

Luzernertagung: Digitale Identitäten

Prof. Dr. Bernhard M. Hämmerli

Willkommen und Begrüssung

UNISYS
imagine it. done.

HIS | IT-SECURITY
WE MANAGE IT RISKS

security
zone 06
PLATTFORM FÜR INFORMATIONSSICHERHEIT

PortWise
Secure Application Access. Anywhere.

ca



Biometric Security AG

DIE POST 

tetrade.
we Integrate IT

 **Sun.**
microsystems

>> Programm Stuktur

13:15 Eröffnung durch Prof. Dr. Bernhard M. Hämmerli,
HTA Luzern

13:25 Keynotes von:

- > Frank Schwarze (krank) (Killerapplikation)
- > PD Dr. Hannes P. Lubich CA
- > Gian Manetsch, Beate Fiedler: Die Post
- > Beat Lehmann

14:40 Parallele Diskussionsforen

16:20 Pause

16:45 Präsentationen und Diskussion der Resultate aus
den Praxisforen im Plenum

17:30 Abschluss und Apéro

>> Keynote Referate

- Moderation:** Prof. Dr. Bernhard M. Hämmerli, Hochschule Technik+Architektur Luzern
- > **Digitale Identitäten für Nomadic Computing**
Frank Schwarze, Portwise
 - > **Digitale Identitäten bei der Schweizer Post**
Gian Manetsch & Beate Fiedler, Die Schweizerische Post / Postfinance
 - > **Identität und Autorisierung als Grundlage für sichere Web-Services**
PD Dr. Hannes P. Lubich, Principal Consultant, Computer Associates AG
 - > **Sorgfalt, Verantwortung und Haftung beim Umgang mit digitaler Identität**
Beat Lehmann, Fürsprech

>> Foren (1/4)

Forum 1: Digitale Identitäten in der öffentlichen Verwaltung

- Leiter:** Marcel Frauenknecht, Leiter Bereich Informatiksicherheit, Bund
- Co-Leiter:** Dr. Marcus Holthaus, IMSEC GmbH
- Teilnehmer:** Reto Grünefelder, HIS Software AG
Daniel Messerli, EJPD
Urs Jermann, SIK
Malte Naumann, tetrad AG

Wie will der Bund den Bürger digital identifizieren? Welche digitalen Identitäten verwenden die Kantone? Welche Zertifikate benötigen Mitarbeiter der öffentlichen Verwaltung? Weshalb kommen Zertifikate zum Einsatz? Wer stellt die Zertifikate aus? Welche Prozesse sind dazu erforderlich? Welche Rolle spielt die Smartcard (Smart Crypto Card) in diesem Umfeld? Wer ist für das Management der Smartcards (USB Token) verantwortlich und welche Anforderungen muss diese Organisation erfüllen können?

>> Foren (2/4)

Forum 2: Die Anwendung der Digitalen Identität in der Wirtschaft

- Leiter:** Thomas Kohler, UBS AG
Co-Leiter: Frank Heinzmann, PWC
Teilnehmer: Adolf Dörig, Gründungspräsident FGSec
Hanspeter Koller, UBS AG
Roger Bürgler, UBS AG
Joseph Doekbrijder, SwissSign AG

Welche Bedeutung hat die digitale Identität für die Bank? Wie sind die Umsetzungen heute? Wie sieht die Bank die Zukunft? Wie ist die Akzeptanz beim Kunden heute und wie kann diese beeinflusst werden?

>> Foren (3/4)

Forum 3: Technologien und Umsetzung der sicheren Digitalen Identität

Leiter: Dr. Urs E. Zurfluh, CEO Ad Vantis AG
Co-Leiter: Thomas Schlienger
Teilnehmer: PD Dr. Hannes P. Lubich, Computer Associates AG
Willy Müller, ISB
Beate Fiedler, Postfinance
Thomas Krieg, Sun

Welche Angebote sind auf dem Markt? Welche unterschiedlichen Qualitäten digitaler Identitäten sind heute im Einsatz? Was ist zu beachten bei der Verwaltung von digitalen Identitäten in einer heterogenen IT-Umgebung? Wie sieht eine moderne Provisionierungslösung aus? Wie sehen die Zukunftsperspektiven aus? Wie kann ich Security Compliance sicher stellen? Wie wird die Digitale Identität gegen Verlust und Missbrauch gesichert? Welche Restrisiken bleiben? Welches Sparpotenzial ist für diese Anwendergruppe zu realisieren? Wie wird eine sichere Web-Service Architektur aufgebaut? Welche Sicherheits-Standards sind relevant? Welche Rolle spielt die Smartcard (Smart Crypto Card) in diesem Umfeld?

>> Foren (4/4)

Forum 4: *Biometrie, der neue Trend: Grundlagen, Praxiserfahrungen und Ausblick...*

Leiter: Robert de Boer, inovate.ch GmbH

Co-Leiter: Peter Fürst, Wirtschaftspublizist

Teilnehmer: Urs Schmied, Unisys

Rico Barandun, Swissport Aviation Security

Klaus Keus, Bundesamt für Sicherheit in der Informationstechnik, D (BSI)

René Brüderlin, Biometric Security AG

Biometrie ist auf dem Vormarsch und wird mit rasanten Tempo erwachsen. Was leistet Biometrie in der IT Sicherheit? Wie zuverlässig ist ihre Verifikation von Identitäten? Was bietet die Branche? Wo und wie kann Biometrie eingesetzt werden? Welche physiologischen Merkmale (Fingerabdruck, Iris, Netzhaut, Handgeometrie, Venenmuster, Gesicht) eignen sich? Was meint das Gesetz dazu? Was braucht es, um Biometrie in der IT-Sicherheit einzusetzen? Was können die Kosten sein? Wo liegen die Grenzen? Wie ist der technische Stand?

Nächste grosse Tagungen der FGSec

Zürcher Tagung: 11. Mai 2006:

IT-Governance

Berner Tagung: 14. November 2006

***Sponsoren, Vortragende, Experten sind
gesucht. Bitte bei mir melden.***

>> Programm

13:15 Eröffnung durch Prof. Dr. Bernhard M. Hämmerli,
HTA Luzern

13:25 Keynotes von:

- > Frank Schwarze
- > PD Dr. Hannes P. Lubich
- > Gian Manetsch, Beate Fiedler
- > Beat Lehmann

14:40 Parallele Diskussionsforen

16:20 Pause

16:45 Präsentationen und Diskussion der Resultate aus
den Praxisforen im Plenum

17:30 Abschluss und Apéro

Public Key Kryptographie

- 1976 lösen Withfield Diffie und Martin Hellman das Problem des Key-Managements mit dem Konzept der Public Key Kryptographie.
→ **Diffie-Hellman**
- 1977 wurde von Ron Rivest, Adi Shamir und Leonard Adelman die erste praktische Realisierung entwickelt.
→ **RSA Algorithmus**

$$\begin{aligned} P \ \& \ Q \ \text{PRIME} \\ N &= PQ \\ ED &\equiv 1 \pmod{(P-1)(Q-1)} \\ C &= M^E \pmod N \\ M &= C^D \pmod N \end{aligned}$$

RSA Algorithm

Public Key Kryptographie II

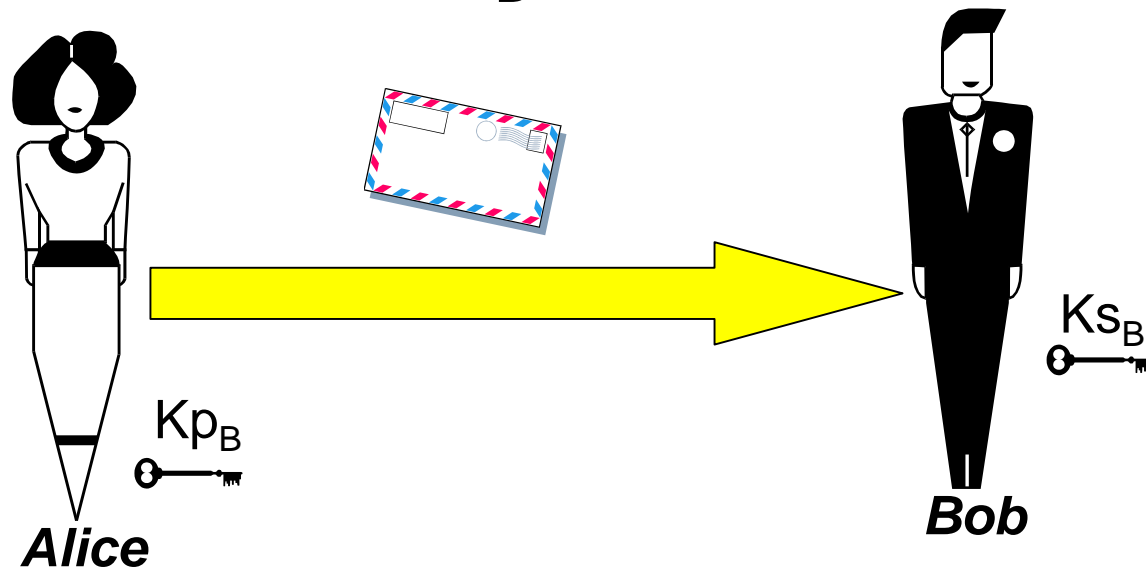
- Asymmetrische Kryptographie erlaubt es **Verschlüsselung** und **Authentizität** (Digitale Signatur) zu gewährleisten.
- Verwendet einen geheimen (K_s) und einen öffentlichen Schlüssel (K_p).
→ **Private & Public Key**
- Schlüssellänge z.B. **1024 Bit**
- Ist langsamer als sym. Verschlüsselung
- Es müssen keine geheimen Schlüssel ausgetauscht werden.

Public Key Kryptographie III

- Der **geheime Schlüssel** (K_s) bleibt beim Eigentümer.
- Der **öffentliche Schlüssel** (K_p) kann in einem öffentlichen Verzeichnis publiziert werden.
- Die Kommunikationspartner beziehen die öffentlichen Schlüssel von einem Verzeichnis einer Trusted Third Party (auch CA genannt).
- **Trusted Third Party** (= TTP) und **Certified Authority** (= CA) verwalten öffentliche Schlüssel.

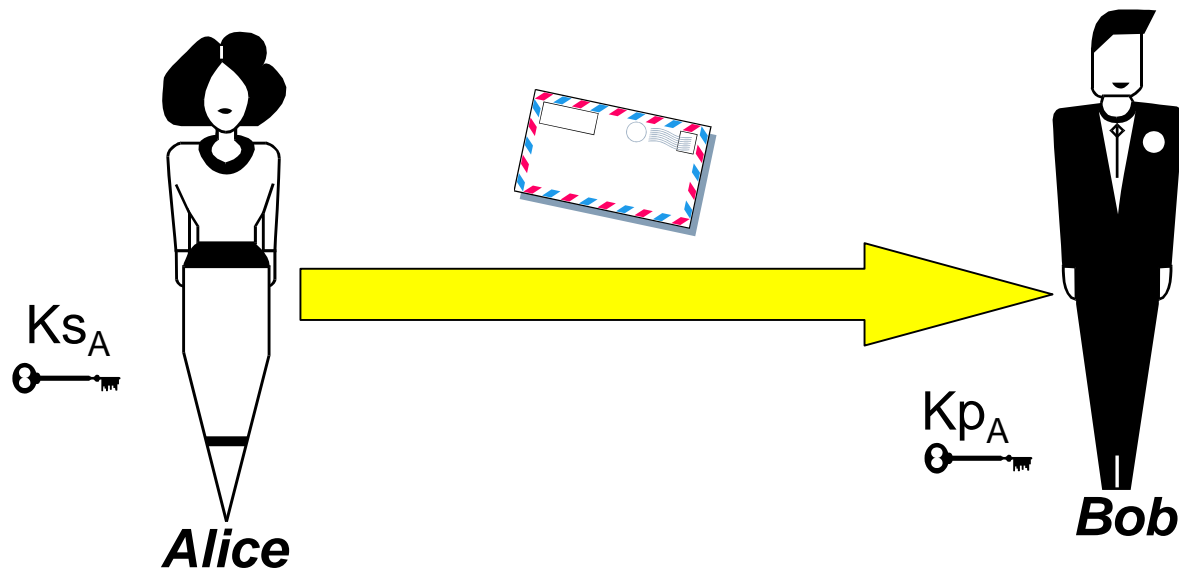
Asymmetrische Verschlüsselung (privater und öffentlicher Schlüssel)

- **Alice verschlüsselt** die **Nachricht** mit dem **öffentlichen Schlüssel** von Bob (K_{p_B}).
- Nur **Bob** kann die **Nachricht mit** seinem **privaten Schlüssel** (K_{s_B}) **entschlüsseln**.



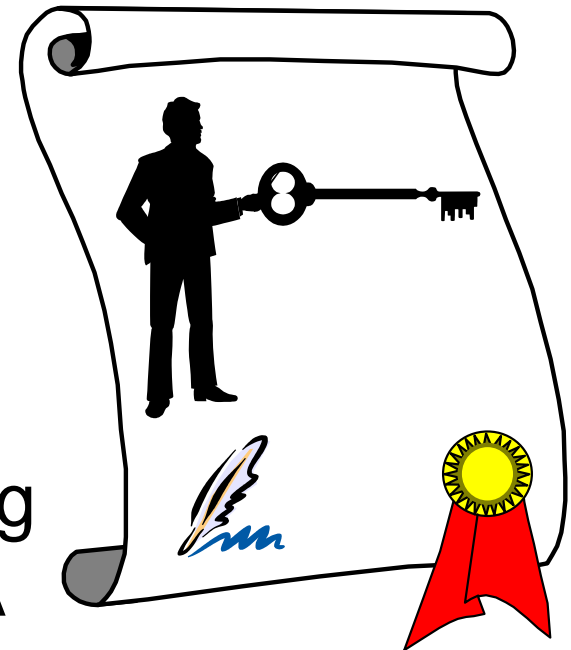
Verbindlichkeit durch Digitale Signatur

- **Alice unterschreibt die Nachricht mit ihrem privaten Schlüssel** (K_{s_A}).
- **Bob (Jedermann) überprüft die Unterschrift mit dem öffentlichen Schlüssel** von Alice (K_{p_A}).



X.509 Zertifikate

- Ein Zertifikat stellt eine eindeutige **Verbindung zwischen** einem **Subjekt** (Person, Firma, Server, ...) und seinem **Public Key** (öffentlicher Schlüssel) her.
- Die **Richtigkeit** dieser Zuordnung wird durch den Herausgeber (CA = Certificate Authority) des Zertifikats mit seiner digitalen Unterschrift **bestätigt**.



>> Dank

Wir danken den Sponsoren!

UNISYS
imagine it. done.

HIS | IT-SECURITY
WE MANAGE IT RISKS

security
zone 06
PLATTFORM FÜR INFORMATIONSSICHERHEIT

PortWise
Secure Application Access. Anywhere.

ca



Biometric Security AG

DIE POST 

tetrade.
we Integrate IT

 **Sun.**
microsystems

>> Apéro

Bitte bleiben Sie noch kurz sitzen, damit die Rückwand geöffnet werden kann!