

Technische Grundlagen und Anforderungen

Thomas Kessler, In&Out AG

28. März 2001

1

FGSec PKI

Inhalt

- Public Key Kryptographie
 - Verschlüsseln und signieren
- Das PKI Puzzle
 - Anwendungsfälle und deren Anforderungen
- “Advanced PKI”
 - Akzeptieren von externen Zertifikaten

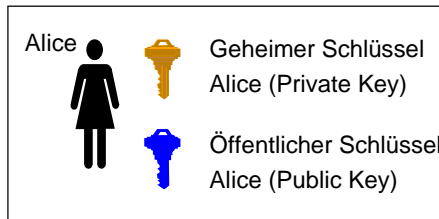
28. März 2001

2

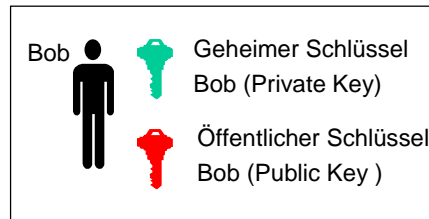
FGSec PKI

Public Key Kryptographie

Schlüsselpaar von Alice:



Schlüsselpaar von Bob:



Verschlüsseln: Alice verschlüsselt mit dem Public Key von Bob, Bob entschlüsselt mit seinem Private Key.

Signieren: Alice verschlüsselt („signiert“) mit ihrem Private Key, Bob entschlüsselt („prüft“) mit dem Public Key von Alice

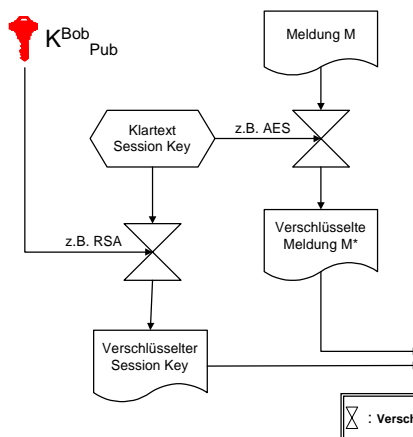
28. März 2001

3

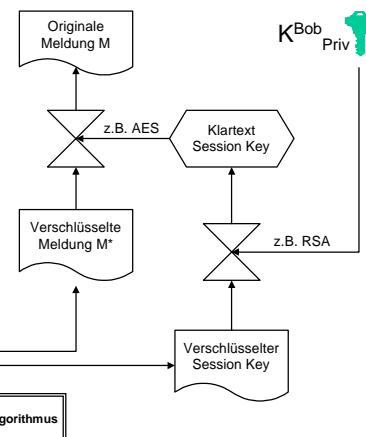
FGSec PKI

Verschlüsseln

Alice verschlüsselt:



Bob entschlüsselt:



⊗ : Verschlüsselungsalgorithmus

28. März 2001

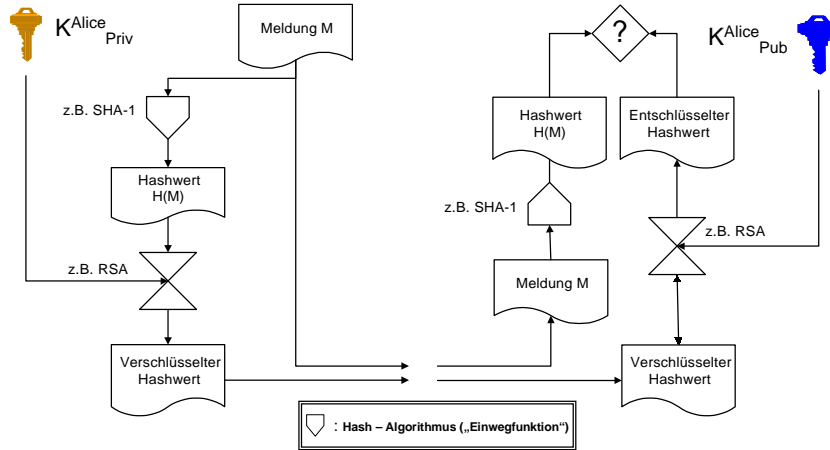
4

FGSec PKI

Signieren

Alice signiert:

Bob prüft die Unterschrift:

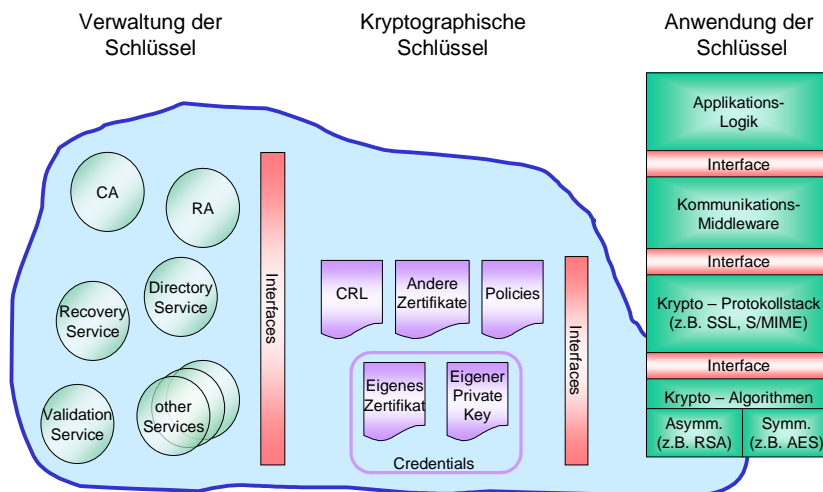


28. März 2001

5

FGSec PKI

Das PKI Puzzle



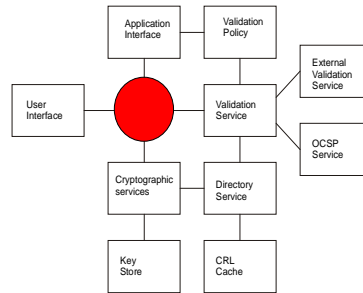
28. März 2001

6

FGSec PKI

Personal Security Environment

- Generieren des Schlüsselpaares
 - Qualität der Schlüssel (insb. Zufälligkeit)
 - Länge der Schlüssel
- Schützen des Private Key
 - Sichere Speicherung
 - Sichere Verarbeitung
- Bereitstellen von Interfaces
 - Benutzerinterface (GUI)
 - Applikationsinterfaces (API)
 - Verwaltungsinterfaces



28. März 2001

7

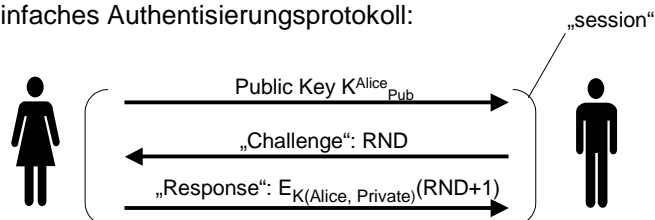
FGSec PKI

Erster (einfachster) Anwendungsfall:

Authentisierung

Kommunikationspartner sicher identifizieren

Ein einfaches Authentisierungsprotokoll:



Das Grundproblem:
Wie kann Bob sicher sein, dass $K^{\text{Alice}}_{\text{Pub}}$ wirklich Alice gehört ?

28. März 2001

8

FGSec PKI

Das Zertifikat

- Fälschungssichere Verknüpfung von Schlüsselhaber und Schlüsselpaar
- Das Zertifikat enthält folgende Informationen:
 - Name des Zertifikatsinhabers
 - Public Key des Zertifikatsinhabers
 - Name der Certification Authority (CA)
 - Digitale Signatur der CA
 - Weitere Angaben zum Zertifikat
 - z.B. Ausstellungs- und Verfalldatum, zulässige Nutzung
 - Evt. weitere Angaben zum Zertifikatsinhaber

28. März 2001

9

FGSec PKI

Zertifikats-Varianten

- X.509 v3: Das Standard-Zertifikat
 - SSL hat X.509 (Server-)Zertifikaten zum Durchbruch verholfen
 - S/MIME etabliert sich für Secure Mail und Fileverschlüsselung
 - IPSEC ISAKMP basiert ebenfalls auf X.509 Zertifikaten
- PGP-Zertifikat: Der Vorreiter
 - Lange vor SSL und S/MIME waren PGP-Zertifikate da
- SET-Zertifikat: Der Sonderling
 - SET Zertifikate sind zwar X.509 v3 aber inkompatibel
- SWIFT, EDIFACT, Lotus Notes, W2K, ...

28. März 2001

10

FGSec PKI

Extensions

- Um beliebige Attribute erweiterter Zertifikatsinhalt
 - Sicherheitsattribute und Rollen (Administrator,...)
 - Organisatorische Attribute (Organisation, Rang,...)
 - Persönliche Attribute (Muttersprache, Geburtsdatum,...)
 - Anwendungsspezifische Attribute (E-Mail Adresse,...)
- Extensions sind mit Vorsicht einzusetzen !
 - Erhöhter Administrationsaufwand
 - Verminderte Interoperabilität
 - “Attribute Certificates” als Lösung der Zukunft

28. März 2001

11

FGSec PKI

Browser-Darstellung



28. März 2001

12

FGSec PKI

Certification Authority

- Die CA “garantiert” für den Inhalt ihrer Zertifikate
 - CP (Certification Policy) und CPS (Certification Practice Statement) beschreiben den Umfang der “Garantie”
- Die CA zeichnet sich durch hohe Sicherheit aus
 - Sicherheit von CA-Signaturschlüssel und Betriebsumgebung
- Der CA Public Key ist jedem Teilnehmer bekannt
 - “Root-Zertifikat” muss verteilt werden

**Zertifikatsausstellung = Ausstellung eines Identitätsausweises
(oder einer „Member Card“ in geschlossenen Umgebungen)**

28. März 2001

13

FGSec PKI

Registration Authority

- Die RA erfasst die Zertifikats-Daten
 - Sehr unterschiedliche Verfahren sind möglich und im Einsatz
 - Registrierungsprozess ist zwischen CA und RA zu regeln
- Die RA zeichnet sich durch Nähe zum Benutzer aus
 - Erfahrung bei der zuverlässigen Identifizierung von Kunden
 - Engmaschiges Filialnetz bzw. Mitarbeiter-Betreuer vor Ort
- Die RA verbindet Effizienz und Sicherheit

**Der Registrierungsprozess ist eine Umsetzung
der „analogen Identität“ in eine „digitale Identität“**

28. März 2001

14

FGSec PKI

Registrierungsverfahren

- **E-Mail**
 - Die CA sendet einen PIN an die angegebene E-Mail Adresse. Der Antragsteller kann damit das Zertifikat auslösen.
- **Postweg**
 - Der PIN wird per Briefpost (allenfalls eingeschrieben) zugestellt
- **Starke Authentisierung**
 - Registrierung anhand eines bereits vorhandenen Authentisierungsverfahrens (v.a. bei firmeninternen Lösungen)
- **Persönliches Erscheinen mit Ausweiskontrolle**
 - Antragsteller erscheint persönlich bei einer Registrierungsstelle

28. März 2001

15

FGSec PKI

Certificate Revocation Checking

- **Certificate Revocation Lists (CRL)**
 - CRL enthalten revozierte Zertifikate (bzw. deren Serie-Nr.)
 - Die CA erstellt, signiert und publiziert CRL
 - CRL können zwischengespeichert und lokal geprüft werden
 - Skalierungs- und Verteilungsprobleme sind beträchtlich
- **Online Certificate Validation**
 - Online - Abfrage des Revokationsstatus bei einem Responder
 - Die Qualität ist abhängig von der Aktualität der Daten (CRL)
 - Der Responder kann Zertifikate mehrerer CA unterstützen
 - OCSP (Online Certificate Status Protocol, RFC 2560, Juni 1999)
 - SCVP (Simple Certificate Validation Protocol, draft-ietf-pkix-scvp-04.txt, November 2000)

28. März 2001

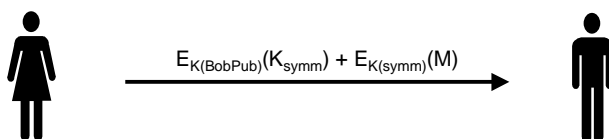
16

FGSec PKI

Datenverschlüsselung

Daten sicher speichern und übermitteln

Übertragung verschlüsselter Daten:



Zusätzliche Probleme:

- Woher kennt Alice den Public Key von Bob ?
- Was geschieht, wenn Bob seinen Private Key verloren hat ?

Directory

- Ausnahmefall: Zertifikat des Empfängers lokal verfügbar
 - z.B. wenn dieser früher einmal ein signiertes Mail geschickt hat
- Normalfall: Zertifikat wird aus einem Directory bezogen
 - Zertifikat sollte zusammen mit der Mail-Adresse abfragbar sein
 - Standard Mail Clients erfordern meistens separate Lookups
 - LDAP ("Lightweight Directory Access Protocol") Zugriffsprotokoll
 - CRL werden ebenfalls im Directory publiziert
- Und die Zertifikate von Kunden oder Lieferanten ?
 - Firmenübergreifende Directories existieren noch kaum

Data Recovery

- Verlust verschlüsselter Daten bei Schlüsselverlust
 - Bei Geschäftsdaten kann dieses Risiko nicht getragen werden
 - Es ist heikel, die Backup-Verantwortung dem Benutzer zu übertragen
- Schlüsselbasierende Lösung:
 - Separate Schlüsselpaare für Verschlüsselung und Signatur
 - Zentrale Generierung mit Backup des Encryption Private Key
- Datenbasierende Lösung:
 - Bei jeder Verschlüsselung wird eine Kopie an ein Recovery-Center geschickt (eine Art obligatorische Verteilerliste)

28. März 2001

19

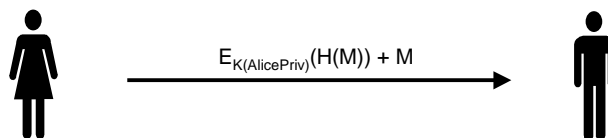
FGSec PKI

Dritter (schwierigster) Anwendungsfall:

Digitale Signatur

Garantie der Urheberschaft einer Nachricht

Signieren von Daten:



Zusätzliches Problem:
Wie wird die Gültigkeit einer Digitalen Signatur zu einem bestimmten Zeitpunkt gegenüber Dritten bewiesen ?

28. März 2001

20

FGSec PKI

Weitere Services

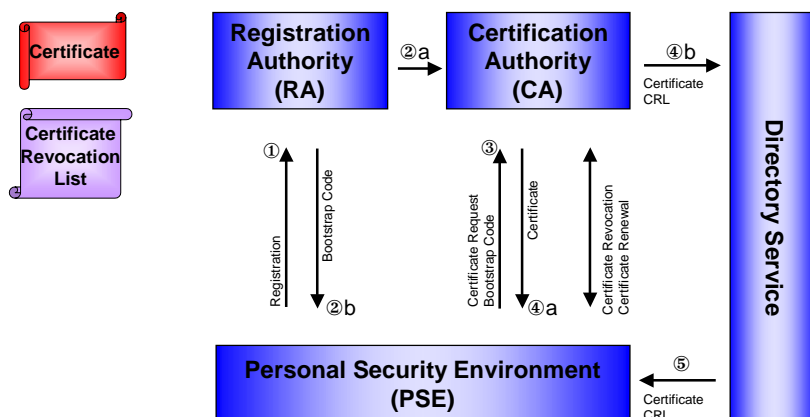
- Time Stamping Service:
 - Einen Zeitpunkt zuverlässig bestimmen und festhalten
- Notariatsdienst:
 - Beglaubigen einer Digitalen Signatur (incl. Time Stamp)
 - Validierung (u.a. CRL-Checking) durch vertrauenswürdige Instanz
- Certificate History:
 - Damit Digitale Signaturen nach Jahren noch geprüft werden können

28. März 2001

21

FGSec PKI

Zusammenfassung

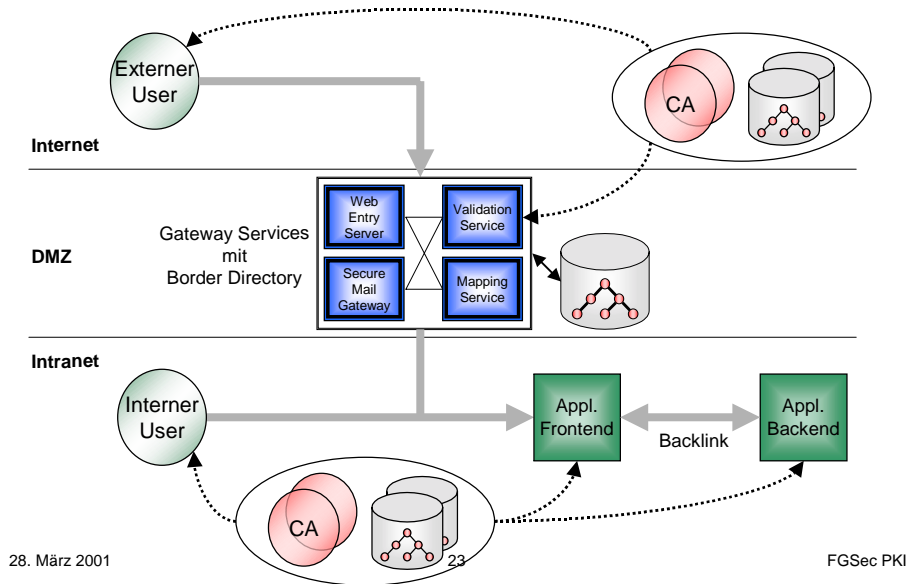


28. März 2001

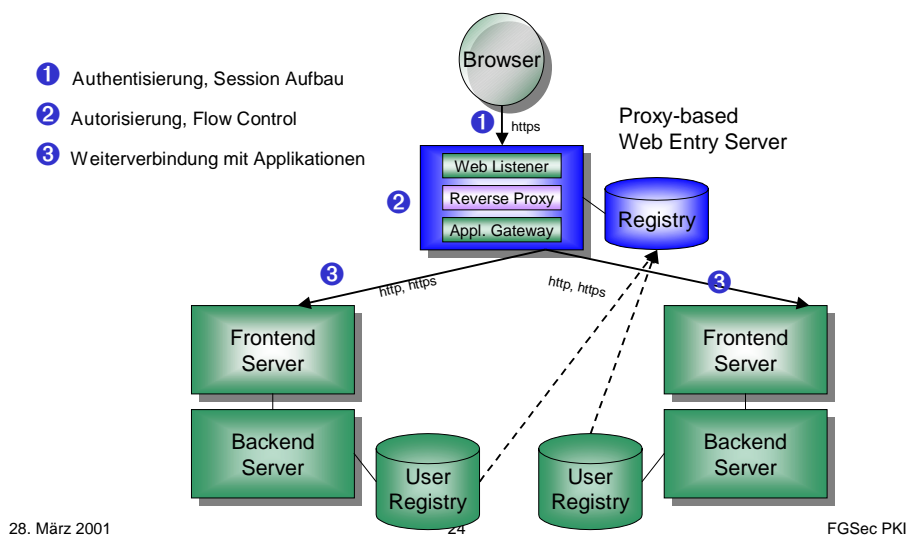
22

FGSec PKI

„Advanced PKI“



Web Entry Server



Validation Service

- Validieren von externen Zertifikaten
 - Prüfen der Signatur
 - Prüfen der Gültigkeitsdauer
 - Prüfen des Revokationsstatus
 - Prüfen der Nutzungsbeschränkungen („Key Usage“)
 - Prüfen der Vertrauenswürdigkeit der CA
 - Prüfen des firmeninternen Status des Zertifikats
- Benötigt ein „Rating“ für externe CA
 - Definieren und Zuordnen von „Trust Levels“
- Benötigt Anbindung der externen CA
 - Zugriff auf Revokationsdaten

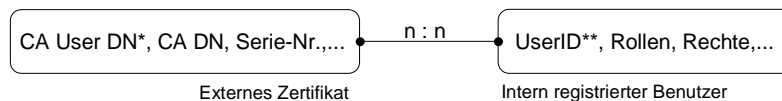
28. März 2001

25

FGSec PKI

Mapping Service

- Zuordnen externer Zertifikate zu internen Usern



- Möglichkeiten für das „Initial Mapping“:
 - Matching Rule (falls Namensgebungen übereinstimmen)
 - Bootstrap – PIN (als generische Lösung)

* CA User DN = Distinguished Name des Users **im Directory der CA**

** UserID = Name des Users **im internen Benutzerverzeichnis**

28. März 2001

26

FGSec PKI

Links zu PKI

- PKIX Working Group:
 - www.imc.org/ietf-pkix/
- The PKI Page
 - www.pki-page.org
- PKI Page des Deutschen Forschungsnetzes:
 - www.pca.dfn.de/dfnpca/pki-links.html
- BAKOM Page zur Digitalen Signatur:
 - www.bakom.ch/ger/subpage/?category_104.html