ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

Cryptography

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe
Freiburg

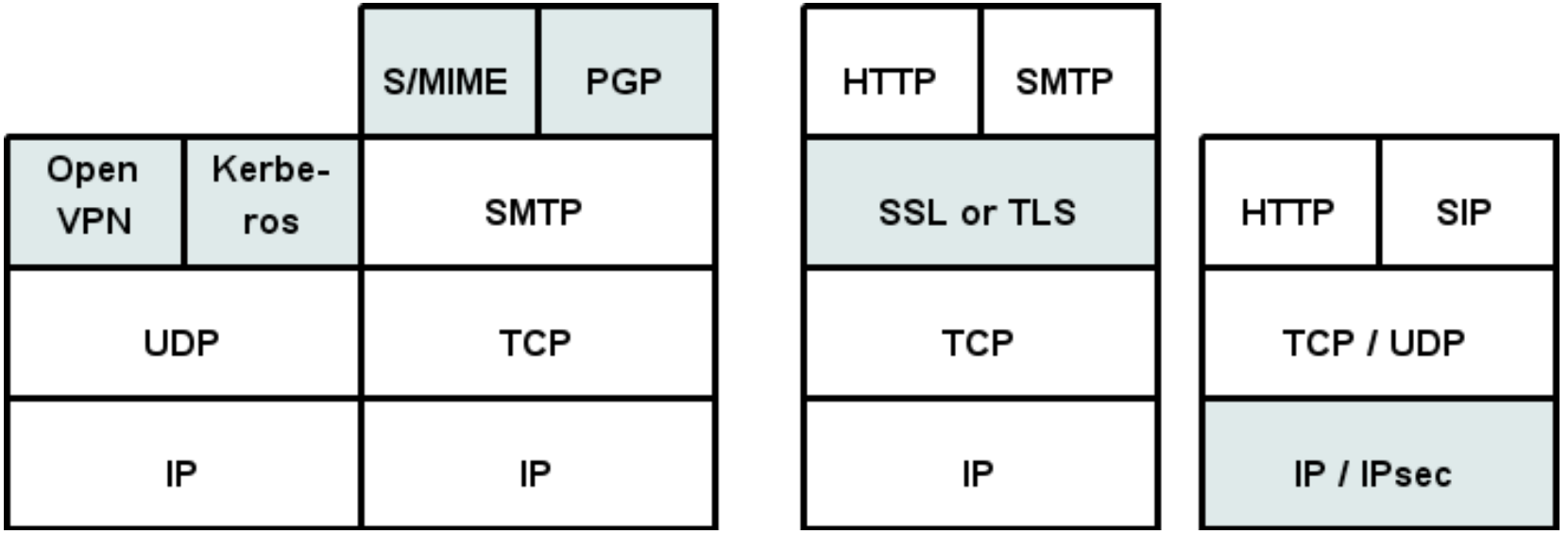
IIF
INSTITUT FÜR
INFORMATIK
FREIBURG

Organization

- I. Data and voice communication in IP networks
- **II. Security issues in networking**
- III. Digital telephony networks and voice over IP

Network Security on Different Layers

- Talked of transport Layer (SSL/TLS): easy, widely used, classical web security and application Layer (PGP, S/MIME) in todays practical
- Implicitly talked of certificates to be exchanged between partners
  - But how to trust/exchange them?
  - How to trust each endpoint of the connection?



Secure Communication

- Protection against:
  - eavesdrop: intercept messages
  - actively insert messages into connection
  - impersonation: can fake (spoof) source address in packet (or any field in packet)
  - hijacking: “take over” ongoing connection by removing sender or receiver, inserting himself in place
  - denial of service: prevent service from being used by others (e.g., by overloading resources)
- Use cryptography for
  - Confidentiality (encryption)
  - Message authentication
  - Signatures and Certificates

Secure Communication – Symmetric encryption

- Encryption methods
- symmetric key cryptography: shared secret key (e_B=d_B)
- public-key cryptography: communicating party has a public encryption key e_B and a matching private decryption key d_B
- Symmetric (shared) key: Parties A and B share key k, e.g. a One-Time Pad (bitwise XOR): $E_k(m)=k \oplus m$, $D_k(c)=k \oplus m$
  - Attacker can't learn anything new on m (regardless of his speed/time)
  - But: key is as long as total length of messages sent
  - Too long for most scenarios
  - Other schemes use shorter keys but are "computationally secure"
  - Standards in use: 1977-2000: DES (56 bit key), 2001-: AES (128 bit key)

Secure Communication – Asymmetric encryption

- Asymmetric or Public Key Cryptosystem (PKCS): Party A knows only party B's public key eB, B knows its private key dB
- Most common PKCS: RSA: [Rivest, Shamir, Adelman, 1978]
- Orders slower than symmetric (shared) key cryptosystems
- Longer keys (e.g. 1024b) for same level of security (e.g. 128b AES)
- Slow encryption, decryption operations
- Thus: Use RSA only to encrypt an shared key, AES to encrypt message

Secure Communication – Encryption

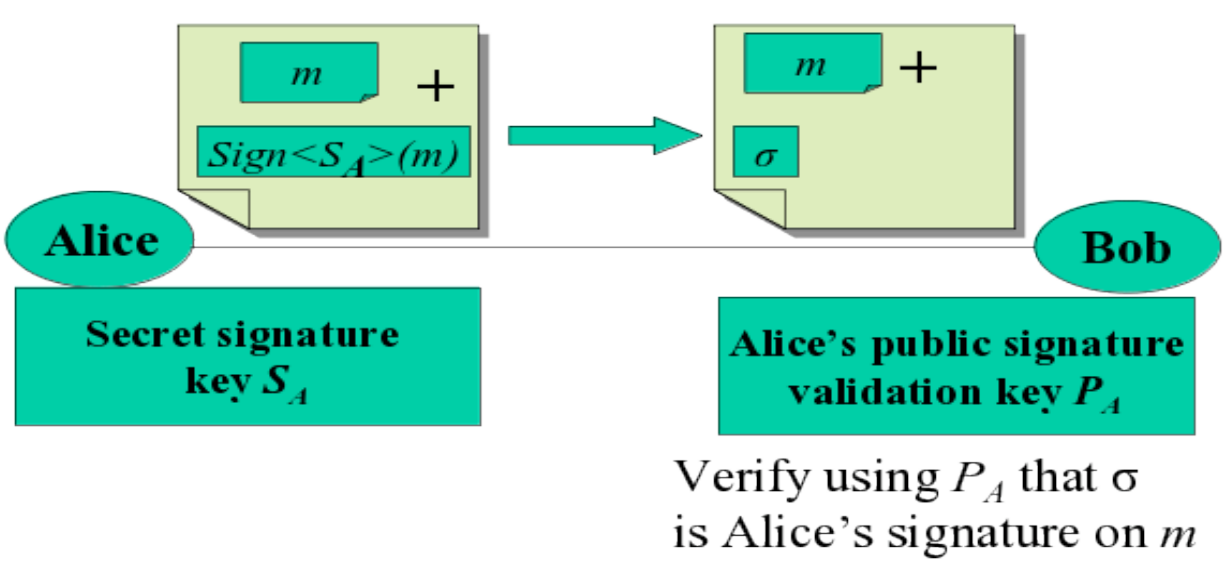
- Encryption hides messages from third party
  - Question: can a third party change/forge messages?
  - Is message integrity really ensured by encryption?
- In Public Key Encryption scenarios:
  - Attackers can replace $E_{BPub}(m)$ with fake: $E_{BPub}(m')$
- In Symmetric (Shared) Key Encryption setups:
  - This seems more difficult to do
    - But given $c=m \oplus k$, attacker can send $c \oplus mask$, to invert any bit in decrypted message (use mask)
    - Encryption does not ensure integrity!

Secure Communication – Message Authentication Code

- Shared key message authentication (integrity)
- Message sent together with Tag=$MAC_k(m)$
- Received message, tag are valid iff Tag=$MAC_k(m)$
- Efficient (even more than shared-key encryption)
- But: party A can later deny having sent m to party B (why?)

Secure Communication – Public Key Digital Signatures

- Sign using a private, secret signature key
- Everybody knows the public validation key
- Everybody can validate signatures at any time
  - Provides non-repudiation – signer is committed



Public Key Signatures – The idea

- Think of ancient seals used in kingdoms all over the world signing important documents (e.g. the rights granted to medieval cities in Europe)
- Private key: sealing ring or chop
- Public key: publicly known impression of seal
- Document: added blob of special sealing wax
- Signed document: paper, scroll, parchment with impression of seal in the blob of wax
- Hard to create impression without seal
- Hard to change rolled and sealed messages without breaking the closing seal

Public Key Signatures – The idea

- Hard to copy impression
- Wax seals last long time
- Same needed for the digital world
- RSA can also be used for digital signature scheme
- Remains the key distribution problem

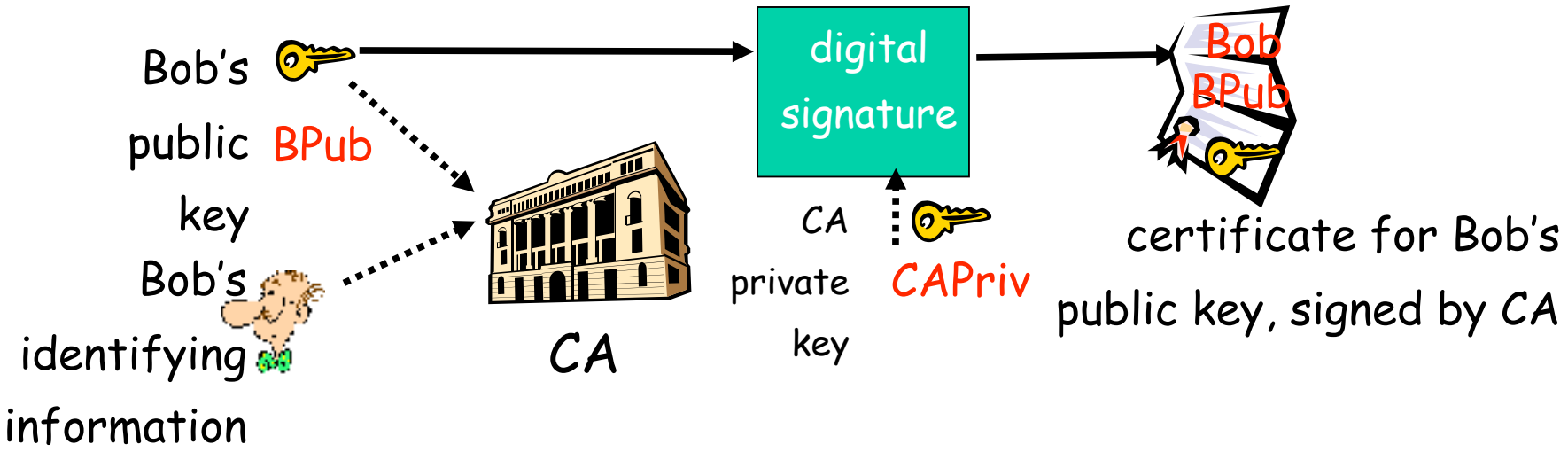
Public Key Signatures – Distribution Problem

- Symmetric key distribution problem:
  - How do two entities establish shared secret key over insecure network?
- Solution:
  - trusted key distribution centers (KDC) acting as intermediary between entities
  - KDC needs shared key with each entity, work online

- Public key cryptography problem:
  - When party A obtains B's public key (from web site, e-mail, USB stick, DNS, ...), how does A know it is B's public key, not from untrusted third party
- Solution:
  - trusted certification authority (CA)
  - Works offline, knows only public keys

Certificate Authorities (CA)

- Certification authority (CA): binds public key (e.g. BPub) to identifier (e.g. name: `Bob`)
- Bob (person, server) registers BPub with CA.
  - Bob convinces the CA that his name is Bob, sends Bpub
  - CA creates certificate binding “Bob” to Bob’s public key
  - Certificate is digitally signed by CA – CA says “BPub is `Bob’s public key”

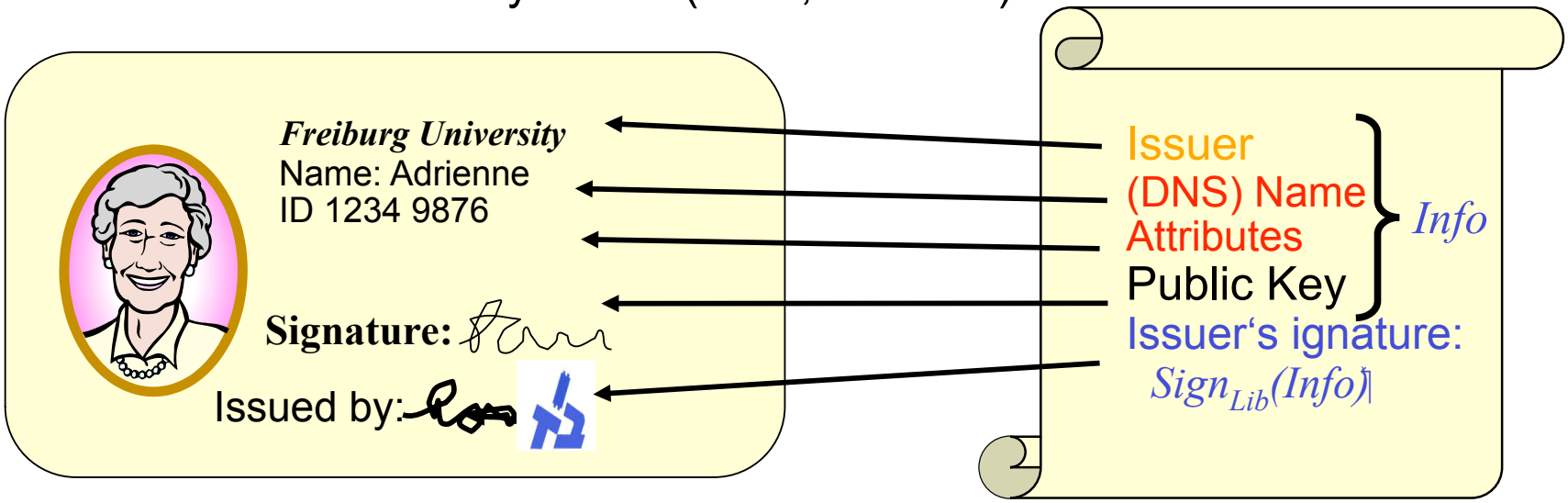


Certificate Authorities (CA)

- Using Public Key Certificates
- When Adrienne wants Bob's public key (to encrypt message to Bob or validate Bob's signature):
- Gets Bob's certificate (Bob or elsewhere)
- Apply CA's public key to Bob's certificate, get Bob's public key (validated)
- Several such authorities world-wide
- Think of the differences of the concept of the Internet (de-centrally managed) versus CA infrastructure and control
- DFN offers such a service in Germany for the scientific community

Certificate Authorities (CA)

- Certificates similar to “official documents” like passport or student ID card
- Binds a public key to a name and/or other attributes of keyholder, e.g. DNS name for web site
- signed by a trusted party (Issuer / Certification Authority)
- Allows relying party (Bob, client) to validate name, attributes of key owner (Alice, web site)



Certificate Authorities (CA)

- If a CA can be subverted
  - Security of the entire system is lost for each user for whom the CA is attesting a link between a public key and an identity
  - Interesting case of “CA subversion” - certificate authority Verisign issued two certificates to a person claiming to represent Microsoft (in 2001 – how to trust the CAs)
  - Often easy to get test certificates from commercial CAs – typically used for forged banking sites to produce a proper certificate chain
  - Or if signatures could be forged: MD5 attack presented at the CCC 2008 in Berlin (see heise link sent round as a starter)
- Other problem: Long lasting CAs
  - Institution should be round for a while, otherwise lots of certificate chains are broken
  - How to establish identity in 20, 30 years!?

Literature

- Lecture partly taken from hl2.biu.ac.il
- Overview e.g.: “Understanding PKI – Concepts, Standards, and Deployment Considerations”, 2nd ed. By Adams&Lloyd)
- General reading on network security “Security in Computer Networks” (chapt. 7 in Kurose&Ross)
- Lots of online resources

ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

Communication Systems

University of Freiburg
Computer Science
Computer Networks and Telematics
Prof. Christian Schindelhauer

CoNe
Freiburg

IIF
INSTITUT FÜR
INFORMATIK
FREIBURG