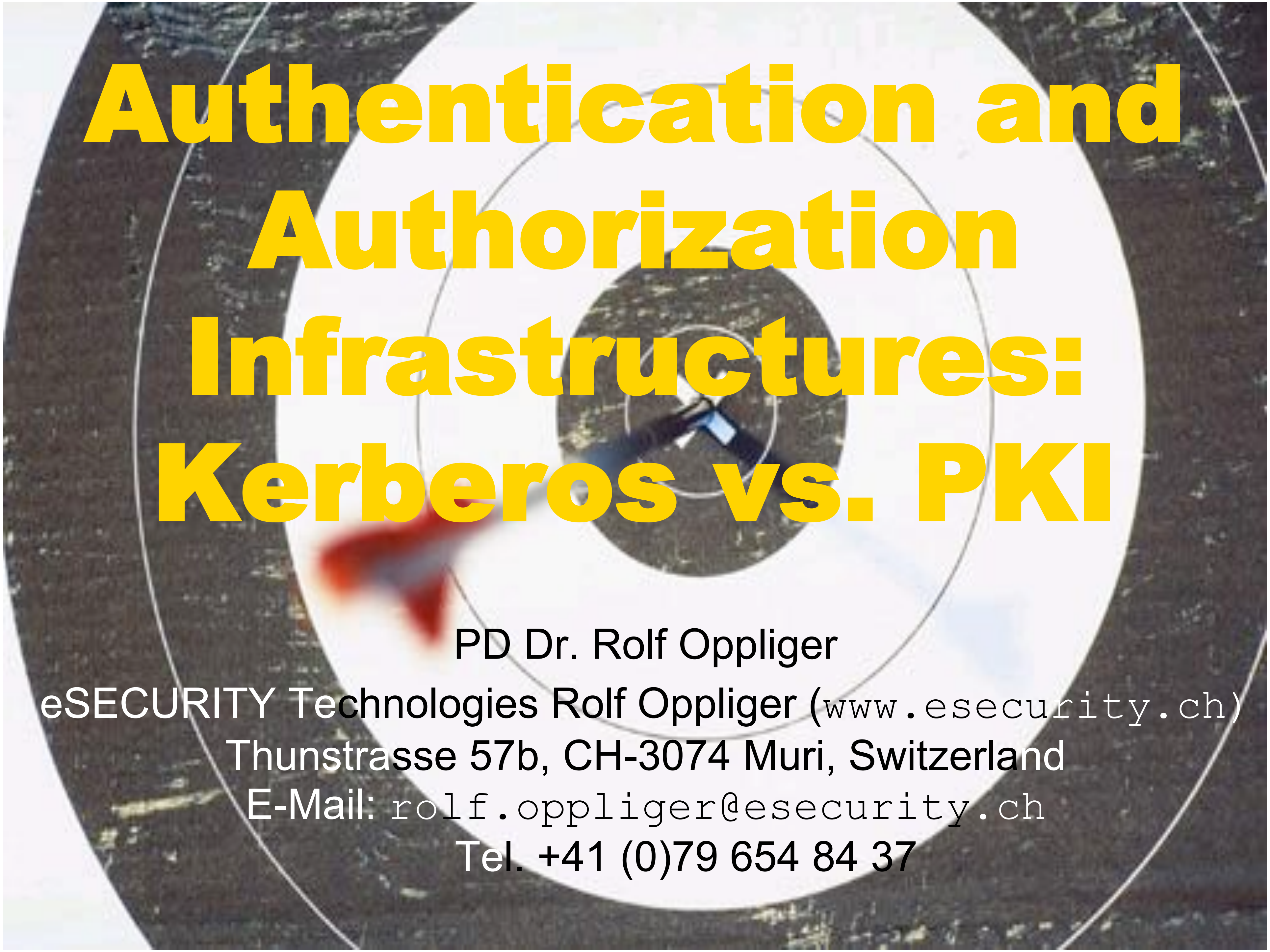


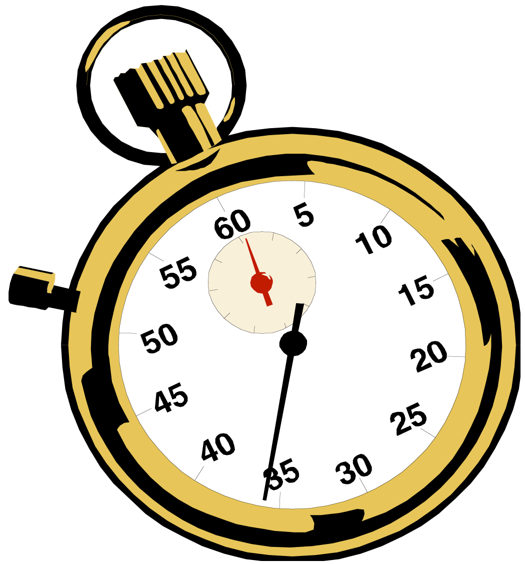
Authentication and Authorization Infrastructures: Kerberos vs. PKI

PD Dr. Rolf Oppliger
eSECURITY Technologies Rolf Oppliger (www.esecurity.ch)
Thunstrasse 57b, CH-3074 Muri, Switzerland
E-Mail: rolf.oppliger@esecurity.ch
Tel. +41 (0)79 654 84 37

eSECURITY Technologies Rolf Oppliger

Agenda

1. Introduction
2. Cryptographic Techniques
3. Kerberos
4. Kerberos-based AAIs
5. PKI
6. PKI-based AAIs
7. Comparison
8. Conclusions and Outlook

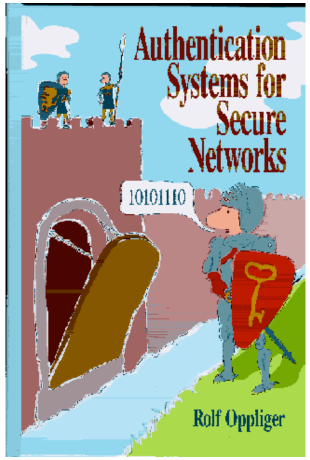


References (Cryptography)

- N.I. Koblitz. **A Course in Number Theory and Cryptography** (2nd Edition). Springer-Verlag, Berlin, 1994, ISBN 0387942939
- D.R. Stinson. **Cryptography: Theory and Praxis**. CRC Press, Boca Raton, FL, 1995, ISBN 0849385210
- B. Schneier. **Applied Cryptography: Protocols, Algorithms, and Source Code in C** (2nd Edition). John Wiley & Sons, New York, NY, 1996, ISBN 0471117099
- A.J. Menezes, P.C. van Oorschot and S.A. Vanstone. **Handbook of Applied Cryptography**. CRC Press, Boca Raton, FL, 1997, ISBN 0849385237 (PDF files available at `http://cacr.math.uwaterloo.ca/hac/`)

eSECURITY
Technologies Rolf Oppliger

References (Kerberos and Kerberos-based AAIs)



- R. Oppliger. **Authentication Systems for Secure Net-works,** Artech House, Norwood, MA, 1996, ISBN 0890065101
- B. Tung. **Kerberos: A Network Authentication System**. Addison-Wesley, Reading, MA, 1999, ISBN 0201379244
- P. Ashley and M. Vandenwauver. **Practical Intranet Security: Overview of the State of the Art and Available Technologies**. Kluwer Academic Press, 1999, ISBN 0792383540

References (PKI and PKI-based AAIs 1/2)

- S. Garfinkel and E.H. Spafford. **Web Security & Commerce**. O'Reilly & Associates, Sebastopol, CA, 1996, ISBN 1565922697
- W. Stallings. **Cryptography and Network Security: Principles and Practice** (2nd Edition). Prentice Hall, Upper Saddle River, NJ,1997, ISBN 0138690170
- W. Ford and M. Baum. **Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption**. Prentice Hall, Upper Saddle River, NJ,1997, ISBN 0134763424
- J. Feghhi, J. Feghhi and P. Williams, **Digital Certificates: Applied Internet Security**, Addison-Wesely, Reading, MA, 1999, ISBN 0201309807

References (PKI and PKI-based AAIs 2/2)

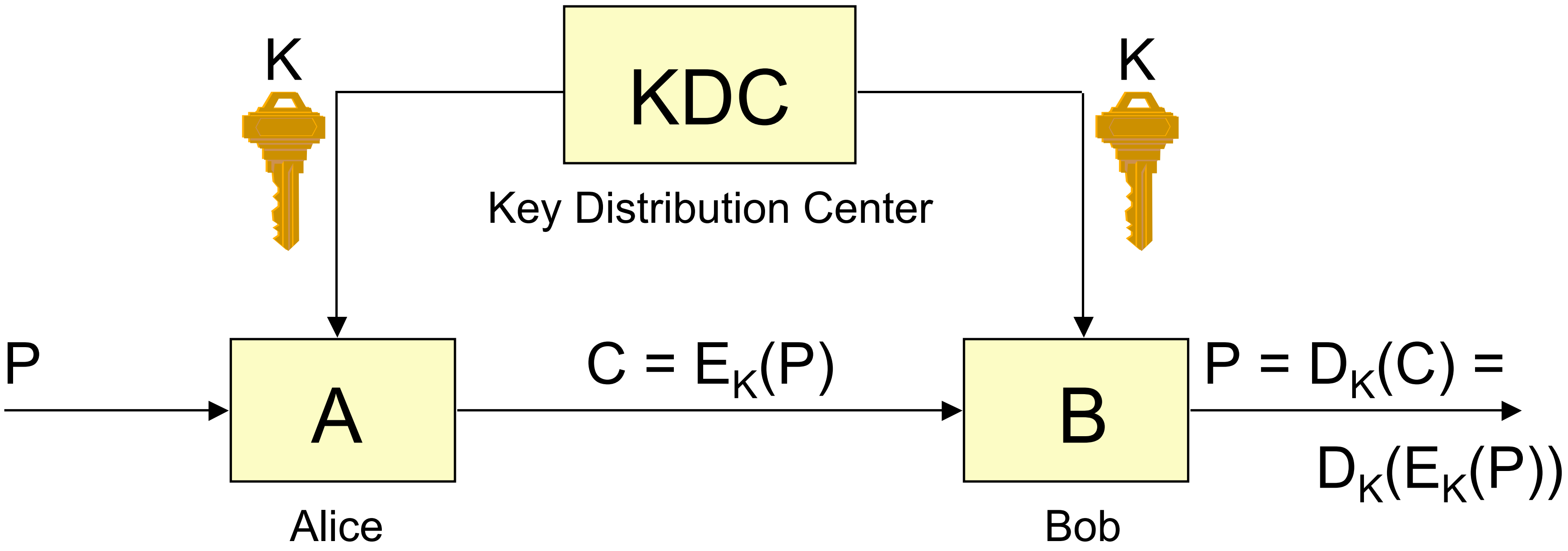
- C. Adams and S. Lloyd. **Understanding the Public-Key Infrastructure**. New Riders Publishing, 1999, ISBN 157870166X
- T. Austin, D. Huaman and T.W. Austin. **Public Key Infra-structure Essentials,** John Wiley & Sons, New York, NY, 2000, ISBN 0471353809
- S.A. Brands. **Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy**. MIT Press, 2000, ISBN 0262024918
- R. Housley and T. Polk. **Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure**. John Wiley & Sons, New York, NY, 2001, ISBN 0471397024

Introduction

- According to the „Internet Security Glossary" (RFC 2828)
  - **Authentication** refers to the process of verifying an identity claimed for a system entity
  - **Authorization** refers the process of granting a right or permission to a system entity to access a system resource
- An **authentication and authorization infrastructure (AAI)** is an infrastructure that provides support for authentication and authorization
- AAIs are getting increasingly important in todays networked and distributed environments
- Development roots:
  - Kerberos authentication system
  - Public key infrastructures (PKIs)

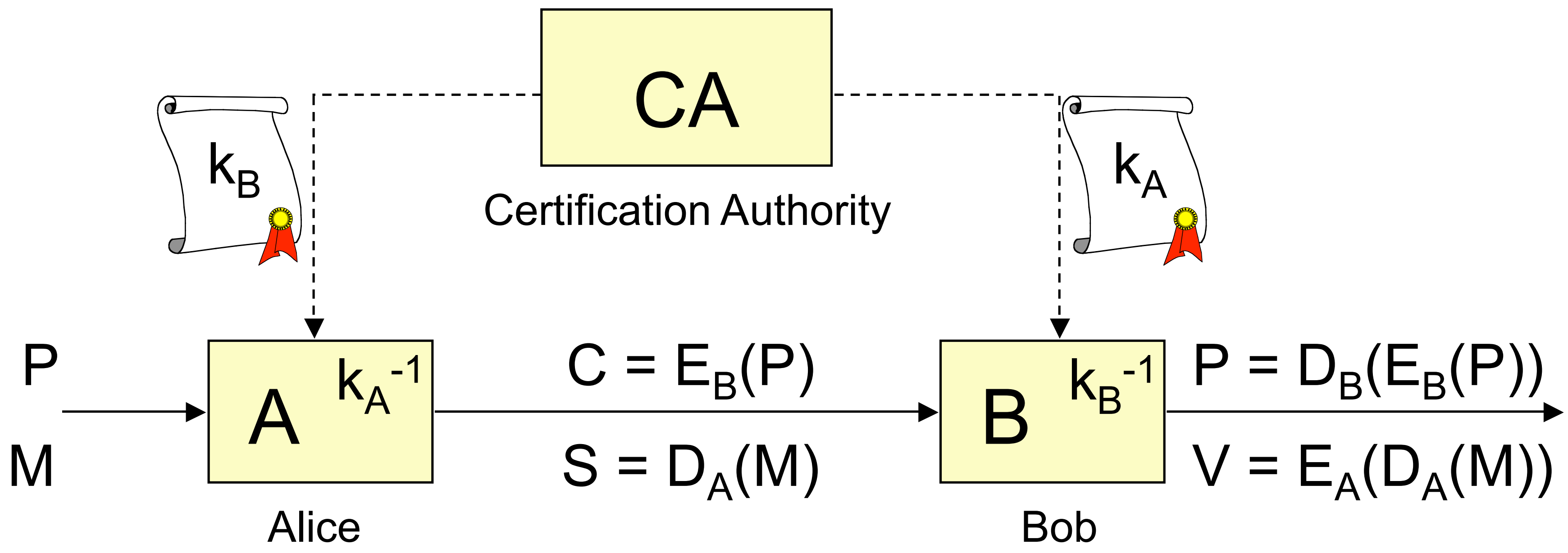
Cryptographic Techniques 1/4

- Secret key (symmetric) cryptography
- Algorithms: DES, 3DES, AES (Rijndael), IDEA, Blowfish, RC4, ...



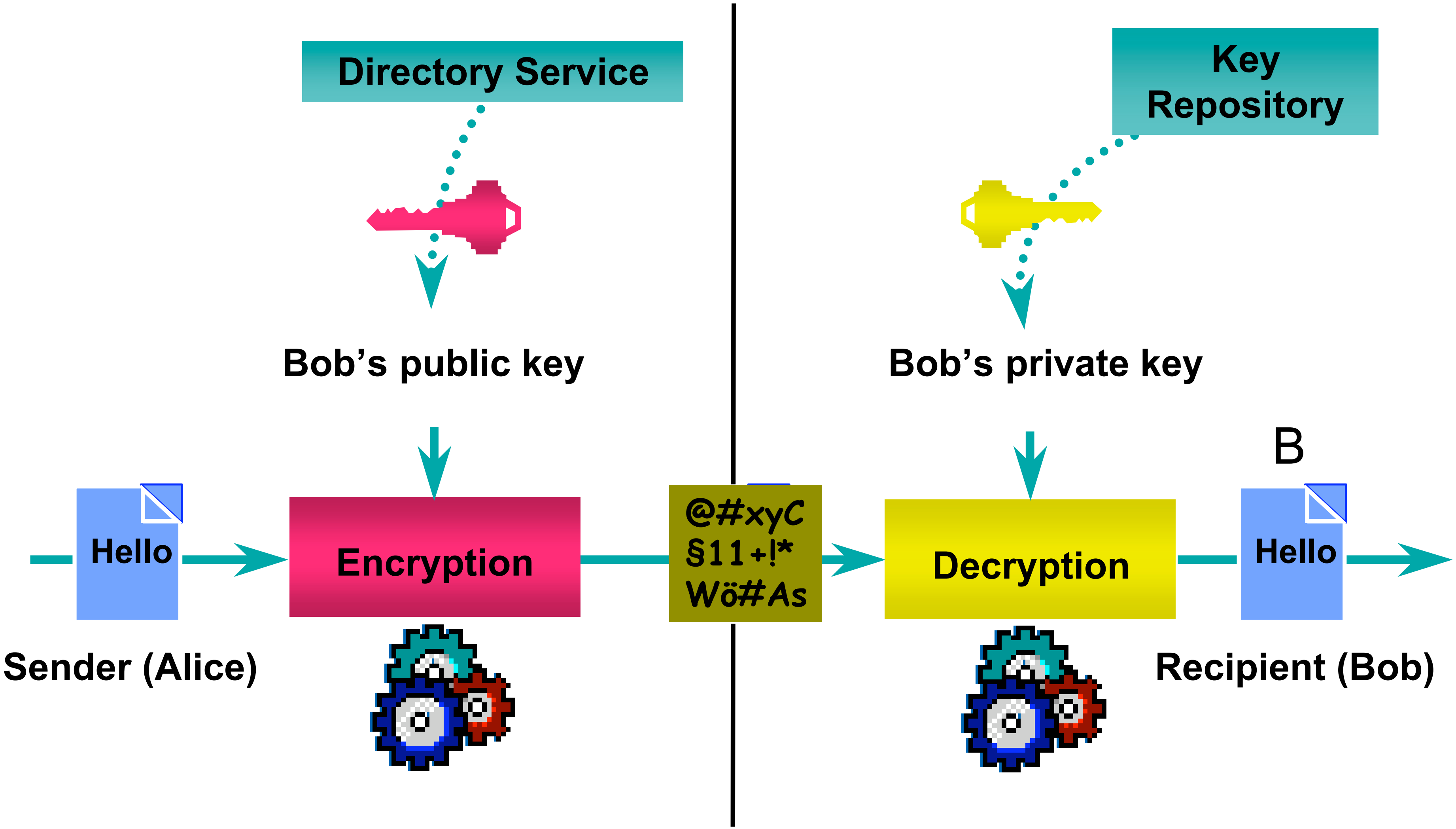
Cryptographic Techniques 2/4

- Public key (asymmetric) cryptography
- Algorithms: RSA, Diffie-Hellman, ElGamal, DSS, ECC, ...

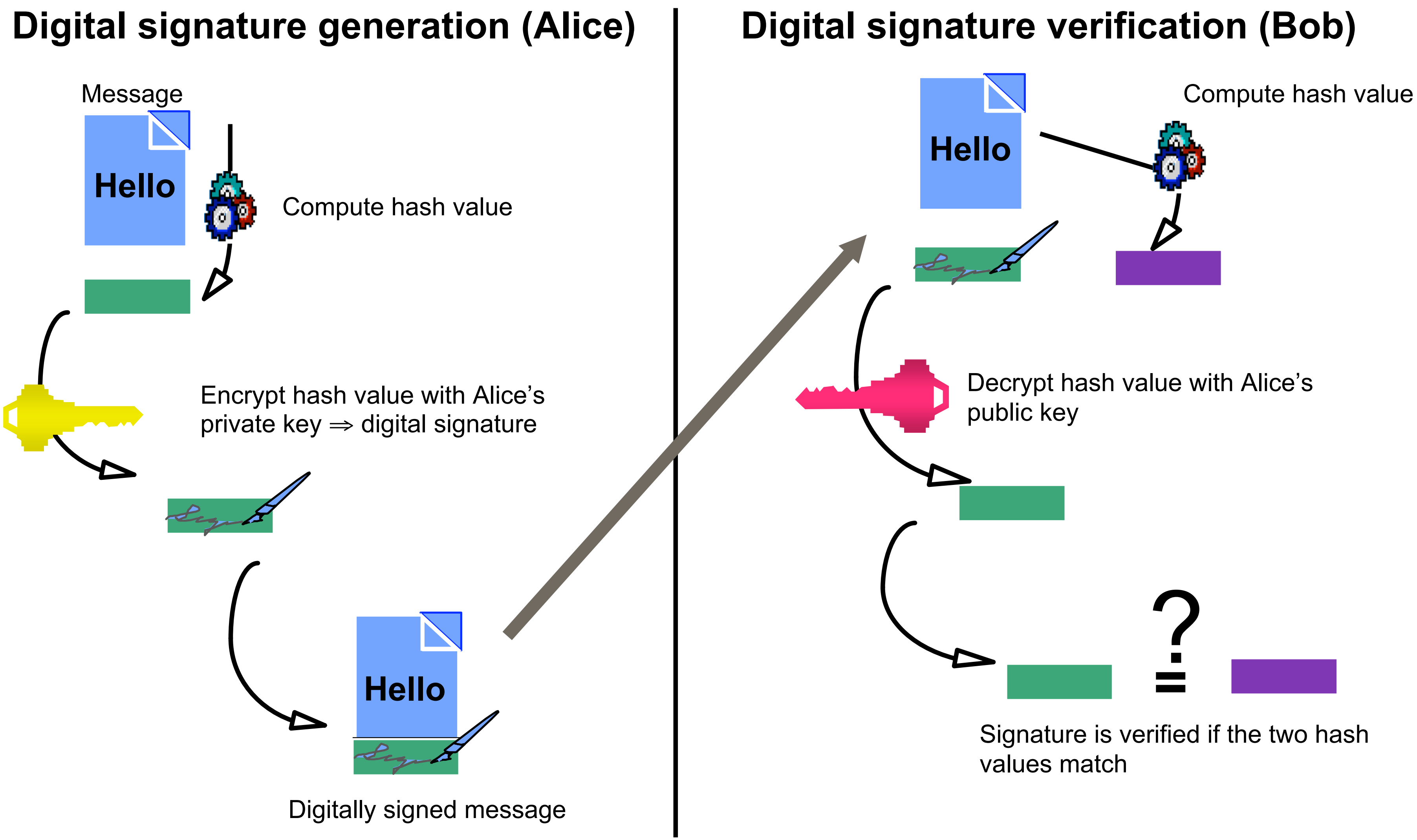


eSECURITY
Technologies Rolf Oppliger

Cryptographic Techniques 3/4



Cryptographic Techniques 4/4



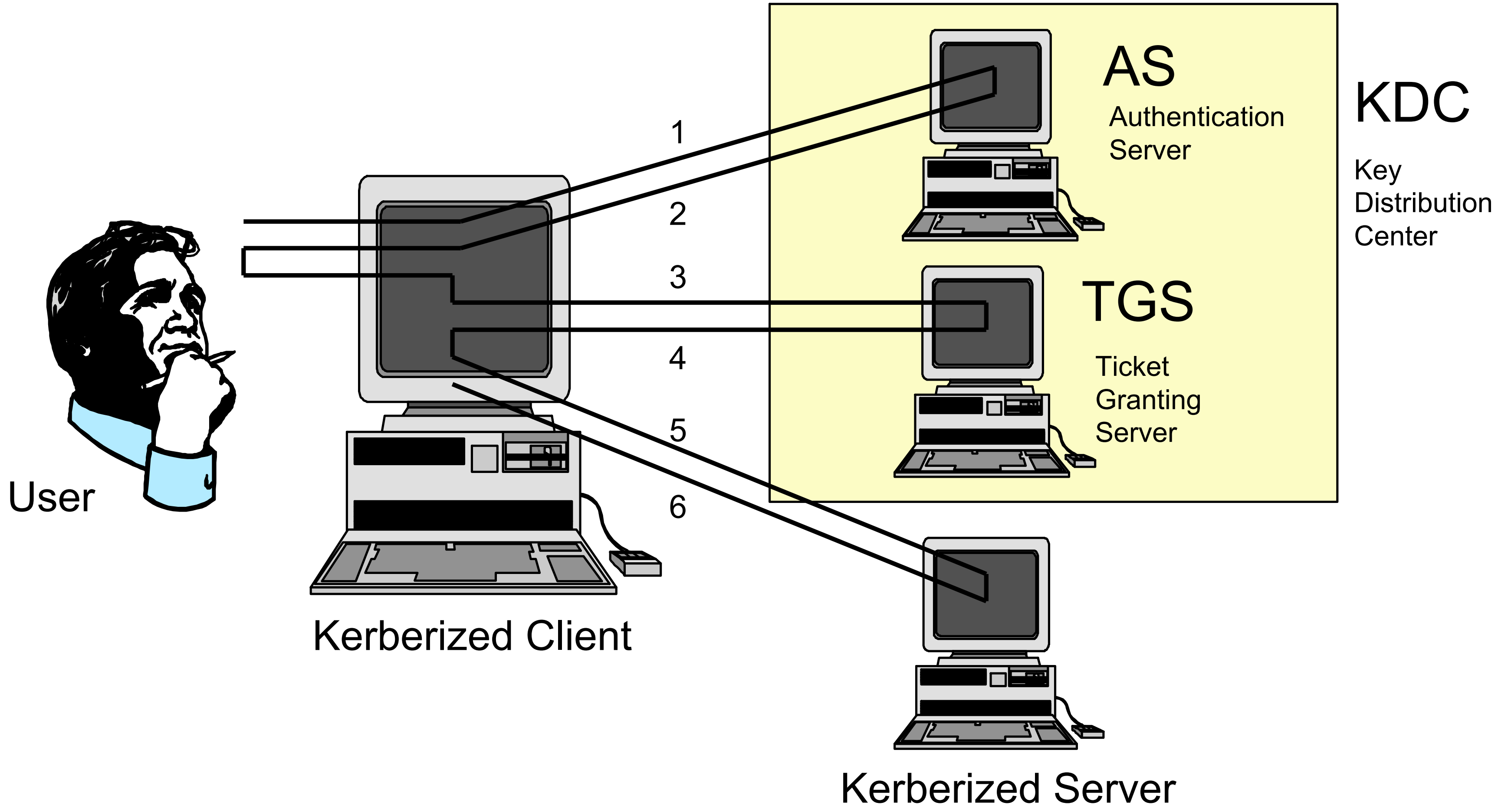
3. Kerberos 1/6

- The **Kerberos authentication system** was developed at MIT as part of the Athena project
- Since version 4, the MIT reference implementation is publicly and freely available
- In addition, there are many commercial Kerberos implementations
- Kerberos version 5 is specified in RFC 1510 and submitted to the Internet standards track
- The IETF Security Area hosts a Kerberos WG (KRB-WG)

Kerberos 2/6

- Design requirements:
  - Single sign-on (i.e., the password is used only once for the initial login sequence)
  - Passwords are not transmitted in the clear (i.e., the system is resistant against password sniffing attacks)
  - No use of public key cryptography
- In the Kerberos architecture, every realm (security domain) must operate a physically secure environment that hosts a key distribution center (KDC)
- The KDC maintains a database with a secret key K_p for every principal P

Kerberos 3/6


AS
Authentication Server
KDC
Key Distribution Center
1
2
3
4
5
6
TGS
Ticket Granting Server
User
Kerberized Client
Kerberized Server

Kerberos 4/6

1) $C \longrightarrow AS : U, TGS, L_1, N_1$

2) $AS \longrightarrow C : U, T_{c,tgs}, \{TGS, K, T_{start}, T_{expire}, N_1\}K_u$

3) $C \longrightarrow TGS : S, L_2, N_2, T_{c,tgs}, A_{c,tgs}$

4) $TGS \longrightarrow C : U, T_{c,s}, \{S, K', T'_{start}, T'_{expire}, N_2\}K$

5) $C \longrightarrow S : T_{c,s}, A_{c,s}$

6) $S \longrightarrow C : \{T'\}K'$

$T_{c,tgs} = \{U, C, TGS, K, T_{start}, T_{expire}\}K_{tgs}$ $A_{c,tgs} = \{C, T\}K$

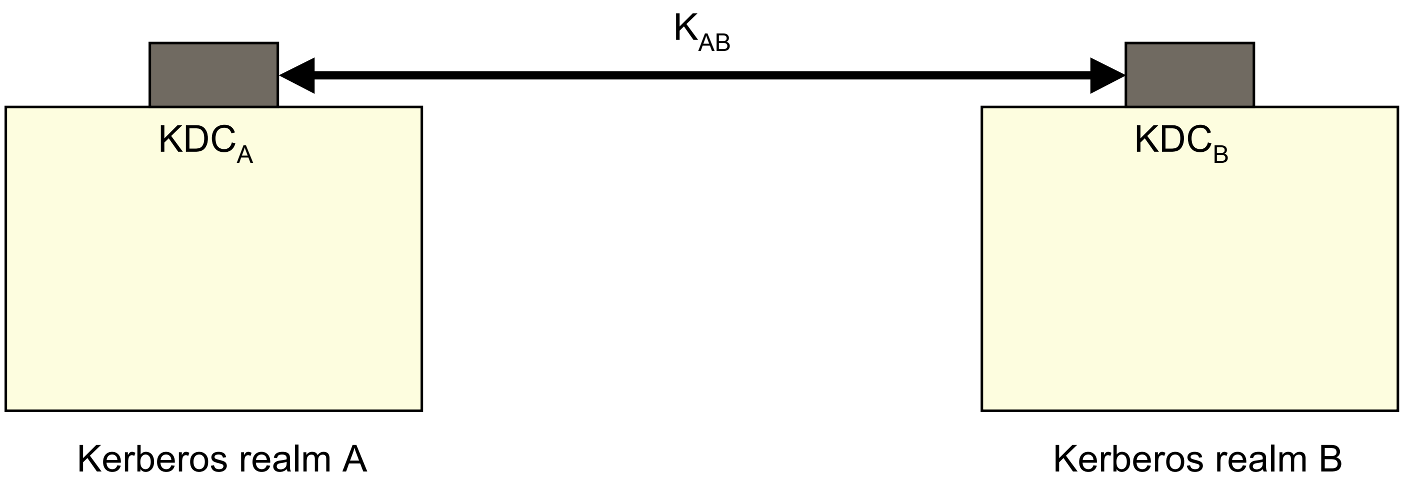
$T_{c,s} = \{U, C, S, K', T'_{start}, T'_{expire}\}K_s$ $A_{c,s} = \{C, T'\}K'$

Kerberos 5/6

- Major drawbacks and shortcomings:
  - The KDC must be completely trusted (“big brother”-property)
  - Verifiable password guessing attacks
- Any proposal to overcome these drawbacks and short-comings must use public key cryptography
- Proposal to overcome the “big brother”-property:
  - Yaksha (Ganesan et al.)
  - Public key extensions for Kerberos (IETF KRB-WG)
- Proposals to protect against verifiable password guessing attacks:
  - Encrypted Key Exchange (EKE)
  - Similar proposals by Gong et al.

Kerberos 6/6

- A major obstacle for the large-scale deployment of the Kerberos system is inter-realm authentication
- Kerberos inter-realm authentication requires mutual trust between the two participating KDCs (does not scale)



4. Kerberos-based AAIs 1/3

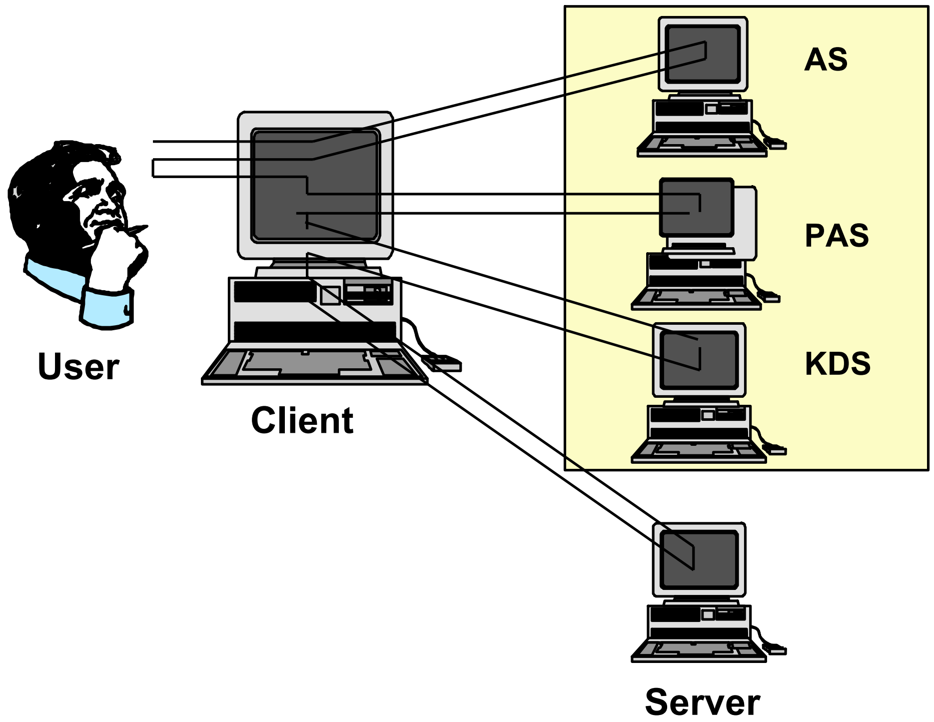
- The original Kerberos authentication system does not address authorization (i.e., authorization is left to the server)
- Consequently, some AAIs have been developed
  - that make use of the Kerberos system for authentication and
  - that extend the basic Kerberos model with regard to authori-zation (resulting in Kerberos-based AAIs)
- Exemplary Kerberos-based AAIs:
  - A Secure European System for Applications in a Multi-vendor Environment (**SESAME**) developed by Bull, ICL, and SSE
  - Distributed Computing Environment (**DCE**) promoted by the Open Group (formerly known as OSF)
  - Microsoft Windows 2000
  - ...

Kerberos-based AAIs 2/3

- SESAME is based on
  - a Kerberos V5 authentication service
  - an ECMA-based authorization and access control service
- In short, SESAME uses **privilege attribute certificates (PACs)** to grant privileges to entities
- A PAC
  - is a digitally signed statement about the privileges of an entity
  - is issued by a privilege attribute server (PAS)
  - is conceptually similar to an attribute certificate (as discussed later)
- The Open Group‘s DCE and Microsoft‘s Windows 2000 use similar concepts

Kerberos-based AAIs 3/3

- Further information about the SESAME project and products is available at
  `https://www.cosic.esat.kuleuven.ac.be/sesame/`



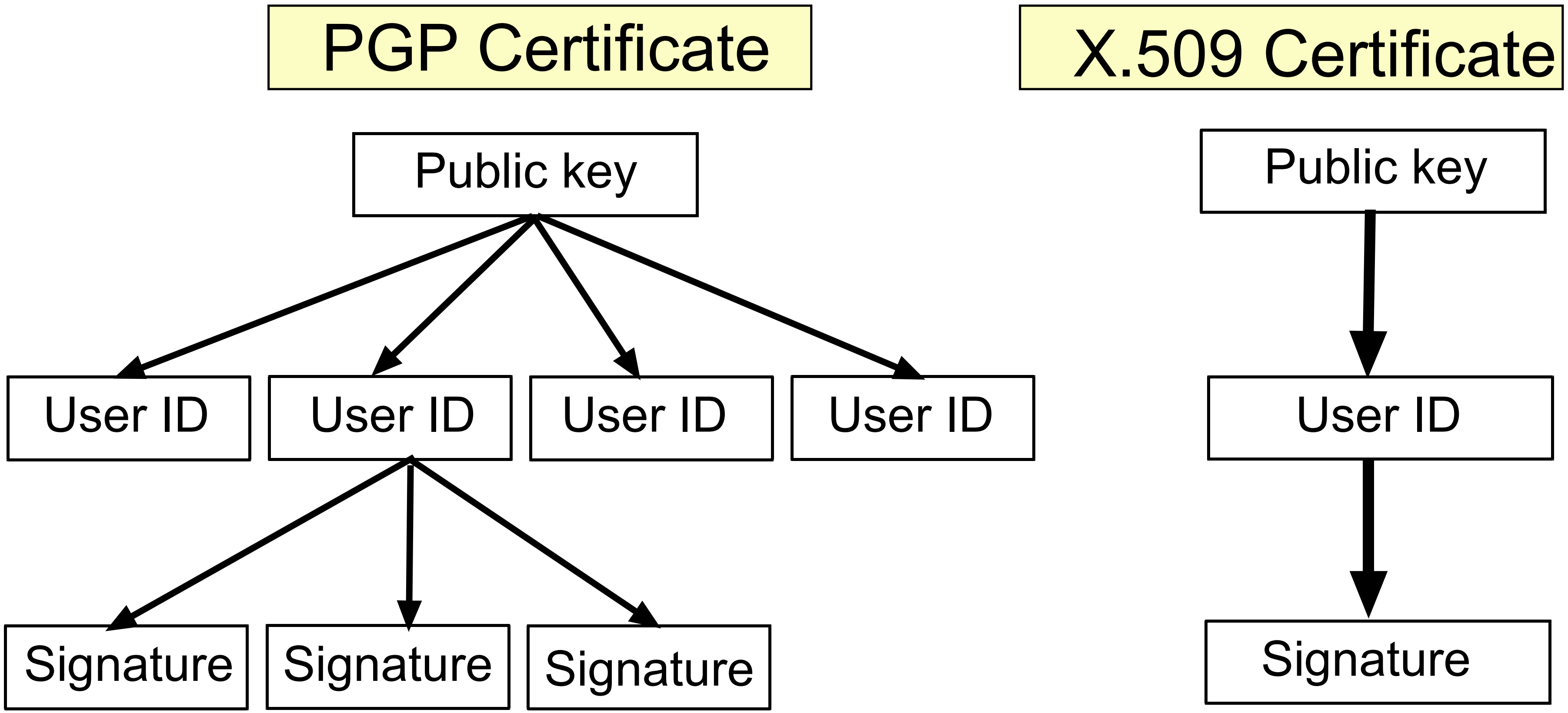
5. PKI 1/9

- **Public key certificates** are required to protect the authenticity and integrity of public keys (and to protect against „man-in-the-middle“-attacks)
- **ITU-T X.509** version 3 is the certificate format of choice for most applications
- Nevertheless, ITU-T X.509 version 3 still requires a profiling process for a specific application environment (e.g., IETF PKIX WG for the Internet)
- The IETF SPKI WG is developing and specifying an alternative certificate format and trust model for the Internet application environment

Version
Certificate serial number
Signature algorithm identifier
Issuer
Validity period
Subject
Subject public key information
[Issuer unique information]
[Subject unique information]
[Extensions]
CA's digital signature

PKI 2/9

- Alternative formats for public key certificates:



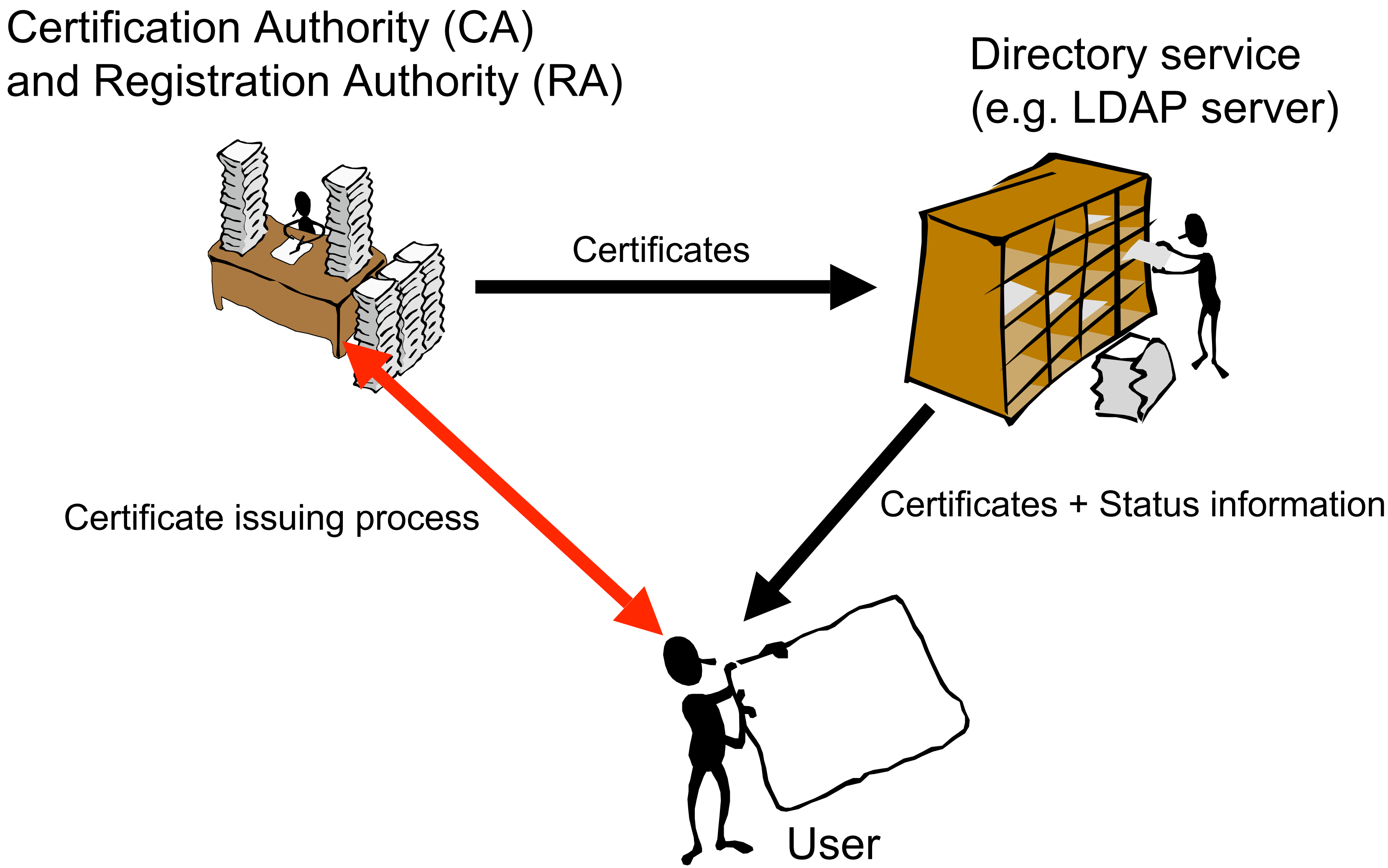
PKI 3/9

- The certification process can be iterated (arbitrarily often), meaning that a CA‘s certificate can be certified by another CA (resulting in a **certificate chain**)
- A certificate chain must be verified until a root CA is reached
- Note, however, that a certificate can only be trusted iff
  - every certificate in the chain is successfully verified
  - every CA in the certificate chain can be trusted
- In practice, certificate chains are short and seldom verified for trustworthiness
- Also, the concept of **cross-certification** is of low practical value and seldom used between certification service pro-viders

PKI 4/9

- According to RFC 2828 „Internet Security Glossary“ a **public key infrastructure (PKI)** is „a system of CAs [...] that perform some set of
  - certificate management,
  - archive management,
  - key management, and
  - token management functions
- for a community of users in an application of asymmetric cryptography.“
- Major applications:
  - SSL/TLS (and WTLS)
  - S/MIME
  - IPSec and virtual private networking

PKI 5/9


Certification Authority (CA)
and Registration Authority (RA)
Directory service
(e.g. LDAP server)
Certificates
Certificate issuing process
Certificates + Status information
User

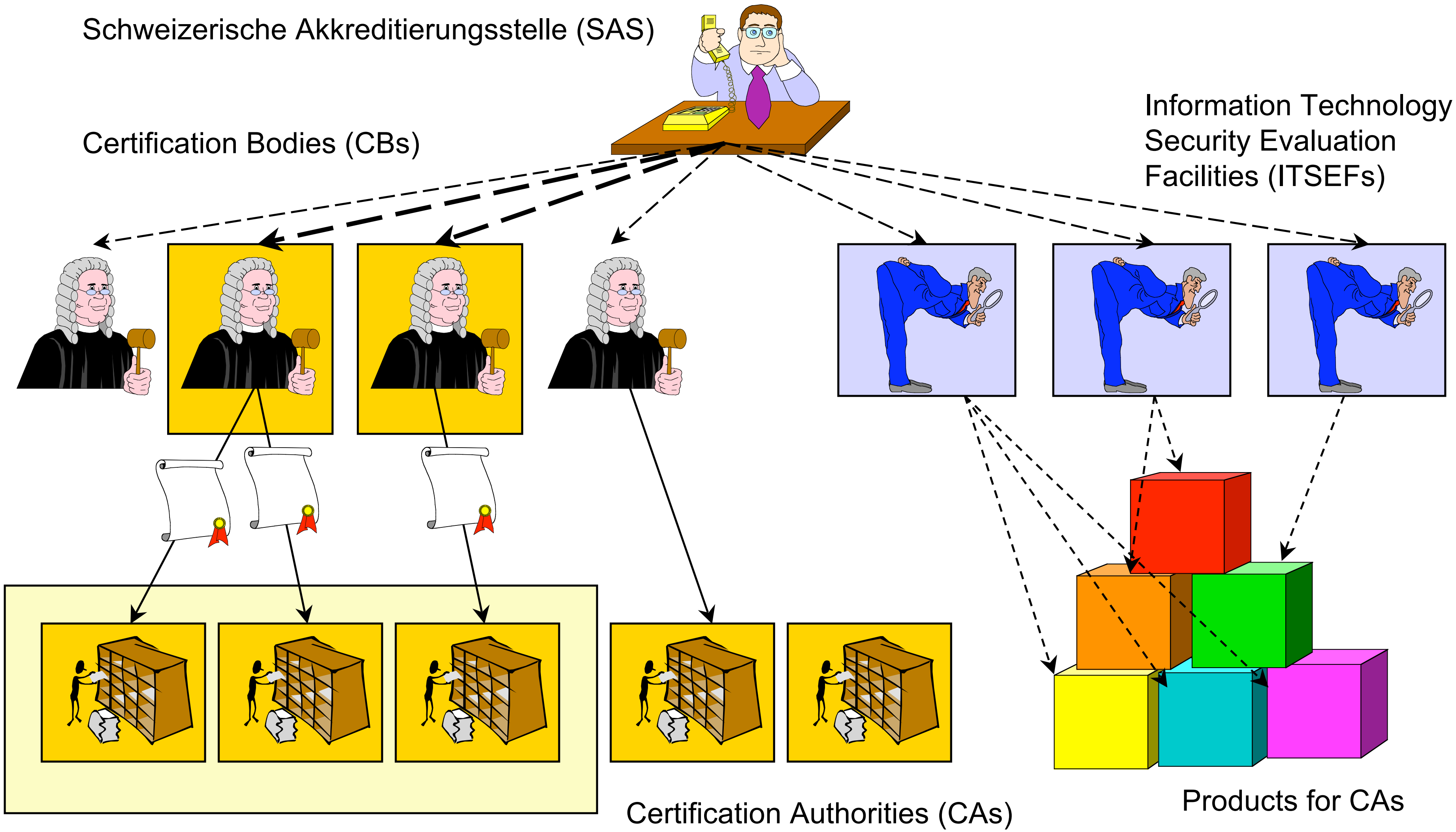
PKI 6/9

- Approaches to provide status information:
  - Certificate Revocation Lists (CRLs)
  - Delta-CRLs
  - Online Certificate Status Protocol (OCSP)
  - Certificate Revocation System (CRS)
  - Certificate Revocation Trees (CRTs)
  - ...
- Unfortunately, the possibility to **revoke certificates** makes it necessary to operate online components (e.g., OCSP servers)
- Furthermore, the possibility to **suspend certificates** makes things even more complicate

PKI 7/9

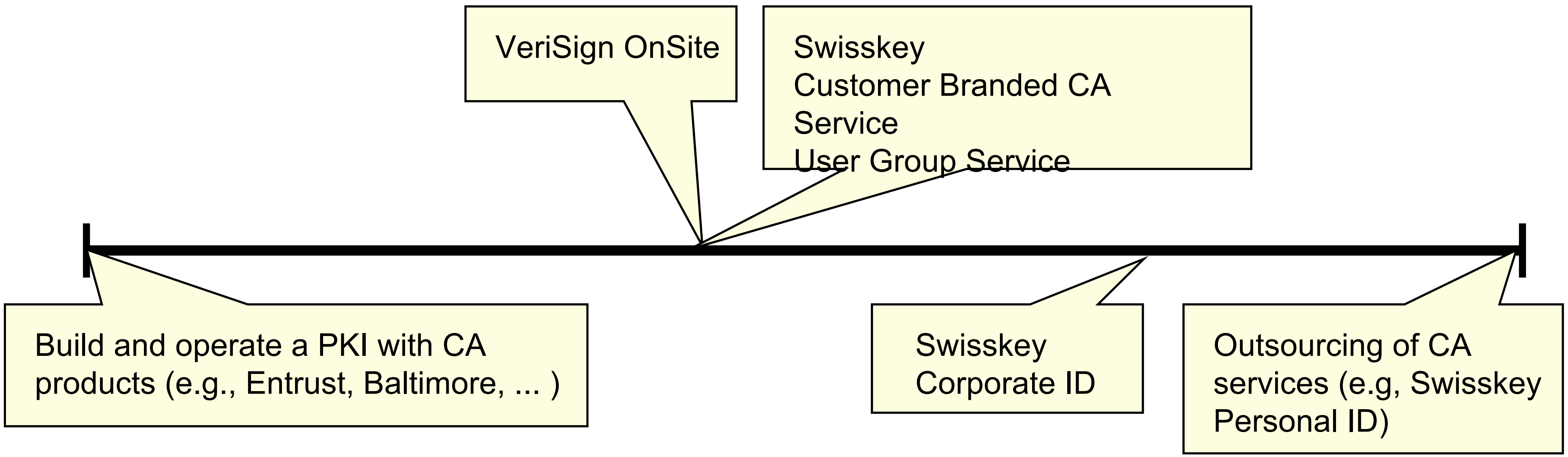
- Legislation for digital signatures and corresponding PKIs is a difficult and very challenging task
- In Switzerland, a „Verordnung über Dienste der elektronischen Zertifizierung“ (**ZertDV**) was put in place on May 1, 2000
- The ZertDV will be replaced by a „Bundesgesetzes über die elektronische Signatur“ (**BGES**)
- In either case, the criteria against which certification service providers (i.e., CAs) would be evaluated and certified are not clear and still under construction
- This is equally true for the **European Electronic Signature Standardization Initiative (EESSI)**

PKI 8/9


Schweizerische Akkreditierungsstelle (SAS)
Certification Bodies (CBs)
Information Technology
Security Evaluation
Facilities (ITSEFs)
Certification Authorities (CAs)
Products for CAs

PKI 9/9

- Today, many companies and organizations are in the process of deciding whether they want to build and operate a PKI and provide corresponding CA services of their own, or whether they want to outsource the corresponding services to commercial service providers (e.g. VeriSign, Swisskey, ...)
- There is a whole range of possibilities



6. PKI-based AAIs 1/5

„On the Internet, nobody cares you‘re a dog - unless you can‘t pay your debts.“

"On the Internet, nobody knows you're a dog."

PKI-based AAIs 2/5

- E-commerce and e-business applications generally need a possibility to authorize entities (in addition to authentication)
- Consequently, some type of **Privilege Management Infrastructure (PMI)** must be put in place
- PMI is the next-generation buzzword in the PKI industry
- A PMI is conceptually similar to a PKI-based AAI
- There are several possibilities to implement PMIs and PKI-based AAIs:
  - Encode authorization information in public key certificates (e.g., using ITU-T X.509 v3 extension fields)
  - Use of attribute certificates
  - Manage authorization information in a database management system (DBMS)

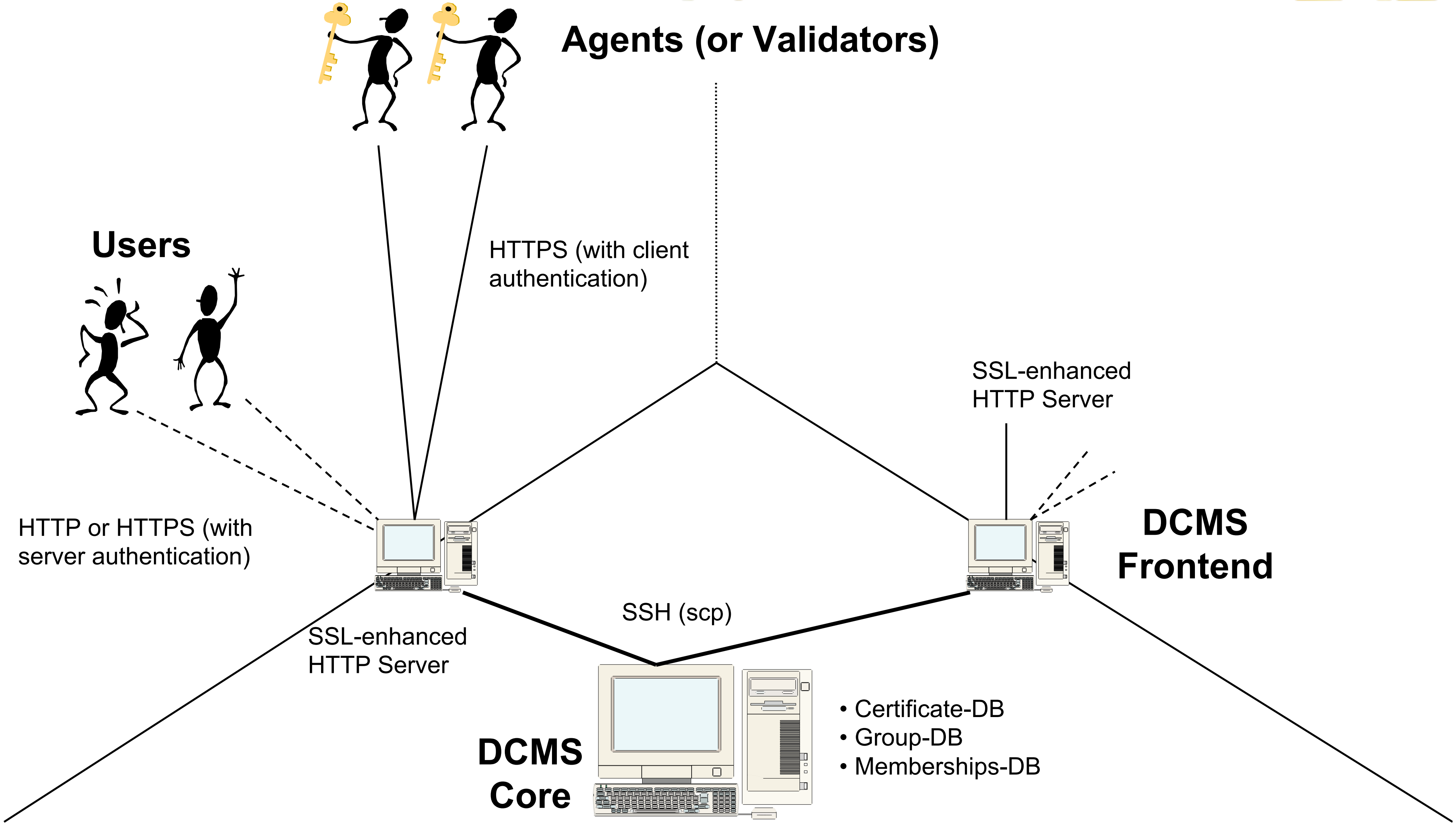
PKI-based AAIs 3/5

- ITU-T **X.509 v3 extension fields** should only be used to carry authorization information that is stable and constant over time
- Otherwise, the use of **attribute certificates (ACs)** is advan-tageous and should be the preferred option
- An AC
  - is conceptually similar to a PAC
  - is issued and digitally signed by an attribute authority (AA)
- Unfortunately, ACs are not supported by many applications and application protocols (e.g., SSL/TLS)
- A **DBMS** can be used to link authorization information to public key certificates, and to implement a PMI accordingly

PKI-based AAIs 4/5

- For example, a **distributed certificate management system (DCMS)** was proposed and prototyped by the Swiss Federal Strategy Unit for Information Technology (FSUIT)
- The DCMS uses a DBMS to match public key certificates to group memberships (and to „simulate" the functionality of ACs accordingly)
- The group membership information can be used to implement role-based access controls
- The authentication part of the DCMS is similar in spirit and provides comparable services to VeriSign OnSite and the Swisskey Customer Branded CA service

PKI-based AAIs 5/5



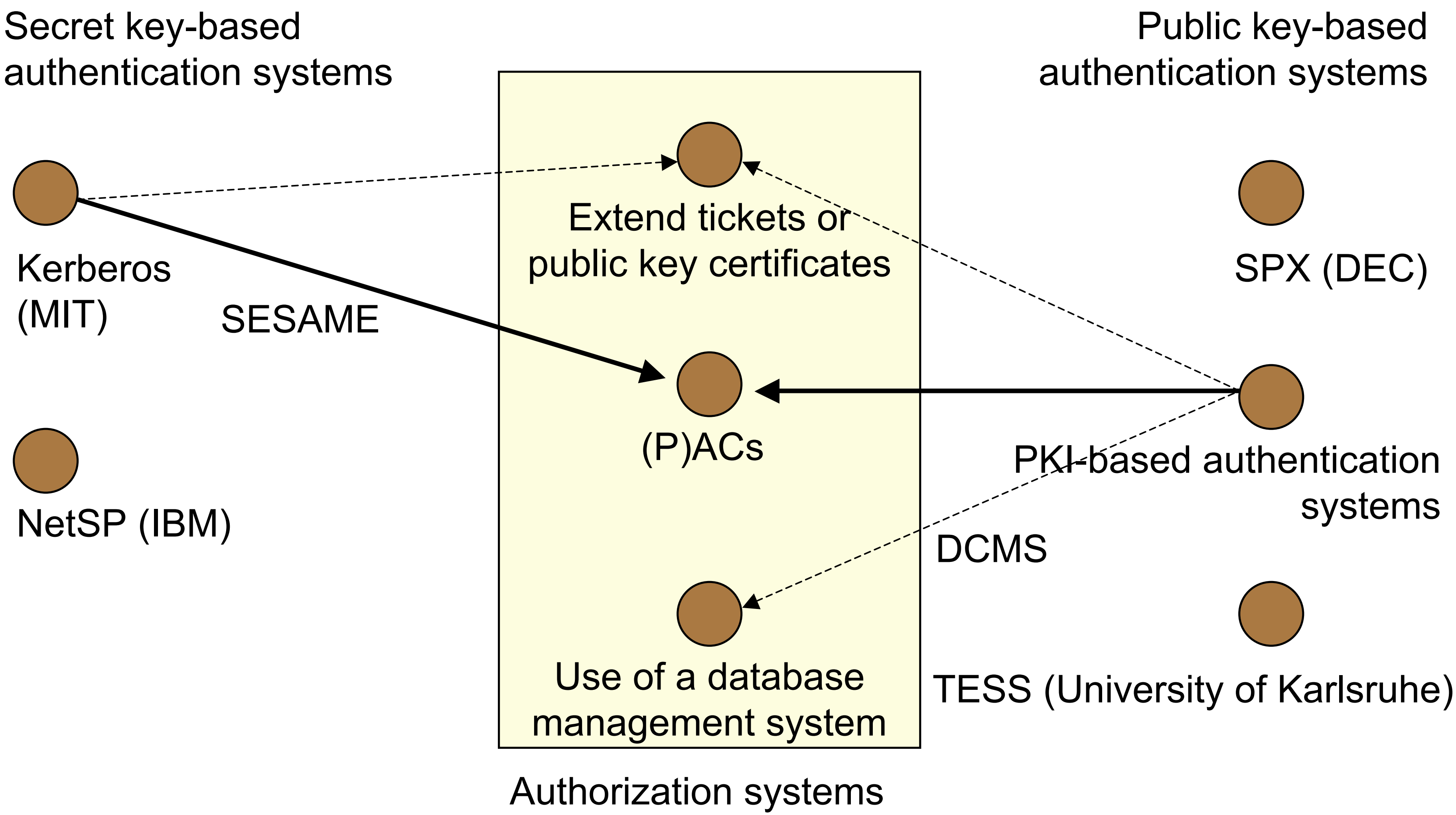
7. Comparison

	Kerberos-based AAIs	PKI-based AAIs
Security	+	+
Non-repudiation	--	++
Trust requirements	-	+
Complexity	-	o
Scalability	--	+
Interoperability	--	-
Application modifications	--	-
Vendor support	o	+
Future perspectives	-	+

8. Conclusions and Outlook 1/2

- Both Kerberos- and PKI-based AAIs are well suited to meet the requirements of contemporary and future applications
- At first sight, the technologies look fundamentally different
- However, the differences are mainly caused by authentication
- With regard to authorization, the technologies are similar in spirit and use comparable constructs (i.e., (P)ACs)
- There is a possibility that the technologies converge in the long term
- In the short- and medium-term, however, it is possible and very likely that we will see different (and not interoperable) AAIs

Conclusions and Outlook 2/2



Query and Answers