GBS

PKI-Grundlagen

- Eine Einführung –

Public-Key-Infrastrukturen und die Verschlüsselungsmethoden PGP und S/MIME

Expertise matters

Inhalt

1 Zusammenfassung

Der Umfang der Kommunikation per E-Mail ist in den letzten Jahren stark gewachsen und wächst immer weiter. Mittlerweile gibt es kaum noch ein Unternehmen, welches E-Mail für die Abwicklung ihrer Geschäftsprozesse sowohl innerhalb des Unternehmens als auch mit externen Geschäftspartnern nicht verwendet. Neben schnellen Reaktionszeiten, ständiger Erreichbarkeit und kostengünstiger Kommunikation steht die Frage nach der Sicherheit von E-Mails im Vordergrund, u. A. die Sicherstellung der E-Mail-Vertraulichkeit. Viele Unternehmen setzen deshalb auf E-Mail-Sicherheitslösungen, die auch die Verschlüsselung von E-Mails beinhalten. Die iQ.Suite von GBS Software bietet eine umfassende und vollständige richtlinienbasierte Lösung mit dem Modul iQ.Suite Crypt Pro.

Die vorliegende Dokumentation gibt einen Überblick über Public-Key-Infrastrukturen und die beiden Verschlüsselungsmethoden PGP und S/MIME.

2 Public-Key-Infrastrukturen

In diesem Abschnitt geht es um das Management von öffentlichen Schlüsseln. Werden die öffentlichen Schlüssel z.B. in einer Datenbank oder einem Verzeichnis verwaltet und sind dort auch jedem zugänglich, so wird von einer Public-Key-Infrastruktur (PKI) gesprochen.

2.1 Grundbegriffe und Definitionen

Eine PKI ist eine Kombination aus Hardware- und Softwarekomponenten, Policen und verschiedenen Prozeduren. Sie basiert auf Objekten, die Zertifikate genannte werden, und als digitale Ausweise dienen. Zertifikate verbinden die Benutzer mit ihren öffentlichen Schlüsseln.

Eine PKI besteht aus:

- einer Sicherheitsrichtlinie - definiert den Sicherheitsgrad, die Prozesse und Verwendungen der Kryptographie; beinhaltet Angaben über das Handling von Schlüsseln und wertvollen Informationen,
- einer Zertifizierungsstelle (Certification Authority – CA) – diese Instanz ist die Vertrauensbasis der PKI und erstellt die Zertifikate,
- einer Registrierungsstelle (Registration Authority – RA) - die Schnittstelle zwischen Benutzer und CA; erfasst und authentifiziert die Identität der Benutzer und reicht die Anfrage nach einem Zertifikat an die CA weiter,
- einem Verteilungssystem für die Zertifikate - beispielsweise die Verteilung durch die Nutzer selbst oder einen Verzeichnisserver wie LDAP. Die Verteilung hängt von der PKI-Umgebung ab.
- PKI-Applikationen: z.B. E-Mails, Kommunikation zwischen Webserver und Webbrowser.

Die Einheit aus CA und RA wird auch als TrustCenter bezeichnet und dient der Authentifizierung von Personen und ihren Nachrichten.

2.2 Alternativen zu PKI

Der Aufbau einer Public Key Infrastruktur ist in Abhängigkeit von der Anzahl der in der PKI enthaltenen Benutzer oft sehr aufwändig. Eine PKI wird in den meisten Fällen dann eingerichtet, wenn neben einer E-Mail-Verschlüsselung auch Zugangskontrollen zu Einrichtungen, Bereichen oder Gebäuden über eine einzige Karte oder Themen wie Single-Sign-On mit Smartcards gelöst werden sollen. Wenn es um die sichere (verschlüsselte) Übertragung von Nachrichten über das Internet geht, ist eine serverbasierte Lösung ein alternativer Weg (siehe dazu auch das Whitepaper „PKI-Alternative“). Eine sichere Verbindung von beliebigen Clients zum Server wird in den Unternehmen durch andere Möglichkeiten realisiert, z.B. durch VPN. Um eine E-Mail während der Übertragung über das Internet zu verschlüsseln oder die Unveränderbarkeit einer Nachricht durch eine Signatur zu gewährleisten, ist unter Berücksichtigung des Kosten-Nutzen-Aufwandes ein serverbasierter Ansatz eine sehr gute Lösung.

2.3 LDAP

LDAP (Lightweight Directory Access Protocol) ist ein offener Standard für globale oder lokale Verzeichnisdienste, z.B. im Netzwerk und/oder im Internet. Vergleichbar ist ein Verzeichnis mit einem Telefonbuch. Meist wird ein LDAP-Verzeichnis dazu verwendet, Namen mit Telefonnummern und E-Mail-Adressen zu verknüpfen, es kann aber auch andere Informationen verarbeiten. LDAP-Verzeichnisse sind so konzipiert, dass unter der Voraussetzung, dass sich die Daten im Verzeichnis nicht sehr häufig ändern, eine hohe Performance bei vielen Anfragen gewährleistet wird.

LDAP hat folgende Eigenschaften:

- LDAP ist ein Client-Server-System. Der LDAP-Client liefert oder erhält Informationen vom LDAP-Server. Der LDAP-Server verwaltet in dem Verzeichnis die Informationen, gibt gegebenenfalls Anfragen an einen anderen LDAP-Server weiter oder übernimmt die Informationen in sein Verzeichnis.
- LDAP wird manchmal auch als X.500 Lite bezeichnet. X.500 ist ein internationaler Standard für Verzeichnisse. X.500 ist mit umfangreichen Funktionen ausgestattet, sehr komplex, erfordert hohe Rechenleistungen und beinhaltet das vollständige OSI-Schichtenmodell[1]. LDAP kann im Gegensatz dazu ohne weiteres auf einem PC und über TCP/IP ausgeführt werden. LDAP kann auf X.500-Verzeichnisse zugreifen, unterstützt jedoch nicht alle Funktionen von X.500.
- Der Hauptvorteil von LDAP ist die Verdichtung von bestimmten Informationsarten und die im Vergleich zu X.500 leichte Implementierung.
- LDAP kann nur in Verbindung mit LDAP-fähigen Anwendungsprogrammen oder LDAP-Gateways verwendet werden. LDAP unterstützt zwar die Funktionen zur Zugangskontrolle in bestimmtem Umfang, verfügt jedoch nicht über so viele Sicherheitsmerkmale wie X.500.
- LDAP ist ein offenes, konfigurierbares Protokoll. Es kann fast alle Informationen im Zusammenhang mit bestimmten Organisationsstrukturen speichern.

[1] Open Systems Interconnection (OSI - eine Arbeitsgruppe der ISO). Das danach benannte Schichtenmodell ist ein internationales Referenzmodell für die Datenübertragung in Netzwerken. Es besteht aus sieben Schichten.

- LDAP wird häufig als zentraler Authentifikationsservice verwendet. Benutzer haben damit ein einheitliches Login, z.B. für Konsolen-Login, POP-Server, IMAP-Server, mit dem Netzwerk verbundenen Computern etc. Bei der Verwendung von LDAP kann eine Benutzer-ID und ein Passwort für alle Logins verwendet werden. Die Administration wird damit erheblich vereinfacht.

Allgemein beschreibt die LDAP-Terminologie:

- Ein Eintrag (Entry) stellt in einem LDAP-Verzeichnis eine Einheit dar. Ein Eintrag wird durch seinen eindeutigen Namen (Distinguished Name, DN) identifiziert bzw. referenziert.
- Ein Eintrag besitzt Attribute, bei denen es sich um direkt mit dem Eintrag verbundene einzelne Informationen handelt. Eine Organisation könnte zum Beispiel ein LDAP-Eintrag sein. Mit dieser Organisation verknüpfte Attribute können zum Beispiel die Faxnummer, die Adresse usw. sein. Auch Mitarbeiter können Einträge in einem LDAP-Verzeichnis sein. Übliche Attribute für Mitarbeiter sind Telefonnummern und E-Mail-Adressen.
- Bestimmte Attribute sind obligatorisch, während andere Attribute optional sind. In einer Objektklasse (object class) ist festgelegt, welche Attribute obligatorisch und welche optional sind.
- Das LDAP-Datenaustauschformat (LDAP Data Interchange Format, LDIF) ist ein ASCII-Textformat für LDAP-Einträge. Dateien, die Daten von einem LDAP-Server importieren oder zu einem LDAP-Server exportieren, müssen im LDIF-Format vorliegen.

2.4 Zertifikate

2.4.1 Grundlagen

Zertifikate sind Dokumente, die eine bestimmte Identität bezeugen. Ein Zertifikat ist vergleichbar mit einer amtlichen Urkunde oder einem Reisepass.

Im Zusammenhang mit iQ.Suite Crypt Pro werden nur Zertifikate betrachtet, die in digitaler Form vorliegen. Im Weiteren wird nicht von digitalem Zertifikat, sondern nur noch von Zertifikat gesprochen.

Mit dem Zertifikat garantiert die Zertifizierungsstelle (CA), das der vorliegende öffentliche Schlüssel (Public-Key) wirklich zu der Person, Gruppe, Firma gehört, die den Schlüssel vorlegt. Zu diesem Zweck werden die benötigten identifizierenden Informationen im Zertifikat festgehalten. Nachdem die Registrierungsstelle (RA) die Identität festgestellt hat, wird das Zertifikat von der Zertifizierungsstelle (CA) unterschrieben (digital). Damit bürgt die Zertifizierungsstelle für die Identität. Die Zertifizierungsstelle unterschreibt mit ihrem eigenen privaten Schlüssel (Privat-Key).

Zertifikate können zum Beispiel für Personen, Gruppen, Unternehmen oder für Server ausgestellt werden. Man spricht dann von Personen-, Gruppen-, Unternehmens- oder Serverzertifikaten.

Zur Identitätsprüfung werden -- abhängig von den Ansprüchen im jeweiligen Fall -- unterschiedliche Techniken eingesetzt. Vielleicht wird lediglich die E-Mail-Adresse einer Person geprüft. In manchen Fällen muss eine Person allerdings persönlich vorsprechen und einen amtlichen Ausweis vorlegen, um ein Zertifikat zu erhalten.

Zertifikate können mittels Softwarelösungen erstellt werden, z.B. S-Trust, PGP, Microsoft CA-Server.

Die am häufigsten verwendeten Zertifikate sind:

- PGP Zertifikat (siehe Zertifikatsarten in PGP)
- X.509 Zertifikat (siehe Zertifikat X.509 v3)

2.4.2 Notwendigkeit von Zertifikaten

Das Problem der Schlüsselverteilung bei asymmetrischen Kryptosystemen wird oft nicht richtig erkannt. Es wird betrachtet, dass öffentliche Schlüssel über einen unsicheren Kanal ausgetauscht werden. Dabei wird „Abhören“ als einzige Gefährdung der Kommunikationssicherheit betrachtet.

Es muss jedoch mit aktiven Angriffen gerechnet werden:

- Der öffentliche Schlüssel KA von Benutzer A wird durch Benutzer B abgefangen und durch einen eigenen Schlüssel KA* ersetzt.
- In der Datenbank befindet sich der ausgetauschte Schlüssel KA*, der von einem anderen Benutzer abgeholt wird, damit seine Nachricht verschlüsselt und an Benutzer A sendet.
- Benutzer B fängt die Nachricht ab und entschlüsselt sie mit dem zu KA* gehörigen privaten Schlüssel. Er kann die Nachricht lesen und verändern.
- Dann verschlüsselt Benutzer B die Nachricht mit dem öffentlichen Schlüssel von Benutzer A und sendet sie an Benutzer A, der sie mit seinem privaten Schlüssel entschlüsselt.

Weder Benutzer A noch der Sender der Nachricht haben den Angriff bemerkt.

Um sich vor diesen aktiven Angriffen zu schützen, werden Zertifikate verwendet. Mittels Zertifikaten kann ein sicherer Austausch von Schlüsseln erfolgen.

Zertifikate müssen deshalb wie Ausweise geschützt werden vor:

- Fälschung: durch die Unterschrift der autorisierten Stelle
- Missbrauch: es wird eine Gültigkeitsspanne eingesetzt. Diese kann sehr kurz sein, da die Ausstellung neuer Zertifikate relativ unproblematisch ist.

Eine Datenbank mit Einträgen gesperrter Zertifikate heißt Certificate Revocation List (CRL).

2.4.3 Zertifikat X.509 v3

Das CCITT und die ISO haben eine Standardisierung für digitale Zertifikate vereinbart, das Directory Authentication Framework [CITT509], auch X.509-Protokoll genannt.

Das X.509-Protokoll beschreibt den Aufbau von Zertifikaten, ist zur Zeit in der Version 3 verfügbar und wurde in ANSI und ISO übernommen. X.509 ist der aktuell am meisten verbreitete Standard.

Ein Zertifikat muss mindestens

- den Inhaber
- den öffentlicher Schlüssel des Inhabers
- die Signatur der CA

enthalten.

Ein X.509-Zertifikat hat folgende zusätzliche notwendige Informationen:

- Version
- Seriennummer
- Algorithmus
- Name des Ausstellers
- Geltungsdauer
- Name des Benutzers
- Öffentlicher Schlüssel des Benutzers
- Unique Identifier des Ausstellers
- Unique Identifier des Benutzers
- Erweiterungen
- Signatur

Im Feld der Erweiterungen sind als Wichtigste zu nennen:

- Certificate Policies - beinhaltet die Konditionen, unter denen die CA arbeitet (z.B. Sicherheitsvorkehrungen bei der Zertifizierung, usw.).
- CRL Distribution Points - bezeichnet den Punkt (IP-Adresse), wo die Information über widerrufene Zertifikate gefunden werden können.

Gegenüber PGP-Zertifikaten bestehen eine Reihe von Unterschieden:

- X.509 Zertifikate erhält man von einer CA-Stelle, PGP Zertifikate kann man selbst erstellen.
- X.509 Zertifikate unterstützen nur einen Namen für den Schlüsseleigner.
- X.509 Zertifikate unterstützen nur eine einzige Signatur, um den Schlüssel zu bestätigen.

2.4.4 Widerrufene Zertifikate (Certificate Revocation)

Missbrauchte Zertifikate müssen erkannt und für alle erkennbar widerrufen werden. Widerrufene Zertifikate werden in einer Certificate Revocation List (CRL) aufgeführt. Zertifikate werden während ihrer Gültigkeitsperiode von der Zertifizierungsstelle z.B. in folgenden Fällen für ungültig erklärt: Bekannt werden des Passwortes, Missbrauch des Zertifikates, Zertifikatsbesitzer verlässt das Unternehmen, für welches das Zertifikat ausgestellt worden ist, etc. Eine CRL Version 2 hat folgenden Aufbau:

- Version
- Algorithmus
- Name des Ausstellers
- Ausgabezeitpunkt dieser CRL
- Ausgabezeitpunkt einer neuen CRL
- Seriennummer der widerrufenen Zertifikate
- Erweiterungen
- Signatur

Ein gesperrtes Zertifikat muss wenigstens solange in der Sperrliste verbleiben, bis die Gültigkeitsdauer abgelaufen ist.

Die Sperrliste muss den Teilnehmern der Sicherheitsinfrastruktur regelmäßig aktuell zur Verfügung gestellt werden, damit diese jederzeit die Vertrauenswürdigkeit eines Zertifikates überprüfen können und der Missbrauch durch Angreifer, die sich unerlaubt in den Besitz fremder Zertifikate und der dazugehörigen Schlüssel gebracht haben, zu verhindern.

Probleme mit CRLs:

1. Wenn ein Zertifikat widerrufen wird, kann es erst bei der Ausgabe der nächsten CRL bekannt gemacht werden. Die Zeitspanne kann einige Stunden bis zu einige Wochen betragen.
2. Die Größe der CRL hängt von der Anzahl der Benutzer einer Zertifizierungsstelle und der Gültigkeitsdauer der ausgestellten Zertifikate ab.

2.5 Zertifizierungsstelle

Infrastrukturen für Sicherheit mit einer zentralen Zertifizierungsstelle (CA) haben die Aufgaben:

- Ausstellen von Zertifikaten/Zertifizieren von Schlüsseln,
- Sperrlisten pflegen und veröffentlichen.

Beim Ausstellen eines Zertifikates bindet die CA den Namen eines Anwenders an dessen öffentlichen Schlüssel. Der Aufbau eines x.509-Zertifikates ist in Zertifikate: Grundlagen beschrieben. Die CA bürgt dafür, dass der Name und der öffentliche Schlüssel im Zertifikat zu derselben Person gehören. Die CA stellt sicher, dass sich der Antragsteller für ein Zertifikat gegenüber der CA identifiziert.

Es ist deshalb notwendig, dass alle beteiligten Personen dem öffentlichen Schlüssel der CA vertrauen. Wird der private Schlüssel der CA kompromittiert, müssen alle Anwenderzertifikate neu ausgestellt werden.

Eine CA ist mit einer Ausweisstelle vergleichbar. Bekommt ein unbefugter Benutzer die Möglichkeit, Ausweise zu erzeugen, kann damit großer Schaden angerichtet werden. Dementsprechend sollte eine Umgebung, in der eine CA betrieben wird, entsprechend gesichert sein.

CAs lassen sich in einer Baumstruktur darstellen. Die Baumstruktur kann beliebig komplex sein. Die Basis-CA ist die Wurzel des Baumes, seine Blätter sind die zertifizierten Anwender. Dazwischen können noch weitere CAs liegen, die von der jeweils übergeordneten CA zertifiziert werden. Die Basis-CA wird von keiner anderen Stelle zertifiziert, d.h. sie ist per se für alle vertrauenswürdig.

Für die Verbindung zweier verschiedener Public-Key-Infrastrukturen gibt es zwei alternative Wege:

1. Man verschafft sich eine dritte CA, die über den beiden zu verbindenden steht.
2. Die beiden CAs zertifizieren sich gegenseitig und erkennen damit auch alle Benutzerzertifikate an, die die andere CA ausgestellt hat.

2.6 Zertifizierungsvorgang

Ein Zertifikat besteht im Wesentlichen aus dem eigenen öffentlichen Schlüssel. Um diesen von der zuständigen Zertifizierungsstelle beglaubigen zu lassen, muss zunächst das Schlüsselpaar erzeugt und dann der öffentliche Schlüssel von der Zertifizierungsstelle signiert werden.

Es gibt zwei Wege, wie eine CA Zertifikate ausstellt:

1. Der Anwender generiert sein Schlüsselpaar selbst und gibt den öffentlichen Schlüssel der CA zur Zertifizierung.
2. Die CA erstellt die Schlüsselpaare für die Anwender.

Die beiden Varianten haben Vor- und Nachteile.

Fall 1. - Anwender erzeugt den Schlüssel:

Vorteil:

- Der Anwender erzeugt sein Schlüsselpaar selbst und schickt nur den öffentlichen Schlüssel an die CA. Diese signiert ihn und schickt das dadurch entstandene Zertifikat an den Anwender zurück. Die CA muss sich davon überzeugen, dass der erhaltene öffentliche Schlüssel auch wirklich zu dem Anwender gehört, bevor eine Signatur geleistet, also das Zertifikat ausgestellt wird. Hierzu kann es nötig sein, dass sich die Person mit einem Ausweis (Personal- oder Werksausweis) bei der CA meldet. Ein Telefonat oder eine E-Mail zur Prüfung der Identität sind hierzu nicht geeignet. Dieses Verfahren gibt dem Anwender die Gewissheit, dass kein Zweiter im Besitz seines privaten Schlüssels ist.
- Die übermittelten Informationen wie öffentlicher Schlüssel und Zertifikat verursachen keine Sicherheitsprobleme. Alle transportierten Informationen sind ohnehin öffentlich. Alle sensitiven Informationen wie Passwort oder privater Schlüssel verbleiben beim Anwender. Es muss nur z.B. durch eine Überprüfung des öffentlichen Schlüssels sichergestellt werden, dass dieser nicht manipuliert wurde.

Nachteil:

- Der Anwender muss dafür sorgen, dass er eine Kopie seines Schlüsselpaars an einem sicheren Platz aufbewahrt (z. B. Tresor) falls er es im Verlustfall (z. B. Plattencrash) nochmals benötigt. Sonst muss ein neues Schlüsselpaar generiert werden und der neue öffentliche Schlüssel muss erneut von der CA zertifiziert werden.
- Der Transport des öffentlichen Schlüssels vom Anwender zur CA und des Zertifikates von der CA zurück zum Anwender muss erfolgen.

Fall 2. - CA erzeugt Schlüssel:

Vorteil:

- Die CA erzeugt die Schlüssel. Damit ist es möglich, sie CA-seitig aufzubewahren. Benötigt der Anwender sein Schlüsselpaar irgendwann einmal wieder (z. B. wegen Datenverlust nach Plattencrash), dann kann er sich dieses von der CA erneut geben lassen.
- Der Anwender ist von sämtlichen Sicherungsaufgaben entbunden.
- Die CA kann das Zertifikat in einem einzigen Arbeitsgang erstellen, d.h. die Durchführung ist sehr einfach.

Nachteil:

- Es muss ein Vertrauensverhältnis zwischen den Teilnehmern der Sicherheitsinfrastruktur und der CA existieren, da der private Schlüssel des Teilnehmers auch auf der Seite der CA vorhanden ist.

Bei der Auslieferung der Zertifikate an die jeweiligen Anwender muss die CA sicherstellen, dass die Zertifikate korrekt zugeordnet werden.

3 PGP

PGP wurde von Phil Zimmerman, einem Programmierer aus den USA, implementiert und in der Public Domain, also für jeden Internet-Teilnehmer zugänglich, freigegeben. Für kommerzielle Anwender wurde das Programm von der Firma PGP Corporation in Lizenz genommen.

3.1 Verschlüsselung und Signatur

PGP ist ein hybrides Kryptoverfahren. Wenn ein Benutzer eine Nachricht mit PGP verschlüsselt, so arbeitet PGP mit folgenden Schritten:

1. PGP komprimiert die Nachricht (Plain Text). Viele Plain Texte haben ein Dateimuster (Filepattern), den kryptoanalytische Verfahren zur Analyse und zum Erkennen des Schlüssels nutzen können. Durch die Komprimierung wird es deutlich schwerer, den Schlüssel zu analysieren.
2. PGP erzeugt einen Sitzungsschlüssel (Session Key), der nur einmal verwendet wird. Dieser zufällig erzeugte Session Key dient als Schlüssel für einen starken, konventionellen Verschlüsselungsalgorithmus. Anschließend liegt eine verschlüsselte Nachricht vor.
3. Der Sitzungsschlüssel wird mit dem öffentlichen Schlüssel des Empfängers der Nachricht verschlüsselt.
4. Der vom Public-Key verschlüsselte Session Key und die verschlüsselte Nachricht werden versandt.
5. Die Entschlüsselung beim Empfänger erfolgt umgekehrt.

Die Nachrichten können mit PGP auch signiert werden. PGP nutzt eine sichere Hashfunktion, um aus einem Nachrichtentext den Hashwert zu erzeugen. Der Hashwert hat eine feste Länge, unabhängig von der Nachricht. Mit diesem Hashwert und dem privaten Schlüssel des Absenders erfolgt die Signatur der Nachricht. PGP transportiert die Nachricht und die Signatur zum Empfänger. Falls der Empfänger ebenfalls PGP verwendet, kann er die Signatur unter Verwendung des öffentlichen Schlüssels des Absenders überprüfen.

3.2 Zertifikatsarten in PGP

PGP unterscheidet zwei Arten von Zertifikaten für Schlüssel:

- PGP Zertifikate
- X.509 Zertifikate (siehe Zertifikat X.509 v3)

Das PGP Zertifikat beinhaltet (ist nicht begrenzt):

- die PGP-Version,
- den öffentlichen Schlüssel des Benutzers - zusammen mit seinem Algorithmus: RSA, Diffie-Hellman oder DSS,
- Informationen über den Zertifikats Benutzer – z.B. den Namen, die Benutzer-ID, usw.,
- die digitale Signatur des Zertifikat,
- die Gültigkeitsdauer des Zertifikates,
- der bevorzugte symmetrische Verschlüsselungs-Algorithmus – unterstützte Algorithmen sind u. A. CAST, IDEA oder Triple-DES.

PGP bietet verschiedene Funktionen. Es generiert ein oder mehrere Schlüsselpaare für den Benutzer. Es nimmt neue öffentliche Schlüssel von Empfängern auf, verwaltet diese, und ermöglicht die Verwendung von Verschlüsselungs- und Authentifizierungsprozeduren für Nachrichten.

Die Länge des Schlüssels kann 512, 768,1024 oder 2048 Bit sein, je nach PGP-Version. Die Erstellung und Zuordnung der Schlüssel geht folgendermaßen vor sich:

- Um die Originalität und Zufälligkeit zu garantieren, wird eine zufällige Eingabe vom Anwender gefordert. Damit werden der öffentliche und der private Schlüssel generiert. Beide erhalten einen Timestamp (Zeitstempel, genaue Zeit ihrer Generierung nach Zeitzonen) und einen Identifier, der die 64 am wenigsten signifikanten Bits darstellt.
- Dem öffentlichen Schlüssel wird eine Benutzer-ID zugeordnet, die den Schlüssel einem bestimmten Mailempfänger zuordnet. Typischerweise ist das der Name, gefolgt von der E-Mail-Adresse in spitzen Klammern.
- Die Schlüssel werden in Schlüsselbunde, so genannte Key Rings, eingebunden. Man unterscheidet zwischen zwei Schlüsselbunden, einem öffentlichen Schlüsselbund (Public Key Ring) und einem privaten Schlüsselbund (Private Key Ring). Beide ordnen die Schlüssel nach Zeitstempel, Schlüssel-ID und Benutzer-ID. Der private Schlüsselbund enthält außerdem den öffentlichen Schlüssel des Anwenders und den privaten Schlüssel in verschlüsselter Form. Die Sicherung des privaten Schlüssels geschieht mittels Passwort (Passphrase), das bei jeder Verwendung abgefragt wird.

- Der öffentliche Schlüsselbund enthält die eingelesenen Schlüssel der Partner und für jeden dieser Schlüssel ein Vertrauenszeichen (Owner Trust), ein Originalitätszeichen (Key Legitimacy) sowie zwei weitere Absicherungskennzeichen (Signature(s), Signature Trust).

Zur Ablage der öffentlichen Schlüssel können grundsätzlich neben den lokalen Schlüsselbund-Dateien auch öffentliche Schlüsselserver (Key-Server) verwendet werden.

3.3 PGP Varianten

Einige Produkte/Programme auf Basis des PGP-Verfahrens werden im Folgenden kurz beschrieben.

- OpenPGP
  - Spezifikation für einen offenen Verschlüsselungsstandard, seit 1998 als IETF-Standard verabschiedet
  - keine Implementierung, lediglich Spezifikation
  - Abwärtskompatibel zu alten PGP-Versionen
- GnuPG
  - Aufgrund von Inkompatibilitäten zwischen PGP 6.0 und älteren Versionen entstanden
  - Neuimplementierung des OpenPGP-Standard
  - Kommandozeilenprogramm (eigentliches Verschlüsselungsprogramm)
  - Kann sowohl mit alten als auch mit neuen PGP-Versionen kommunizieren
  - GnuPG steht unter GPL-Lizenz
  - Weiterentwicklung wird von BMWi gefördert
  - Frontends sind z.B. GnuPP für Windows mit Plug-Ins z.B. für MS-Outlook, Pegasus etc.
- Kommerzielle Versionen
  - sind von der Firma PGP
  - Lizenz- und kostenpflichtig

4 S/MIME

S/MIME ist eine Erweiterung des E-Mail-Standards MIME. MIME (Multimedia Internet Mail Extension) erlaubt das Anhängen von Binärinformationen (Bilder, Klänge, Programme).

S/MIME steht für Secure Multipurpose Internet Mail Extension und ist in der Version 3 als Verschlüsselungsstandard von der Internet Engineering Task Force (IETF) anerkannt. Die Entwicklung wurde durch ein Herstellerkonsortium um RSA Security entwickelt. Dieser Verschlüsselungsstandard wird u. A. in den Mailkomponenten der Webbrowser von Microsoft unterstützt.

4.1 Verschlüsselung

S/MIME verwendet eine hybride Verschlüsselungstechnologie, d.h. eine schnelle symmetrische Verschlüsselung der eigentlichen Nachricht mit einem Sitzungsschlüssel und eine anschließende asymmetrische Verschlüsselung des Sitzungsschlüssels mit dem öffentlichen Schlüssel des Nachrichtenempfängers.

Für S/MIME in Version 3 bedeutet das, der asymmetrische Anteil des Schlüsselaustauschverfahrens erfolgt nach Diffie-Hellman und der symmetrische Anteil nach Triple-DES. RSA und MD5 werden ebenfalls unterstützt.

Zwischen den Versionen von S/MIME und PGP besteht keine Kompatibilität, trotz gleicher Algorithmen.

Die Schlüsselerzeugung kann mit geeigneter Software auf dem Client erfolgen. Die Software erstellt dabei ein so genanntes Zertifikat, das den öffentlichen Schlüssel, den privaten Schlüssel und die Signatur des Zertifikatsausstellers enthält. Aus diesem Zertifikat können mit der gleichen Software die einzelnen Schlüssel herausgelöst werden. Durch Export des Zertifikats lässt sich die Verwendbarkeit auch auf andere Programme ausdehnen, z.B. den Mail-Client The Outlook oder Thunderbird, die Mailkomponente in Mozilla.

4.2 Zertifikate

Um den öffentlichen Schlüssel zur Verschlüsselung und zur Verifikation der Signatur für andere zur Verfügung zu stellen, werden zwei verschiedene Wege eingeschlagen:

1. Anfrage beim Zertifizierer/Zertifikatsinhaber
2. Der öffentliche Schlüssel wird den signierten Daten automatisch angefügt

Die Gültigkeit eines Zertifikats wird in der Regel automatisch angezeigt. Zurückgezogene Zertifikate können beim Zertifizierer abgefragt werden.

Bei der Zertifizierung setzt S/MIME im Gegensatz zu PGP ausschließlich auf eine hierarchische Zertifizierungsstruktur mit X.509-Protokoll, d.h. die für die asymmetrische Verschlüsselung erforderlichen Schlüsselpaare werden von einer CA nach Prüfung der Identität elektronisch beglaubigt.

Dabei werden unterschiedliche Stufen der Identitätsprüfung angeboten:

- Prüfung, ob die Mailadresse existiert
- Prüfung der Identität des Schlüsseleigentümers anhand der Postanschrift
- Prüfung der Identität des Schlüsseleigentümers anhand von Dokumenten
- Prüfung der Identität des Schlüsseleigentümers durch einen Notar oder eine andere öffentliche Person

Die Anwendung von S/MIME hat zum heutigen Zeitpunkt einige Schwachstellen:

- Mit S/MIME signierte Daten, gemäß IETF-Spezifikation, werden in zwei Teilen gesendet. Die Daten getrennt von der Unterschrift. Beide Teile werden als zwei Teile einer mit dem MIME-Typ "Multi-part/Signed" formatierten Nachricht interpretiert. Vorteil ist, dass MIME-fähige Mailclients feststellen können, dass eine digitale Signatur anhängt. Für den Fall, dass der Client das Verschlüsselungsprotokoll nicht unterstützt, kann der Client dieses ignorieren und nur die Nachricht zur Anzeige bringen.
- Nachteil ist, dass einige Gateways diese Multipart-Nachrichtentypen als "nichttransparent" betrachten. Die Gateways prüfen, ob der nächste Knoten MIME oder 8bit unterstützt und wenn nicht, dann wandeln sie die Daten in ein passendes Format. Dabei wird in aller Regel die Signatur ungültig.

4.3 Unterschiede zwischen S/MIME und PGP

- Zertifikate erstellen
  - PGP wendet das sogenannte Web-of-Trust an, ein „Netzwerk gegenseitigen Vertrauens“. Die Gültigkeit eines Schlüssels einer Person wird auch dann anerkannt, wenn der zugehörige Schlüssel nicht überprüft wurde. Beim Web-of-Trust unterschreiben die Benutzer ihre Schlüssel, nach Überprüfung der Echtheit, gegenseitig. Dadurch hat jeder Nutzer die volle Kontrolle darüber, wem er wie weit vertraut. Der Nutzer kann verschiedene Vertrauensstufen einstellen. Damit das Web-of-Trust nicht umgangen werden kann, ist es wichtig, eine Stelle zu haben, der alle Nutzer vertrauen. Von dieser Stelle kann sich jeder Nutzer bestätigen lassen, dass ein Schlüssel wirklich der Person gehört, der er zu gehören vorgibt. Eine solche Stelle kann ein TrustCenter sein.
  - S/MIME hat eine strenge Hierarchie von X.509 Zertifikaten (siehe Public-Key-Infrastrukturen). **Hinweis:** Microsoft nimmt Nutzern mit Windows XP die Entscheidung über die Vertrauenswürdigkeit einer CA aus der Hand. Zertifikate werden automatisch als vertrauenswürdig eingestuft, wenn die ausstellende CA als von Microsoft vertrauenswürdig eingestufte CAs betrachtet wird.
- Zertifikate widerrufen
  - PGP kann eine Widerrufurkunde für erzeugte Schlüssel erstellen. Damit können andere Nutzer in Kenntnis gesetzt werden, dass der zugehörige öffentliche Schlüssel nicht mehr gültig ist. Das schließt die Möglichkeit des weiteren Einsatzes des Schlüssels nicht aus. Unterschriebene Dokumente können weiterhin mit dem Schlüssel überprüft werden. PGP speichert widerrufene Schlüssel auf dem gleichen Key-Server. Der Widerruf wird als eigene Signatur an den Schlüssel gehängt.
  - S/MIME verwendet die CRL (siehe Public-Key-Infrastrukturen). Die Benutzer müssen sich die Liste von speziellen CRL-Servern regelmäßig herunterladen.

Über GBS

GROUP Business Software ist führender Anbieter von Lösungen und Services in den Bereichen Messaging Security und Workflow für die IBM und Microsoft Collaboration Plattformen. Weltweit vertrauen mehr als 5.000 Kunden und 4 Millionen Anwender auf die Expertise von GBS. Der Konzern ist in Europa, Nordamerika sowie Asien tätig.

Weitere Informationen unter www.gbs.com