Patrick Hammer / Sylvia Nagl / John Appoldt

Public Key Infrastructure

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

Impressum:

Copyright © 2000 GRIN Verlag
ISBN: 9783640089550

Patrick Hammer, Sylvia Nagl, John Appoldt

Public Key Infrastructure

GRIN Verlag


PKI

Public Key Infrastructure

1 Verschlüsselung und Sicherheit

2 Public Key Verschlüsselung

3 Public Key Infrastructure

4 PKI Einsatzszenarien

5 Bewertung von PKI

6 Herausforderungen für PKI

7 Risiken von PKI

8 Beispiel: Entrust

1 Verschlüsselung und Sicherheit

1.1 Wozu Verschlüsselung?

On the Internet nobody knows you're a dog.

1.1 Wozu Verschlüsselung?

- hohe Verbreitung von Netzwerken
  elektronische Abbildung von Geschäftsvorfällen
- ausgetauschte Daten als schützenswerte Güter
- meist nachträgliche Sicherung durch
  aufgesetzte Systeme
- effektive Sicherheit erleichtert E-Commerce
  und private Netzwerkkommunikation

1.1 Wozu Verschlüsselung?

- Sicherheit vor Betrug
- Ermöglichung der Einhaltung gesetzlicher Regelungen bzgl. E-Business
- Bereitschaft des Kunden, Angebote zu nutzen und seine Daten zur Verfügung zu stellen
- hohe Kosten durch Sicherheitslöcher

1.2 Sicherheit: E-Security

- Datenschutz
- Imagesicherung
- notwendig aufgrund gesetzlicher Bestimmungen
- neue Geschäftsfelder im Internet
- neue Arbeitsweisen (Intranet)
- Stärkung des Vertrauens der Kunden

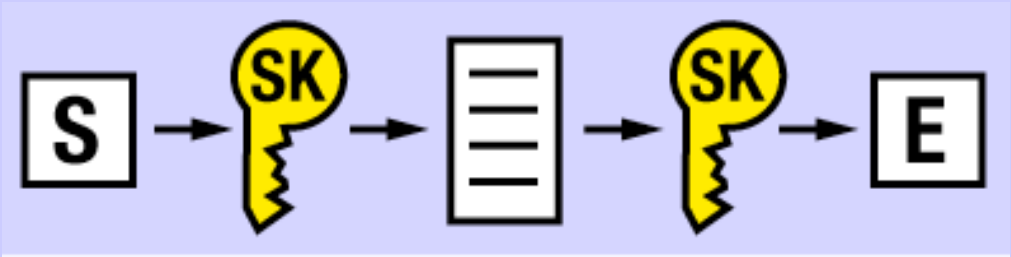
1.2 Sicherheit: Grundwerte

- **Verfügbarkeit**
- **Vertraulichkeit**
- **Integrität**
- **Verbindlichkeit / Nachweisbarkeit**

2 Public Key Verschlüsselung

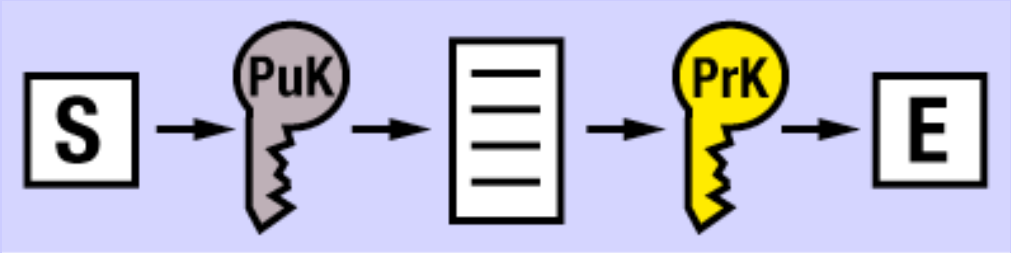
2.1 Secret Key Verschlüsselung

- symmetrische Verschlüsselung
- Sender und Empfänger benutzen gleichen Schlüssel
- Problem: Schlüsseltransfer



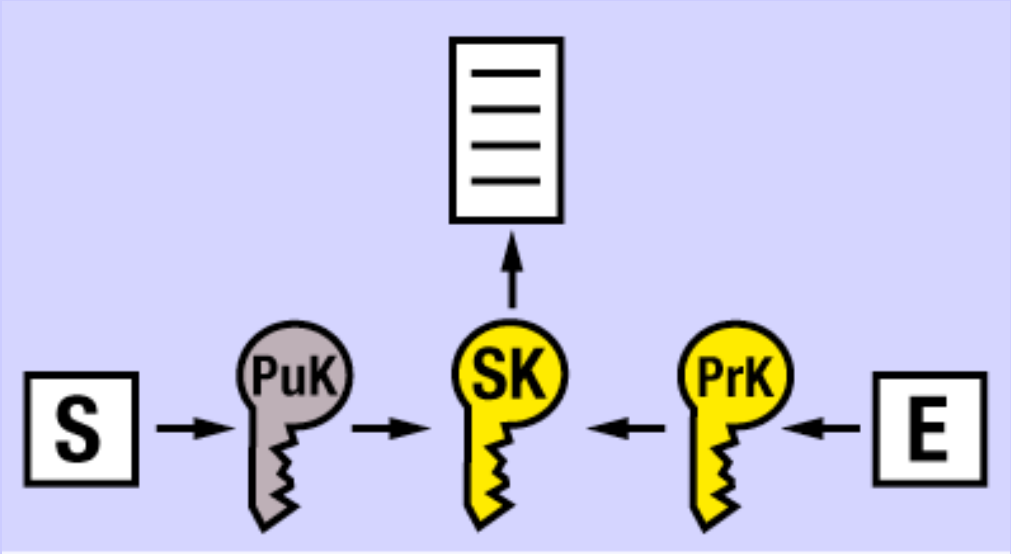
2.2 Public Key Verschlüsselung

- asymmetrische Verschlüsselung
- Schlüsselpaar
  - Public Key: allgemein zugänglich
  - Private Key: geheim (Empfänger)
- Sender: Verschlüsselung mit Public Key des Empfängers
- Empfänger: Entschlüsselung mit eigenem Private Key



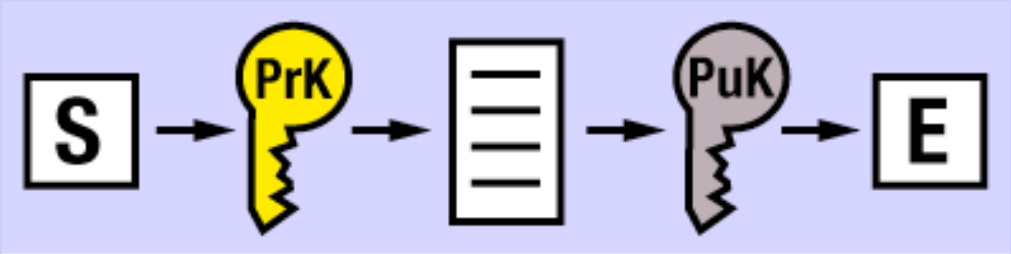
2.3 Kombinierte Verschlüsselung

- Verschlüsselung der Nachricht mit Secret Key
- Verschlüsselung des Secret Key mit Public Key
- Entschlüsselung des Secret Key mit Private Key
- Entschlüsselung der Nachricht mit Secret Key



2.4 Digital Signature

- Authentisierung durch verschlüsselte Signatur
- Umkehrung des Verschlüsselungsvorganges
- Sender: Verschlüsselung mit eigenem Private Key
- Empfänger: Entschlüsselung mit Public Key des Senders



2.5 Hash Function

- Methode für digitale Signatur
- Zerhackung (hashing) der Nachricht
- Verschlüsselung der zerhackten Nachricht (hash) per Private Key
- Versendung von Nachricht und hash
- Entschlüsselung des hash per Public Key und hashing der übertragenen Nachricht
- Vergleich der hash values

2.6 Anforderungen

- **Security Policies: Definition der Regeln und Bedingungen für die Verschlüsselung**
- **Software und Hardware zur Erzeugung, Speicherung und Verwaltung der Schlüssel**
- **festgelegte Prozeduren zur Generierung, Verteilung und Nutzung der Schlüssel**

3 Public Key Infrastructure

3.1 Was ist Public Key Infrastructure?

- **PKI als Kombination von Software, Hardware und Verschlüsselungstechnologien sowie den relevanten Richtlinien und Prozeduren zur sicheren Übertragung von Informationen**
- **netzwerkübergreifende Sicherheitsarchitektur**
- **basiert auf digitalen Zertifikaten (digital certificates): „elektronischer Personalausweis“**

3.2 Komponenten einer PKI

- Security Policy
- Certificate Authority (CA)
- Registration Authority (RA)
- Certificate Verteilungs- und Managementsystem
- PKI-fähige Anwendungen

3.3 Security Policy

- **Definition der obersten Richtlinien für die Informationssicherheit einer Organisation**
- **Prinzipien für Verschlüsselung**
- **Certificate Practice Statement (CPS): detaillierte Operationalisierung der Security Policy**

3.4 Certificate Authority

- verwaltet Public Key Certificates
- Zertifizierung:
  Vergabe von Certificates
- Validierung:
  Überprüfung der Gültigkeit von Certificates
  Certificate Revocation List (CRL)
- organisationseigene CA vs. Commercial CA vs.
  Trusted Third Party

3.4 Certificates nach ITU X.509

- Version
- Seriennummer
- Signaturverfahren
- Herausgeber
- Gültigkeitszeitraum
- Benutzername
- öffentlicher Schlüssel
- Bezeichner des Herausgebers
- Bezeichner des Benutzers
- Erweiterungen

3.5 Registration Authority

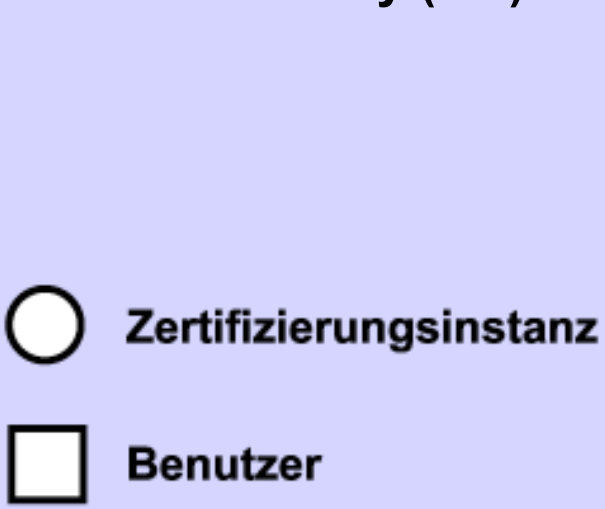
- Interface zwischen Nutzer und CA
- Aufnahme und Authentisierung der Nutzeridentität
- Anforderung von Certificates von CA
- Validierung

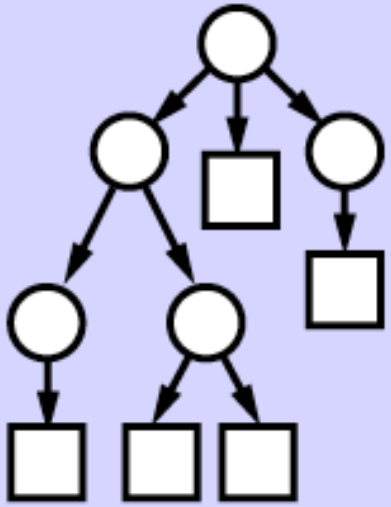
3.6 Certificate Verteilungssystem

- hierarchisches Trustmodell
- Zertifizierungsnetze
- hybrides Modell

3.6 hierarchisches Trustmodell

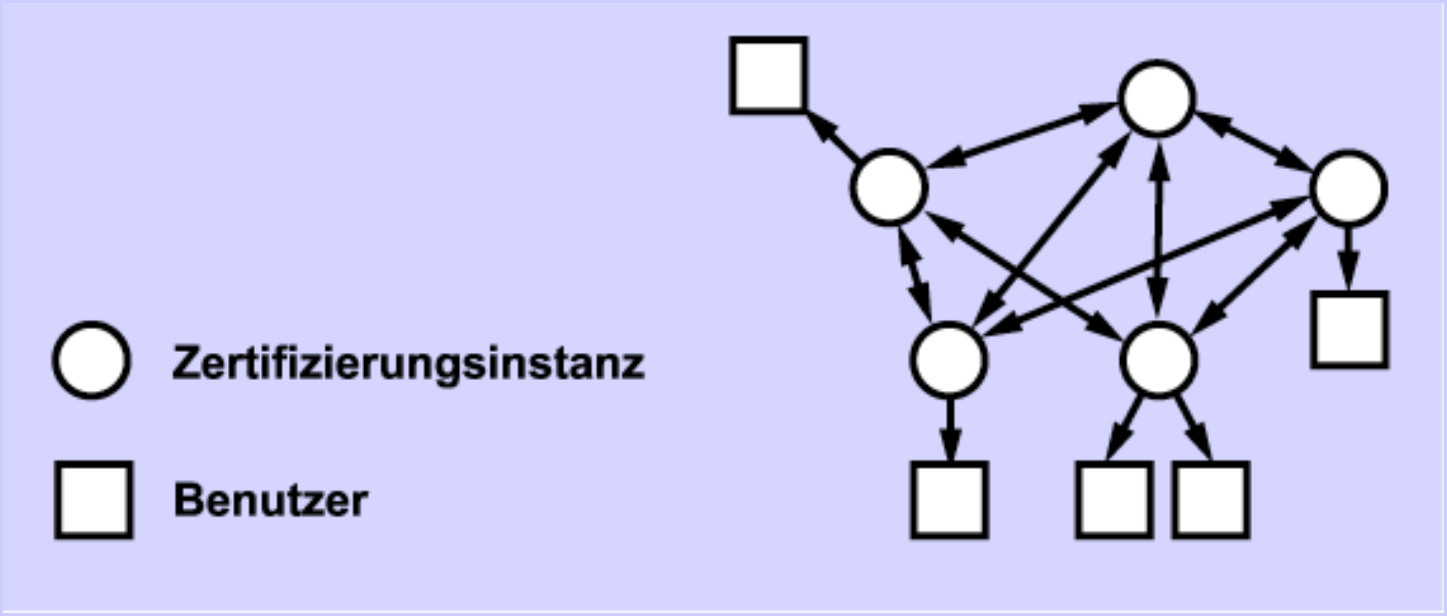
- Policy Approving Authority (PAA)
- Policy Certification Authority (PCA)
- Certificate Authority (CA)





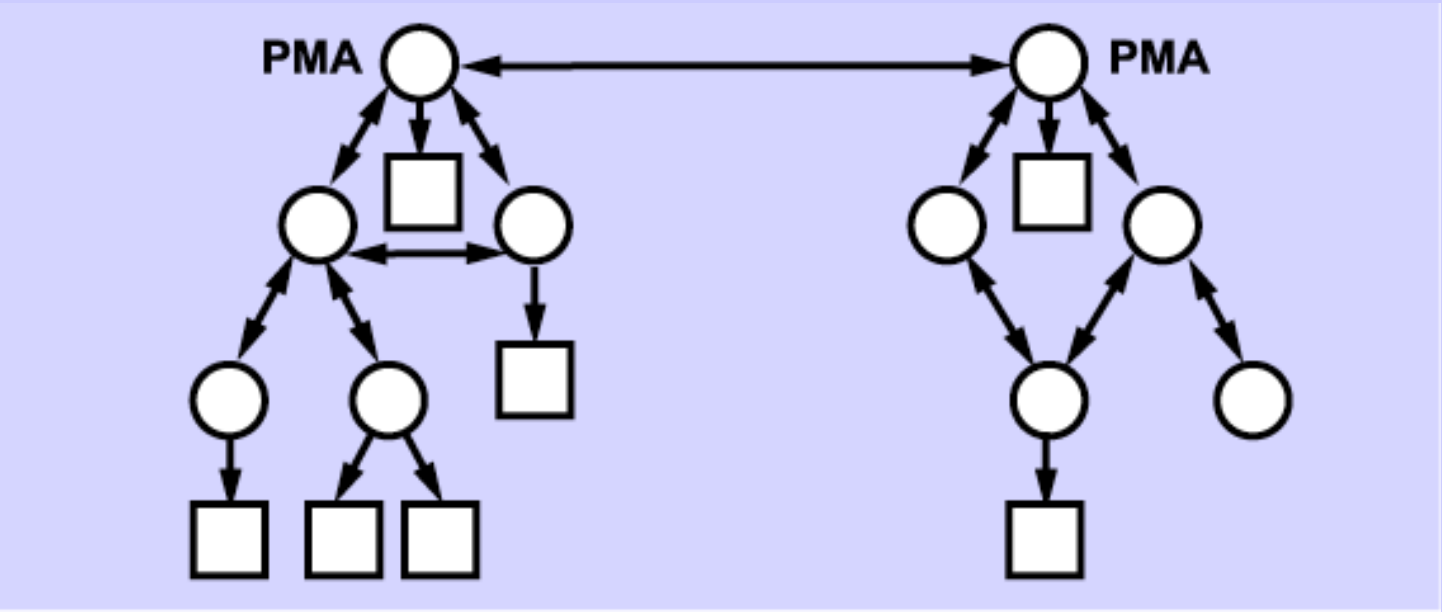
3.6 Zertifizierungsnetze

- Cross-Zertifizierung
- keine hierarchischen Beziehungen



3.6 Hybrides Modell

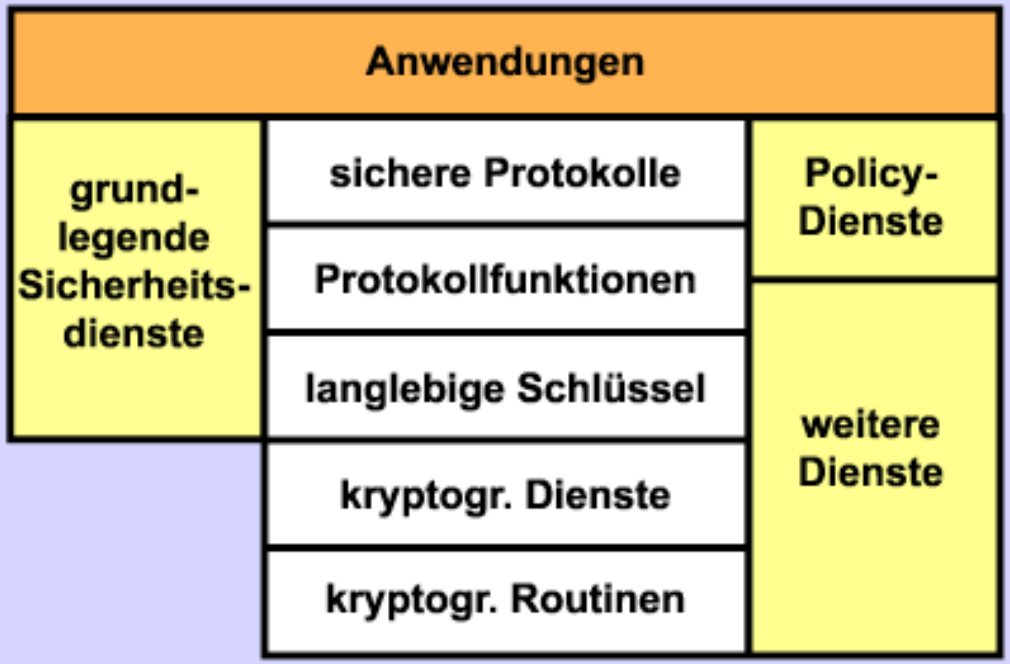
- **Mischform aus hierarchischem Ansatz und Cross-Zertifizierung**
- **Policy Management Authority (PMA)**



3.7 PKI-fähige Anwendungen

- Kommunikation zwischen Web-Server und Browser
- E-mail
- Electronic Data Interchange (EDI)
- Zahlungstransaktionen über das Internet
- Virtual Private Networks

3.8 PKI-Dienstmodell



4 PKI Einsatzszenarien

4 PKI Einsatzszenarien

- End-zu-End-Sicherheit
- unternehmensweite Sicherheit

4.1 End-zu-End-Sicherheit

- Home Banking
- Bestellwesen
- Kreditkartenzahlung per Secure Electronic Transaction (SET)
- etc.

4.2 Unternehmensweite Sicherheit

- **Managebarkeit**
- **Konsistenz**
- **Integrierbarkeit**

5 Bewertung von PKI

4 Bewertungskriterien von PKI

- Flexibilität
- Nutzerfreundlichkeit, einfaches Management
- Unterstützung individueller Sicherheitspolitik
- Skalierbarkeit, Erweiterbarkeit
- Interoperabilität
- Sicherheit der CA/RA

5 Herausforderungen an PKI

5 Herausforderungen an PKI

- rechtliche
- organisatorische
- technische

7 Risiken von PKI

7 Risiken von PKI

- Wem vertraue ich worin?
- Wer benutzt meine Schlüssel?
- Wie sicher ist der überprüfende Rechner?
- Wie sinnvoll ist die Verbindung von Schlüsseln mit Namen?
- Wie weit geht die Autorität der CA?
- Wie sicher sind die Certificate Practices?
- Wie identifiziert die CA den Halter des Zertifikats?

Entrust