mobile business

Q & A Session

Mobile Business II (SS 2023)

Prof. Dr. Kai Rannenberg

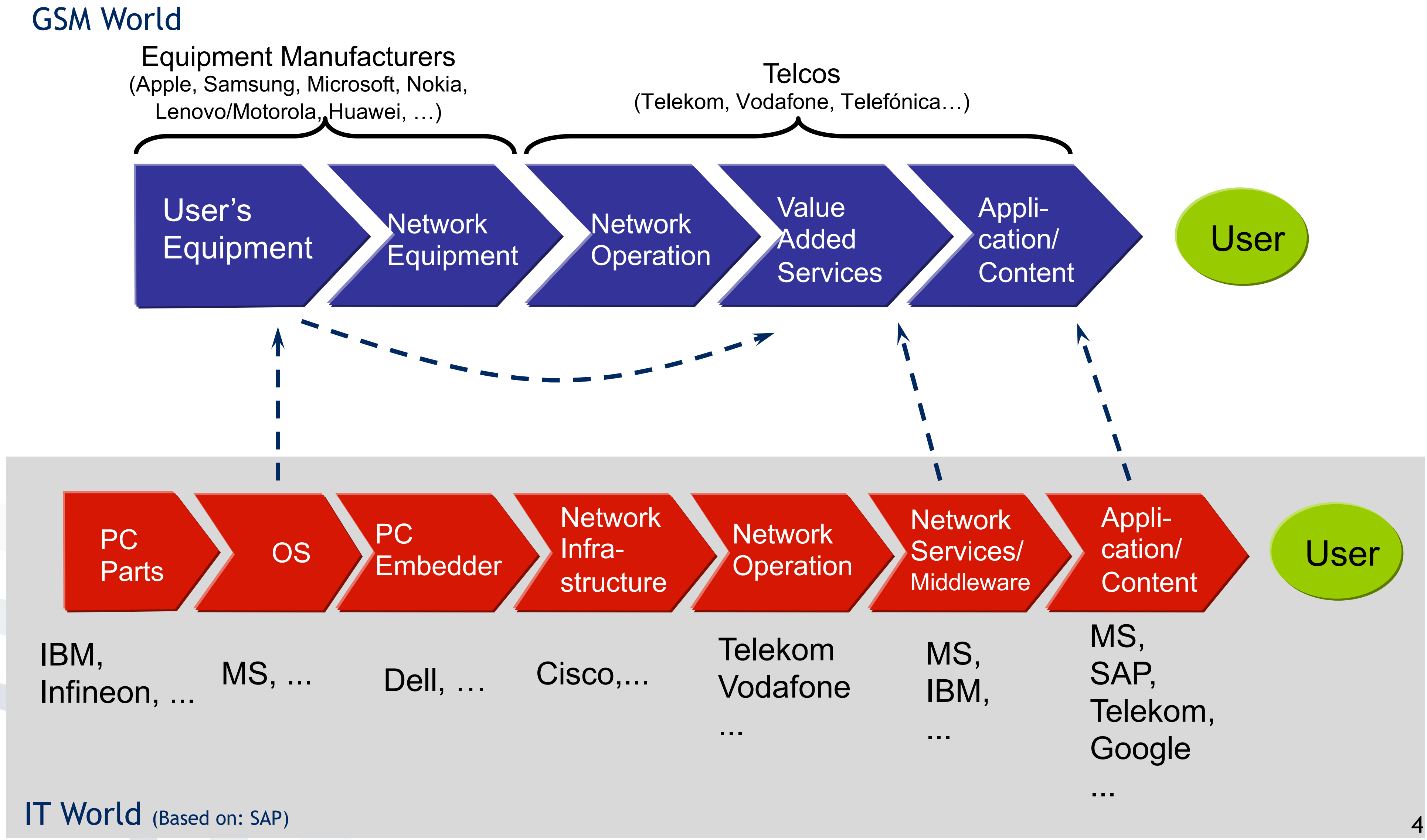
Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Lecture 1

Question 1

- *S.31: could you explain the key takeaways of this slide?*

Value Chains merge



Lecture 2

Question 2

- *it would also be nice if you could explain the differences in TDOA and E-OTD, since both use the signal and the arrival. I still don’t really get the difference between them.*

Time Difference of Arrival – TDOA

Time Difference of Arrival (TDOA)

- Measuring of time intervals
- Using_the “uplink-data” (data, that are sent out from the terminal)
- TDOA supports legacy-terminals:
  All base stations have to be equipped with “Monitoring Software”.

TDOA

- Advantages:
  - Slightly more precise than Cell-ID (50-125 m)
  - No modification of the software on the terminal
- Disadvantages:
  - Slower response time than Cell-ID (< 10 seconds)
  - High costs due to the needed upgrade of the network,
  - Relocation of the “intelligence” into the network.
  - The customer has no control over his location information anymore.

Enhanced Observed Time Difference – E-OTD

- Terminal (Mobile Station, MS) observes the time difference of the arrival of signals from two different base stations (Observed Time Difference (OTD)).
- However the clocks of the base stations may not be synchronized, so OTD may be imprecise.
- A Location Measurement Unit (LMU) with a fixed location estimates the transmission time offset between the two base stations (Real Time Difference (RTD)).
- OTD – RTD = Geometric Time Difference (GTD)
- To locate the terminal, one needs two BTS.

E-OTD

Usage in M-Business:

- Advantages:
    - Slightly more precise than Cell-ID (50-125 m)
- Disadvantages:
    - Modification of the software on the terminal
    - A bit slower response time than Cell-ID (< 5 seconds)

Question 3

- *Slide deck 2, page 10*
  We distinguished between "Network external source of information about location" and "Network internal source of information about location". Are there specific names we should know with regard to the overview of positioning methods?

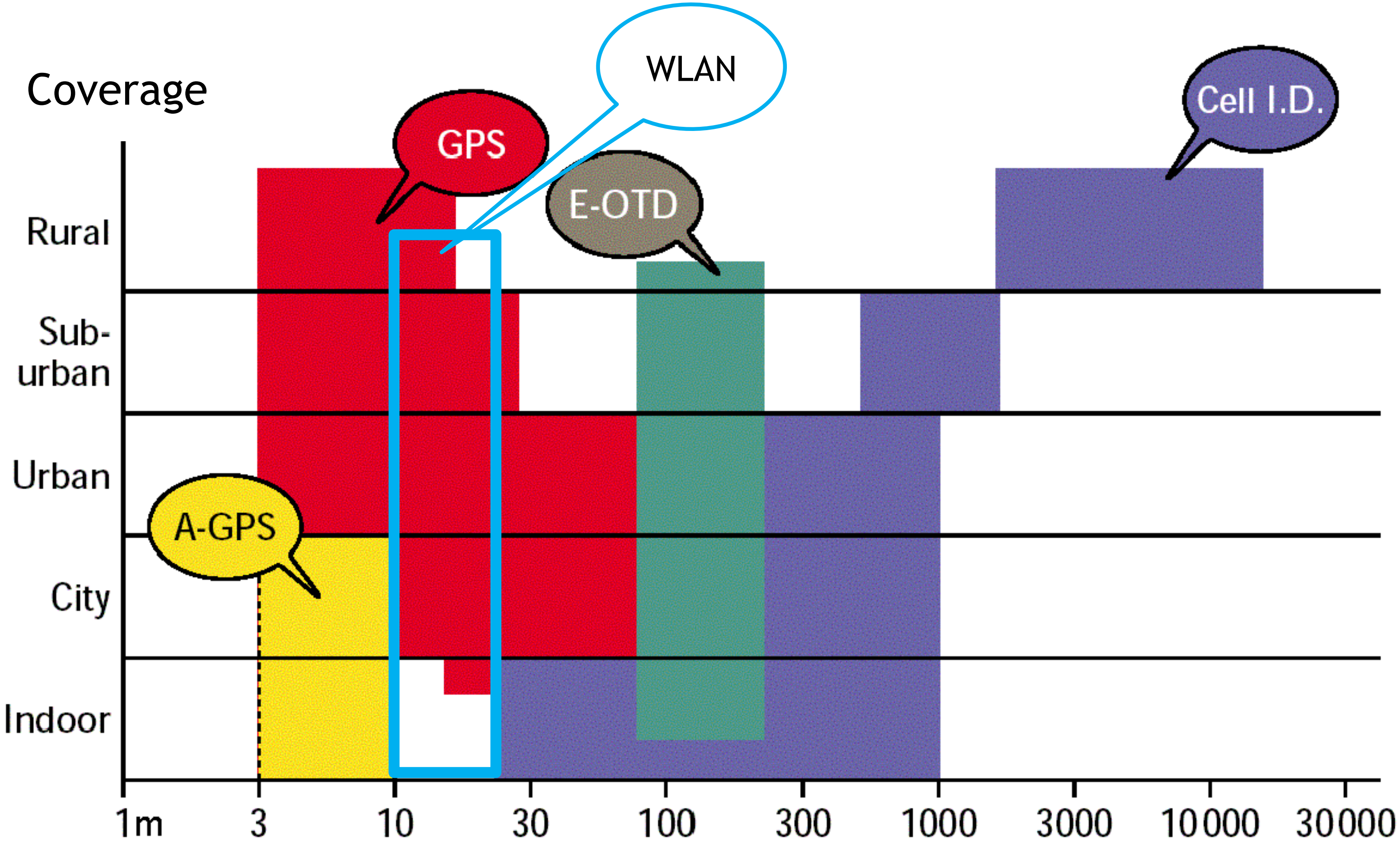
Overview Positioning Methods

- Network external source of information about location
  - User input to the device
  - Satellite Systems: GPS (USA), Galileo (EU), GLONASS (Russia)
  - Position sender (Radio, Infrared)
  - WLAN positioning
  - Peer to Peer
- Network internal source of information about location
  - Cell-ID
  - Time Difference of Arrival (TDOA)
  - Enhanced Observed Time Difference (E-OTD)
  - Angle of Arrival (AOA)
  - Signal Attenuation (SA)
- Hybrid solutions
  - Assisted GPS (A-GPS)
- Often the terminal is involved in the positioning
  - Terminal positioning
  - Hybrid positioning

Question 4

- *Slide deck 2, page 58*
  The graph does not have titles for the x-axis. What does this picture exactly illustrate? Why are there different systems working parallel?

Precision of positioning



[Source: based on Nokia]

Question 5

- *Slide deck 2, page 62*
  Could you please once again go over this slide?

Altitude and Direction

- What is missing in mobile communication based methods presented so far?
  - Measuring of the line of sight
  - Measuring of the altitude
  - Direction of a movement
- Solutions
  - Infrared beacons
  - Electrical compasses
- Some technical solutions are very complex.

Lecture 3

Question 6

- *slide 27, could you explain to us the calculation of the cost? (CPT)*

Mobile Multimedia as Advertising Medium

Example: Distribution of a 30-seconds commercial spot

Television - RTL

- CPT for a booking on a Saturday morning in the childrens' program of RTL: € 0,12
- CPT for a booking at a simulcast of a popular sports show at primetime: € 154,00
- **CPT: € 0,12 - 154,00**

Preset costs based on assumptions and statistical analyses

UMTS-Streaming

- Assumptions:
  - Resolution 128x96 Pixels (ITU H.261)
  - 15 frames/sec. in an MPEG4 coding
  - Mono Audio channel in a mp3 coding
  - Average necessary bandwidth 64 kbps
- 30 seconds x 64 kbps add up to 234 KB broadcasted data volume
- Current GPRS rate: € 0,20 per megabyte
- So the transmission costs € 0,0468
- **CPT: € 46,80**

Variable costs based on matching of Customer profiles

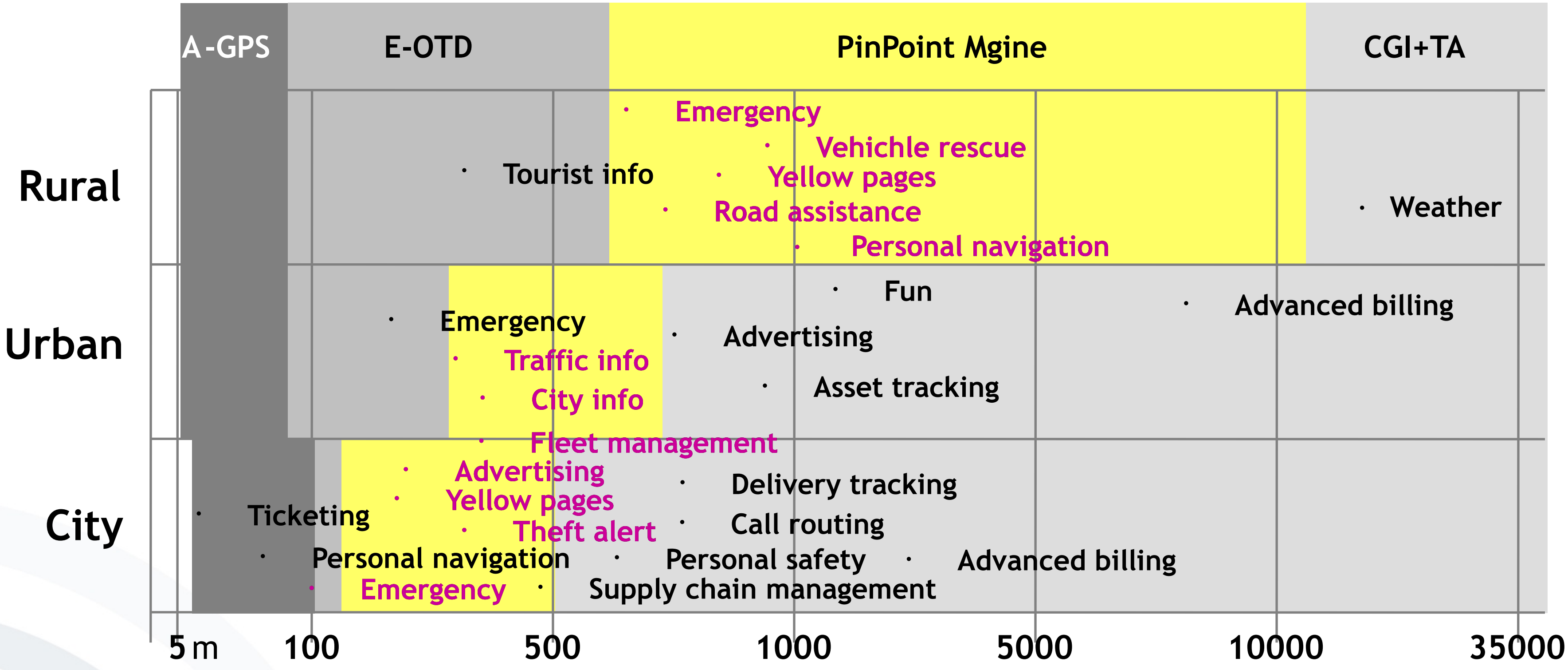
Question 8

- *S. 72: What is Pinpoint Mgine and CGI + TA? Could you explain the main points of this slide?*

Question 9

- *L3, p72: What exactly are the takeaways from this graph? I find it hard to read it, as there is no description for the x-axis and I am unsure how to understand the different color-codings.*

Services and Precision



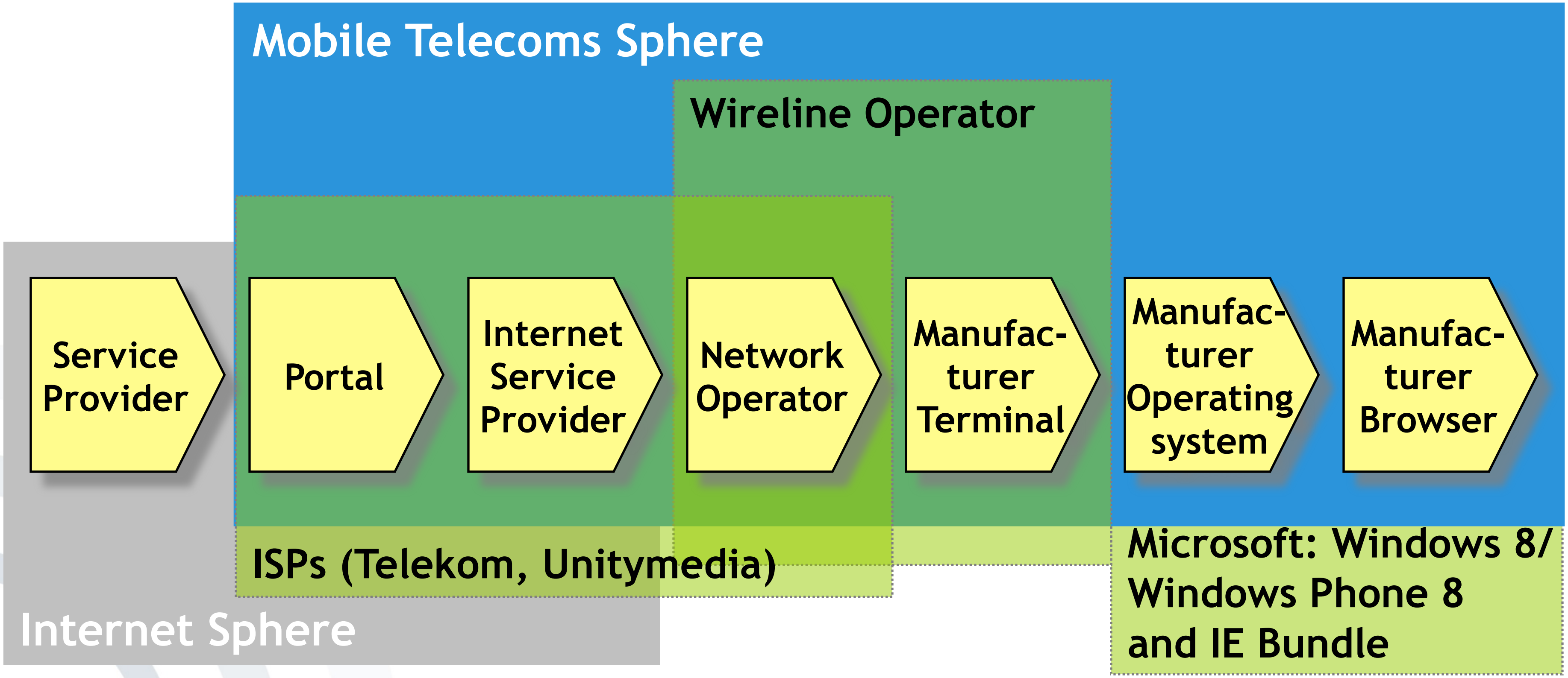
[Source: EMT]

Question 10

- *S.9: could you explain the key takeaways of this slide?*

(2) Architecture of the Added Value

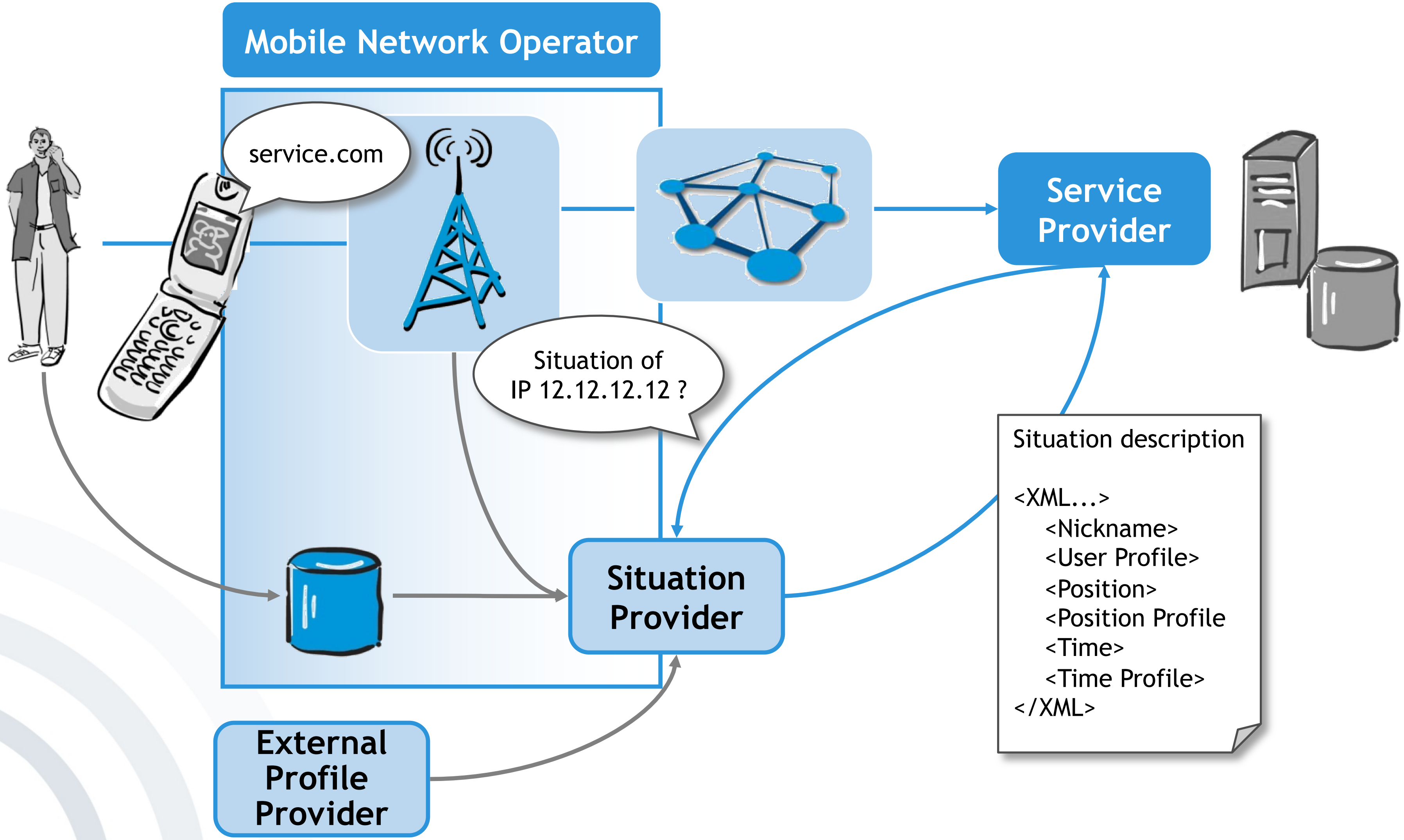
- Value chains to model the architecture of the added value.



Question 11

- *Slide deck 3, page 23:*
- *If the depiction of the process shown in the illustration is relevant for the examination, could you please shortly explain the most important steps?*

Situation Dependency and its Technical Implementation



Situation description

```
<XML...>
    <Nickname>
    <User Profile>
    <Position>
    <Position Profile
    <Time>
    <Time Profile>
</XML>
```

Lecture 4

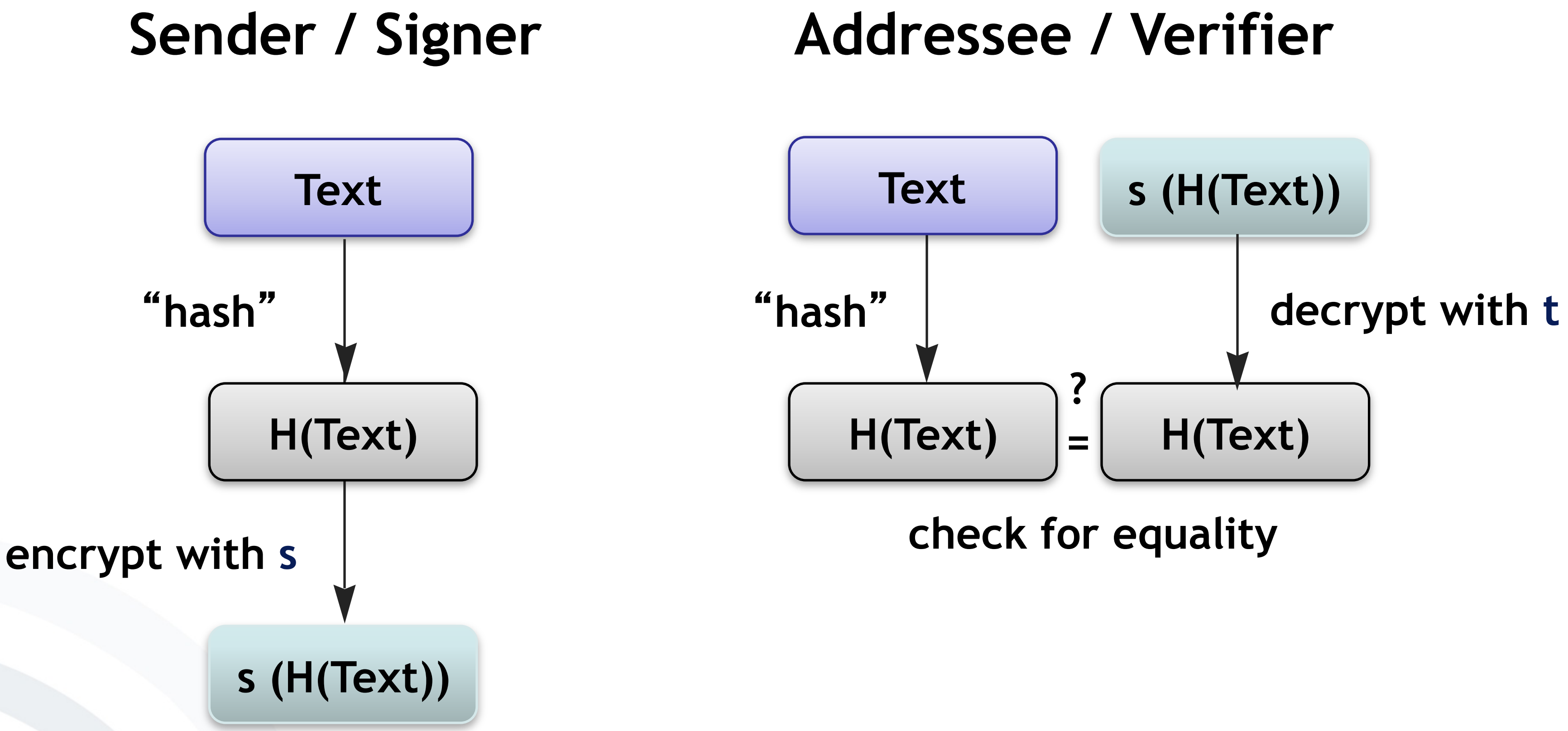
Question 12

- *Please explain again the concept of hash functions.*

Hash Functions

- **General** hash functions *(H(s))*
  - Transformation of an input string *s* into an output string *h* **of fixed length** which is called hash value.
  - Example: mod 10 in the decimal system
- **Cryptographic** hash functions
  - Generally require further characteristics
    - *H*(*s*) is easily to compute for each *s*.
    - *H*(*s*) must be difficult to invert: In terms of figures it is difficult to compute *s* from *h*.
    - Virtual collision freedom: In terms of figures it is difficult to create collisions H(s1) = H(s2).
  - Examples: SHA-1, MD5, MD4

Asymmetric Signature System (Example RSA)



- ➲ Signing key s only with the sender, test key t public
- ➲ Example is often mistakenly generalized.

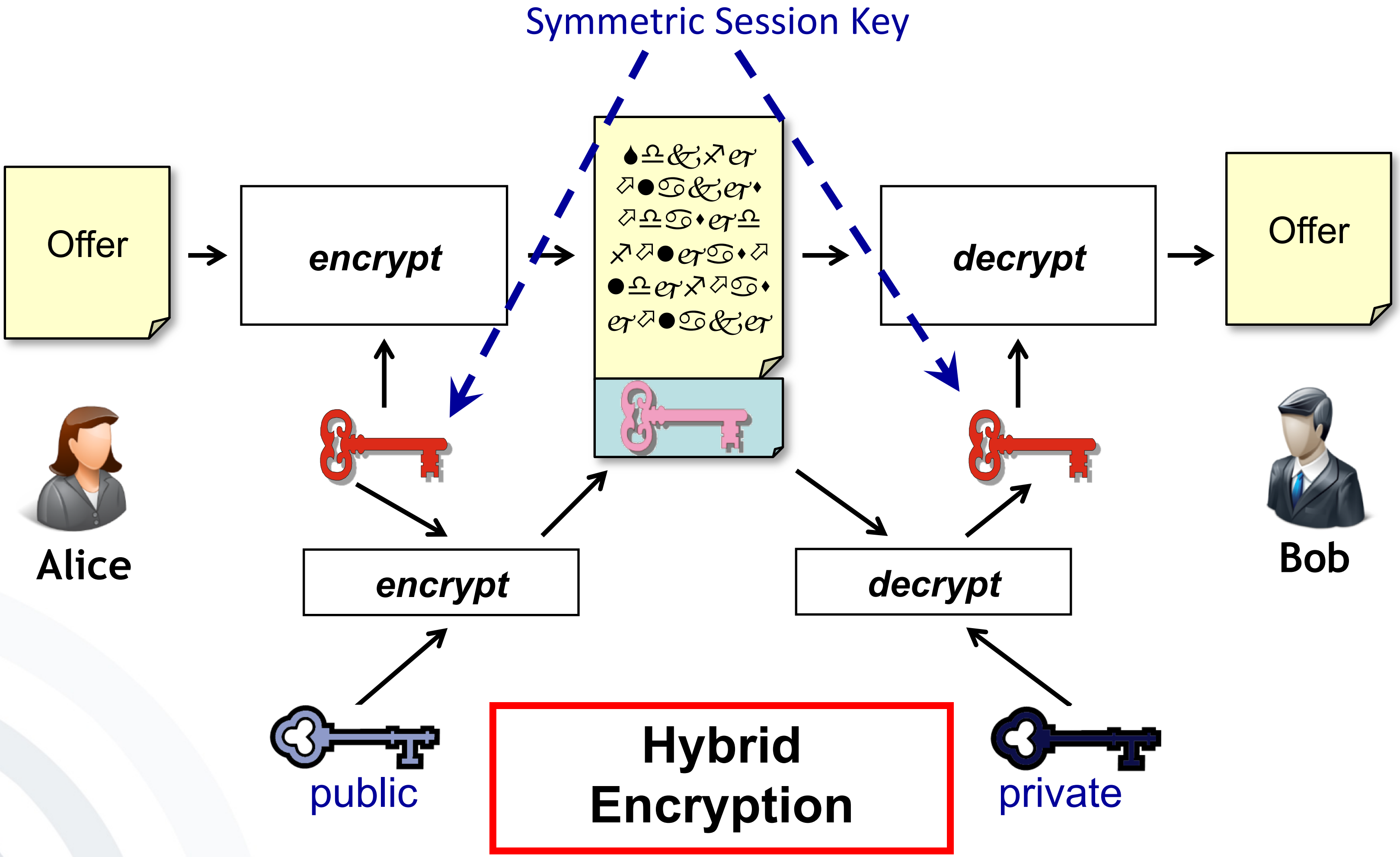
Question 13

- *In symmetric encryption the key is generated by thee key generator. HOW exactly is the key generated in asymmetric encryption?*

Question 14

- *slide 30, could you explain to us the what is symmetric session key? and how does it function and transfer from encryption to decryption? is it sort of like a private key..?*

Solution: Hybrid Systems



[based on: J. Buchmann 2005: Lecture Public Key Infrastrukturen, FG Theoretische Informatik, TU-Darmstadt]

Question 15

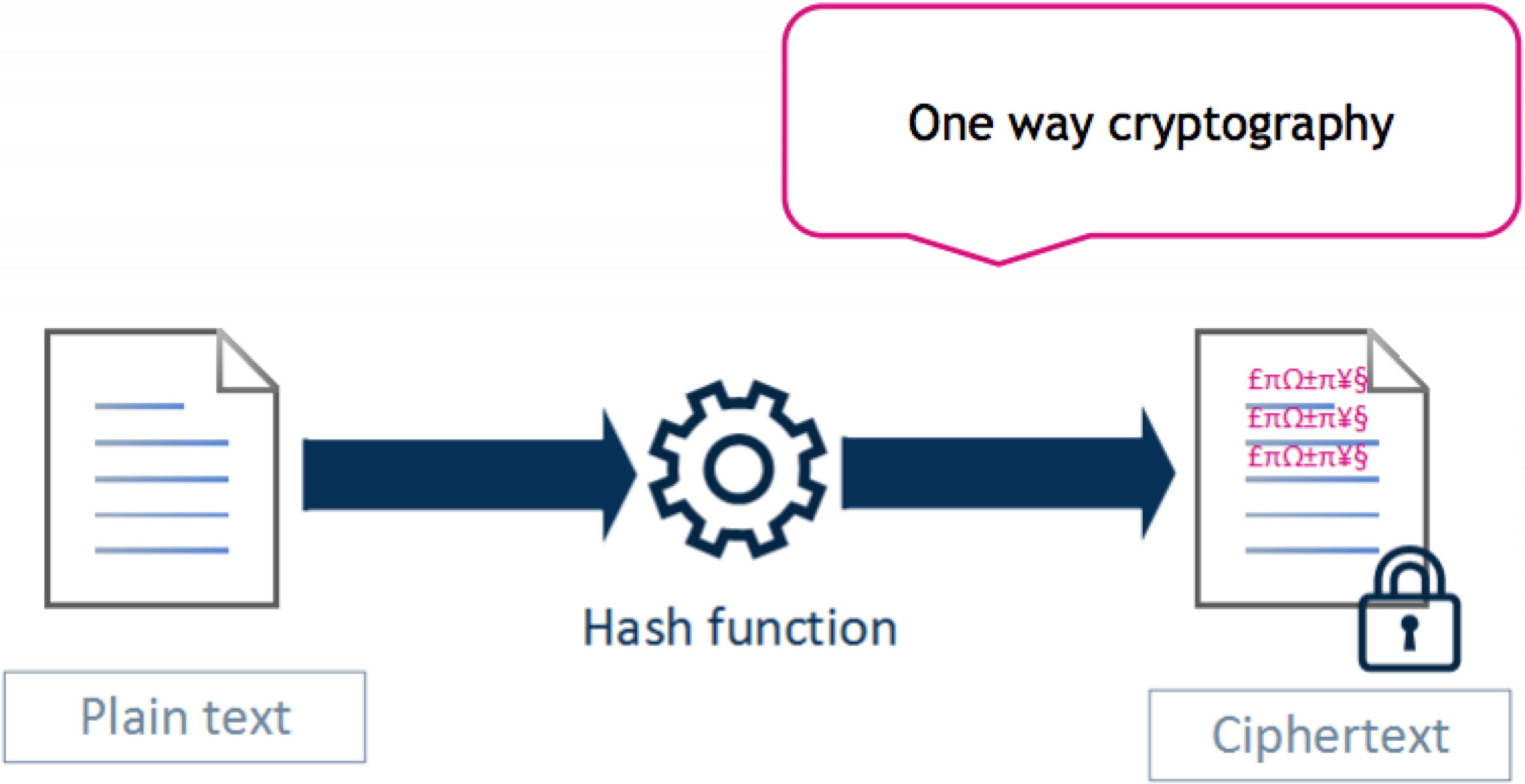
- *As I understand it, a text is encrypted with a symmetric key. The symmetric key is then encrypted with the recipient's public key. Then both (message and key) are sent to the recipient, is that correct? The message itself is not encrypted with the public key in this process, is it? (Otherwise, the advantage of speed would be lost I guess)*

Lecture 5

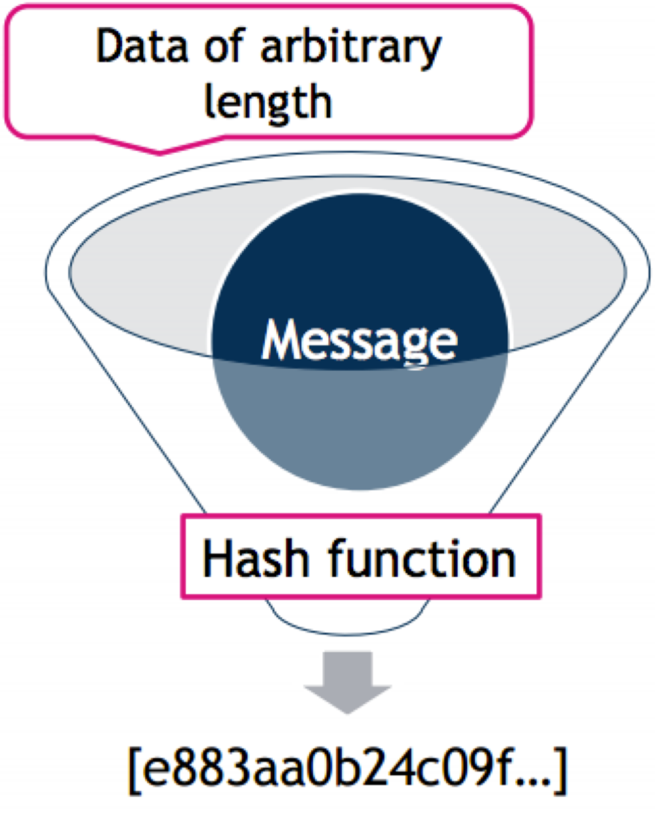
Question 16

- *S.11-18: What is the benefit and disadvantage of using hash functions?*

Hash Functions I



Hash Functions II



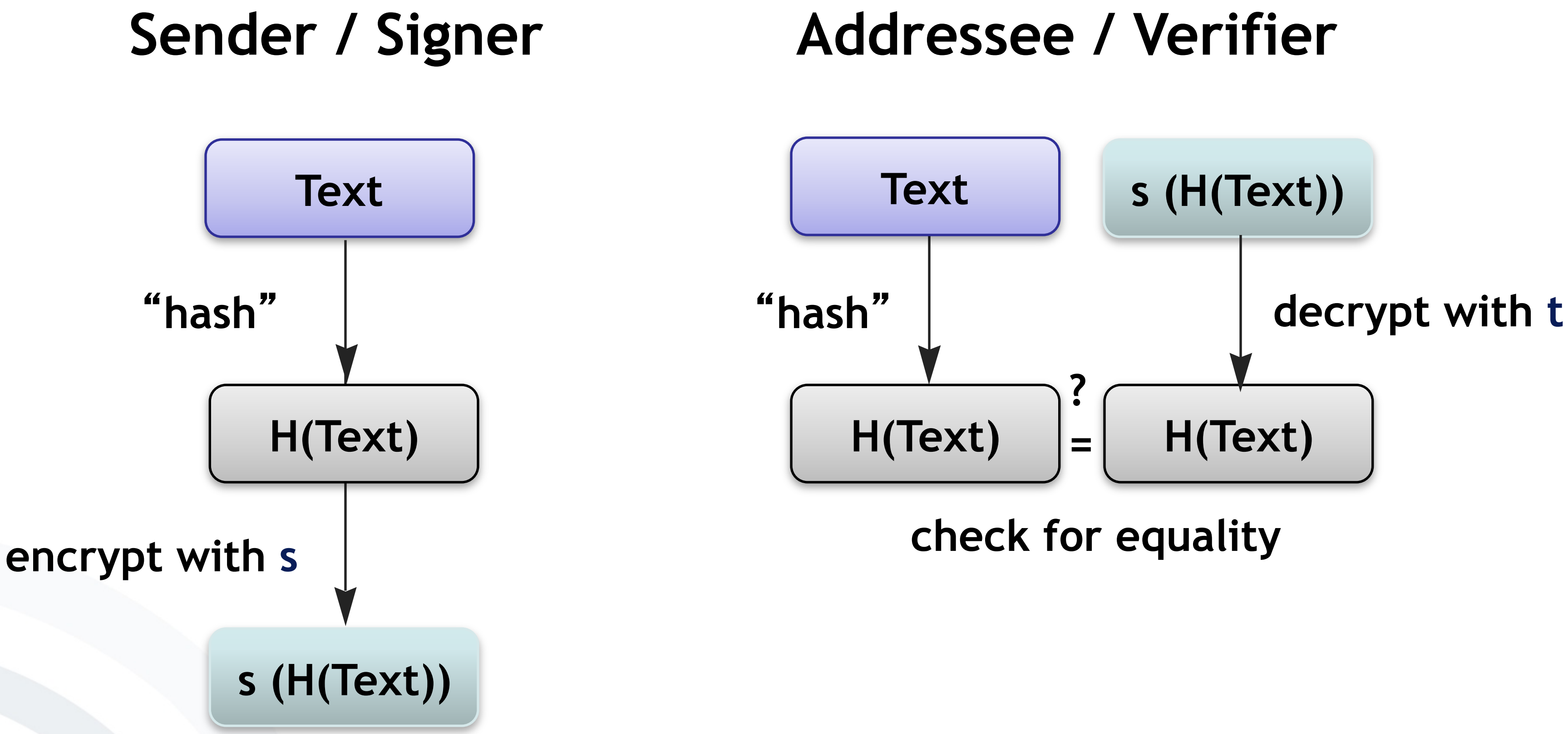
Fixed length hash (digest)

General hash functions *(H(s))*
Transformation of an input string *s* into an output string *h* **of fixed length** which is called hash value.
Example: mod 10 in the decimal system

Question 17

- *Could you explain again how the RSA algorithm works(S. 13-14)?*

Asymmetric Signature System (Example RSA)

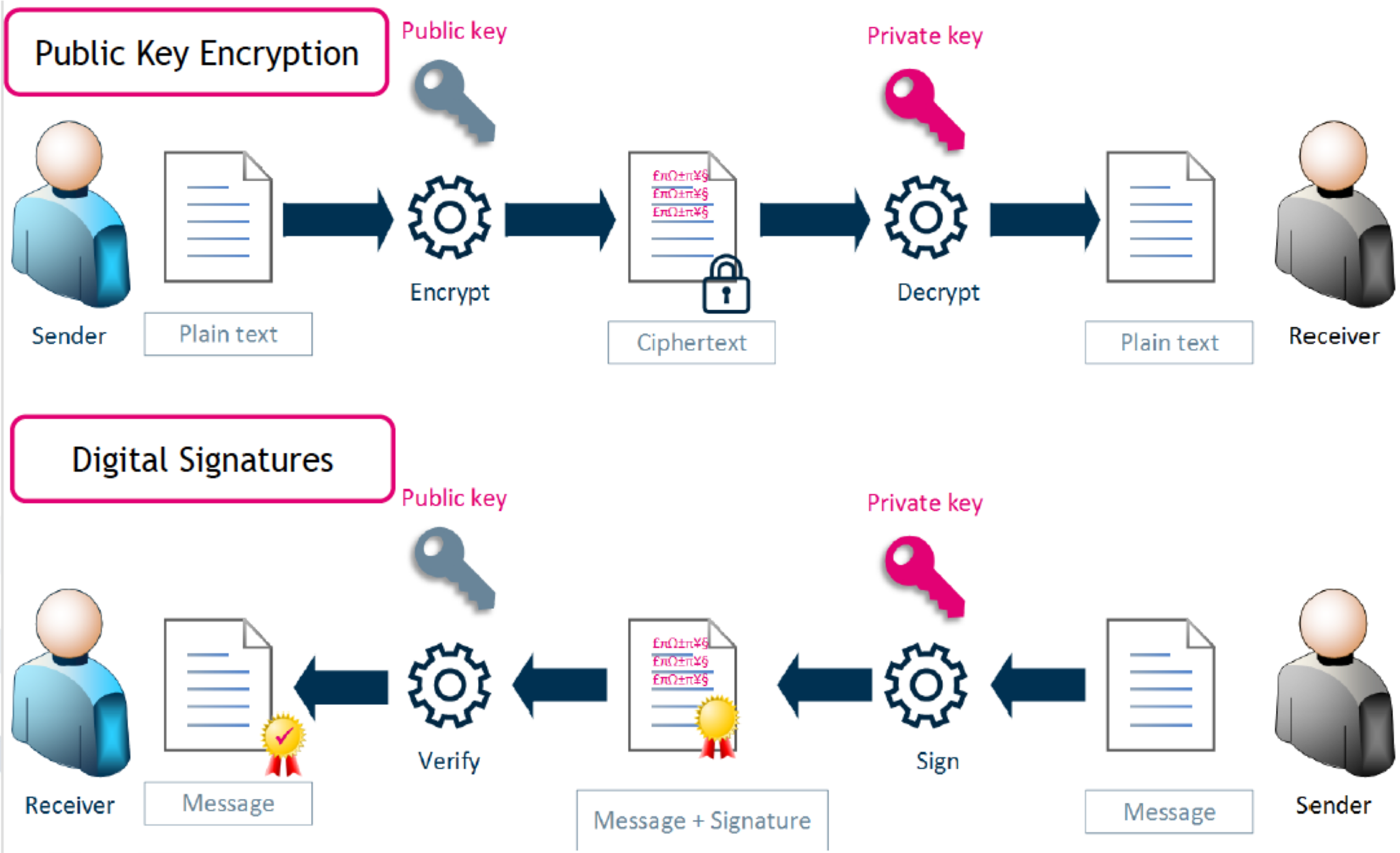


- ➲ Signing key s only with the sender, test key t public
- ➲ Example is often mistakenly generalized.

Question 18

- *slide 6, is it correct that I explain the digital signature as " using the private key to generate the message and the signature, then receiver verify the document with public key", one addition question on top of that, whose public is it? the sender's or receiver's?*

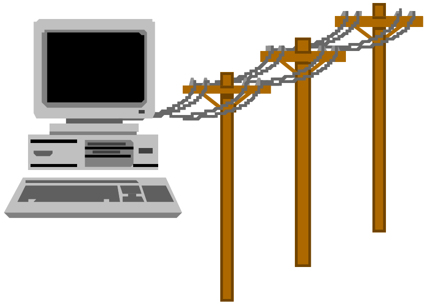
Asymmetric Signature System



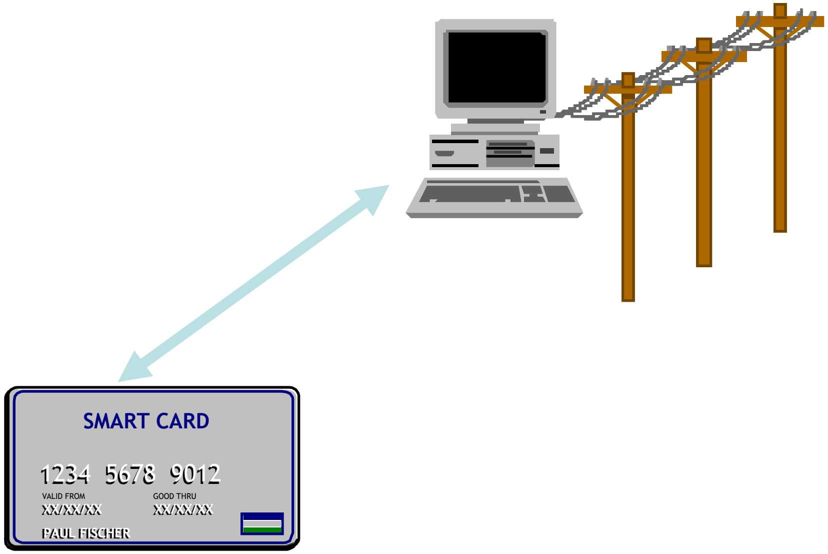
Question 19

- *slide 39, could you explain again the idea behind?*

Secure Equipment: Threats from Trojan Horses



Private key on HD, in memory



Private key and signature function in chip card

Question 20

- *slide 47-48, it's mentioning the secure element, in slide 47, it said that " secure elements are hardware tokens", does it refers to slide 48, the 3 things?(embedded secure element, mSD karte, UICC karte)?*

Tech & Sys | Secure Element

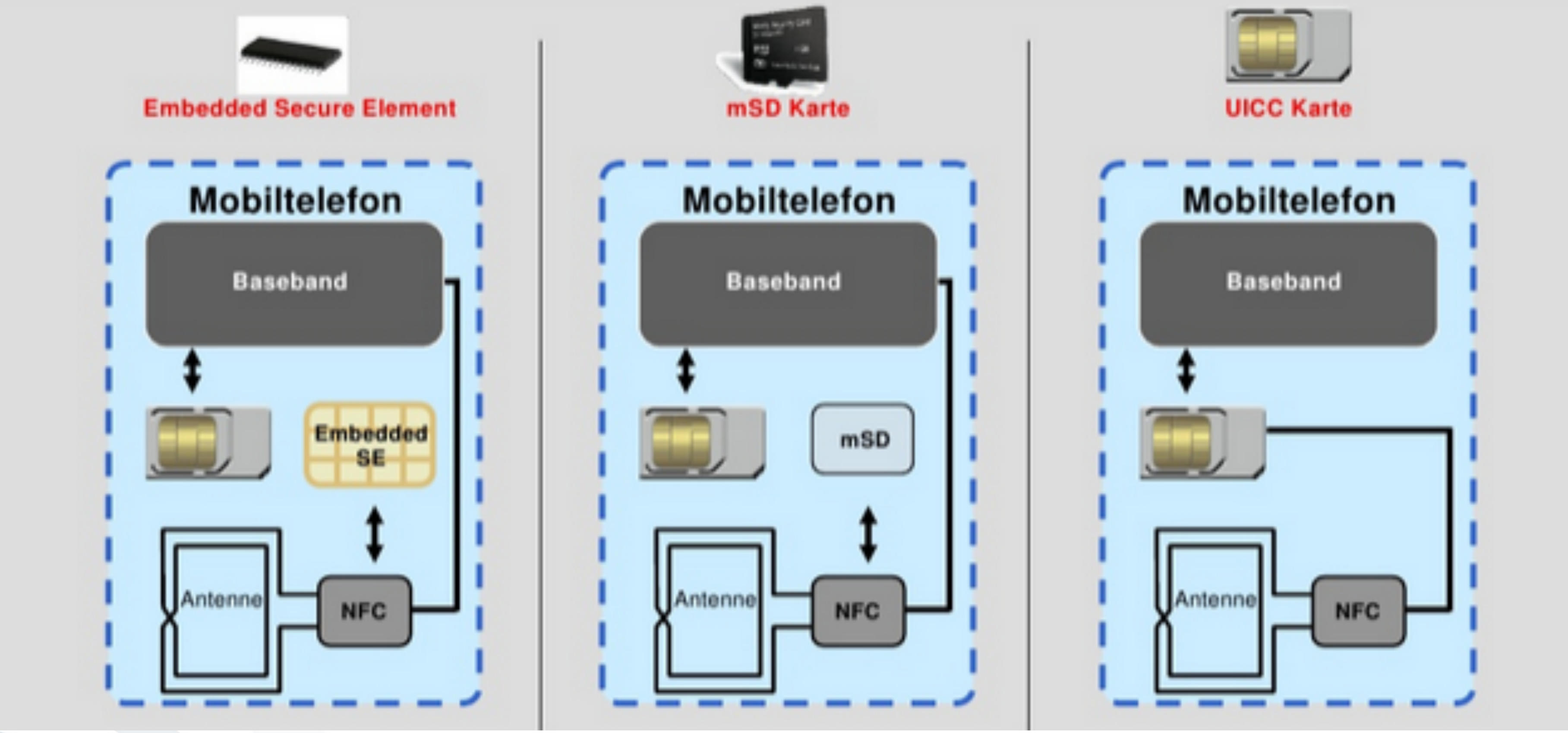
Overview 1

- The combination of NFC and secure elements on smartphones is the key technological enabler for **mobile wallets**.

- Secure elements are hardware tokens, that enable secure mobile applications, services and payments.

- They can be provided as:
  - integrated non-replaceable hardware components or
  - interchangeable hardware such as UICCs or mSD

Tech & Sys | Secure Element Overview 2



Source: Giesecke & Devrient GmbH

Lecture 7

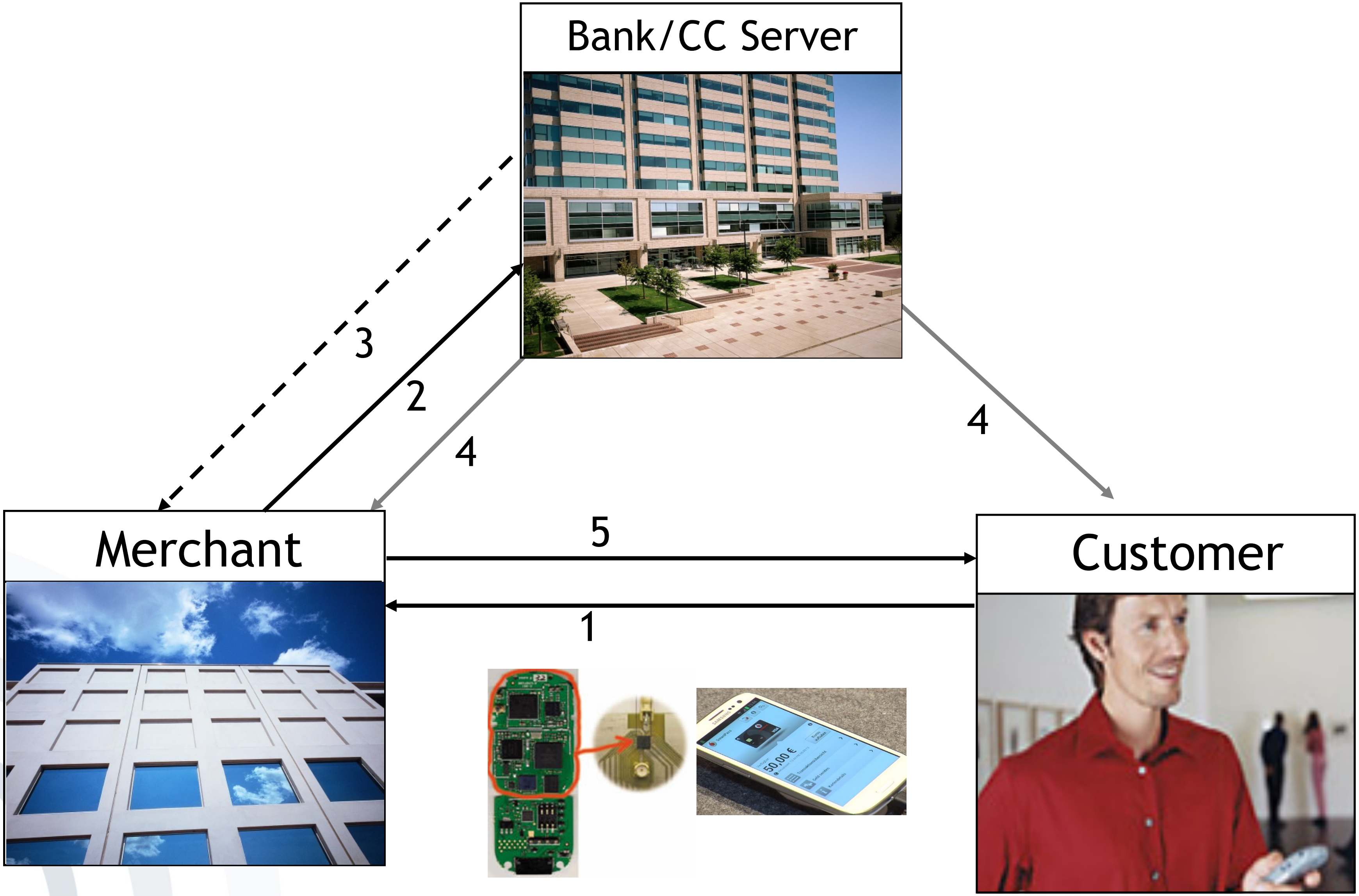
Question 21

- *What is the difference between a handset wallet and a server wallet?*

mobile business

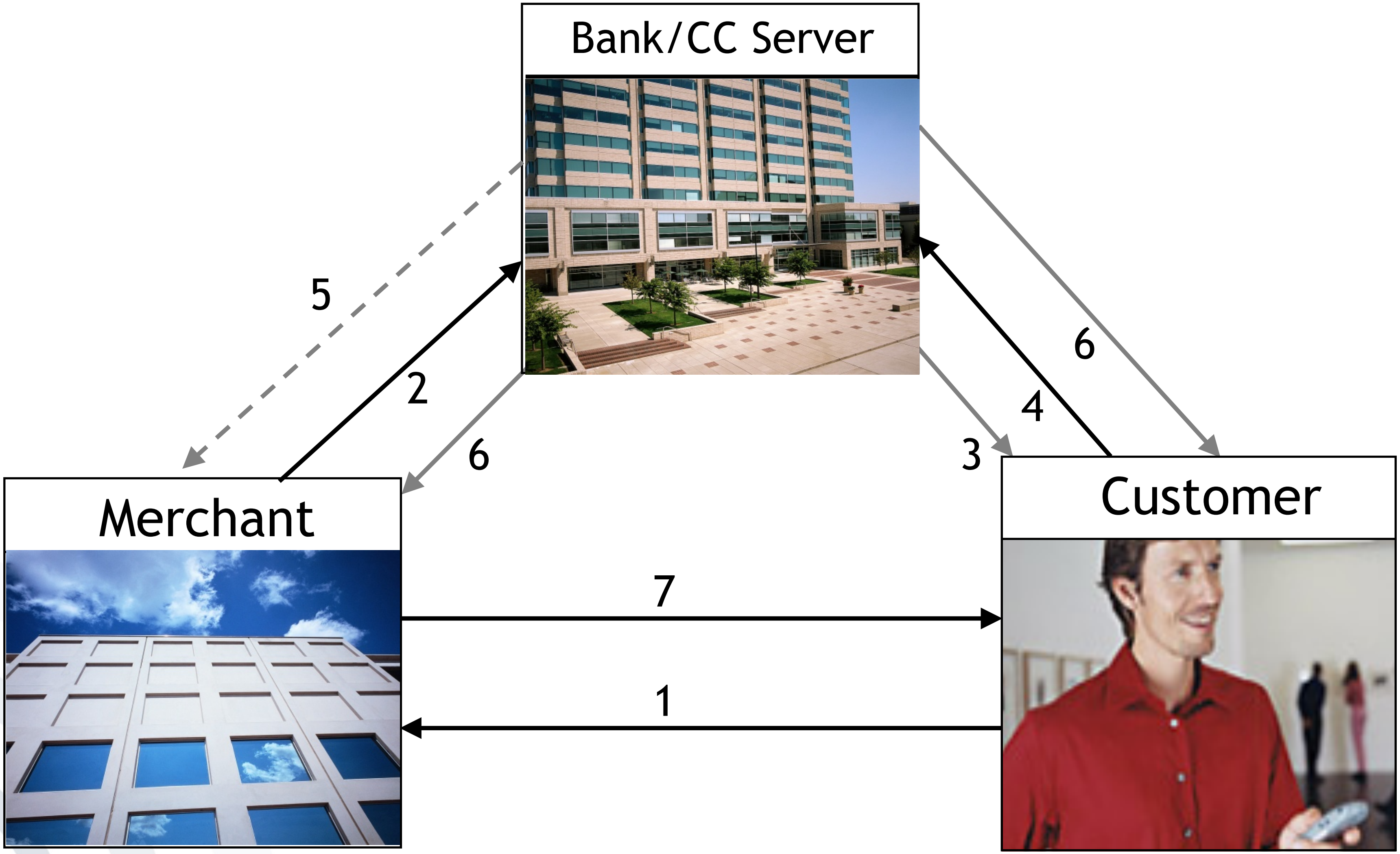
M-Payment Infrastructures

Transactions processed by Banks (Handset Wallet)



M-Payment Infrastructures

Transactions processed by Banks (Server Wallet)

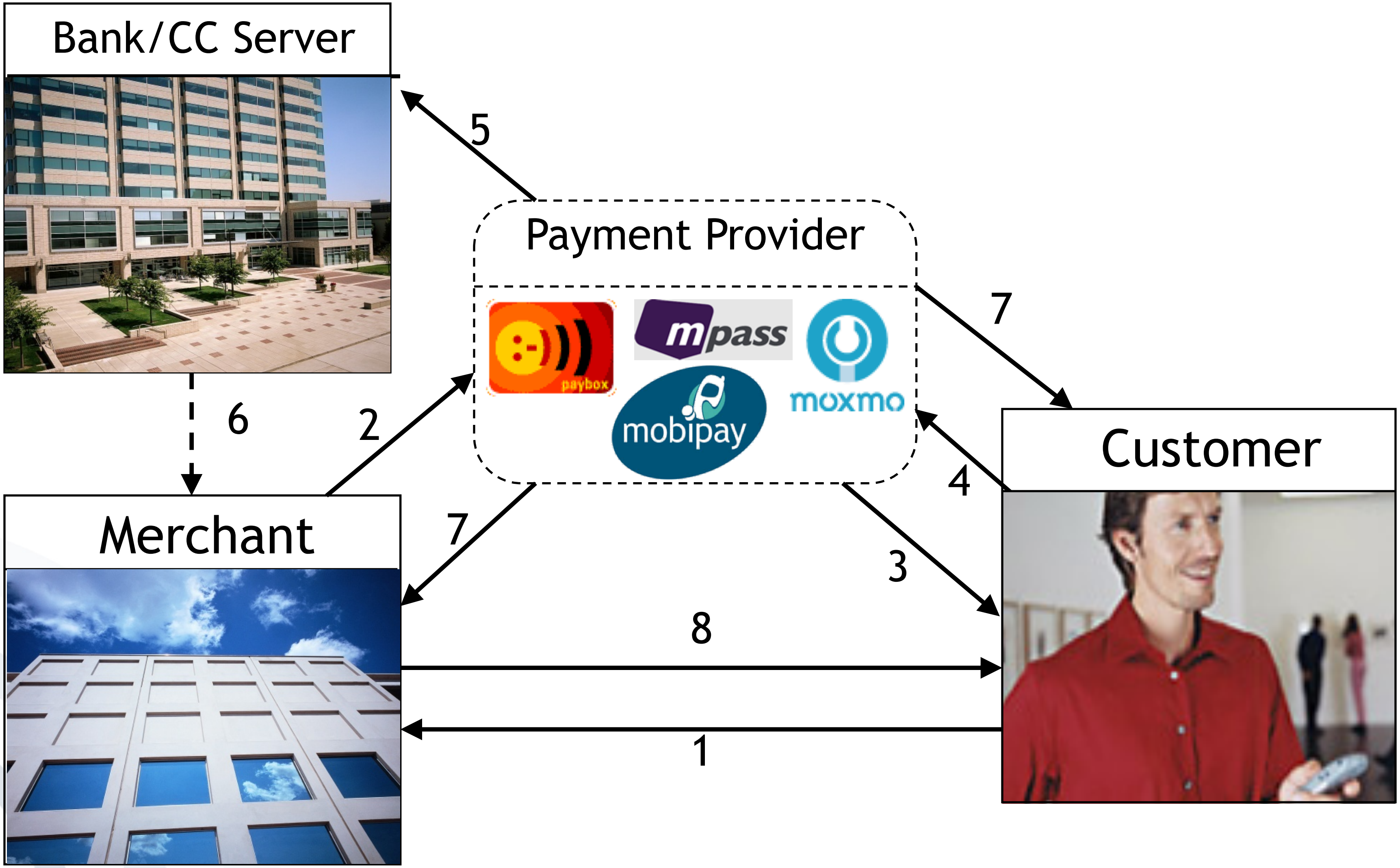


Question 22

- *What is the difference between payment providers and payment intermediaries?*

M-Payment Infrastructures

Transactions processed by Payment Providers



Bank/CC Server

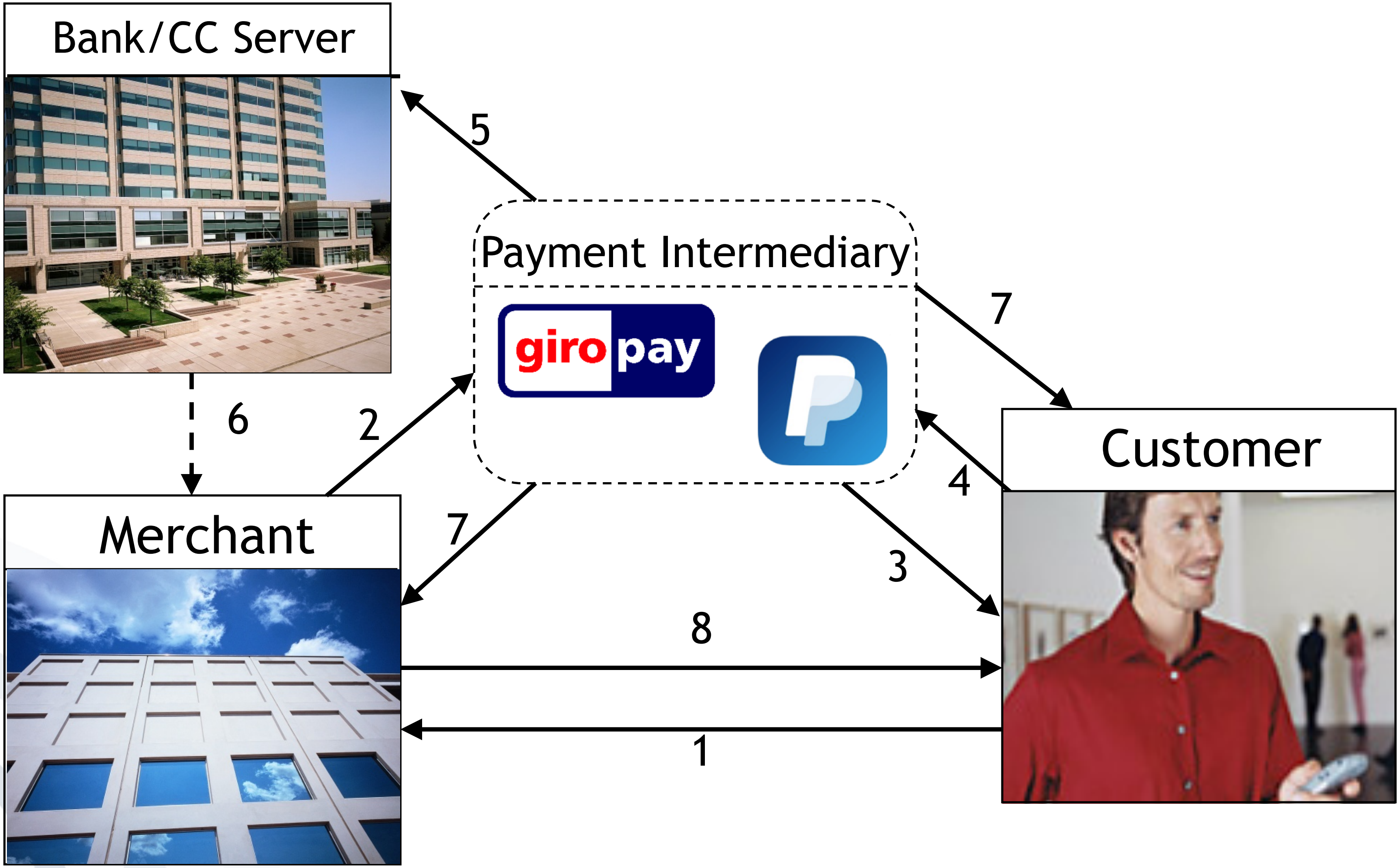
Payment Provider

Merchant

Customer

M-Payment Infrastructures

Transactions processed over Intermediaries



Question 23

- *slide 30, what are the payment providers mean? also what's the difference between payment providers and payment intermediaries (paypal)?*

Question 24

- *Slide deck 7, page 27 - 37*
  Could you please go over the different m-payment infrastructures? What aspects should we keep in mind?

Lecture 8

Question 25

- *Please point out again the problem regarding prepaid SIM registration and what the current status is here.*

Enforced Registration of Prepaid-SIMs

- Since 1997, the Federal Network Agency demands:
  - Buyers of a Prepaid-SIM have to identify themselves by showing an official photo identification
  - The ID number of the identification document has to be stored in an adequate way by the provider
  - Name and address according to the proof of identity, the related number as well as other identification credentials for telecommunications have to be transferred to the directory immediately (§ 90(1) TKG).
  - The telecommunication services may only be activated once the identification process is finalised.
- Providers took legal actions:
  - Won at first instance
  - Lost at second instance
  - Won at third instance

  ➲ Finally, the law was changed.

Prepaid-SIM Conflicts and beyond

- Increased information surveillance not in proportion with the investigations' success rate? [AlDK03]
- Telecommunications data retention
  - Without an explicit cause, telecommunications data retention is unacceptable and unconstitutional according to the Federal Constitutional Court of Germany (BVerfG, 1 BvR 256/08, 2.3.2010).
- Prepaid-SIM registration is required by the legislator.
- Ineffectiveness of these measures due to foreign anonymous prepaid cards?
- In future: Who controls and surveys the location data?

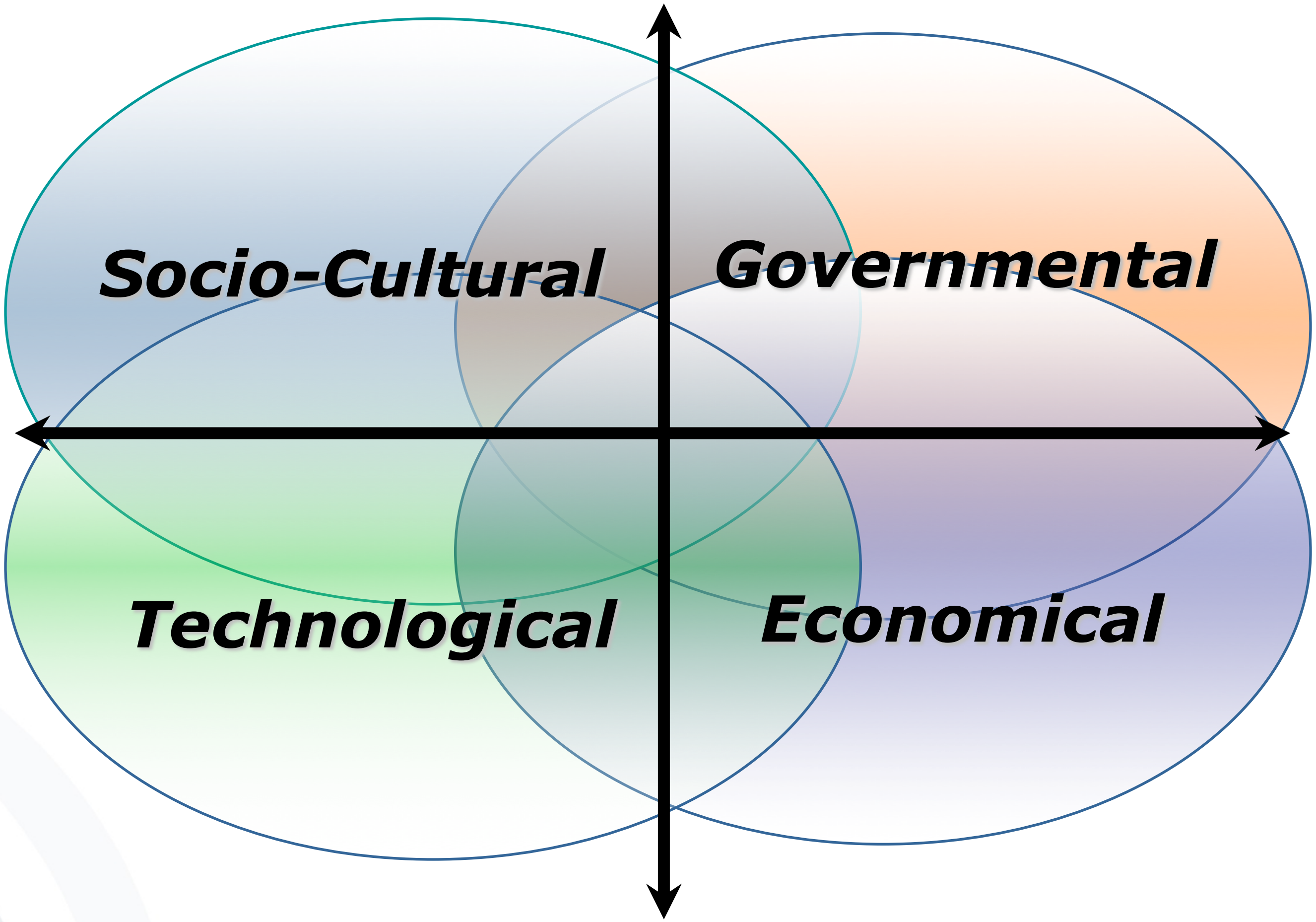
Question 26

- *Pls explain again Lecture 8, slides 98 to 106 about the interdisciplinary Aspects Dimension*

Agenda

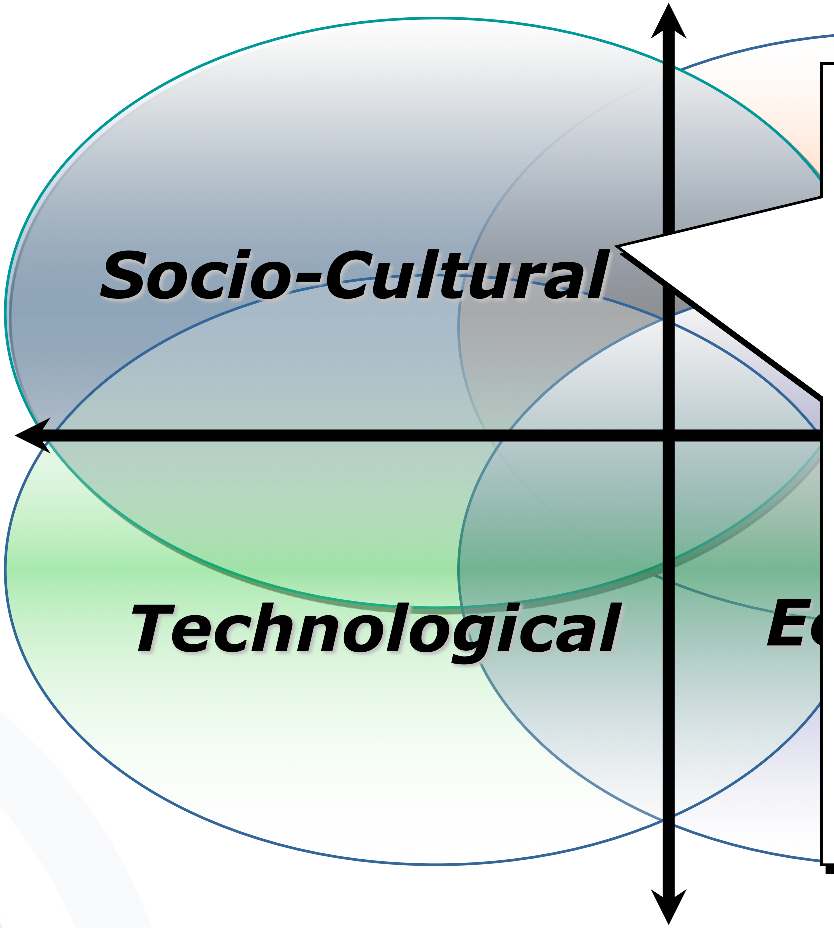
- Surveillance
  - Legitimation and types of surveillance
  - Public Agencies ("Bedarfsträger") and their control
  - Legal foundations
  - Practical implementation
  - Legal conflicts
- Data Protection & privacy
  - Terminology and background
  - Applications in the telecommunications area
  - (National) implementation
- Identity & mobile identity
  - Identity concepts
  - Identity management
  - Interdisciplinary aspects of mobility and identity

Interdisciplinary aspects of Mobility and Identity



Source: **[RR2006]**

Interdisciplinary Aspects
Dimension: Socio-Cultural



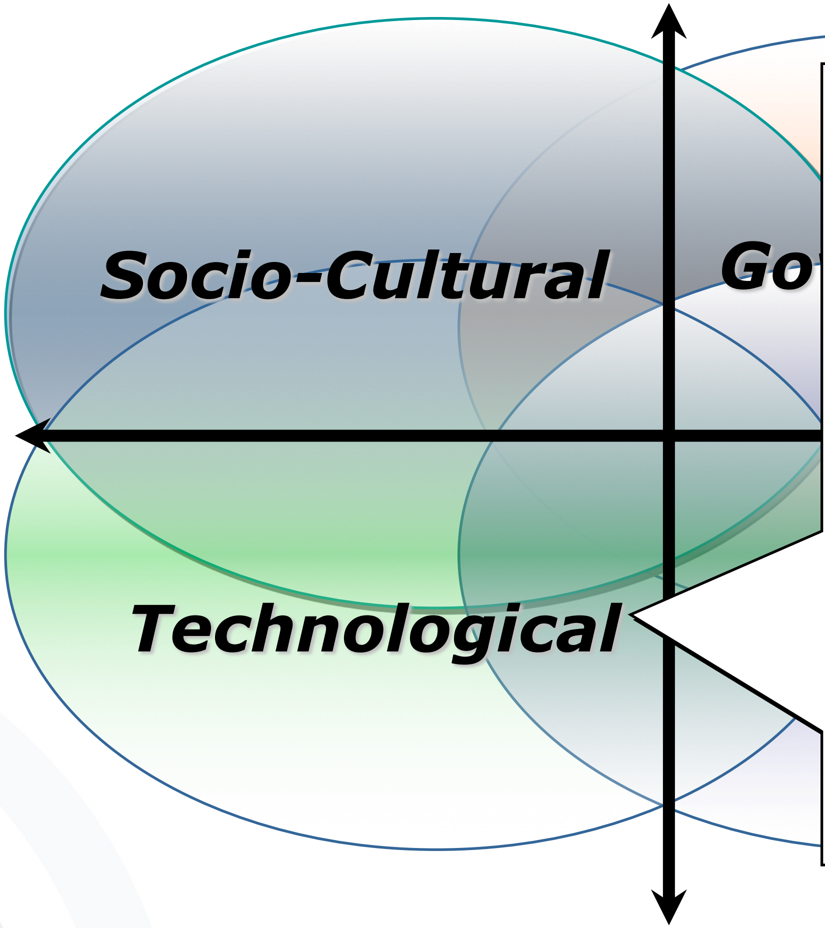
- Group dynamics
- Awareness
- Trust
- Right of Privacy
- Perceived freedom

Socio-Cultural Impacts

- ***Concepts being observed***
  - ***Idem Identity***, categorisation
  - ***Ipse Identity***, sense of self

- Analysis of conceptual and sociological issues of the impact of idem-identification on ipse-identity, in the case of mobile devices
  - E.g.: how someone establishes communication using mobile devices
  - E.g.: how we/others perceive ourselves/us

Interdisciplinary Aspects Dimension: Technological



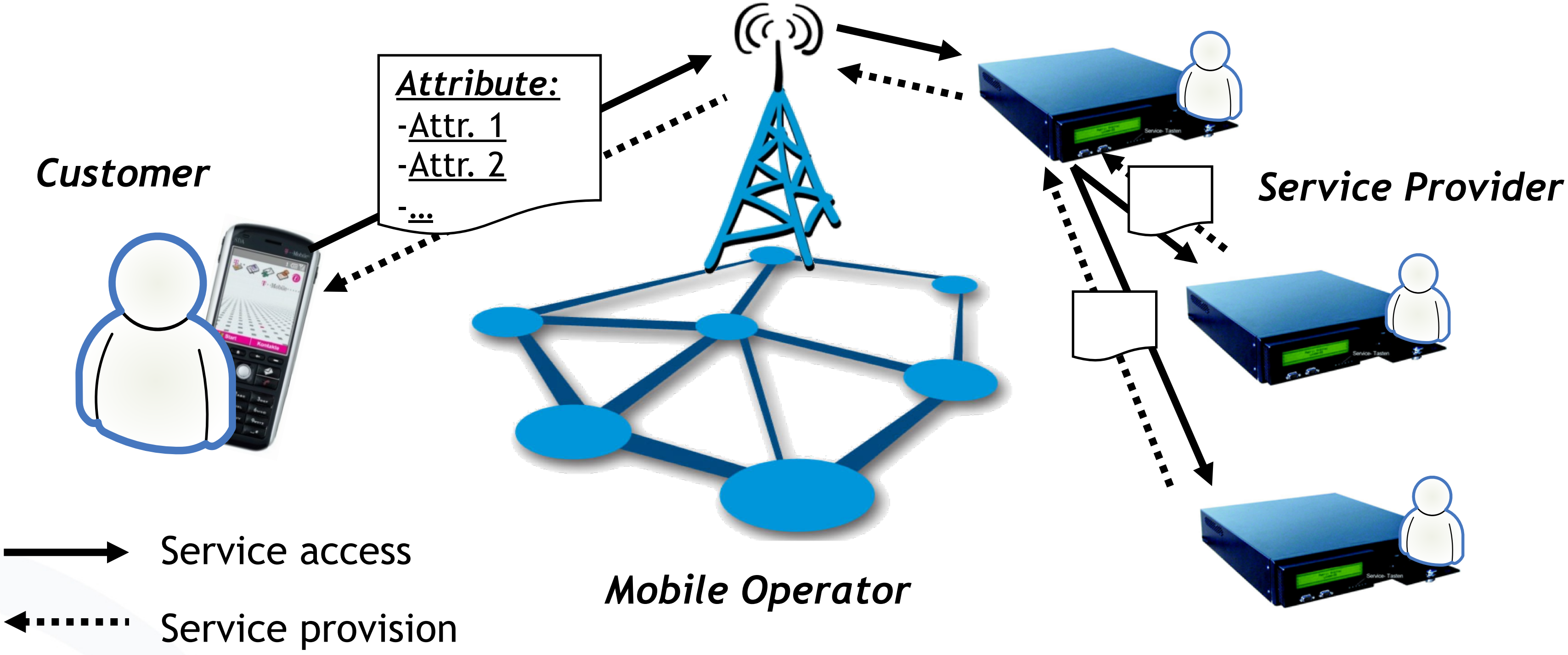
- Technologies
  - PETs
  - Protocols
  - Network Access
- Interoperability
- Standards

Mobile Identity Management

- Management of identities through the use of mobile devices
  - Management of social interactions in life, rather than Management of mobility

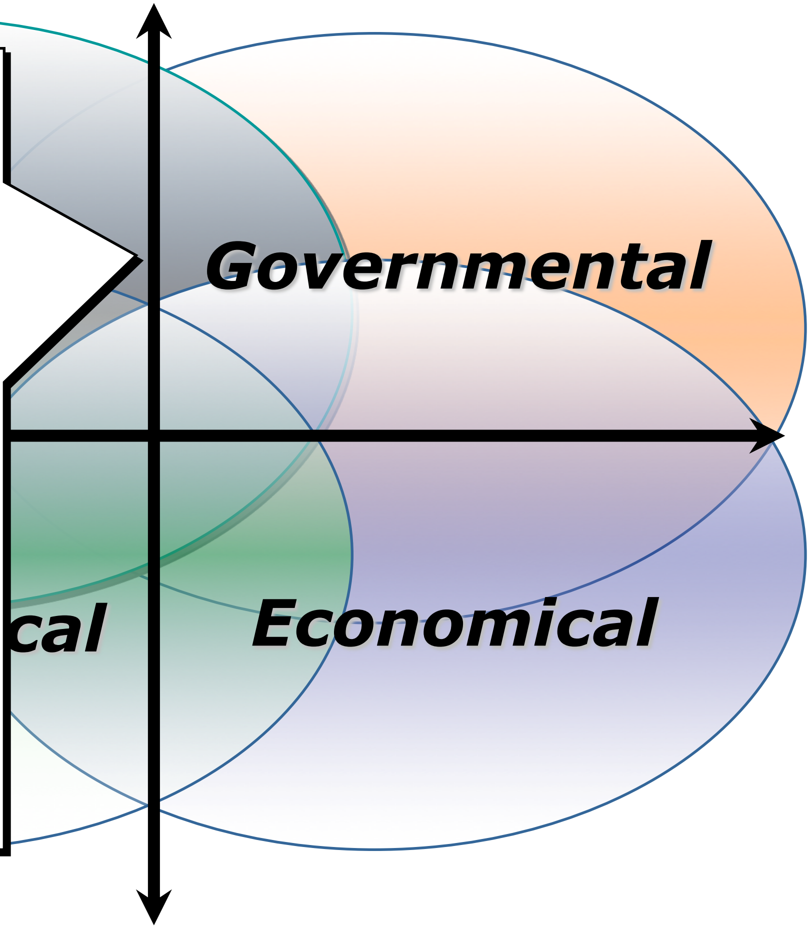
- Management of Mobile Identities
  - Usage of location data

Transfer of Attributes

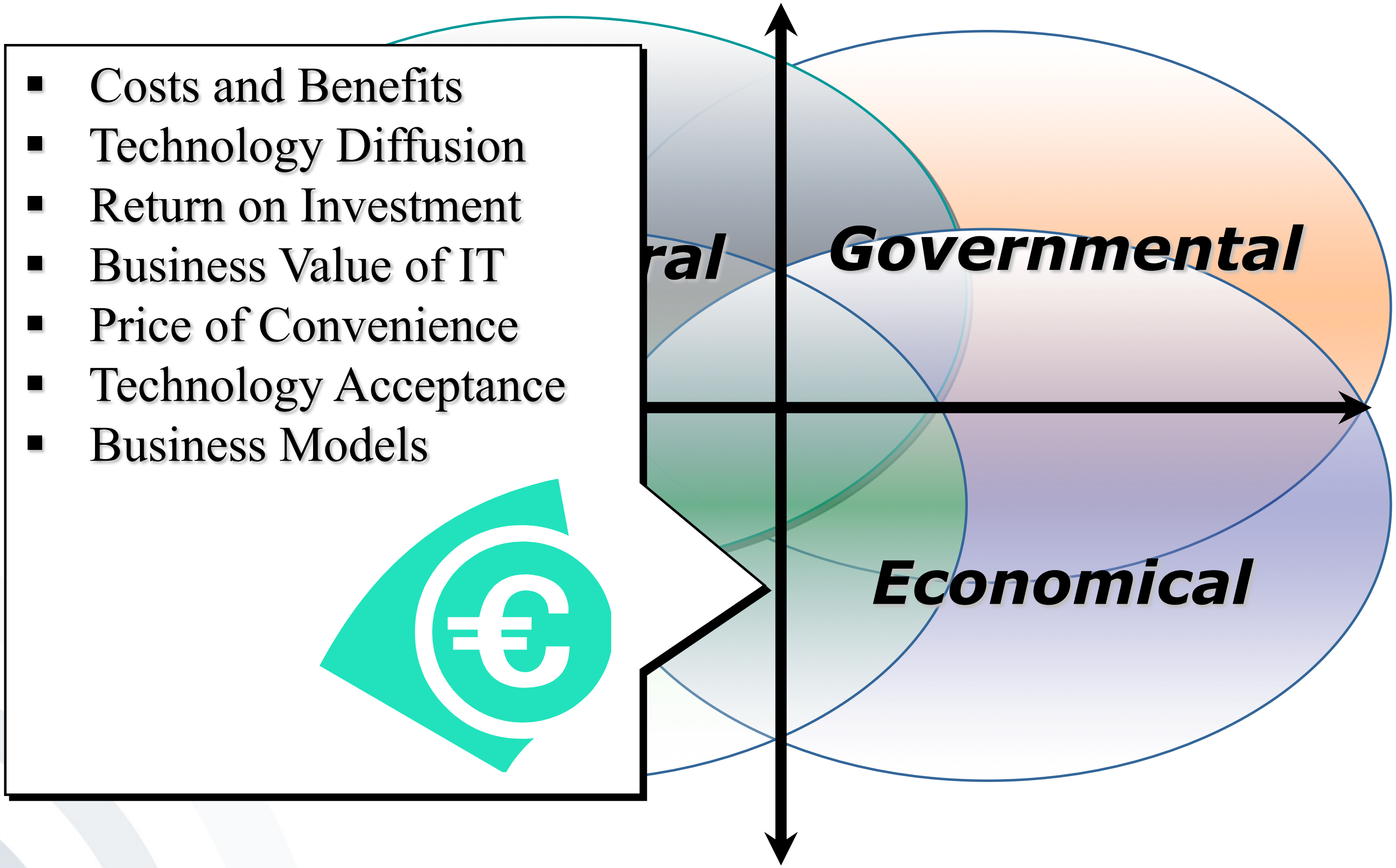


Interdisciplinary Aspects Dimension: Governmental

- Laws
- Directives
- Regulations



Interdisciplinary Aspects
Dimension: Economical



- Costs and Benefits
- Technology Diffusion
- Return on Investment
- Business Value of IT
- Price of Convenience
- Technology Acceptance
- Business Models

Design Principles for mobile Identity Management

- General success factors:
  - Locality principle
  - Reciprocity principle
  - Principle of understanding

- Protecting the privacy of a user:
  - User controlled linkage of personal data
  - Data minimisation
  - Awareness of data being disclosed
  - Sufficient usability towards the user

Question 27

- *Pls explain again Lecture 8, slides 30 about the Costs of Surveillance: Connection-queries*

Costs of Surveillance

Connection-queries search account databases

- **Example:** „All calls to phone number ***n*** at the point of time ***t***“ searches the complete account database (due to data protection data is stored as „***a*** *calls* ***n*** *at time* ***t***“).

➲ ***Results in tremendous costs for the servers and the database licences.***

The interception of phone-calls causes costs:

- Provision of online access
- Purchasing of cryptography hardware (Elcrodat) and maintenance personnel with security clearance
- 24h-availability of the infrastructure

Question 28

- *Pls explain again Lecture 8, slides 38 about Prepaid-SIM conflicts and beyond*

Prepaid-SIM Conflicts and beyond

- Increased information surveillance not in proportion with the investigations' success rate? [AlDK03]
- Telecommunications data retention
  - Without an explicit cause, telecommunications data retention is unacceptable and unconstitutional according to the Federal Constitutional Court of Germany (BVerfG, 1 BvR 256/08, 2.3.2010).
- Prepaid-SIM registration is required by the legislator.
- Ineffectiveness of these measures due to foreign anonymous prepaid cards?
- In future: Who controls and surveys the location data?

Lecture 9

Question 29

- *To what extent are the legal foundations and EU directives important for the exam? Do we need to know each of these regulations and their content?*

Question 30

- *Slide deck 9, page 26-27*
  To what extend should we know about the "Regulation in Germany - services and relevant regulation"? Should we - for example - know, which relevant laws have been passed and the corresponding regulation measures?

Regulation in Germany

Actors in Regulation

Means	Responsibility
Law	Parliament (“Bundestag”)
Ordinance	Government
Ordinance / Decree	Ministry / Department
State treaty	State governments
Licensing	Authority (e.g. Federal Network Agency)
Supervision	

Regulation in Germany

Services and relevant Regulation

	Technical Services	Content Services		
Service Category	Telecommunication Services	Voice Telephony and Annex Services	Tele & Media Services	Broadcast
Relevant Law	Telekommunikations-gesetz (TKG)	Telekommunika-tionsgesetz (TKG)	Telemediengesetz (TMG)	Rundfunkstaatsvertrag (RSTV)
Holder of Competence	Federation (Bund)	Federation (Bund)	Federation (Bund)	Federal states
Regulation Measures	Limited economic freedom: universal service duty, tariff regulation, control competence of the federal state's media institutes over the broadband cable network, mobile number portability	Limited economic freedom: license obligation; ex-ante tariff control	Economic freedom: no mandatory admission and registration, no supervision	No economic freedom; broadcast freedom (Rundfunkfreiheit) as institution; dual system
Specific Responsible Institutions	Federal Network Agency	Federal Network Agency	none	Supervision bodies of the broadcasting institutions; state media institutions as well as KEF and KEK

Based on: **[Siemer2003]**

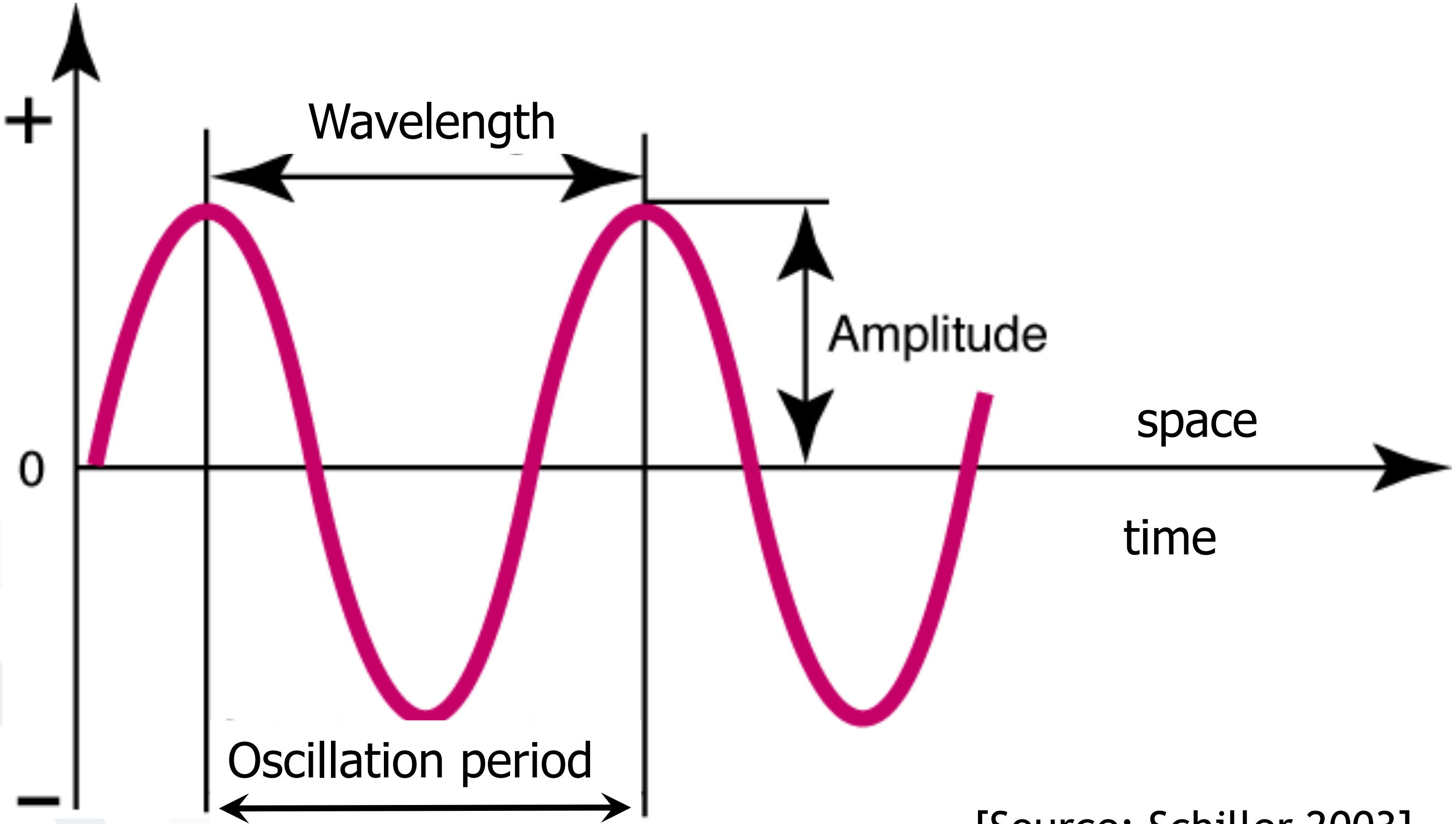
Lecture 10

Question 31

- *Could you pls explain again Lecture 10, slides 11 to 17 about the process of the auction including the Excursion: Frequencies?*

Excursion: Frequencies & Co |1

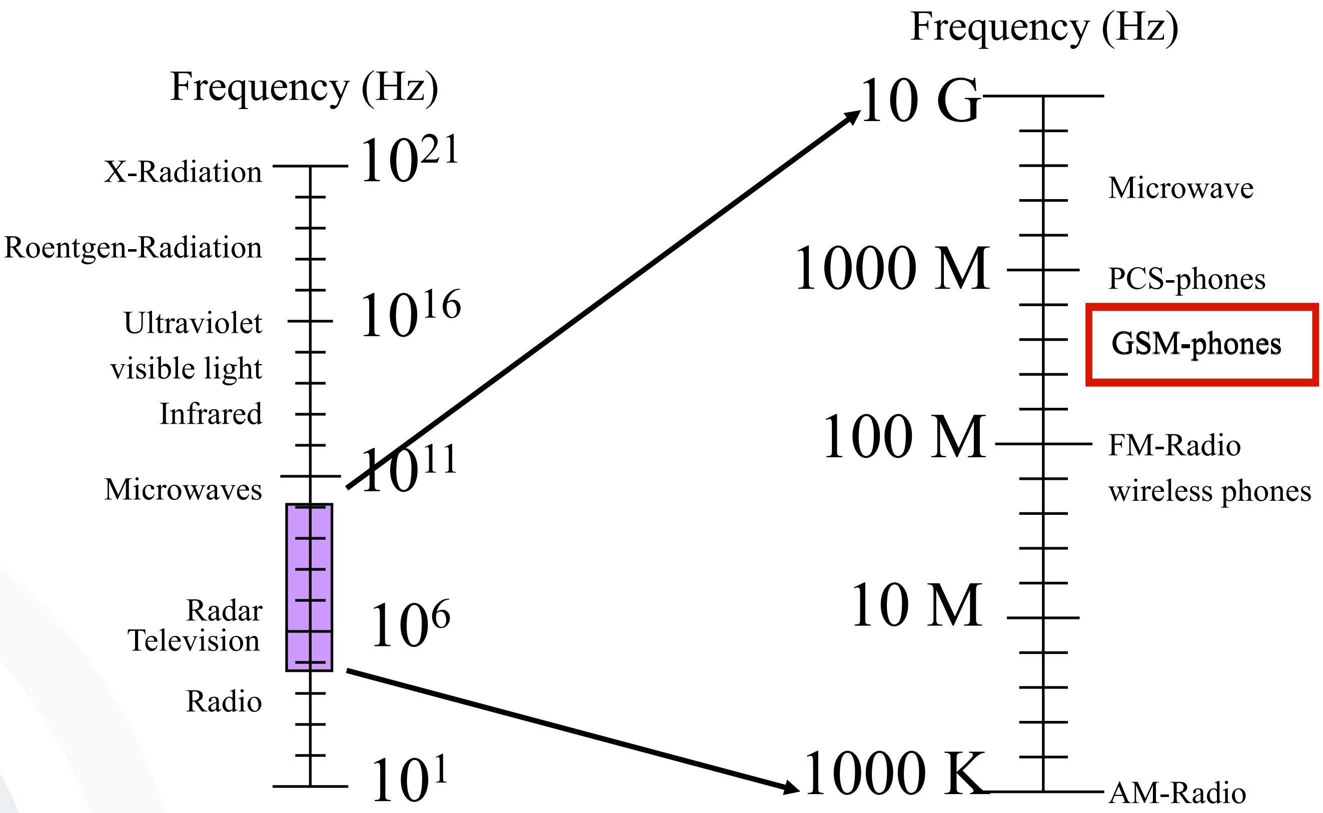
- **Electromagnetic waves and frequencies**



[Source: Schiller 2003]

Excursion: Frequencies & Co |2

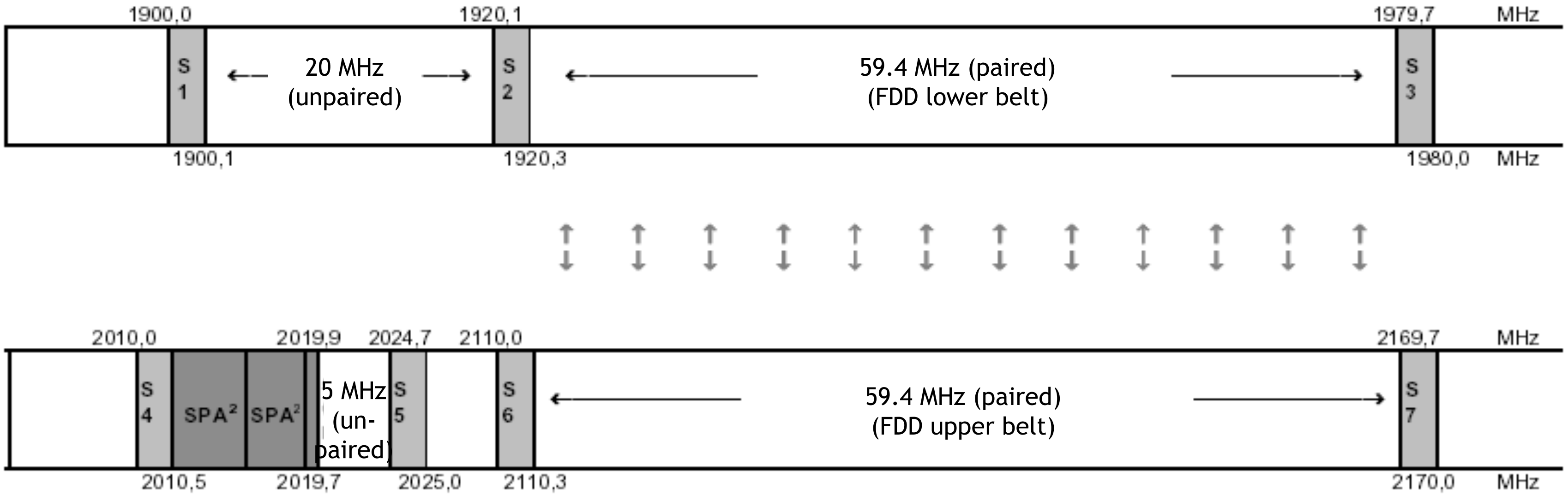
- **Frequency range of entertainment and communication electronics**



Excursion: Frequencies & Co |3

UMTS/IMT-2000 channel plan for the frequency areas 1920–1980 MHz, 2010–2025 MHz and 2110–2170 MHz (in accordance to ERC/DEC(99)25)

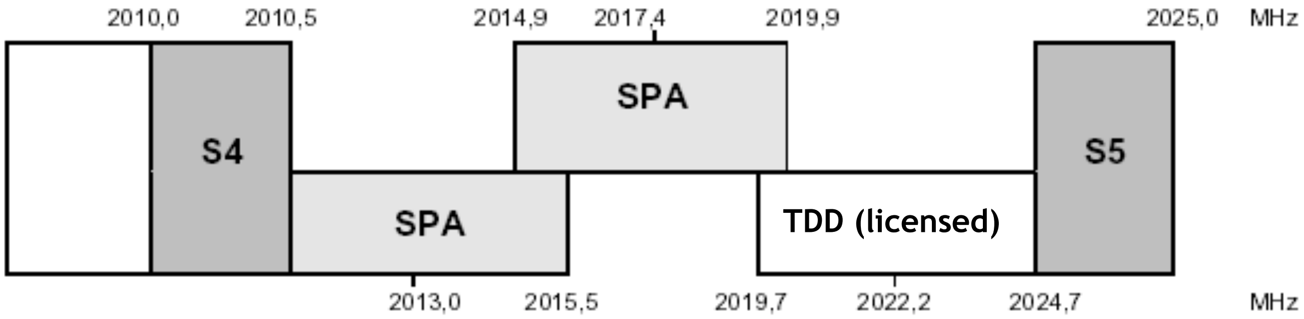
- **FDD Spectrum:** Sending frequencies for mobile stations in FDD mode (1920 – 1980 MHz),
  Sending frequencies for basis stations in FDD mode (2110 – 2170 MHz)
- **TDD Spectrum:** Sending frequencies for mobile and basis stations in TDD mode (1900 – 1920 MHz, 2010 – 2025 MHz), the lowest two TDD frequency blocks of the area 2010 – 2025 MHz are reserved for public domain applications (SPA)[1] according to ERC/DEC(99)25.



[1] Public domain applications (SPA = Self provided applications operating in a self coordinated environment)
[2] Reserved for public domain applications (SPA) according to ERC/DEC(99)25

Excursion: Frequencies & Co |4

Detailed fragmentation of the frequency range between 2010 MHz and 2025 MHz



Process of the Auction | 4

- 2 x 60 MHz (paired) and 1 x 25 MHz (unpaired) available.
- Two auction stages

- 1st Stage:
  - Licences are offered whose frequency equipment amounts at least 2 x 10 MHz (paired) and at most 2 x 15 MHz (paired).
  - Hence the **amount of the licenses** which are up for auction in the first stage amounts **between four and six** depending on the demand of frequency blocks and the actual bidding behaviour of the candidates.
  - The spectrum of 2 x 60 MHz (paired) is offered in 12 abstract blocks, each per 2 x 5 MHz (paired).

Process of the Auction | 5

- 2nd Stage:
  - **Five blocks** of 1 x 5 MHz unpaired spectrum and any blocks of 2 x 5 MHz paired spectrum not bought in the first stage shall be auctioned.
    - Block one to four: 1 x 5 MHz unpaired spectrum shall be offered as abstract frequency blocks, i.e. with no defined spectral position.
    - Fifth block shall be offered with a defined spectral position.
- If, at the close of the bidding proceedings, there is no valid bid for a frequency block or if a bidder is the highest bidder for one frequency block only, the block shall not be awarded in the first stage. The unbought spectrum shall be auctioned in the second stage in blocks of 2 x 5 MHz among the successful bidders from the first stage, together with the other auctionable (unpaired) spectrum.
- Only those bidders are admitted to the participation in the second stage who have purchased licences by auction in the first stage.

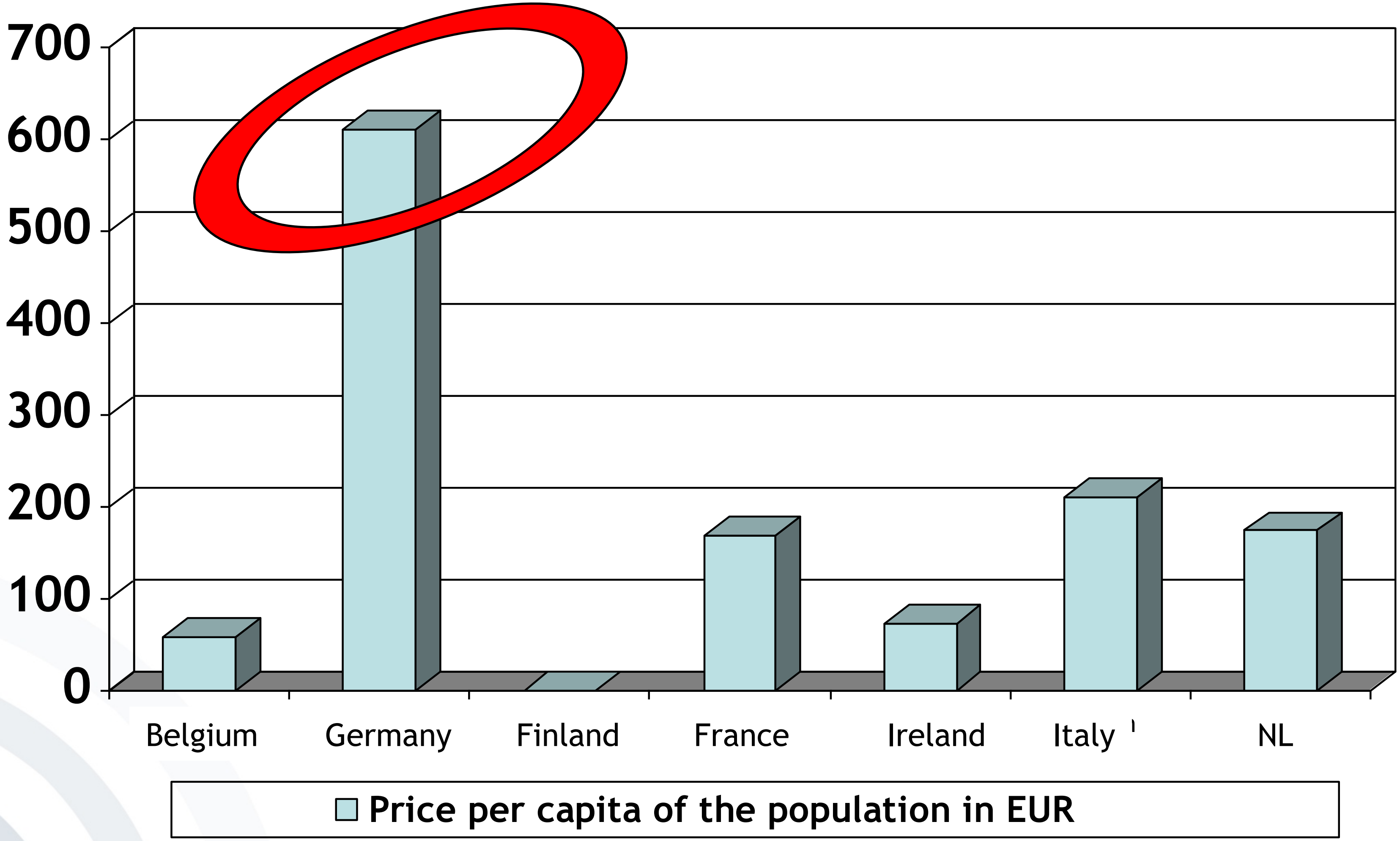
Process of the Auction | 6

- The bidding rights in the first stage are limited to at least 2 x 10 MHz (paired) and at most 2 x 15 MHz (paired).
- Unpaired frequencies can be purchased by auction (in the second stage) without limitation.
- Minimum bidding in the **1st stage**
  - For one licence with a basis equipment of 2 x 10 MHz (paired) 200 million DM/102.258 million EUR,
  - For one licence with an equipment of 2 x 15 MHz (paired) 300 million DM/153.387 million EUR.
- Minimum bidding in the **2nd stage**
  - 50 million DM/25.565 million EUR per 1 x 5 MHz frequency block unpaired,
  - As far as a paired frequency spectrum is auctioned in the second stage the minimum bidding per 2 x 5 MHz frequency block (paired) amounts 100 million DM/51.129 million EUR.

Question 32

- *Slide deck 10, page 52, 78*
  Why did companies bid for UTMS? What's so special about it or what were the special circumstances? Why were the bids so high especially in Germany and UK?

International UMTS Licensing |2



Summary, consequences, and outlook|1

- UMTS licence payments in 2000 were initially excessive.
- Network expansion obligations of 800 MHz auctions in 2010 have already increased network coverage in rural areas.
- Digital Agenda of the Federal Government has led to stricter coverage and bandwidth obligations for operators in 2015 auction.
- The 5G auction in 2019 resulted in 6,549,651,000 €.
- Not all coverage obligations are being fulfilled by licensed operators.

https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Frequenzen/OeffentlicheNetze/Mobilfunknetze/mobilfunknetze-node.html

Exam related

Question 33

- *I have a question regarding slides marked as "Annexes".*
  Are they exam relevant or not?

- *Should we expect some computations on the exam?*

Question 34

- *What is your opinion for questions 5B and 5C in 2015 old exam?*
- *5B: Please make your point on whether a harmonized (unified) European data protection law is necessary or not. Which consequences might result from this for companies offering products and services throughout the European Union (EU)?*
- *5C: Are strict requirements together with severe fines for data controllers an appropriate measure to protect citizens against careless handling of their personal data?*

Question 35

- *In 2016 old exam, question 1D described the 9 principled of the EU privacy law which were different from those in Lecture 8 (from slides 50 to 52: GDPR Principles). If we would be asked in the exam the same question, then which principles should be written?*

Question 36

- *auf ihrer Homepage ist angegeben, dass die Prüfung auf Englisch beantwortet werden soll. (The language of the exam is English. The exam is also to be answered in English.) Nichtsdestotrotz wollte ich nachfragen, ob die Gesetze (bspw. in Kapitel 8) auf Englisch angegeben werden müssen, oder, ob wir ausnahmsweise auch die Gesetze auf Deutsch "benennen" dürfen.*
- *Also können wir anstatt "Telecommunications Traffic Surveillance Ordinance" -> Telekommunikations-Überwachungsverordnung schreiben? Oder anstatt Federal Office for the Protection of the Constitution -> Bundesamt für Verfassungsschutz? (Da es sich ja auch im Deutsche Gesetzte handelt....)*

Missed Questions

Question 33

- *1. Lecture 2, page 10 : What is difference between Network internal and external source of information about location.*

- *(Already Covered)*

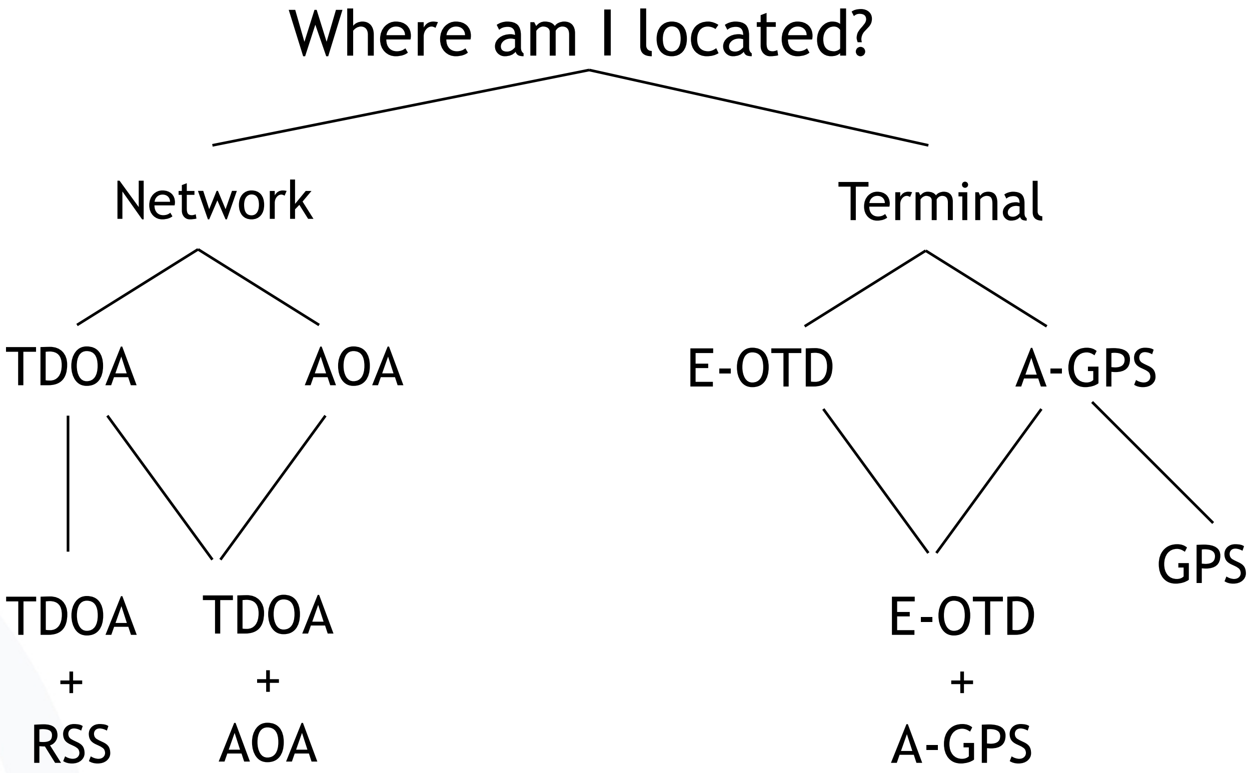
Overview Positioning Methods

- Network external source of information about location
  - User input to the device
  - Satellite Systems: GPS (USA), Galileo (EU), GLONASS (Russia)
  - Position sender (Radio, Infrared)
  - WLAN positioning
  - Peer to Peer
- Network internal source of information about location
  - Cell-ID
  - Time Difference of Arrival (TDOA)
  - Enhanced Observed Time Difference (E-OTD)
  - Angle of Arrival (AOA)
  - Signal Attenuation (SA)
- Hybrid solutions
  - Assisted GPS (A-GPS)
- Often the terminal is involved in the positioning
  - Terminal positioning
  - Hybrid positioning

Question 33

- *2. Lecture 2, page 57: Please explain Positioning Tree*

Summary: Positioning-“tree“



Where am I located?

Network

Terminal

TDOA

AOA

E-OTD

A-GPS

TDOA + RSS

TDOA + AOA

E-OTD + A-GPS

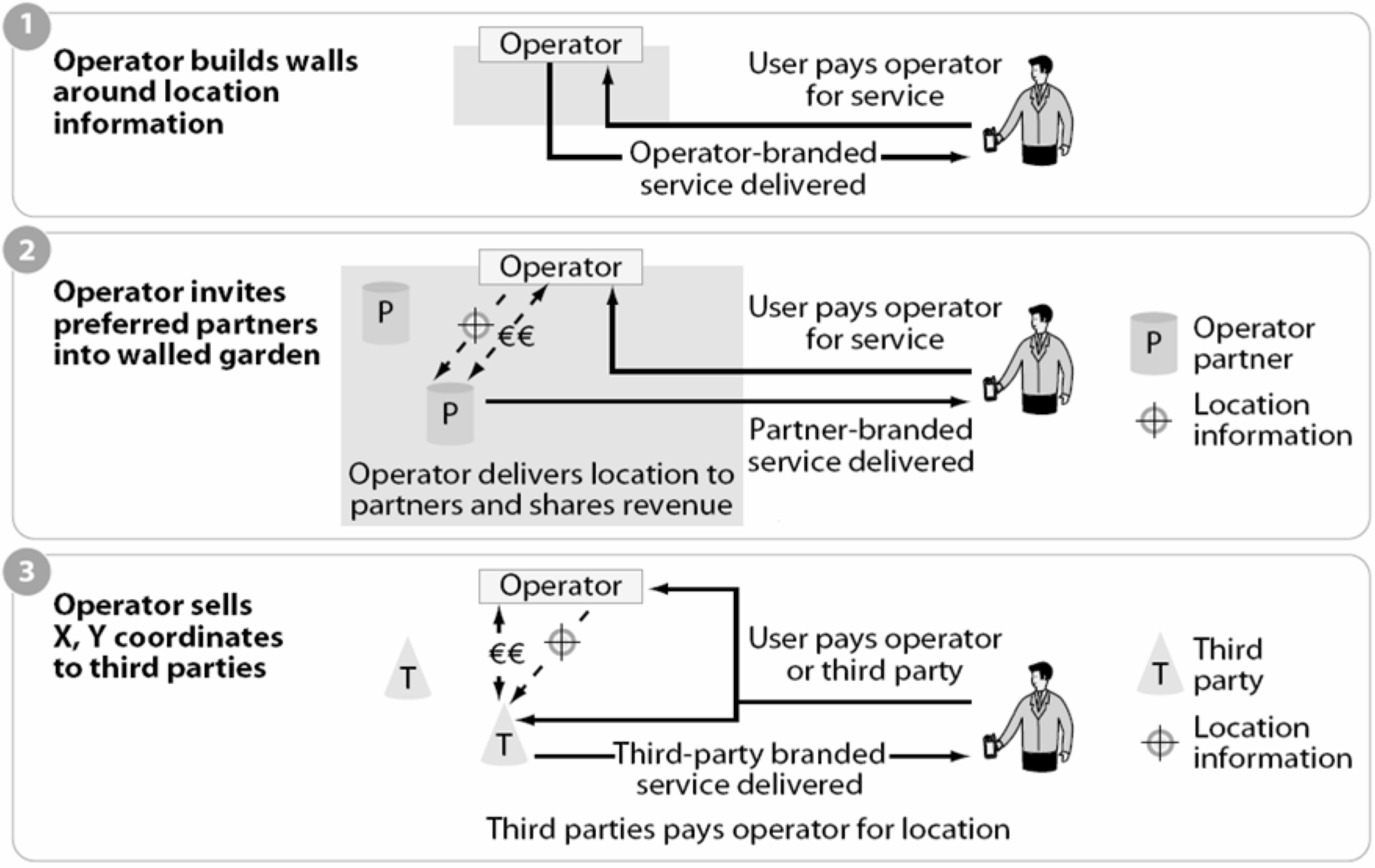
GPS

[Source: Motorola]

Question 33

- *3. Lecture 3, page 10: What is difference between 2 and 3 (Options for MNOs)*

Options for the Mobile Network Operator (MNOs)

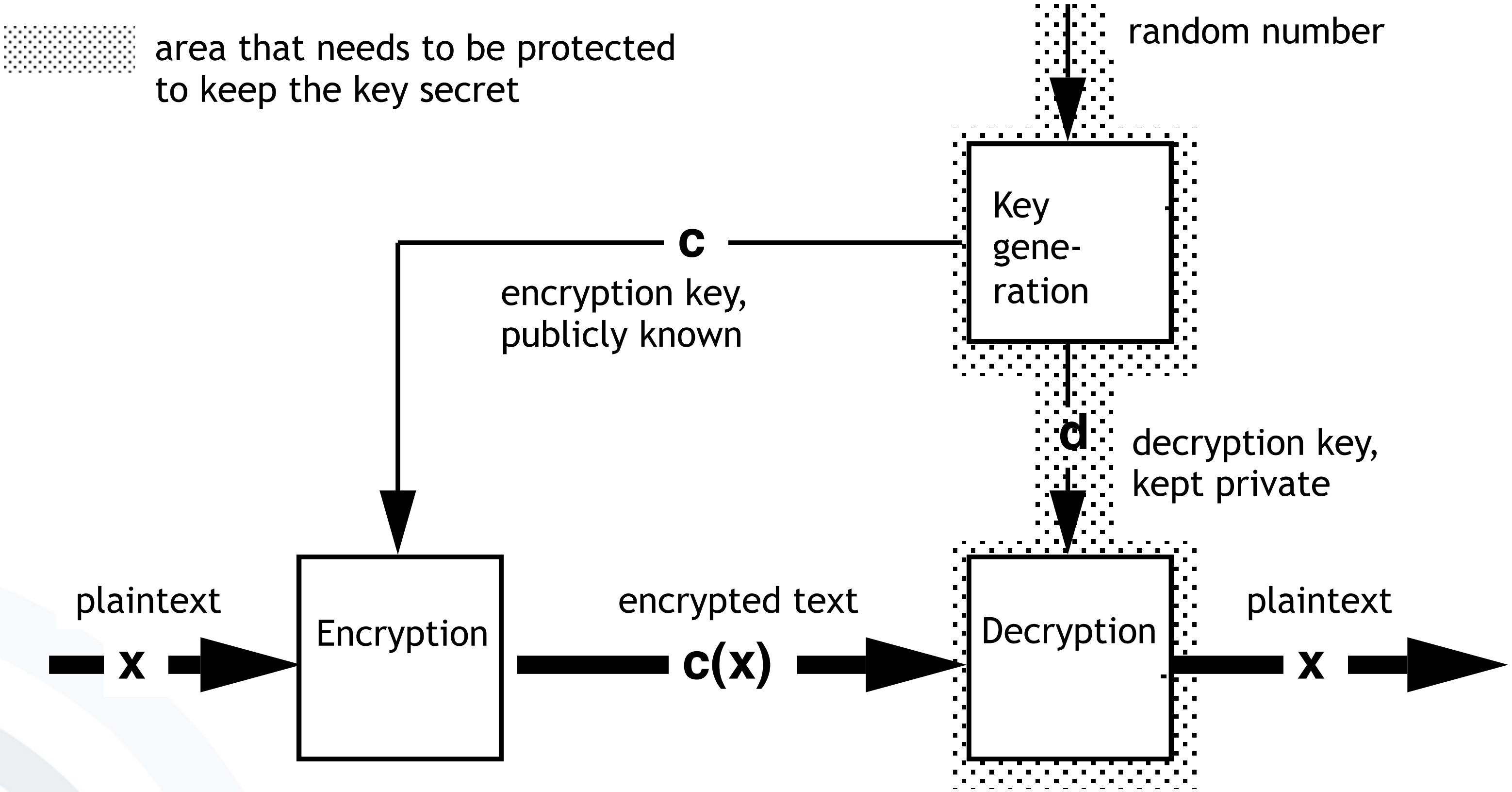

1
Operator builds walls around location information
Operator
User pays operator for service
Operator-branded service delivered
2
Operator invites preferred partners into walled garden
Operator
P
€€
P
User pays operator for service
Partner-branded service delivered
Operator delivers location to partners and shares revenue
P
Operator partner
Location information
3
Operator sells X, Y coordinates to third parties
Operator
T
€€
T
User pays operator or third party
Third-party branded service delivered
Third parties pays operator for location
T
Third party
Location information

Source: Forrester Research, Inc.

Question 33

- *4. Lecture 3 page 25; page 38: are those exam relevant?*

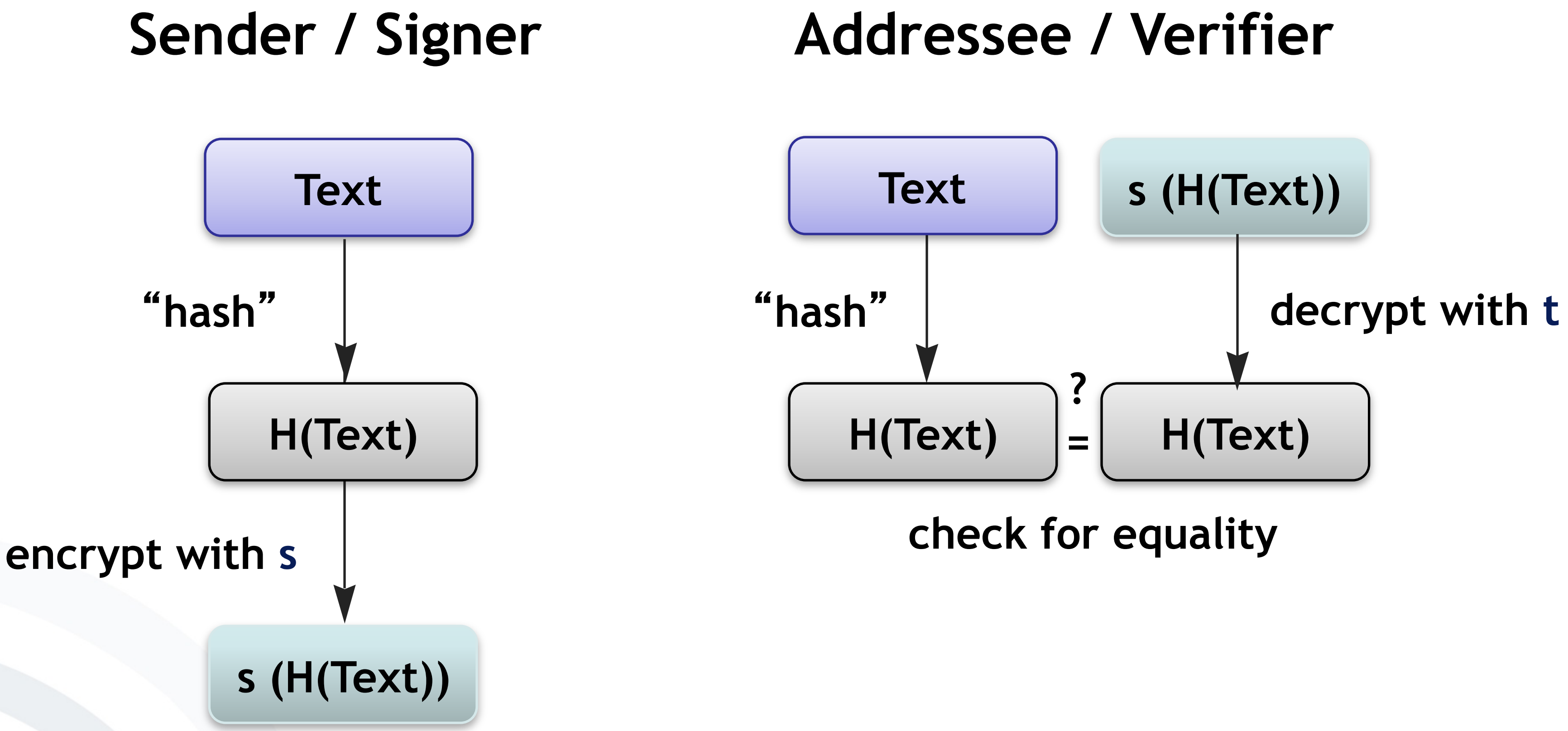
Asymmetric Encryption Systems


area that needs to be protected to keep the key secret
random number
Key generation
c
encryption key, publicly known
d
decryption key, kept private
plaintext
x
Encryption
encrypted text
c(x)
Decryption
plaintext
x

box with slot, access to messages only with a key

[based on Federrath and Pfitzmann 1997]

Asymmetric Signature System (Example RSA)

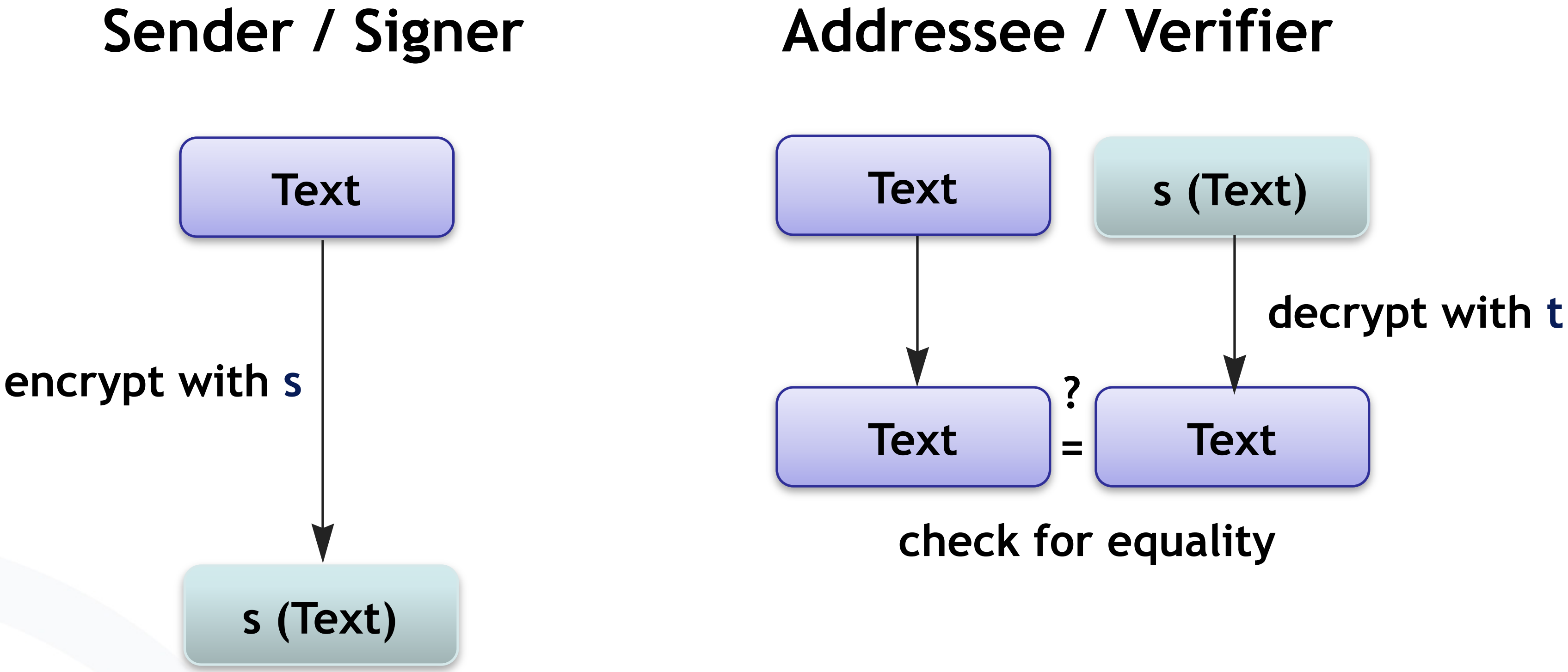


- ➲ Signing key s only with the sender, test key t public
- ➲ Example is often mistakenly generalized.

Question 33

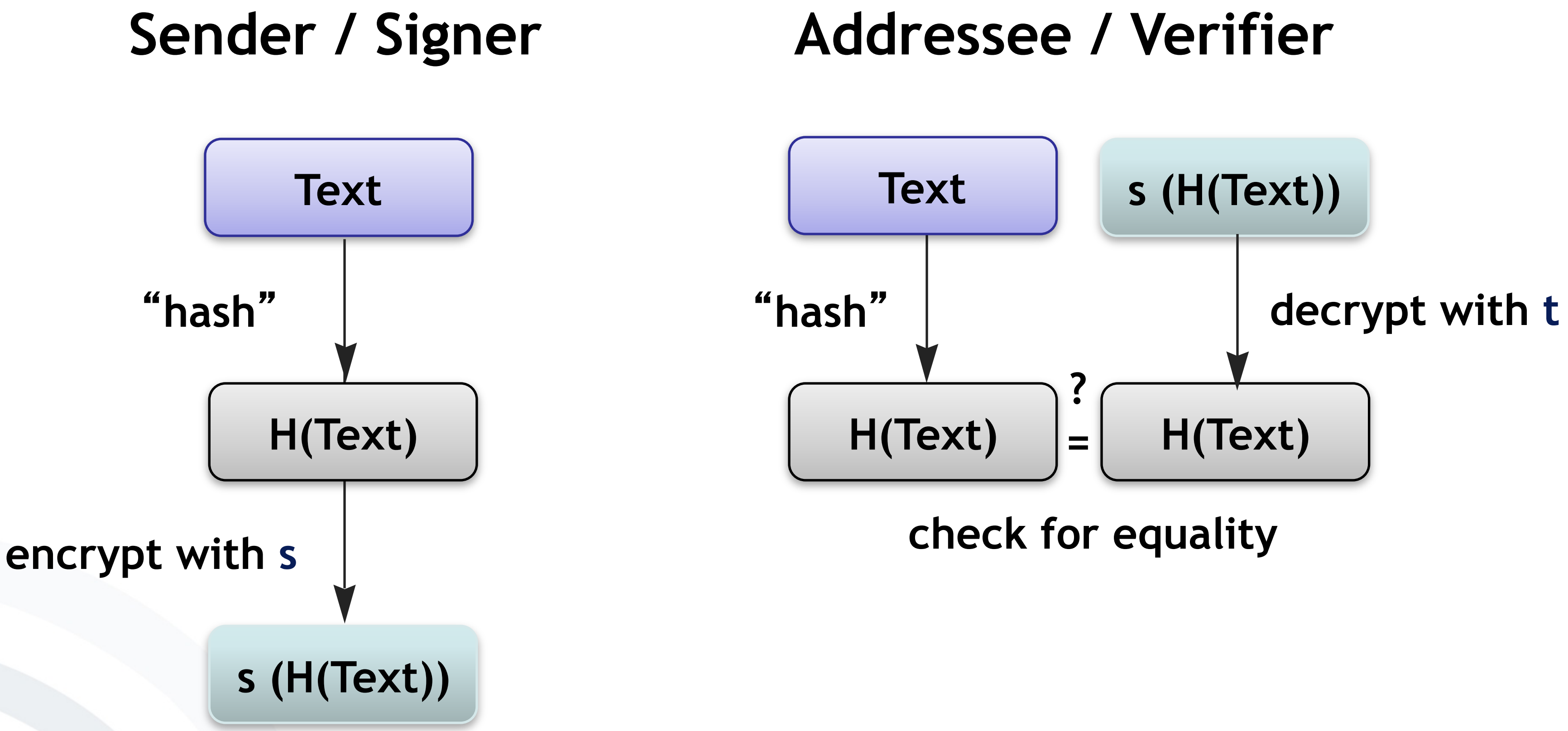
- *5. Lecture 4, page 37,38: Explain please*

Asymmetric Signature System (Simplified Example RSA)



- ➲ Signing key s only with the sender, test key t public
- ➲ Example is often mistakenly generalized.

Asymmetric Signature System (Example RSA)



➲ Signing key s only with the sender, test key t public

➲ Example is often mistakenly generalized.

Question 33

- *6. Lecture 4, page 48: Explain please: Web of Trust*

Tasks of a Certification Authority

(according to German Signature Law and Regulation)

- Reliable identification of persons who apply for a certificate
- Information on necessary methods for fraud resistant creation of a signature
- Provision for secure storage of the private key
  - at least Smartcard (protected by PIN)
- Publication of the certificate (if wanted)
- Barring of certificates
- If necessary issuing of time stamps
  - for a fraud resistant proof that an electronic document has been at hand at a specific time

Question 33

- *7. Lecture 5,: are annex exam relevant?*

Agenda

- General Concept & Applications
- Algorithms
- Legal Framework
- Mobile Signatures
- Secure Display Components and Personal Security Assistants
- Wallets
- Annexes

Annexes

- Annex I
  - EU eIDAS regulation 2014,
    requirements for qualified certificate
- Annex II
  - Client Signatures
    SIM based
- Annex III
  - Certification on Demand

Annex I
EU eIDAS regulation 2014, requirements for qualified certificate

- an indication that the certificate has been issued as a qualified certificate …
- Data about the qualified trust service provider issuing the qualified certificates …
- … name of the creator of the seal and, where applicable, registration number as stated in the official records;
- … validation data and details of the beginning and end of the certificate’s period of validity;
- the certificate identity code
- the advanced electronic signature or advanced electronic seal of the issuing qualified trust service provider;
- the location where the certificate supporting the advanced electronic signature or advanced electronic seal is available;
- the location of the services that can be used to enquire as to the validity status of the qualified certificate;
- An indication where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device…

[EU eIDAS Regulation 2014]

Annex II
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]

Annex II
Challenges of SIM Signatures I

- 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.

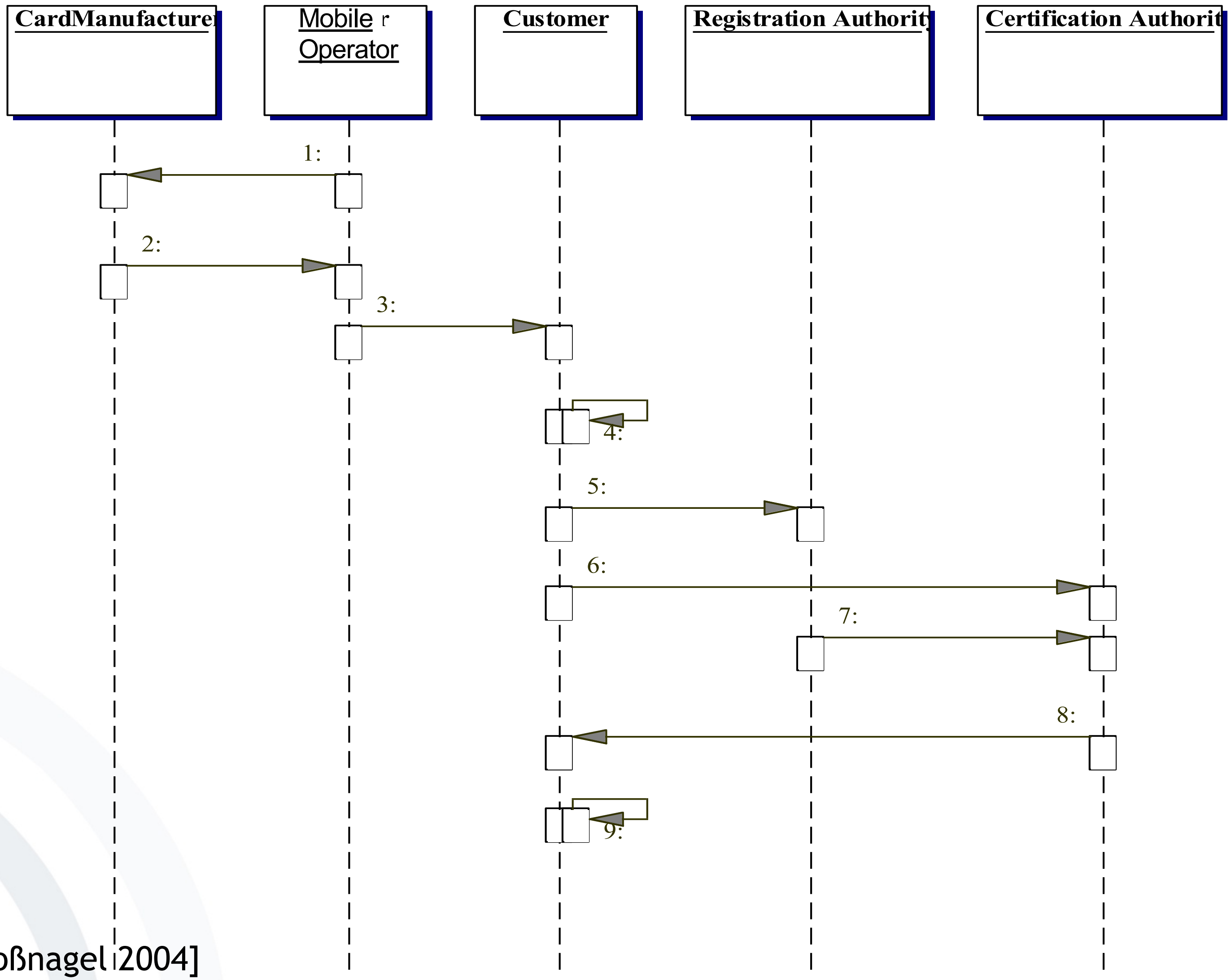
[Roßnagel 2004]

Annex II
Challenges of SIM Signatures II

- 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]

Annex III 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]

Annex III
Certification on Demand

- Distribution scheme of Mobile Operator stays intact.
- 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]

AOB ?