mobile business

Exam Preparation Session

10 July 2012

Information & Communication Security
(SS 2012)

MSc. Fatbardh Veseli
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe-University Frankfurt a. M.

mobile business

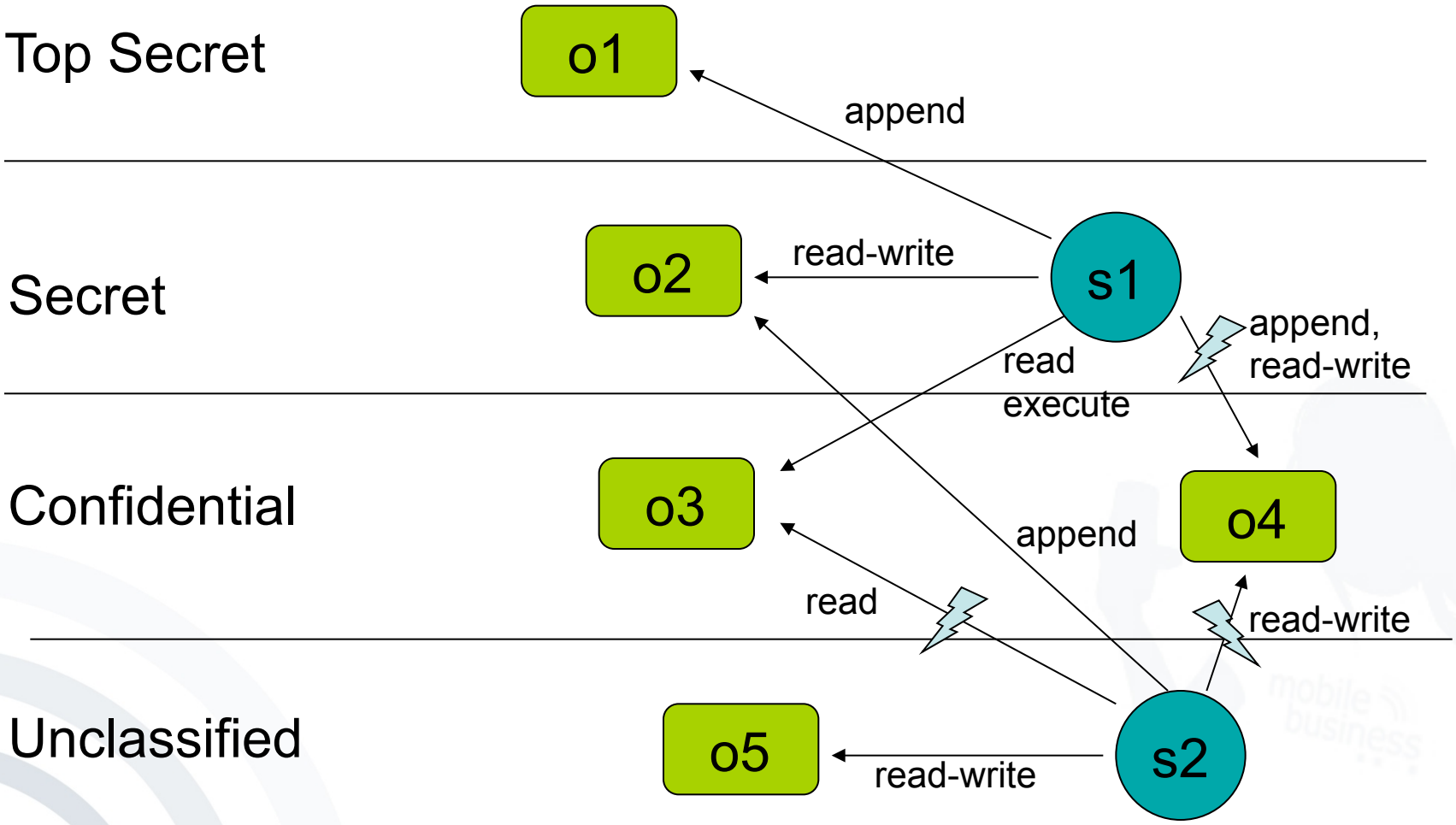
Agenda

- Announcement for two seminars
- Exam date
- Questions
- Misc.

Exam date

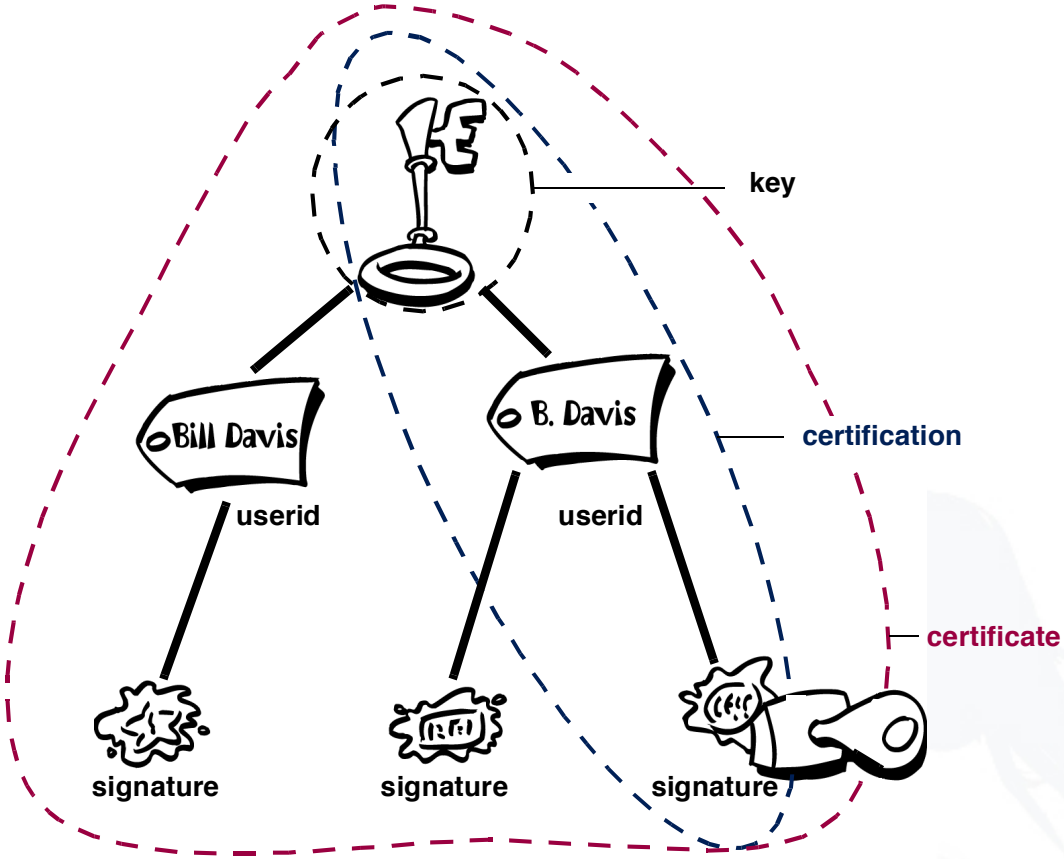
- Exam is scheduled on the 17th of July 2012 at 15:00.
  - Check http://www.wiwi.uni-frankfurt.de/mein-wiwi-studium/pruefungsamt.html

Q1: *On this slide we made indirect statements about "append" and "execute". However, on the previous slide we have only defined "read" and "write". Why can we make there statements about "append" and "execute"?*



Q2: PGP Certificates

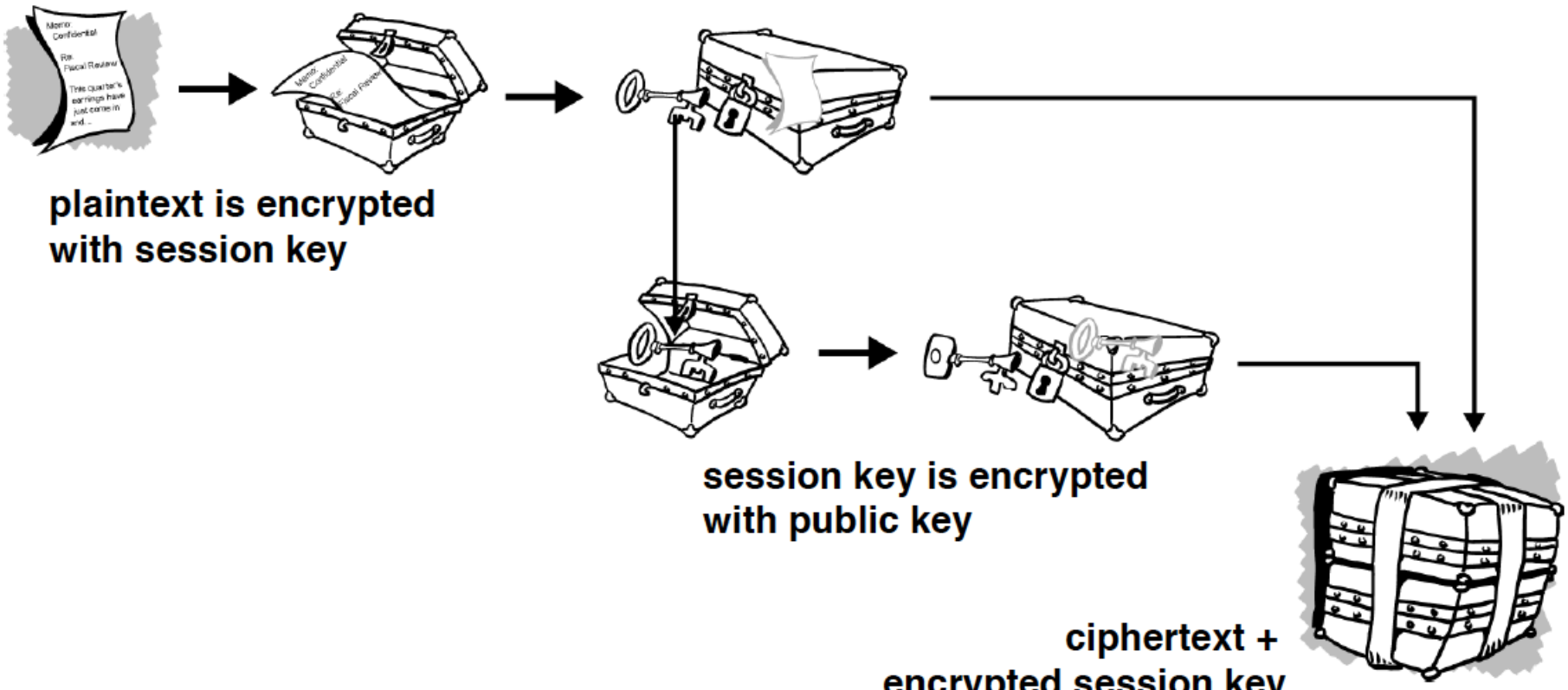
- PGP version number
- Holder's public key
  - Together with the algorithm of the key: RSA, DH or DSA
- Holder's information
  - Name, user id, photo, etc.
- Digital Signature of the signature owner
  - "Self-signature" of own public key
- Validity period
- Preferred symmetric encryption algorithm for the key
  - CAST, IDEA or Triple-DES
- May contain more than one signature (unique for PGP)
  - Several people may sign the key assuring the binding between the key and the holder



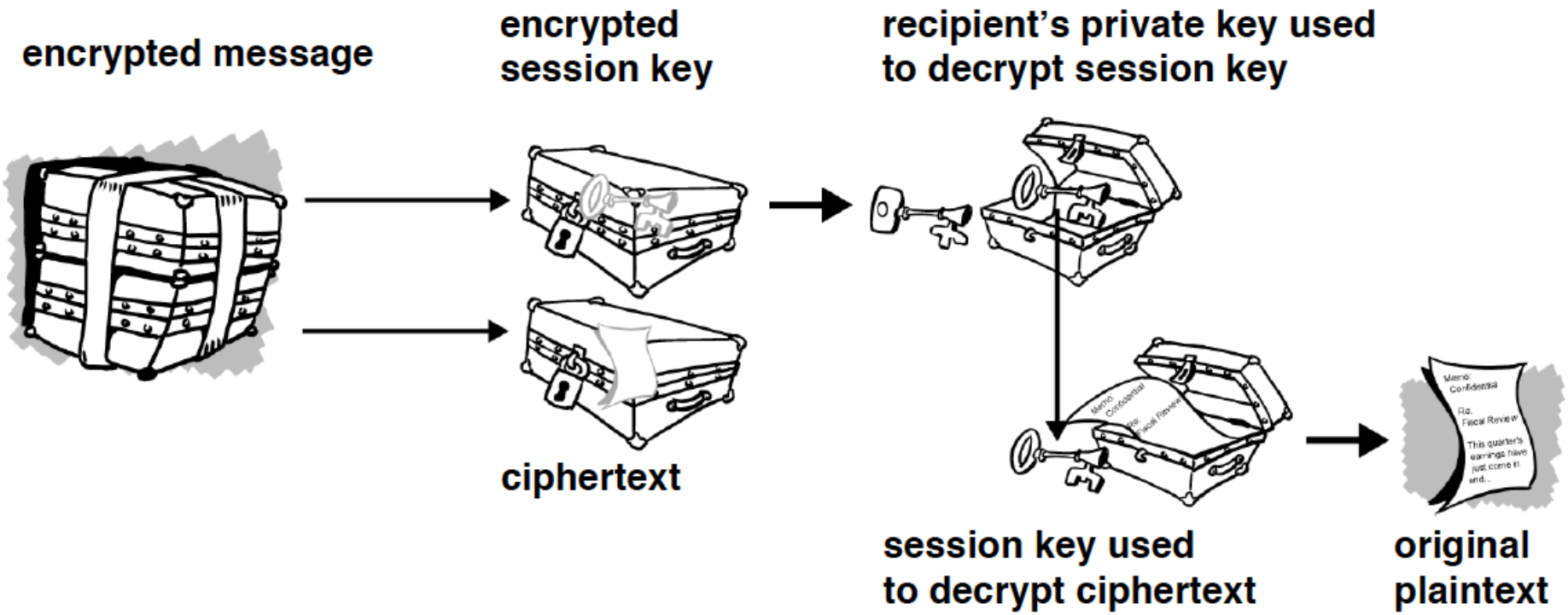
For more info, refer to the documentation of PGP.

mobile business

PGP Encryption



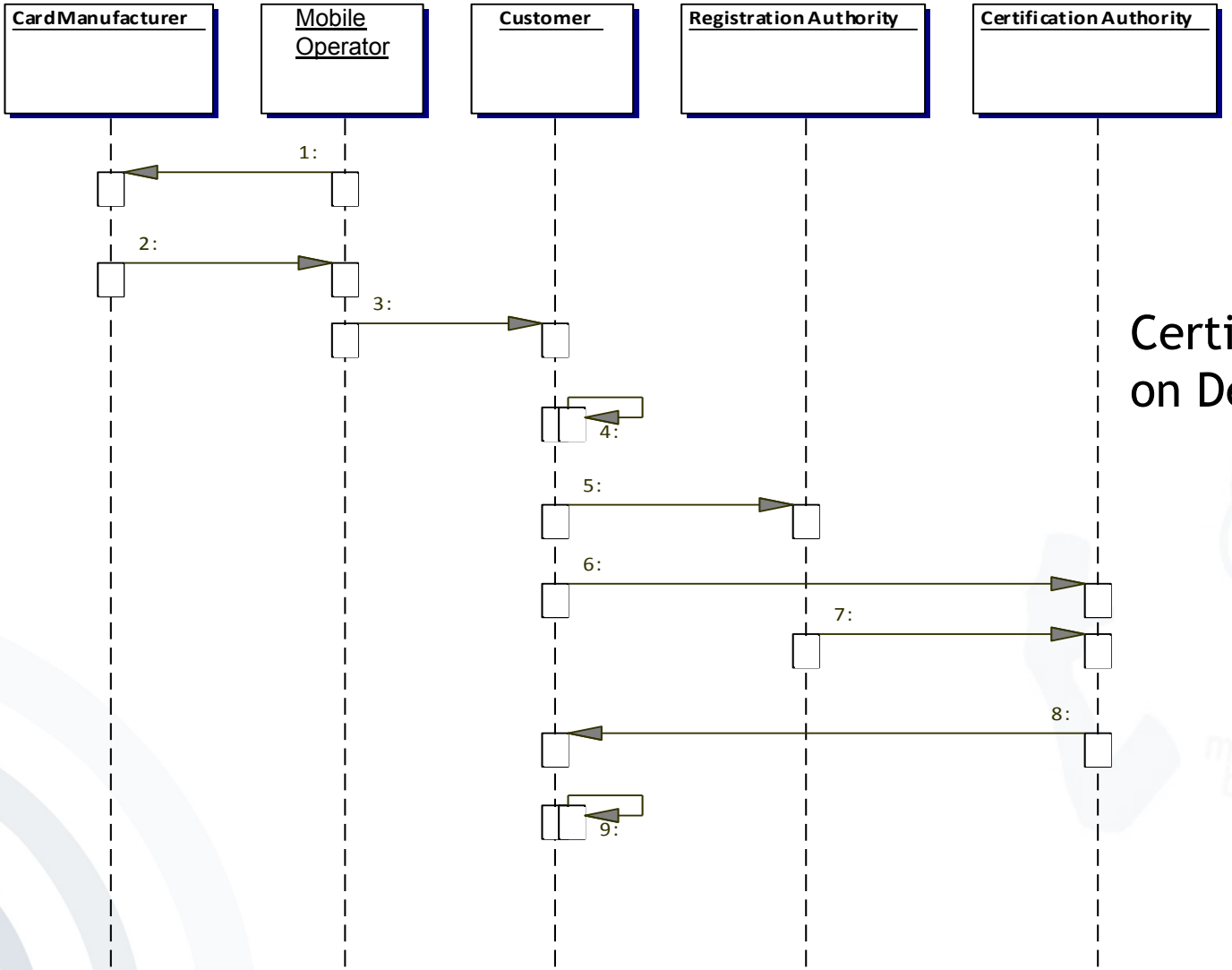
PGP Decryption



PGP Certificate distribution

- Manual public key distribution
  - I.e. Copy by USB stick
- Certificate Servers
  - Storage-only of the public keys
- Checking the fingerprint value
  - Calling the person on the phone or asking them to send you the fingerprint of the certificate

Q3: *What is the difference between Certification on Demand and other Certification methods (like CA-Certification)?*



Certification on Demand

Mobile Signatures

- Mobile signatures are signatures, which are created using a mobile device and which rely on signature or certification services in a location-independent telecommunication environment.
- Usage: signatory mobility beyond fixed, secure desktop workstation with trusted, personal signing equipment.

[Roßnagel 2004]

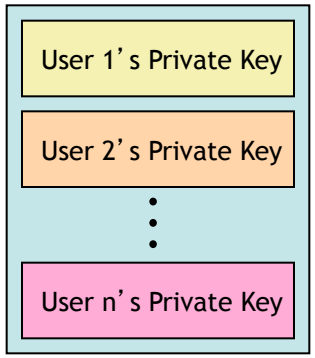
Server vs. Client Signatures

- Server based electronic signatures are signatures, that are created by a service provider for a user.
- Client signatures are electronic signatures created only by means of the mobile device.

[Roßnagel 2004]

Server Signatures Infrastructure

Mobile device



Signature Server

CSP

Relying party

0: Certificate Service Provider (CSP) creates certificate.
1: Mobile user authorizes signature on server.
2: Server creates signature for mobile user.
3: Signature sent to mobile user
4: Signature sent to relying party

[Roßnagel 2004]

Client Signatures: SIM based

- One smart card with both functions
  - Can be equivalent to established SSCDs
  - Can be certified according to security evaluation criteria
  - Under control of the user
- Needs two different PIN codes!

[Roßnagel 2004]

Challenges of SIM Signatures |1

- Who owns the smart card?
  - SIM issued by Mobile Operator (MO)
  - SSCD issued by CSP
  - SIM stores keys that belong to MO & user.
  - What happens to signature when user changes Mobile Operator?
- Challenge:
  Provide a shipment model for SIM cards within the MO distribution scheme that gives users a choice of their CSP.

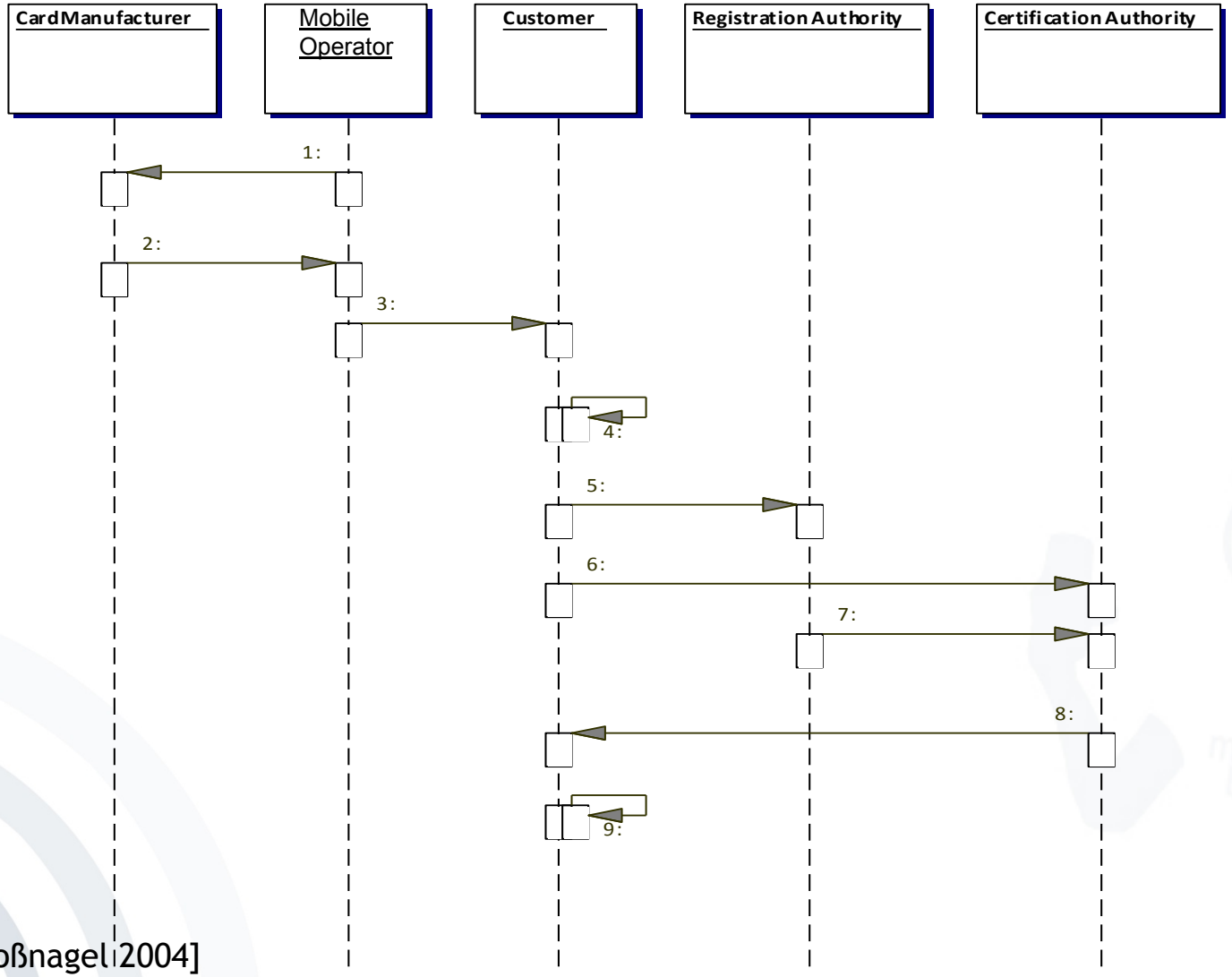
[Roßnagel 2004]

Challenges of SIM Signatures |2

- Customer wants to use SIM right away, but certification for signature takes time.
- Solution:
  - Handing out the signature capable SIM Card and
  - adding signing functionality later on request.
- Is this still an advanced signature based on a qualified certificate?

[Roßnagel 2004]

Certification on Demand



[Roßnagel 2004]

Certification on Demand

1. The MO gives IMSI/Ki pairs to a card manufacturer (or lets them be generated there based on information from the MO).
2. The card manufacturer returns (or provides) a SIM card containing an IMSI/Ki pair, a key generator for the signature application and the public key of the RootCA to the Mobile Operator.
3. The SIM card is sold to the customer and the Mobile Operator provides a nullpin, that is used to activate the signing functionality.
4. The customer activates the signing functionality by entering the nullpin.
5. The customer registers at a Registration Authority of his choice, providing identification information and his public key.
6. The customer sends his identification information signed with his private key over the air to the Certification Authority.
7. The Registration Authority sends the public key and the identification information to the Certification Authority.
8. If the information provided by the customer and the Registration Authority match, the Certification Authority issues a certificate for the customer and sends it over the air to his mobile phone.
9. The user can verify the validity of his certificate by checking the certificate issued by the RootCA for the Certification Service Provider

[Roßnagel 2004]

Certification on Demand

- Distribution scheme of Mobile Operator stays intact.
- Separation of the telephone and certification functionality
  - both functions can be sold separately and can be obtained from different providers.
- Signature-capable SIM will be more expensive, but MO can create revenue with:
  - Increase in traffic
  - Selling signature-capable SIM cards at a higher price
- CSP gains large potential customer base

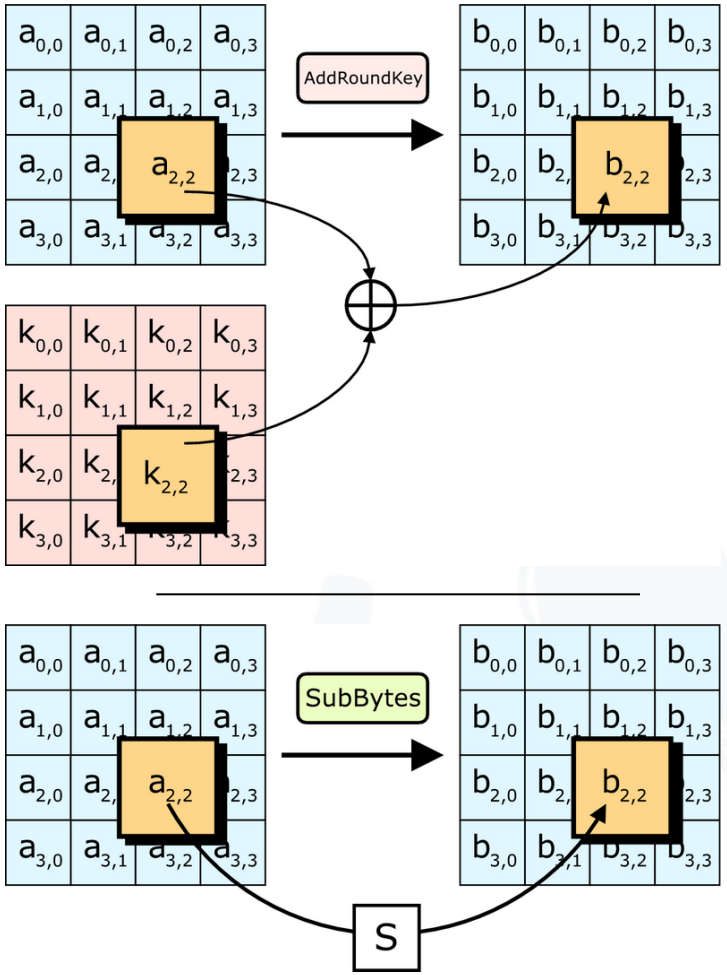
[Roßnagel 2004]

Q4: *AES Encryption*

- AES encryption
  - has a variable number of rounds
  - depending on key size.
- To encipher a block of data in AES
  - Initialize (key schedule…)
    - Stretch key data
    - Initialization Round
  - Then several rounds of encryption
    - Shifting and mixing bits
  - Finally, some postprocessing
    - perform a round with the last step omitted

Encryption Round (1)

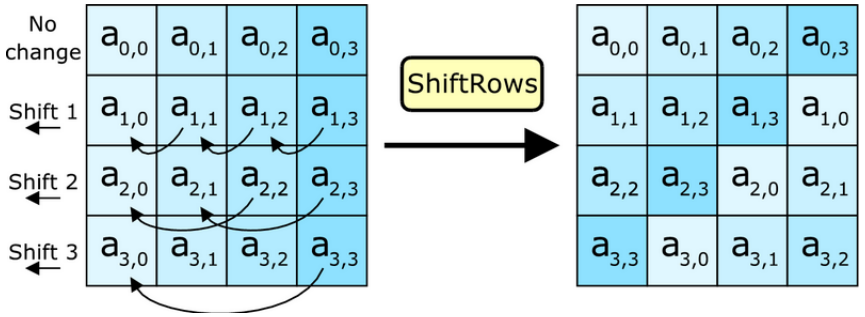
- AddRoundKey
  - XOR (mix bits of) current state a and round key
  - Round key k derived using key schedule
- SubBytes
  - Substitution using a lookup table (S-Box)

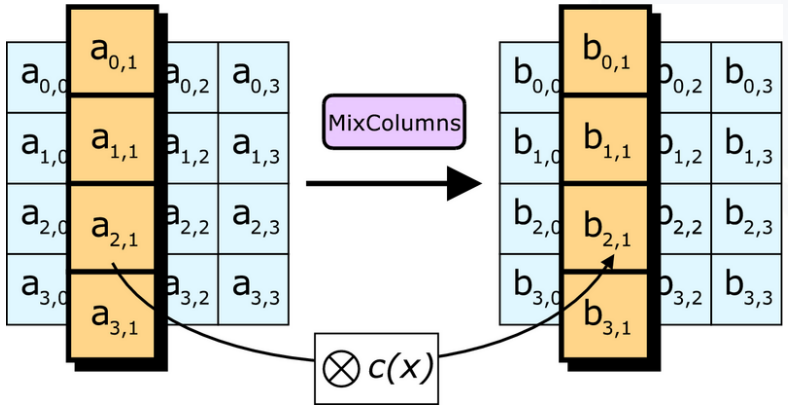


Images: Wikipedia

Encryption Round (2)

- ShiftRows
  - Shift each row by row index
- MixColumns
  - 4 key bytes combined into each column using polynomial multiplication modulo 2^8 [in GF(2^8)]

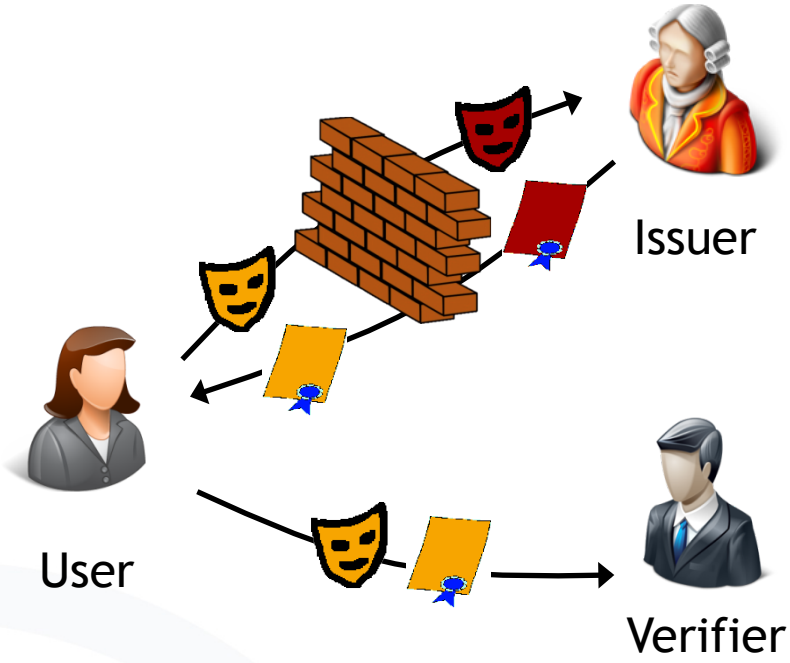




Images: Wikipedia

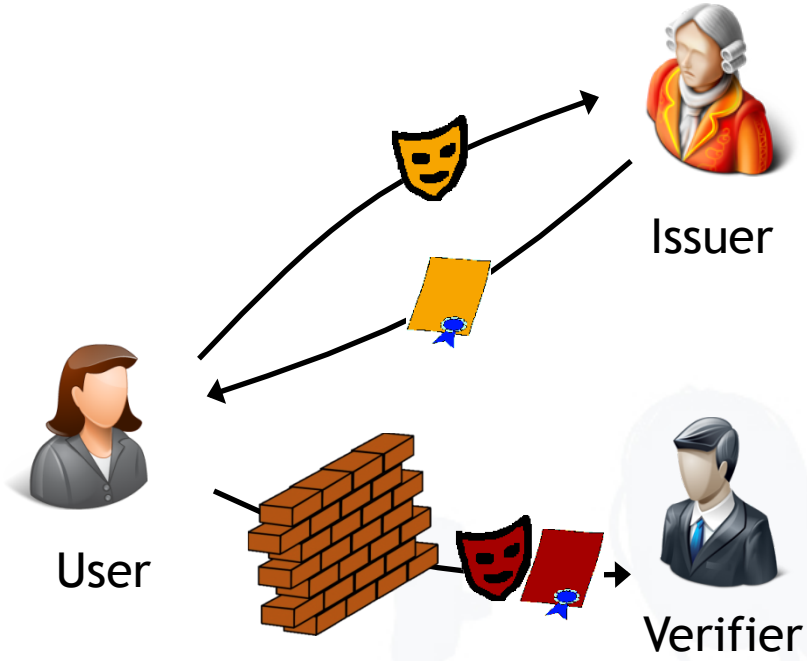
mobile business

Q5: *What exactly is the meaning of the light-grey shaded and the dark-grey shaded masks in the picture?*



U-Prove

Chaum, Brands et al.
Discrete Logs, RSA,..



Idemix (Identity Mixer)

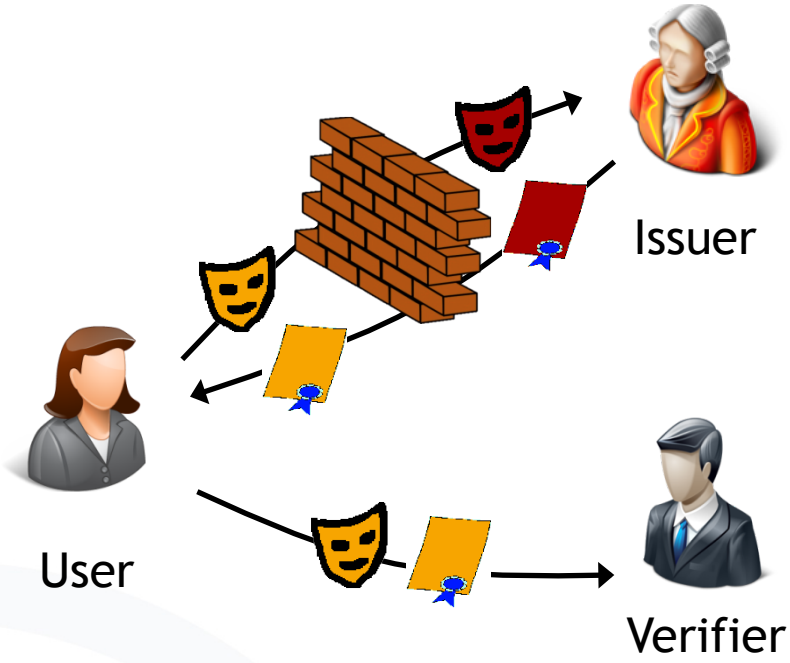
Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)

mobile business

Privacy-ABCs

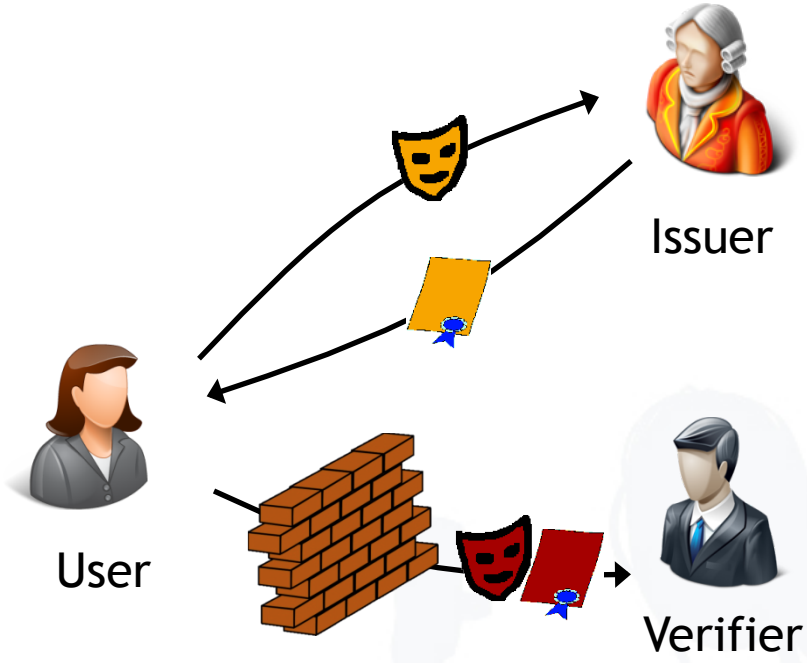
- Anonymous credential systems allow users to authenticate themselves in a privacy-preserving manner.
- In a credential system, a user can obtain credentials from an organization, and then at some later point, she can prove to the organization (or any other party) that she has been given appropriate credentials.
- In an anonymous credential system, she can do this without revealing anything else about her identity.
- Such a system needs to have the following properties:
  - Unforgeability of credentials
  - Unlinkability of credentials
  - No credential sharing
  - Consistency of credentials

Q6: What is the difference between U-Prove and Idemix?



U-Prove

Chaum, Brands et al.
Discrete Logs, RSA,..



Idemix (Identity Mixer)

Damgard, Camenisch & Lysyanskaya
Strong RSA, pairings (LMRS, q-SDH)

Q7: *Could you repeat in a short manner, what the PRIME Project is all about?*

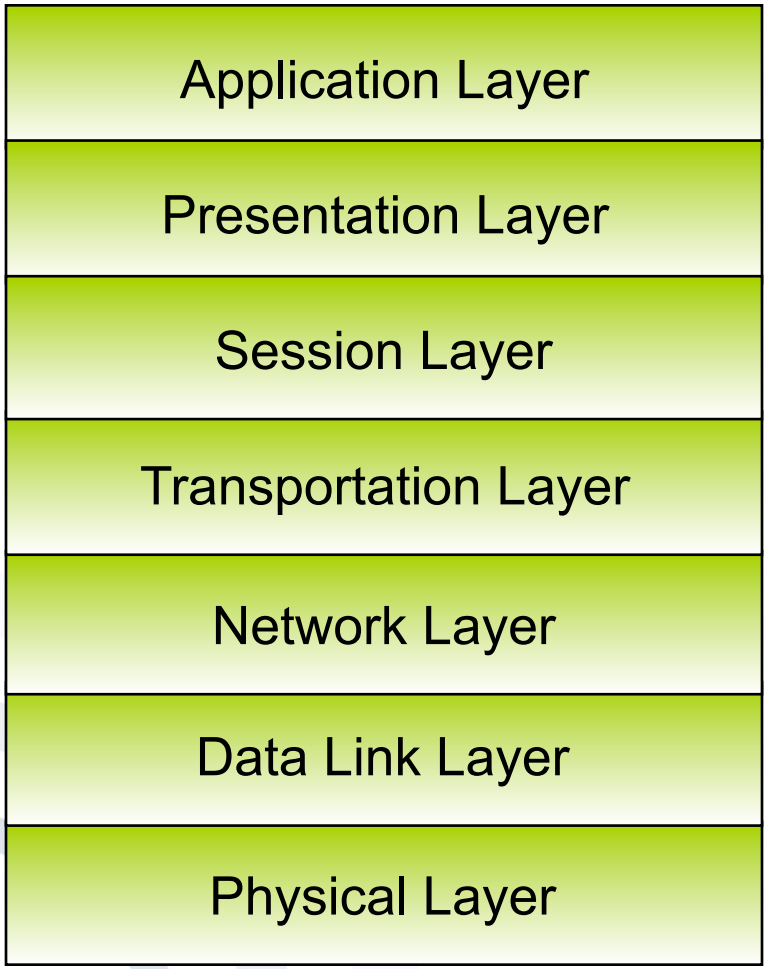
- The PRIME project is a research project that aims to demonstrate viable solutions to privacy-enhancing identity management by delivering a reference framework, requirements, an architecture, design guidelines, protocols and prototype implementations that are evaluated from a multidisciplinary perspective. The prototypes are not intended as final products for commercial deployment.
- http://prime-project.eu/

OSI and *Internet* reference models

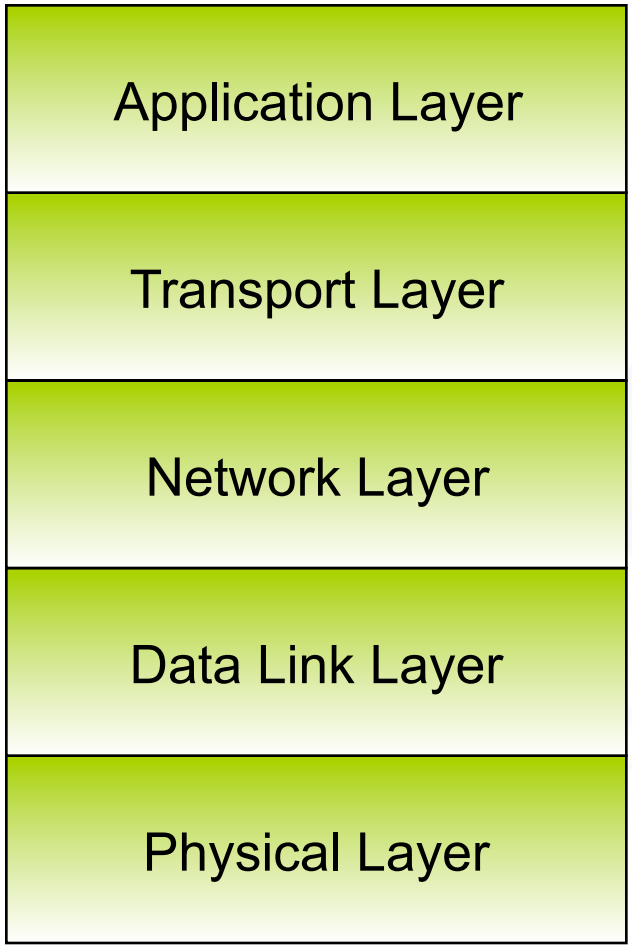
- Protocols associated with the OSI model are rarely used any more, but the model itself is actually quite general and still valid.
- The Internet (TCP/IP) model has the opposite properties: the model itself is not of much use but the protocols are widely used.

Comparison of the two models

- OSI



- Internet (TCP/IP)

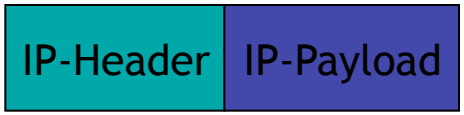


Why do they have different layers

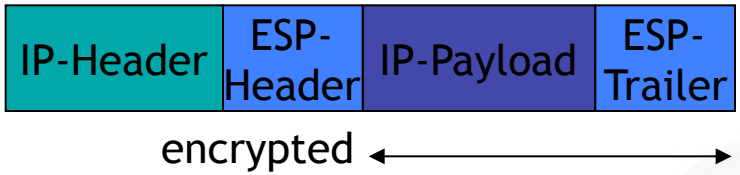
- It's a matter of design
  - OSI was designed based on the layers, protocols were hidden from the model (protocol-independent)
  - TCP/IP was designed based on protocols, then common layers were created (protocol dependent)
  - OSI was created before the advent of Internet, while TCP/IP after.

Q8: IPsec Encapsulating Security Payload (ESP)

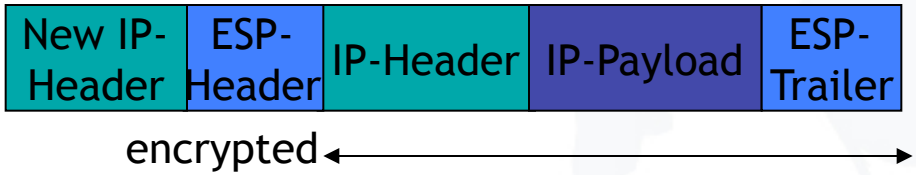
- Data Packet



- ESP-Transport-Mode



- ESP-Tunnel-Mode



[J. Buchmann: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU Darmstadt]

When is each IPSec mode used?

- IPSec *tunnel mode* is the default mode and is used to create virtual private networks for network-to-network (e.g. between routers), host-to-network and host-to-host communications (e.g. private chat).
- In *transport mode*, only the payload of the IP packet is encrypted. Mostly used for host-to-host communication, e.g. client-to-server. This mode is usually combined with another tunneling protocol, which is first used to encapsulate the IP data packet (the tunnel traffic).
- *Authentication Headers* (AH) provide **integrity** and data origin **authentication**, and **protection against replay attacks**.
- *Encapsulating Security Payloads* (ESP) provide **confidentiality**, data-origin **authentication**, **integrity**, an **anti-replay** service (a form of partial sequence integrity), and *limited traffic-flow confidentiality*.

Q9: Mobile IP, what is the difference between “Dynamic IP” and “Dynamic DNS”?

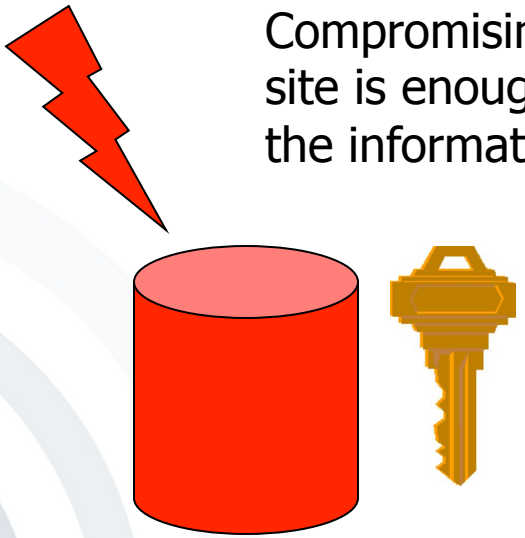
- Dynamic IP means that the IP address of the customer is dynamic, it changes each “session”.
- A dynamic DNS service updates, in real time, a Domain Name System whenever an IP address changes on the Internet (globally distributed, which normally takes more time in a static DNS). Usually a router or computer (customer) sends a detected IP change to a Dynamic DNS service and is usually automatic.

Q10: *Explain the Distribution of Trust*

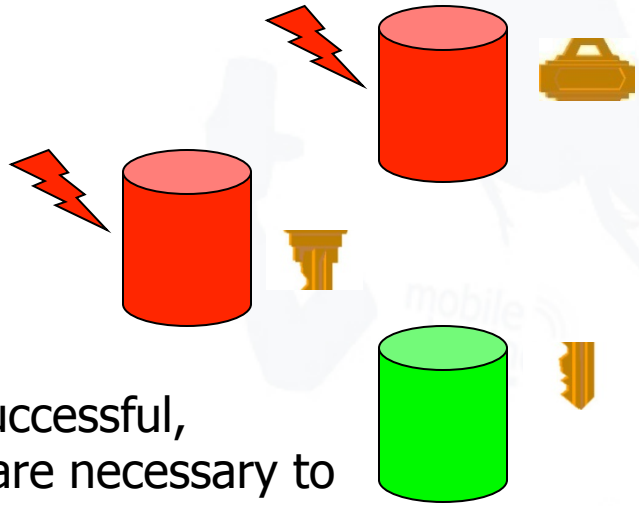
Decentralise Trust: reduce damage in the case of

- successful external attack
- malicious or careless management

Centralized trust vs. Distributed trust



Compromising a single site is enough to access the information



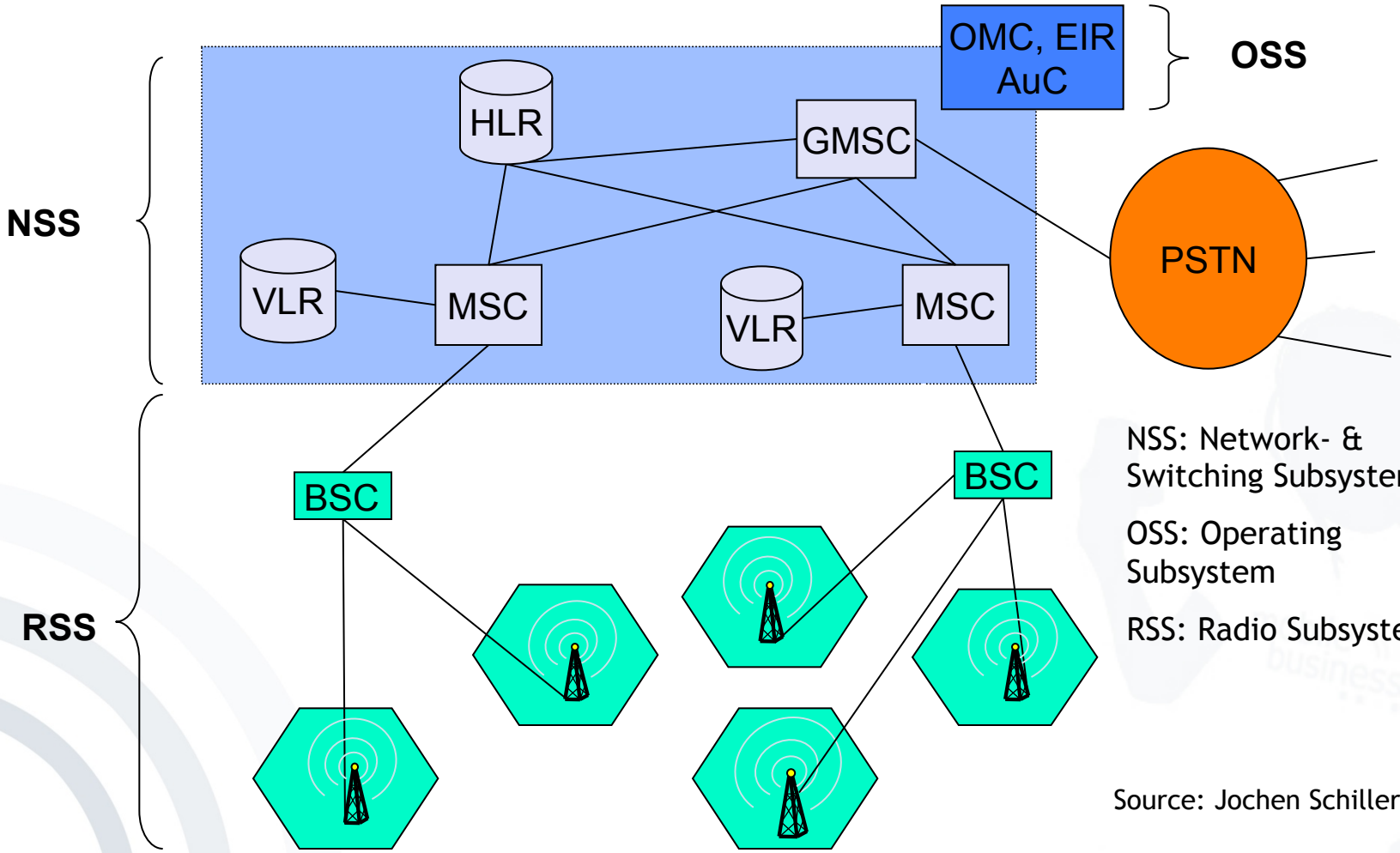
Many, successful, attacks are necessary to access the information

Distribution of Trust

- Define “Administrative Domains”
  - Each domain is administered and operated independently from the others
  - The administrators of one domain do not have access to the others
- Set requirements on the allocation of
  - information
  - processing activities (generates information)

mobile business

Q11: *Could you please explain once more the functioning or the flow of data between the nodes in the network?*



NSS: Network- & Switching Subsystem

OSS: Operating Subsystem

RSS: Radio Subsystem

Source: Jochen Schiller

Misc. questions

- In Lecture 8, **Identity Management II**, we skipped slides 56-70. Are those slides relevant for the exam?
  - *These slides are detailed examples the whole lecture (project such as PRIME, ABC4Trust and so on). They will not be in the exam.*
- In Lecture 9, **Computer System Security,** we skipped slide 51, 53, 54, 57, 58. Are those slides relevant for the exam?
  - *Everything that is in the lecture is a potential exam question. However, if something was skipped, it has less chance of appearing in the exam.*
- (Guest) Lecture 12, **Security Management**: This lecture is very large and has many different definitions in it. What are the important aspects of this lecture? What should we take away?
  - *Do not focus on the details, but rather on the big picture of Security Management, related standards and certifications (national and international, differences and what they mean). Specifically focus on ISO 27000 series, its definitions, process model, etc. Different parts of the standard and requirements.*