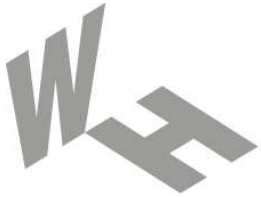


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Digitale Signatur und Public Key Infrastruktur (PKI)

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- **Einführung**
  - Verfahren und Prinzipien der digitalen Signatur
  - Elektronische Zertifikate
  - Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
  - Vertrauensmodelle
  - Gesetzlicher Hintergrund
  - Standards
  - Umsetzungskonzepte
  - Realisierungen
  - Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Eigenhändige Unterschrift

Prof. Dr. (TU NN) Norbert Pohlmann
Bonhoefferstr. 40a
52078 Aachen

13.01.04

Fachgroßhandel für Waschmaschinen
Aachenerstr. 70
50674 Köln

Sehr geehrter Herr Maier,
hiermit bestelle ich, auf der Grundlage Ihres Angebotes (Nr.345/10/02)
vom 13.10.02, bei Ihnen eine Waschmaschine im Wert von 320 Euro.
Mit freundlichen Grüßen

Norbert Pohlmann

Welchen Wert hat eine handgeschriebene Unterschrift ?

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Funktionen einer Unterschrift

- **Abschlußfunktion**
  Vollendung einer Erklärung - hebt sich vom Entwurf ab

- **Identitätsfunktion**
  Unterschrift macht die Identität des Ausstellers kenntlich

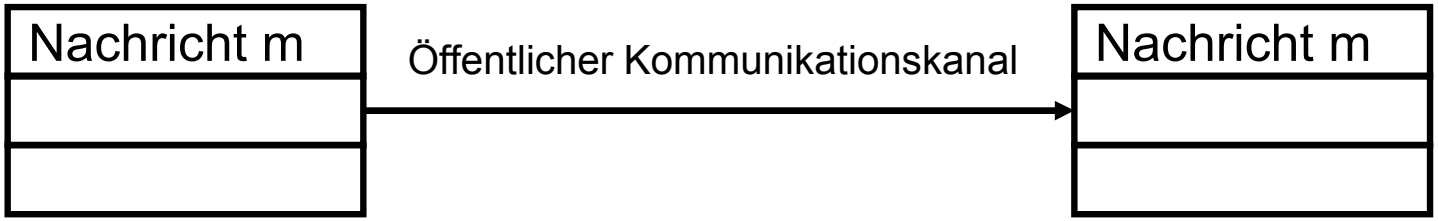
- **Echtheitsfunktion**
  Dokument stammt vom Aussteller

- **Warnfunktion**
  Schutz des Unterzeichners vor Übereilung

- **Beweisfunktion (Urkundenbeweis)**
  Erleichtert die Beweisführung im Streitfall (D: § 415 ZPO)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Kommunikation in der elektronischen Welt



Sender A

Empfänger X

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- **Verfahren und Prinzipien der digitalen Signatur**
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Signatur-Algorithmus - RSA-Verfahren

Schlüsselgenerierung:

n=p*q	p, q sind Primzahlen
n: 1728 oder 2048 Bit lang	
wähle e, sodass	ggT(e,(p-1)*(q-1))=1
bestimme d, sodass	e*d (mod ((p-1)*(q-1))=1

e,n = öffentlicher Schlüssel (**OS**)

d = geheimer Schlüssel (**GS**)

Signatur zur Nachricht m:

$$s=S(m, (d,n)) = m^d \bmod n$$

Verifikation:

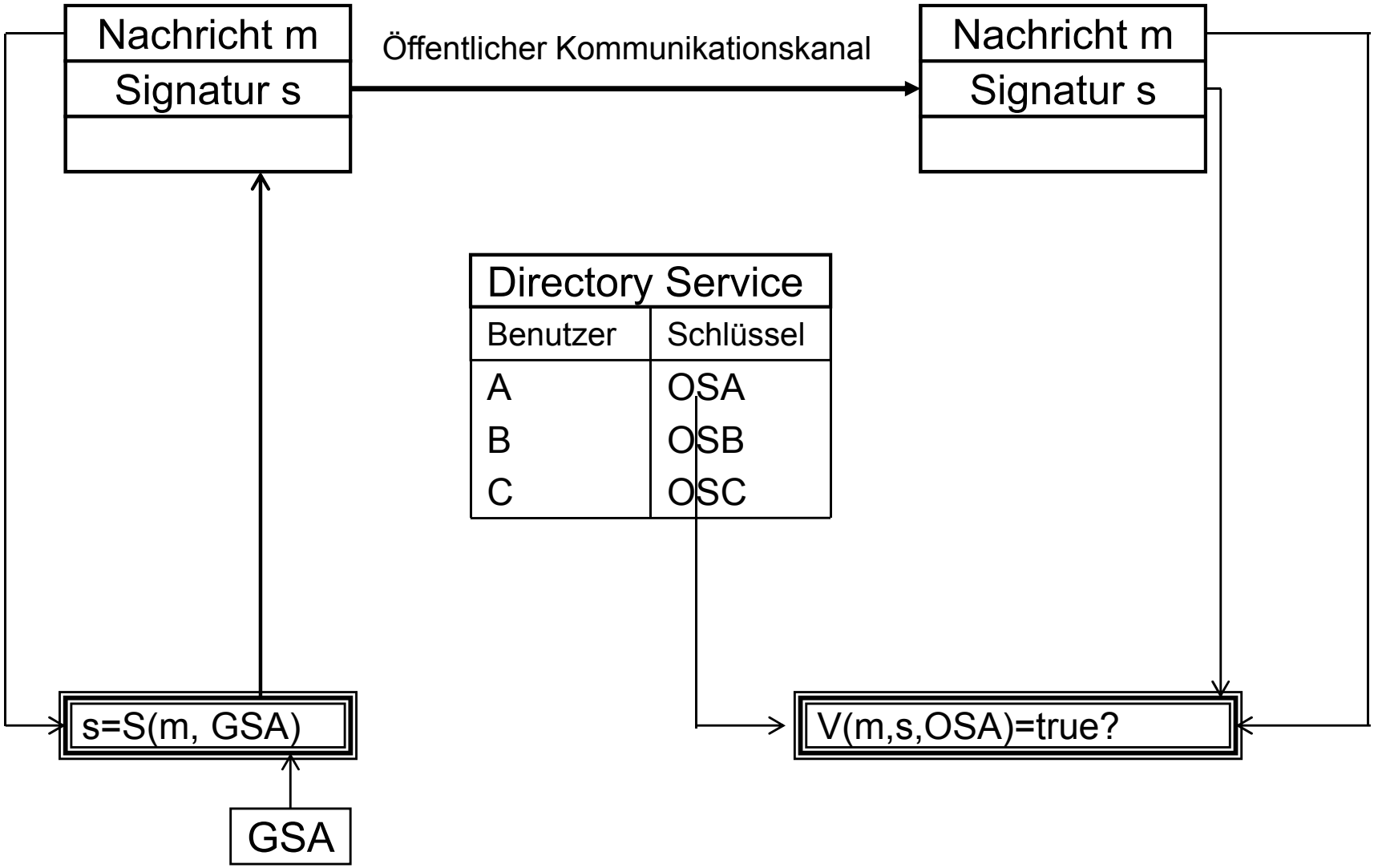
$$V(m,s,(e,n)): s^e \bmod n = m?$$

Allgemein:

$$x = PK(y, key) = y^{key} \bmod n$$

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzip einer digitalen Signatur



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Prinzip einer digitalen Signatur

Ziel: **V(m, s, OSA) = true ⇒ m wird akzeptiert**

V:	Verifikationsfunktion
m:	Nachricht
s:	Signatur
OSA:	öffentlicher Schlüssel des Urhebers von A

Was benötigen wir sonst noch?

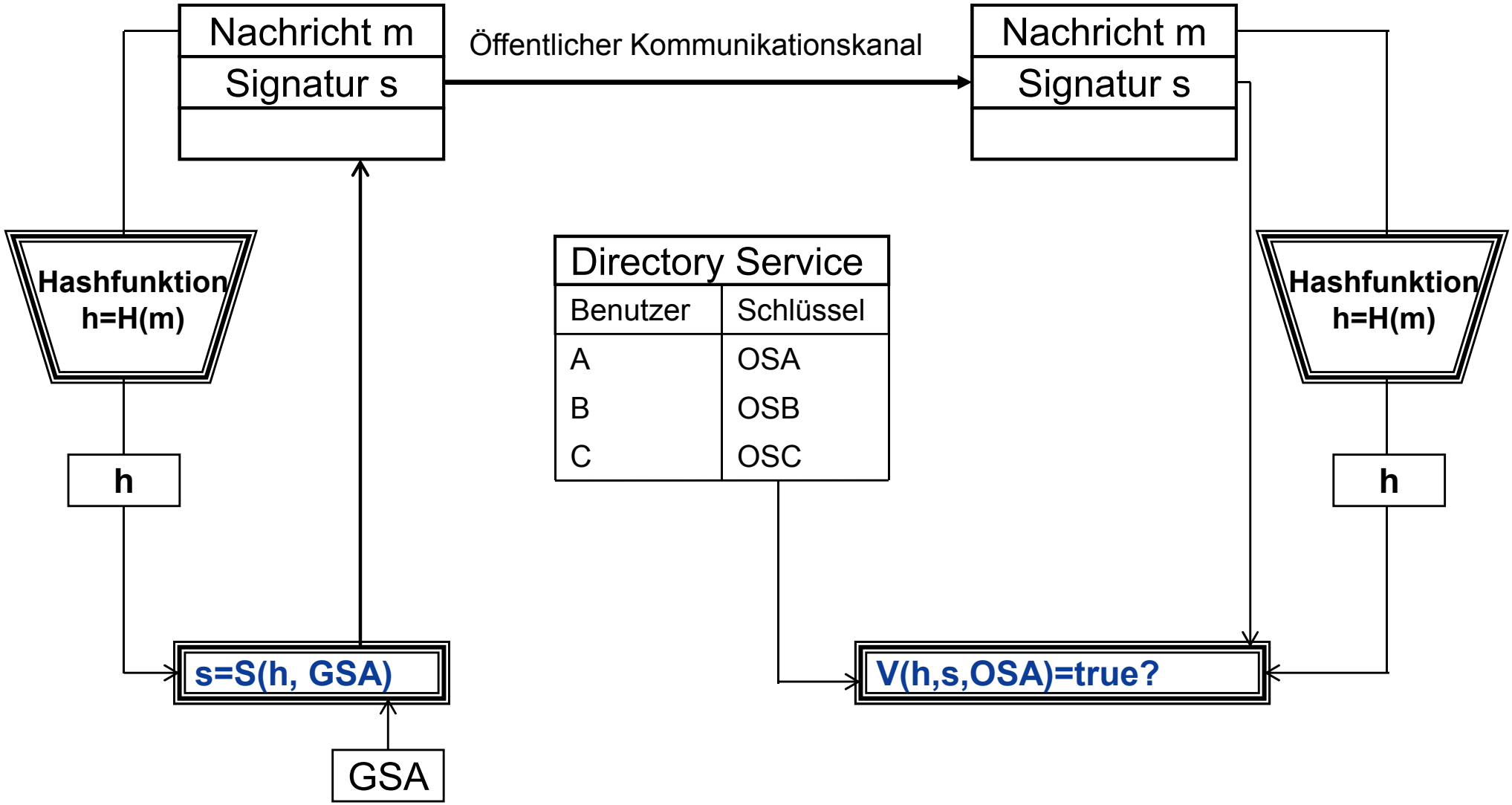
- Eine einfache Möglichkeit, längere Nachrichten signieren zu können.
  → **Hashfunktionen**

Grund:

- Public-Key-Verfahren haben eine relativ hohe Verarbeitungszeit für eine Operation
  - 30 ms für eine 1024 Bit Operation (650 MHz PC)
  - für eine Nachricht von 10 MByte sind ca. 40 min. notwendig
  - die Zusammengehörigkeit von Einzelsignaturen ist nicht gegeben

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Digitale Signatur mit Hashfunktion



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Digitale Signatur mit Hashfunktion

Ziel: Jeder kann die Signatur verifizieren:

V(h=H(m), s, OSA) = true ⇒ m wird akzeptiert

Anforderungen an kryptographische Hashfunktionen:

- H ist eine öffentlich bekannte kontrahierende Einwegfunktion
- H ist kollisionsresistent (d.h. es ist praktisch unmöglich, systematisch eine Nachricht m´ zu finden, die denselben Hashwert h=H(m´) ergibt)
- m kann beliebig lang sein, h hat eine feste Länge, z.B. 160 Bit
- Die Berechnung des Funktionswertes h ist einfach
  (10 MByte in ca. 8 Sekunden, incl. Festplattenzugriffe, 650 MHz PC)

Vorteile:

- Eine beliebig lange Nachricht kann signiert werden
- Bindung der Nachricht an die digitale Signatur
  Gewährleistung der Integrität einer Nachricht
  (jedes Bit der Nachricht ist eingeschlossen ! ! !)

Was benötigen wir sonst noch?

- Gewährleistung der Authentizität des öffentlichen Schlüssels → **Zertifikate**

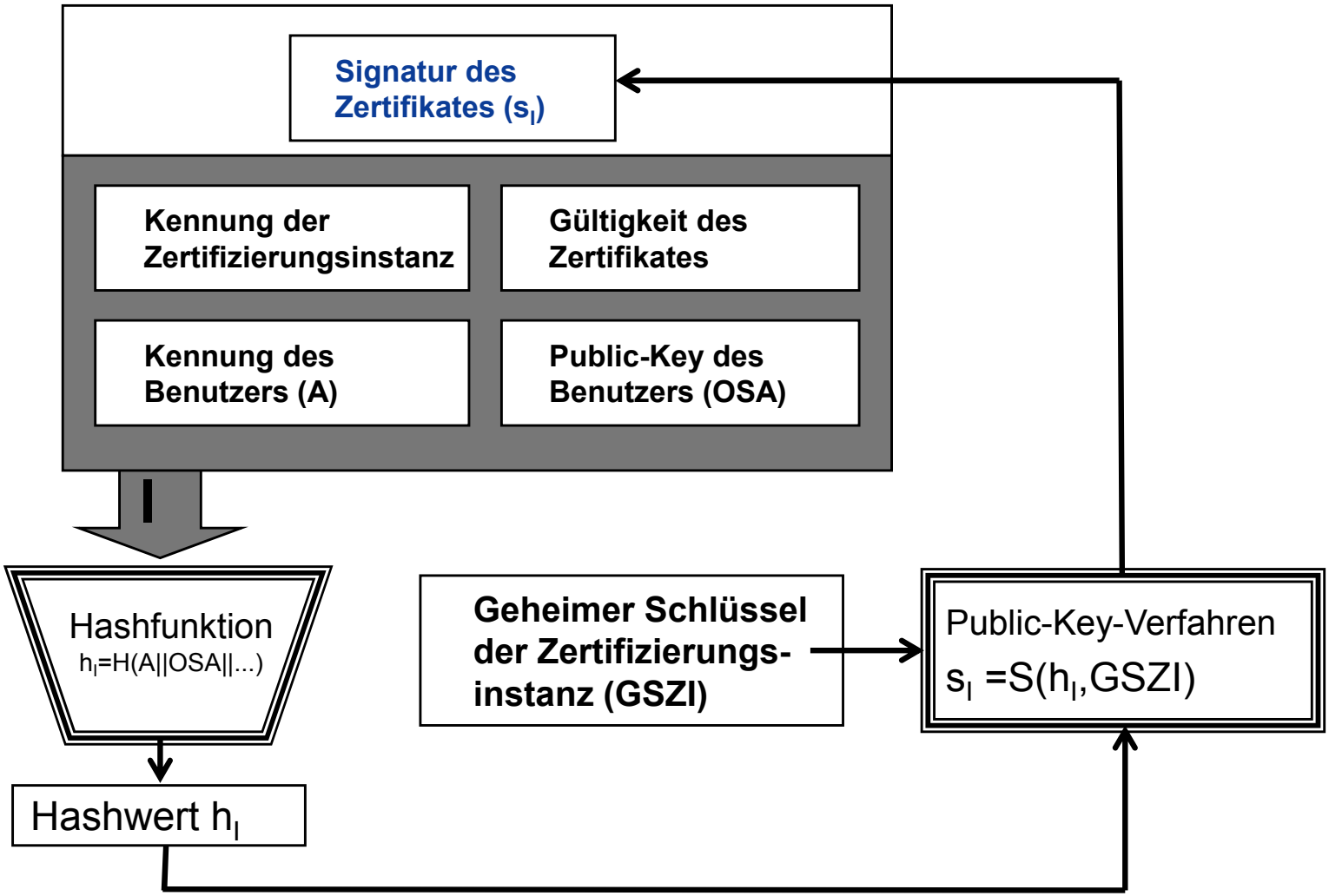
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- **Elektronische Zertifikate**
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt und Erstellung eines Zertifikates

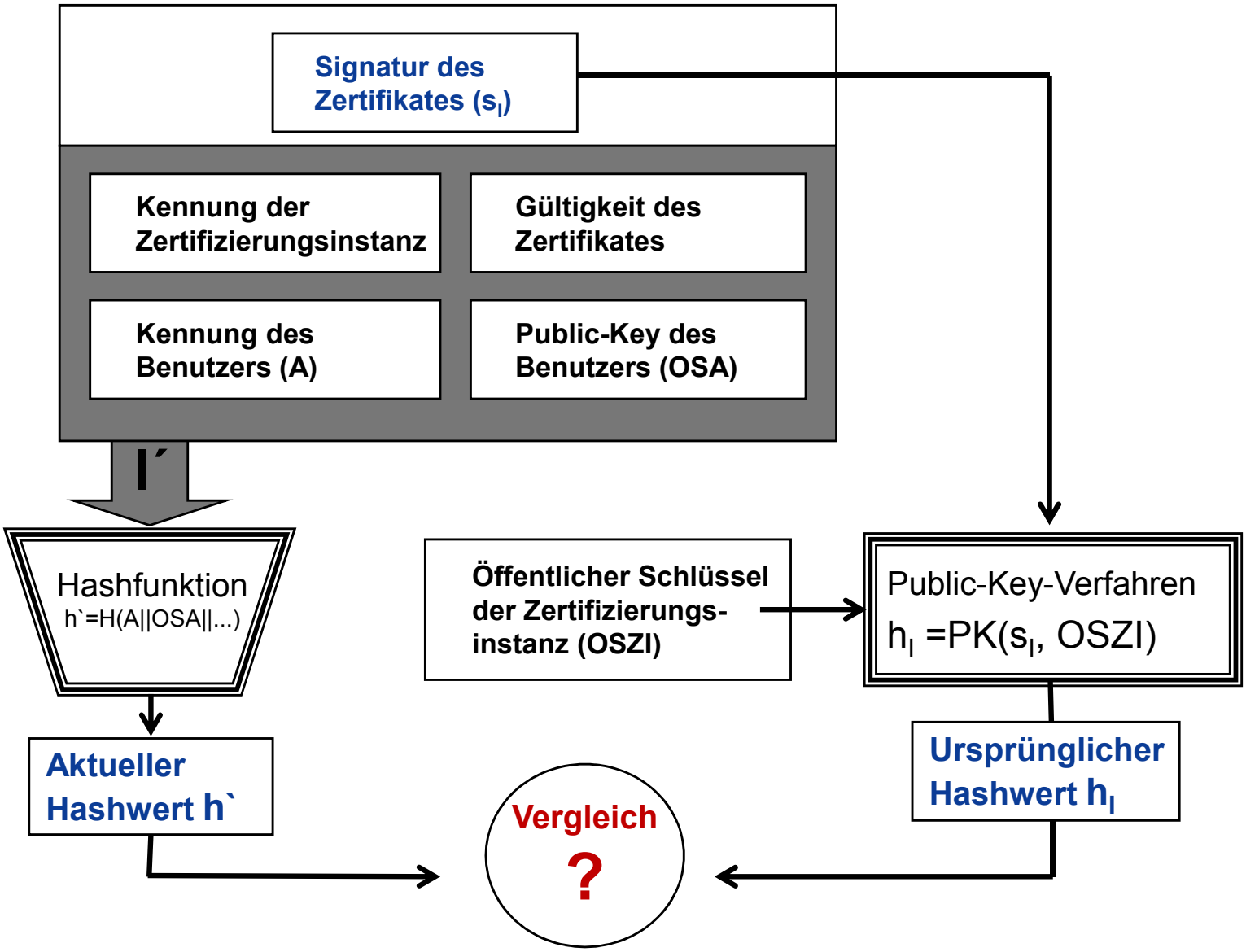


ZA=(A||OSA||..., S(h_I, GSZI))

Standard für Zertifikate: X.509 V.3

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

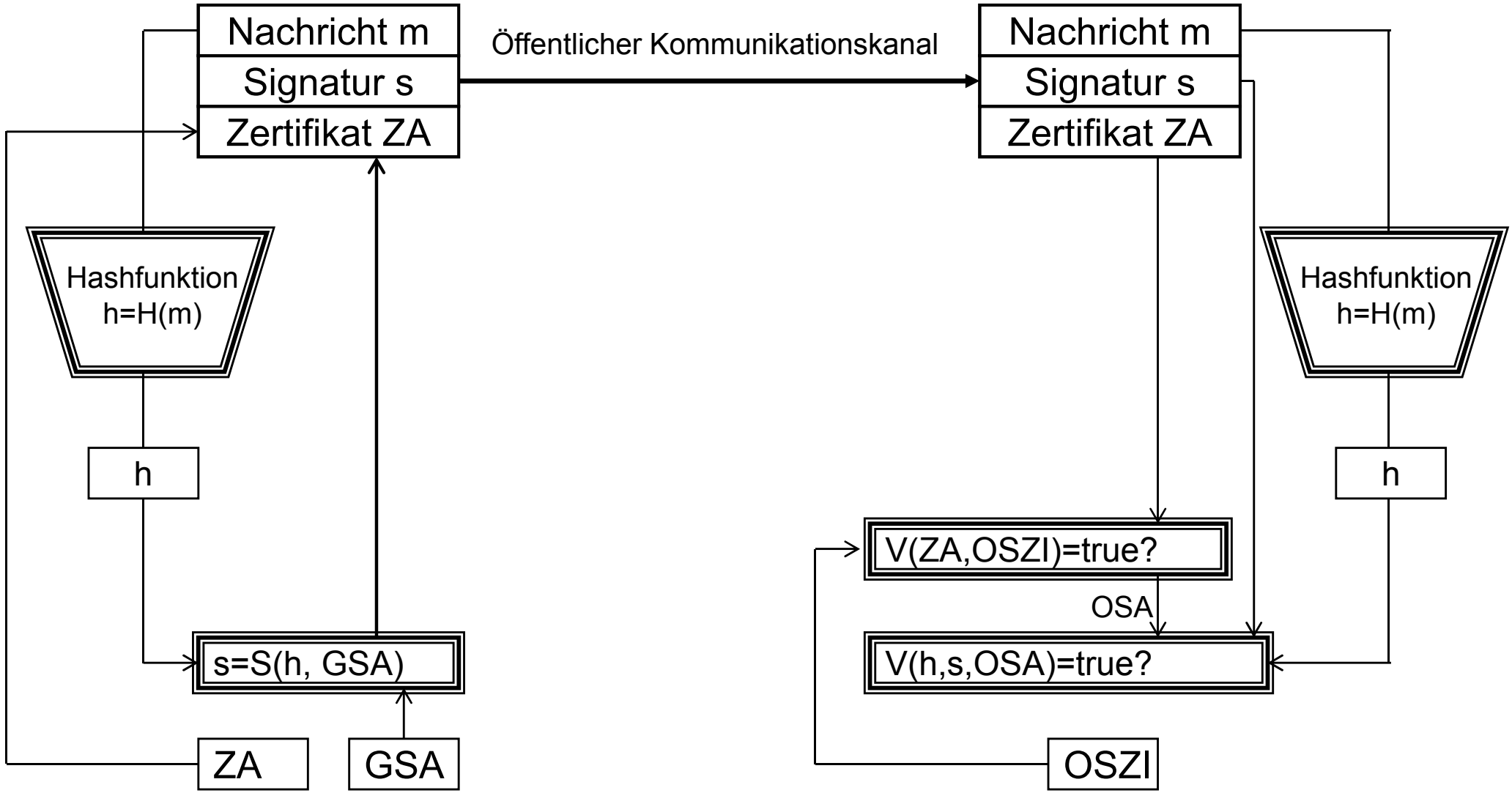
Verifikation eines Zertifikates



V(ZA, OSZI) = true $\Rightarrow$ Zertifikat ist gültig

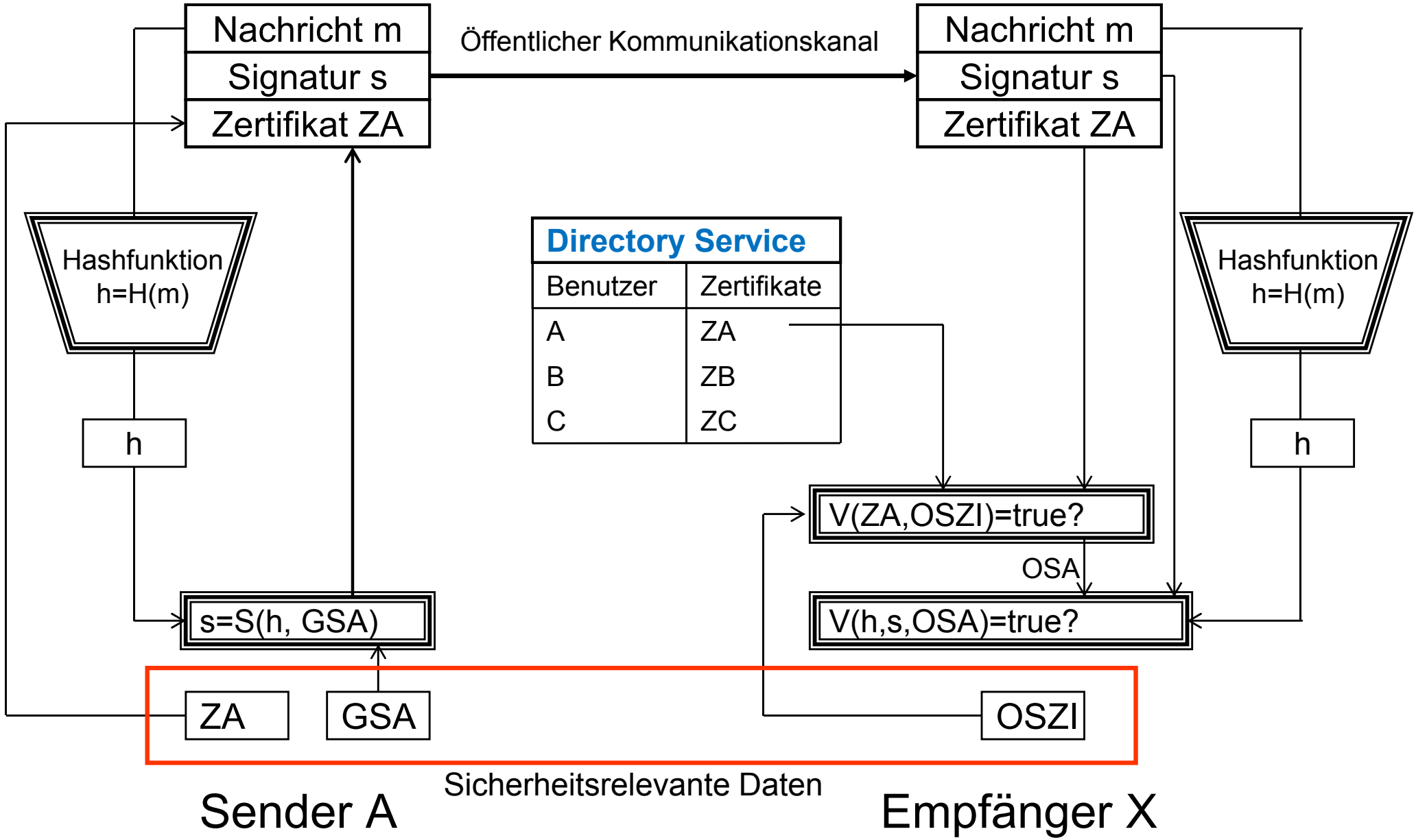
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Digitale Signatur mit Zertifikaten



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Digitale Signatur mit Zertifikaten



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Digitale Signatur mit Zertifikaten

Nur Zertifizierungsinstanz ZI stellt Zertifikate aus:

ZA=(A||OSA||..., S(H(A||OSA||...), GSZI)) = (I,s)

Jeder kann die Korrektheit eines Zertifikates verifizieren:

V(I,s, OSZI) = true ⇒ Zertifikat ist gültig

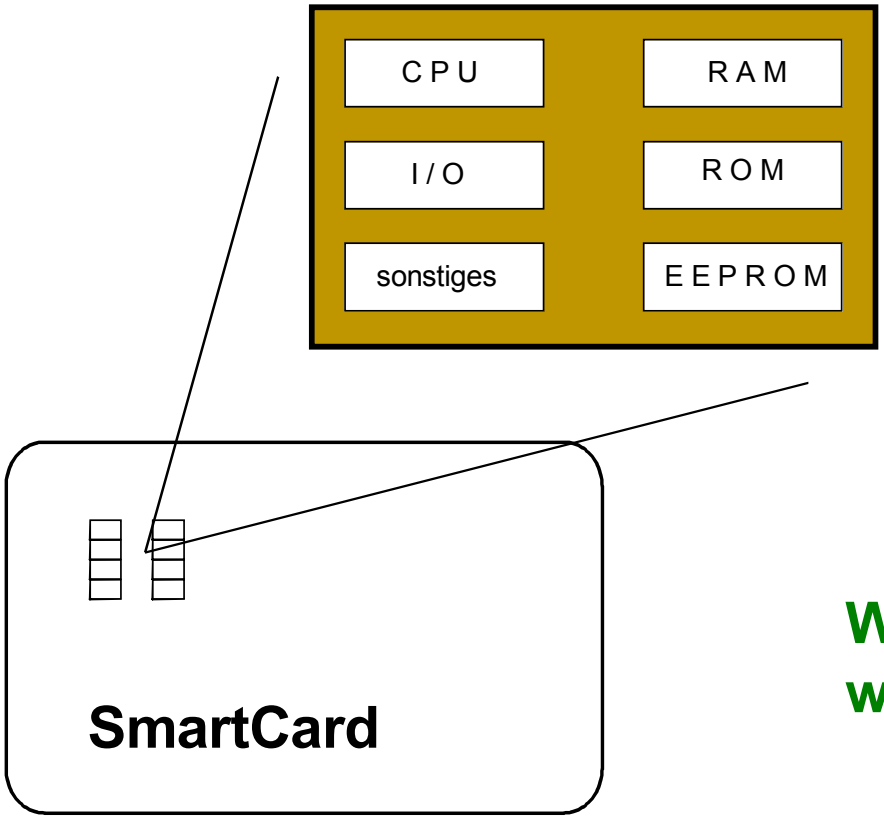
Was benötigen wir sonst noch?

- Die sichere Speicherung des eigenen geheimen Schlüssels → **PSE**
- Den authentischen öffentlichen Schlüssel OSZI von der ZI → **PKI (CA)**
- Die Gewährleistung, dass die Kennung des Benutzers wirklich zu der Person gehört, und dass die Kennung eindeutig ist → **PKI (RA)**
- Die Möglichkeit zu überprüfen, ob ein Zertifikat gesperrt wurde → **PKI (DIR)**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Personal Security Environment (PSE)

- **Aufgabe:** Die Sammlung aller sicherheitsrelevanten Daten (Zertifikat (ZA) und der geheime Schlüssel des Teilnehmers (GSA) sowie der öffentliche Schlüssel der Zertifizierungsinstanz (OSZI))
- **Formen:** Software, USB-Token, Sicherheits-Module, SmartCards, SIM-Karte im Handy, TPM, **neuer Personalausweis (nPA)**, ...
- z.B. **SmartCards**



Was benötigen wir sonst noch?

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Restrisikobereich
→ Kartenlesegeräte

- 3 Kategorien an Lesegeräten für den nPA (BSI TR 03119)
  - Basisleser (Cat-B)
  - Standardleser (Cat-S)
  - Komfortleser (Cat-K)

Merkmal	Basisleser	Standardleser	Komfortleser
Kontaktlose Schnittstelle	x	x	x
Kontaktbehaftete Schnittstelle	o	o	x
Pinpad	o	x	x
Zweizeiliges Display	o	o	x
Qualifiz. Signatur	–	–	x

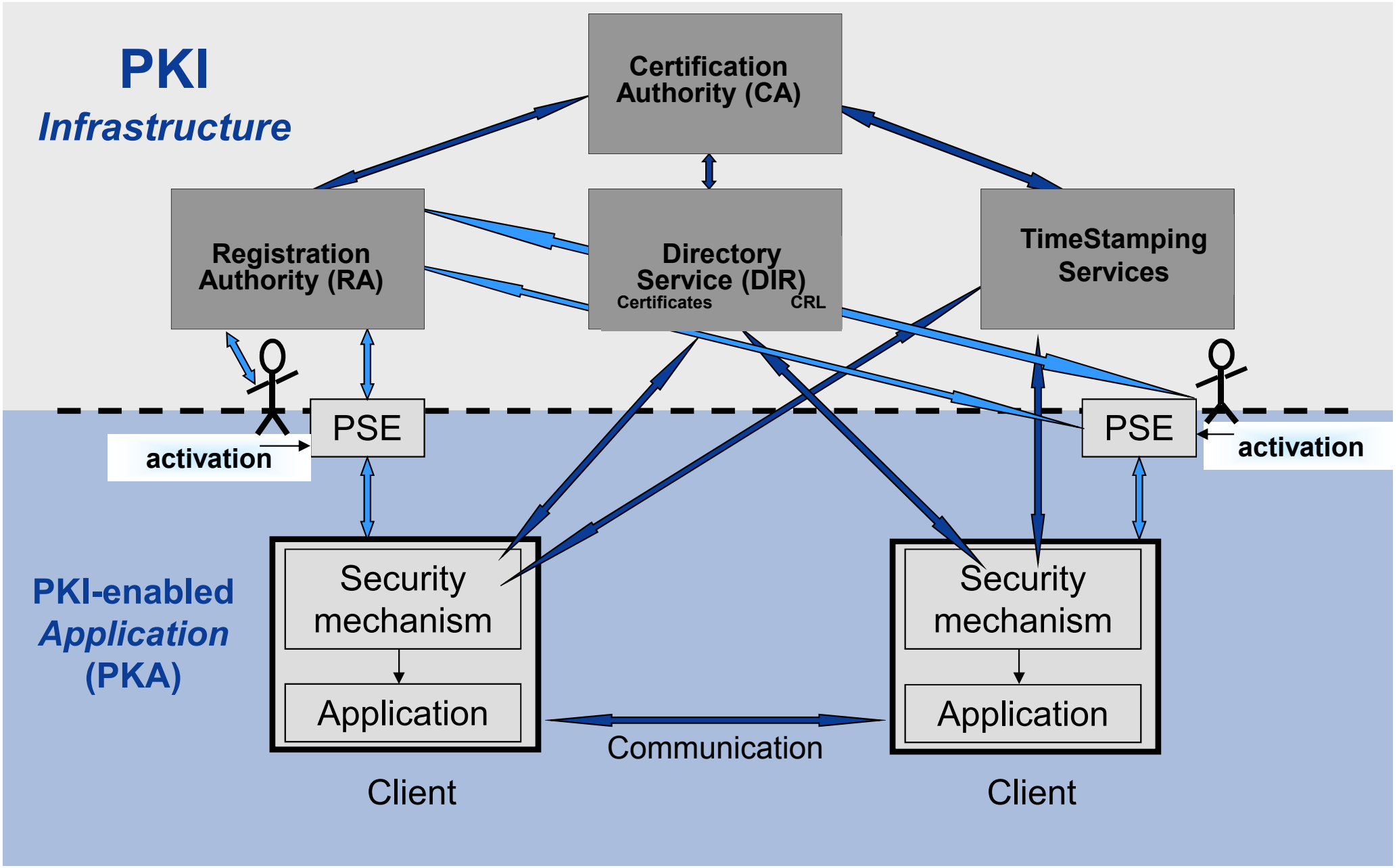
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- **Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)**
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Public-Key-Infrastruktur
→ Zertifizierungsinstanz



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Public-Key-Infrastruktur
→ Komponenten (1/2)

- **Policy**
  - Sicherheitskonzept
  - Benutzerrichtlinien
  - Organisations- und Arbeitsanweisungen

- **RA - Registration Authority**
  - Schnittstelle zum Teilnehmer
  - Identitätsfeststellung (inkl. Registrierung) der Teilnehmer entsprechend der Policy

- **CA - Certification Authority**
  - Schlüsselgenerierung für die Zertifizierungsstelle
  - Zertifizierung öffentlicher Teilnehmerschlüssel, Attribute
  - Personalisierung des PSEs für Zertifikat, Schlüsselpaar etc.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Public-Key-Infrastruktur
→ Komponenten (2/2)

- **Zeitstempeldienst**
  - Service für die Erstellung gesicherter Zeitsignaturen gemäß Policy
- **DIR - Directory Services**
  - Verzeichnisdienst für Zertifikate und Sperrlisten
- **PSE (Personal Security Environment)**
  - Die Sammlung aller sicherheitsrelevanter Daten (Zertifikate und die geheimen Schlüssel des Teilnehmers sowie der Öffentliche Schlüssel der Zertifizierungsinstanz)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Public-Key-Infrastruktur
→ Aufgaben

- **Betrieb von Registrierungsstellen (RA)**
  - Benutzeranfragen erfassen und die Identifizierung der Benutzer (z.B. mit Personalausweis)
  - Weiterleitung des Antrages an die CA
- **Vergabe von eindeutigen Identitäten (CA)**
  - gemäß der Identitätsfeststellung der RA
- **Herausgabe und Verwaltung von Zertifikaten (CA)**
  für die Verifizierung von:
  - Öffentlichen Schlüsseln
  - Attributen (Position/Rechte im Unternehmen, ...)
- **Bereitstellung von Verzeichnissen für (Directory Service)**
  - gültige Zertifikate und
  - Sperrliste für Zertifikate (CRL - Certificate Revocation List)
- **Bereitstellung von Zusatzdiensten (Zeitstempel u.a.)**

Was benötigen wir sonst noch?

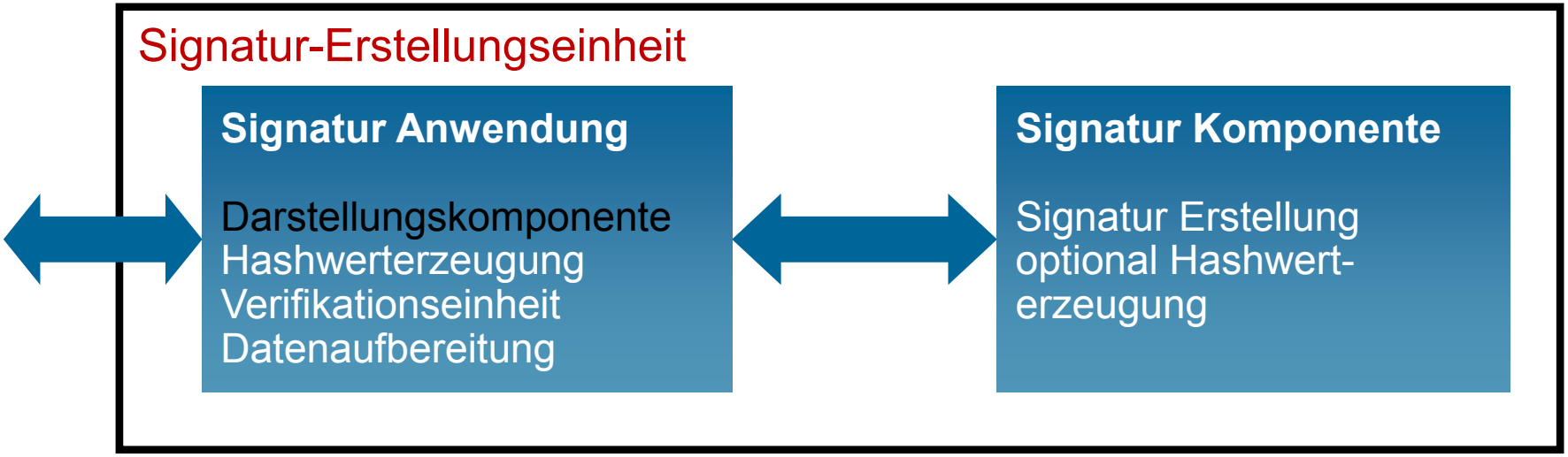
- Die Zusammenarbeit verschiedener Zertifizierungsinstanzen
  → Zertifizierungshierarchie - Vertrauensmodell

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Was ist eine PKI-enabled Application (PKA)?

- Ein Anwendung, die von der Public-Key-Infrastruktur zur Verfügung gestellte Sicherheitsdienste nutzt, um eine vertrauenswürdige Anwendung zu realisieren.

- Beispiel digitale Signatur: Eine Signatur-Erstellungseinheit besteht immer aus einer Signaturkomponente, die die Signatur erzeugt und der Signatur Anwendung.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ziele von PKIs und PKAs

Mehr Vertrauenswürdigkeit in den Geschäftsprozessen

Anforderungen:		Lösungen:
Authentizität	→	Signatur
Integrität	→	Signatur
Verbindlichkeit	→	Signatur
Einmaligkeit	→	TimeStamp
Vertraulichkeit	→	Verschlüsselung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

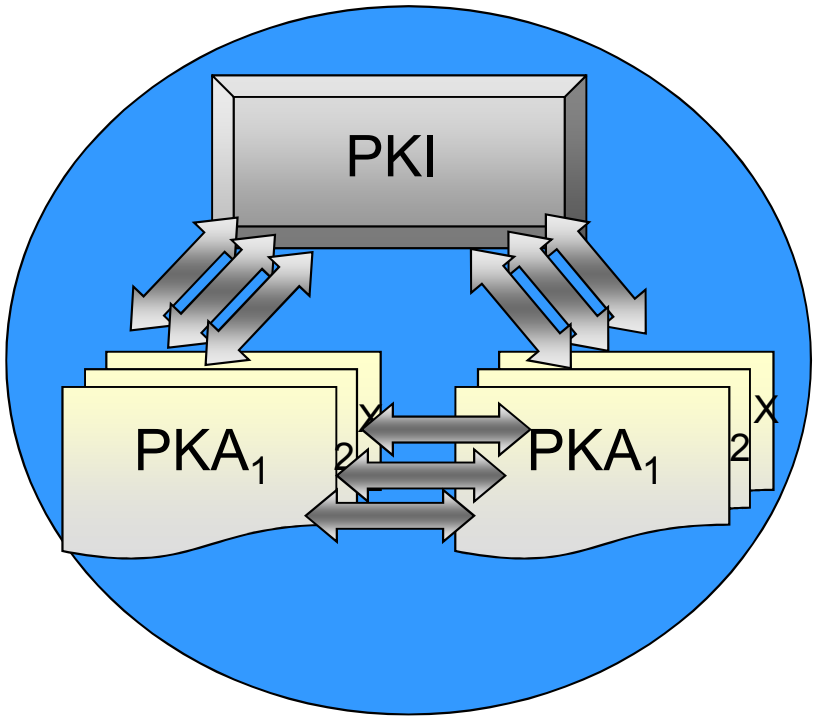
Nutzung von Public-Key-Infrastrukturen

- **PKIs sind kein Selbstzweck !**
- **Sicherheitsinfrastrukturen bilden eine Basis für vertrauenswürdige Anwendungen (PKI-enabled Applications) wie:**
  - E-Mail
  - Dokumente (Word, Excel, PowerPoint, ...)
  - Transaktionen (EDIFACT, XML, ...)
  - SSL-Kommunikation
  - VPN-Kommunikation
  - Identifikations- und Authentikationsprozesse
  - Bezahlsysteme
  - ...

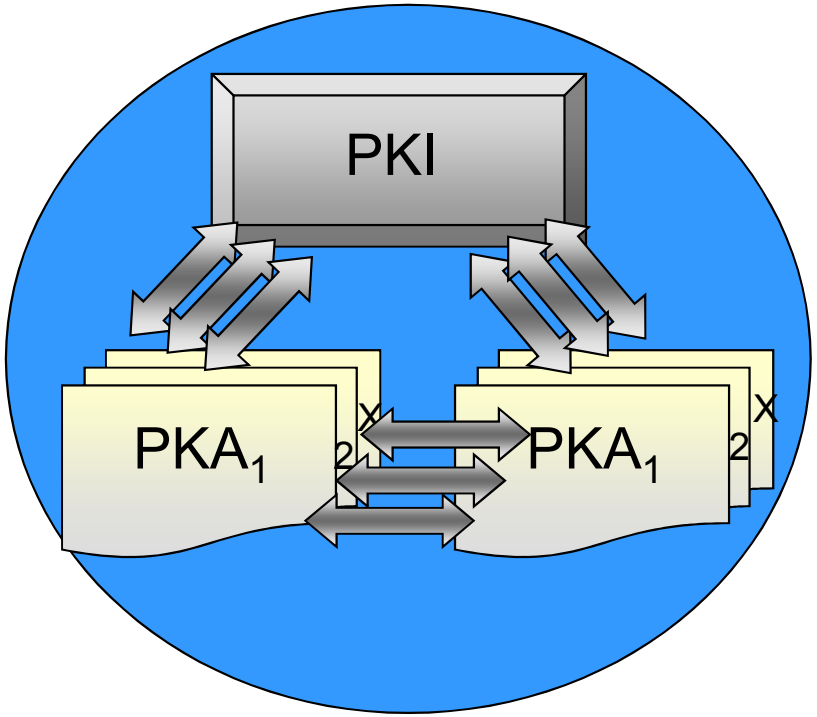
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Modelle von Public-Key-Infrastrukturen (1/3)

- **Geschlossene Systeme**
  - Eine Organisation betreibt die PKI für eine oder mehrere Anwendungen, die in ihrem eigenen Verantwortungsbereich liegen.



Organisation 1

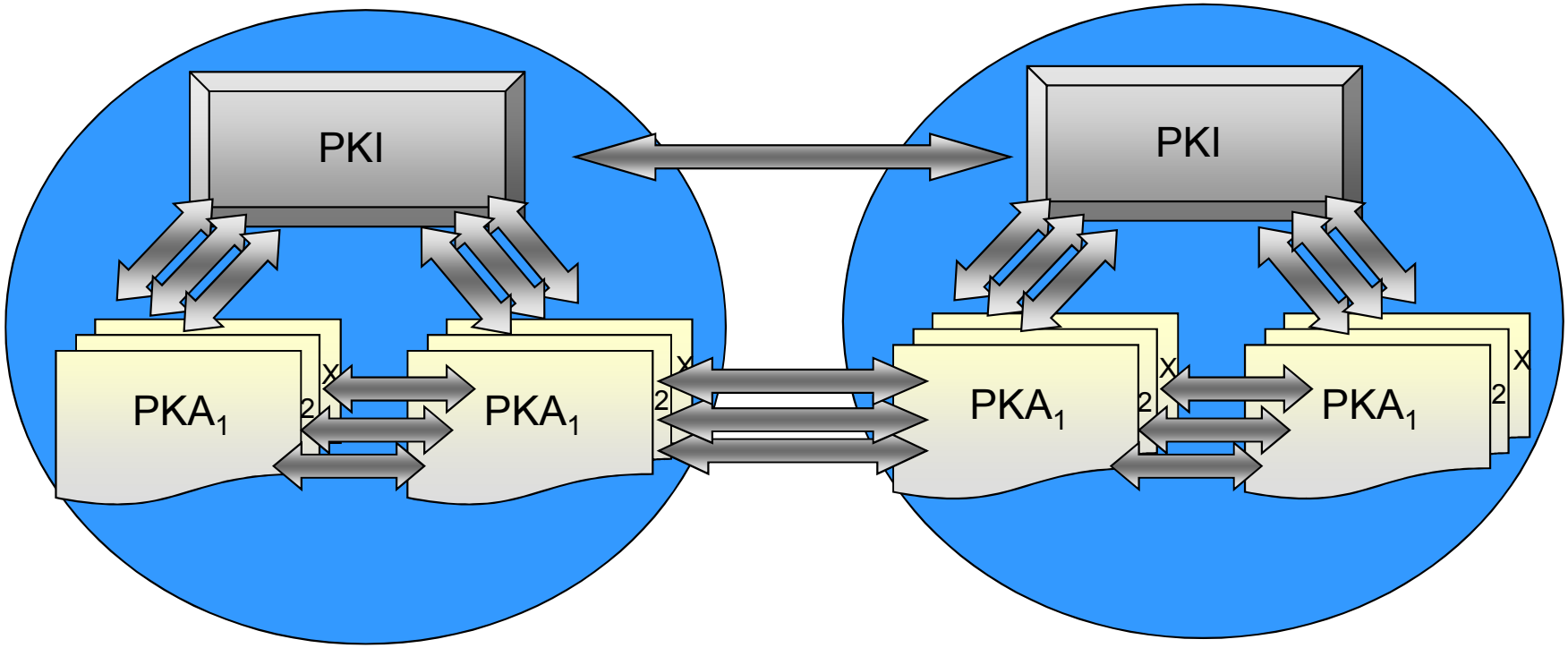


Organisation X

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Modelle von Public-Key-Infrastrukturen (2/3)

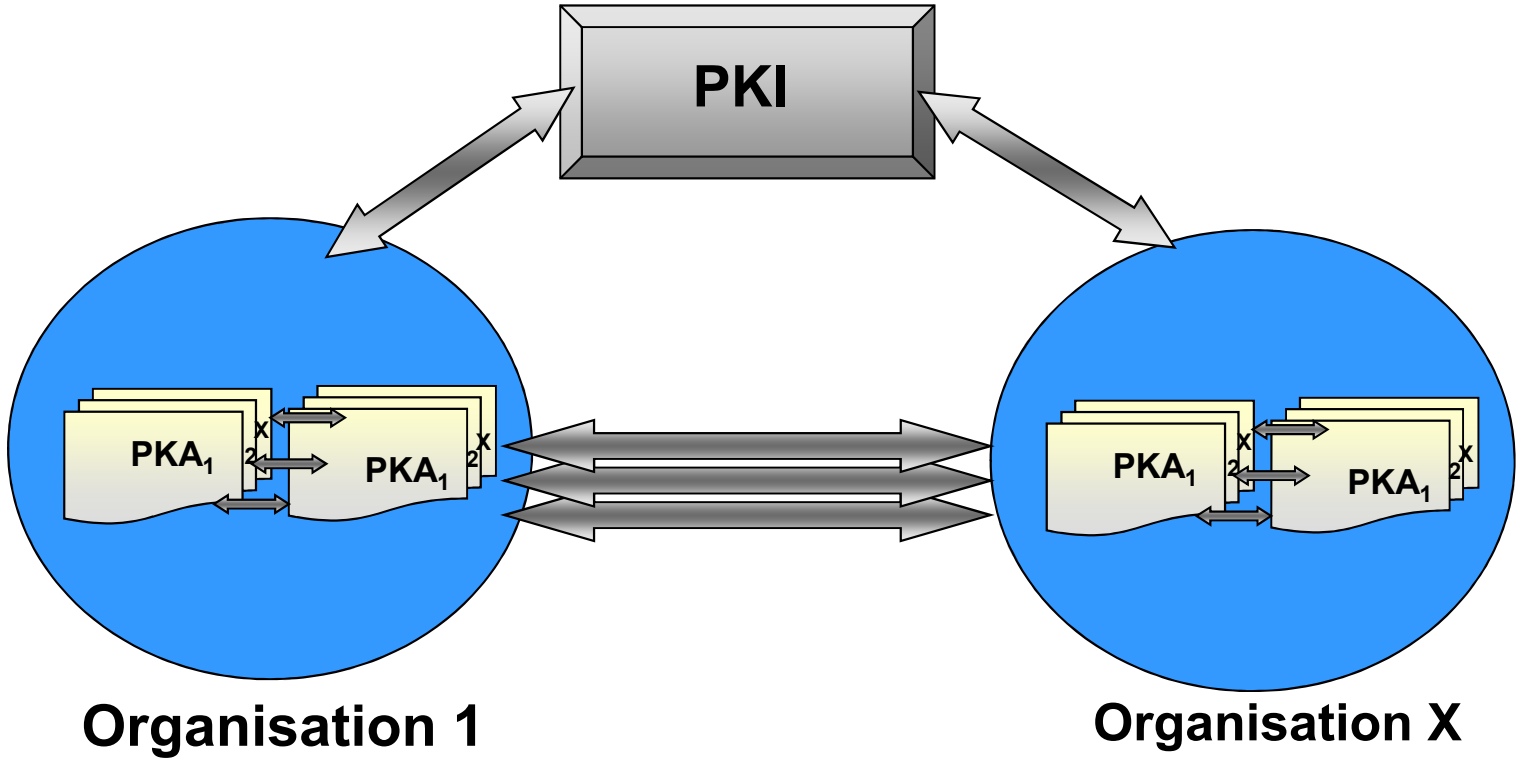
- **Offene Systeme**
  - Organisationen betreiben PKIs für eine oder mehrere Anwendungen. Die Verantwortung liegt bei der jeweiligen Organisation.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Modelle von Public-Key-Infrastrukturen (3/3)

- **Offene Systeme**
  - Ein PKI-Anbieter betreibt die PKI für eine oder mehrere Anwendungen, die in den Verantwortungsbereichen der nutzenden Organisationen liegen.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Probleme in der Praxis (1/2)

- **Bei geschlossenen Systemen**
  - Nicht nutzbar für organisationsübergreifende Prozesse
    → sehr starke Einschränkung

- **Bei offenen Systemen**
  - unterschiedliche Policies
    - Sicherheitslevel/Modell
      - Personenbezogen (Kostengesichtspunkt)
        - nach dem Signaturgesetz
        - nicht nach dem Signaturgesetz
      - Dienstbezogen
      - unterschiedliche PSEs
  - Vertrauen in die Sicherheit der Lösung
  - Standards
    (sehr viele, sehr komplex, ständige Weiterentwicklung, ...)
  - verschiedene Anwendungen haben unterschiedliche Anforderungen (SSL, E-Mail, ...)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Probleme in der Praxis (2/2)

- **Unterschiedliche Verantwortung von PKIs und PKAs in den Unternehmen**
  - die Abhängigkeit voneinander
  - erst mehrere PKAs führen zu hohem Nutzen
- **Henne-Ei-Problem**
  - nur wenn viele mitmachen, dann macht es ökonomisch Sinn
- **hoher personeller und organisatorischer Aufwand**
  - Sensibilisierung der Anwender für die IT-Sicherheit
  - Schulung der Anwender auf die Produkte
  - Roll-Out
- **Key-Recovery bei der Verschlüsselung**
- **...**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- **Vertrauensmodelle**
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

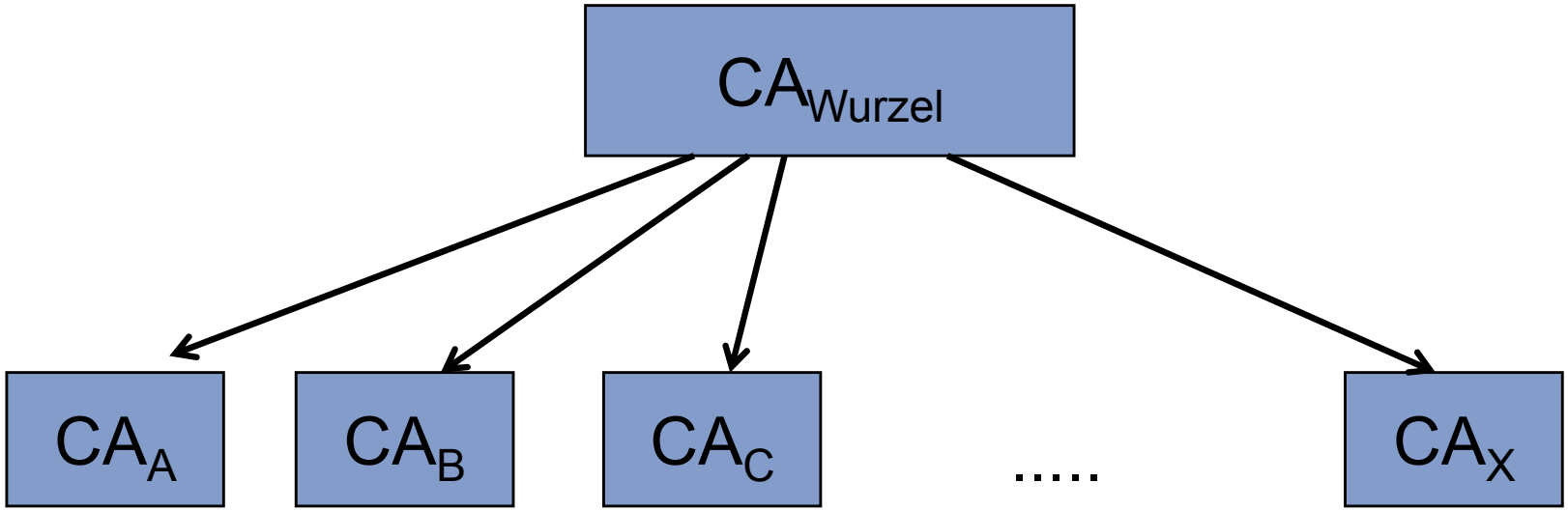
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauensmodelle
→ Motivation

- Es gibt sehr viele unterschiedliche Public-Key-Infrastrukturen.
- Es muss dafür gesorgt werden, dass die Zertifikate der unterschiedlichen Public-Key-Infrastrukturen auf Gültigkeit, Richtigkeit und den passenden "Level-of-Trust" überprüft werden können.
- Dazu gibt es verschiedene Vertrauensmodelle.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauensmodelle
→ Übergeordnete CA (Wurzel CA, Root CA)



Ablauf:

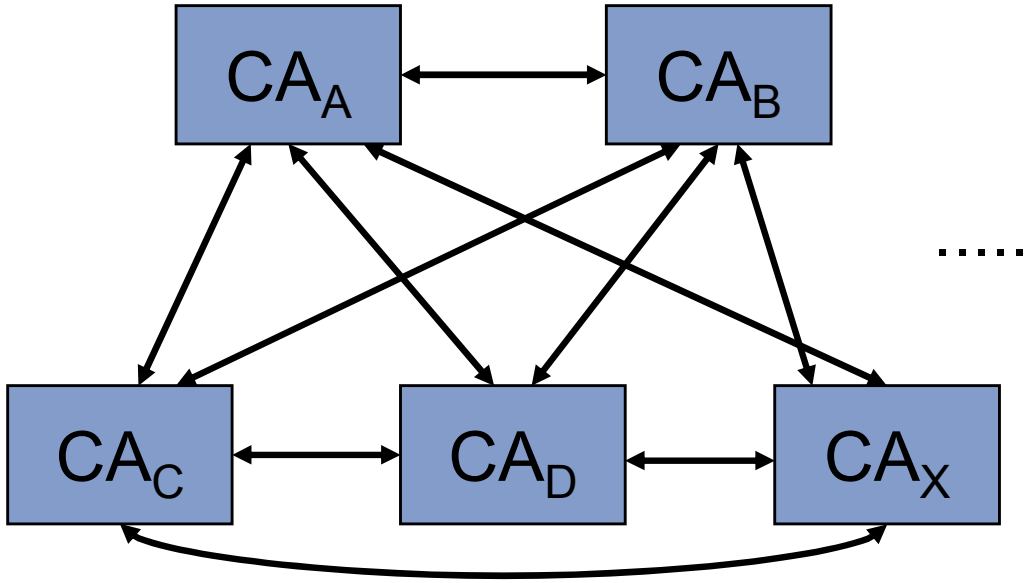
- CA_{Wurzel} generiert Zertifikate der öffentlichen Schlüssel der untergeordneten CAs
- Der öffentliche Schlüssel der CA_{Wurzel} steht in der PSE oder wird als Zertifikat der untergeordneten CAs zur Verfügung gestellt

Bewertung:

- Unternehmen, Organisationen, Länder akzeptieren nicht ihre Unterordnung → Welt CA

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauensmodelle
→ n:n Cross-Zertifizierung



Ablauf:

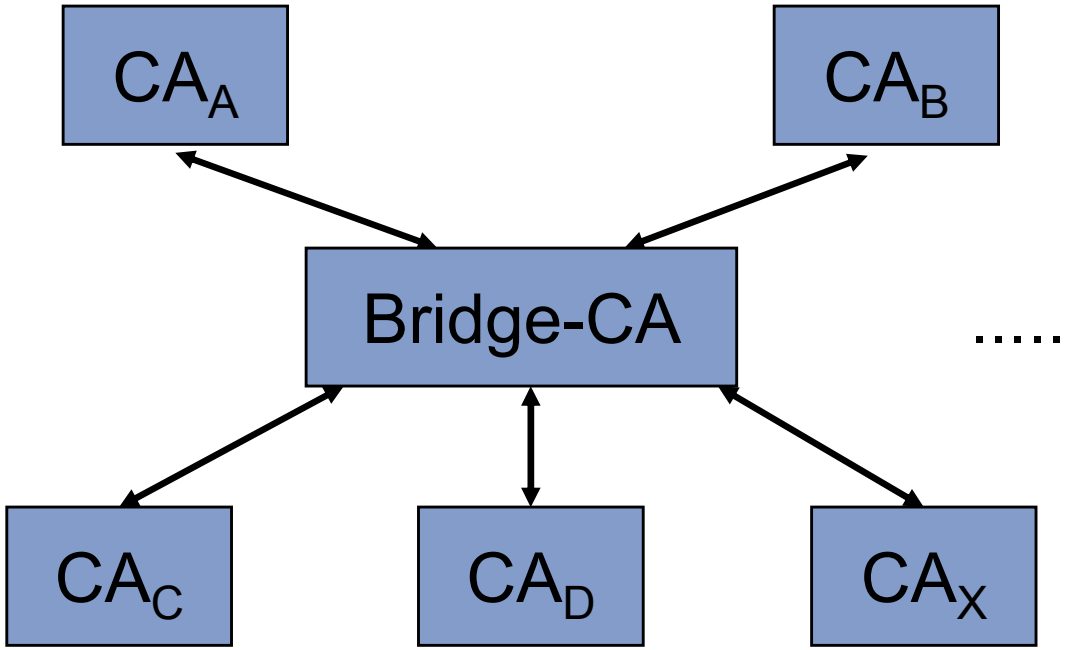
- Die CAs tauschen **authentisch** ihre öffentlichen Schlüssel aus
- Die eigene CA stellt Zertifikate der öffentlichen Schlüssel der anderen CAs zur Verfügung

Bewertung:

- Komplexe und unökonomische Administration
- Multiple Vertragsverhandlungen, sowie abweichende Verträge und Vereinbarungen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauensmodelle
→ 1:n Cross-Zertifizierung (Bridge CA)



Ablauf:

- Die CAs übergeben authentisch ihren öffentlichen Schlüssel an die Bridge-CA
- Die Bridge-CA signiert eine Tabelle der öffentlichen Schlüssel aller CAs
- Der öffentlichen Schlüssel der Bridge-CA wird von der eigenen CA als Zertifikat zur Verfügung gestellt

Bewertung:

- Nur ein Vertragspartner
- Maßgeschneiderte Vertrauenskette

Beispiel: www.bridge-ca.org

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Vertrauensmodelle
→ Weitere Aufgaben

- Da es Signaturen auf unterschiedlichen Vertrauensebenen gibt, muss ein Service dafür sorgen, diese unterschiedlichen Zertifikate nach einer vorgegebenen Sicherheitsrichtlinie bewerten zu können.
- XKMS ist ein Standard, der dies unterstützt.
- Der XKMS-Service übernimmt hierzu drei Aufgaben:
  - Bereitstellung von Zertifikaten und Schlüssel zum Aufbau einer gesicherten Verbindung.
  - Validierungs-Services, welche die Gültigkeit der Schlüssel/ Zertifikat nachweisen.
  - Registrierungs-Services, zur Bereitstellung und Annullierung von Schlüsseln.
- Ein XKMS Service unterstützt viele unterschiedliche PKI Protokolle und Datenformate, wie CRL (Certification Revocation List**), OCSP (Online Certifcation Status Protokoll)**, LDAP, CMS (Certification Managment Protocol) und SCEP (Simple Certification Entrolment Protocol).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle

- **Gesetzlicher Hintergrund**

- Standards
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Gesetzlicher Hintergrund

Die EU-Richtlinie (bis 01.07.2016 gültig)

- Das Europäische Parlament hat zusammen mit dem Rat der EU am 19. Januar 2000 eine vereinheitlichende Richtlinie veröffentlicht.

Signatur Gesetz (SigG)

- Die maßgeblichen Vorschriften zur Einführung der Elektronischen Signatur wurden in einem gesonderten **Signaturgesetz (SigG)** festgeschrieben und in der **Signaturverordnung (SigV)** explizit erläutert.
- Das **Formanpassungsgesetz** regelt die Gültigkeit elektronischer Signaturen im herkömmlichen Rechtsverkehr, indem das Bürgerliche Gesetzbuch an den entsprechenden Stellen angepasst wird.
- **Unterschiedliche Formen der elektronischen Signatur**
  - einfache Signatur
  - fortgeschrittene Signatur
  - qualifizierte Signatur (mit und ohne Anbieterakkreditierung)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Formen der elektronischen Signatur (1/4)

Einfache Signatur

- An diese Klasse der Signaturen werden nur sehr geringe Anforderungen gestellt.
- Es handelt sich um alle Daten, die einem Dokument beigefügt werden und zur Authentifizierung dienen, z.B. eine eingescannte Unterschrift oder eine Namenswiedergabe.
- Hierbei gibt es ein sehr geringes Maß an Authentizitätsfunktion und überhaupt keine Integritätsfunktion.
- **Die Beweisqualität ist also als gering zu bewerten.**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Formen der elektronischen Signatur (2/4)

Fortgeschrittene elektronische Signatur

- An die fortgeschrittene elektronische Signatur werden folgende Anforderungen gestellt:
  - dass sie ausschließlich dem Signaturschlüssel-Inhaber zugeordnet ist
  - mit der Signatur eine Identifizierung möglich ist
  - der Signaturschlüssel unter der Kontrolle des Inhabers gehalten werden kann
  - die Signatur mit den Daten verknüpft ist, damit eine nachträgliche Veränderung der Daten erkannt werden kann
  - dass es einen vertrauenswürdigen Dritten gibt, der als Zertifizierungsdienst fungiert und die Identität des Inhabers verifiziert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Formen der elektronischen Signatur (3/4)

Qualifizierte elektronische Signatur (1/2)

- Die qualifizierte elektronische Signatur ist eine Steigerung der fortgeschrittenen elektronischen Signatur.
- Es werden höhere Anforderungen an den Zertifizierungsdienst gestellt, welcher diese Signatur ausgibt.
- Dieser Zertifizierungsdienst muss von der Bundesnetzagentur akkreditiert werden.
- In Deutschland gibt es zurzeit drei solcher Zertifizierungsdienste für Normalbürger.
  - Telesec der T-Systems,
  - Signtrust der Deutschen Post und
  - D-Trust der Bundesdruckerei.
- Weiterhin können Rechtsanwälte und Steuerberater sich an die Datev wenden und Kunden der Deutschen Bank und Sparkasse an ihre Bank.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Formen der elektronischen Signatur (4/4)

Qualifizierte elektronische Signatur (2/2)

- Zertifikate von einem **akkreditierten Zertifizierungsdienst** enthalten eine Art Gütezeichen nach §15 Abs. 1 Satz 4 SigG.
  - Bei diesen wurde durch die Prüfung der „technischen und administrativen Sicherheit“ durch die Bundesnetzagentur vorab die Beweisqualität sichergestellt und von den Gerichten auch ohne weitere Prüfung des Verfahrens anerkannt.
  - Die Beweisführung vor Gericht wird damit erleichtert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

eIDAS
→ Übersicht

Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Zertifikate von einem **akkreditierten Zertifizierungsdienst** enthalten eine Art Gütezeichen nach §15 Abs. 1 Satz 4 SigG.

- Bei diesen wurde durch die Prüfung der „technischen und administrativen Sicherheit“ durch die Bundesnetzagentur vorab die Beweisqualität sichergestellt und von den Gerichten auch ohne weitere Prüfung des Verfahrens anerkannt.
- Die Beweisführung vor Gericht wird damit erleichtert.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

eIDAS
→ Was ist neu?

- **Zertifikat kann temporär suspendiert werden**
  Bsp.: Smartcard wird verlegt, dann aber wiedergefunden
- **Spezifische Zertifikatsattribute**
  Meister, Doktor, Master, …
- **Elektronische Siegel** als Pendant zu elektronischen Signaturen für Organisationen
- **Fernsignaturen möglich**
  Idee: SSEE bleibt beim VDA; Auslöser wird mit technischen Mitteln verlängert, VDA stellt vertrauenswürdige Umgebung sicher. Darf nur von qualifizierten VDA angeboten werden
- **Elektronische Einschreiben**
  Identifizierung des Absenders, Identifizierung des Empfängers vor Versand, Senden/Empfang durch FES eines qualifizierten VDA
  vor Veränderung geschützt, Datenveränderungen werden deutlich hervorgehoben. Zeit, Datum von Versand/Empfang oder Datenänderung wird durch qualifizierte Zeitstempel angezeigt

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Geeignete Kryptoalgorithmen
→qualifizierte elektronische Signatur in D

- **Geeignete Signaturalgorithmen**
  - RSA: $h^d \bmod n$

Zeitraum Parameter	Ende 2010	Ende 2017
n	1728 (Mindestw.) 2048 (Empf.)	1976 (Mindestw) 2048 (Empf.)

  - DSA (Digital Signatur Algorithms - FIPS-186)

Zeitraum Parameter	Ende 2015	Ende 2017
p	2048	2048
q	224	256

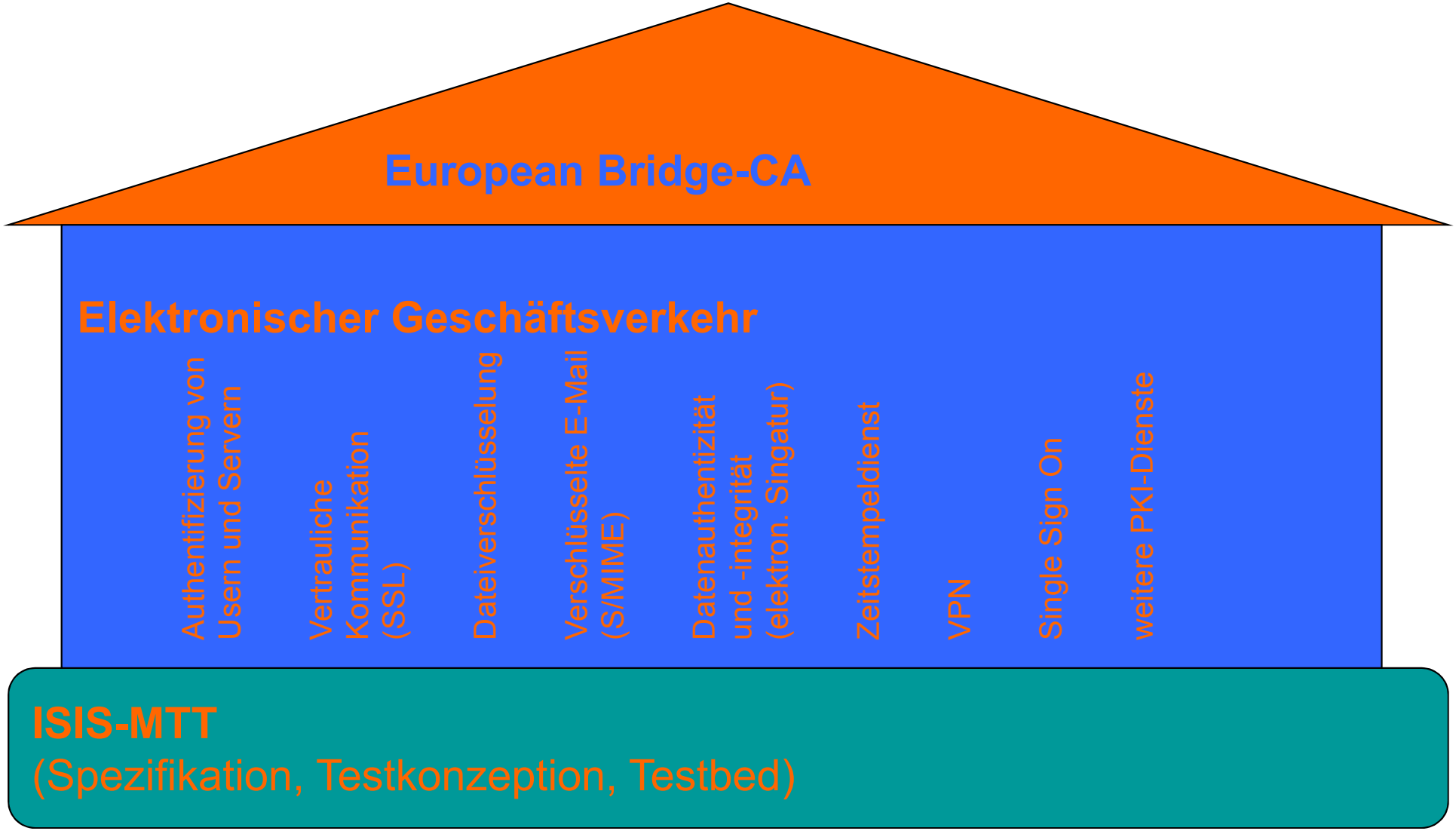
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- **Standards**
- Umsetzungskonzepte
- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

ISIS-MTT
→ Das Fundament



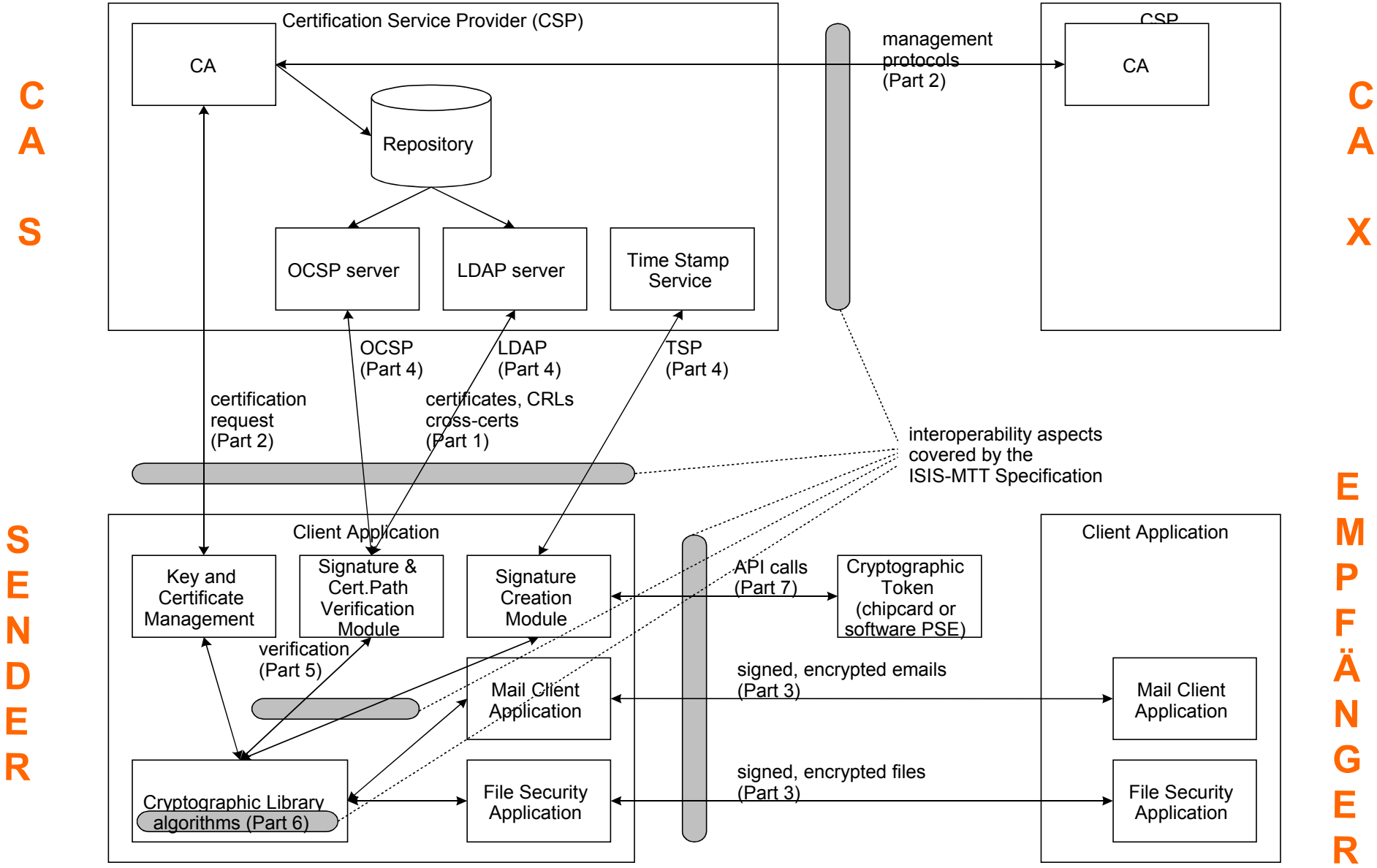
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

ISIS-MTT
→ Motivation der Beteiligten

- Internationale Standards lassen zu hohe Freiheitsgrade bei der Implementierung.
- Auch zwischen deutschen Anbietern gab es keine Interoperabilität. Ohne Interoperabilität keine Marktrelevanz für deutsche Anbieter.
- Durchsetzung deutscher Gestaltungswünsche bei der internationalen Standardisierung ohne gemeinsame Spec. nicht möglich.
- Interoperabilität zwischen Signaturen mit unterschiedlichen Anforderungen, z.B. zwischen fortgeschrittenen und qualifizierten Signaturen.
- Investitionssicherheit für PKI-Anwender und –Anbieter.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

ISIS-MTT
→ Übersicht



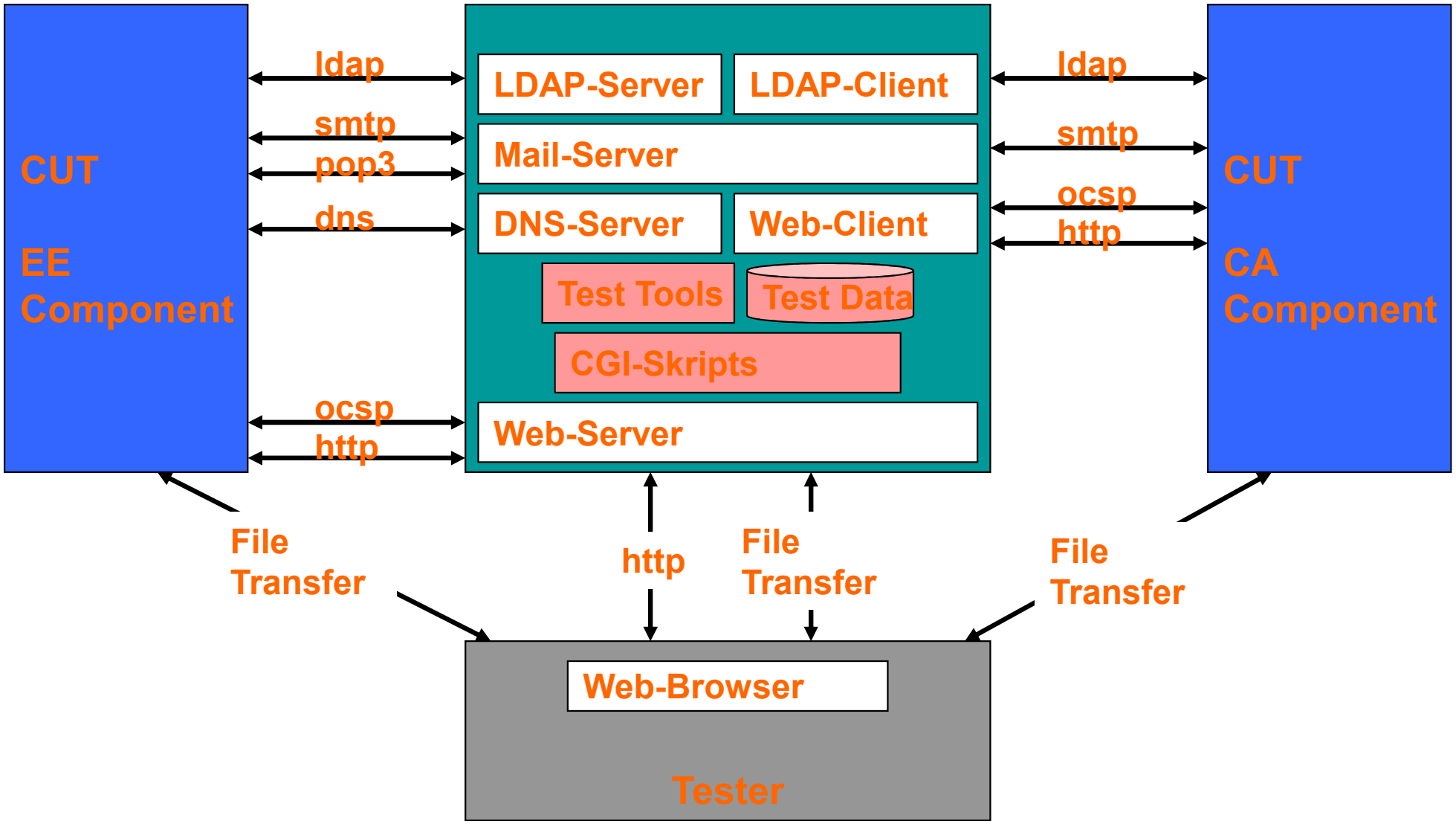
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

ISIS-MTT
→ Dokumentenstruktur

- Part 1: Certificate and CRL Profiles,
- Part 2: PKI Management,
- Part 3: Message Formats,
- Part 4: Operational Protocols,
- Part 5: Certificate Path Validation,
- Part 6: Cryptographic Algorithms,
- Part 7: Cryptographic Token Interface,
- Profile: SigG-conforming Systems and Applications
- Profile: Optional Enhancements to the SigG-Profile.

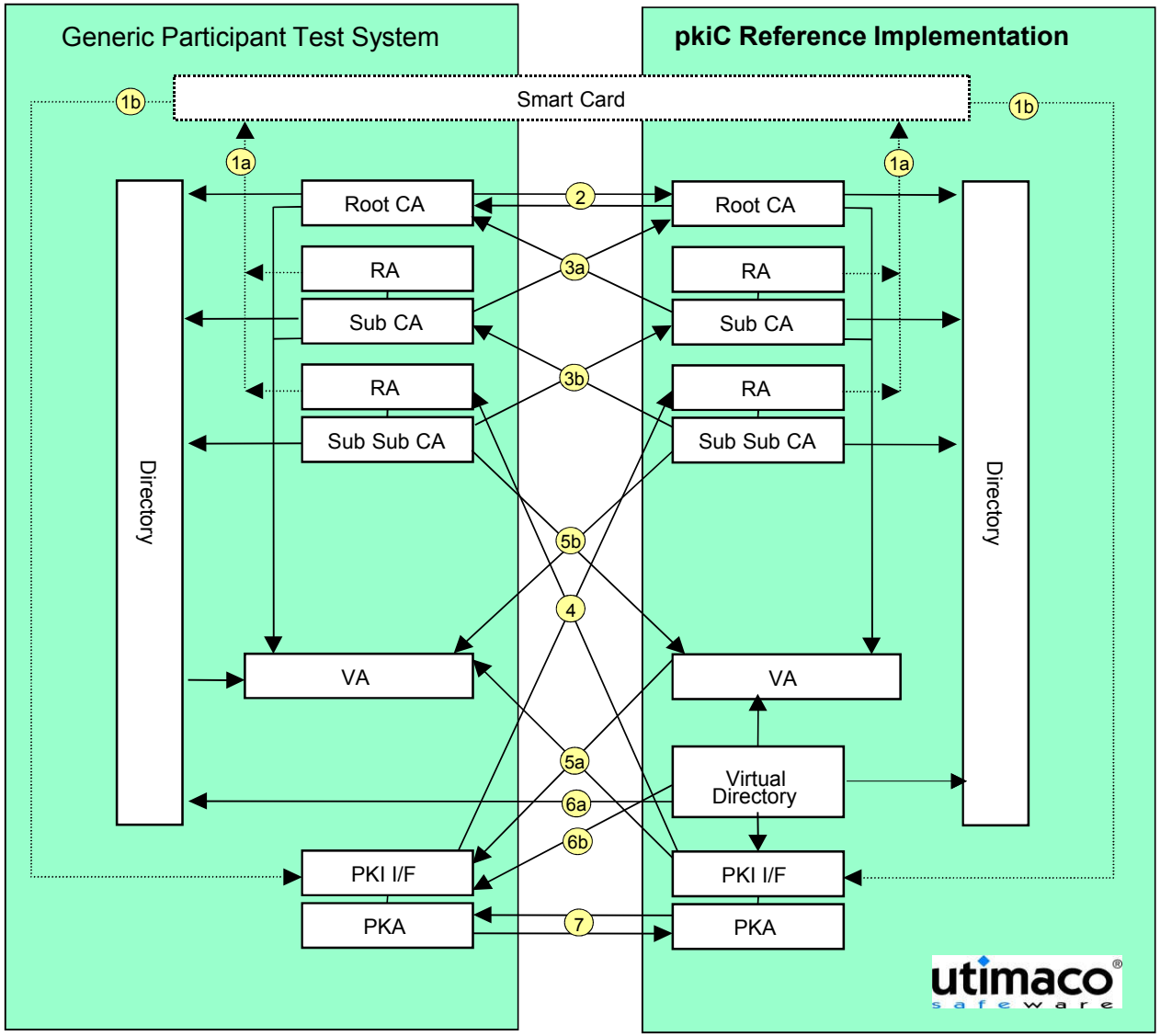
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

ISIS-MTT
→ Testbed Prototype Platform



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

PKI-Challenge (EU)
→ Migration und Interoperabilität



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards

- **Umsetzungskonzepte**

- Realisierungen
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Umsetzungskonzepte

- Verschiedene Anwendungen haben unterschiedliche Sicherheitsbedürfnisse!
- Unterschiedliche Sicherheitsbedürfnisse können isoliert einfacher realisiert werden!
- Isolierte Lösungen haben einen klaren Fokus!
- Ein klarer Fokus hat wenige Probleme und ist daher schnell, einfacher und kostengünstiger zu realisieren.

- **Wir brauchen pragmatische Ansätze!**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Umsetzungskonzepte
→ SSL

- Vertrauliche Kommunikation zwischen Client und Web-Server
  - die ausgetauschten Daten sollen nicht mitgelesen werden
  - eine explizite **Datenschutzanforderung!**
  - Infrastruktur ist bereits heute schon vorhanden, PKI etabliert, Clients unterstützen den Standard (Browser)
  - Web Server sind für die SSL Verschlüsselung vorbereitet.
  - SSL als Open Source etabliert im Markt
  - Industrie hat den Markt erkannt: SSL Accelerator
  - **Aspekt der leichten Anwendbarkeit (integrierte Zertifikate)** vs. Sicherheitsabwägungen (200+ CAs im Browser)

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Umsetzungskonzepte
→ E-Mail-Sicherheit

- Zu schützende Unternehmensdaten sollen ausgetauscht werden (personenorientiert)
- Vertraulichkeit der Kommunikation zwischen sich kennenden Personen ist von zentraler Bedeutung!
- Verbindlichkeit, wenn eine kostenintensive Aktion aus der E-Mail abgeleitet wird.
- E-Mail als Medium ist dem Nutzer bekannt und vertraut, sicherheitsrelevante Funktionen sollen sich verständlich in das Benutzerinterface einfügen, um den Nutzer nicht zu verwirren.
- Bei der E-Mail-Sicherheit hat der **Benutzer eine aktive Rolle** gegenüber der passiven Rolle bei SSL

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Umsetzungskonzepte
→ Verbindlicher Austausch von Transaktionsdaten

- Der Empfänger muss die Verbindlichkeit abschätzen können, weil er kostenintensive Aktionen daraus ableitet!
- Diese Anwendungen sind meist firmen- bzw. geräteorientiert
- Basieren meistens auf geschlossenen Systemen
- Ziel ist immer die Integration in bestehende Workflows (Arbeitsabläufe)
- Von kleinen Datenmengen pro Monat bis hin zu einer hohen Anzahl von Transaktionen pro Minute.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- **Realisierungen**
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Realisierungen von Digitalen Signaturen

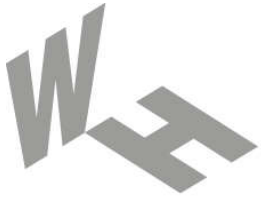
Realisierungen in

- ***E-Mail-Programmen***
- Office Anwendungen wie Word, Excel, ...
- VPN, SSL
- Web-Anwendungen
- Anwendungen wie z.B. SAP (z.B. Materialwirtschaft)
- ...

Anwendungen

- ***Lotto (ODDSET)***
- Steuererklärungen (ELSTER)
- BundOnline2005
- Remote Access (Authentikation)
- Integrität von SW
- Elektronische Wahlen
- Elektronischer Zahlungsverkehr
- ...

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

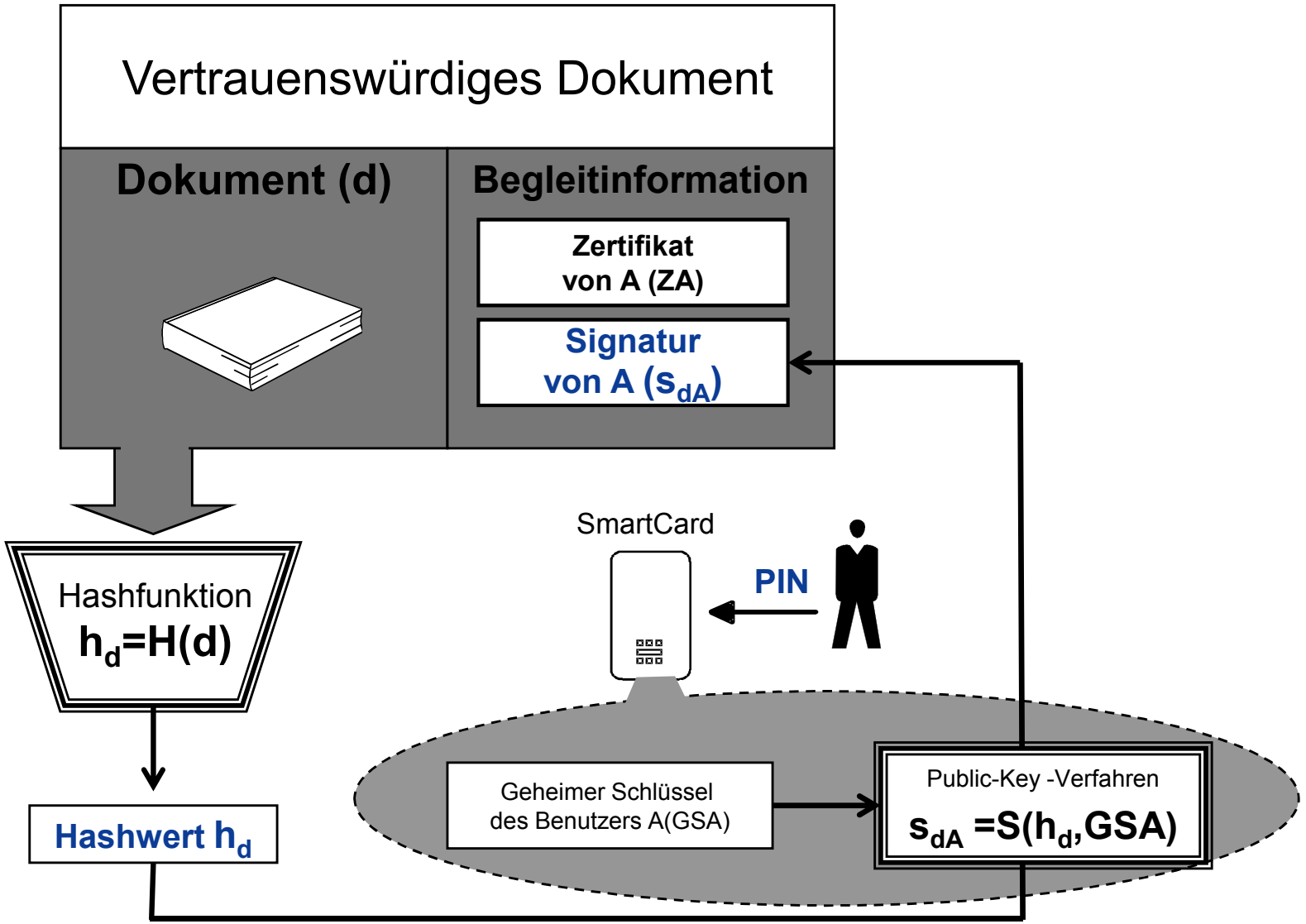
E-Mail Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

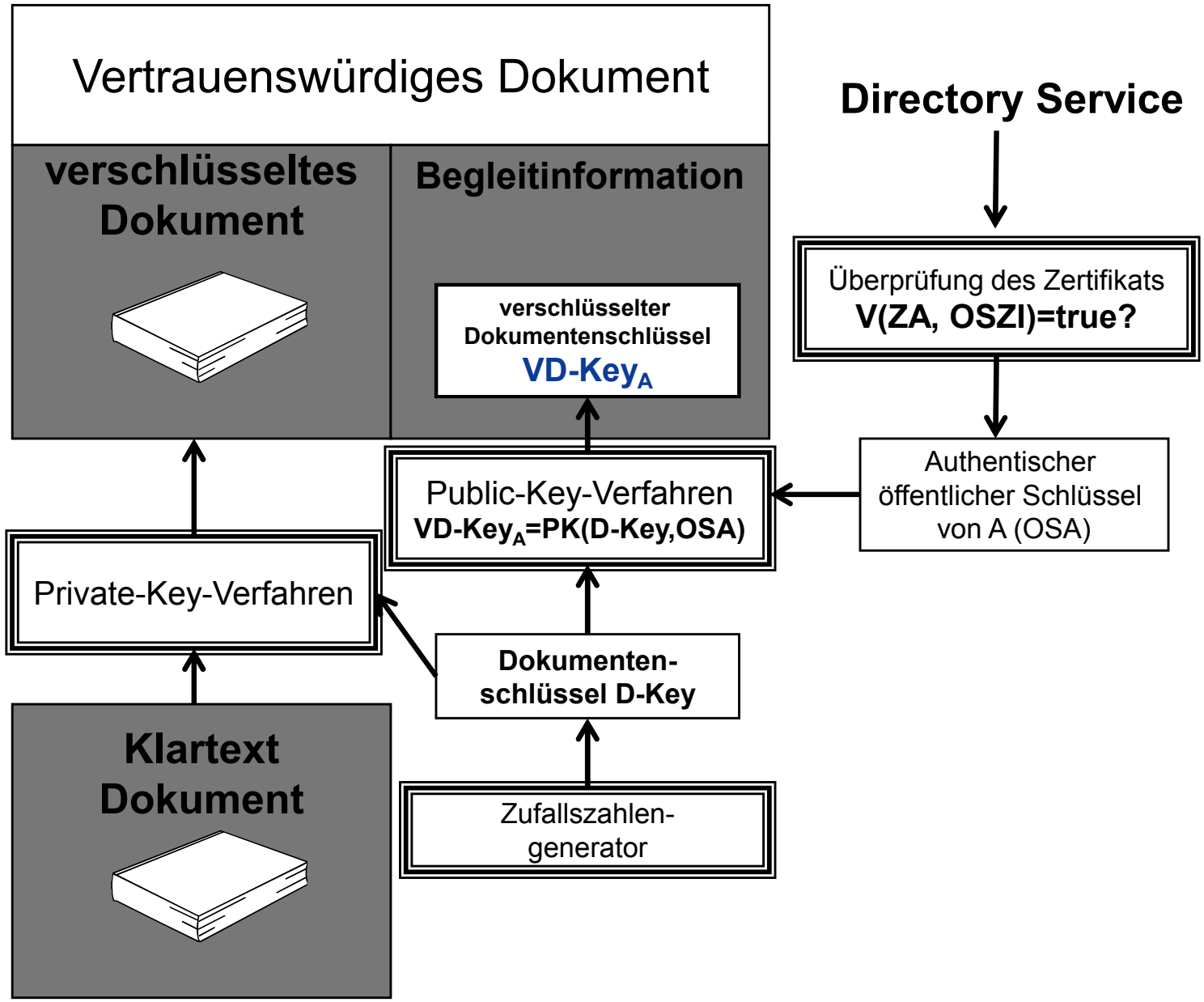
if(is) internet-sicherheit.

E-Mail Sicherheit
→ Signatur



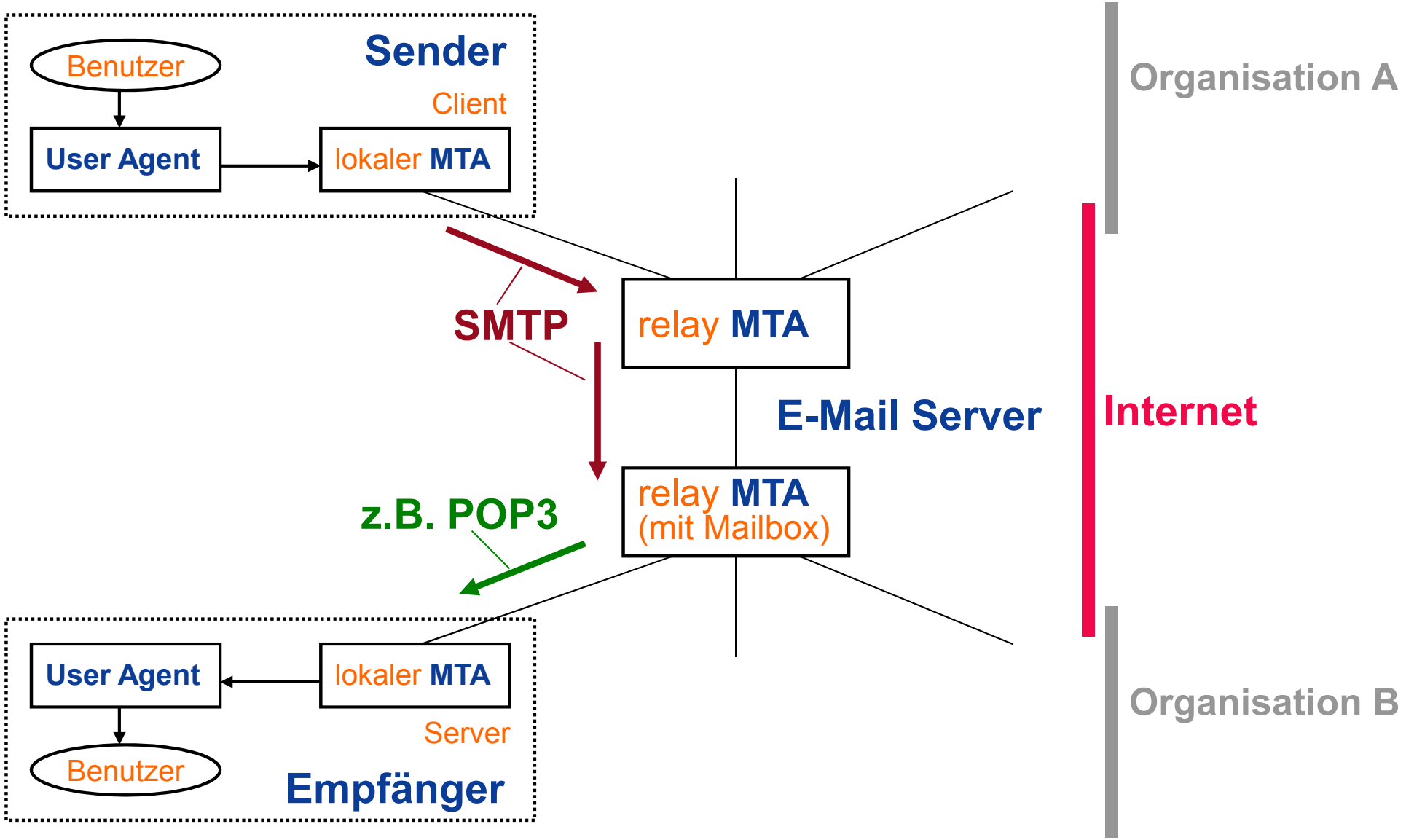
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

E-Mail Sicherheit
→ Verschlüsselung



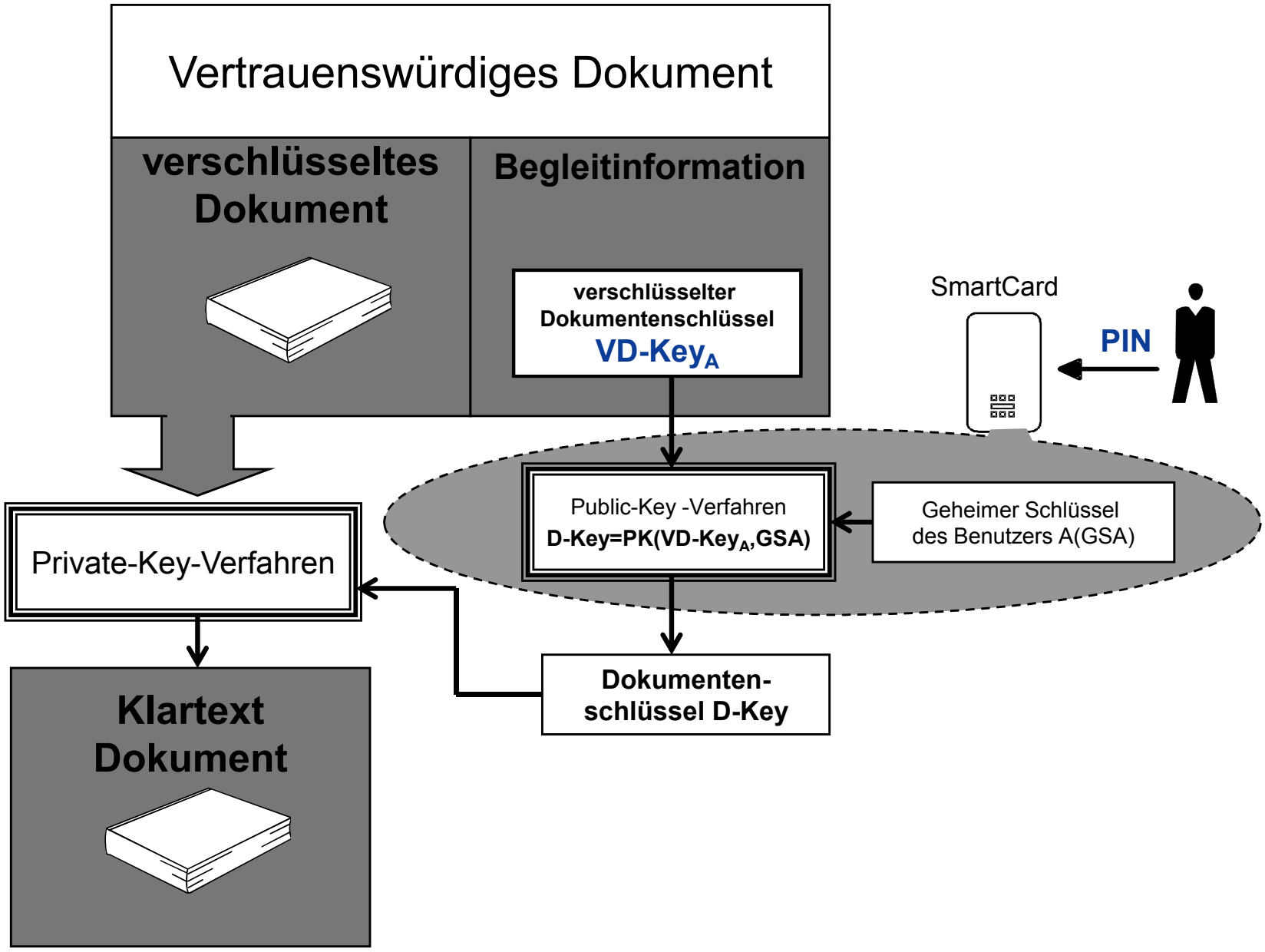
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

E-Mail Sicherheit
→ Übertragung



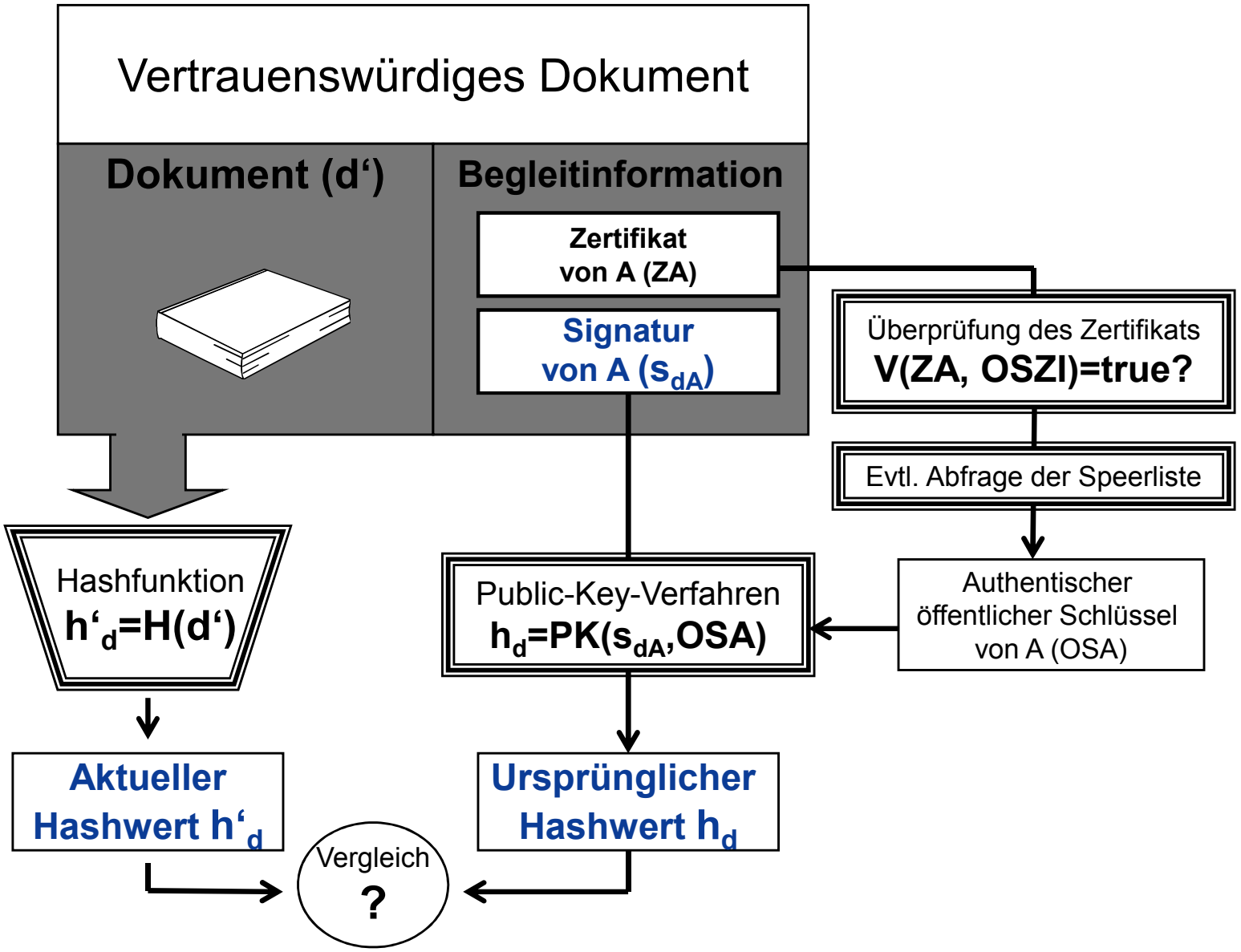
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

E-Mail Sicherheit
→ Entschlüsselung

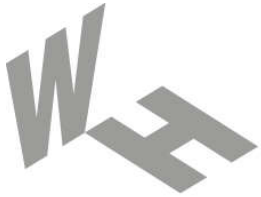


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

E-Mail Sicherheit
→ Verifikation



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

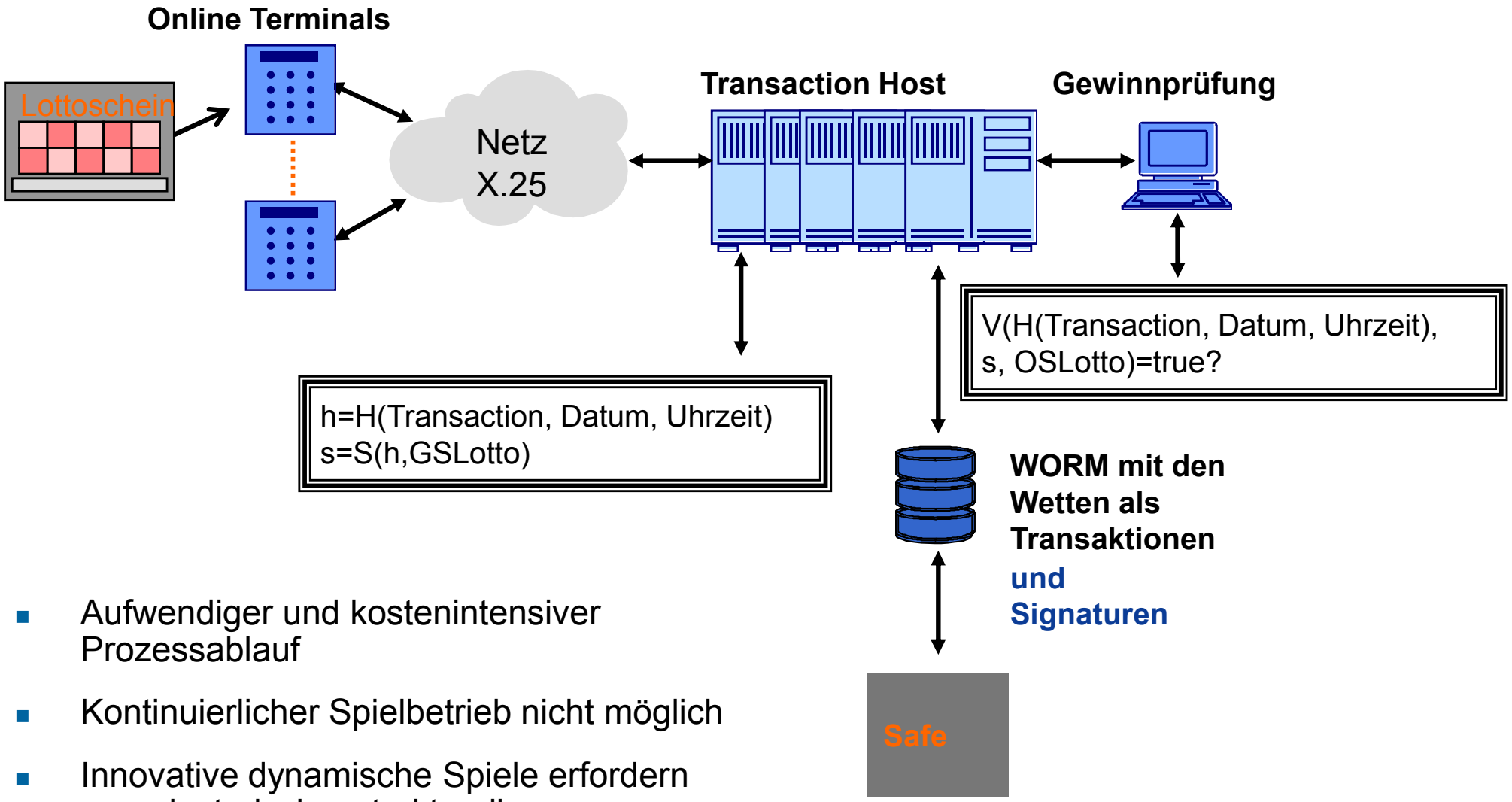
Lotterie Gesellschaften

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Lotterie Gesellschaften



- Aufwendiger und kostenintensiver Prozessablauf
- Kontinuierlicher Spielbetrieb nicht möglich
- Innovative dynamische Spiele erfordern organisatorische, strukturelle und kryptographische Maßnahmen

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Inhalt

- Einführung
- Verfahren und Prinzipien der digitalen Signatur
- Elektronische Zertifikate
- Public-Key-Infrastrukturen (PKI) und PKI-enabled Application (PKA)
- Vertrauensmodelle
- Gesetzlicher Hintergrund
- Standards
- Umsetzungskonzepte
- Realisierungen
- **Zusammenfassung**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Zusammenfassung

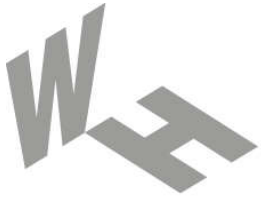
- Kryptographische Algorithmen, Einbindungstechnologie, SmartCards und PKIs sind vorhanden.
- Realisierungen in geschlossenen Anwendungen laufen sehr gut (digitaler Dienstausweis, Zugriffskontrolle, ...).
- Probleme zur Zeit
  - Vertrauenskette organisations- und länderübergreifend
  - einheitliche Verwendung von Standards
- Pragmatische Lösungen
  - European Bridge-CA
  - Signaturbündnis; Jobkarte, Gesundheitskarte
  - XKMS

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Literaturhinweise

- G.Simmons(Hrsg.): „Contemporary **Crytology** - The Science of Information Integrity“, IEEE Press, New York
- F.P.Heider, D. Kraus, M. Welschenbach: „**Mathematische Methoden der Kryptoanalyse**“, Vieweg Verlag 1985
- P. Horster (Hrsg.): „**Trust Center** - Grundlagen, rechtliche Aspekte, Standardisierungen, Realisierungen“, Vieweg, Wiesbaden
- A. Glade, H. Reimer, R. Struif (Hrsg.): „**Digitale Signatur & Sicherheitssensitive Anwendungen**“, Vieweg, Wiesbaden
- N. Pohlmann: **„Nutzen und Chancen von Public-Key-Infrastrukturen"**, in "Sicherheitsinfrastrukturen in Wirtschaft und Verwaltung", Hrsg.: P. Horster, IT Verlag, 2002
- P. Laing, N. Pohlmann: **„Digitale Signatur im elektronischen Materialzeugniswesen"**, in "DACH Security ", Hrsg.: P. Horster, syssec Verlag, 2003
- Anja Miedbrodt: „**Signaturregulierung im Rechtsvergleich** - Ein Vergleich der Regulierungskonzepte in Deutschland, Europa und in den Vereinigten Staaten von Amerika“, Nomos Verlagsgesellschaft, Baden-Baden
- C.Langenbach, O. Ulrich (Hrsg.): „**Elektronische Signaturen** - **Kulturelle Rahmenbedingungen** einer technischen Entwicklung, Springer Verlag, Berlin
- www.bsi.de, www.teletrust.de, www.bridge-ca.org, www.regtp.de

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Planung einer PKI

Literatur: Nash, Duane, Joseph, Brink, Deutsche Ausgabe PKI, e-security implementieren

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Planung einer PKI (1/6)

- **Bestimmenden Faktoren** im Unternehmen erkennen
  - E-Business zur Reduzierung von Kosten und Absicherung von Transaktionen
  - Vertraulichkeit, Integrität und Authentizität von Informationen
  - Reduzierung des Papieraufkommens
  - Geringere User-Support-Kosten (Stichwort: SSO)
  - Gesetzliche Bestimmungen (D: KontraG, TKG; USA: HIPAA)
  - Zusätzliche Sicherheit durch verbesserte Authentifizierung, Autorisierung und Zugangssteuerung
- **Grad der Integration der PKI ins Unternehmen definieren**
- **Entscheidungen:**
  - Welche sind die wichtigsten bestimmenden geschäftlichen Faktoren für die PKI? Wie werden sich diese in Zukunft entwickeln?
  - Wer wird die PKI auf Vorstandsebene befürworten?
  - Wer vergibt die Gelder für die PKI-Planung? Wenn die Entscheidung für die Realisierung der PKI fällt, woher werden diese Gelder kommen?

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Planung einer PKI (2/6)

- Eine mögliche **Migration der Anwendungen** und Prozesse im Unternehmen auf die Verwendung einer PKI untersuchen

- ROI stellt sich bei einigen Anwendungen schneller ein als bei anderen. Manchmal benötigt ein Unternehmen erst die Kombination aus mehreren Anwendungen (unterschiedlicher Abteilungen), um von einer PKI zu profitieren.
  - Sichere E-Mail
  - Sichere Kommunikation
  - Sichere Business Transaktionen
  - Einheitliche Anmeldung (Single Sign-On)

- Entscheidungen:
  - Welche Anwendungen werden die PKI nutzen? Prioritäten?
  - Wie werden bestehende Anwendungen auf PKI migriert und in welcher Reihenfolge?
  - Werden neue Anwendungen im Unternehmen die PKI unterstützen müssen? Richtlinie, Überwachung, Zuständigkeiten

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Planung einer PKI (3/6)

- Einschätzen der zumutbaren **Beeinträchtigungen für die Benutzer** einschätzen
  - Geänderte Programmabläufe nach Migration der Anwendung
  - Registrierung bedeutet Aufwand für den Benutzer (wesentlicher Grundsatz einer sicheren PKI ist die eindeutige Identifizierung der Benutzer)
  - Verschärfte Verbindlichkeit für den Benutzer (elektronische Signatur)

- Entscheidungen
  - Wie viele Benutzer sollten ein Zertifikat bekommen? (interne Mitarbeiter und externe Geschäftspartner?)
  - Gibt es unterschiedliche Benutzerkategorien in den Zertifikaten, wie Angestellte, freie Mitarbeiter, Kunden, Lieferanten usw.?
  - Welche Beeinträchtigung der Benutzer ist akzeptabel, um die Ziele des Unternehmens erreichen zu können?

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Planung einer PKI (4/6)

- Planung der **Architektur**
  - Regiestierungsstelle (RA), Zertifizierungsstelle (CA) …
  - Offenes System oder geschlossenes System
  - Vertrauensmodell mit anderen Unternehmen
  - Standards, Zertifikatsinhalt …

- **Auswirkungen auf die Infrastruktur**
  - Physisches Absichern des Zertifizierungsservers
  - Stärkere Belastung der Netzwerkressourcen
  - Hohe Anforderungen an Sicherheit und Verfügbarkeit

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Planung einer PKI (5/6)

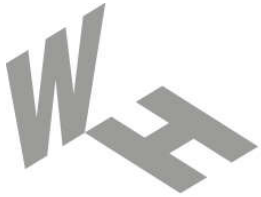
- Planungsphase sorgfältig durchführen, um schwerwiegende und zeitaufwendige Probleme in der Umsetzungsphase zu minimieren.
  - Definieren und Dokumentieren der Entscheidungen in der **Zertifizierungsrichtlinie** (Certificate Policy – CP) und **Ausstellererklärung** (Certification Practices Statement – CPS)
    - Haftungsbeschränkungen, Gewährleistung
    - Anforderungen für die Ausstellung eines Zertifikats (Registrierungsprozedur)
    - Sperrung von Zertifikaten, Sperreintragslisten, Überprüfung der Gültigkeit von Signaturen
    - Helfen bei der gegenseitigen Zertifizierung zwischen Unternehmen (Vertrauensmodelle)
    - Erstellen nach RFC 3647 (früher RFC 2527) oder ETSI TS 101 456

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Planung einer PKI (6/6)

- Die Planung, Umsetzung und der Betrieb einer PKI erfordert die Berücksichtigung verschiedener technischer, finanzieller und zwischenmenschlicher Aspekte
  - Sehr komplex, erfordert spezifisches Wissen, muss gewissenhaft und genau durchgeführt werden, großer Zeit und Ressourcen Aufwand
- Der Betrieb einer PKI umfasst mehr als die Erzeugung von Zertifikaten
- Eine PKI muss sicher betrieben werden und eine bindende Aussage zwischen einem Public-Key und einer damit verbundnen Identität erlauben
- Einzelne Insellösungen im Unternehmen oder zwischen Geschäftspartner führen nicht zu einem rentablen Ergebnis

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Digitale Signatur und Public Key Infrastruktur (PKI)

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule
http://www.internet-sicherheit.de

if(is) internet-sicherheit.