und/oder nach Bedarf) an die Standorte geschickt werden. Da für Registrierungsstellen geschultes Personal erforderlich ist, können mit derartigen Einrichtungen zur Auslastung des Personals durchaus Einsparungen erfolgen. Wenn die Nachfrage nach Zertifizierungsdiensten so stark zunimmt, dass sie selbst mit Registrierungsstellen an den Orten mit besonders großer Nachfrage kaum zu befriedigen ist, oder wenn aus anderen Gründen eine eigene Zer-

tifizierungsstelle an einem Standort betrieben werden soll, dann sollten so genannte nachgeordnete Zertifizierungsstellen (Sub- oder Intermediate-CAs) etabliert werden. Diese können dann eigenverantwortlich die Schlüssel ihrer Nutzer zertifizieren, stehen aber unter der Aufsicht der übergeordneten Zertifizierungsstelle und müssen sich an deren Richtlinien (Policy) halten. LRAs und Sub-CAs stellen eine Möglichkeit der Lastverteilung dar, erfordern aber auch einigen zusätzlichen Betreuungs-, Prüf- und Koordinationsaufwand von Seiten der CA.
Eine RA übernimmt Aufgaben des Identifikations Managements (IM). Das IM selber ist ein breites Gebiet. Ein Identity Management System besteht in der Regel aus vier Teilen:

- Repository
- Policies
- Identity Provider
- Policy Control

Repository ist eine Datenbasis mit einem Datenmodell, das die Identität beschreibt.

Policies regeln Verwendung und den Zugriff auf Daten.

Identity Provider ist für die primäre Authentifizierung zuständig, die eine Person mit einer gespeicherten Identität verknüpft.

Policy Control steuert den Zugriff und Nutzung von Informationen.

Innherhalb einer Public Key Infrastruktur ist ein Identifikationsmanagement von essenzieller Bedeutung [MI005]. Dabei soll nicht an der ersten Stelle an die Identitätsfeststellung gedacht werden, sondern an die richtige Zuordnung von Rechten an Personen bzw. Identitäten. Dazu ist eine geeignete Informationsdarstellung nötig. Dies kann man auf mehrere Arten Realisieren:

- Abbildung der Information in der CA Struktur
- Speicherung der Information in den Zertifikaten
- Informationen werden in einer externen Datenbasis gehalten

Die Identitätsüberprüfung bzw. der Datenabgleich kann Probleme verursachen, die von Unternehmensprozessen aufgefangen werden müssen.
Schritte:

- Firmenagehörige müssen sich bei der Einstellung sich identifizeiren (Personalausweis, Lohnsteuerkarte, Abschluß-Urkunden etc.).
- Die Firma muss diese Daten gut geschützt aufbewahren und mit spezieller Zugriffskontrolle versehen.
- Bei der Zertifikatsverteilung kann nur bedingt auf ein Teil dieser Daten zugegriffen werden

Die Registrationsstelle, deren Organisation und deren Aufgaben müssen gut durchdacht und beschrieben werden, weil die CA auf die Daten der Registrationsstelle zugreift und anhand dieser Daten die Zertifikate ausstellt.

Certificate Repository

In dem Zertifikatsrepository publiziert die ausstellende CA die öffentlichen Zertifikate und die Zertifikatssperrliste. Das Zertifikatsrepository dient zum Verteilen von Zertifikaten. Diese Aufgabe kann ein Verzeichnisdienst übernehmen oder die CA selber erledigen.

5.2.3 Andere in der Fachliteratur erwähnten Einheiten

Es gibt verschiedene Ansätze, die man in verschiedenen Literaturen findet. Diese folgen unterschiedlichen Ansätzen mit verschiedenem Aufbau und Komponenten einer PKI. In den kommenden Abschnitten werden diese anderen Komponenten kurz behaldelt.

Verzeichnisdienst – Directory Service

Directory Service als solcher ist kein Teil einer PKI, sondern ein Lösungsansatz. Ein Directory Service kann mehrere Aufgaben (Benutzerverwaltung, Certifacte Repository etc.) in einer PKI übernehmen. Vorteil eines Directory Services ist, dass mehrere Aufgaben an einer Stelle verwaltet werden können. Aus diesem Grund muss der Zugriff auf den Directory Service genau geregelt werden. Wer wie auf die Daten zugreifen kann und darf.
Ein weiterer wichtiger Punkt ist, wie die Daten in das Directory Service kommen. Dabei spielt nicht nur die Datenübertragung sondern auch die Authentizität und Integrität der Daten eine wesentliche Rolle. Man muss bei der Speicherung der Daten auch die Datenschutzgesetze beachten.

Certificate Policy

Zertifikatspolicy beschreibt die Zertifikate im Detail. Das heißt, wie ein Zertifikat aussieht, welche Informationen ein Zertifikat beinhalten soll und für welchen Zweck ein Zertifikat benutzt wird.

CPS - Certificate Practices Statement

Ein CPS beschreibt die Prozesse und operative Praxis einer PKI. Das heißt, in diesem Dokument wird der Zertifikatslebenszyklus von der Generierung bis zum Widerruf beschrieben.
Das CPS muss auch beschreiben, wie ein Authentifizierungsprozess ablaufen soll, bevor ein Endeinheit als validiert gilt.

5.3 Certificate Lifecycle Management

Das Certificate Lifecycle Management bildet die Grundlage für die Verwaltung von Cryptomaterialien. Das Certificate Lifecycele Management beschreibt den Zertifikats-

lebenszyklus mit allen Prozessen der Anwendungsfälle verbunden ist. Der Lebenszyklus besteht aus drei Phasen:

1. Initialisierung
2. Verwendung
3. Vernichtung

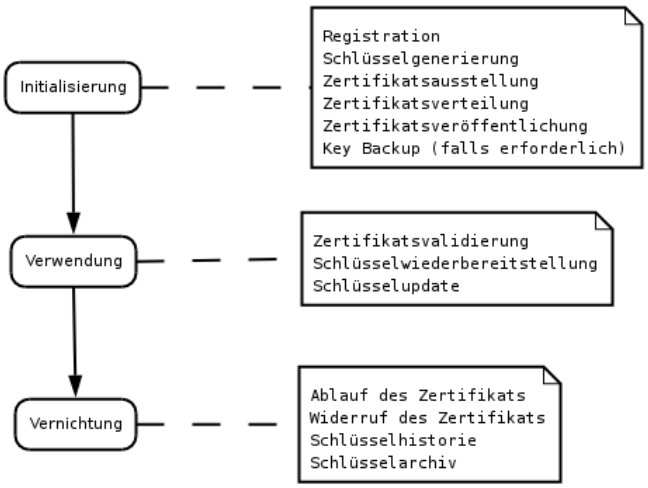

Abbildung 5.2: Lifecycle Management

Jede Phase besteht aus verschiedenen Teilprozessen.

5.3.1 Initialisierungsphase

Die **Initialisierung** besteht aus folgenden Teilprozessen:

Registration: da ein Zertifikat einem Endbenutzer zugeordnet wird, muss diese Zuordnung eindeutig erfolgen. Dies kann nur dann erfolgen, wenn der Endbenutzer vorher anhand bestimmter Daten identifiziert wird. Dies kann z.B. über persönliche Identitätsüberprüfung anhand eines Ausweises (z. B. Personalausweis) geschehen.

Schlüsselgenerierung: In jedem Zertifikat ist ein Schlüssel vorhanden. Dieser Schlüssel muss vorher erzeugt werden. Die Generierung kann entweder auf dem Client oder auf einer zentralen PKI Komponente (z.B. CA) erfolgen. Diese Betrachtung ist sehr wichtig und bietet die Grundlage für rege Debatten.

Zertifikatsausstellung: Der Schlüssel wird in einen sog. Umschlag integriert. Der Umschlag ist genau spezifiziert. Zusammen mit dem Schlüssel nennt man ihn Zertifikat.

Zertifikatsverteilung: Bei der Zertifikatsverteilung wird das erstellte Zertifikat dem registrierten Endanwender zur Verfügung gestellt.

Wie das Zertifikat zum Endanwender gelangt, ist von der Art der Schlüsselgenerierung abhängig. In der Regel kann es offline oder online erfolgen. Wenn die Schlüsselgenerierung auf dem Client (SmartCard, Browser etc.) erfolgt, verlässt der private Schlüssel den Client nicht, was höhere Sicherheit bietet. In diesem Fall kann aber keine Wiederbereitstellung oder Schlüsselbereitstellung an vertrauenswürdige Dritte (escrow) erfolgen.
Falls eine zentrale Komponente die Schlüsselgenerierung übernimmt, kann eine Wiederbereitstellung oder Schlüsselbereitstellung an vertrauenswürdige Dritte gelöst werden. Dies setzt aber ein Keybackup voraus. Dieser Ansatz hat einen Schwachpunkt: Wie gelangt der Schlüssel zum Endanwender? Das kann entweder offline oder online geschehen. Bei dem Offline-Weg wird das Material in der Regel nach einer Authentifizierung auf einem Datenträger ohne Verwendung von elektronischer Infrastruktur überreicht. Der Datenträger kann aber in fremde Hände geraten, weshalb das Material zusätzlich mit einem Initialpasswort gesichert werden muss. Dadurch wurde das Problem nur verschoben und aufgeteilt, da das Initialpasswort von dem Datenträger getrennt dem Endanwender mitgeteilt werden muss.
Bei dem Online Ansatz gelangt das Zertifikat in elektronischer Umgebung zum Eigentümer. Wenn der Schlüssel nicht auf dem Client erzeugt wird, muss der private Schlüssel (Zertifikat) auf sicherem Weg zum Schlüsselinhaber gelangen. Der [RFC2510] beschreibt mehrere Mechanismen dafür.

Zertifikatsveröffentlichung: Nach dem das Zertifikat zu dem Inhaber gelangt ist, müssen die öffentliche Zertifikate den anderen Endeinheiten zugänglich gemacht werden. Es gibt zwei Möglichkeiten:

Out-of-band Veröffentlichung: die öffentlichen Zertifikate gelangen ohne Verwendung elektronischen Techniken zu anderen Endeinheiten.

Veröffentlichung in Datenbasis: die öffentlichen Zertifikaten werden in einer Datenbasis (z.B. in einer Verzeichnisdienst) veröffentlicht.

In-Band Veröffentlichung: die öffentlichen Zertifikate werden mit einem geeigneten Protokoll, das vor allem zu anderen Zwecken (z. B. S/MIME) verwendet wird, übertragen. Dies kann meisten mit Hilfe der digitalen Signatur (vor allem bei Emails) durchgeführt werden. (Siehe Abschnitt 2.3.2)

Key-Backup: Bei den meisten Unternehmen ist es erforderlich, verschlüsselte Daten auch dann wieder entschlüsseln zu können, wenn der Verschlüsselungsschlüssel verloren geht. Während der Initialisierungsphase muss das private Schlüsselmaterial gesichert werden.
Wenn aber das Schlüsselmaterial zur digitalen Signatur verwendet wird, soll nie eine Sicherungskopie angefertigt werden. Damit kann ein Missbrauch des Signaturschlüssels vermieden werden. In der Fachliteratur [AAL 02] wird sogar die Generierung auf der Endeinheit gefordert, damit keine Möglichkeit besteht, dass der Signaturschlüssel die Endeinheit verlässt.

Bemerkung zu Schlüsselbereitstellung an vertrauenswürdige Dritte (escrow)

Der Zweck der Anfertigung einer Sicherheitskopie des Schlüsselmaterials wurde schon beschrieben. Eine weitere Forderung kommt noch zusätzlich dazu. Das Unternehmen

muss auf berechtigte Anforderung von Rechtsvertreter staatlicher Einrichtungen verschlüsselte Informationen entschlüsseln können und diese Informationen in entschlüsselter Form bereitstellen. Demnach muss ein berechtigter Mitarbeiter des Unternehmens das private Schlüsselmaterial zur Verfügung stellen, damit die verschlüsselte Informationen wieder entschlüsselt werden können.

5.3.2 Verwendungsphase

Wenn das Schlüsselmaterial generiert und verteilt wurde, beginnt die Auslieferungsphase. Die einzelnen Prozesse dieser Phase werden weiter unten beschrieben.

Zertifikatsvalidierung Die Integrität eines öffentlichen Zertifikates kann überprüft weden, weil das Zertifikat von der ausstellenden CA signiert ist. Das ist der erste Schritt während der Validierung. Es sind aber noch weitere Schritte nötig, damit ein Zertifikat als gültig angesehen werden kann. Der zweite Schritt zur Validierung ist die Überprüfung, ob das Zertifikat von einer vertrauenswürdigen CA ausgestellt ist. Dies beinhaltet auch die Prüfung des Zertifikatspfades. Wenn das erfolgreich abgeschlossen ist, ist die Integrität des Zertifikats geprüft. Der nächste Schritt ist die Überprüfung, ob das Zertifikat bereits gültig ist bzw. noch nicht abgelaufen ist. Die letzte Prüfung der Gültigkeit erfolgt anhand der Widerrufliste. Wenn das Zertifikat nicht in der Widerrufliste ist, kann das Zertifikat als gültig bewertet werden.
Ob das Zertifikat für die gewählte Operation verwendet werden kann, entscheiden die Zertifikatserweiterungen und der Zertifikatsverwendungszweck. Wenn die erwünschte Operation in den Zertifikatserweiterungen und in dem Zertifikatsverwendungszweck erlaubt ist, kann das Zertifikat verwendet werden.

Schlüsselwiederbereitstellung Die Bedeutung der Erstellung einer Sicherheitskopie des privaten Schlüssels wurde schon diskutiert. Die Schlüsselwiederbereitstellung ist das Gegenstück zu der Anfertigung der Sicherheitskopie. Wenn ein Benutzer das Schlüsselmaterial verliert, können ohne Sicherheitskopie des Schlüsselmaterials die verschlüsselten Informationen nicht wieder entschlüsselt werden. Da es sich bei den Informationen um Unternehmensinformationen handelt, wären diese Informationen ohne Schlüsselwiederbereitstellung für das Unternehmen verloren.

Schlüsselupdate Die Zertifkate haben eine bestimmte Lebensdauer. Nur innerhalb dieses Zeitintervalls sind Zertifikate gültig. Die Lebensdauer der Zertifikate wird durch Certificate Policy bzw. Certification Practice Statement festgelegt. Wenn ein Zertifikat zeitlich nahe am Ablaufdatum ist, kann ein neues Zertifikat bereits ausgestellt werden, damit in der Kommunikation keine Zwangsunterbrechung stattfindet.

5.3.3 Vernichtungsphase

Der Schlüssellebenszyklus wird mit der Vernichtungsphase abgeschlossen. Diese Phase beinhaltet folgendes:

- Der Ablauf eines Zertifikats liegt in der Eigenschaft des Zertifkats selber, da jedes Zertifkat eine nach oben und nach unten begrenzten Lebenssdauer hat.

- Der Zertifikatswiderruf bedeutet, dass ein öffentliches Zertifikat und das korrespondierendes privates Zertifikat nicht mehr gültig sind. Die Liste der widerrufenen Zertifikaten werden in sogenannten Widerruflisten veröffentlicht.
- Die Zertifikatshistorie ist erforderlich, damit verschlüsselte Daten auch nach dem Ablauf des Zertifikats entschlüsselt werden können.
- Das Zertifikatsarchiv ist ein sicherer und vertraulicher Speicher für Cryptomaterial und für die Zertifikatshistorie.

Zertifikatsablauf Wenn sich ein Zertifikat ausserhalb seines gültigen Zeitraumes befindet, kann eines der drei folgenden Ereignisse auftreten:

- Kein Ereignis passiert, wenn sich die Endeinheit nicht mehr innerhalb der PKI befindet.
- Zertifikatserneuerung, d.h. ein neues Zertifikat mit demselben Schlüsselmaterial wird erzeugt und verteilt.
- Zertifikatsupdate, wenn ein neues Zertifikat mit neuem Schlüsselmaterial generiert und verteilt wird.

Zertifikatswiderruf bedeutet, dass ein Zertifikat als ungültig (widerrufen) markiert wird, bevor das Zertifikat abläuft. Unter bestimmten Umständen kann es erforderlich sein, dass ein Zertifikat vor dem Ablauf widerrufen werden soll. Wenn das ptivate Zertifikat komprimittiert wird, muss der Zertifikatsinhaber den Widerrufprozess bei der CA oder RA direkt initiieren.

Zertifikatshistorie beinhaltet alle (gültigen, widerrufenen, abgelaufenen) bisherigen für die Endentität ausgestellten Zertifikate. Dies kann erforderlich sein, wenn z. B. der Rechner des Zertifikatsinhabers neuinstalliert wird, und der Zertifikatspeicher sich auf dem Rechner befindet.

Zertifikatsarchiv speichert für längere Zeit die Schlüsselmaterialien. Diese Aufgabe kann entweder die CA selber oder eine vertraute Stelle übernehmen.

Bemerkung zu Zertifikatserneuerung und Zertifikatsupdate

Der Grund für eine Zertifikatserneurung ist ein anderer als für ein Zertifikatsupdate. Der Unterschied liegt in den Schlüsseln der Zertifikate. Solange die Zertifikatserneurung ein neues Zertifikat mit dem bisherigen Schlüssel ausstellt, wird während dem Zertifikatsupdate ein neues Zertifikat mit neuem Schlüssel ausgestellt.
Während die alten verschlüsselten Informationen nach der Zertifikatserneuerung mit dem neuen Zertifikat entschlüsselt werden können, können die verschlüsselten Informationen nach einem Zertifikatsupdate nicht mehr mit dem neuen Zertifikat entschlüsselt werden. Hier schafft die Zertifikatshistorie Abhilfe.

Bemerkung zu Zertifikatshistorie und Zertifikatsarchiv

Die Zertifikatshistorie ist an eine Endeinheit gebunden und bietet Zugang zu dem Entschlüsselungsmaterial.
Das Zertifikatsarchiv speichert Zertifikate von vielen Endeinheiten. Das Zertifikatsarchiv besteht zum größten Teil aus Zertifikatshistorien. Eine Zertifikatshistorie wird

benötigt, wenn die lokale Zertifikatshistorie einer Endeinheit beschädigt oder verloren gegangen ist. In so einem Fall kann die im Zertifikatsarchiv gespeicherte Zertifikatshistorie von dem Zertifikatsarchiv angefordert werden.

5.4 Eigene Lösung: Möglichkeiten für die E-Mail-Verschlüsselung

Eine eigene Komplettlösung für eine PKI benötigt die Anwendungsfälle als Grundlage für die Überlegungen. Es sind vielleicht Komponenten der PKI im Unternehmen vorhanden. Das lässt sich erst nach der Analyse der Anforderungen und nach der Analyse der Lösungsmöglichkeiten feststellen. Weil der Anwendungsfall Emailverschlüsselung der aufwendigste und der häufigst benutzte ist, werden die Umsetzungsmöglichkeiten für die Emailverschlüsselung vorgestellt.

5.4.1 Organisatorische Prozesse

In der Regel bieten die organisatorischen Prozesse die Grundlage und Anforderungen an die Technik. Aus diesem Grund werden zuerst die Möglichkeiten für verschiedene organisatorische Prozesse vorgestellt. Als erstes muss von der Benutzerregistration geschrieben werden, weil sie die Grundlage für eine PKI bietet. (vgl. 5.2.2)

Organisatorische Einheit: Registrationstelle und deren Aufgabe

Bei den organisatorischen Prozessen spielt die Registrationsstelle eine zentrale Rolle. Die Registrationsstelle und deren Aufgabe muss definiert werden, damit die anderen organisatorischen Prozesse greifen.
In einer PKI sind auch organisatorische Einheiten eingebunden. Eine PKI besteht zwar zum größten Teil aus Technik, es müssen aber auch die organisatorischen Einheiten klar definiert und die organisatorischen Prozesse klar beschrieben werden, damit die PKI als ganzes reibungslos funktioniert.
Die Registrationsstelle wurde bereits im Abschnitt 5.2.2 beschrieben. Hier werden nur einige Umsetzungsmöglichkeiten erwähnt.
Aufgaben einer Registrationsstelle sind:

1. Registration des Anwenders
2. Feststellung der Identität des Anwenders
3. Überprüfung der Identität des Anwenders

Bei der Registrationsstelle gibt es zwei Möglichkeiten; entweder wird eine eigene Registrationsstelle eingerichtet oder es werden einige der Aufgaben an die Personalabteilung delegiert und die anderen Aufgaben automatisiert.

Bei der eigenen Registrationsstelle könnten alle Registrationsufgaben erledigt werden. Es muss aber beachtet werden, dass eine Registrationsstelle in jedem Land

eingerichtet werden muss, wenn die Wahl auf die Einrichtung einer eigenen Registrationsstelle fällt. Dabei dürfen die nationalen Gesetze der Länder, in denen eine Registrationsstelle eingerichtet werden soll, nicht außer Acht gelassen werden. Dabei spielen die datenschutzrechtlichen Bestimmungen eine wesentliche Rolle, weil die Registrationsstelle persönliche Daten speichern muss. Aus diesem Grund ist eine genaue Untersuchung der nationalen datenschutzrechtlichen Bestimmungen erforderlich. Zu der Erstellung der rechtlichen Richtlinien der Registrationsstellen müssen in der Regel Juristen miteinbezogen werden. Weil das ein eigenes und sehr breites Gebiet ist, wird darauf nicht näher eingegangen. Es gibt mehrere Möglichkeiten, wie die Struktur von Registrationsstellen aufgebaut werden kann. Dabei muss zwischen Nutzen und Kosten abgewogen werden. Eine Möglichkeit wäre, in jedem Land eine Registrationsstelle einzurichten. Dann müsste jeder Mitarbeiter dorthin fahren und sich registrieren lassen. Das verursacht Fahrkosten und Arbeitszeiten. Eine andere Möglichkeit ist, die Einrichtung mobiler Registrationsstellen. Diese Registrationsstelle fährt von Standort zu Standort, um die Registration der Mitarbeiter vorzunehmen. Die Einrichtung mobiler Registrationsstelle mit entsprechender Sicherheit verursacht ebenfalls nicht zu unterschätzende Kosten.

Bei einer verteilten Registrationsstelle kann die Personalabteilung einige Aufgaben übernehmen. Die Personalabteilung erfasst in der Regel die persönliche Daten. Der Vorteil der Delegation der Registration an die Personalabteilungen liegt darin, dass sich die Personalabteilungen jeweils in dem jeweiligen Land befinden und die nationalen datenschutzrechtlichen Bestimmungen kennen müssen.
Bei den meisten mittelständischen Unternehmen existiert ein zentrales Adressbuch, das aus dem Personalverfahren mit Daten versorgt wird. Dadurch ist die Konsistenz der Daten gewährleistet. In der Regel lassen sich solche Datenbasen mittels LDAP Protokoll abfragen. Im Microsoft Umfeld übernimmt diese Aufgabe das Active Directory. Die Benutzerüberprüfung über eine Webseite lässt sich mit Hilfe der integrierten Authentifizierung von Microsoft vornehmen. Wenn man ganz sicher sein will, kann auch eine zusätzliche Passworteingabe verlangt werden.

Die zwei wichtigsten Ansätze einer Registrationssstelle werden in der Tabelle 5.1 zusammengefasst. Es gibt im Prinzip diese zwei Möglichkeiten für die Organisation einer Registrationsstelle. Von diesen zwei Möglichkeiten lassen sich weitere Mischformen ableiten. Wie eine Registrationsstelle aussehen soll, hängt von der Abwägung zwischen Sicherheit, Konformität und Kosten ab.
Nachdem in diesem Abschnitt die Wichtigkeit und Aufgaben einer Registrationsstelle diskutiert wurden, wird in den nächsten Abschnitten auf nochmalige Beschreibung dieser Prozesse verzichtet.

Erste Umsetzungsvariante für organisatorische Prozesse

Es gibt den traditionellen und strikten Ansatz, dass der Anwender alles nur persönlich bei der Registrationsstelle erledigen kann. Demnach muss der Anwender immer zur Registrationsstelle, wenn er ein neues Schlüsselmaterial bestellen, ein vorhandenes Material zurückrufen lassen oder vorhandenes Schlüsselmaterial wiederbereitstellen lassen will. Dieser strikter Ansatz bietet zwar die höchste Sicherheit, ist aber in der Praxis schwer und teuer umzusetzten. Man könnte zwar mehrere Umsetzungsvarianten ausarbeiten, hier werden nur zwei Möglichkeiten nacheinander vorgestellt.

Aufgabe	eigene zentrale Registrationsstelle	verteilte Registrationsstelle
Registration	persönliche Anwesenheit des Mitarbeiters bei der zentralen Registrationsstelle erforderlich	diese Aufgabe übernimmt die Personalabteilung
Identifizierung	persönliche Anwesenheit des Mitarbeiters bei der zentralen Registrationsstelle erforderlich	erfolgt elektronisch (mit Hilfe von Active Directory und Microsoft integrated authetication und Eingabe von Passwort des Domainen Logins)
Autorisierung	nach erfolgreicher Registration und Identifikation	nach erfolgreicher Registration und Identifikation

Tabelle 5.1: Vergleich der verschiedenen Ansätze für Registrationsstellen

Umsetzungsmöglichkeit 5.4.1 *Eine Möglichkeit für die Bestellung ist, dass das Cryptomaterial automatisch für jeden neuen Mitarbeiter nach der Einstellung gemeinsam mit einem Email- und Domainaccount bestellt wird. Da die Einstellung über die Personalabteilung geht und die Bestellung des Emailaccounts ebenfalls von der Personalabteilung ausgeht, kann das Schlüsselmaterial für die Emailverschlüsselung auch mitbeantragt werden. (Siehe Abbildung 5.3)*
Die anderen Mitarbeiter können die Bestellung des Cryptomaterials über den zuständigen Personalberater bestellen. Das ist möglich, weil die Personalberater die Mitarbeiter für die sie zuständig sind in der Regel kennen.

Umsetzungsmöglichkeit 5.4.2 *Die Personalabteilung sendet die Bestellung an die Sicherheitsabteilung. Die Sicherheitsabteilung veranlasst bei der CA die Bestellung. Der Sicherheitsadministrator hat auf die Generierung keinen Einfluss.*

Umsetzungsmöglichkeit 5.4.3 *Die CA sendet dem Mitarbeiter eine automatisch generierte Email, dass er sein Emailverschlüsselungschlüssel bei der Sicherheitsabteilung abholen kann. Diese Email beinhaltet auch die Import PIN.*

Umsetzungsmöglichkeit 5.4.4 *Der Mitarbeiter holt persönlich das Cryptomaterial bei einer zentralen Stelle ab. Bei der Übergabe wird die Identität des Mitarbeiters überprüft und erst nach einer positiven Überprüfung erhält er das Cryptomaterial entweder auf seinen Firmenausweis (SmartCard Lösung) oder auf einem Datenträger.*

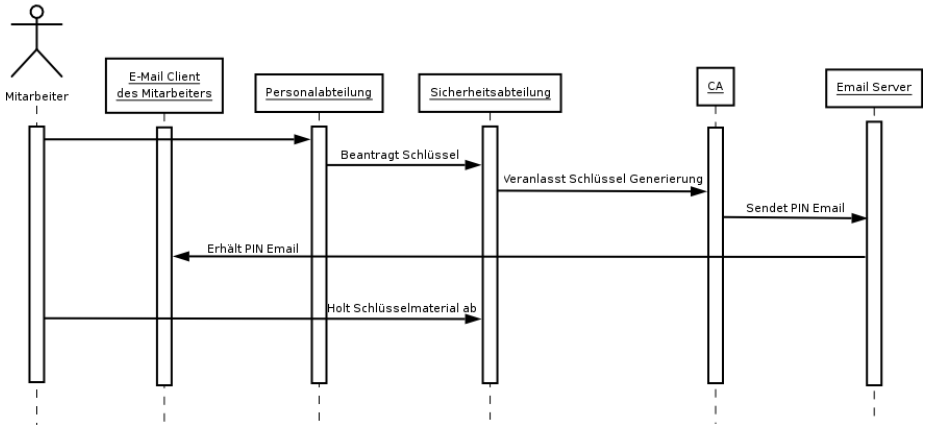

Abbildung 5.3: Erste Umsetzungsmöglichkeit für den Bestellprozess

Umsetzungsmöglichkeit 5.4.5 *Nach dem das Cryptomaterial abgeholt wurde, wird der öffentliche Teil veröffentlicht.*

Umsetzungsmöglichkeit 5.4.6 *Den Importvorgang muss der Anwender selbst mit Hilfe einer Anleitung vornehmen.*

Die Verwendung ist abhängig von der Clientsoftware, deshalb wird sie bei den technischen Ansätzen beschrieben.

Umsetzungsmöglichkeit 5.4.7 *Der Rückruf des Verschlüsselungsschlüssels kann der Mitarbeiter über eine Email an die Sicherheitsabteilung vornehmen. Die Sicherheitsabteilung kann den Verschlüsselungsschlüssels nach telefonischer Bestätigung des Mitarbeiters (Zertifikatsinhaber) widerrufen. Der Sicherheitsadministrator holt die Telefonnummer aus dem globalen Adressbuch. Dadurch wird gewährleistet, dass der Benutzer mit dem Widerruf des Zertifikats einverstanden ist. Der ganze Vorgang wir in der Abbildung 5.4 gezeigt.*

Umsetzungsmöglichkeit 5.4.8 *Eine Wiederbereitstellung kann über eine sichere Intranetseite angefordert werden. Der Benutzer identifiziert sich mit seinem persönlichen Passwort. Die Benutzerdaten werden überprüft und bei Übereinstimmung werden die Zertifikatsdaten angezeigt. Auf dieser Seite muss der Benutzer die Wiederbereitstellung bestätigen. Nach der Bestätigung wird eine Anfrage an die CA gesendet. Die CA generiert eine PIN Email und sendet sie an den Benutzer. Die PIN Email beinhaltet auch den Hinweis, dass der Benutzer bei der Sicherheitsabteilung oder bei der örtlichen LRA das Zertifikat abholen kann. Die Abbildung zeigt diesen Vorgang.*

Diese Variante bietet sichere aber aufwendige Prozesse. Da das Unternehmen weltweit Standorte mit ungleicher Anzahl von Mitarbeitern hat, ist es schwierig, eine zentrale Stelle überall einzurichten. Es muss zwischen Sicherheit, Aufwand und Kosten abgewogen werden.

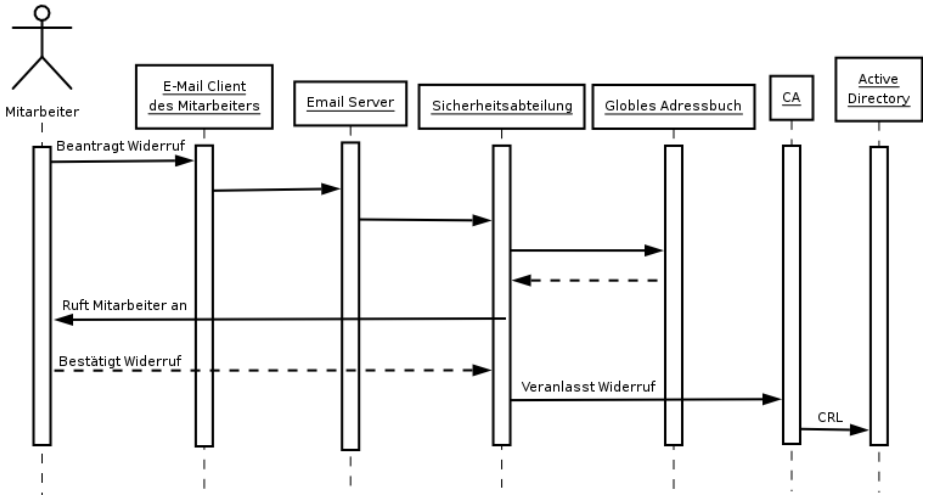

Abbildung 5.4: Erste Umsetzungsmöglichkeit für den Zertifikatswiderruf

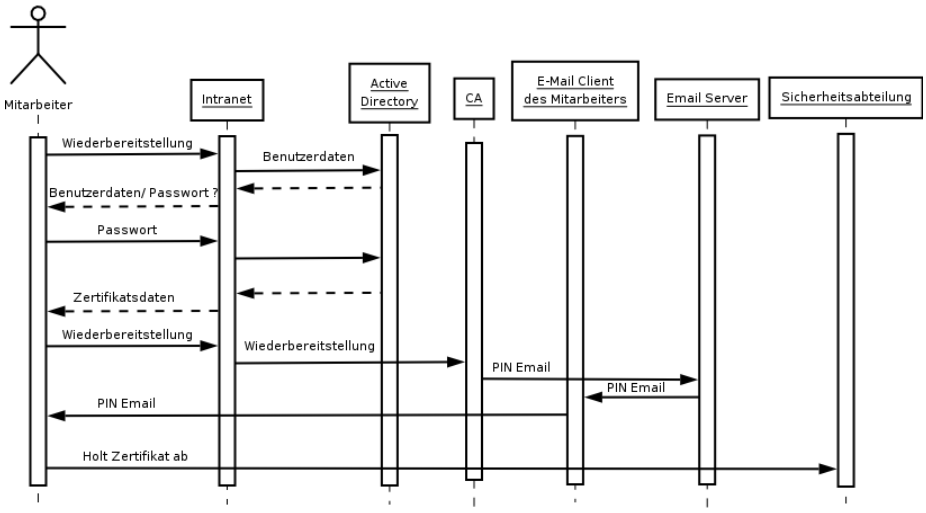

Abbildung 5.5: Erste Umsetzungsmöglichkeit für die Zertifikatswiederbereitstellung

Zweite Umsetzungsvariante für organisatorische Prozesse

Umsetzungsmöglichkeit 5.4.9 *Eine Möglichkeit wäre, dass der Mitarbeiter eine Meldung mit einem Intranetlink auf die Bestellseite erhält, wenn er ohne eigenes Cryptomaterial verschlüsselte Email zu versenden versucht. Dies setzt womöglich eine entsprechende Unterstützung und Konfiguration der Clientsoftware voraus.*

Umsetzungsmöglichkeit 5.4.10 *Alle Mitarbeiter können die Bestellung über eine sichere Intranetseite vornehmen. Die Mitarbeiter werden anhand des Domainlogins und nach der Eingabe des persönlichen Login-Passwortes authentifiziert. Danach kann er die Zertifikate bestellen, wobei der Mitarbeiter keine Möglichkeit hat, irgendwelche*

Daten einzugeben, weil alle Daten aus dem Active Directory im Hintergrund geholt werden. Anhand dieser Daten erzeugt die CA das Zertifikat und zeigt die Import-PIN an. Die CA sendet an die Emailadresse des Mitarbeiters eine automatisch generierte Email mit einem Verweis, wo er das Zertifikat herunterladen kann.

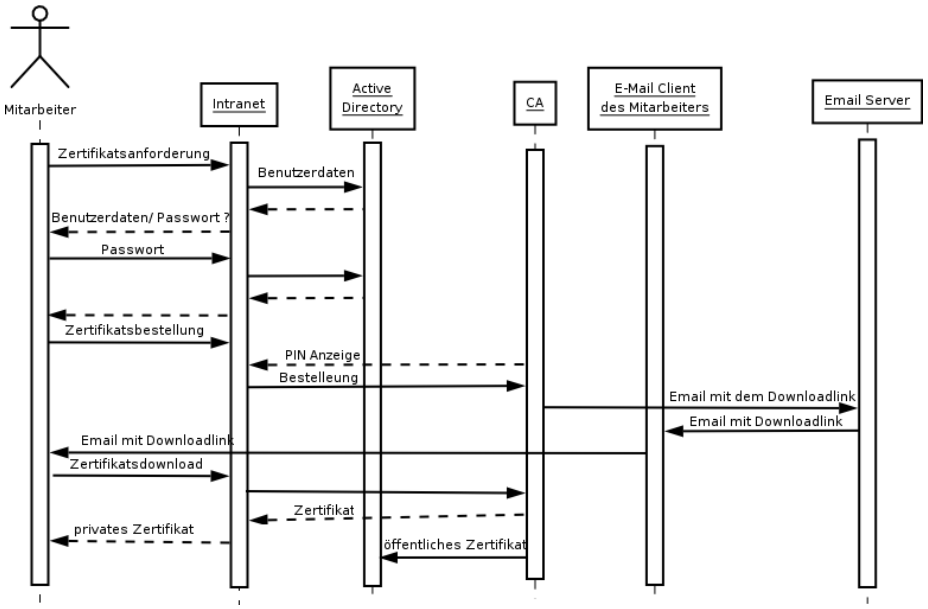

Abbildung 5.6: Zweite Umsetzungsmöglichkeit für den Bestellprozess

Umsetzungsmöglichkeit 5.4.11 *Kurz danach erhält der Mitarbeiter eine automatisch generierte Email mit dem Downloadlink, wo er das Cryptomaterial herunterladen kann. Dieser Verweis kann nur einmal aufgerufen werden, wodurch ein Missbrauch bemerkbar gemacht wird. Falls der Mitarbeiter nochmal auf die sichere Intranetseite geht, erhält er nach erfolgreicher Authentifizierung die Meldung, dass er bereits Schlüsselmaterial ausgeliefert bekommen hat. Da der Mitarbeiter nur nach der Domainanmeldung auf die Emails zugreifen kann, ist eine grundlegende Authentifizierung gewährleistet. Diesen Prozess zeigt die Abbildung 5.6.*

Umsetzungsmöglichkeit 5.4.12 *Der Mitarbeiter holt sein Cryptomaterial von der in der Email angegebenen und sicheren Intranetseite nach erfolgreicher Authentifizierung und importiert es mit Hilfe der Anleitung.*

Umsetzungsmöglichkeit 5.4.13 *Nachdem der Mitarbeiter sein Cryptomaterial von der sicheren Intranetseite geholt hat, wird der öffentliche Teil des Cryptomaterials veröffentlicht. Der Ort soll gewählt werden, auf den die internen Mitarbeiter und die Clientsoftware zugreifen können. Es muss aber auch eine Schnittstelle für die Geschäftspartner eingerichtet werden.*

Umsetzungsmöglichkeit 5.4.14 *Den Rückruf des eigenen Zertifikates kann der Mitarbeiter selber nach einer erfolgreichen Authentifizierung über eine sichere Intranetseite vornehmen. Über den Rückruf erhält er eine Email.*

Umsetzungsmöglichkeit 5.4.15 *Eine Wiederbereitstellung kann der Mitarbeiter auch selber nach einer erfolgreichen Authentifizierung über eine sichere Intranetseite vornehmen. Er erhält die Import-PIN angezeigt und eine Email mit dem Intranetverweis, wo er das Zertifikat nach einer erfolgreichen Authentifizierung herunterladen kann. Der Verweis ist auch nur eimal aufrufbar.*

5.4.2 Technische Strukturen

Da es mehrere verschiedene Ansätze bezüglich der Emailverschlüsselung gibt, werden diese in den folgenden Abschnitten einzeln behandelt. Dabei muss vorangehend erwähnt werden, dass diese Ansätze im Prinzip disjunkte Lösungen sind. Manche lassen sich mit unterschiedlichem Aufwand miteinander verknüpfen bzw. zu einer PKI ausbauen.

Clientsoftware

Bei der Clientsoftware gibt es die Anforderung, dass die Clientsoftware anhand des Schlüsselmaterials des Empfängers den Verschlüsselungsstandard erkennt und die entsprechenden verschlüsselten Emails generiert. Das Problem besteht vor allem bei Empfängerlisten, wobei die verschiedenen Empfänger unterschiedliche Schüsselmaterialien haben können. In diesem Fall muss die Clientsoftware stets den richtigen Standard verwenden und eine für den Empfänger entschlüsselbare Email generieren. Die verschlüsselten Emails müssen von dem Absender stets wieder entschlüsselt werden können. Bei der Clientsoftware gibt es zwei unterschiedliche Ansätze. Der eine Ansatz folgt dem Prinzip der höchsten Konformität für den Benutzer. Bei dieser Lösung erfährt der Benutzer von der Verschlüsselung wenig, und kann davon ausgehen, dass die Emails in der Regel verschlüsselt den Client verlassen. Zuerst wird dieser Ansatz vorgestellt, der in der Fachliteratur als Proxy Lösung bezeichnet wird.

Umsetzungsmöglichkeit 5.4.16 *Bei der sogenannten **Proxy Lösung**, handelt es sich um eine Applikation, die auf dem Client im Hintergrund läuft und die Emails vom Emailclient abfängt, verschlüsselt und an den Emailserver weiterleitet. Die Idee dabei ist, dass der Anwender sich nicht um die Zertifikats- und Schlüsselverwaltung kümmern muss. [TR05] Drei Bekannte Lösungen sind Ciphire Mail (https://www.ciphire.com/), PGP Desktop (www.pgp.com/de/products/desktop/index.html) und GPG-Relay (http://sites.inka.de/tesla/gpgrelay.html).*

Umsetzungsmöglichkeit 5.4.17 ***PGP Desktop** arbeitet mit PGP Schlüsseln und X.509 Zertifikaten. Bei PGP Desktop lassen sich Regeln definieren, wie die Software eine Email behandeln soll. Diese Software lässt sich nur in Verbindung von PGP Universal zentral verwalten. Die Software PGP Desktop alleine genügt in einem Unternehmen nicht, da sie eine zentrale Verwaltung der Regeln erfordert.*

Umsetzungsmöglichkeit 5.4.18 ***Ciphre Mail** arbeitet mit eigenem Cryptomaterial. Bei Ciphre Mail gibt es bisher keine Administrationssoftware.*

Bei diesem Ansatz verlässt die Email den Absenderrechner bereits verschlüsselt. Problematisch ist bei dieser Lösung die Einbindung in eine PKI, da die Schlüsselbestellung

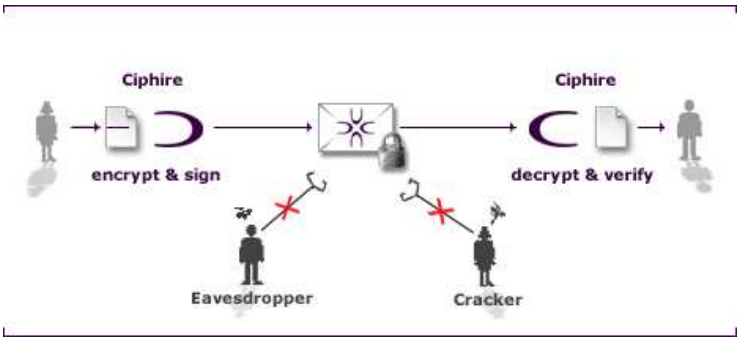

Abbildung 5.7: Funktionsweise der Proxylösung bei Ciphire Mail (Quelle:Ciphire Mail)

in der Regel automatisch im Hintergrund abläuft, oder der Schlüssel auf dem Client generiert wird. Bei diesen Produkten werden die Schlüssel auf dem Client erzeugt. Falls das Schlüsselmaterial beschädigt oder gelöscht wird, kann eine Wiederbereitstellung nur bei PGP Desktop in Verbindung mit PGP Universal bei entsprechender Konfiguration ermöglicht werden. Dies könnte ein Hindernis bei einer Wiederbereitstellung sein. Der Absender erhält wenig Information über das Ergebnis der Verschlüsselung. Probleme können beim Empfänger ohne öffentlichen Schlüssel auftreten. Das Problem des Schlüsselaustausches mit externen Geschäftspartner ist nicht trivial.

Bewertung der Proxy Lösung:

+ Einfache Handhabung für den Anwender
+ Einfache Schlüsselverwaltung für den Anwender
+ Unterstützung von PGP und S/MIME (PGP Desktop)
- Komplexe Integration in PKI
- Zentrale Schlüsselverwaltung schwierig und umständlich (bei Ciphire Mail unmöglich)
- Zentrales Schlüsselbackup lässt sich nur schwer realisieren (bei Ciphire Mail unmöglich)
- Propriotäres Schlüsselformat bei Ciphire Mail
- bei PGP Desktop ist PGP Universal erforderlich zur Clientverwaltung (Regeln und Schlüssel)
- Virensuche auf dem Server nicht möglich, Antivirenanwendung auf dem Client notwendig
- Zusätzlicher Dienst wird auf dem Client installiert
- Ergebnis der Verschlüsselung für den Anwender nicht ersichtlich

Der andere Ansatz ist die Erweiterung des Emailclients mit einer Zusatzsoftware. Diese Zusatzsoftware nistet sich in den Emailclient ein und zeigt sich mit ihren speziellen Ikonen in der Ikonenleiste. Dieser Ansatz wird generell als Plug-In Lösung bezeichnet.

Bei dieser Lösung verhält sich die installierte Software wie ein Teil des Emailclients und erweitert dessen Funktionalität. Durch die angezeigten Ikonen wird die Steuerung dem Benutzer übergeben, ob er eine Email verschlüsselt absenden will oder nicht.

Umsetzungsmöglichkeit 5.4.19 *Bei der **Plug-In Lösung** ist die Clientsoftware für die Verschlüsselung verantwortlich. Bei dieser Lösung können die Schlüssel zentral verwaltet werden. Theoretisch könnte man die Schlüsselverwaltung auch am Client erledigen, dabei stößt man in der Regel auf verschiedene Probleme, wie z.B. der Anwender kennt sich nicht mit der Verschlüsselung an sich aus, weshalb er fahrlässig mit dem Cryptomaterial bzw. Cryptospeicher umgeht.*
Bei einem mittelständischen Unternehmen ist eine End-To-End Verschlüsselung und eine Wiederbereitstellung des Schlüselmaterials in der Regel erwünscht.
Durch die Ikonen wird dem Benutzer die Wahl des verschlüsselten Versendens überlassen.

Bewertung der Plug-In Lösung:

+ Einfache Handhabung für den Anwender
+ Unterstützung von PGP und S/MIME (je nach Produkt)
+ Echte End-To-End Verschlüsselung
+ Sicherheit gegen innere Angriffe
+ Zentrale Schlüsselverwaltung möglich
+ Einfache Integration in eine PKI
+ Ergebnis der Verschlüsselung für den Anwender offensichtlich
- Zusätzliche Clientsoftware erforderlich
- Virensuche auf dem Server nicht möglich, Antivirenanwendung auf dem Client notwendig

Es gibt mehrere Produkte für die Plug-In Lösung mit unterschiedlichen Möglichkeiten:

- CryptoEx Outlook
- Trusted Mime von IC-Compas (http://www.ic-compas.de/)
- G-Data GNUPG Plug-In (http://www3.gdata.de/gpg/), [Golem2]
- WinPT (http://winpt.sourceforge.net/de/index.php)
- GPGol (http://www.g10code.com/de/p-gpgol.html)

Diese Liste beinhaltet nur die bekanntesten Lösungen und kann aus diesem Grund keineswegs vollständig sein.
Es darf nicht unerwähnt bleiben, dass die Firma G-Data am eigenen Produkt GNUPG Plug-In nicht mehr interessiert ist. Eine verbesserte und neuere Version dieses Produktes ist unter dem neuen Namen GPGol erhältlich.
Bei WinPT handelt es sich um eine OpenSource Entwicklung. Hinter dieser Entwicklung stehen die Entwickler aber kein Unternehmen, was die Anfragen und Anforderung bezüglich Unterstützung, Support und Wartung erschwert.

In der Tabelle 5.2 sind die clientseitigen Lösungen miteinander verglichen. In der Tabelle wird die Microsoft Benennung AddIn statt PlugIn verwendet.
In der Tabelle werden noch die Kosten gelistet. Die Kosten für

- Microsoft Oulook sind bereits in den Kosten für Microsoft Office enthalten.
- CryptoEx werden über die Anzahl der verwendeten Schlüsselmaterialien errechnet. Ein Wartungsvertrag für die Software muss separat abgeschlossen und bezahlt werden.
- TrustedMime werden vertraglich geregelt, wobei der Produktpreis und die Wartungskosten mit einem Vertrag geregelt werden.
- GPGol werden nicht berechnet, weil es einerseits frei verfügbar ist. Das Produkt befindet sich aber noch in der Entwicklung, weshalb der Hersteller keinerlei Haftung übernimmt. Die Wartungskosten werden auf Anfrage mit einem Vertrag geregelt.
- PGP Desktop werden die Lizenzgebühren nach Anzahl der installierten Produkte errechnet. Für Unternehmen gibt es sog. Bundle-Preise.
- Ciphire Mail Client werden auf Anfrage vom Hersteller genannt.

Wie man aus der Tabelle entnehmen kann, gibt es drei Varianten für eine Alternative zu der Proxy-Lösung:

1. Microsoft Outlook mit GPGol:
   + Kann PGP und S/MIME
   + Günstig
   - GPGol befindet sich in der Entwicklung $\Rightarrow$ es können Fehler augtreten
   - Keine Behandlung von Empfängerlisten mit gemischten Empfängern (PGP und S/MIME)
   - Entweder PGP oder S/MIME
   - Keine Möglichkeit der manuellen Zertifikatszuweisung zu einem Empfänger in Outlook
2. CryptoEx Outlook
   + Erkennt PGP und S/MIME anhand des Schlüsselmaterials des Empfängers und generiert die entsprechende Email.
   + Behandlung von Empfängerlisten mit gemischten Empfängern (PGP und S/MIME).
   + Möglichkeit der manuellen Schlüssel-/Zertifikatszuweisung zu einem Empfänger.
3. TrustedMime

	Microsoft Outlook	CryptoEx Outlook	Trusted Mime	GPGol	PGP Desktop	Ciphire Mail Client
verwendetes Schlüssel-material	X.509	X.509 und PGP	X.509 und PGP	nur PGP	X.509 und PGP	eigenes Schlüssel-material
automatische Erkennung der Standards	nur X.509	ja, beide	ja, beide	nur PGP	ja, beide	n.a.
verwendeter Cryptospeicher	CPBS	Eigener und CPBS	Eigener	Eigener	Eigener	Eigener
Arbeitsweise	AddIn	AddIn	AddIn	AddIn	RGLB kein AddIn	RGLB kein AddIn
Kosten	Niedrig	Mittel	Mittel	Niedrig	Hoch	Mittel

Tabelle 5.2: Produktvergleich der clientseitige Lösungen für die Emailverschlüsselung

Bemerkungen zu der Tabelle:
CPBS – Cryptospeicher des Betriebssystems
RGLB – Regelbasiert

+ Erkennt PGP und S/MIME anhand des Schlüsselmaterials des Empfängers und generiert die entsprechende Email.
+ Behandlung von Empfängerlisten mit gemischten Empfängern (PGP und S/MIME).
+ Möglichkeit der manuellen Schlüssel-/Zertifikatszuweisung zu einem Empfänger.

Bemerkung 5.4.1 *Microsoft Outlook greif auf den Zertifikatsspeicher des Betriebssystems zu. Falls Outlook ein Zertifikat mit einer Emailadresse im Zertifikat findet, die mit einem der Empfängeradressen übereinstimmt, wird es genommen. Man hat aber in Outlook keine Möglichkeit einem Empfänger ein Zertifikat zuzuweisen. [MSOL05]*

Zentralisierte Ansätze

Bei den bisherigen Ansätzen wurde die Verschlüsselung auf dem Client vorgenommen. Es gibt einen anderen Ansatz, bei dem die Verschlüsselung auf eine zenrale Komponente ausgelagert wird. Diese zentrale Komponente ist für die Verschlüsselung in der

gesamten Infratsruktur zuständig.

Umsetzungsmöglichkeit 5.4.20 *Bei der **Gateway Lösung** werden die Emails an einen anderen Dienst (Gateway) gesendet, diser verschlüsselt die Emails und leitet sie weiter. Das Gateway holt sich die öffentlichen Schlüssel automatisch. [KF05] Dabei kann der Gateway Dienst entweder auf einem eignen zentralen Rechner oder auf dem selben Rechner, wie der Mailserver laufen. Ob der Gateway vor dem Mailserver oder danach geschaltet wird, spielt aus der Sicht der Verschlüsselung keine Rolle.*
Bei dieser Lösung ist die Email zwischen Client und Emailserver bzw. Emailserver und Gateway an sich nicht verschlüsselt. Falls der Kommunikationsweg nicht in einer sicheren Umgebung (SSL bzw. TLS) stattfindet, ist es prinzipiell möglich Emails abzufangen bzw. manipulieren. Die Absicherung des Kommunikationsweges lässt sich mit Hilfe von X.509 Zertifikaten und mit Hilfe von TLS bzw. SSL Protokollen erledigen. Die erforderliche Zertifikate müssen entweder zu diesem Zweck teuer eingekauft oder kostengünstig von einer eigenen CA ausgestellt werden. Abhängig von der Netzkonfiguration sind mehrere Gateways erforderlich. Je mehr Gateways erforderlich sind, umso teurer kann es werden.
Das Gateway verschlüsselt, d.h. es ist im Besitz aller Schlüsselpaare, was ein Sicherheitsrisiko darstellt, da je nach Verwaltungsansatz die Verschlüsselungsmaterialien exportiert werden können. (siehe [KF05]) Manche Produkte setzten bei dieser Lösung nur ein einziges Schlüssselpaar ein, d.h. der gesamte eingehende Emailverkehr wird mit demselben sog. Firmenschlüssel verschlüsselt. Dieser Ansatz bietet zwar einen Schutz von aussen, nicht aber von innen. D.h. ein Mitarbeiter mit entsprechendem Wissen bzw. Berechtigung kann eine Email entweder auf dem Mailserver, oder falls die Email nicht auf gesichertem Weg zum Empfänger zugestellt wird, auch auf dem firmeninternen Netzwerk abfangen, lesen bzw. manipulieren.
Der Schlüsselaustausch mit anderen ist bei dieser Lösung, falls es mehrere Schlüsselpaare gibt, nicht einfach zu lösen. Falls es nur ein Firmenschlüsselpaar gibt, gestaltet sich der Schlüsselaustausch relativ einfach.

Es gibt mehrere Produkte, die diesem Ansatz folgen, einige von denen werden nachfolgend gelistet.

- SigabaNet, http://www.sigaba.com/
- Voltage SecureMail Gateway Server, http://www.voltage.com/
- Freenigma Server von Freenigma GmbH[1], http://www.freenigma.org/
- GPG-Relay, http://sites.inka.de/tesla/gpgrelay.html
- PGP Universal, http://www.pgp.com/products/universal/index.html

Bewertung der Gateway Lösung:

+ Einfache Handhabung für den Anwender
+ Einfache Schlüsselverwaltung für den Anwender
+ Unterstützung von PGP und S/MIME (in der Regel)

[1]Die freenigma gmbh positioniert sich damit als direkter europäischer Wettbewerber zu der US-amerikanischen PGP Corporation. Quelle: http://www.freenigma.org/firma/

+ Virusscan ist auf dem Mailserver möglich
+ Nur ein Schlüsselpaar erforderlich (ja nach Produkt)
+ Keine zusätzliche Clientsoftware erforderlich
- Keine zentrale Schlüsselverwaltung möglich
- Keine echte End-To-End Verschlüsselung
- Keine echte Sicherheit gegen innere Angriffe
- Zusätzlicher Server bzw. Serverdienst erforderlich
- Aufwendige Integration in eine PKI
- Ergebnis der Verschlüsselung für den Anwender nicht ersichtlich

Als Zusammenfassung werden die verschiedenen Ansätze in der Tabelle 5.3 dargestellt. Jede Lösung hat Vorteile und Nachteile. Die Proxy-Lösung bietet einfache Handhabung für die Benutzer, da er die Verschlüsselung und Signatur durch das Setzen von Emaileigenschaften beeinflussen kann. Bei der Gateway Lösung wird davon ausgegangen, dass

(a) der verschlüsselte Emailverkehr an das Unternehmen gerichtet wird

(b) für die ausgehenden Emails das Unternehmen haftet

Weiterführende Auslegung der Aspekte dieser Lösung befindet sich in [KF05]. Diese Lösung bietet gegen interne Angriffe keinen Schutz. Gegen interne Angriffe bietet die so genannte End-To-End Verschlüsselung. Darunter versteht man eine Verschlüsselung, die auf Absenderseite auf dem Client erfolgt. Auf der Empfängerseite sollte die Entschlüsselung auch auf dem Client erfolgen. Bei den vorgestelleten Ansätzen kann festgestellt werden, ob eine End-To-End Verschlüsselung auf der Absenderseite durch die Lösung ermöglicht wird. Bei den vorgestellten Ansätzen lässt sich die Lokalität der Entschlüsselung nicht beeinflussen. Wenn hier über End-To-End Verschlüsselung gesprochen wird, dann wird dies auf die Empfängerseite bezogen. Damit wird verdeutlicht, dass die Verschlüsselung auf dem Client erfolgt.

	Proxy Lösung	Gateway Lösung	Plug-In Lösung
echte Ende zu Ende Verschlüsselung	Absenderseitig Ja, beim Empfänger von Lösung abhängig	Nein	Absenderseitig Ja, beim Empfänger von Lösung abhängig
spezielle Clientsoftware erforderlich	Nein, es werden nur bestimmte Emailclients unterstützt	Nein	Von Serversoftware abhängig
Verwendung	Meistens durch Setzen einer Emaileigenschaft (Wichtigkeit, spezielles Subject etc.)	Keine Benutzerinteraktion erforderlich	Einfach
Schlüssel-verwaltung	Eigenes Cryptomaterial und Zugriff auf Keyserver	Keine erforderlich	eigenes Cryptomaterial und Zugriff auf Keyserver
Virenscan	Clientseitig erforderlich	Auch auf dem Server möglich	Clientseitig erforderlich
Schutz gegen innere Angriffe	Ja	Nein	Ja
Integration in eine PKI	Einfach	Nicht anwendbar	Einfach

Tabelle 5.3: Vergleich verschiedener Lösungen zur Emailverschlüsselung

5.5 Umsetzungsmöglichkeiten für die Emailsignatur

Da die Emailsignatur mit der Emailverschlüsselung Ähnlichkeiten aufweist und in der Regel mit derselben Anwendung erzeugt wird, gibt es hier auch die Möglichkeiten wie bei der Emailverschlüsselung im Abschnitt 5.4. Aus diesem Grund wird darauf hier nicht näher eingegangen.

5.5.1 Wahl des Cryptomaterials

Eine grundlegende Eigenschaft der Emailsignatur liegt in ihrer Natur. Es gibt eine allgemeine Anforderung an das Cryptomaterial für Signaturen, dass es nicht zentral gesichert und nicht wiederherstellungsfähig sein darf [AAL 02]. Nach dieser Forderung soll das Cryptomaterial für die Emailsignatur nicht zentral gesichert und wiederbereitstellungsfähig sein. Damit soll Missbrauch vorgebeugt werden. Aus diesem Grund wird zu einem getrennten Cryptomaterial zur Emailsignatur geraten. Bei dem X.509 Standard ist es kein Problem, da die Verwendungszwecke eines Zertifikats festgelegt werden können. Bei PGP lässt sich die PGP Signatur nicht steuern. Mit einem gültigen PGP Schlüsselpaar ist eine Emailsignatur in der Regel möglich. Einige Verschlüsselungsclients bieten in der Regel eine Auswahlmöglichkeit der Schlüssel zur Emailverschlüsselung bzw. zur Emailsignatur.

5.6 Umsetzungsmöglichkeiten für die Benutzerauthentifizierung

Die Zertifikatsbasierte Anmeldung wird bereits zur Anmeldung an einige Intranetanwendungen verwendet. Die Bestellung selber funktioniert langsam und mit erheblichem Aufwand (vgl. 3.7.7). Der Prozess und der technische Ablauf der Verwendung sollen nicht geändert werden, sondern nur das Zertifikat und die Bestellung den Anforderungen entsprechend angepasst werden. Die Benutzerauthentifizierung soll mit Hilfe von X.509 Zertifikaten erfolgen. Wie ein Mitarbeiter ein Zertifikat bestellen kann, beschreibt der folgende Absatz.

5.6.1 Organisatorische Prozesse

Jeder Mitarbeiter soll ein Authentifizierungszertifikat auf Anforderung erhalten. Es soll aber zwischen Angestellten und externen Mitarbeiter differenziert werden. In der Regel sollen nur die Angestellten ein Authentifizierungszertifikat anfordern und erhalten dürfen. (Vergleiche mit den Anforderungen 4.4.1, 4.4.2 und 4.4.3) Demnach sind berechtigte Personen nur die Angestellten.
Die Bestellung ist der erste Schritt. Während des Bestellprozesses muss der Besteller authentifiziert werden.

Umsetzungsmöglichkeit 5.6.1 *Die Authentifizierung kann, wie bei einigen Unternehmen mit eigener Registrationsstelle, über eine persönliche Identifikation anhand des Firmenausweises und anhand des Personalausweises vorgenommen werden. Dabei*

muss die Person, die die Identifikation durchführt, auf Informationen aus dem Corporate Directory und globalen Adressbuch zwecks Datenüberprüfung zugreifen können. Diese Person muss natürlich auch eine Vertrauensperson sein. Bei der örtlichen Verteilung und bei der Unternehmensgröße müssen mehrere Stellen, die die Identifikation durchführen können, eingerichtet werden.
Diese Stelle kann den Mitarbeitern das automatisch erzeugte Authentifizierungszertifikat auf einem Datenträger aushändigen. Die Import-PIN kann dem Mitarbeiter entweder über Email oder auf Spezialpapier abgedrucktem PIN Brief im Spezialumschlag mitgeteilt werden.

Diese Variante erfordert spezielle Zugriffsberechtigung auf die CA für die Vertrauensperson, die die Identifizierung und die Zertifikatsübergabe durchführt.

5.6.2 Technische Strukturen

Da sich die Einträge der Mitarbeiter und externe Mitarbeiter im Active Directory unterscheiden, kann in der Bestellung zwischen den beiden differenziert werden. Ein Mitarbeiter hat in einem der Attribute eine spezielle Zeichenkette. Anhand dieser Eigenschaft kann erkannt werden, ob der Besteller berechtigt ist ein Authentifizierungszertifikat zu bestellen oder nicht.

Das Zertifikat

Die Eigenschaften des Zertifikats für die Benutzerauthentifizierung wurden bereits in 3.7.4 beschrieben. Das Zertifikat für die Benutzerauthentifizierung soll anhand existierenden Zertifikaten und anhand der Anforderungen unter Beachtung des Standards erstellt werden. Die Spezifikation eines X.509 Zertifikat wurde in [RFC2459] festgelegt.

Clientsoftware

Um auf die Intranetanwendung zugreifen zu können, benötigt man nur einen Browser. Da im Unternehmen Microsoft Produkte eingesetzt werden, gibt es eine beschränkte Auswahl an Clientsoftware. Weil aber die Unternehmenspolicy Microsoft Produkte vorschreibt, kann hier nichts anderes als der Microsoft Internet Explorer vorgeschlagen werden.

5.7 Umsetzungsmöglichkeiten für die Dateiverschlüsselung

Die Dateiverschlüsselung soll nach Anforderung 4.3.1 schlüsselbasiert erfolgen. Aus diesem Grund scheiden schon etliche Produkte aus, da viele Produkte ohne den Einsatz eines Schlüsselmaterials arbeiten. Nach der Anforderung 4.3.3 soll ein Produkt für Dateiverschlüsselung eingesetzt werden, das das Schlüsselmaterial der Emailverschlüsselung verwenden kann.

5.7.1 Organisatorische Prozesse

Nach der Anforderung 4.3.3 soll das Produkt für die Dateiverschlüsselung mit dem Schlüsselmaterial der Emailverschlüsselung arbeiten können. Aus diesem Grund bedarf es keines neuen organisatorischen Prozesses.

Umsetzungsmöglichkeit 5.7.1 *Um die zur Dateiverschlüsselung benötigte Software zu verteilen, soll die neue Software*

- *bei neuen Clients mit Neuinstallationen mitinstalliert werden,*
- *bei vorhandenen Clients mittels SMS verteilt werden.*

5.7.2 Technische Strukturen

Um die Dateiverschlüsselung benutzen zu können, benötigt man Clientsoftware, die mit dem Schlüsselmaterial der Emailverschlüsselung arbeiten kann. Im Folgenden werden ausgewählte Produkte vorgestellt und verglichen.

Clientsoftware

Es gibt mehrere technische Möglichkeiten für die Dateiverschlüsselung. Nach der Anforderung 4.3.1 muss die Dateiverschlüsselung schlüsselbasiert erfolgen, weshalb nur entsprechende Möglichkeiten betrachtet werden. Da die Produktpalette inzwischen sehr groß ist, wird die Betrachtung hier nur auf eine kleine Auswahl eingeschränkt.

Umsetzungsmöglichkeit 5.7.2 *Bei dem Unternehmen wird als Client Microsoft Windows XP Professional eingesetzt. Dieses Betriebssystem beinhaltet auch* ***Microsoft EFS*** *(**E**ncrypted **F**ile **S**ystem). EFS ist eine von Microsoft entwickelte Lösung zur Dateiverschlüsselung. EFS arbeitet auch schlüsselbasiert, benötigt aber eins spezielles X.509 Zertifikat, welches eine eigene Erweiterung im Zertifikat hat.*

Weitere Informationen befinden sich im Internet auf den Microsoft Seiten [MSEFS02] und in [GRA05, GRA05b]

Bewertung von Microsoft EFS:

+ Schlüsselbasiert (X.509)
+ Keine Installation zusätzliches Produktes erforderlich
+ Verwendung des Zertifikatsspeicher des Betriebsystems
- Spezielles X.509 Zertifikat erforderlich
- Keine Wiederherstellung der Schlüssel möglich
- Unterstützung nur über Microsoft
- Nicht containerbasiert

Umsetzungsmöglichkeit 5.7.3 *Das Produkt* ***CryptoEx Volume*** *wurde bereits in kleinem Kreis von Pilotbenutzern getestet. Es kam bisher keine negative Rückmeldung zurück. CryptoEx Volume arbeitet schlüsselbasiert und greift auf den Schlüsselspeicher von CryptoEx Outlook zu. Dadurch wird kein erneuter Import von Cryptomaterial nötig.*

Bewertung von *CryptoEx Volume* :

+ Schlüsselbasiert (OpenPGP und X.509)
+ Kein spezielles Cryptometrial erforderlich
+ Verwendung eines gemeinsamen Schlüsselspeichers mit *CryptoEx Outlook*
+ Bereits getestet
+ Verschlüsselung für mehrere Anwender bzw. mit mehreren Schlüsseln möglich
+ Wiederbereitstellung der Schlüssel möglich
+ Containerbasiert
+ Bei unversehrter Containerdatei ist eine Wiederherstellung möglich

Umsetzungsmöglichkeit 5.7.4 *Ein weiteres Produkt ist* ***PGP Desktop****. PGP Desktop besteht aus mehreren Komponenten. Eines davon ist PGP Disk. Damit lassen sich Verzeichnisse schlüsselbasiert verschlüsseln. Weitere Informationen befinden sich auf der Seite des Herstellers:*
http://www.pgp.com/de/products/desktop/index.html

Bewertung von PGP Desktop:

+ Schlüsselbasiert (OpenPGP + X.509)
+ Kein spezielles Cryptometrial erforderlich
+ Verwendung gemeinsamer Schlüsselspeicher mit der Emailverschlüsselung
+ Verschlüsselung für mehrere Anwender bzw. mit mehreren Schlüsseln möglich
+ Wiederbereitstellung der Schlüssel möglich
+ Containerbasiert
+ Bei unversehrter Containerdatei ist eine Wiederherstellung möglich
- Nur als ganzes Softwarepaket einsetzbar

Umsetzungsmöglichkeit 5.7.5 *Das Produkt* ***SecuFile von IC Compas*** *ist ein relaitiv neues Produkt. SecuFile ist eine Laufwerksverschlüsselung mit flexiblen Sicherheitsstufen. Nachdem eine Laufwerksdatei eingerichtet wurde, steht ein zusätzliches, virtuelles Laufwerk zur Verfügung.*

Nähere Details zum Produkt können von der Herstellerseite:
http://www.ic-compas.de/index.php?page=tr_secufile
bezogen werden.

Bewertung von SecuFile:

+ Schlüsselbasiert (X.509)
+ Kein spezielles Cryptometrial erforderlich
+ Verwendung eines gemeinsamen Schlüsselspeichers mit der Emailverschlüsselung (TrustedMime)
+ Verschlüsselung für mehrere Anwender bzw. mit mehreren Schlüsseln möglich
+ Wiederbereitstellung der Schlüssel möglich
+ Containerbasiert
+ Bei unversehrter Containerdatei ist eine Wiederherstellung möglich

Nachdem die Clientprodukte für die Dateiverschlüsselung vorgestellt wurden, werden in der folgenden Tabelle die wichtigsten Eigenschaften der Produkte dargestellt und miteinander verglichen.

	Microsoft EFS	CryptoEx Volume	PGP Desktop	SecuFile
Schlüsselbasiert	Ja, X.509 Zertifikat	Ja, X.509 Zertifikat und PGP Schlüssel	Ja	Ja, X.509 Zertifikat
spezielles Schlüsselmaterial erforderlich	Ja	Nein	Nein	Nein
Zertifikatsspeicher	Betriebsystem	Eigener oder Betriebssystem	Eigener	Eigener
Verschlüsselungs-algoritmus	AES mit 256	AES mit 128/192/256 Bit	AES mit 128/192/256 Bit CAST mit 128 Bit Twofish mit 256 Bit	AES mit 256 Bit
Containerbasiert	Nein	Ja	Ja	Ja
Filesystem des virtuellen Laufwerkes	Nicht anwendbar	NTFS/FAT/FAT32	NTFS/FAT/FAT32	FAT
Verwaltung von Berechtigungen	Nicht möglich	Nur über das Filesystem nur bei NTFS	über das Filesystem bzw. Delegation von Berechtigungen	Delegation von Berechtigungen
Mehrbenutzerfähig	Beschränkt Ja, nur lokal, nicht übers Netzwerk	Ja, gleichzeitige Verwendung beschränkt* möglich wird aber nicht empfohlen	Nur über das Filesystem	Delegation von Berechtigungen
Zusammenarbeit mit anderen Produkten	Nein	Ja, mit anderen *CryptoEx* Produkten	Ja, mit anderen PGP Produkten	Ja, mit TrustedMime

Tabelle 5.4: Vergleich verschiedener Clientsoftware

Bemerkung zu der Tabelle:
*) – Die gleichzeitige Verwendung der Containerdatei von mehreren Benutzern ist nur mit Lesezugriff möglich. Es wird aber von dem Hersteller ausdrücklich nicht empfohlen.

5.8 Umsetzungsmöglichkeiten für die Dateisignatur

Da die Dateisignatur bisher keine starke Verbreitung fand, wird auf die Betrachtung hier verzichtet.

5.9 Umsetzungsmöglichkeiten für die Dokumentensignatur

Bei der Dokumentensignatur muss zwischen Datei-, Dokumenten- und Emailsignatur auf Grund der bereits vorhandenen Softwarelösungen für diese Anwendungsfälle differenziert werden. Zur Zeit gibt es keinen Softwarehersteller, der ungeachtet der Art des Dokuments eine allgemeine Lösung für die Dokumentensignatur anbietet. Im Abschnitt 5.8 wurden die Möglichkeiten für die Dateisignatur schon abgehandelt. Deshalb wird nur die Dokumentensignatur betrachtet. Microsoft bietet zwar eine Lösung für die Emailsignatur, aber nur was S/MIME betrifft. Für die Dokumenten- und Dateisignatur bietet Microsoft keine Lösung. Es gibt mehrere Produkte auch für die Dateisignatur.

Umsetzungsmöglichkeit 5.9.1 *In Deutschland gibt es das Produkt GERVA von Datev EV. Dieses Produkt wird in Verbindung mit einer zertifizierten Signaturkarte und entsprechender Hardware geliefert. Dieses Produkt richtet sich nach Angaben des Herstellers vor allem an Rechstanwälte. Diese Produkt erfüllt laut Hersteller die Vorgaben des Signaturgesetzes.*

Bewertung von GERVA:

+ Schlüsselbasiert (X.509)
- Nur in Deutschland verwendbar
- Zusätzliche Hardware (SmartCard und Lesegerät) erforderlich
- Propriotäres Dokumentenformat

Umsetzungsmöglichkeit 5.9.2 *Eine andere Möglichkeit bietet Adobe Acrobat. Damit ist eine Dokumentensignatur möglich, die nicht nur auf Deutschland beschränkt ist.*

Bewertung von Adobe Acrobat:

+ Schlüsselbasiert (X.509)
+ PDF als Dokumentenformat weit verbreitet
+ Adobe Acrobat wird bereits als optionale Software angeboten
- Qualifizierte Signatur nur in Verbindung mit entsprechender Hardware (vlg. Tabelle 2.1)
- Komplizierte Verwendung mehrerer Schlüsselspeicher
- Kein automatischer Zugriff auf den Schlüsselspeicher des Betriebssystems voreingestellt $\Rightarrow$ Probleme bei der Validierung

5.10 Umsetzungsmöglichkeit für Serverprodukte

Es wurden bisher nur die Möglichkeiten für die Clientanwendungen vorgestellt. In den folgenden Abschnitten werden die Möglichkeiten für die Serveranwendungen vorgestellt. Eine der wichtigsten serverseitigen Komponenten ist die Zertifikatsstelle (Certificate Authority). Es gab früher auf dem Markt viele Produktanbieter. Die Anzahl der Anbieter hat sich in der letzten Zeit stark reduziert. In den folgenden Abschnitten werden einige CA Produkte beschrieben und miteinander verglichen.

5.10.1 Microsoft CA

Da das Unternehmen Microsoft Produkte einsetzt, stellt sich die Frage, ob die Fähigkeiten der Mircosoft CA, die bei dem Betriebssystem Microsoft Windows 2003 Server mitgeliefert wird, für die Lösung ausreichend sind. Es gibt zwei unterschiedliche Serverprodukte: Standard und Enterprise. Diese liefern jeweils eine CA Software mit unterschiedlichem Funktionsumfang mit.

Bei der Standard CA können nur die Bestellseiten angepasst werden, ansonsten können keine Einstellungen (z. B. Änderung der Zertfikatsvorlage) vorgenommen werden.

Bei der Enterprise CA, die ungleich mehr kostet, können die Zertifikatsvorlagen angeschaut, angepasst und neue angelegt werden.

Beide CA Typen sind über die Microsoft Management Konsole zu verwalten. Während bei der Standard CA nur Zertifikate ausgestellt und widerrufen werden können, können die Zertifikatsvorlagen der Enterprise CA verwaltet werden. Dies ist besonders wichtig, wenn man angepasste X.509 V3 Zertifikate ausstellen will.

Umsetzungsmöglichkeit 5.10.1 *Die erste Umsetzungsmöglichkeit fütr die serverseitige CA Softwarelösung ist die Microsoft Enterprise Certificate Services. Da die Microsoft Enterprise CA nur X.509 Cryptomaterial generiert, muss diese CA fütr die Lösung fütr PGP Material um eine zusätzliche Software erweitert werden.*

5.10.2 OpenCA

Es gibt mehrere OpenSource CA Software, die ernstzunehmende Alternativen zu den kommerziellen Produkten sind. Die bekanntesten OpenCAs sind:

- EJBCA -http://http://ejbca.sourceforge.net
- OpenCA - http://www.openca.org
- PyCA - http://www.pyca.de/

Die EJBCA läuft auf JAVA Basis, die OpenCA basiert auf OpenSSL und Perl Modulen und die PyCA arbeitet auf OpenSSL mit Python Klassen. Weil diese OpenCAs auf Linux entwickelt werden und weil das Unternehmen Microsoft Produkte einsetzt, ist eine Portierung und Anpassung an Microsoft Windows Server und Clients erforderlich. Obwohl diese CA Software frei verfügbar sind, was die Anschaffungskosten erheblich reduziert, bietet diese Möglichkeit unter Umständen keine günstigere Alternative als

eine kommerzielle Lösung.
Weil die OpenCAs keine Out-of-the-Box Lösung für die gestellten Anforderungen anbieten, müssten die OpenCAs angepasst werden. Ein Unternehmen müsste mit der Anpassung und Wartung beauftragt werden.

Umsetzungsmöglichkeit 5.10.2 *Die zweite Umsetzungsmöglichkeit für die serverseitige PKI Software bietet eine der OpenCAs. Da alle OpenCAs nur X.509 Cryptomaterial generiern und liefern, müsste die gewählte um die Funktionalität der Generierung von PGP Cryptomaterial erweitert werden.*

Weitere und ausführliche Informationen zu OpenCA und Microsoft CA befinden sich in [BZ05].

5.10.3 PGP Enterprise CA

Die dritte Alternative ist auch ein kommerzielles Produkt. Diese CA wurde entwickelt, um beide Standards mit einer CA abdecken zu können. Diese CA liefert sowohl X.509 als auch PGP Material. Die Enterprise CA von PGP wird in diesem Abschnitt vorgestellt. Dieses Produkt setzt auf die Microsoft CA, bietet aber eine zentrale Verwaltungsoberfläche für die Cryptomaterialien, die Bestellseiten und für die Konfiguration.

Umsetzungsmöglichkeit 5.10.3 *Eine dritte Alternative bietet für die serverseitige PKI Software die Enterprise CA von PGP. Diese CA Software liefert sowohl X.509 als auch PGP Cryptomaterial.*

5.10.4 Neuentwicklung der CA Software

Da es viele zum größten Teil kommerzielle Produkte auf dem Markt gibt, aber nur wenige den Anforderungen nahe kommen, stellt sich die Frage, ob das Ausschreiben für eine an die Anforderungen angepasste Neuentwicklung einer CA Software durch ein Unternehmen die ideale Lösung wäre. Eine angepasste Neuentwicklung einer CA Software erfordert ein genaues Pflichtenheft und eine enge Zusammenarbeit mit den Entwicklern. Das Unternehmen muss sich dabei auf die Erfahrungen und Kenntnisse der Entwickler verlassen.

Umsetzungsmöglichkeit 5.10.4 *Die Neuentwicklung der CA Software bietet mit Sicherheit die ideale Lösung, da sie speziell an die Anforderungen angepasst ist. Diese Möglichkeit ist aber mit hohen Kosten verbunden.*

5.10.5 Vergleich der Produkte

Nach dem verschiedene Produkte vorgestellt wurden, werden sie miteinander verglichen. Man kann den Vergleich am besten in einer Tabelle darstellen. Die Tabelle 5.5 zeigt den Vergleich verschiedener CA Produkte.

	Micorosoft CA	OpenCA	PGP Enterprise CA	Neuentwicklung
Integration in Microsoft Umfeld	Gut	mäßig	Gut	Gut
Zusammenarbeit mit Microsoft Clients	Gut	Gut	Gut	Gut
eigene Clientsoftware	nicht erforderlich	nicht erforderlich	erforderlich	erforderlich
Zusammenarbeit mit Microsoft-eigenem Verzeichnisdienst	Gut	Gut (über LDAP)	Gut	Gut
Anpassung der Bestellseiten	erforderlich	erforderlich	erforderlich	nicht erforderlich
Admininistrations-oberfläche	Schlecht	Gut	Gut	Gut
Geliefertes Cryptomaterial	Nur X.509	Nur X.509	PGP und X.509	PGP und X.509
Anpassung des Cryptomaterials	möglich (Enterprise CA)	möglich	möglich	möglich
Anpassung des CA Produktes erforderlich	Ja, mind. die Bestellseiten	Ja, mind. die Bestellseiten	Ja, Konfiguration erforderlich	Nicht
Wartung und Support	über Microsoft	Nur über ein beauftragtes Unternehmen	Über Hersteller, mit Wartungsvertrag	Über Hersteller, mit Wartungsvertrag
Kosten	Hoch, für Microsoft Windows Enterprise Server	niedrige Anschaffungs-, hohe Anpassungskosten	Hoch	Sehr Hoch

Tabelle 5.5: Vergleichsmatrix der CA Produkte

5.11 Vertrauensmodell

Bei der Planung einer PKI spielt das Vertrauensmodell eine wichtige Rolle. Obwohl es mehrere Vertrauensmodelle gibt, lassen sich die meisten aus den zwei grundlegenden Modellen ableiten:

- Das hierarchische Modell
- Das anarchische Modell

Von den vielen Modellen werden einige in den kommenden Abschnitten vorgestellt.

5.11.1 Definition von Vertrauen

Bevor auf die verschiedenen Modelle eingegangen wird, soll das Vertrauen definiert werden. Es gibt viele Definitionen für das Vertrauen. Im Folgenden werden zwei vorgestellt. Die erste ist eine allgemeinere Definition, die andere stammt aus der Fachliteratur.

> Vertrauen ist die subjektive Überzeugung (auch Glaube) der Richtigkeit bzw. Wahrheit von Handlungen und Einsichten eines anderen oder von sich selbst (Selbstvertrauen). Zum Vertrauen gehört auch die Überzeugung der Möglichkeit von Handlungen und der Fähigkeit zu Handlungen. Das Gegenteil des Vertrauens ist das Misstrauen.
> (Quelle: http://de.wikipedia.org/wiki/Vertrauen)

> Generally, an entity can be said to „trust“ a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects.
> (Quelle: [AAL 02])

> Zuversicht, dass die andere Partei in einem Austausch nicht die eigene Verwundbarkeit ausnutzt.
> (Quelle:[KM00])

Das Vertrauen hat auch mehrere Eigenschaften, von denen mehrere für die PKI relevant sind. Einige der wichtigen Eigenschaften sind:

- Gerichtet (einseitig, gegenseitig)
- Geordnet (Misstrauen $<$ Ungewissheit $<$ Blindes Vertrauen)
- Bedingt transitiv (nimmt mit der Transitivität ab)
- An Fragestellung gebunden
- Risikoabhängig (mit ansteigendem Risiko nimmt das Vertrauen ab)
- Erfahrungsbasiert (gute Erfahrungen stärken, negative zerstören meistens in größerem Maße)

All diese Eigenschaften lassen sich natürlich nicht durch Zertifikate und Beziehungen (Hierarchien) abbilden. Diese Eigenschaften beschreiben Beziehungen, die man eingeschränkt aber modellieren kann. Kein Vertrauensmodell kann alle diese Eigenschaften

erfüllen oder modellieren. Aus diesem Grund muss man das Vertrauensmodell definieren und den Zweck eines Vertrauensmodells einschränken. Ein Vertrauensmodell besteht aus folgenden Komponenten:

- Zertifizierungsstelle(n) (CA)
- Endeinheiten
- Zertifikaten

Ein Vertrauensmodell beschreibt mit Hilfe dieser Komponenten:

- Welchen Zertifikaten vertraut werden kann
- Wie das Vertrauen mit den Elementen dieses Modells abgeleitet werden kann
- Wie das Vertrauen eingeschränkt werden kann

Eine CA ist technisch gesehen ein signiertes Zertifikat. Dabei muss zwischen Wurzel (oberste) CA und Sub CA unterschieden werden. Die Wurzel CAs haben ein selbstsigniertes Zertifikat, die Sub-CAs ein von einer anderen CA signiertes Zertifikat.
Falls ein Zertifikat weitere Zertifikate signieren kann und darf, handelt es sich dabei um eine CA. In jedem Modell gibt es mindestens eine oberste CA (Wurzel CA). Diese CA ist ein selbst signiertes Zertifikat mit der Eigenschaft, dass sie weitere Zertifikate signieren kann und darf.
Jedes Vertrauensmodell hat Schwachpunkte und kommt an das Vertrauen in dem wirklichen Leben nicht heran. Einige der wichtigsten Modelle werden im nächsten Abschnitt vorgestellt.

5.11.2 Verschiede Vertrauensmodelle:

Die hier beschriebenen Modelle verwenden den Begriff CA und Zertifikate. Dabei geht es wie in der PKI um Zertifizierungsstelle und Zertifikate. Der wichtigste Punkt ist bei jedem Modell, wie sich das Vertrauen in ein Zertifikat feststellen lässt (Validierung).

Hierarchisches Modell: Single CA

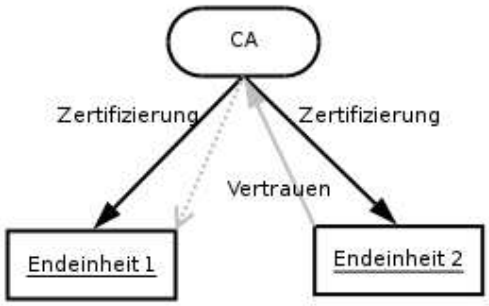

Abbildung 5.8: Hierarchisches Vertrauensmodell: Single CA

Das einfachste Modell besteht aus einer CA, die die Zertifikate ausstellt. Bei diesem Modell geht das Vertrauen über diese einzige CA. Wer dieser CA vertraut, vertraut allen Zertifikaten, die von dieser CA ausgestellt wurden.

Bewertung:

+ Nur eine CA nötig, das die Zertifikatsvalidierung erleichtert
+ Alle Teilnehmer müssen dieser einen CA trauen
- Verifikation der Daten aufwendig / unsicher (eine CA ist für alle Registrierungen zuständig)
- Kompromittierung des CA-Schlüssels hat globale Konsequenzen
- CA hat Monopolstellung

Die meisten Vertrauensmodelle lassen sich aus diesem Modell ableiten.

Hierarchisches Modell: Oligarchie von CAs

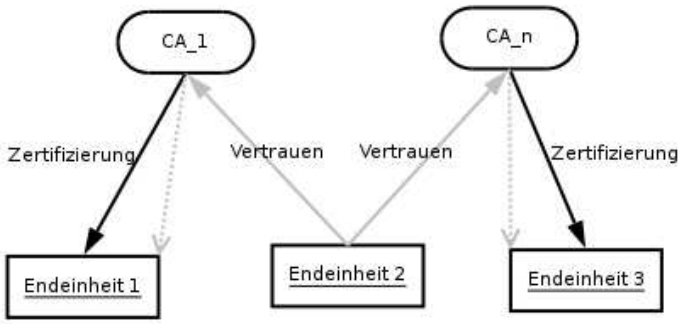

Abbildung 5.9: Oligarchie von CAs

Bei diesem Modell gibt es mehrere CAs. Jede CA stellt Zertifikate für ihre eigene Domain aus. Jede CA muss allen Clients als vertrauenswürdig bekannt sein, damit das Vertrauen hergestellt ist. Die Zertifikatsvalidierung geht hier auch über die CA, die das Zertifikat ausgestellt hat. Die Abbildung 5.9 zeigt dieses Vertrauensmodell. Im Bild bedeuten die schwarzen Pfeile die Richtung der Zertifizierung, die grauen Pfeile die Richtung des Vertrauens, wobei man zwischen direkten und indirekten Vertrauen unterscheidet. Der durchgängige Pfeil zeigt das direkte Vertrauen.

Bewertung:

+ Verifikation der zu registrierenden Daten ist sicherer (geogr. Nähe)
+ Keine Monopolstellung einer CA mehr
+ Kompromittierung hat begrenzte Auswirkung

- Initiale Prüfung mehrerer CA-Schlüssel
- Validierung mittels mehrerer CA Schlüssel
- Mehrere CA-Schlüssel müssen geschützt werden

Hierarchisches Modell: Top Down

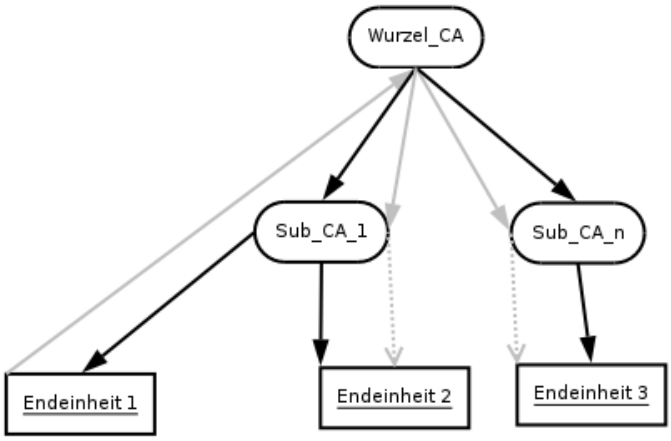

Abbildung 5.10: Hierarchisches Vertrauensmodell: Top-Down

Bei diesem Modell gibt es mehrere CAs. Es gibt eine oberste CA, die auch Wurzel CA genannt wird. Die anderen CAs befinden sich unterhalb dieser CA. Die Wurzel-CA zertifiziert die untergeordneten CAs. Jede CA (bis auf die Wurzel-CA) hat genau eine übergeordnete CA. Die untergeordneten CAs, die auch aussteller CA genannt werden, stellen die Zertifikate für die Endeinheiten aus. Die untergeordneten CAs dürfen in diesem Modell keine weiteren untergeordeneten CAs einsetzen. Die untergeordneten CAs dürfen nur Endeinheiten zertifizieren. Das Vertrauen geht immer über die CAs. Zwei Zertifikate dieses Modells vertrauen einander nur, wenn sie von derselben CA ausgestellt sind. Bei diesem Modell gibt es nur zwei CA Ebenen. In der oberste Ebene befindet sich nur die Wurzel-CA, alle anderen befinden sich in der zweiten Schicht.

Bewertung:

+ Keine Monopolstellung einer CA mehr
+ Kompromittierung der untergeordnete CA hat begrenzte Auswirkung
+ Kontrollierte Delegation
- Validierung mittels mehrerer CA Schlüssel
- Validierung des ganzen Pfades (nie One-Hop)
- Mehrere CA-Schlüssel müssen geschützt werden

Hierarchisches Modell: Top-Down mit Delegierung

Dieses Modell ist eine Erweiterung des vorherigen Modells. Die Eigenschaften des vorherigen Modells sind hier auch vorhanden. Bei diesem Modell wird die Einschränkung auf zwei Schichten durch eine Erweiterung aufgehoben. Diese Erweiterung wird bei diesem Modell durch die Einführung der Delegierung erreicht. Delegierung heißt, dass CAs untergeordnete CAs einsetzen können und dürfen. Dadurch ist die Hierarchie nicht mehr auf zwei Schichten beschränkt, sondern lässt sich erweitern. Bei diesem Modell ist streng hierarchische und lockere Vertrauensbildung möglich. Die folgende CA-Bezeichnungen müssen auch eingeführt werden:

Root-CA: Wurzel CA, oberste CA

Parent-CA: Direkt übergeordnete CA

Sub-CA: Eine untergeordnete CA

Child-CA: Eine direkt untergeordnete CA

Bewertung:

+ Komfort: mehr Zertifizierungsstellen
+ Kompromittierung eines Sub-CA-Schlüssels hat beschränkte Auswirkung
+ Nur ein Vertrauensanker muss geprüft werden
- Höhere CA-Schlüsselanzahl
- Validierung aufwändiger

Anarchisches Modell

Dieses Modell wird auch als Vertrauensnetz (Web-of-Trust) genannt. Dieses Modell ist in der PGP Welt sehr stark verbreitet. Bei diesem Modell ist jeder Anwender gleich eine CA. Die CAs zertifizieren sich gegenseitig. Dadurch wird das Vertrauen transitiv weitergereicht. Das Vertrauen an einen Schlüssel lässt sich wegen schwieriger Pfadfindung und transitivem Vertrauen mit verschiedenen Vertrauensstufen ggf. schwer nachvollziehen.

Bewertung:

+ Auswirkung bei Kompromittierung beschränkt
- Alle Schlüssel sind CA-Schlüssel
- Hohe Anzahl von Zertifikaten bzw. Signaturen
- Pfadfindung schwer, da nicht eindeutig
- Keine einheitliche Zertifizierungspolitik, somit Transitivität von Vertrauen problematisch
- Zertifizierungen nicht kontrollier- bzw. einschränkbar

5.12 Informationsrepräsentation

Wie eine PKI serverseitig aufgebaut werden soll, bestimmen mehrere Auforderungen. Bei der Planung müssen das Vertrauensmodell, die Anforderungen der Anwendungen und die Informationsrepräsentation beachtet werden. Letzteres hat Auswirkungen sowohl auf die CA Hierarchie als auch auf die Cryptomaterialien. Aus diesem Grund wird diese Problematik angesprochen.
Die Informationsrepräsentation ist ein wichtiger Aspekt, wie eine vorhandene Informationsstruktur in technischen Strukturen abgebildet werden kann. Es gibt im Prinzip drei Repräsentationsmöglichkeiten, die folgend vorgestellt werden.

5.12.1 Informationsrepräsentation in der Struktur

Die erste Möglichkeit der Repräsentation ist die Anordnung der Objekte in einer Struktur. Man kann die gleiche Informationen mit mehreren Strukturen darstellen. Die Wahl der Struktur hängt in der Regel davon ab, wie Informationen gewichtet werden. Man kann die Struktur eines Unternehmens z.B. anhand der Personalstruktur, aber auch anhand der Aufgabenbereiche darstellen. Diese beiden Darstellungen können, müssen aber nicht miteinander übereinstimmen. Es kann z.B. vorkommen, dass mehrere Abteilungen dieselbe Aufgaben haben. Auf den ersten Blick scheint es überflüssig zu sein. Ein gutes Beispiel geben die Personalabteilungen in einem internationalen Unternehmen. Im jedem Land gibt es in der Regel eine eigene Personalabteilung. Alle Personalabteilungen haben ähnliche Aufgaben, können jedoch nicht zusammengelegt werden.

5.12.2 Informationsrepräsentation im Objekt

Als nächstes gibt es die Möglichkeit, dass alle Informationen in dem Objekt selber kodiert werden. Ein gutes Beispiel dafür ist der Eintrag eines Mitarbeiters im Verzeichnisdienst. Viele unternehmensrelevante Informationen werden von einem Mitarbeiter in einem Verzeichnisdienst erfasst.

5.12.3 Informationsrepräsentation in einer Datenbasis

Die letzte erwähnte Möglichkeit für Informationsrepräsentation ist, dass das Objekt nur einen Verweis auf einen Eintrag in einer Datenbasis enthält. Die Informationen werden nicht in dem Objekt selber, sondern in der Datenbasis gehalten. Dadurch ist eine größere Flexibilität möglich.

5.12.4 Bewertung der Möglichkeiten für die Informationsrepräsentation

Die vorgestellten Möglichkeiten für die Informationsrepräsentation wurde abstrakt gehalten, weil das Problem der Informationsrepräsentation nicht nur im dem Bereich der

PKI, sondern allgemein gültig ist. In der Tabelle 5.6 werden die vorgestellten Möglichkeiten zusammenfassend miteinander verglichen.

	Informationsrepräsentation in der Struktur	Informationsrepräsentation im Objekt	Informationsrepräsentation in einer Datenbasis
Ort der Information	Struktur	Objekt	Datenbasis
zusätzliche Hilfsstruktur	nicht erforderlich	nicht erforderlich	erforderlich, Datenbasis
Schutz der Information	durch Schutz der Struktur	durch Schutz des Objektes	Schutz der Datenbasis erforderlich
Flexibilität	Schlecht, da Änderung der Struktur erforderlich	mäßig, weil das Objekt geändert werden muss oder neues Objekt erzeugt werden muss	Gut, weil nur Änderung der Daten in der Datenbasis erforderlich

Tabelle 5.6: Zusammenfassung und Bewertung der Möglichkeiten für die Informationsrepräsentation

Kapitel 6

Konzepte

In diesem Kapitel werden die verschiedene Konzepte, die zum Betreiben einer PKI unerlässlich sind vorgestellt. Es sind mehrere Konzepte für die Berechtigungen, Prozesse erforderlich. Man kann auch zwischen organisatorischen und technischen Konzepten unterscheiden. Weil die technische Konzepte die organisatorische Konzepte voraussetzen, werden zuerst die organisatorischen Konzepte beschrieben.

6.1 Berechtigungskonzept

Um die Berechtigungen beschreiben zu können, müssen zuerst Rollen definiert werden. Diesen Rollen können dann entsprechende Berechtigungen zugewiesen werden.

6.1.1 Rollen in der PKI

Nach den Forderungen 4.1.1, 4.1.2, 4.4.1, 4.4.2 bzw. nach der Darstellung der Berechtigungsmatrix (Tabelle 4.1) können folgende Rollen definiert werden:

Mitarbeiter: ist jede Person im Unternehmen, die im Corporate Directory einen gültigen Eintrag hat und auf der Gehaltsliste des Unternehmens steht. Bei diesem Mitarbeiter handelt es sich um einen Angestellten. Der Active Directory Eintrag dieses Mitarbeiters hat in einer der Eigenschaften (ExtensionAttribute) eine spezielle Zeichenkette.

Sekretärin: ist jede Mitarbeiterin, die nach dem eigenen gültigen Eintrag im Corporate Directory als Sekretärin einem Mitarbeiter/Vorgesetzter zugeordnet ist.

Vorgesetzter: ist jede Mitarbeiter, der nach mindestens einem Eintrag im Corporate Directory als Vorgesetzter gekennzeichnet ist.

LRA: ist jede Funktionskennung, in deren Emailadresse LRA vorkommt. Einer LRA Kennung ist pro Standort ein vertrauenswürdiger Mitarbeiter in der Regel der lokale Sicherheitsadministrator zugeordnet.

Zentraler Sicherheitsadministrator: ist derjenige Mitarbeiter, der in der Sicherheitsabteilung des Unternehmens für die sicherheitsrelevante Emailverschlüsselung zuständig ist. Die Rolle des zentralen Sicherheitsadministrators sollte nicht direkt an einer Mitarbeiterkennung, sondern einer Funktionskennung zugeordnet werden.

Externer Mitarbeiter: ist jede Person im Unternehmen, die im Corporate Directory keinen, aber im Globalen Adressbuch einen gültigen Eintrag mit hat und bei dem Unternehmen nicht auf der Gehaltsliste steht. Der Active Directory Eintrag dieses Mitarbeiters hat in der selben Eigenschaft, wie der Mitarbeiter (ExtensionAttribute) eine andere Zeichenkette. In der Emailadresse dieses Mitarbeiters taucht die Bezeichnung *External* auf.

Zu dem Unterschied zwischen dem globalen Adressbuch und dem Corporate Directory wird an dieser Stelle an die Bemerkung 3.1.1 verwiesen.

6.1.2 Berechtigungen

Nach dem die Rollen definiert wurden, müssen die Berechtigungen den Rollen eindeutig zugeordnet werden. Die Berechtigungen sind das Bindeglied zwischen den Rollen und den Prozessen. Durch die Berechtigung wird einem erlaubt, einen Prozess zu starten.

Berechtigungen für die Bestellung

Berechtigung 6.1.1 *Jeder Mitarbeiter ist berechtigt für sich Cryptomaterial für die Emailverschlüsselung zu beantragen.*

Berechtigung 6.1.2 *Kein Mitarbeiter, keine Sekretärin, kein Vorgesetzter und kein externer Mitarbeiter ist berechtigt für einen anderen Cryptomaterial für die Emailverschlüsselung zu beantragen.*

Berechtigung 6.1.3 *Spezielle Berechtigungen haben nur die lokale LRAs und der zentrale Sicherheitsadministrator.*

Berechtigung 6.1.4 *Die lokale LRA ist berechtigt nach einer persönlichen Authentifizierung des Mitarbeiters am gleichen Standort für einen anderen authentifizierten Mitarbeiter in Ausnahmefällen Verschlüsselungsmaterial anzufordern.*

Berechtigung 6.1.5 *Der zentrale Sicherheitsadministrator ist in Ausnahmefällen berechtigt, für Mitarbeiter auf Anforderung der Personalabteilung oder des direkten Vorgesetzten, Cryptomaterial für Emailverschlüsselung anzufordern.*

Berechtigung 6.1.6 *Jeder Mitarbeiter ist berechtigt sich ein Signaturzertifikat zu bestellen,*

(a) der im Active Directory einen gültigen Eintrag hat und

(b) dessen Active Directory Eintrag in einer der Eigenschaften (ExtensionAttribute) eine spezielle Zeichenkette hat.

In der Regel sind diese: Mitarbeiter (Angestellter), Sekretärin und Vorgesetzter.

Berechtigung 6.1.7 *Jeder Mitarbeiter ist berechtigt sich ein Authentifizierungszertifikat zu bestellen,*

(a) der im Active Directory einen gültigen Eintrag hat und

(b) dessen Active Directory Eintrag in einer der Eigenschaften (ExtensionAttribute) eine spezielle Zeichenkette hat.

In der Regel sind dies: Mitarbeiter (Angestellter), Sekretärin und Vorgesetzter.

Berechtigungen für die Wiederbereitstellung

Berechtigung 6.1.8 *Jeder Mitarbeiter ist berechtigt fitr sich die Wiederbereitstellung des eigenen Cryptomaterials zu beantragen.*

Berechtigung 6.1.9 *Kein Mitarbeiter, keine Sekretärin, kein Vorgesetzter und kein externer Mitarbeiter ist berechtigt die Wiederbereitstellung des Cryptomaterials eines anderen zu beantragen.*

Berechtigung 6.1.10 *Die lokale LRA ist berechtigt nach der persönlichen Authentifizierung des Mitarbeiters am gleichen Standort für diesen authentifizierten Mitarbeiter in Ausnahmefällen die Wiederbereitstellung des Cryptomaterials von diesem Mitarbeiter anzufordern.*

Bemerkung 6.1.1 *Cryptomaterial fitr Benutzerauthentifizierung und Signatur werden nicht wiederbereitgestellt.*

Berechtigungen für den Widerruf

Berechtigung 6.1.11 *Jeder Mitarbeiter ist berechtigt das eigene*

(a) Cryptomaterial für die Emailverschlüsselung

(b) Cryptomaterial für die Signatur

(c) Benutzerauthentifizierungszertifikat

sperren zu lassen.

Berechtigung 6.1.12 *Kein Mitarbeiter, keine Sekretärin, kein Vorgesetzter und kein externer Mitarbeiter ist berechtigt die Sperrung des Cryptomaterials eines anderen zu beantragen.*

Berechtigung 6.1.13 *Die lokale LRA ist berechtigt nach der persönlichen Authentifizierung des Mitarbeiters am gleichen Standort für diesen authentifizierten Mitarbeiter die Sperrung des Cryptomaterials diesen Mitarbeiters anzufordern.*

Berechtigung 6.1.14 *Mitarbeiter der Personalabteilung sind berechtigt bei der zentralen Sicherheitsabteilung den Widerruf des Cryptomaterials eines Mitarbeiters zu benatragen. Dies kann erforderlich sein, falls ein Mitarbeiter das Unternehmen im Unfrieden verlassen hat.*

Berechtigung 6.1.15 *Ein direkter Vorgesetzter ist berechtigt den Widerruf*

(a) des Cryptomaterials eines Mitarbeiters für die Emailverschlüsselung

(b) des Cryptomaterials eines Mitarbeiters für die Signatur

(c) Benutzerauthentifizierungszertifikat eines Mitarbeiters

zu benatragen, falls dieser Mitarbeiter das Unternehmen im Unfrieden verlassen hat.

Spezielle Berechtigungen

In Ausnahmefällen werden spezielle Berechtigungen Bei den speziellen Berechtigungen handelt es sich um Berechtigungen, die zu keiner der obigen Kategorie zugeordnet werden kann.

Berechtigung 6.1.16 *Auf Anforderung höherer Gewalt (z. B. Staatsanwaltschaft) mit einem entsprechenden Beschluß ist ausschliesslich nur der zentrale Sicherheitsadministrator in Anwesenheit des direkten Vorgesetzten berechtigt ein Cryptomaterial aus der CA bereit zu stellen (escrow). Das Cryptomaterial ist nicht dem Vertreter höherer Gewalt auszuhändigen, sondern einem vertrauenswürdigen Mitarbeiter, der mit Hilfe des Cryptomaterials die von der höheren Gewalt angeforderten verschlüsselten Unterlagen entschlüsseln kann. Dieser Mitarbeiter ist verpflichetet, eine schriftliche Erklärung der Sicherheitsabteilung zu unterschreiben, wodurch er sich zu folgendem verpflichtet:*

(a) Das nicht mehr benötigtes Cryptomaterial umgehend zu vernichten.

(b) Keine Kopie des Cryptomaterials anzufertigen.

(c) Das Cryptomaterial nicht wieder herstellbar zu löschen, falls es auf einem wiederbeschreibbares Medium (z.B. USB-Stick) gesichert wurde.

(d) Das Medium, welches das Cryptometarial enthält, zu vernichten, falls das Medium nur einmal beschreibbar (z.B. CD-R) ist.

(d) Dieser Mitarbeiter ist nicht berechtigt das Cryptometarial an Dritte weiter zu geben.

(e) Falls jemand den Mitarbeiter nach dem betreffenden Cryptometarial fragt, ist dieser verpflichetet, die Sicherheitsabteilung darüber zu informieren.

Berechtigung 6.1.17 *Die Sicherheitsabteilung ist berechtigt in Ausnahmefällen für externe Mitarbeiter Benutzerauthentifizierungszertifikat auf schriftliche Anfrage eines berechtigten internen Mitarbeiters mit der schriftlichen Zustimmung der Personalabteilung zu bestellen.*

6.2 Organisatorisches Prozesskonzept

6.2.1 Registration des Mitarbeiters

Weil die Daten aller Mitarbeiter von der Personalabteilung während der Einstellung elektronisch erfasst werden und aus Kostengründen, wird der verteilte Ansatz zur Re-

gistration verwendet. (vgl. Abschnitt 5.4.1 bzw. Tabelle 5.1) Die Mitarbeiterdaten kommen in das Personalverfahren. Ein Teil der erfassten Daten aus dem Personalverfahren kommen ins Active Directory. Da dieser Datenfluß automatisiert erfolgt, kann davon ausgegangen werden, dass diese Daten authentisch sind. Diese Daten werden nicht mehr manuell geändert. Wenn eine Änderung (z. B. Mitarbeiterin heiratet) erforderlich ist, wird die Änderung über die Personalabteilung vorgenommen und in den normalen automatisierten Datenfluß eingegeben.
Die Registration des Benutzers erfolgt nicht während des Bestellprozesses, sondern früher wärend der Einstellung in der Personalabteilung.
Die Aufgaben der Registrationsstelle wird zwischen der Personalabteilung und dem Active Directory geteilt.

6.2.2 Authentifizierung des Mitarbeiters

Da die Anmeldung der Mitarbeiter zur Intranet-Anwendungen über das persönliche Domain-Passwort von den Unternehmens-Policies als authentisch anerkannt ist, wird diese Anlmeldung über Loginname und persönliches Passwort hier zur Benutzerauthentifizierung verwendet. Jeder Benutzer identifiziert sich mit der Domainenanmeldung, mit dem persönlichen Domainlogin und authentisiert sich und mit dem persönlichen Domainpasswort. Nach erfolgreicher Authentifizierung hat der Benutzer Zugriff auf die Emails, Corporate Directory, Intranet, Extranet und andere Unternehmensbereiche.

Bemerkung 6.2.1 *Wenn der Anwender dreimal ein falsches Passwort bei der Anmeldung angegeben hat, wird das Domainkonto gesperrt. Danach hat der Mitarbeiter keinen Zugriff mehr auf persönliche und geschützte Bereiche. Die Freischaltung erfolgt erst nach einem persönlichen Anruf bei der Hotline. Der Mitarbeiter erhält eine Troubleticket-Nummer und muss dann eine Kopie seines Ausweises und die erhaltene Troubleticket-Nummer an eine von der Hotline bekanntgegebene Faxnummer senden. Danach erfolgt in der Regel die Freischaltung des Kontos.*

Bemerkung 6.2.2 *Wenn ein Benutzer seinen Windows Domainloginnamen und das zugehörige Passwort weitergibt, handelt grob fahrlässig und kann dafür haftbar gemacht werden. Jeder Mitarbeiter unterschreibt diesbezüglich eine Verpflichtungserklärung während der Einstellung.*

6.2.3 Autorisierung der Bestellung

Wenn der Mitarbeiter auf die sichere Bestellseite für Cryptomaterial geht, wird er, wie auf den meisten Intranetseiten bereits praktiziert wird, automatisiert identifiziert. Später wird darauf noch näher eingegangen.
Ob eine Bestellung autorisiert wird, hängt von der Berechtigung des Mitarbeiters und vom Schlüsselmaterial ab. Aus diesem Grund wird die Autorisierung in den einzelnen Abschnitten behandelt.

6.2.4 Schlüssel- bzw. Zertifikatsgenerierung

Nach der Autorisierung werden die zur Generierung erforderlichen Daten aus dem Active Directory geholt. Diese Daten werden dann auf der Bestellseite für das Cryptomaterial angezeigt. Der Mitarbeiter bestätigt die Richtigkeit dieser Daten. Auf der nächsten Seite kann er zwischen drei Möglichkeiten wählen:
Möchte er Schlüsselmaterial für

1. die Emailverschlüsselung
2. die Emailsignatur
3. die Benutzerauthentifizierung

bestellen.

Bemerkung 6.2.3 *Diese Auswahl gilt nur für die Mitarbeiter. Die Externen Mitarbeiter haben keine Auswahl. Sie können nur Schlüsselmaterial für die Emailverschlüsselung bestellen.*

Nach dem er eine dieser Möglichekeiten ausgewählt hat, wird der Generierungsprozess im Hintergrund bei der Zertifizierungsstelle angestossen. Dadurch wird die Zertifizierungsstelle direkt angesprochen, weshalb der Sicherheitsadministrator keinen Einfluß auf die Generierung hat. Dadurch werden die Anforderungen 4.1.3, 4.1.4, 4.1.5 erfüllt. Nachdem die Zertifizierungsstelle die Anforderung erhlaten hat, prüft sie, ob für den Mitarbeiter ein bereits gültiges Material für den gewählten Anwendungsfall ausgestellt wurde.

Bemerkung 6.2.4 *Die Zertifizierungsstelle speichert die Schlüsselmaterialien in einer externen Datenbasis verschlüsselt. In dieser Datenbasis werden die Sicherheitskopien der Schlüsselmaterialien gehalten. Von den Schlüsselmaterialien für die Emailsignatur und für die Benutzerauthentifizierung werden keine Sicherheitskopien angelegt.*

Falls für den Mitarbeiter bereits ein Schlüsselmaterial ausgeliefert wurde, kann der Mitarbeiter selber entscheiden, ob er eine Wiederbereitstellung oder einen Widerruf des eigenen Cryptomaterials vornehmen möchte. (vgl. Anforderung 4.1.6) Das ist nur für die Emailverschlüsselung anwendbar.
Nach der Generierung erhält der Benutzer die Import-PIN angezeigt, so wie es in der Anforderung 4.1.11 beschrieben wurde. Er wird auf der Seite darauf hingewiesen, dass er diese Import-PIN notieren oder ausdrucken soll.
Die Beschaffenheit des Schlüsselmaterials wir unter den technischen Aspekten behandelt.

6.2.5 Auslieferung von Schlüsselmaterialien

Die Auslieferung von Schlüsselmaterialien erfolgt out-of-band, d. h. dass eine automatisch generierte Email an die von der Registrationsstelle erhaltene Emailadresse des Bestellers mit dem Verweis auf das Schlüsselmaterial geschickt wird. Der Mitarbeiter besucht diese sichere Seite, wo er das Schlüsselmaterial erhält. Damit werden

Passwortbrief und Datenträger als Gefahrenquelle eliminiert, die auch in den Anforderungen 4.1.8 und 4.1.9 festgehalten wurde. Die Seite, wo der Mitarbeiter das Cryptomaterial erhält, ist nur einmal aufrufbar. Bei dem zweiten Aufruf wird der Hinweis angezeigt, dass das Cryptomaterial bereits geholt wurde. Auf dieser Seite werden auch die Kontaktdaten der Sicherheitsabteilung angezeigt, damit ein Missbrauch gemeldet werden kann.
Eine zusätzliche Sicherheit kann durch die explizite Zustimmung der zentralen bzw. lokalen Sicherheitsadministrator eingebaut werden. In diesem Fall kann der Benutzer zwar Zertifikate bestellen, erhält aber solange keine Email, bis der Sicherheitsadministrator der Bestellung nicht zustimmt.

6.2.6 Veröffentlichung der Schlüsselmaterialien

Nach dem der Benutzer das Auslieferung von Schlüsselmaterial geholt hat, wird das öffentliche Teil des Cryptomaterials in das Zertifikatsrepository veröffentlicht. Für diesen Zweck muss keine extra Datenbasis eingerichtet werden, da für diesen Zweck das Active Directory verwendet werden kann (Siehe dazu Anforderung 4.1.13).

6.2.7 Sicherung von Schlüsselmaterial (Backup)

Nach der Generierung wird eine zentrale Sicherheitskopie des Schlüsselmaterials für die Emailverschlüsselung in der Datenbasis der Zertifizierungsstelle nach Anforderung 4.1.7. angelegt. In dieser Datenbasis werden die Sicherheitskopien der Schlüsselmaterialien gehalten. Vom Schlüsselmaterial für die Emailsignatur und für die Benutzerauthentifizierung werden keine Sicherheitskopien angelegt.
Die Datenbasis, die die verschlüsselten Cryptomaterialien speichert, wird regelmäßig gesichert.
Die in der Datenbasis gespeicherten Cryptomaterialien dürfen nur über die Zertifizierungsstelle erhalten werden. Damit kein Export von Cryptomaterialien aus der Datenbasis erfolgen kann, muss die Datenbasis verschlüsselt gehalten werden.

6.2.8 Import von Schlüsselmaterial

Der Import von Schlüsselmaterial erfordert keine speziellen Kenntnisse, sondern nur die Eingabe der Import-PIN. Die Import-PIN wurde während der Bestellung angezeigt. Während dem Importvorgang wird der Mitarbeiter aufgefordert ein Passwort für das Schlüsselmaterial zu vergeben. Danach kann der Mitarbeiter die Emailverschlüsselung verwenden und mit anderen verschlüsselt Informationen austauschen. Falls er noch Fragen hat, kann er sich an die Sicherheitsabteilung wenden.

6.2.9 Ablauf von Schlüsselmaterial

Jedes Schlüsselmaterial hat eine zeitlich begrenzte Lebens- bzw. Gültigkeitsdauer. Wenn diese Grenze überschritten wird, wird das Zertifikat ohne jegliche Aktion ungültig. Ob diese Grenze überschritten wurde, erfolgt während der Validierung auf dem Client.

Bemerkung 6.2.5 *Auf einen Update des Schlüsselmaterials, der im Prinzip möglich ist, wird aus Sicherheitsgründen verzichtet.*

6.2.10 Widerruf von Schlüsselmaterial

Falls ein Mitarbeiter sein eigenes Cryptomaterial widerrufen möchte, kann er dies über die Bestellseite nach erfolgreichen Identifizierung und Authentisierung für das eigene Schlüsselmaterial vornehmen. Nur der Mitarbeiter selber kann beurteilen, ob das eigene Schlüsselmaterial in fremde Hände geraten sein könnte. Falls dieser Fall nicht auszuschließen ist, muss der Mitarbeiter sein bisheriges Schlüsselmaterial widerrufen und sich ein neues Schlüsselmaterial bestellen.

6.3 Technisches Prozesskonzept

Weil die Bestellprozesse in den Anwendungsfällen einen gemeinsamen Teil haben, wird dieser Teil hier behandelt.

Der erste Teil der Bestellung ist die Authentifizierung der Mitarbeiter. Dieser Vorgang wird in der Abbildung 6.1 dargestellt. Der Mitarbeiter ruf die Bestellseite für Cryptomaterial im Intranet auf. Wenn der Mitarbeiter diese sichere Seite aufruft, wird er mit Hilfe der Microsoft integrierten Authentifizierung authentifiziert. Dies geschieht im Hintergrung mit Hilfe des Active Directory. Dieses Verfahren benötigt eine reine Microsoft Infrastruktur (Microsoft Internet Explorer 5, Microsoft Internet Information Server 6, Microsoft Windows 2003 Server SP1, Microsoft Active Directory).
Die zusätzliche Passworteingabe ist nur als zusätzlicher Schutz und Sicherheit gedacht. Das Passwort wird nicht durch das Netzwerk gesendet, sondern nur ein Hashwert. [MSIWA] Wenn das persönliche Passwort falsch eingegeben wird, wird ein Hinweis angezeigt, dass das Benutzerkonto nach drei Fehlversuchen gesperrt wird. Siehe dazu die Bemerkung 6.2.1.
Mehr Informationen zur Microsoft Windows integrierten Authentifizierung sind in [MSTNIWA] zu finden.

Nachdem der Mitarbeiter authentifiziert wurde, werden die Daten des Mitarbeiters, die im Hintergrund aus dem Active Directory geholt wurden und auf der sicheren Webseite angezeigt. Diese Daten sind:

- Nachname, Vorname
- Abteilung
- Emailadresse
- ID des Mitarbeiters

Um zum dem nächsten Schritt der Bestellung kommen zu können, muss der Mitarbeiter diese Daten bestätigen. Damit erklärt der Mitarbeiter zusätzlich, dass er persönlich vor dem Rechner sitzt und das die angezeigten Daten zutreffend und richtig sind. Wenn die Daten nicht richtig sind, kann er die Korrektur der Daten in der Personalabteilung beantragen.
Auf der nächsten Seite kann er zwischen den verschiedenen Schlüsselmaterialien wählen:

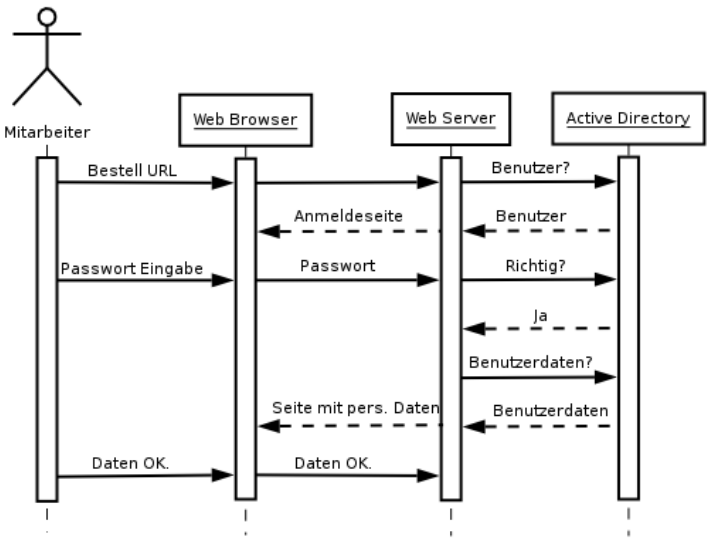

Abbildung 6.1: Benutzerauthentifizierung bei der Bestellung

- Schlüsselmaterial für die Emailverschlüsselung
- Schlüsselmaterial für die Benutzerauthentifizierung
- Schlüsselmaterial für die digitale Signatur

Wie es schon im Abschnitt 6.2.4 beschrieben ist, stehen alle diese drei Möglichkeiten nur für die Mitarbeiter zur Verfügung. Die externen Mitarbeiter haben keine Auswahl, sie können nur Schlüsselmaterial für die Emailverschlüsselung bestellen. Die Mitarbeiter werden anhand der Eigenschaft ExtensionAttribute des Eintrages im Active Directory erkannt werden. (vgl. 6.1.1). Anhand dieser Eigenschaft kann man die angezeigte Auswahl steuern.

Wenn der Mitarbeiter auf die nächste Seite geht, werden die Daten im Hintergrund

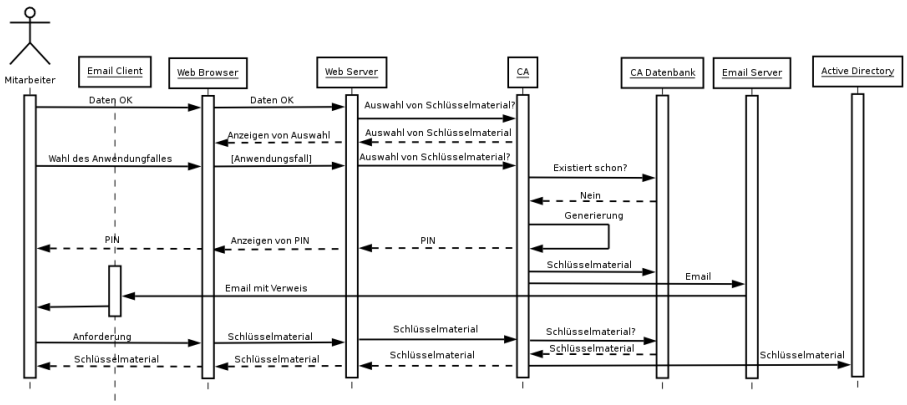

Abbildung 6.2: Generierung, Auslieferung und Veröffentlichung von Schlüsselmaterial

zu der Zertifizierungsstelle mit Anforderung für ein neues Schlüsselmaterial für die Emailverschlüsselung auf sicherem Kanal weitergereicht. Die Zertifizierungsstelle generiert im Hintegrund das Schlüsselmaterial anhand der erhaltenen Daten für diesen Mitarbeiter und gibt als Antwort die Import-PIN oder den Hinweis zurück, dass ein Schlüsselmaterial für diesen Mitarbeiter bereits ausgestellt wurde. Die Zertifizierungsstelle legt eine verschlüsselte Sicherheitskopie des Schlüsselmaterials (Key-Backup) in der eigenen Datenbasis der Zertifizierungsstelle an.
Wenn die Import-PIN angezeigt wurde, sendet die Zertifizierungsstelle eine automatisch generierte Email mit dem Verweis auf das Schlüsselmaterial.
Wie schon im Abschnitt 6.2.5 beschrieben wurde, kann eine zusätzliche Sicherheit durch eine erforderliche Zustimmung eines lokalen/zentralen Sicherheitsadministrators eingestellt werden.

6.4 Konzept für die Emailverschlüsselung

Weil der Anwendungsfall der Emailverschlüsselung der aufwendigste ist, wird zuerst das Konzept hierfür entwickelt. Nachdem der Anwendungsfall der Emailverschlüsselung in Kapitel 3.1 ausführlich beschrieben und bewertet wurde, kann mit Hilfe der Umsetzungsmöglichkeiten ein neues Konzept entworfen werden. Zuerst müssen die organisatorischen Angelegenheiten geklärt werden, danach kann die Technik entsprechend gestaltet werden.

6.4.1 Konzept für die Bestellung von Cryptomaterial für Emailverschlüsselung

Der Anwendungsfall Emailverschlüsselung muss, wie jeder Anwendungsfall, genau geplant und organisiert werden. Die beteiligten Personen, deren Berechtigung und deren Aufgabe müssen klar definiert werden, damit der Ablauf möglichst nur deterministisch erfolgen kann. Ein allgemeines Prozesskonzept wurde schon in dem Abschnitt 6.2 beschrieben. Aus diesem Grund werden hier nur die Unterschiede beschrieben.

An der Emailverschlüsselung beteiligten Personen

Im Abschnitt 6.1.1 wurden bereits die Rollen und im Abschnitt 6.1.2 die Berechtigungen definiert. Die dort beschriebenen sind ohne Einschränkung für die Emailverschlüsselung gültig.

Autorisierung des Benutzers bzw. der Bestellung

Nach der Anforderung 4.1.1 soll jeder Mitarbeiter an der Emailverschlüsselung teilnehmen. Da im Unternehmen jeder Mitarbeiter ohne Beschränkung für sich selber Emailverschlüsselungsmaterial nach Abschnitt 6.1.2 bestellen darf, kann die Bestellung nach erfolgreicher Authentifizierung des Mitarbeiters autorisiert werden.

Schlüssel- bzw. Zertifikatsgenerierung

Die Schlüsselgenerierung erfolgt ohne Eingriff des Sicherheitsadministrators in einer sicheren Umgebung, wie es in dem Abschnitt 6.2.4 beschrieben ist. Nach der Generierung erhält der Benutzer die Import-PIN angezeigt, so wie es in der Anforderung 4.1.11 beschrieben wurde. Er wird auf dieser Seite darauf hingewiesen, dass er diese Import-PIN notieren oder ausdrucken soll.
Die Beschaffenheit des Schlüsselmaterials wird unter den technischen Aspekten behandelt.

Auslieferung von Schlüsselmaterialien

Die Auslieferung von Schlüsselmaterialien erfolgt Out-Of-Band, d. h. dass eine automatisch generierte Email an die von der Registrationsstelle erhaltene Emailadresse des Bestellers mit dem Verweis auf das Schlüsselmaterial geschickt wird. Der Mitarbeiter besucht diese sichere Seite, wo er das Schlüsselmaterial erhält. Damit werden Passwortbrief und Datenträger als Gefahrenquelle eliminiert, wie es auch in den Anforderungen 4.1.8 und 4.1.9 festgehalten wurde. Die Seite, wo der Mitarbeiter das Cryptomaterial erhält, ist nur einmal aufrufbar. Bei dem zweiten Aufruf dieser Seite wird der Hinweis angezeigt, dass das Material bereits abgeholt wurde. Auf dieser Seite werden auch die Kontaktdaten der Sicherheitsabteilung angezeigt, damit ein Missbrauch gemeldet werden kann.

6.4.2 Konzept für die Verwendung von Cryptomaterial für Emailverschlüsselung

Nach dem die Schlüsselmaterialien generiert und verteilt wurden, müssen diese importiert und verwendet werden. Diese Vorgänge werden in diesem Abschnitt beschrieben.

Import von Schlüsselmaterial

Der Import von Schlüsselmaterial erfordert keine speziellen Kenntnisse, sondern nur die Eingabe der Import-PIN. Die Import-PIN wurde während der Bestellung angezeigt. Während des Importvorgangs wird der Mitarbeiter aufgefordert ein Passwort für das Schlüsselmaterial zu vergeben. Danach kann der Mitarbeiter die Emailverschlüsselung verwenden und mit anderen verschlüsselt Informationen austauschen. Falls er noch Fragen hat, kann er sich an die Sicherheitsabteilung wenden.

6.4.3 Wiederbereitstellung von Schlüsselmaterial

Falls ein Mitarbeiter eine Wiederbereitstellung benötigt, kann er über die Bestellseite nach erfolgreicher Identifizierung und Authentisierung die Wiederbereitstellung für das eigene Schlüsselmaterial für die Emailverschlüsselung anfordern. (vgl. 6.2.7) Während der Wiederbereitstellung erhält der Mitarbeiter das bereits abgelaufene oder widerrufene Schlüsselmaterial (Historie des Schlüsselmaterials) auch. Die Wiederbereitstellung des eigenen Schlüsselmaterials ist möglich, wenn auszuschließen ist, dass das

Schlüsselmaterial in unbefugte Hände geraten sein kann. Das kann der Fall sein, falls der Rechner des Mitarbeiters neu installiert wurde.

6.4.4 Bereitstellung von Schlüsselmaterial (escrow)

Die Berechtigungen für die Bereitstellung von Schlüsselmaterial (escrow) wurden im Abschnitt *Spezielle Berechtigungen* behandelt. Weil der zentrale Sicherheitsadministrator die einzige Person ist, der unter Aufsicht Schlüsselmaterial bereitstellen kann, kann es nur über die Administrationsoberfläche der Zertifizierungsstelle vorgenommen werden.

6.4.5 Ablauf und Widerruf von Cryptomaterial für Emailverschlüsselung

Der Lebenszyklus eines Schlüsselmaterials kann auf zwei Arten enden. Entweder läuft das Schlüsselmaterial ab, weil es die Obergrenze der Gültigkeit überschritten hat, oder weil es widerrufen wurde.
Jedes Schlüsselmaterial hat eine zeitlich begrenzte Lebens- bzw. Gültigkeitsdauer. Falls diese Grenze überschritten wird, wird das Zertifikat ohne jegliche Aktion ungültig. Die Prüfung, ob diese Grenze überschritten wurde, erfolgt während der Validierung auf dem Client.
Falls ein Mitarbeiter sein eigenes Cryptomaterial widerrufen möchte, kann er es über die Bestellseite nach erfolgreicher Identifizierung und Authentisierung für das eigene Schlüsselmaterial vornehmen. (vgl. Abschnitt 6.2.10)

6.4.6 Technisches Konzept für die Emailverschlüsselung

In diesem Abschnitt werden die technischen Aspekte für die Emailverschlüsselung beschrieben. Als erstes werden die technischen Aspekte der Prozesse beschrieben.

Technische Aspekte der Bestellung

Der Bestellprozess für Bestellung von Schlüsselmaterial für die Emailverschlüsselung wurde bereits im Abschnitt 6.4.1 beschrieben. Hier werden nur die technische Aspekte berschrieben.

Beschreibung der Registrationsstelle

In dem Abschnitt 6.2.1 wurde bereits die Registrationsstelle beschrieben. Nach dem sich der Mitarbeiter in der Personalabteilung mittels seiner Zeugnisse und persönlichen Unterlagen identifiziert hat, werden die Daten zuerst im Personalverfahren erfasst. Von dort erfolgt eine Übernahme in das Active Directory übernommen. Der genaue Datenfluß der Mitarbeiterdaten wurde bereits in der Abbildung 3.7 gezeigt. Weil dieses Datentransfer automatisiert erfolgt, sind diese Daten als authentisch anzusehen. Das Active Directory dient deshalb zur Grundlage für die Benutzerauthentifizierung. Der

Vorteil von Active Directory ist, dass es mit Hilfe des LDAP Protokolls abgefragt werden kann.

Technische Aspekte der Bestellung

Der Bestellprozess wurde im Allgemeinen im Abschnitt 6.3 beschrieben. Diese Beschreibung geht bis zu der Anzeige der Import-PIN.
Falls der Mitarbeiter bei der Bestellung eines Schlüsselmaterials für die Emailverschlüsselung hat, kommt es nicht zu der Anzeige der Import-PIN, sondern ein Hinweis wird angezeigt, dass er bereits Schlüsselmaterial für die Emailverschlüsselung hat. Auf dieser Seite kann der Mitarbeiter zwischen:

(a) einer Wiederbereitstellung des eigenen Schlüsselmaterials

(b) dem Widerruf des eigenen Schlüsselmaterials

wählen. Auf dieser Seite wird der Unterschied zwischen den beiden Möglichkeiten beschrieben. Die Wiederbereitstellung wird in dem nächsten Abschnitt behandelt.
Falls der Mitarbeiter noch kein Schlüsselmaterial hat, kommt er auf die letzte Seite, auf der die Import-PIN angezeigt wird.
Nach kurzer Zeit erhält der Mitarbeiter eine Email von der Zertifizierungsstelle, worin sich ein Verweis auf das Schlüsselmaterial befindet. Nachdem der Mitarbeiter diese Email erhalten hat, kann er auf die sichere Intranetseite gehen, um das Schlüsselmaterial zu holen. Er kann das Schlüsselmaterial holen und gleich importieren, wobei er die während des Importvorganges angezeigte PIN eingeben muss. Bevor der Importvorgang abgeschlossen wird, muss der Mitarbeiter ein persönliches Passwort für das Schlüsselmaterial wählen. Das Passwort muss den Firmenvorschriften folgen, d. h. es muss aus mindestens 8 Zeichen bestehen, kleine und große Buchstaben und mindestens ein Sonderzeichen beinhalten.
Nach dem der Mitarbeiter das Schlüsselmaterial geholt hat, veröffentlicht die Zertifizierungsstelle das öffentliche Schlüsselmaterial. Dadurch wird die verschlüsselte Kommunkikation zwischen diesem Mitarbeiter und den anderen sowie den Geschäftspartnern ermöglicht.

Technische Aspekte der Wiederbereitstellung

Weil es eine Wiederbereitstellung nur für die Emailverschlüsselung gibt, wird sie nur hier beschrieben.
Wenn der Mitarbeiter sein Schlüsselmaterial versehentlicht löscht oder es beschädigt wird, kann er über die Bestellseite nach erfolgreicher Authentifizierung eine Wiederbereitstellung anfordern. Dieser Prozess wurde bereits in dem vorherigen Abschnitt angesprochen.
Die Wiederbereitstellung wird nur durch die Führung einer Sicherheitskopie und Historie des Schlüsselmaterials ermöglicht.
Der Mitarbeiter geht auf die Bestellseite und authentifiziert sich wie im dem Bestellprozess. Er bestätigt seine Daten und erst danach kann er die Wiederbereitstellung auswählen. Dem Mitarbeiter wird eine Import-PIN angezeigt, womit er in der Lage ist, das Schlüsselmaterial zu importieren.
In dieser Zeit holt die Zertifizierungsstelle das Schlüsselmaterial des Mitarbeiters aus

der Datenbasis (Schlüssel-Archiv), entschlüsselt es und stellt es auf einer sicheren Seite zum einmaligen Abholen bereit.
Der Mitarbeiter erhält eine Email mit dem Verweis, wo er das Schlüsselmaterial holen kann. Ab diesem Punkt läuft es genauso ab wie beim Importvorgang nach einer normalen Bestellung.

Technische Aspekte des Widerrufes von Schlüsselmaterial

Wenn das Schlüsselmaterial die Obergrenze seiner Gültigkeit noch nicht erreicht hat, kann es widerrufen werden. Fall die Obergrenze seiner Gültigkeit bereits erreicht ist, kann es im Prinzip auch widerrufen werden, obwohl das Schlüsselmaterial an sich nicht mehr verwendbar ist. (Das setzt aber eine Clientsoftware mit vernünftiger Schlüsslelvalidierung voraus.)
Wenn der Mitarbeiter sich sicher, dass die Möglichkeit besteht, dass das Schlüsselmaterial missbraucht werden könnte, kann er über die Bestellseite nach erfolgreicher Authentifizierung sein eigenes Schlüsselmaterial widerrufen.
Nachdem über die technische Aspekte der Prozesse geschrieben wurde, wird die Beschaffenheit des Schlüsselmaterials bestimmt.

Eigenschaften des Schlüsselmaterials für die Emailverschlüsselung

Nach der Anforderung 4.1.1 müssen beide Standards PGP und S/MIME unterstützt werden. Aus diesem Grund müssen beide Schlüsselmaterialien beschrieben werden. Zuerst werden die Eigenschaften des PGP Schlüsselpaares definiert. Diese sind in der Tabelle 6.1 zusammengefasst.

Schlüsseleigenschaften	
Anzeigename	[Name],[Vorname]
Emailadresse	[Vorname].[Nachname]@[Unternehmensdomain].[TopLevelDomain]
Schlüsselalgorithmus	RSA Algorithmus
Schlüssellänge	1024 bit
Lebensdauer	2 Jahre

Tabelle 6.1: Eigenschaften des neuen PGP Schlüsselpaares

Als nächstes werden die Eigenschaften des X.509 Zertifikats für Emailverschlüsselung

anhand der Anforderungen festgelegt. Diese Eigenschaften sind in der Tabelle 6.4 zusammengefasst.

X.509 Zertifikat für die Emailverschlüsselung	
Schlüssellänge	1024 Bit
Schlüsselalgorithmus	RSA
Zertifikatsverwendungszweck** (Key Usage)	Data Encipherment
erweiterter Zertifikatsverwendungszweck** (Extended Key Usage)	Secure Email*
Subject	O = [Name des Unternehmens] CN = [Mitarbeitername] Email = [Emailadresse des Mitarbeiters]
Lebensdauer	2 Jahre

Tabelle 6.2: Beschaffenheit des X.509 Zertifikats für die Emailverschlüsselung

Bemerkungen zu der Tabelle:
*) – in der Fachliteratur von Microsoft wird es als SecureEmail, in anderen Fachliteraturen als *Email Protecion* bezeichnet. Dabei handelt es sich aber um die gleiche Erweiterung.
**) – diese Erweiterungen werden als kritisch markiert. Dadurch wird gewährleistet, dass das Schlüsselmaterial nur zur Emailverschlüsselung verwendet werden kann.

Auswahl der Clientsoftware für die Emailverschlüsselung

Wenn man die Tabelle 5.2 und den folgenden Vergleich betrachtet, ergeben sich nur zwei Möglichkeiten für die Clientsoftware. Die anderen Ansätze (Gateway bzw. Proxylösung) werden nicht betrachtet, weil diese eine Umstellung und dadurch höheren Migrationsaufwand verursachen.
Obwohl *CryptoEx Outlook* und *TrustedMime* den gleichen Funktionsumfang bieten, empfiehlt sich der Einsatz von *CryptoEx Outlook Version 3*, weil das Unternehmen bereits *CryptoEx Outlook* einsetzt. Der Einsatz von *CryptoEx Outlook Version 3* ist nur ein Upgarde. Die Verteilung dieses Upgrades verursacht keine große Umstellung

für die Anwender und kein aufwendige Migration.

6.5 Konzept für die Emailsignatur

Die Emailsignatur benötigt ein anderes Konzept als die Emailverschlüsselung, weil nur die internen Mitarbeiter Emails signieren dürfen. Daraus ergibt sich, dass der Kreis der berechtigten Mitarbeiter an der Emailsignatur kleiner im Vergleich zu der Emailverschlüsselung ist.

6.5.1 Organisationskonzept für die Bestellung von Cryptomaterial für Email-signatur

Die Rollen, die in dem Abschnitt 6.1.1 definiert wurden, sind hier auch gültig. Wie schon erwähnt muss bei diesem Anwendungsfall zwischen internem Mitarbeiter und externem Mitarbeiter differenziert werden. In dem Abschnitt 6.1.2 wurde auch der Kreis der Berechtigten beschrieben.

Berechtigung 6.5.1 *Nach der Berechtigung 6.1.6 können nur interne Mitarbeiter Emailsignatur verwenden.*

Berechtigung 6.5.2 *In einzelnen Ausnahmefällen kann Cryptomaterial für Emailsignatur für einen externen Mitarbeiter auf schriftliche Anfrage der Führungskraft dieses externen Mitarbeiters bei der Sicherheitsabteilung bestellt werden.*

Nach der Anforderung 4.2.1 sollen Mitarbeiter Emails signieren können. Die Bestellung läuft genauso ab, wie es in den Abschnitten 6.2 und 6.3 beschrieben ist. Nach dem Bestellvorgang bekommt der Mitarbeiter die Import-PIN angezeigt. Kurze Zeit später erhält er von der Zertifizierungsstelle eine Email mit dem Verweis auf das Schlüsselmaterial für die Emailsignatur. Er kann das Schlüsselmaterial nur mit Hilfe der Import-PIN importieren. Vor dem Abschluß des Importvorganges wird der Mitarbeiter aufgefordert ein persönliches Passwort für das Schlüsselmaterial zu vergeben. Das Passwort muss die Firmenvorschriften folgen, d. h. es muss aus mindestens 8 Zeichen bestehen und muss kleine und große Buchtaben bzw. mindestens ein Sonderzeichen beinhalten.
Der Mitarbeiter kann dann mit der Eingabe dieses Passwortes die Emails signieren.

6.5.2 Technisches Konzept für die Emailsignatur

In diesem Abschnitt werden die technische Aspekte für die Emailverschlüsselung beschrieben. Als erster werden die technische Aspekte der Prozesse beschrieben.

Technische Aspekte der Bestellung

Weil der Bestellprozess für Schlüsselmaterial für die Emailsignatur wurde bereits im Abschnitt 6.4.1 beschrieben wurde, werden hier nur die technische Aspekte behandelt. In der technischen Anforderung 4.2.3 wurde der Verzicht auf eine zentrale Sicherung

beschrieben. Weil es nach der Anforderung keine zentrale Kopie des Schlüsselmaterials für die Signatur nach der Generierung angelegt wird, ist eine Wiederbereitstellung nicht möglich.

Technische Aspekte der Bestellung

Der Bestellprozess im Allgeminen wurde in dem Abschnitt 6.3 beschrieben. Diese Beschreibung geht bis zu der Anzeige der Import-PIN. Falls der Mitarbeiter bei der Bestellung bereits Schlüsselmaterial für die Emailsignatur hat, kommt es nicht zu der Anzeige der Import-PIN, sondern ein Hinweis wird angezeigt, dass er bereits Schlüsselmaterial für die Emailsignatur hat. Auf dieser Seite kann der Mitarbeiter sein Schlüsselmaterial für die Emailsignatur widerrufen.
Falls der Mitarbeiter noch kein Schlüsselmaterial hat, kommt er auf die letzte Seite, auf der die Import-PIN angezeigt wird.
Nach kurzer Zeit erhält der Mitarbeiter eine Email von der Zertifizierungsstelle, worin sich ein Verweis auf das Schlüsselmaterial befindet. Nachdem der Mitarbeiter diese Email erhalten hat, kann er auf die sichere Intranetseite gehen, um das Schlüsselmaterial zu holen. Er kann das Schlüsselmaterial holen und gleich importieren, wobei er die während dem Importvorgang angezeigte PIN eingeben muss. Bevor der Importvorgang abgeschlossen wird, wird der Mitarbeiter gebeten, ein persönliches Passwort für das Schlüsselmaterial zu wählen. Das Passwort muss die Firmenvorschriften folgen, d. h. es muss aus mindestens 8 Zeichen bestehen und muss kleine und große Buchtaben bzw. mindestens ein Sonderzeichen beinhalten.
Nachdem der Mitarbeiter das Schlüsselmaterial geholt hat, veröffentlicht die Zertifizierungsstelle das öffentliche Schlüsselmaterial. Dadurch wird die verschlüsselte Kommunkikation zwischen diesem Mitarbeiter und den anderen sowie den Geschäftspartnern ermöglicht.

Technische Aspekte für den Widerruf von Schlüsselmaterial

Wenn das Schlüsselmaterial die Obergrenze seiner Gültigkeit noch nicht erreicht hat, kann es widerrufen werden. Falls die Obergrenze seiner Gültigkeit bereits erreicht ist, kann es im Prinzip auch widerrufen werden, obwohl das Schlüsselmaterial an sich nicht mehr verwendbar ist. (Das setzt aber eine Clientsoftware mit vernünftiger Schlüsselvalidierung voraus.)
Wenn der Mitarbeiter sich sicher ist, dass die Möglichkeit besteht, dass das Schlüsselmaterial missbraucht werden könnte, kann er über die Bestellseite nach erfolgreicher Authentifizierung sein eigenes Schlüsselmaterial widerrufen.

- Der PGP Schlüssel für die Emailsignatur wird widerrufen und veröffentlicht.
- Die Seriennummer des Zertifikats für die Emailsignatur kommt in die Zertifikatssperrliste, die von der Zertifizierungsstelle regelmäßig veröffentlicht wird.

Nachdem über die technischen Aspekte der Prozesse geschrieben wurde, wird die Beschaffenheit des Schlüsselmaterials bestimmt.

Eigenschaften des Schlüsselmaterials für die Emailsignatur

Nach der Anforderung 4.2.2 müssen beide Standards PGP und S/MIME unterstützt werden. Aus diesem Grund müssen beide Schlüsselmaterialien beschrieben werden. Zuerst werden die Eigenschaften des PGP Schlüsselpaares definiert. Diese sind in der Tabelle 6.3 dargestellt.

Schlüsseleigenschaften	
Anzeigename	[Name],[Vorname]
Emailadresse	[Vorname].[Nachname]@[Unternehmensdomain].[TopLevelDomain]
Schlüsselalgoritmus	RSA Algorithmus
Schlüssellänge	1024 bit
Lebensdauer	1 Jahr

Tabelle 6.3: Eigenschaften des neuen PGP Schlüsselpaares

Als nächstes werden die Eigenschaften des X.509 Zertifikats für Emailsignatur anhand der Anforderungen festgelegt. Diese Eigenschaften sind in der Tabelle 6.4 zusammengefasst.

Auswahl der Clientsoftware

Weil die gleiche Clientsoftware für die Emailsignatur, wie für die Emailverschlüsselung verwendet wird, wird an dieser Stelle auf den Abschnitt *Auswahl der Clientsoftware für die Emailverschlüsselung* verwiesen.

6.6 Konzept für die Benutzerauthentifizierung

Der Anwendungsfall Benutzerauthentifizierung wird in diesem Abschnitt beschrieben. Dabei wird oft auf die allgemeine Konzepte am Anfang dieses Kapitels verwiesen.

X.509 Zertifikat für die Emailsignatur	
Schlüssellänge	1024 Bit
Schlüsselalgoritmus	RSA
Zertifikatsverwendungszweck* (Key Usage)	Non Repudiation Digital Signature
Subject	O = [Name des Unternehmens] CN = [Mitarbeitername] Email = [Emailadresse des Mitarbeiters]
Lebensdauer	1 Jahr

Tabelle 6.4: Beschaffenheit des X.509 Zertifikats für die Emailsignatur

Bemerkungen zu der Tabelle:
*) – diese Erweiterungen werden als kritisch markiert. Dadurch wird gewährleistet, dass das Schlüsselmaterial nur zur Emailsignatur verwendet werden kann.

6.6.1 Organisatorisches Konzept für die Benutzerauthentifizierung

Der Kreis der beteiligten Personen ist bei diesem Anwendungsfall ein anderer als bei der Emailverschlüsselung. Die im Abschnitt 6.1.1 definierten Rollen und die im Abschnitt 6.1.2 definierten zugehörigen Berechtigungen sind auch für diesen Anwendungsfall gültig. Bei diesem Anwendungsfall bekommt der Unterschied zwischen Mitarbeiter und externem Mitarbeiter eine Bedeutung. Während Mitarbeiter (Angestellte) die Benutzerauthentifizierung nutzen und sich somit z. B. an Intranetapplikationen anmelden können, dürfen externe Mitarbeiter dies nicht.

Berechtigung 6.6.1 *Nach der Berechtigung 6.1.7 nehmen nur interne Mitarbeiter an der Benutzerauthentifizierung teil.*

Berechtigung 6.6.2 *In einzelnen Ausnahmefällen kann ein Authentifizierungszertifikat für einen externen Mitarbeiter auf schriftliche Anfrage der Führungskraft dieses externen Mitarbeiters bei der Sicherheitsabteilung bestellt werden.*

Nach der Anforderung 4.4.1 und 4.4.2 sollen nur Mitarbeiter (Angestellte) ein Authentifizierungszertifikat bestellen können. Die Bestellung läuft genauso ab, wie es in den Abschnitten 6.2 und 6.3 beschrieben ist.
Nach dem Bestellvorgang bekommt der Mitarbeiter die Import-PIN angezeigt. Kurze Zeit später erhält er von der Zertifizierungsstelle eine Email mit dem Verweis auf das

Authentifizierungszertifikat. Er kann das Schlüsselmaterial nur mit Hilfe der Import-PIN importieren. Nach dem Importvorgang kann sich der Benutzer mit Hilfe dieses Zertifikats über zertifikatsbasiertes Login anmelden. Dadaurch kann er auf geschützte Unternehmensbereiche zugereifen.

6.6.2 Technisches Konzept für die Benutzerauthentifizierung

Auf die Benutzerauthentifizierung, wie sie im einzelnen abläuft, wird hier nicht näher eingegangen. Im vorherigen Abschnitt wurde beschrieben, wie die Bestellung abläuft.

Technische Aspekte für den Widerruf von Schlüsselmaterial

Wenn das Schlüsselmaterial die Obergrenze seiner Gültigkeit noch nicht erreicht hat, kann es widerrufen werden. Fall die Obergrenze seiner Gültigkeit bereits erreicht ist, kann es im Prinzip auch widerrufen werden, obwohl das Schlüsselmaterial an sich nicht mehr verwendbar ist. (Das setzt aber eine Clientsoftware mit vernünftiger Schlüsselvalidierung voraus.)
Wenn der Mitarbeiter sich sicher ist, dass die Möglichkeit besteht, dass das Schlüsselmaterial missbraucht werden könnte, das kann er über die Bestellseite nach erfolgreicher Authentifizierung sein eigenes Schlüsselmaterial widerrufen. Die Seriennumer des Zertifikats kommt in die Zertifikatssperrliste, die von der Zertifizierungsstelle regelmäßig veröffentlicht wird.
Nachdem über die technischen Aspekte der Prozesse geschrieben wurde, wird die Beschaffenheit des Schlüsselmaterials bestimmt.

Eigenschaften des X.509 Authentifizierungszertifikats

Nach den im Abschnitt 4.4.2 gestellten genauen Anforderungen und nach den Möglichkeiten des X.509 Standards können die Eigenschaften des Authentifizierungszertifikats, wie die Tabelle 6.5 zeigt, festgelegt werden.
Weil man die Möglichkeit des Einsatzes der vorhandenen SmartCards offen halten will, ist die Schlüssellänge auf 1024 Bit eingeschränkt. SmartCards konnten längere Zeit mit längerem Schlüssel nicht arbeiten. Obwohl eine Schlüsselläge von 2048 Bit angemessen wäre, kann man mit dieser Länge die Shanonsche Forderung (siehe A.1 im Anhang) nicht erfüllen. Eine Lösung würde hier die Verwendung von Elliptische-Kurven-Kryptosystem (EKK) bieten. Durch die EKK-Verschlüsselung ist es möglich, bei einer geringeren Schlüssellänge von z. B. 160 Bit genauso sicher wie bei anderen asymmetrische Verfahren mit 1024 Bit zu verschlüsseln. EKK eignet sich daher immer dann, wenn die Speicher- oder Rechenkapazität begrenzt ist, z. B. in Smartcards. Die Verwendung von EKK in X.509 Zertifikaten ist leider bisher noch nicht standardisiert. Es liegt lediglich ein Vorschlag (Draft) vor [ECCdraft]. Eine kurze Einführung befindet sich unter [CVECC05].
Damit das Schlüsselmaterial zu verschiedenen Authentifizierungen verwendet werden kann, müssen Zertifikatsverwendungszweck und erweiterter Zertifikatsverwendungszweck entsprechend gesetzt werden.
Bei der Authentifizierung werden verschiedene Daten abgeglichen. Deshalb müssen

die Zertifikate auch einige benutzerspezifischen Daten, wie Emailadresse, Mitarbeitername, ID des Mitarbeiters beinhalten. Das Feld *Subject Alternativ Name* beinhaltet die Login Daten (UPN - **U**ser **P**rincipal **Name**) des Mitarbeiters, damit das Zertifikat später auch zu Login Zwecken verwendet werden kann.

X.509 Authentifizierungszertifikat	
Schlüssellänge	1024 Bit
Schlüsselalgorithmus	RSA
Zertifikatsverwendungszweck (Key Usage)	Key Encipherment Data Encipherment
erweiterter Zertifikatsverwendungszweck (Extended Key Usage)	Client Authentication
Subject	O = [Name des Unternehmens] CN = [Mitarbeitername] Email = [Emailadresse des Mitarbeiters] 1.3.6.1.4.1.1201.1.1.2.2.75 = [ID des Mitarbeiters]
Subject Alternativ Name (SAN)	Unified Principal Name (UPN) [Mitarbeitername]@[Unternehmens-Domäne]
Lebensdauer	1 Jahr

Tabelle 6.5: Beschaffenheit des X.509 Benutzerauthentifizierungszertifikats

6.7 PKI Strukturkonzept

Die Architektur einer PKI besteht generell aus mehreren Teilen. Zum einen müssen die Komponenten, deren Aufgaben und die Schnittstellen definiert werden. Im zweiten Schritt muss die CA Struktur geplant werden.

6.7.1 PKI Architektur

Die PKI Architektur soll auf dem PKIX Standard basieren und an das Unternehmen angepasst werden. Demnach sind folgende Strukturen erforderlich:

- Registrationsstelle (RA)
- Zertifikatsstelle (CA)
- Zertifikatsbasis (Repository)
- Endeinheit (EE)

Die Abbildung 6.3 zeigt eine mögliche Struktur für die PKI.

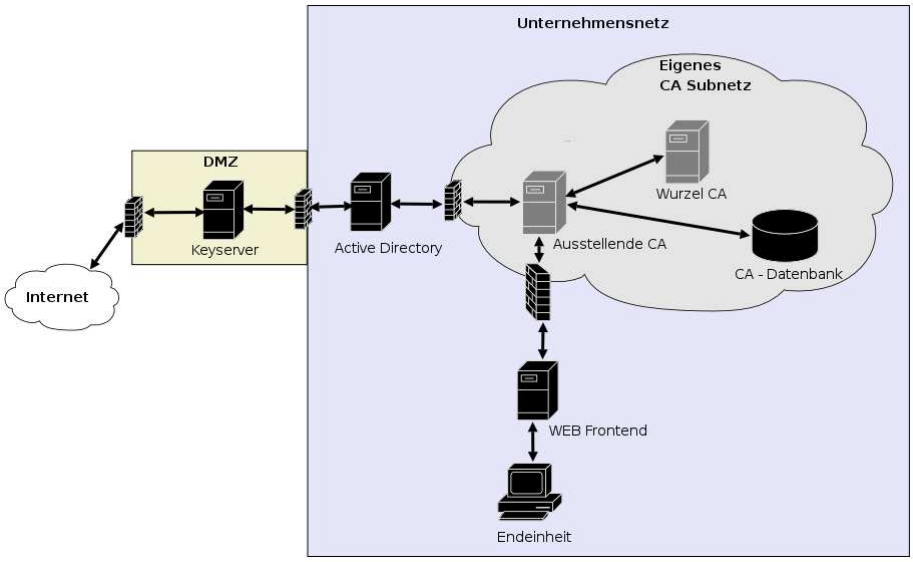

Abbildung 6.3: Mögliche Netzwerkstruktur für eine PKI

6.7.2 Struktur für die Registrationsstelle

Die Registrationsstelle wurde bereits öfters erwähnt und beschrieben. Aus diesem Grund wird sie hier nur kurz beschrieben.
Die Aufgaben der Registrationsstelle sind die Registration und Authentifizierung der Mitarbeiter. Die Registration wird in der Personalabteilung während der Einstellung

anhand der vorgelegten Unterlagen von der Personalabteilung vorgenommen. Die erfassten Daten kommen in das Personalverfahren. Das Active Directory erhält einen Teil dieser Daten automatisch. Diese Daten werden von der Zertifikatsstelle genutzt. Weil das Active Directory mit Hilfe des LDAP Protokolls abgefragt werden kann, nutzt die Zertifikatsstelle diese Möglichkeit, damit die Daten direkt aus dem Active Directory geholt werden. Das hat den Vorteil, dass der Mitarbeiter keine Daten mehr manuell eingeben muss. Das ist einerseits eine Konformität andererseits eine gute Eigenschaft, weil die Daten die in das Schlüsselmaterial kommen authentisch sind. Damit wird gewährleistet, dass die Schlüsselmaterialien zu den im Active Directory vorhandenen Daten passen.
Das Active Directory übernimmt Aufgaben der Registrationsstelle und speichert die öffenlichen Schlüssel sowie die CRL.

6.7.3 Struktur für die Zertifikatsstelle

Bei der Aufbau einer CA Struktur kann man sich inzwischen auf eine Reihe von Falluntersuchungen stützen, weil es mehrere Möglichkeiten gibt, wie eine CA Struktur aufgebaut werden kann. Bei der Gestaltung der Struktur von Zertifikatsstellen helfen die Informationsrepräsentation und die Vertrauensmodelle.
In dem Abschnitt 5.12 wurden drei Möglichkeiten für die Informationsrepräsentation vorgestellt. Bei dem Unternehmen ist eine Datenbasis mit Mitarbeiterinformationen vorhanden. Aus diesem Grund wird als Informationsrepräsentation die Informationsrepräsentation in einer Datenbasis gewählt. D.h. dass die Daten eines Mitarbeiters in der Datenbasis anhand der Informationen, die in dem Zertifikat gespeichert sind, gefunden werden müssen. Das hat natürlich auch Auswirkung auf die Gestaltung von Zertifikaten. Weil es aber eine genaue Anforderung der Zertifikate gibt, ist diese Anforderung bereits erfüllt.
Das andere Hilfsmittel bei der Gestaltung der Struktur von Zertifikatsstellen sind die Vertrauensmodelle. Einige wurden in dem Abschnitt 5.11 vorgestellt. Nach der Bewertung der verschiedene Modelle muss zwischen drei Modellen entschieden werden:

1. Oligarchie von CAs
2. Top Down
3. Top Down mit Delegierung

Weil das Unternehmen

- hierarchisch strukturiert ist,
- eine Abteilung für die interne Sicherheit zuständig ist,
- begrenzte Mittel für die Umsetzung einer PKI zur Verfügung hat

kommt nur das Top-Down Model in Betrachtung. Das heißt, dass eine drei Schichten Architektur aufgebaut wird. Bei dieser Architektur gibt es eine geschützte Wurzel CA. Diese Wurzel CA zertifiziert die anderen CAs, die direkt unter der Wurzel CA liegen. Nachdem die Wurzel CA diese Sub CAs zertifiziert hat, wird sie aus Sicherheitsgründen abgeschaltet.
Die Sub CAs sind auch die ausstellenden CAs. Sie stellen die Zertifikate für die Endeinheiten aus. In unserem Fall reicht eine Sub CA für das Ausstellen der Schlüsselmaterialien völlig aus.

Die Wurzel CA, und der Rechner auf dem diese CA läuft, benötigt speziellen Schutz, weil die gesamte PKI mit der Kompromittierung dieser Wurzel CA unbrauchbar wird. Aus diesem Grund empfiehlt sich die Sicherung der Wurzel CA und der Schlüssel der Wurzel CA. Dieser Rechner muss ausgeschaltet und für andere (unbefugte) sowohl physisch als auch übers Netzwerk unerreichbar gemacht werden.

Wahl der Lebensdauer für die CA Zertifikate

Die Empfehlungen für die Lebensdauer der Zertifikate für die Wurzel CA und für die ausstellende CA gehen in der Fachliteratur auseinander. Aus der Fachliteratur lässt sich aber feststellen, dass man für das Zertifikat der Wurzel CA eine hohe (10 bis 30 oder manchmal bis 50 Jahre) Lebensdauer wählen soll. Für das Zertifikat der ausstellenden CA soll man eine 5 bis 10 jährige Lebensdauer wählen. Diese Werte sind natürlich von der Lebensdauer der Zertifikate für die Endeinheiten abhängig. Wenn ein Zertifikat für eine Endeinheit eine Lebensdauer von 5 Jahren haben soll, dann soll die Lebensdauer der ausstellenden CA mindestens die doppelte bzw. dreifache Lebensdauer haben. Das Zertifikat der Wurzel-CA soll mindestens die zwei- bis dreifache Lebensdauer der ausstellenden CA haben.
In unserem Fall hat das Zertifikat für die Emailverschlüsselung eine Lebensdauer von 2 Jahren. Das Zertifikat der ausstellenden CA soll demnach eine Lebensdauer von mindestens 4 bis 6 Jahren haben. Die Lebensdauer für das Zertifikat der Wurzel CA soll demnach 20 bis 30 Jahre betragen. Ob man hier 20 oder 30 Jahre wählt, ist in Anbetracht der Geschwindigkeit der Informationstechnologie egal. In 20 oder 30 Jahren wird man wahrscheinlich auf andere Methoden umgestiegen sein.

6.7.4 Zertifikatsbasis

Die Aufgabe der Zertifikatsbasis ist das Speichern von öffentlichen Schlüsselmaterialien und von Zertifikatssprerrlisten. In der Fachliteratur werden Konfigurationen erwähnt, wobei diese Aufgabe von der CA selber übernommen wird. Dies ist aber von der CA Software abhängig. In unserem Fall übernimmt diese Aufgabe das Active Directory. Das Active Directory kann ohne weiteres Schlüsselmaterial und Zertifikatssperrliste aufnehmen. Das Schlüsselmaterial wird in der Eigenschaft *UserCertificates* eines Benutzer-Objektes gespeichert.
Die Zertifikatssperrliste wird in der Eigenschaft *certificateRevocationList* des CA-Objektes gespeichert. Der Pfad einer CA im Active Direactory könnte wie folgt aussehen: *CN=CA Name,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=Domain*

Active Directory

In dem Unternehmen werden Microsoft Produkte eingesetzt. Das Active Directory von Microsoft besitzt die Fähigkeit, X.509 Zertifkate aufzunehmen. Ein Schemaupdate ist dazu nicht erforderlich. Wenn die PGP Schlüssel dort auch veröffentlicht werden, muss das Schemaupdate für PGP eingespielt werden.
Da das Microsoft Active Directory auch mittels LDAP Protokoll abgefragt werden kann, liegt es auf der Hand, das Microsoft Active Directory als Keyrepository zu verwenden. Ein anderer Grund dafür ist, dass die empfohlene Clientsoftware das Active

Directory nach Schlüsseln abfragen kann.
Die ausstellende CA schreibt die öffenlichen Zertifikate und die Zertifikatssperrliste in einen bestimmten Active Directory Server. Die Einträge werden dann von einem Active Directory Server zu anderen repliziert. Die ausstellende CA kann nur über eine Firewall

- von einem bestimmten Active Directory Server über einen sicheren Kanal auf dem Port 389 (LDAP) und
- von einem bestimmten Webserver, der die CA Seiten hostet, über einen sicheren Kanal einem bestimmten Port

erreicht werden. Da das Active Directory nur unternehmensintern erreichbar ist, muss eine Lösung für die Geschäftspartner gefunden werden. Es muss eine Schnittstelle oder Dienst definiert werden, welche(r) das Active Directory erreicht und nach Schlüsselmaterial fragen darf und das Ergebnis der Abfrage nach aussen, ins Internet weiterreichen kann. So ein Dienst ist der Keyserver, der im nächsten Abschnitt vorgestellt wird.

Keyserver

Für die Geschäftspartner muss auch eine Schnittstelle definiert werden. Über diese Schnittstelle sollen die Geschäftspartner die Zertifikate bzw. Schlüssel abrufen und auf die Zertifikatssperrliste zugreifen können. Die bisherige Infrastruktur war PGP basiert. Bei der bisherigen Lösung war es kein Problem einen Keyserver von innen und von außen erreichbar zu machen. Der Keyserver selber steht in der DMZ (**Dem**ilitarized **Z**one – demilitarisierte Zone) und wurde sowohl von aussen als auch aus dem internen Netz erreicht.
Der bisherige Keyserver hat eine Schlüsselringdatei, woraus er auf Anfrage den Schlüssel holt und dem Abfragenden zur Verfügung stellt. Die Schlüsselringdatei musste bisher manuell aktualisiert werden.
Weil das Active Directory sowohl PGP als auch X.509 Zertifikate aufnehmen kann, liegt es auf der Hand, dass die neue Lösung aus dem Microsoft Active Directory die Cryptomaterialien auf Anfrage holen und zur Verfügung stellen soll. Der neue Keyserver soll daher nicht dateibasiert arbeiten, sondern das Active Directory bei einer ankommenden Anfrage abfragen. Da im Unternehmen mehrere Active Directory Server in Betrieb sind, soll der neue Keyserver den Active Directory Server abfragen, auf dem die Cryptomaterialien zuerst veröffentlicht werden, weil die Replikation der Daten zwischen den Active Directory Servern ein bis zwei Stunden dauert.
So eine Lösung könnte über CGI (**C**ommon **G**ateway **I**nterface) Skript gelöst werden. Die Firma PGP bietet aber einen Keyserver an, der auch Active Directory abfragen kann. Weil der Keyserver nach wie vor in der DMZ stehen muss, muss auf dem Firewall der Port (389) für LDAP für die bidirektionale Kommunikation zwischen dem Keyserver und dem Active Directory Server geöffnet weden.

6.7.5 Endeinheiten

Durch die Endeinheiten wird eine PKI zu einem Ganzen, weil sie das Gegenstück zu den Servern in einer PKI bilden. In einer PKI sind mehrere Arten von Endeinheiten

denkbar. In den Anwendungsfällen wurden auch einige vorgestellt. Weil der Anwendungsfall Emailverschlüsselung der aufwendigste ist, wurde er detailliert vorgestellt.
Weil das Unternehmen Microsoft Produkte einsetzt, wird der Kreis der in Frage kommenden Produkte stark eingeschränkt. Demnach wird Microsoft Outlook für die Emailkommunikation eingesetzt. In dem Abschnitt 5.4.2 wurden auch die Möglichkeiten für und mit Outlook vorgestellt. In dem Abschnitt 6.4.6 wurde eine Empfehlung für die Emailverschlüsselung ausgesprochen.
Als Clientsoftware zur Authentifizierung wird aus technischen Gründen (vgl. 6.3) Microsoft Internet Explorer.

6.7.6 Wahl der CA Software

Nachdem alle Teile der PKI beschrieben wurden, muss auch über die Software für die CA geschrieben werden. In dem Abschnitt 5.10 wurden ein paar CA Softwareprodukte vorgestellt. Es gibt wesentlich mehr Produkte auf dem Markt, die Auswahl wurde aber eingeschränkt. Viele andere CAs bieten mehr und bessere Konformität für höhere Preise, aber keine Unterstützung für diese duale (PGP und S/MIME) Welt. Das einzige auf dem Markt erhältliche Produkt, die PGP Enterprise CA bietet Unterstützung für diese beiden Verschlüsselungsstandards. Aus diesem Grund soll diese Software eingesetzt werden. Ein anderer Grund für die Wahl ist die gute Zusammenarneit dieser CA mit der Verschlüsselungssoftware *CryptoEx Outlook Version 3*.

Kapitel 7

Migration

Unter Migration versteht man die Einführung eines neuen Verfahrens in das vorhandene Umfeld. In unserem Fall müssen die clientseitige und die serverseitige Strukturen in das vorhandene Umfeld eingeführt werden.

7.1 Serverseitige Migration

Damit die Migration ohne große zwischenfälle ablaufen kann, empfiehlt sich, dass zuerst die serverseitige Strukturen geschaffen werden. Im ersten Schritt muss das Active Directory vorbereitet werden. Das Schemaupdate für die PGP Schlüssel muss eingespielt und unternehmensweit repliziert werden.
Als nächstes müssen die CAs eingerichtet werden.

7.1.1 Einrichtung der Wurzel CA

Als erstes soll die Wurzel CA aufgesetzt werden. Dabei müssen die Empfehlungen zu der Lebensdauer von CA Zertifikaten beachtet werden. Ein weiterer wichtiger Punkt ist die Benennung der CA. Es muss auch geklärt werden, welche Informationen das CA Zertifikat beinhalten soll. Die Benennung der Wurzel CA könnte in unserem Fall *[Unternehmensname] Root CA* sein. Eine wichtige Information ist der Ort der CRL. Diese CRL soll sowohl im Internet als auch unternehmensintern erreichbar sein. Diese Information ist auch im Zertifikat selber beinhaltet. Wenn nicht nötig, sollen die unternehmenseigenen Clients die Abfrage intern erledigen. Für die externe Publikation empfiehlt sich ein HTTP Link.

7.1.2 Einrichtung der ausstellenden CA

Im zweiten Schritt muss die ausstellende CA installiert und in die Domäne integriert werden. Aus Sicherheitsgründen empfiehlt sich für die ausstellende CA einen anderen Rechner zu verwenden als für die Wurzel CA. Die Wurzel CA und das Zertifikat der Wurzel CA müssen in einer PKI am besten geschützt werden. Wer das Zertifikat der

Wurzel CA hat, kann für die ganze Domäne der Wurzel CA beliebige Zertifikate ausstellen und dass soll natürlich vermieden werden. Bevor die Wurzel CA abgeschaltet wird, muss die Wurzel CA für die ausstellende CA ein Zertifikat erzeugen. Dabei sollen die Empfehlungen bezüglich der Lebensdauer und Erweiterungen des Zertifikats der Aussteller-CA beachtet werden. Dieses Zertifikat muss dann in die ausstellende CA importiert werden.
Bei der Konfiguration der ausstellenden CA muss darauf geachtet werden, dass die CA keine Zertifikate an die Clients über die Mircosoft-eigene Enrollmentfunktion oder Autoenrollment verteilt. Diese Funktionalität kann in der Microsoft CA bzw. in den Zertifikatsvorlagen eingestellt werden. Nachdem beide CAs eingerichtet wurden, kann die Wurzel CA vom Netz genommen und gesichert werden. Danach müssen die Zertifikatsvorlagen auf der ausstellenden CA eingerichtet werden. Die Zertifikatsvorlagen richten sich nach den Anwendungsfällen bzw. nach den Anforderungen. Sie müssen in der Testphase auch auf Testsystemen vorgenommen werden.
Die ausstellende CA muss in das Active Directory die öffentlichen Zertifikate veröffentlichen, weshalb auch diese Integration gemacht werden muss.

Einrichtung der Datenbasis der ausstellenden CA

Die ausstellende CA legt die Zertifikate in eine Datenbasis verschlüsselt ab. Diese Datenbasis soll in dem geschützten Bereich aber auf einem anderen Rechner abgelegt werden. Diese Datenbasis soll dann regelmäßig gesichert werden. Die Datenbasis soll nur von der ausstellenden CA angesprochen werden dürfen.

7.1.3 Einrichtung von Schutzmechanismen

Ein ganz wichtiger Punkt bei diesen Rechnern ist deren Schutz. Die Rechner auf denen die CAs laufen müssen durch strikte Zutritts- und Zugangskontrolle vor unbefugten Anmeldeversuchen geschützt werden. Aus diesem Grund müssen diese Rechner in einem mit Zutrittskontrolle versehenen Serverraum in einem abschließbaren Rack montiert werden.
Der Neztwerkzugriff auf diese Rechner muss durch spezielle Firewalleinträge geregelt werden.

Einrichtung des Netzwerkschutzes

Der Neztwerkzugriff der gesamten PKI muss durch spezielle Firewalleinträge geregelt werden.
Der Keyserver muss sowohl mit Hilfe eines Web-Browsers als auch über das Keyserverprotokoll, das auf HTTP basiert aber den Port 11371 benutzt, verwendet werden. Für die Nutzung des Keyserver muss also der Port 11371 bidirektional geöffnet werden.
Da sich der Keyserver selber im DMZ befindet und das Active Directory nach öffentlichen PGP Schlüsseln und Zertifikaten abfragt, muss auf dem Firewall zwischen DMZ und Unternehmensnetz der Port des LDAP Protokolls (389) bidirektional geöffnet werden.
Es wurde empfohlen, dass die CA Server in einem gesonderten Netz arbeiten sollen.

Die Aussteller-CA muss die öffentlichen Zertifikate in das Active Directory, genauer auf einem bestimmten AD Server publizieren.Aus diesem Grund muss der LDAP Port 389 zwischen dem gesonderten CA Netzwerk und dem restlichen Unternehmensnetzwerk geöffnent werden.
Da die Zertifikatsbestellung auf einem Web-Front-End abläuft, das über WEB-Service mit der CA kommuniziert, muss der entsprechende Port antürlich auch geöffnet werden. Dabei darf nur der Server (IP bekannt) über Web-Service den CA Server kontaktieren.
Die Wurzel CA ist zwar die meiste Zeit offline, soll aber trotzdem für die Benutzer netzwerktechnisch nicht erreichbar sein. Dasselbe gilt auch für die Datenbasis der CA. Die Datenbasis selber soll nur für die Aussteller-CA und für die Sicherungsagenten erreichbar sein.

Einrichtung von Anmeldeberechtigungen

Obwohl der Rechner, auf dem die Aussteller-CA läuft in der Domäne integriert ist, sollen nur berechtigte Administratoren sich an dem Rechner anmelden können. Eine Remote-Administration kann durch Einträge in der Firewall zusätzlich gesteuert werden.

Regelmäßige Sicherung der ausstellende CA

Nach dem die Wurzel CA eingerichtet wurde, muss sie gesichert werden. Die ausstellende CA und die Datenbasis müssen regelmäßig (z. B. jede Nacht) gesichert werden. Bei der Sicherung muss eine professionelle Backup-Lösung zum Einsatz kommen.

7.1.4 Einrichtung des neuen Keyservers

Der vorhandene Keyserver kann nur PGP Schlüsselmaterial verwalten. Aus diesem Grund muss eine neue Lösung gefunden werden. Der neue PGP Keyserver bietet die Möglichkeit der Abfrage von Active Directory und eines weiteren PGP Keyservers. Dieser Keyserver kann aber auch als PGP Keyserver dienen. Ein großer Vorteil dieses Produktes ist, dass man die Abfrage dieser verschiedenen Datenbasen kombinieren kann. Deshalb empfiehlt sich der Einsatz dieses Produktes. Mit dem Einsatz des Keyservers wird die serverseitige Infrastruktur abgerundet.
Mit dem Einsatz des Keyservers ist die neue Umgebung fertiggestellt für die Testphase. Damit die Umgebung getestet werden kann, müssen ein paar Testclients vorbereitet werden.

7.2 Clientseitige Migration

Dieser Abschnitt spricht einen wichtigen Punkt des Changemanagements an. In jedem Unternehmen ist es erforderlich, dass Software oder allgemeine Komponenten ausgetauscht werden müssen. In der Regel kann dies nur schrittweise gemacht werden, weshalb ausführliche Tests im Vorfeld gefahren werden müssen, ob die neue Komponenten

sowohl in der alten als auch in der neuen Umgebung funktionieren. In den meisten mittelständischen Unternehmen ist eine weiche Migration erforderlich. Das erfordert das paralle Betreiben der vorhandnen und der neuen Infrastruktur.
Die neue Clientsoftware muss zuerst unter Laborbedingungen installiert, konfiguriert und getestet werden. In den meisten mittelständischen Unternehmen gibt es ein Testlabor zum Testen neuer Software.

7.2.1 Einrichtung von Testclients

Zuerst müssen ein paar Testclients eingerichtet und konfiguriert werden. Eine Konfiguration muss aus der Standardkonfiguration ausgehend erarbeitet werden. Die angestrebte Konfiguration muss sowohl mit der bisherigen Lösung als auch mit der neuen Lösung zusammenarbeiten können, d. h. die neue Clients müssen gleichzeitig

- in der vorhandenen Infrastruktur arbeiten können
- mit der vorhandenen Software zusammenarbeiten
- den vorhandenen Keyserver abfragen können
- vorhandenes Schlüsselmaterial (PGP) verwenden können
- vorhandenene verschlüsselten Materialien entschlüsseln können
- mit der neuen Infrastruktur nahtlos zusammenarbeiten
- den neuen Keyserver abfragen können
- neues Schlüsselmaterial (X.509) verwenden können

Diese ist die wichtigste Voraussetzung für eine weiche Migration. Eine weiche Migrations ist erforderlich, weil nicht alle Client in dem Unternehmen gleichzeitig umgestellt werden können. Aus diesem Grund muss die neue Clientsoftware mit der alten Clientsoftware und mit der alten Umgebung kommunizieren können. Falls es erforderlich ist, muss eine automatische Konvertierung der Storedateien bei der automatischen Installation neuer Software vorgenommen werden, damit die Anwender nach der Installation möglichst problemlos mit der neuen Software arbeiten kann.

7.2.2 Pilotphase

Nach erfolgreichen Labortests in der Testumgebung, können ein paar ausgewählte Mitarbeiter die neue Infrastruktur testen. Diese Pilotphase kann als eine erweitere Testphase unter realen Bedingungen auf produktiven Systemen in einem kleinen Kreis von Anwendern gesehen werden. Die Pilotphase dient zur eventuell erforderlichen Verbesserung der Konfiguration anhand der Rückmeldungen der Pilotbenutzer.

7.2.3 Vorbereitung der neuen Clientsoftware zur automatisierten Software-verteilung

Nachdem die Pilotphase abgeschlossen wurde, kann die Clientsoftware für die automatische Softwareverteilung vorbereitet werden. Dies wird in der Fachliteratur (Softwa-

re)Paketierung genannt. Diese ist erforderlich, damit die neue Clientsoftware automatisiert verteilt werden kann. Wichtiger Schritt während der automatisierten Installation ist der automatisierte Import von vorhandenem Schlüsselmaterial in die neue Clientsoftware. Die Installation und der Importvorgang von vorhandenem Schlüsselmaterial muss ohne Benutzerinteraktion erfolgen. Das ist ja der Zweck und Sinn der automatischen Softwareverteilung.
Die Einstellungen der Clientsoftware müssen auch durch die automatisierte Softwareverteilung gesetzt werden. Die Default-Einstellungen müssen in der Regel für das Unternehmen, bzw. an die Standard-Clients angepasst werden. Die Anpassung beinhaltet unter anderem die Einstellungen der Clientsoftware bezüglich der Schlüsselverwaltung, Sende- und Empfängerregeln für die Verschlüsselung. In dem Unternehemen ist z. B. die Schlüsselgenerierung nicht erlaubt. Ausserdem muss der Zugriff auf den zertalen Schlüsselspeicher (Active Directory) eingerichtet werden. Für eine reibunslose Kommunikation über verschlüsselte Email müssen natürlich folgendes eingestellt werden:

- In welchem Schlüsselspeicher nach Schlüsseln gesucht werden muss/kann.
- Welchem Empfänger mit welchem Verschlüsselungsstandard (PGP oder S/MIME) verschlüsslet werden muss.
- Wie die Verteilerlisten mit Empfänger verschiedener öffentlichen Schlüssel/Zertifikat behandelt werden sollen.
- Wie PGP Schlüssel und X.509 Zertifikate validiert werden sollen. (CRL Abfrage etc.)
- Wie Groß des Zeitintervalls für die Passwortcache sein soll.

Falls es, wie oben empfohlen wurde, die neue Version der vorhandenen Clientsoftware *CryptoEx Outlook Version 3* statt eines anderen Prodkuts zum Einsatz kommen wird, kann die Benutzerschulung entfallen. Mit dieser Software ist die Weiterverwendung vorhandenes Schlüsselmaterial und verschlüsselter Materialien ohne große Umstellung möglich.
Bei *CryptoEx Outlook Version 3* müssen die sog. Policy Dateien erstellt werden. Die erste und Ausgangspolicy liegt in dem Verzeichnis der Anwedendung in der Regel

```
[SystemDrive]:\%Program Files%\CryptoEx\Common\EASserver.pol
```

Diese Policy Datei beinhaltet den Ort der anderen Policy Dateien. Diese Policy muss in dem selben Verzeichnis, wie die Anwendung selber liegen. Diese Policy steuert,

- ob eine Gruppenpolicy (GroupOverridesPath) in betracht gezogen wird.
- wo die zentrale Unternegmenspolcy (rootURL) liegt.
- wo die Benutzerpolicy abgelegt wird.

```
[engine]
LogLevel=dword:00000001
LogPath=file://%AppData%\\CryptoEx\\
UserPath=file://%AppData%\\CryptoEx\\userconfig.pol
rootURL=http://server.locality.companydomain.net:8080/Company-Policy.txt
CachePath=
CacheValidity=
```

```
IdleMode=dword:
GroupOverridesPath=file://%programfiles%\\CryptoEx\\common\\easgroup.pol
```

Sie finden ein Beispiel für eine Unternehmenspolicy im Anhang (D).
Die Gruppenpolcy könnte wie folgt aussehen:

```
[Engine]
Groupoverrides=multisz:StandardClient\00
```

In der Unternehmenspolicy können die Einstellungen als

- obligatorisch
- mit Zeitstempel versehen
- änderbar
- nicht belegt

gesetzt werden. Die lokale Benutzerpolicy wird aus den Einstellungen der Unternehmenspolicy, der Gruppenpolicy und von den Anwender vorgenommenen Einstellungen zusammengestellt. Falls der Sicherheitsadministrator an der zentralen Policy Änderungen vornimmt, werden diese Einstellungen nach einem Neustart des Dienstes *EASServer.exe* vom Server geholt und mit den anderen Einstellugen gemischt. Dabei kann es vorkommen, dass Benutzereinstellungen überschrieben werden, falls diese auf obligatorisch gesetzt wurden, oder diese Einstellung mit einem Zeitstempel versehen wurde. Nachdem diese Policy bzw. Policystruktur zusammengebaut wurde, kann zu der Softwareverteilung übergangen werden.

7.2.4 Verteilung der neuen Clientsoftware

Bevor die neue Clientsoftware verteilt wird, müssen die Mitarbeiter über die Verteilung neuer Clientsoftware benachrichtigt werden. Das kann entweder mit der Platzierung einer Nachricht auf der zentralen internen Portal (Intranet) gemacht werden, oder über den Versand einer Benachrichtigungsemail an alle Mitarbeiter.
Nach dem die Verteilung neuer Clientsoftware bekannt gegeben wurde, kann mit der Softwareverteilung mittels SMS begonnen werden.
Es empfiehlt sich zuerst einige Standorte in Deutschland mit der neuen Clientsoftware zu versorgen, damit auf die bisher nicht bekannten Probleme schnell reagiert werden kannn. Für die automatische Softwareverteilung per SMS muss ein Zeitraum von ein bis drei Monate eingeplant werden. Während dieser Zeit müssen beide Infrastrukturen paralell laufen. Nach dieser Zeit kann die alte Infrastruktur abgeschaltet werden.

7.2.5 Verteilung der CA Zertifikate

Damit die CAs, die Wurzel-CA und die ausstellende CA von allen Clients als vertrauenswürdig bewertet werden, müssen die öffentlichen Zertifikate dieser CAs allen Clients bekannt gemacht werden. Das kann auch über die automatische Softwareverteilung erledigt werden. Die Zertifikate der Wurzel-CA und der Ausstellenden-CA müssen sowohl in den betriebssystem-eignenen Zertifikatsspeicher als auch in die Verschlüsselungsclient importiert werden.

Durch diesen Schritt werden die Zertifikate, die von der Aussteller-CA ausgestellt wurden, als vertrauenswürdig eingestuft.

Kapitel 8

Zusammenfassung und Ausblick

8.1 Ausblick

Das erstellte Konzept ist einsatzfähig. Es soll aber darauf hingewiesen werden, dass Microsoft die nächste Version seines Betriebsystems Vista bzw. Longhorn für 2006 angekündigt hat. Es gibt derzeit keine genaue Information darüber, ob sich und was sich bezüglich der Zertifikatsverwaltung und -behandlung in den neuen Betriebssystemen ändern wird.
Es ist bekannt, dass Microsoft einen PKI Hersteller, namens Alacris übernommen hat [MSALA][Golem]. Was genau Microsoft mit der Übernahme dieses Softwarehauses erreichen will, ist zur Zeit unbekannt.
Microsoft arbeitet zur Zeit auch an einer Rights-Management-System, das keine Verschlüsselung sondern nur eine Zugriffkontorlle darstellt. Ob sich dieses System in eine PKI in der Zukunft integrieren läßt, kann man nicht voraussagen.
Es läßt sich aber vorhersagen, dass Microsoft von sich aus weiterhin keine Lösung und Unterstützung für den PGP Standard bieten wird. In diesem Bereich wird der Anwender weiterhin auf Dritthersteller angewiesen sein.

Anhang A

Anforderungen an die Verschlüsselungsverfahren

Es werden an das Verschlüsselungsverfahren verschiedene Anforderungen gestellt. Eine wichtige ist das Kerckhoffs-Prinzip, das besagt, dass die Sicherheit nur auf der Geheimhaltung des Verschlüsselungsmaterials und nicht auf der Geheimhaltung des Verschlüsselungsalgorithmus beruhen darf.
Die anderen Anforderungen gehen auf Claude E. Shannon zurück. Er wird für den Wegbereiter und Begründer der modernen Informationstheorie gehalten. Mehr Information zu Ihm finden Sie unter: http://en.wikipwdia.org/wiki/Claude_E._Shannon

Konfusion: Der funktionale Zusammenhang zwischen Klartext, Chiffrat und Schlüssel sollte möglichst komplex sein.

Diffusion: Jeder Buchstabe im Chiffrat sollte von möglichst vielen Buchstaben des Klartextes und vom gesamten Schlüssel abhängen, damit sich die statistischen Eigenschaften und Besonderheiten eines Klartextes verwischen.

A.1 Shannon'sche Kriterien:

Shannon gab 1949 die folgenden fünf Kriterien zur Beurteilung der Güte eines Chiffrierverfahrens an:

Stärke der Sicherheit: Ein Chiffrierverfahren heißt bedingungslos sicher (unconditionally secure), wenn selbst unter Zuhilfenahme eines unendlich langen Chiffrats eine Kryptoanalyse nicht möglich ist. Dieser Idealzustand wird nur von einem einzigen bekannten Verfahren, dem one time pad, erfüllt. Ein Chiffrierverfahren heißt berechenbar sicher (computationally secure), wenn auch der bestmögliche Angriff nicht zielführend ist. Den bestmöglichen Angriff kennt man aber nicht, sondern man versucht ihn durch den bestbekanntesten Angriff zu approximieren. Ein Chiffrierverfahren heißt praktisch sicher, wenn der bestbekannteste Angriff nicht einfacher ist, als die vollständige Schlüsselsuche, d.h. das Durchprobieren aller Schlüssel (sog. Brute Force Angriff).

Schlüssellänge: Die verwendete Schlüssel sollten sie nicht zu groß sein, da sie auch gespeichert oder übertragen werden müssen.

Komplexität des Ver- und Entschlüsselungsalgorithmus: Die Komplexität des zugrundeliegenden Algorithmus sollte nicht zu hoch sein, damit seine Hardware-Realisierung nicht zu aufwendig ist und damit die Ver- und Entschlüsselungsrate hoch ist.

Fehlerfortpfanzung: Die Fehlerausbreitung sollte hinreichend klein sein.

Nachrichtenausdehnung: Das Chiffrat sollte nicht viel größer sein als der Klartext.

Diese Anforderungen und Kriterien sind bei der Wahl der Verschlüsselungsalgorithmus wichtig und sollten bei der Planung von Sicherheitssystemen stets beachtet werden.

Anhang B

Anhang B: PGP Standards

PGP (Pretty Good Privacy = ziemlich gute Privatsphäre) ist ein ursprünglich von Phil Zimmermann 1991 geschriebenes öffentliches Verschlüsselungsprogramm. Spätere PGP-Versionen sind von MIT, ViaCrypt, PGP Inc. und jetzt Network Associated Inc. (NAI) entwickelt und vermarktet worden.
PGP ist heute ein De-Facto Standard für die E-Mail-Verschlüsselung mit Millionen von Benutzern weltweit. PGP liegt außerhalb der USA in einer internationalen Variante vor (PGPi), die aber ebenfalls starke Kryptographie verwendet. Für den privaten Bereich ist PGP lizenzfrei einsetzbar. Der Sourcecode ist öffentlich zugänglich und darf im nichtkommerziellen Bereich auch frei genutzt werden.
Die freie Verfügbarkeit des Produktes hat aber auch den Nachteil, dass lizenzpflichtige Algorithmen und Standards in diesem Produkt vermieden oder für den kommerziellen Einsatz lizensiert werden müssen. Aus diesem Grund mußte der RSA-Algorithmus zeitweise aus den PGP-Formaten entfernt werden. RSADSI erlaubte nur die Implementierung in Freeware von der auch RSA den kompletten Source Code erhält. Dies war aber für NAI aus kommerziellen Interessen untragbar. Nach Einführung des Crypto-APIs in Microsoft Betriebssystemen wurde RSA in den Microsoft-Freeware-Versionen auch über das MS-Crypto-API durchgeführt. In den letzten Versionen, die nach Ablauf des RSA-Patents mit September 2000 entstanden, wird RSA in den Freeware-PGP-Versionen wieder als Eigenkodierung angeboten.
Für den kommerziellen Einsatz ist auch ein Patent der Fa. Ascom SysTec AG für den IDEA Algorithmus erforderlich, weshalb IDEA nicht mehr der Standardalgorithmus für PGP-Freeware Produkte ist, aber für den nichtkommerziellen Einsatz trotzdem verfügbar bleibt. In lizensierten Produkten, wie CryptoEx, ist IDEA durchwegs verfügbar.
Da PGP als erfolgreiches Produkt in den USA kommerzialisiert wurde und dies einige Zweifel an der Produktintegrität aufkommen ließ, seien hier ein paar Fakten zur Geschichte von PGP angeführt:

Die erste PGP-Version wurde im Juni 1991 im Internet als Freeware veröffentlicht. Mit der Ausgabe der Version 2.0 wurde das Format geändert, so dass V2.0 und alle Nachfolger inkompatibel mit V1.0 wurden. Diese Version und alle folgenden Fehlerkorrekturen bis PGP 2.3a waren nichtkommerzielle Programme unter Verwendung von einem gemeinsamen RSA-Schlüsselpaar sowohl zur Signaturerstellung als auch für die Verschlüsselung, IDEA zur Verschlüsselung und MD5

als Hashalgorithmus für die Signatur. Diese Originalversionen werden von einigen Puristen immer noch verwendet, da bis zu diesem Zeitpunkt kein kommerzieller Einfluss erfolgt ist.

PGP 2.4 war die erste kommerzielle PGP-Version die von der Firma ViaCrypt bereitgestellt wurde. ViaCrypt lizensierte die Technologie von Phil Zimmermann. Diese Version enthielt zum ersten Mal den Zwang (falls entsprechende Option aktiviert), neben der Verschlüsselung für den Empfänger auch mit einem Schlüssel der Firma/Organisation des Absenders mitzuverschlüsseln.

PGP 2.5 war die erste Version, die durch Abwandlung des eingesetzten RSA-Verfahrens lizenzrechtlich mit dem RSA-Patent in Einklang gebracht wurde. Die Version war aus diesem Grund aber nicht mehr kompatibel zu den Vorgängerversionen.

PGP 2.6.3g (USA) und PGP 2.6.3ia , die sogenannten Guerillaversionen, waren die letzten Freeware-Versionen vor der Übernahme von ViaCrypt durch Phil Zimmermann. Die Versionen sind kompatibel mit den PGP-Versionen 2.5-2.6.3, wurden aber auf 286er und 386er Code optimiert.

PGP 4.0 von ViaCrypt unterstützt sogenannte "Einfunktionsschlüssel", die entweder zum Ver- und Entschlüsseln oder zum digitalen Signieren dienen konnten. Es waren keine "multifunktionalen Schlüssel", wie sie die meisten der bis dato veröffentlichten PGP-Versionen benutzten. Die dahintersteckende Idee war, dass ein Angestellter in einer Firma einen Schlüssel erstellen und diesen der Firma übergeben konnte, so dass die Firma Nachrichten des Benutzers entschlüsseln sowie mit diesem Schlüssel verschlüsseln konnte, ohne jedoch seine digitale Signatur erzeugen zu können, d.h. ohne seine Unterschrift fälschen zu können. Sowohl die Versionen für Privatanwender und Firmen enthielten dieses Feature. Das Handbuch der 4.0er-Version erwähnt ein "Freeware PGP 3.0", das "später in diesem Jahr" erscheinen sollte. Welches Jahr genau gemeint war, ist nicht bekannt. Wahrscheinlich ist aus PGP 3.0 die Version 5.0 geworden.

PGP-Mail 4.5 entstand mitte 1997 und enthielt auch erstmals Erweiterungen (sogenannte "Plug-Ins") für Netscape 3.x und Eudora 3.x. Die Version konnte kommerziell oder als Privatanwender zu unterschiedlichen Konditionen lizensiert werden.

PGP 5.x ist das erste kommerzielle Produkt der neuen Firma PGP-Inc. Erstmals war ein Outlook Plug-In verfügbar und die Bedienoberfläche wurde stark verbessert. Ab PGP 5.x wird DSS/DH ("Digital Signature Standard" und "DH/ElGamal" für die Verschlüsselung) mit zwei Schlüsselpaaren eingesetzt und bietet eine asymmetrische Verschlüsselung bis 4096 Bit und Signatur mit 1024 Bit an. Außerdem ersetzt der bereits oben besprochene SHA-1 mit 160 Bit den Hashalgorithmus MD5. Für die symmetrische Verschlüsselung stehen IDEA, CAST (128 Bit) und Tripel-DES (168 Bit) zur Verfügung, wobei jeweils einer wahlweise eingesetzt wird. Seit dieser Version ist CAST auch der Default-Verschlüsselungsalgorithmus für PGP.

PGP5.5 wird erstmals in den MS-Explorer zur Dateiverschlüsselung integriert. Außerdem enthält es für Firmen die Möglichkeit des gezwungenen Mitverschlüsselns an einen Firmenschlüssel. Bei den 5.5e-Versionen wird man jedoch vor der Benutzung eines solchen Schlüssels gewarnt. Weiterhin verfügbar, jedoch nicht mit Version 5.5 mitgeliefert, ist ein Pogramm, dass eintreffende Mails einer Firma

überwacht: Falls eine PGP-Mail an einen User innerhalb der Firma eintrifft, diese jedoch nicht an den Firmenschlüssel mitverschlüsselt ist, wird entweder eine Nachricht an den Absender geschickt, oder die Mail sofort gelöscht. In beiden Fällen wird der Benutzer innerhalb der Firma die Mail nie zu Gesicht bekommen.

PGP 5.5.5 war dann die erste Version mit dem Copyright der neuen Firma NAI, die Zimmermanns PGP-Inc übernommen hatte. Funktionell war die Version identisch mit der Vorversion.
Der PGP 5.5 Quellencode wurde, da dieser offengelegt wurde, von "Cyber-Knights Templar" weiter modifiziert, so dass RSA-Schlüssellängen bis zu 16384 Bit sowie DSS/DH-Schlüssellängen bis zu 8192 Bits für die Verschlüsselung und 2048 Bit für die Signaturerstellung verwendet werden können. Derartige Schlüssel sind allerdings mit anderen PGP-Versionen großteils inkompatibel und im Allgemeinen unzweckmäßig.

PGP 6.x waren die ersten Versionen, die nach der Übernahme von PGP-Inc durch NAI entwickelt wurden. In PGP 6.x und den kommerziellen Versionen von PGP 5.x werden sogenannte Key Revocation Certificates (KRC) angeboten. Damit synchronisiert sich PGP automatisch mit den angegebenen Key-Servern und stellt dort dieses Widerrufszertifikat bereit.
PGP 6.0 wurde mit optionaler Unterstützung von RSA-Schlüsseln herausgebracht. Zunächst war auch die Schlüsselgenerierung erlaubt. Diese musste jedoch von NAI sofort wieder zurückgezogen werden (PGP 6.0a). In PGP 6.0.2 war die RSA Unterstützung inkl. Schlüsselgenerierung in den RSA-Versionen wieder voll hergestellt. PGP 6.0.2i (Exportversion) unterstützte keine RSA-Schlüsselgenerierung, die Benutzung war möglich. Durch die Offenlegung des Codes entwickelte Cyber-Knights Templar eine PGP 6.0.2ckt Freeware, die RSA-Schlüsselgenerierung mit RSA-Schlüssellängen bis 16384 Bits erlaubt.

PGP 6.5.x wurde im 2. Quartal 1999 freigegeben, wobei die Freeware-Version PGPdisk, das Festplattenverschlüsselungsprogramm nicht mehr enthielt. Dies ist auch der Grund, warum sich die PGP 6.5-Version im Privatbereich kaum durchsetzen konnte. Andererseits war mit der Version die Übernahme von X.509-Zertifikaten möglich, was für den kommerziellen Bereich interessant ist. Nach anfänglichen Schwierigkeiten mit dem "Additional Decryption Key" (ADK), der einen Zugriff von Firmen auf die Daten der Mitarbeiter erlauben soll, wurden die Sicherheitsprobleme mit der Version 6.5.8 beseitigt.

Die PGP-Version ist PGP 7.0, die nach der Freigabe des RSA-Algorithmus im September 2000 entstand. Der Source Code ist wieder verfügbar, PGPDisk in der Freeware nicht enthalten. RSA-Schlüssel werden nun auch für ADK unterstützt. Die X.509-Zertifikatsbehandlung wurde verbessert.

Parallel zu den zuvor angeführten PGP-Entwicklungen wurde OpenPGP als RFC 2440 der IETF veröffentlicht. In dem Standard sind beliebige Signatur- und Verschlüsselungsmethoden offengelassen. Implementiert werden müssen DSA und ElGamal, SHA-1 und Tripel-DES. Aus Kompatibilitätsgründen sollten jedoch auch RSA, MD5, IDEA und CAST5 zur Nachrichtenerstellung implementiert werden. Um V3-kompatibel zu bleiben, muss zumindest RSA, IDEA und MD5 verarbeitet werden können (siehe unten).
Die Spezifikation von ADK wurde aus Sicherheitsgründen fallengelassen. In OpenPGP

sind zwei Versionen von Schlüsseln und Signaturen definiert. Version 3 (PGP 2.6.x) unterstützt nur die Basisfunktionalität, während Version 4 ein erweiterbares Format mit Signaturinformationen beschreibt. OpenPGP-Implementierungen müssen V3- und V4-Schlüssel akzeptieren.
Nur PGP 5.5.3 Freeware und PGP5.x Commercial ohne RSA unterstützen den RSA-Algorithmus nicht. In PGP 6.0.2 Freeware und Commercial ohne RSA wird RSA in Microsoft-Betriebssystemen über MS-Crypto-API abgewickelt.

Anhang C

Eigenschaften der Authentifizierungszertifikate

Die Eigenschaften eines Zertifikates lassen sich mit dem dazu gut geeigneten Werkzeug OpenSSL http://www.openSSL.org anzeigen. Das Tool gibt es inzwischen auch für Windows XP. OpenSSL wird standardmäßig (falls es nicht geändert wurde) in folgendes Verzeichnis installiert:

```
[SystemDrive]:\OpenSSL\bin\
```

Die wichtigste Datei dabei ist die *openssl.exe*. Nach der Installation von OpenSSL lassen sich die Zertifikatseigenschaften mit dem folgenden Befehl anzeigen:

```
[SystemDrive]:\OpenSSL\bin\OpenSSL.exe x509 -serial -subject -issuer
-purpose -alias -text -in [Pfad zu dem Zertifikatsdatei]
```

Nach dem Aufruf wurde folgendes ausgegeben (gekürzt):

```
serial=528000F2
subject= /O=Partner/OU=ext/GN=Muster/SN=Mueller/
      1.3.6.1.4.1.1201.1.1.2.2.57=ADBE9657
issuer= /1.3.6.1.4.1.1201.1.1.2.2.57=ADBE9657/C=DE/
      O=Unternehmen/CN=UnternehmensCA
Certificate purposes:
SSL client : Yes
SSL client CA : No
SSL server : Yes
SSL server CA : No
Netscape SSL server : Yes
Netscape SSL server CA : No
S/MIME signing : Yes
S/MIME signing CA : No
S/MIME encryption : Yes
S/MIME encryption CA : No
CRL signing : Yes
CRL signing CA : No
Any Purpose : Yes
```

```
Any Purpose CA : Yes
OCSP helper : Yes
OCSP helper CA : No
<No Alias>
Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number: 1384120562 (0x528000f2)
      Signature Algorithm: md5WithRSAEncryption
      Issuer: 1.3.6.1.4.1.1201.1.1.2.2.75=ADBE9657, C=DE,
O=Unternehmen, CN=UnternehmensCA
      Validity
         Not Before: Dec 14 07:23:59 2004 GMT
         Not After : Dec 14 07:23:59 2006 GMT
      Subject: O=Partner, OU=ext, GN=Muster, SN=Mueller/
      1.3.6.1.4.1.1201.1.1.2.2.75=ADBE9657
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
            Modulus (1024 bit): ...
            Exponent: 65537 (0x10001)
      X509v3 extensions:
         X509v3 Basic Constraints:
            CA:FALSE
   Signature Algorithm: md5WithRSAEncryption
                                                              ...

- - - - -BEGIN CERTIFICATE- - - - -
...
- - - - -END CERTIFICATE- - - - -
```

Anhang D

Beispiel für eine Unternehmenspolicy

Hier finden Sie ein Beispiel für eine Unternehmenspolicy.

```
[\\\\PolicyMeta]

templateName=CryptoEx.TPL

timeStamp=dword:41DEC3F2


[CMSEngine]

AlternateAIA=multisz:

AlternateAIACHANGEABLE=dword:00000000

AlternateCDP=multisz:

AlternateCDPCHANGEABLE=dword:00000000

BasicConstraints=dword:00000000

BasicConstraintsCHANGEABLE=dword:00000000

CDPMode=dword:00000001

CDPModeCHANGEABLE=dword:00000000

CertCheck=dword:00000001

CertCheckCHANGEABLE=dword:00000000

CRLCheck=dword:00000003
```

```
CRLCheckCHANGEABLE=dword:00000000

CTLCertImport=dword:00000000

CTLCertImportCHANGEABLE=dword:00000000

CTLCheck=dword:00000000

CTLCheckCHANGEABLE=dword:00000000

SymAlgoId=dword:00000003

SymAlgoIdCHANGEABLE=dword:00000000


[CryptoEx]

AdvancedOptions=dword:00000001

AllowSendPlain=dword:00000000

AllowSendPlainCHANGEABLE=dword:00000000

CanDeleteKey=dword:00000003

CanDeletePrivateKey=dword:00000000

CanExportKey=dword:00000001

CanGenerateKey=dword:00000000

CanGenerateKeyCHANGEABLE=dword:00000000

CanImportKey=dword:00000001

CanSeeKeyProps=dword:00000001

CanSeeStoreProps=dword:00000000

EnableRecipientRules=dword:00000001

EnableRecipientRulesCHANGEABLE=dword:00000000

EngineDecisionRange=dword:00000005

EngineDecisionRangeCHANGEABLE=dword:00000000

IconType=dword:00000000

IconTypeCHANGEABLE=dword:00000000

LogLevel=dword:00000001
```

```
PreferredEngine=dword:00000001

PreferredEngineCHANGEABLE=dword:00000000

RecipientResultSortOrder=dword:00000001

RuleRedLevel=dword:0000001E

RuleRedLevelCHANGEABLE=dword:00000000

RuleYellowLevel=dword:00000050

RuleYellowLevelCHANGEABLE=dword:00000000

SeedFilePath=

SeedFilePathCHANGEABLE=dword:00000000

SelfAndFromOnAllClones=dword:00000002

SelfAndFromOnAllClonesCHANGEABLE=dword:00000000

ShowWelcomeWizard=dword:00000000

SignaturePreference=dword:00000001


[CryptoEx\\About]

CustomVersion=Policy Version 15-03-2005

CustomVersionCHANGEABLE=dword:00000000

ProductWebsite=http://my.company.net/encryption

ProductWebsiteCHANGEABLE=dword:00000000

SupportRequest=mailto:IT-Security@company.com

SupportRequestCHANGEABLE=dword:00000000

SupportWebsite=http://intranet.company.net/encryption

SupportWebsiteCHANGEABLE=dword:00000000


[CryptoEx\\AntiVirus]

DownloadURL=

DownloadURLCHANGEABLE=dword:00000000
```

```
Enabled=dword:00000000

EnabledCHANGEABLE=dword:00000000

LastUpdate=dword:00000000

LastUpdateCHANGEABLE=dword:00000000


[CryptoEx\\Chiasmus]

DllPath=

DllPathCHANGEABLE=dword:00000000

Enabled=dword:00000000

EnabledCHANGEABLE=dword:00000000

StorePath=multisz:

StorePathCHANGEABLE=dword:00000000


[CryptoEx\\Corporate]

Download=dword:00000001

DownloadMode=dword:00000001

IntermediateCertificates=multisz:
http://keyserver.company.net:11371/pks/lookup?op\3Dget&search\3D0xBCEADD8D\00


TrustedCertificates=multisz:
http://keyserver.company.net:11371/pks/lookup?op\3Dget&search\3D0xBCEADD8D\00


TrustedCertificatesCHANGEABLE=dword:00000000

UpdateTime=dword:00015180

UseAllStores=dword:00000001


[CryptoEx\\Password]

CacheEnabled=dword:00000001

CacheEnabledCHANGEABLE=dword:00000000
```

```
CacheTimeout=dword:0000003C

CacheTimeoutCHANGEABLE=dword:00000000

MinLength=dword:00000008

MinLengthCHANGEABLE=dword:00000000


[CryptoEx\\Proxy]

Port=dword:00000000

PortCHANGEABLE=dword:00000000

Server=

ServerCHANGEABLE=dword:00000000

ServerConfig=dword:00000001

ServerConfigCHANGEABLE=dword:00000000


[CryptoEx\\RecipientRules]

EnumCHANGEABLE=dword:00000000

KeyQualEncBitsize=multisz:512:80\00

KeyQualEncExpired=dword:00000000

KeyQualEncExpiredCHANGEABLE=dword:00000000

KeyQualEncInvalid=dword:00000050

KeyQualEncInvalidCHANGEABLE=dword:00000000

KeyQualEncRevocNotChk=dword:00000064

KeyQualEncRevocNotChkCHANGEABLE=dword:00000000

KeyQualEncStorePrio=
      multisz:http://keyserver.company.net:11371/pks/:95:95:95\00

KeyQualEncStorePrioCHANGEABLE=dword:00000000

KeyQualEncUsageMismatch=dword:00000000

KeyQualEncUsageMismatchCHANGEABLE=dword:00000000

KeyQualSigBitsize=multisz:512:80\00
```

```
KeyQualSigBitsizeCHANGEABLE=dword:00000000

KeyQualSigExpired=dword:00000000

KeyQualSigExpiredCHANGEABLE=dword:00000000

KeyQualSigInvalid=dword:00000000

KeyQualSigInvalidCHANGEABLE=dword:00000000

KeyQualSigRevocNotChk=dword:00000064

KeyQualSigRevocNotChkCHANGEABLE=dword:00000000

KeyQualSigStorePrio=multisz:*:100:100:0\00

KeyQualSigStorePrioCHANGEABLE=dword:00000000

KeyQualSigUsageMismatch=dword:00000000

KeyQualSigUsageMismatchCHANGEABLE=dword:00000000

ResQualAsymEncProtocolPrio=multisz:PGP:100\00X.509:100\00*:0\00

ResQualAsymEncProtocolPrioCHANGEABLE=dword:00000000

ResQualAsymSigProtocolPrio=multisz:PGP:100\00X.509:100\00*:0\00

ResQualAsymSigProtocolPrioCHANGEABLE=dword:00000000

ResQualGroupRecpt=dword:00000000

ResQualGroupRecptCHANGEABLE=dword:00000000

ResQualKeyQuantityQual=multisz:20:100\0021:80\0025:0\00

ResQualKeyQuantityQualCHANGEABLE=dword:00000000

ResQualMissingEnc=dword:00000064

ResQualMissingEncCHANGEABLE=dword:00000000

ResQualMissingSig=dword:00000064

ResQualMissingSigCHANGEABLE=dword:00000000

ResQualMissingUserEnc=dword:00000000

ResQualMissingUserEncCHANGEABLE=dword:00000000

ResQualMissingUserSig=dword:00000000

ResQualMissingUserSigCHANGEABLE=dword:00000000
```

```
ResQualSigWithoutProt=dword:00000064

ResQualSigWithoutProtCHANGEABLE=dword:00000000

ResQualSymEncProtocolPrio=multisz:PGP:100\00X.509:100\00*:0\00

ResQualSymEncProtocolPrioCHANGEABLE=dword:00000000


[CryptoEx\\RecipientRules\\F000]

Enabled=dword:00000001

EnumItemCHANGEABLE=dword:00000000

EnumORDER=dword:00000000

KeyQualEncBitsize=multisz:512:0\001023:50\002047:95\00

KeyQualEncExpired=dword:00000000

KeyQualEncInvalid=dword:00000032

KeyQualEncRevocNotChk=dword:00000032

KeyQualEncStorePrio=
      multisz:file://%UserProfile%\\keys\\default.cxs:100:100:100\00
      http://keyserver.company.net:11371/pks/:95:95:95\00

KeyQualEncUsageMismatch=dword:00000000

KeyQualSigBitsize=multisz:512:0\001023:50\002047:95\00

KeyQualSigExpired=dword:00000000

KeyQualSigInvalid=dword:00000000

KeyQualSigRevocNotChk=dword:00000032

KeyQualSigStorePrio=
      multisz:file://%UserProfile%\\keys\\default.cxs:100:95:95\00

KeyQualSigUsageMismatch=dword:00000000

MatchPatterns=multisz:SMTP:W:*@company.com\00SMTP:R:.*@company.com\00

Name=Company

ResQualAsymEncProtocolPrio=multisz:PGP:100\00*:0\00

ResQualAsymSigProtocolPrio=multisz:PGP:100\00*:0\00
```

```
ResQualGroupRecpt=dword:00000050

ResQualKeyQuantityQual=multisz:1:100\002:60\004:0\00

ResQualMissingEnc=dword:00000064

ResQualMissingSig=dword:00000064

ResQualMissingUserEnc=dword:00000000

ResQualMissingUserSig=dword:00000000

ResQualSigWithoutProt=dword:00000055

ResQualSymEncProtocolPrio=multisz:PGP:100\00*:0\00


[CryptoEx\\SmartCard]

AllowPINChange=dword:00000000

AllowPINChangeCHANGEABLE=dword:00000000

DLLs=multisz:

DLLsCHANGEABLE=dword:00000000

PreferPinpad=dword:00000000

PreferPinpadCHANGEABLE=dword:00000000

TrustRootCA=dword:00000001

TrustRootCACHANGEABLE=dword:00000000

UserCancelTime=dword:0000000A

UserCancelTimeCHANGEABLE=dword:00000000


[CryptoEx\\Stores]

EnumCHANGEABLE=dword:00000000


[CryptoEx\\Stores\\F000]

BindString=3

DisplayName=Default Store
```

```
Enabled=dword:00000001

EnumItemCHANGEABLE=dword:00000000

EnumORDER=dword:00000000

Moniker=file://%userprofile%\\config\\CryptoEx\\keys\\default.cxs


[CryptoEx\\Stores\\F002]

BindString=1

DisplayName=Company Online Store

Enabled=dword:00000001

EnumItemCHANGEABLE=dword:00000000

EnumORDER=dword:00000001

Moniker=http://keyserver.company.net:11371/pks/


[CryptoEx\\Stores\\F003]

BindString=1

DisplayName=Business Partner Store

Enabled=dword:00000001

EnumItemCHANGEABLE=dword:00000003

EnumORDER=dword:00000002

Moniker=file://%systemdrive%\\config\\CryptoEx\\keys\\outside.cxs


[CryptoEx\\StoreSettings]

CreateableTypes=dword:0000000B

CreateableTypesCHANGEABLE=dword:00000003

LocalBackupCount=dword:00000003

LocalBackupCountCHANGEABLE=dword:00000000
```

```
[File]
AddTrustChain=dword:00000000
AddTrustChainCHANGEABLE=dword:00000000

[Notes]
AddTrustChain=dword:00000000
AddTrustChainCHANGEABLE=dword:00000000
SmimeAnsiTextEncoding=dword:00000000
SmimeAnsiTextEncodingCHANGEABLE=dword:00000000

[Outlook]
AddRecipientsToBody=dword:00000002
AddTrustChain=dword:00000001
AlwaysImportKeys=dword:00000000
CipherNotify=dword:00000001
CipherNotifyOnError=dword:00000000
Compatibility=dword:00000001
DetectOnOpen=dword:00000001
DetectOnOpenCHANGEABLE=dword:00000000
DisableRollbackOnSave=dword:00000000
DoNotAllowSave=dword:00000001
DoNotModifyRecipients=dword:00000002
EncryptToFrom=dword:00000001
EncryptToFromCHANGEABLE=dword:00000000
EncryptToSelf=dword:00000001
EncryptToSelfCHANGEABLE=dword:00000000
HTMLConversion=dword:00000003
```

```
IdleMode=dword:00000002

Language=0

ResolveRecipientKeys=dword:00000001

ResolveRecipientKeysCHANGEABLE=dword:00000000

SearchKeysRemote=dword:00000001

SearchKeysRemoteCHANGEABLE=dword:00000000

ShowResolutionResult=dword:00000000

SmimeAnsiTextEncoding=dword:00000000

SmimeAnsiTextEncodingCHANGEABLE=dword:00000000

UseDetachedSigPGP=dword:00000001

UseDetachedSigPGPAtt=dword:00000001

UseDetachedSigX509=dword:00000000

UseMAPIForms=dword:00000000

WordAsEditorDisable=dword:00000001

WordAsEditorDisableCHANGEABLE=dword:00000000


[PGPEngine]

AnsiTextEncoding=dword:00000001

ArmorComment=Use Encryption for Confidental Communication!

ArmorCommentCHANGEABLE=dword:00000000

GnuPGCompatibility=dword:00000001

SymAlgoId=dword:00000003


[StoreManager]

IdleMode=dword:00000002

Language=0
```

Literaturverzeichnis

[AAL 02] ADAMS, CARLISLE und STEVE LLOYD: *Understanding PKI: Concepts, Standards, and Deployment Considerations,*. Addison Wesley, 2002. 607 S.

[BEGTPE] BUNDESNETZAGENTUR: *Informationen zu der elektronischen Signatur*. 2005, http://www.bundesnetzagentur.de/enid/c2ac3f1eb15cf4b6bfed59c7902bd82c,0/Technische_Regulierung_Telekommunikation/Elektronische_Signatur_gz.html . Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen hieß frühre Regulierungsbehörde für Telekommunikation und Post.

[BRA97] BRANCHAUD, M.: *A survey of public key infrastructures*. Diplomarbeit, McGill University, Dept. of Computer Science, March 1997.

[BSI 04] BSI: *Leitfaden für die IT Sicherheit: IT - Grundschutz kompakt*. Bundesamt für die Sicherheit in der Informationstechnik, 2004, http://bsi.bund.de .

[BSK02] INNERN, BAYER. STAATSMINISTERIUM DES: *Konzept zur Einfülhrung der elektronischen Signatur und von Verschlüsselungsverfahren in der bayerischen Verwaltung*. Technischer Bericht, Bayer. Staatsministerium des Innern, 2002, www.bayern.de/imperia/md/content/stk/egovernment/sigkonzept.pdf .

[BZ05] BOWDEN, ZED: *PKI - Interoperability Document*, jan 2005, http://vtmig.w2k.vt.edu .

[CCC99] CLUB, CHAOS COMPUTER: *Presseinformation des Chaos Computer Club*. September 1999, http://www.ccc.de/press/releases/1999/CCC19990903.html?language=de .

[CKLW00] CAMPHAUSEN, INGMAR, STEFAN KELM, BRITTA LIEDTKE und LARS WEBER: *DFN-PCA Handbuch, Aufbau und Betrieb einer Zertifizierungsinstanz*. DFN-CERT Services GmbH, März 2000.

[CVECC05] GMBH, CV CRYPTOVISION: *ECC ? Kryptographie auf Basielliptischer Kurven, Eine kurze Einführung*. 2005, http://www.cryptovision.com/cvweb/fileadmin/technologie/WP_ECC_a.pdf .

[Ebe98] EBELING, ADOLF: *US-Geheimdienst fängt europaweit E-Mails ab*. Heise Newsticker, Januar 1998, http://www.heise.de/newsticker/meldung/1824.

[ECCdraft] L., BROWN. DANIEL R.: *INTERNET-DRAFT: Additional Algorithms and Identifiers for use of Elliptic Curve Cryptography with PKIX*, Jan 2006, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ecc-pkalgs-02.txt.

[ECRYPT] (VOD), STEVE BABBAGE, DARIO CATALANO (ENS), LOUIS GRANBOULAN (ENS), ARJEN LENSTRA (TUE), CHRISTOF PAAR (RUB), JAN PELZL (RUB), THOMAS PORNIN (CRYPTOLOG), BART PRENEEL (KUL), MATT ROBSHAW (RHUL), ANDY RUPP (RUB), NIGEL SMART (BRIS) und MICHAEL WARD (MASTERCARD): *ECRYPT Yearly Report on Algorithms and Keysizes*. Technischer Bericht, ECRYPT, European Network of Excellence in Cryptology, March 2005.

[EUSIG99] UNION, DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN: *RICHTLINIE 1999/93/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*. Amtsblatt der Europäischen Gemeinschaften, Dezember 1999.

[Golem] GOLEM: *Microsoft übernimmt Alacris*. Golem, 2005, http://www.golem.de/0509/40520.html.

[Golem2] GOLEM: *MS Outlook-PlugIn für GNU Privacy Guard (GnuPG); G Data integriert GnuPG in Outlook*. Golem, 2001, http://www.golem.de/0107/15076.html.

[GRA05] GRIMES, ROGER A.: *Wider die Pessimisten, Sauber verschlüsselte Daten mit EFS Teil 1*. Windows IT Pro, 10/2005:22–25, oct 2005.

[GRA05b] GRIMES, ROGER A.: *Der Weg zum Schlüssel, Sauber verschlüsselte Daten mit EFS Teil 2*. Windows IT Pro, 11/2005:39–41, nov 2005.

[H57134] ONLINE, HEISE: *PGP Kauft Verschlüsselungsspezialisten Glück und Kanja*. Heiese Online Ticker, März 2005, http://www.heise.de/newsticker/meldung/57134.

[Hag96] HAGER, NICKY: *Secret Power, New Zealand's Role in the International Spy Network*. Technischer Bericht, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, Februar 1996. kann unter http://www.fas.org/irp/eprint/sp/index.html bestellt werden.

[Hag97] HAGER, NICKY: *Exposing the Global Surveillance System. CovertAction Quarterly*. Technischer Bericht 59, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, Februar 1997. Online unter http://caq.com/CAQ59GlobalSnoop.html; Auszug aus [Hag96].

[HOBII] HAAR, TOBIAS: *Basel II wird Gesetz?, IT-Sicherheit spielt größere Rolle bei der Kreditvergabe*. Heise Online, Feb 2006, http://www.heise.de/newsticker/meldung/69680.

[KF05] KRESSE, FRANK: *Schlankes Schlüsselbrett - Zentrale Verschlüsselung auf dem Mailserver*. Windows2000 Magazin, 09/2005, Sept 2005, http://www.win2000mag.de/.

[KM00] KORCZYNSKI, M: *The political economy of trust*. Journal of ManagmentStudies, (37):1–21, Januar 2000.

[LeVe 01] LENSTRA, ARJEN K. und ERIC R. VERHEUL: *Selecting Cryptographic Key Sizes*. Journal of Cryptology: the journal of the International Association for Cryptologic Research, 14(4):255–293, 2001, http://www.win.tue.nl/~klenstra/key.pdf.

[LP03] PROF. LINHOFF-POPIEN, CLAUDIA: *Skript zur Vorlesung: Verteilte Systeme*, April 2003. verfügbar im Internet http://mobile.informatik.lmu.de/vorlesungen.

[Mac98] MACHEFSKY, IRA: *A Total Economic Impact Analysis of Two PKI Vendors: Entrust and VeriSign*. Technischer Bericht, Giga Information Group,Norwell, MA, USA,, Sept 1998, http://statistic.gunadarma.ac.id/idkf/idkf/aplikasi/e-commerce/total-economic-impact-of-pki-1999.pdf.

[MFSJ99] MCGRAW, GARY und EDWARD W. FELTEN: *Securing Java: Getting Down to Business with Mobile Code*. Wiley, January 1999, http://www.securingjava.com/.

[MI005] TRAUTMANN, HELMUT UND BUCHBERGER, STEFAN: *Wer bist du? - Mit Identity Management zum effizienten E-Business*. manage-it, 3-4 2005, Sept 2005.

[MSALA] CORPORATION, MICROSOFT: *Microsoft Acquires Identity and Access Management Solutions Provider Alacris*. Microsoft PressPass, 2005, http://www.microsoft.com/presspass/press/2005/sep05/09-19AlacrisPR.mspx.

[MSCS02] KHOR, SIEW-MOI: *Code Signing Office XP Visual Basic for Applications Macro Projects*. 2002, http://www.microsoft.com/whdc/system/platform/64bit/kmsigning.mspx.

[MSEFS02] CORPORATION, MICROSOFT: *Encrypting File System in Windows XP and Windows Server 2003*. 2002, http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/cryptfs.mspx. Updated: April 11, 2003; Microsoft Windows XP and Windows Server 2003 provide many enhancements in the area of data protection-especially Encrypting File System (EFS). This article provides a technical walkthrough that illustrates how to use important data recovery and protection features in various Windows platforms. Also included are best practices and the steps needed to build an effective data recovery and protection strategy.

[MSIWA] CORPORATION, MICROSOFT: *Integrated Windows Authentication (IIS 6.0)*. 2005, http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/523ae943-5e6a-4200-9103-9808baa00157.mspx?mfr=true.

[MSOL05] CORPORATION, MICROSOFT: *How to turn off e-mail matching for certificates in Outlook*. Microsoft Corporation, 2005. When you send a secure message in Microsoft Office Outlook 2003, in Microsoft Outlook 2002, or in Microsoft Outlook 2000, you may need to use a certificate that does not match your e-mail address. This article describes how to turn off e-mail matching for certificates.

[MSTNIWA] CORPORATION, MICROSOFT: *Integrated Windows Authentication (IIS 6.0)*. Microsoft Windows 2003 Server TechNet, Oktober 2005. Microsoft 2003 Server Manual.

[MSV06] CORPORATION, MICROSOFT: *Digital Signatures for Kernel Modules on x64-based Systems Running Windows Vista*. 2006, `http://www.microsoft.com/whdc/system/platform/64bit/kmsigning.mspx`.

[NC98] COMPUTING, NETWORK: *Zertifizierte Sicherheit zahlt sich aus*. Network Computing, Seiten 50–51, Dezember 1998.

[OSI7498-2] ISO: *Information Processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*. Technischer Bericht, ISO, 1989.

[RFC2440] CALLAS, J., L. DONNERHACKE, H. FINNEY und R. THAYER: *RFC2440 - OpenPGP Message Format*. Technischer Bericht, The Internet Engineering Task Force, Network Working Group, November 1998, `http://www.ietf.org/rfc/rfc2440.txt`.

[RFC2459] R., HOUSLEY., W. FORD, W. POLK und D. SOLO: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, Jan 1999.

[RFC2510] ADAMS, C. und S FARRELL: *The Internet X.509 Public Key Infrastructure Certificate Management Protocols*, March 1999.

[SCHB01] SCHNEIER, BRUCE: *Handbook of Applied Cryptography*. CRC Press, aug 2001, `http://www.cacr.math.uwaterloo.ca/hac/`.

[SH98b] SCHULZKI-HADDOUTI, CHRISTIANE: *Überwachungskontinent Europa. EU-Pläne für Überwachungsmaßnahmen enthüllt*. c't Magazin für Computertechnik, 25:48–49, 1998, `http://www.heise.de/ct/98/25/048/`.

[SJS02] SUN MICROSYSTEMS, INC: *jarsigner - JAR Signing and Verification Tool*. Windows2000 Magazin, 2002, `http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/jarsigner.html`.

[SKT02] SUN MICROSYSTEMS, INC: *keytool - Key and Certificate Management Tool*. 2002, `http://java.sun.com/j2se/1.5.0/docs/tooldocs/windows/keytool.html`.

[SLES05] SCHMOLDT, ROLF: *Leitfaden Elektronische Signatur, Signaturen mit und ohne Zertifikate Signaturen mit eigenhändigen Unterschriften*, Juni 2005, `http://www.signature-perfect.com`.

[SM05] SIWEK, MARTIN: *Sesam, logg mich ein*. LANline Spezial, V/2005:52, 2005.

[SSX02] XENITELLIS, SYMEON (SIMOS): *The OpenSource PKI Book:A guide to PKIs and OpenSource Implementations*. http://ospkibook.sourceforge.net/, jun 2002, `http://ospkibook.sourceforge.net/`.

[stw97] UNBEKANNT: *European Union and FBI Launch Global Surveillance System*. Technischer Bericht, Statewatch, PO Box 1516, London N16 0EW, UK, Februar 1997. erhältlich unter: `http://www.privacy.org/pi/activities/tapping/statewatch_tap_297.html`.

[TR05] BEN SCHWAN), MICHELLE DELLO (ÜBERSETZUNG:: *Verschlüsselung soll einfacher werden*. 2005, `http://www.heise.de/tr/aktuell/meldung/print/55303`.

[Wie98] M.J.WIENER: *Performance Comparison of Public-Key Cryptosystems*. RSA CryptoBytes, Volume 4(Number 1), 1998.

[Wri98a] WRIGHT, STEVE: *An appraisal of technologies for political control*. Report für das Europ. Parlament, Januar 1998.

[Wri98b] WRIGHT, STEVE: *An appraisal of technologies for political control*. STOA Interim Study, Executive Summary, 1998, `http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm`.