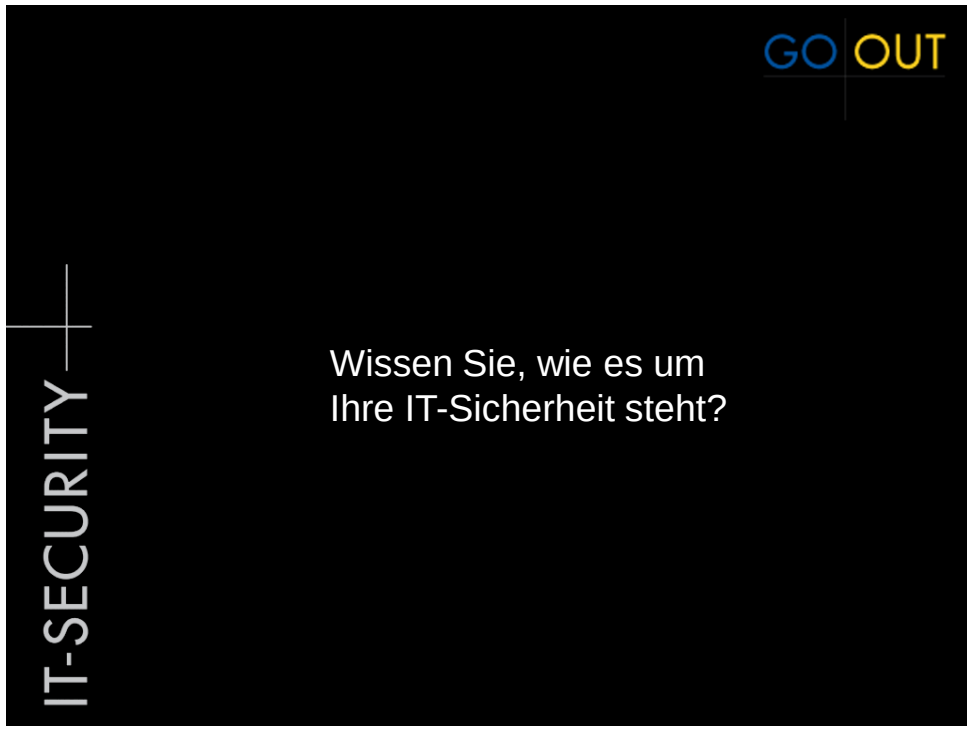

GO OUT
IT-SECURITY
Wissen Sie, wie es um
Ihre IT-Sicherheit steht?

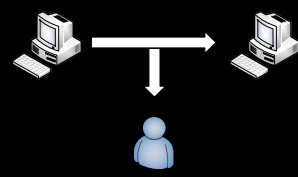

GO OUT
IT-SECURITY
Sichere E-Mail-Kommunikation
Andreas Wisler
GO OUT Production GmbH
Dipl. Ing FH, CISSP, CISA, ISO 27001 Lead Auditor
www.goSecurity.ch / wisler@goout.ch

GO OUT

Bedrohungen

IT-SECURITY

- **Abhören** von Nachrichten oder Einsicht in Nachrichten. Personen nehmen Einblick in Informationen oder Nachrichten, obwohl dies vom Verfasser der Nachricht oder der Information unerwünscht oder ungewollt ist.



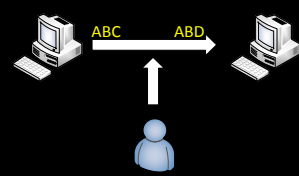
- **Löschen** (Delete) von Nachrichten oder Teile davon. Informationen, welche aufbewahrt oder gesandt werden sollen, werden vom Verfasser der Nachricht ungewollt oder von einem unberechtigten Dritten vorsätzlich gelöscht.

GO OUT

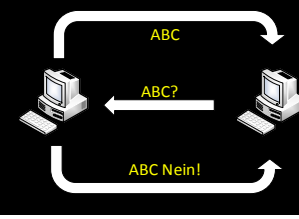
Bedrohungen

IT-SECURITY

- **Verändern** von Nachrichten. Hier wird eine Nachricht soweit verändert, dass der Sinn oder Zweck der ursprünglichen Nachricht nicht mehr mit der veränderten übereinstimmt.



- **Bestreiten** des Versands von Nachrichten (Non Repudiation of origin). Hier wird vom Absender einer Nachricht bestritten, dieNachricht versandt zu haben.

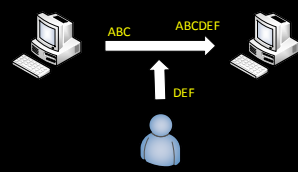


GO OUT

Bedrohungen

IT-SECURITY

- **Bestreiten** des Empfangs von Nachrichten (Non Repudiation of receipt). Hier wird vom Empfänger einer Nachricht bestritten, die Nachricht erhalten zu haben. (Rechts)
- **Einspeisen** von Nachrichten (Insertion). Hier werden von einer Person Nachrichten in die Kommunikation zweier oder mehrerer Teilnehmer eingefügt, welches von diesen Teilnehmern nicht erwünscht oder gewollt ist.

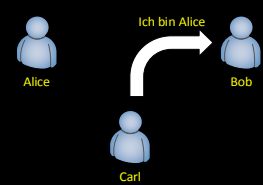


GO OUT

Bedrohungen

IT-SECURITY

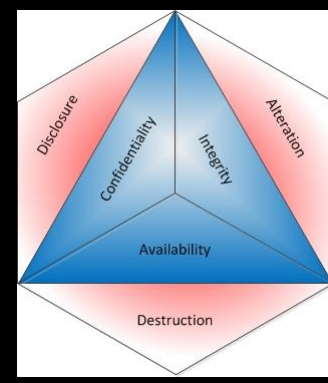
- **Wiederholen** von Nachrichten (Reply). Bei diesem Angriff werden von einer Person bereits versandte Nachrichten noch einmal in die Kommunikation eingespiesen. Doch dies ist den Kommunikationsteilnehmer unerwünscht.
- **Vortäuschen** einer anderen Identität (Masquerade). Eine Person gibt sich als eine andere Person aus, um eine andere Person in die Irre zu führen.



GO OUT

Ziel der Kryptographie

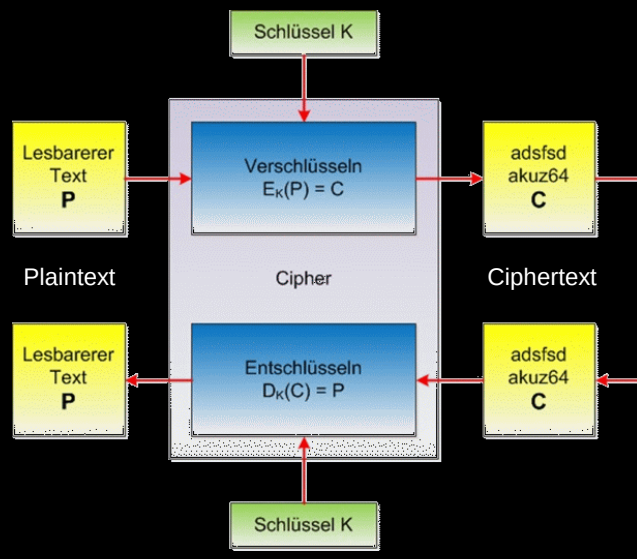
- Gewährleistung von
  - Integrität
  - Vertraulichkeit
  - Authentizität
  - Verbindlichkeit



IT-SECURITY

GO OUT

Begriffe der Kryptographie



IT-SECURITY

GO OUT

Begriffe der Kryptographie

IT-SECURITY

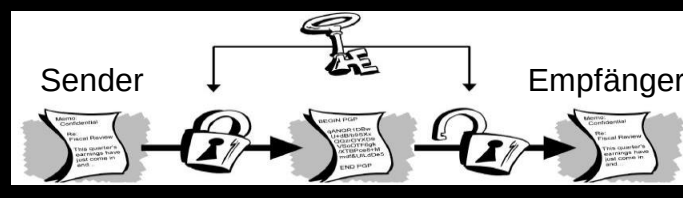
- **Plaintext**
  Daten die von jedermann gelesen und verstanden werden können
- **Encryption**
  verschlüsseln
- **Ciphertext**
  Darin ist die Botschaft vom „plaintext“ verschlüsselt enthalten. Der Inhalt der Botschaft ist nicht ersichtlich, auch nicht für diejenigen, welche den „ciphertext“ sehen können.
- **Decryption**
  Entschlüsseln - Wiederherstellen des Zustandes vor der Verschlüsselung
- **Algorithmus**
  Ein Set von Regeln, welche ver- & entschlüsseln

GO OUT

Symmetrische Verschlüsselung

IT-SECURITY

- ein einziger Schlüssel für die Ver- und Entschlüsselung
- sehr schnell
- Oft für lokale Verschlüsselung verwendet (Bitlocker, TrueCrypt, KeePass, etc.)
- problematische Schlüsselverteilung (darf nicht über den gleichen Weg erfolgen)



GO OUT

IT-SECURITY

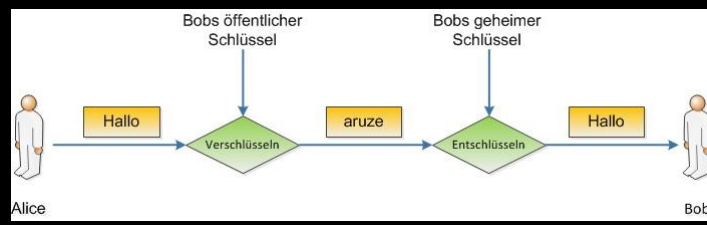
Asymmetrische Verschlüsselung

- Public Key Verschlüsselung
  - zur Verschlüsselung wird ein Schlüssel**paar** verwendet
  - mit dem öffentlichen Schlüssel werden die Daten verschlüsselt mit dem privaten Schlüssel entschlüsselt
  - der öffentliche Schlüssel ist allen bekannt, der private Schlüssel dagegen bleibt geheim

GO OUT

IT-SECURITY

Verschlüsselung

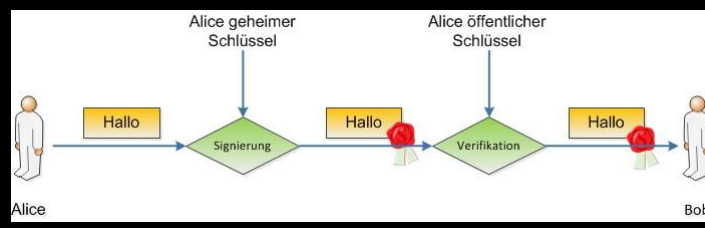


- Die Nachricht von Alice an Bob wird verschlüsselt über-tragen, indem die Nachricht zuerst mit dem öffentlichen Schlüssel (Public Key) verschlüsselt wird. Das Prinzip der PKI liegt darin, dass die Nachricht nur noch mit dem privaten Schlüssel (Private Key) entschlüsselt werden kann.

GO OUT

IT-SECURITY

Signierung



- Alice signiert die Nachricht mit dem eigenen privaten Schlüssel (Private Key) und schickt die Nachricht in Klartext an Bob. Somit ist sie für alle Stellen dazwischen lesbar. Mit dem öffentlichen Schlüssel von Alice (Public Key) kann Bob nun die Echtheit der Nachricht kontrollieren.

GO OUT

IT-SECURITY

Sichere E-Mail

GO OUT

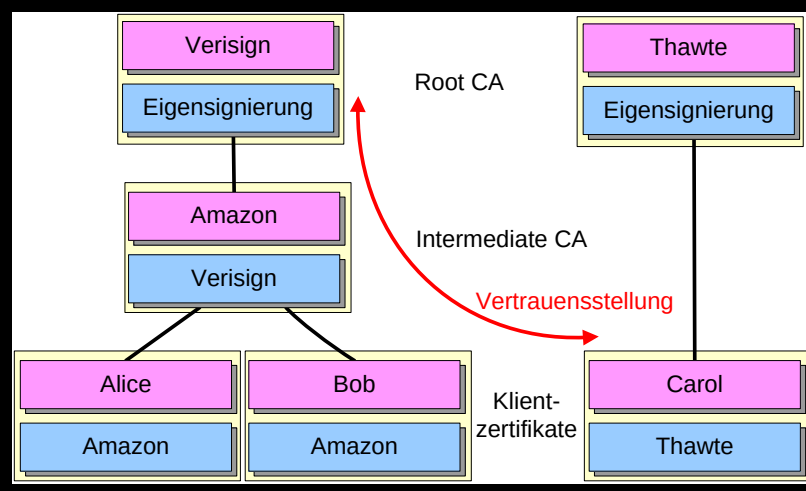
S/MIME Secure Mail Extensions

- S/MIME steht für Secure/Multipurpose Internet Mail Extension und bezeichnet ein Protokoll, welches die sichere Übertragung von MIME-Daten gewährleistet
- S/MIME garantiert dabei Vertraulichkeit und Integrität der Daten sowie die Authentifizierung des Kommunikationspartners
- Ein wesentlicher Vorteil dieses Protokolls ist, dass es völlig im Hintergrund und ohne Eingreifen des Benutzers arbeiten kann

IT-SECURITY

GO OUT

Vertrauenshierarchie

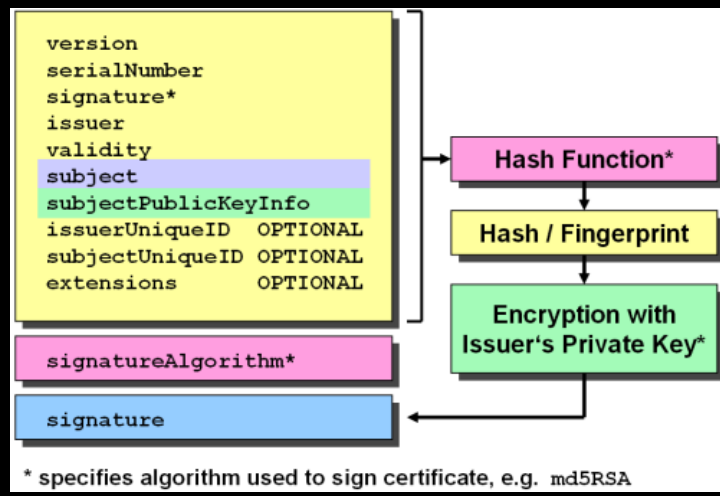


IT-SECURITY

GO OUT

IT-SECURITY

Struktur X.509



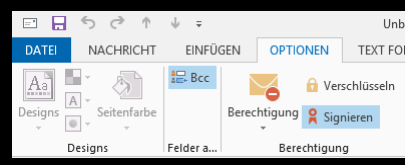
GO OUT

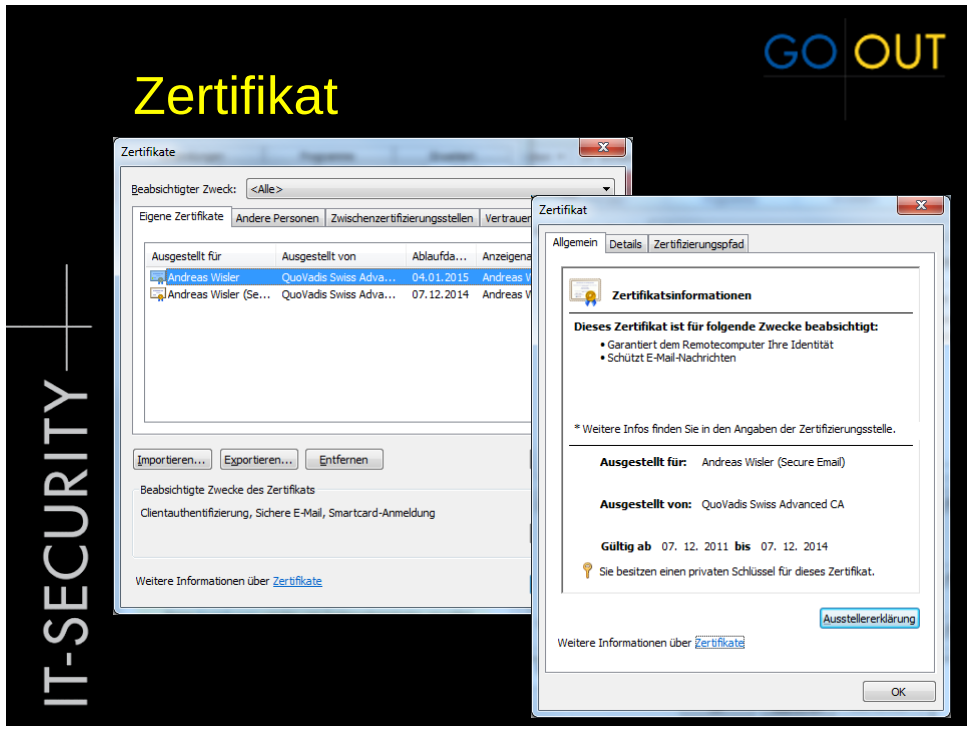
IT-SECURITY

Zertifikat

- Verschlüsselte E-Mail

- E-Mail Optionen




GO OUT
IT-SECURITY
Zertifikat
Zertifikate
Beabsichtigter Zweck: <Alle>
Eigene Zertifikate
Andere Personen
Zwischenzertifizierungsstellen
Vertrauer
Ausgestellt für
Ausgestellt von
Ablaufda...
Anzeigena
Andreas Wisler
QuoVadis Swiss Adva...
04.01.2015
Andreas W
Andreas Wisler (Se...
QuoVadis Swiss Adva...
07.12.2014
Andreas W
Importieren...
Exportieren...
Entfernen
Beabsichtigte Zwecke des Zertifikats
Clientauthentifizierung, Sichere E-Mail, Smartcard-Anmeldung
Weitere Informationen über Zertifikate
Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifikatsinformationen
Dieses Zertifikat ist für folgende Zwecke beabsichtigt:
• Garantiert dem Remotecomputer Ihre Identität
• Schützt E-Mail-Nachrichten
* Weitere Infos finden Sie in den Angaben der Zertifizierungsstelle.
Ausgestellt für: Andreas Wisler (Secure Email)
Ausgestellt von: QuoVadis Swiss Advanced CA
Gültig ab 07. 12. 2011 bis 07. 12. 2014
Sie besitzen einen privaten Schlüssel für dieses Zertifikat.
Ausstellererklärung
Weitere Informationen über Zertifikate
OK

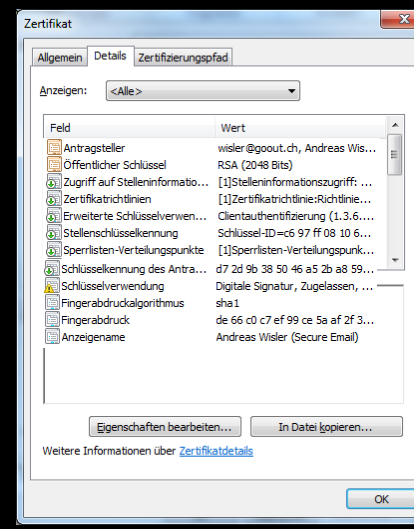

GO OUT
IT-SECURITY
Zertifikat
Zertifikat
Allgemein
Details
Zertifizierungspfad
Zertifizierungspfad
QuoVadis Root Certification Authority
QuoVadis Swiss Advanced CA
Andreas Wisler (Secure Email)
Zertifikat anzeigen
Zertifizierungsstatus:
Dieses Zertifikat ist gültig.
Weitere Informationen über Zertifizierungspfade
OK

GO OUT

IT-SECURITY

Zertifikat

- bestehend aus
  - Öffentlicher Schlüssel
  - Name des Antragstellers
  - Name der Ausgabestelle
  - Signatur des Zertifikates mit privatem Schlüssel der CA
  - Gültigkeit von / bis
  - Version X509
  - Seriennummer
  - Signaturalgorithmus der CA



GO OUT

IT-SECURITY

Gesetzliche Situation

- Seit 1. Januar 2005 werden elektronische Signaturen der handschriftliche Unterschriften gleichgestellt. → Bundesgesetz über die elektronische Signatur
- definiert die Bedingungen, unter denen Anbieterinnen von Zertifizierungsdiensten auf freiwilliger Basis anerkannt werden können, und regelt ihre Tätigkeiten im Bereich der elektronischen Zertifikate. Es legt zudem die Voraussetzungen fest, die eine elektronische Signatur erfüllen muss, um die gleichen Wirkungen wie eine handschriftliche Unterschrift erzielen zu können.
- Die neuen gesetzlichen Bestimmungen sind mit der geltenden Regelung der EU kompatibel.
- Informationen: www.admin.ch/ch/d/ff/2003/8221.pdf

GO OUT

SuisseID

- Die SuisseID ist ein standardisierter elektronischer Identitätsnachweis.
- Das SuisseID-System enthält drei Elemente:
  - Elektronischer Identitätsnachweis
  - Qualifizierte elektronische Signatur
  - Elektronischer Funktionsnachweis
- Anbieter
  - QuoVadis / Trüb
  - Post (Swiss Sign)
  - Swisscom (Unternehmen)
  - BIT (Verwaltungen)

IT-SECURITY

GO OUT

PGP Entstehungsgeschichte

- Verdienst von Phil Zimmermann
  - 1991: erste Freeware Version als Resultat eines Projektes
    - ohne finanzielle Unterstützung
    - ohne industrielle Unterstützung
    - als Ein-Personen Projekt
  - 1993-1996: Strafverfolgung von Phil Zimmermann
    - PGP benützt RSA and Merkle-Hellmann Technologie, beides Patentrechtlich geschützt.
    - Zusätzlich darf Verschlüsselungssoftware nicht aus den USA exportiert werden ohne die explizite Genehmigung vom State Department.

IT-SECURITY

GO OUT

IT-SECURITY

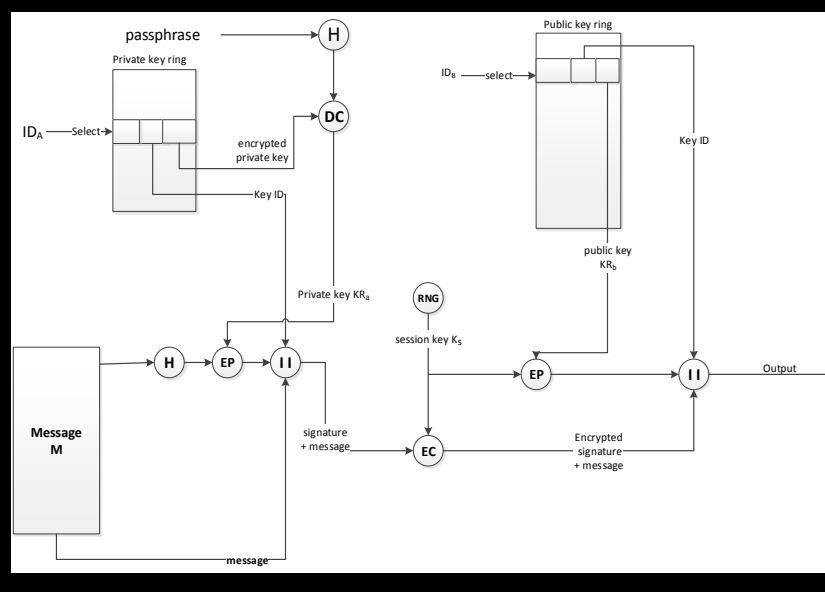
PGP

- Plattformübergreifend
- Weltweit verfügbar
- Basiert auf Algorithmen, die den „Zeittest“ bestanden haben
- viele Anwendungsformen (Benutzer bis Grossfirma)
- Weder entwickelt noch kontrolliert durch
  - Staatliche Institutionen
  - Standardisierungsgremien

GO OUT

IT-SECURITY

Verschlüsselung



GO OUT

Authentifikation

1. Der Sender erstellt die Nachricht.
2. Mit SHA-1 generiert er einen 160-bit langen Hash Code von der Nachricht.
3. Der Hash Code wird mit dem privaten RSA Schlüssel des Senders verschlüsselt und an die Nachricht angehängt.
4. Der Empfänger entschlüsselt den Hash Code mit dem Public RSA Schlüssel des Senders.
5. Der Empfänger berechnet den Hash Code vom Dokument und vergleicht ihn mit dem angehängten..

IT-SECURITY

GO OUT

Verschlüsselung

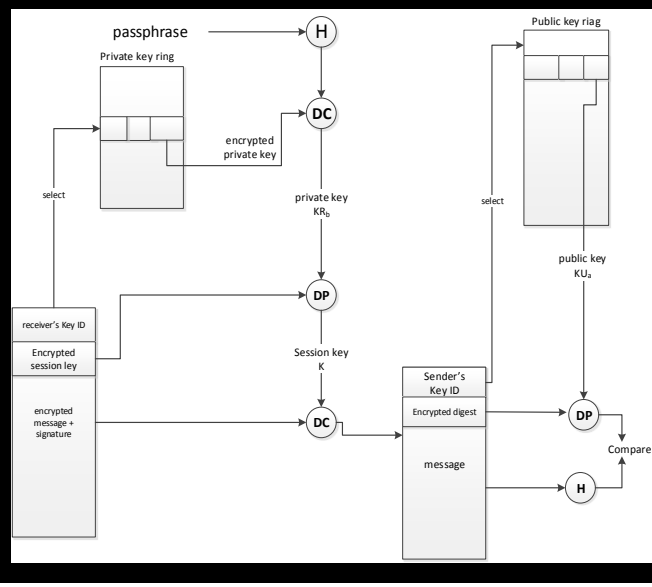
1. Der Sender generiert die Nachricht und eine Zufallszahl von 128 Bit (=Session Key für diese Nachricht).
2. Die Nachricht wird mit dem Session Key verschlüsselt (Algorithmen: CAST-128, IDEA oder 3DES)
3. Der Session Key wird mit dem RSA Public Key vom Empfänger verschlüsselt und der verschlüsselten Nachricht vorgehängt.
4. Der Empfänger entschlüsselt den Session Key mit seinem privaten RSA Key.
5. Mit dem Session Key kann er die Nachricht entschlüsseln.

IT-SECURITY

GO OUT

IT-SECURITY

Entschlüsselung



GO OUT

IT-SECURITY

Vgl. PGP & S/MIME

- Zertifikate haben bei S/MIME eine wesentlich höhere Bedeutung als bei PGP, was auch der Hauptunterschied zwischen den beiden ist
- Während PGP das Vertrauen in fremde Schlüssel dem Anwender überlässt („Web of Trust“) sind bei S/MIME Zertifikate nach dem X.509 Standard obligatorisch
- Praktisch alle E-Mail Clients unterstützen den S/MIME-Standard

Vgl. PGP & S/MIME

- Beide Standards unterscheiden sich in ihren Vetrauensmodellen und Datenformaten
- S/MIME & PGP sind zueinander nicht kompatibel
- Unternehmen streben eher S/MIME mit X.509 Zertifikaten an
- Die unklaren Vertrauensbeziehungen von PGP werden des Öfteren als „risikoreich“ empfunden
- Die PKI-Struktur auf der anderen Seite als sehr „unflexibel“. Das Schlüsselmanagement müssen „bezahlt“ werden
- Vertrauenswürdigkeit ist nur mit org. & techn. Mitteln zu erzielen

Fazit

- E-Mail-Verschlüsselung ist problemlos möglich
- Die Anwendung ist aber «komplex»
- Das Schlüsselhandling ist die grosse Herausforderung

- Nur wenn «alle» mitmachen, kann es sinnvoll genutzt werden

GO OUT

Mit uns wissen Sie,
wie es um Ihre IT-Sicherheit steht!

IT-SECURITY


A. Wisler


Th. Furrer


S. Müller


E. Kauth


A. Kulhanek


S. Walser


C. Wehrli


A. Zlateva


N. Rasstrigina


J. Kappeler

GO OUT

Dienstleistungen …

IT-SECURITY

IT-Security Audit
Quick Audit
Penetration Test

Review

QSEC

Projekt - Begleitung
IT-Security Konzepte