

Lecture 14

Exam Preparation Session

Mobile Business I (WS 2015/16)

Prof. Dr. Kai Rannenberg

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



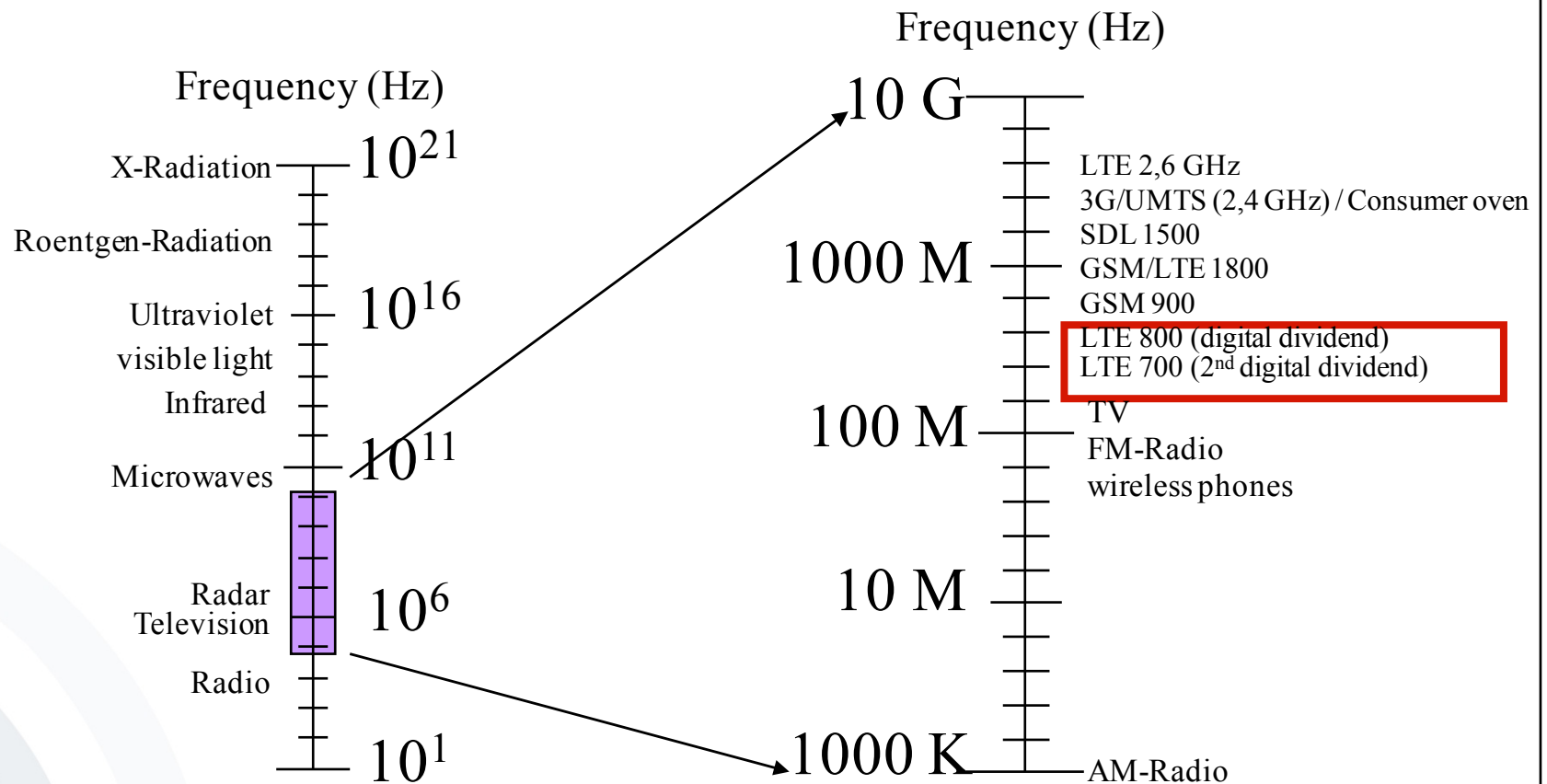
[Source: T-Mobile]

- Is it allowed to use a dictionary during the exam?
 - Yes, not a problem
- Lecture 12: How important is lecture 12 for the exam? We didn't discuss any questions during the exercise sessions about it.
 - It doesn't matter. It is important.
- Are there any multiple choice questions in the exam? If yes, do we get negative points if we answer them wrong?
 - Maybe, you will see it on the exam day
- Just to make sure, if you say "name ..." then you don't expect an explanation, do you?
 - No, we don't.
- Is the annex of lecture 4 relevant for the exam?
 - Yes, it is relevant.

Q: Explain “digital dividend”.

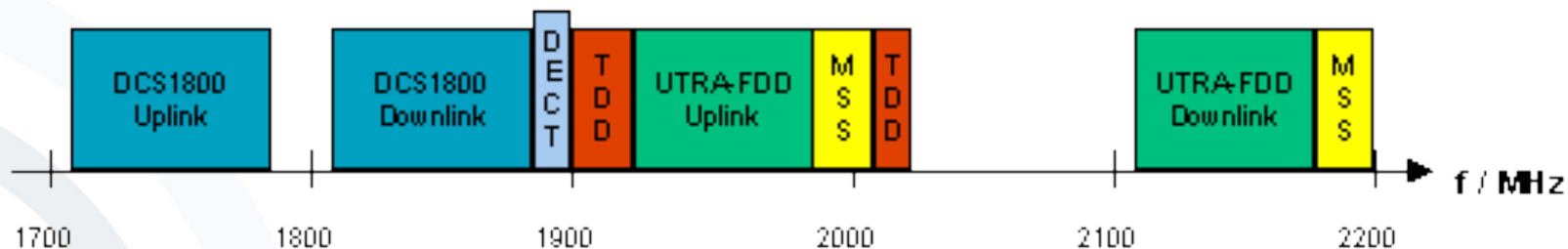


Frequency range of instruments of entertainment and communication electronics



Q: (Lecture 2) slide 44: Can you explain the UMTS frequency allocation in Europe, please (focus on the graphic)?

- **Common approach:**
Worldwide reservation of frequencies in the 2GHz range
- **Problem of competing targets:**
 - Existing national networks and installed network technique shall preferably be transferred into the new standard.
 - ➔ The specification of 3G-Networks, introduced by the ITU, leaves room for national, partly incompatible implementations.
- UMTS (UTRA-FDD/TDD) frequency allocation in Europe:



© 2001 UMTSlink.at

UTRA-FDD: UMTS Terrestrial Radio Access - Frequency Division Duplex

[UMTSlink2006]

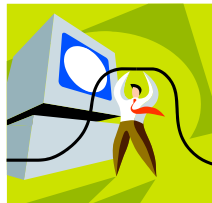


Q: (Lecture 3) slides 24 and 25: What is the difference between these graphics?

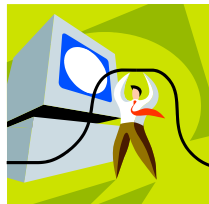




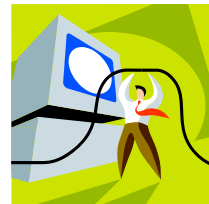
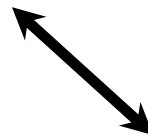
Partner B
IP address, e.g.
61.9.193.200



Router



Router



Router



Partner A
IP address,
e.g. 141.2.74.211

- Routing takes place from Partner A node to Partner B node and in reverse direction.
- Both nodes have their own address.
- The route follows the addresses.
- Routing of data packets by routers

Mobile IP Mobility problem



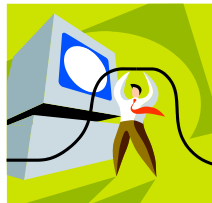
Old IP address (Partner B)



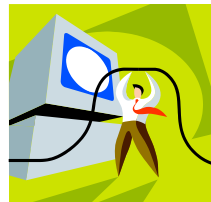
Partner B changes network



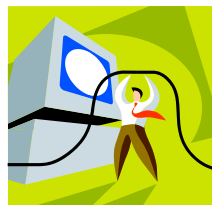
New IP address
(Partner B)



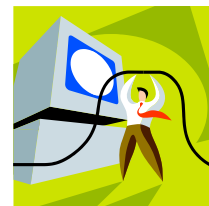
Router



Router



Router

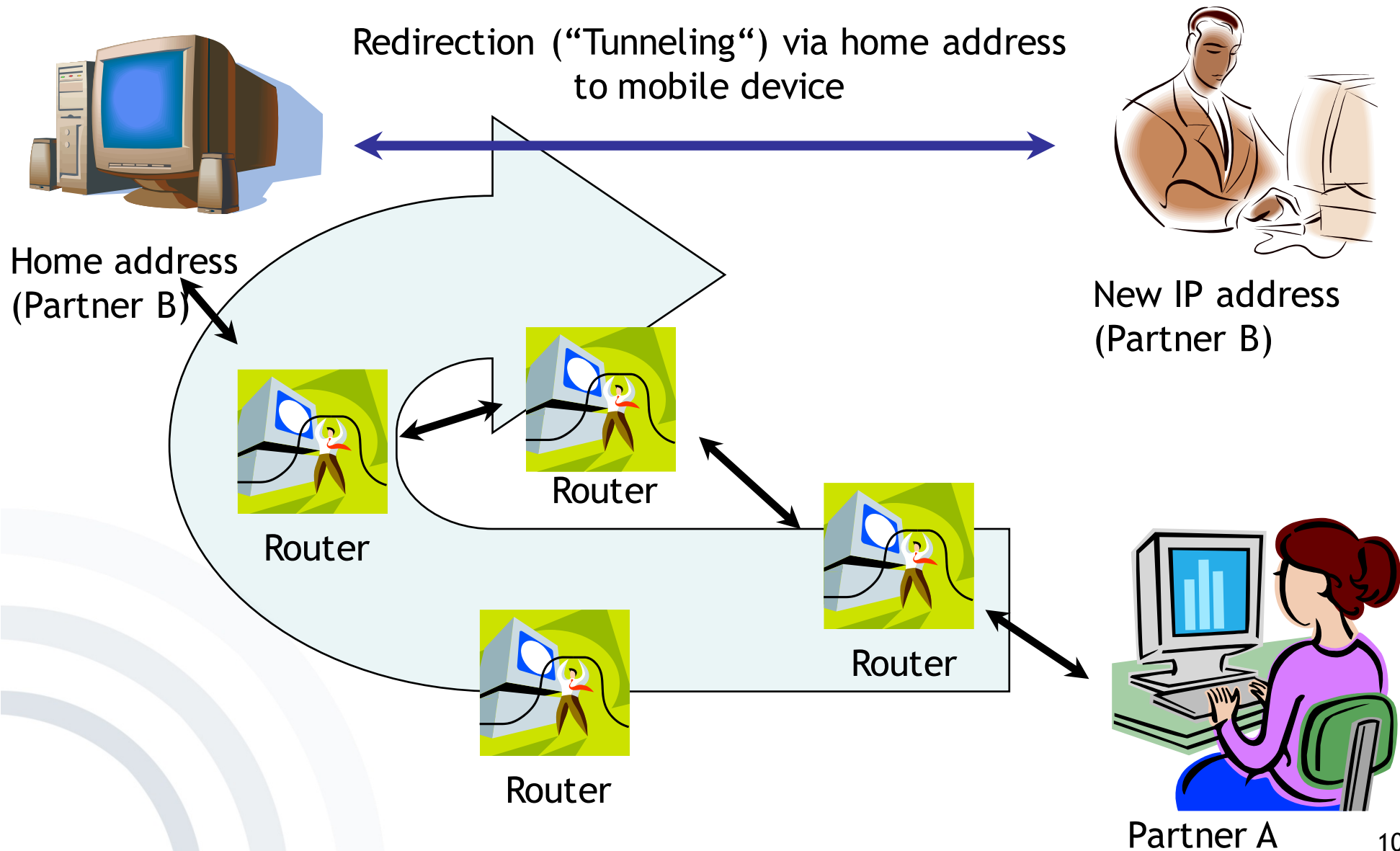


Router



Partner A

Mobile IP Mobility solution - Layer 3



Q: Partial anonymity

Q: TMSI is a temporary user identification. How does it exactly work? Will a new IP address always be generated on the phone, so that the user is identifiable? I thought the user should be identifiable in order to be able to, e.g. charge for roaming. As far as I understand, the TMSI is there to avoid tracking the user.

A: TMSI is randomly assigned by the VLR (Visitor Location Register) to every mobile in the area, the moment it is switched on. The number is local to a location area, and so it has to be updated each time the mobile moves to a new geographical area.

Q: Partial anonymity (cont...)

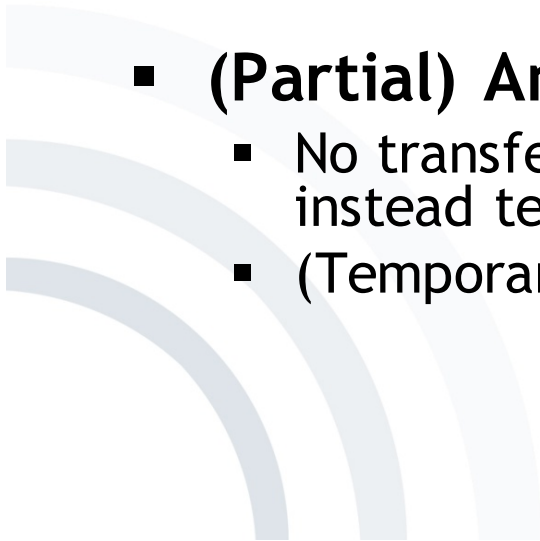
Q: Is TMSI only in GSM or also on other networks later (UMTS / HSPA)?

A: It also works in other networks. E.g. UMTS

Q: To compare, we also have the IMSI. This is there to uniquely identify users. Are the two modes there in parallel used at a mobile user?

A: Yes, IMSI is internationally known identity of a subscriber but TMSI is a temporary identity, which provides anonymous communication.

The GSM system offers different “security services”:

- **Access control and authentication:**
 - Authentication of the subscriber to the SIM by input of a PIN and to the GSM network by Challenge-Response-Procedure
 - **Confidentiality:**
 - Data & voice transferred between mobile station and BTS are encrypted.
 - **(Partial) Anonymity:**
 - No transfer of data which can identify the subscriber via radio, instead temporary identification
 - (Temporary Mobile Subscriber ID, TMSI)
- 
- Three large, light blue curved lines in the bottom left corner, resembling a stylized signal or a decorative graphic element.

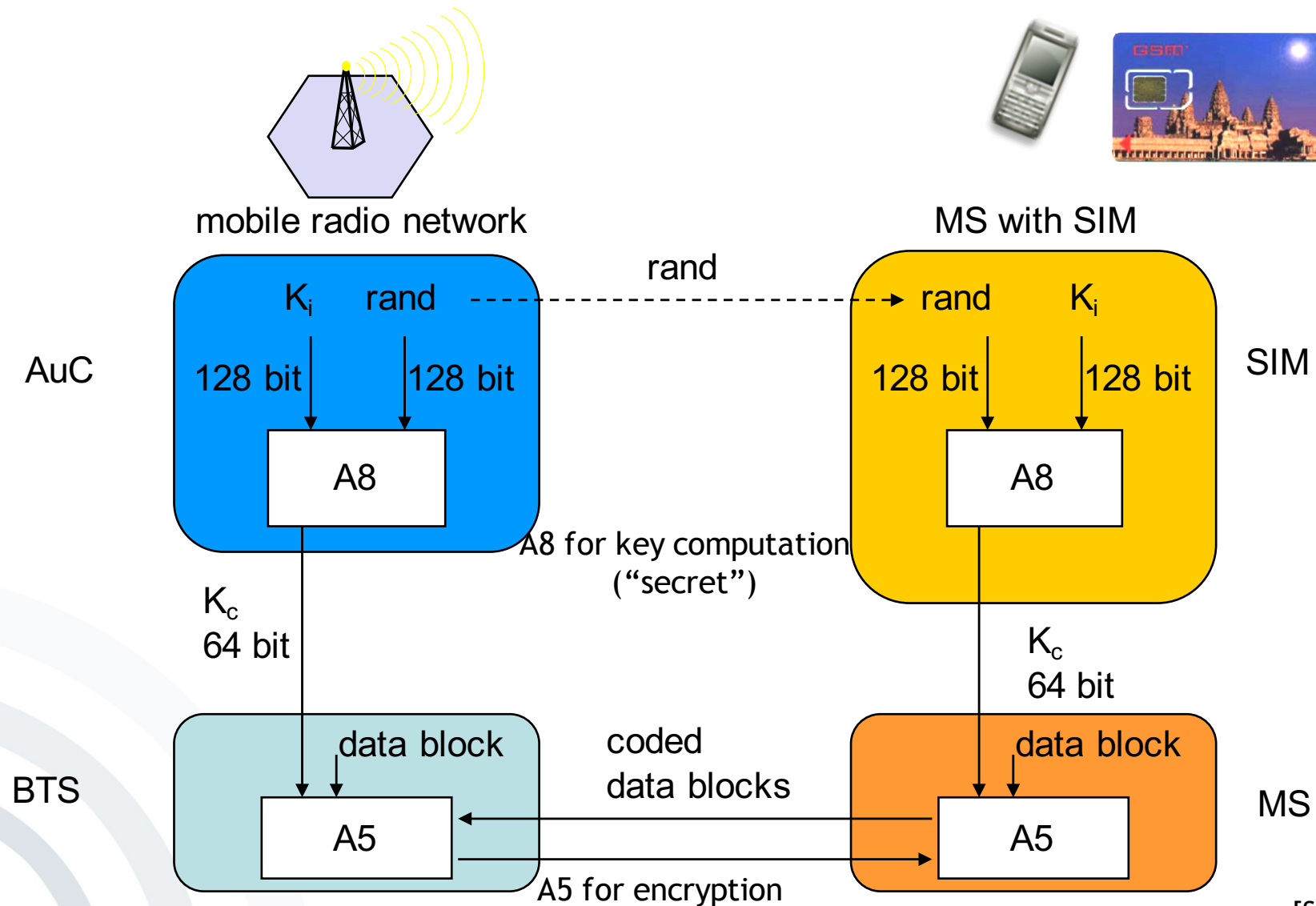
Q: Here we say “Centralized movement tracking is possible”. I thought that with TMSI, the User is not tracked. How come this is so?

Q: What does the fact that A3 and A8 are published without authorization and that non standardised algorithms are used? Are they more secure, or less secure?

- Partial Anonymity:
 - In order to guarantee the anonymity of the users temporary user identification (TMSI) is used.
 - Temporary user identification is updated automatically from time to time or on demand.
 - Data which identify users are not transferred.
 - **Example:** Anonymous charging is (technically) possible via prepaid card.

- Solely authentication of the terminal/subscriber toward the GSM network. The network does not authenticate itself.
 - Assumption that the network is trustworthy per se
 - Security model was developed at a time with a provider monopoly
- Subscriber localization is almost exclusively controlled by the network.
 - Centralized movement tracking is possible
 - In order to avoid localization the subscriber must switch off the terminal.

- Security model bases partly on secret encryption algorithms.
 - A3 and A8 were published without authorization.
 - Some operators use non-standardized algorithms.
- No encryption from terminal to terminal but solely over the air interface
 - Encryption deactivation by the network possible, without notification of the users
- Encryption comparatively “weak” because of key length (64 bit)
 - Sometimes the real key length is shorter.



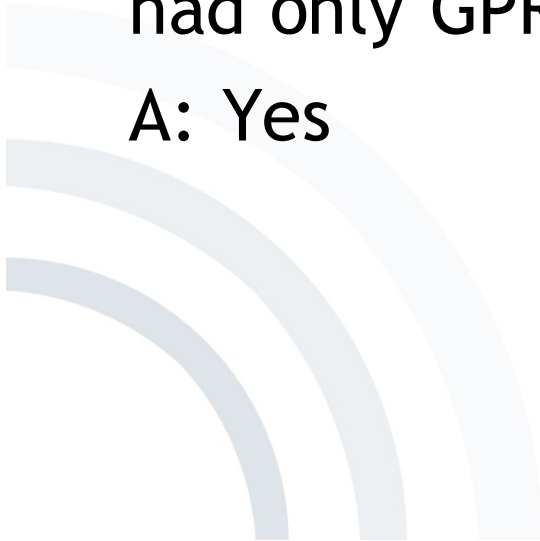


Q: Modem, CSD, HSCSD, GPRS, EDGE are listed under the category “Mobile Data Services”. Do HSPA and LTE not also belong here?

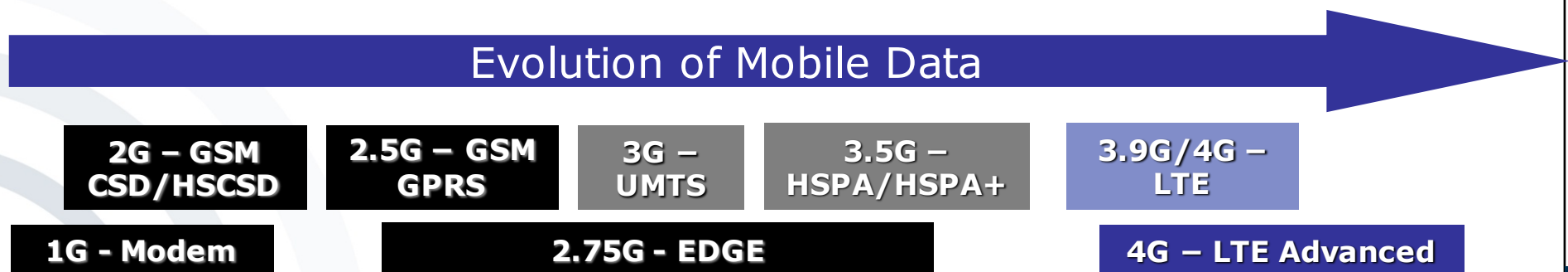
A: Yes

Q: Do CSD and HSCSD belong to the GSM network? I had only GPRS and EDGE in the notes.

A: Yes



- **Modem** (modulator-demodulator) in analogue mobile networks (300 - 2400 bit/s)
- **CSD** (Circuit Switched Data) in GSM networks (9.6 Kbit/s)
- **HSCSD** (High-Speed Circuit Switched Data) in GSM networks (57.6 Kbit/s max.)
- **GPRS** (General Packet Radio Service)
- **EDGE** (Enhanced Data Rates for Global Evolution)







Q: Does WEP also use a pre-shared key?
Have I understood correctly that both the Router and the mobile device have the PSK? How does the PSK come to the device (mobile)?



- There are numerous methods for Wireless LAN encryption.
- We are only looking at methods that use a **pre-shared key (PSK)**.
- WEP encryption methods are outdated and hence insecure:



- Wired Equivalent Privacy (WEP) **64-bit** 
 - Wired Equivalent Privacy (WEP) **128-bit** 
- WEP 128-bit can be by-passed within minutes. [Heise 2007]

- **Wi-Fi Protected Access (WPA)** was developed by the Wi-Fi Alliance. [Wi-Fi 2010]



- There are two versions of **Wi-Fi Protected Access**, WPA and WPA2:
 - **WPA** includes most of the 802.11i standard, but is **outdated and insecure** as it has various weaknesses:
 - Vulnerability to dictionary attacks when using a weak PSK
 - Other weaknesses inherited from earlier standards [ArsT 2008]
 - **WPA2** includes **802.11i** to its full extent and also the Advanced Encryption Standard (AES).

Q: (Lecture 7) Could you please provide the solution for the example on page 51 from lecture 7? (next slide)



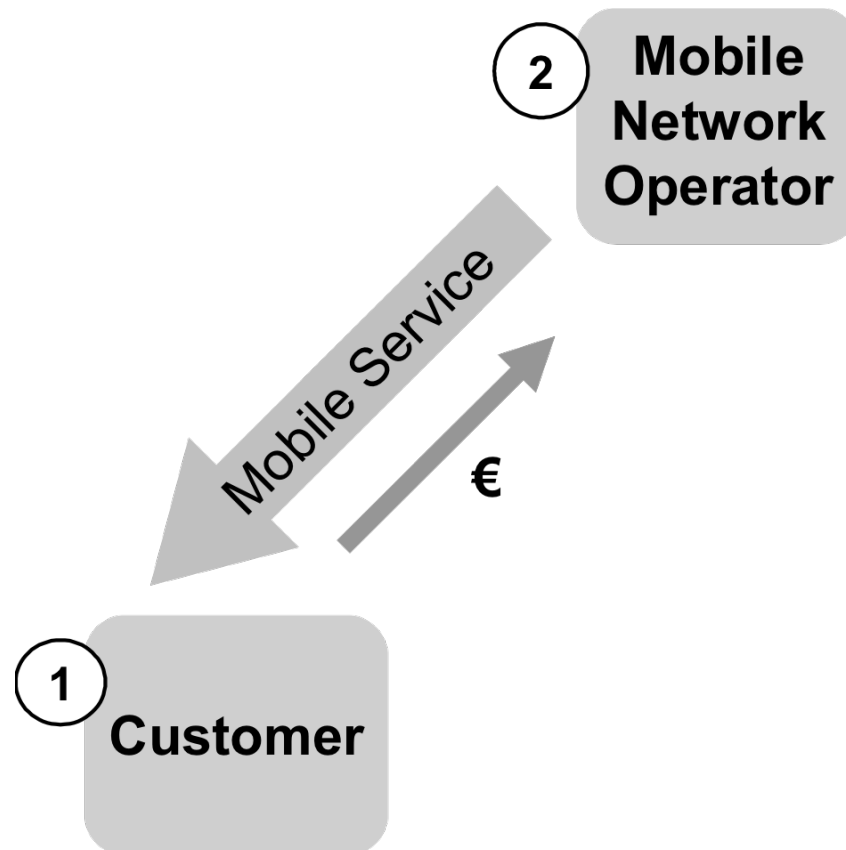
■ New revenue flows:

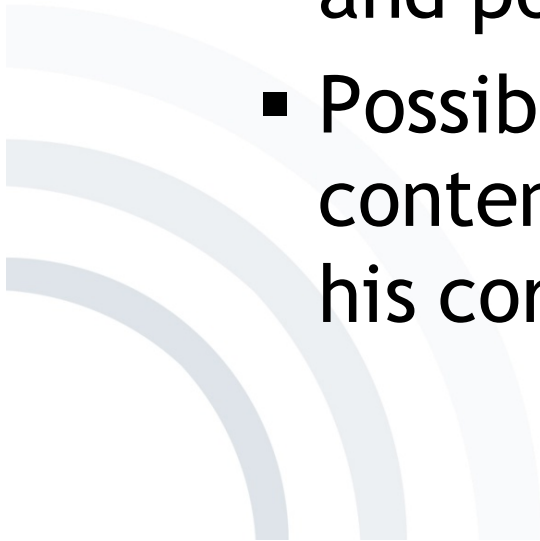
■ Assumptions:

- Service provider pays (for the customer) 10€ for 30 MB of data transfer.
- 18% of 1m customers of the operator use services (because data transfer is free now) and spend 20€ per month.
- ➡ 3,6 Mil. € receipts for the service provider
- For these services, 30 MB of data transfer is necessary per customer and month
- ➡ 10€ expenditures per customer (by the service provider) and 1,8m € revenues for the operator.
- ➡ Revenues of the operator: $0\text{m €} + 1,8\text{m €} = 1,8\text{m €}$
- ➡ Revenues of the service provider: $3,6\text{m €} - 1,8\text{m €} = 1,8\text{m €}$

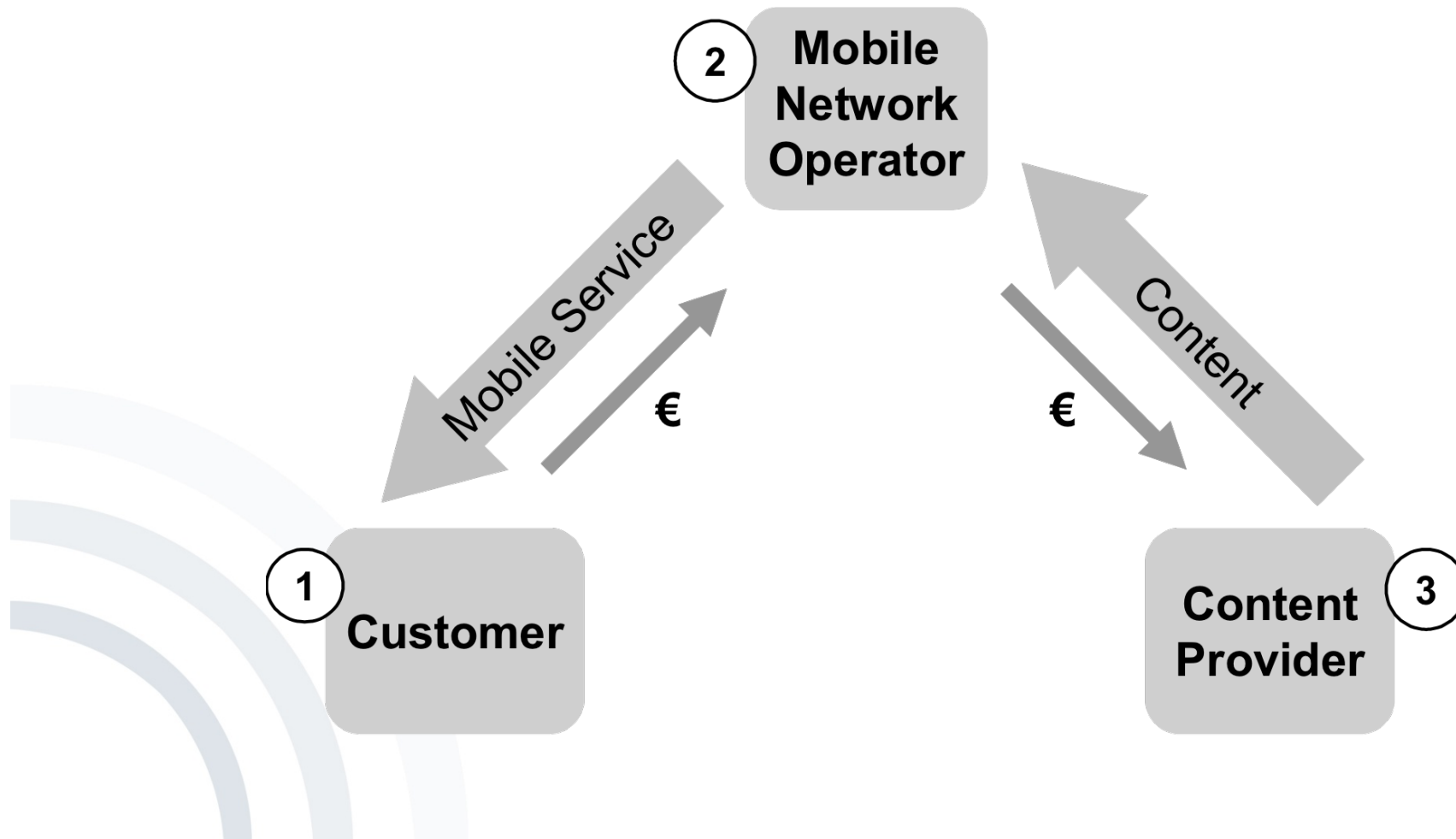
- Business Models
 - Value Proposition
 - Value Creation Architecture
 - Revenue Models
 - Pricing Models
 - Tariff Models
- Classical Business Models for Mobile Network Operators
- New Business Models for Mobile Network Operators

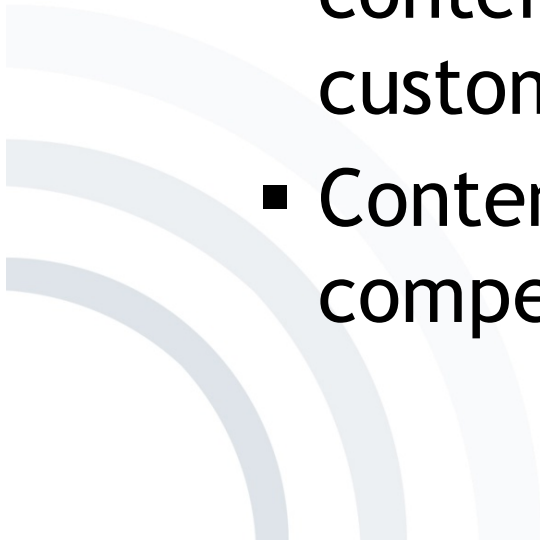
- Classical business model (CBM) I:



- Classical business model I:
 - Two parties: Customer, mobile network operator
 - Operator provides communication services and possibly contents to the customer.
 - Possibly the operator manufactures these contents himself. Providing contents is not his core competence.
- 
- Three large, light blue curved lines in the bottom left corner, mirroring the style of the logo, creating a sense of movement or signal.

- Classical business model II:



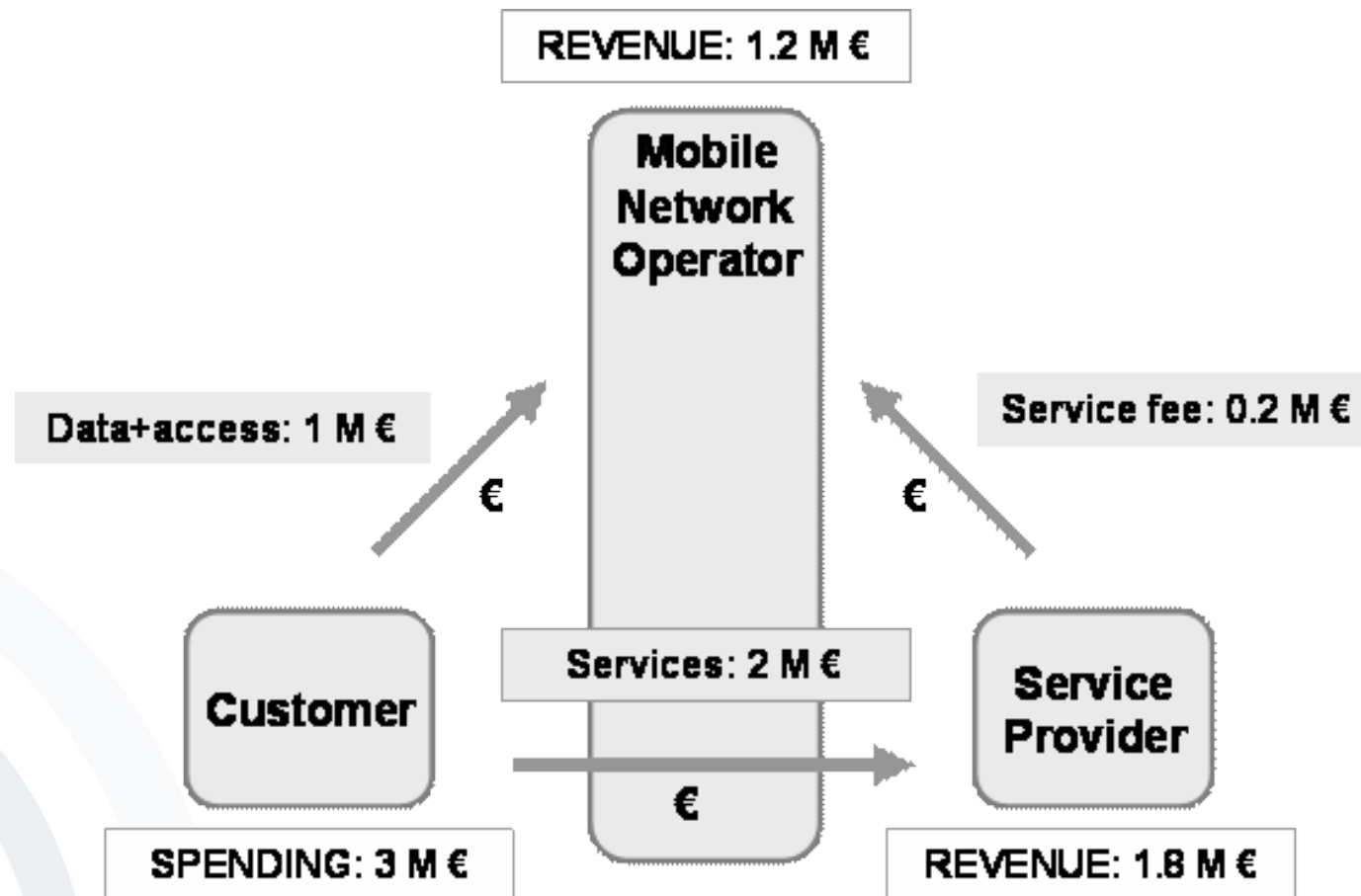
- Classical business model II:
 - Three parties: Customer, mobile network operator, content provider.
 - Operator purchases content (from the content provider) and passes it on to the customer.
 - Content Provision is not the core competence of the network operator.
- 
- Three large, light blue curved lines in the bottom left corner, mirroring the style of the logo, suggesting a signal or network.

■ Traditional revenue flows:

■ Assumptions:

- Customer pays 10€ for 30 MB of data transferred (T-Mobile Data 30)
- 10% of one million (= 100,000) customers of the operator use extra services and spend about 20€ per month .
- 2 million € revenues for the service provider
- For these services, 30 MB of data transfer is necessary per customer and month
- ➡ 10 € expenditures per customer and 1 million € revenues for the operator.
- Service-Provider pays 10% of his receipts as “Service Fee” to the operator.
- ➡ Revenues of the operator: $1\text{m €} + 0,2\text{m €} = 1,2\text{m €}$
- ➡ Revenues of the service provider: $2\text{m €} - 0,2\text{m €} = 1,8\text{m €}$

- Traditional revenue flows



Revenue model:

Direct revenue model:

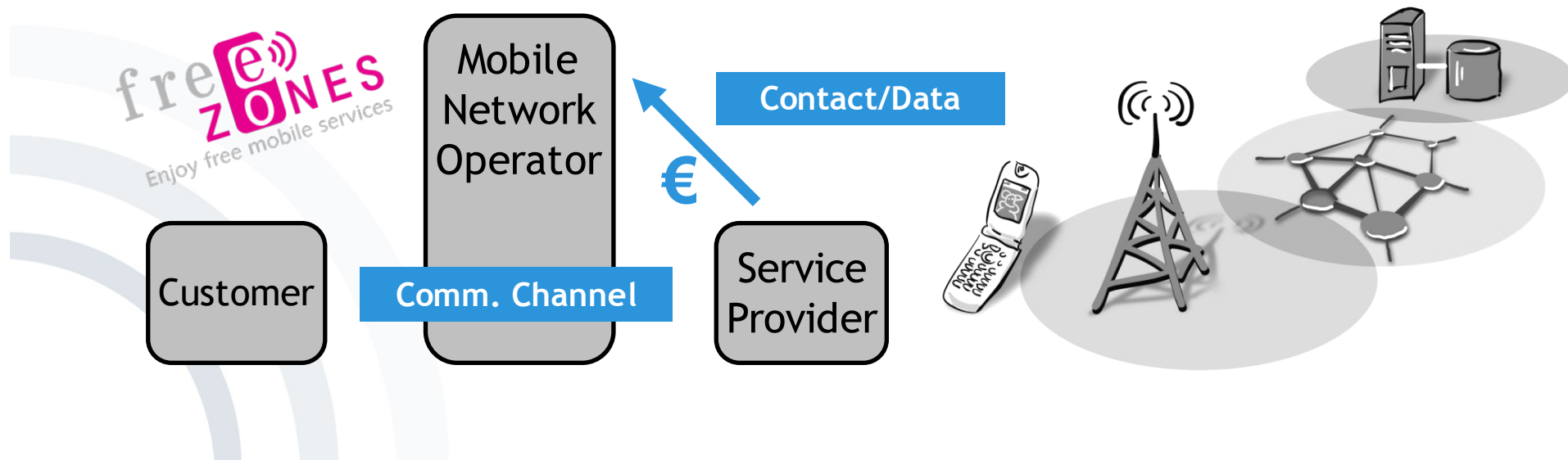
- either transaction-based (charged by data traffic)
- or flat rate

Pricing model:

Pricing based on differential pricing model

- Business Models
 - Value Proposition
 - Value Creation Architecture
 - Revenue Models
 - Pricing Models
 - Tariff Models
- Classical Business Models for Mobile Network Operators
- New Business Models for Mobile Network Operators

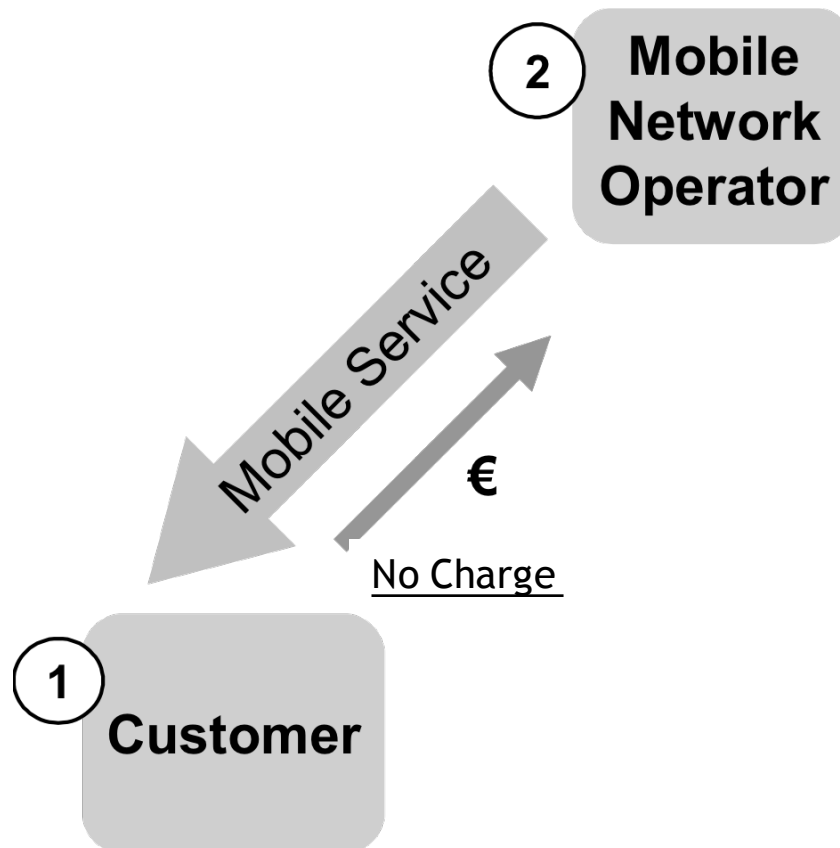
- **Potential:** Mobile network operators have a customer relation with more than 85% of the German population!
- **Offering:** Mobile network operators are providing service providers with a contact/communication channel to potential customers.
- **Objective:** Eliminating data costs for customers while making them marketing costs for service providers.



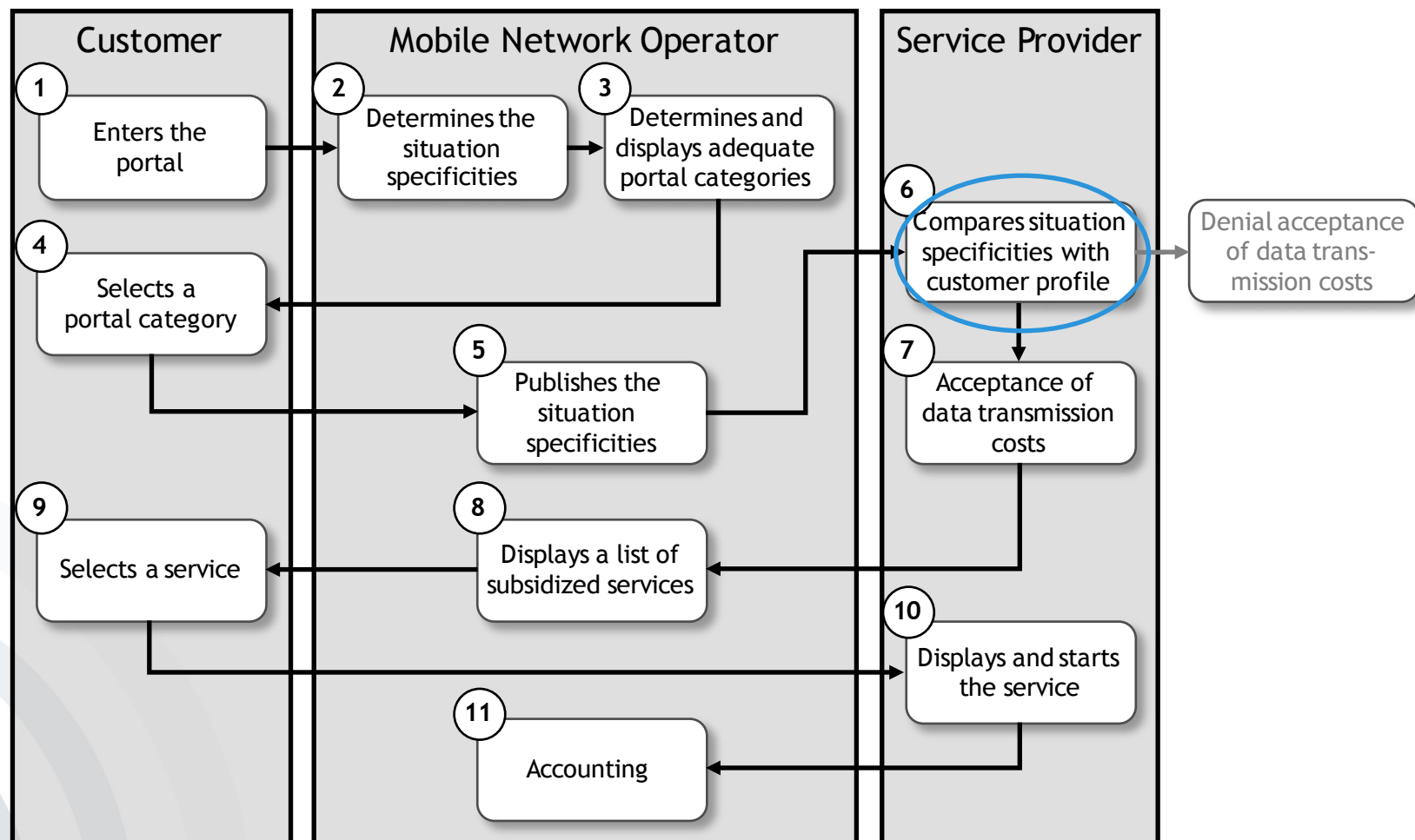
- New approach
 - Disintegration of existing provider constellations through revenue-sharing and sponsoring

- New business model
 - “Reverse“ approach: Instead of charging the customer, the service provider contacts the customer and offers free access.
 - ➡ Sponsoring of interesting (profitable) customers by advertising service providers

- New business model:



■ Process for context sensitive services

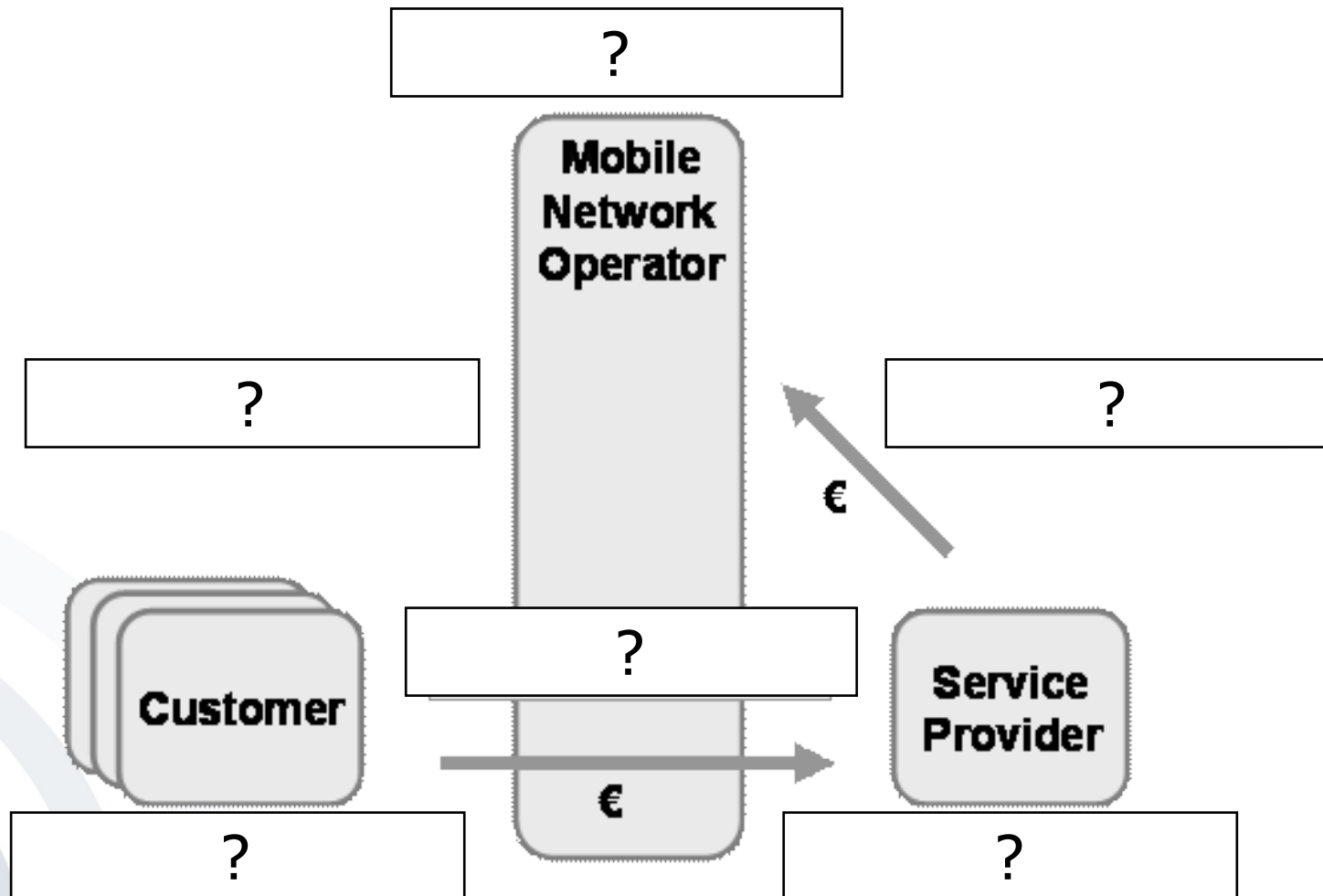


■ New revenue flows:

■ Assumptions:

- Service provider pays (for the customer) 10€ for 30 MB of data transfer.
- 18% of 1m customers of the operator use services (because data transfer is free now) and spend 20€ per month.
- ➔ 3,6 Mil. € receipts for the service provider
- For these services, 30 MB of data transfer is necessary per customer and month
- ➔ 10€ expenditures per customer (by the service provider) and 1,8m € revenues for the operator.
- ➔ Revenues of the operator: $0\text{m €} + 1,8\text{m €} = 1,8\text{m €}$
- ➔ Revenues of the service provider: $3,6\text{m €} - 1,8\text{m €} = 1,8\text{m €}$

- New revenue flows



- Q: (Lecture 9): Why is here a decline of the purchase of mobile devices shown? I would have expected an increase.

Worldwide Mobile Phone Sales to End Users by Vendor 2012 vs. 2011 - A Decline?

In 1.000 Units

Company	2012 Units	2012 Market Share (%)	2011 Units	2011 Market Share (%)
Samsung	384,631.2	22.0	315,052.2	17.7
Nokia	333,938.0	19.1	422,478.3	23.8
Apple	130,133.2	7.5	89,263.2	5.0
ZTE	67,344.4	3.9	56,881.8	3.2
LG Electronics	58,015.9	3.3	86,370.9	4.9
Huawei Technologies	47,288.3	2.7	40,663.4	2.3
TCL Communication	37,176.6	2.1	34,037.5	1.9
Research In Motion	34,210.3	2.0	51,541.9	2.9
Motorola	33,916.3	1.9	40,269.1	2.3
HTC	32,121.8	1.8	43,266.9	2.4
Others	587399.6	33.6	595886.9	33.6
TOTAL	1,746,175.6	100.0	1,775,712.0	100.0

Cf. TOTAL Units sold in 2013: 1,820,200.0

[Statista2014]

[Gartner2013a]

A: In this example, we wanted to show that statistics from different sources may not be directly comparable.

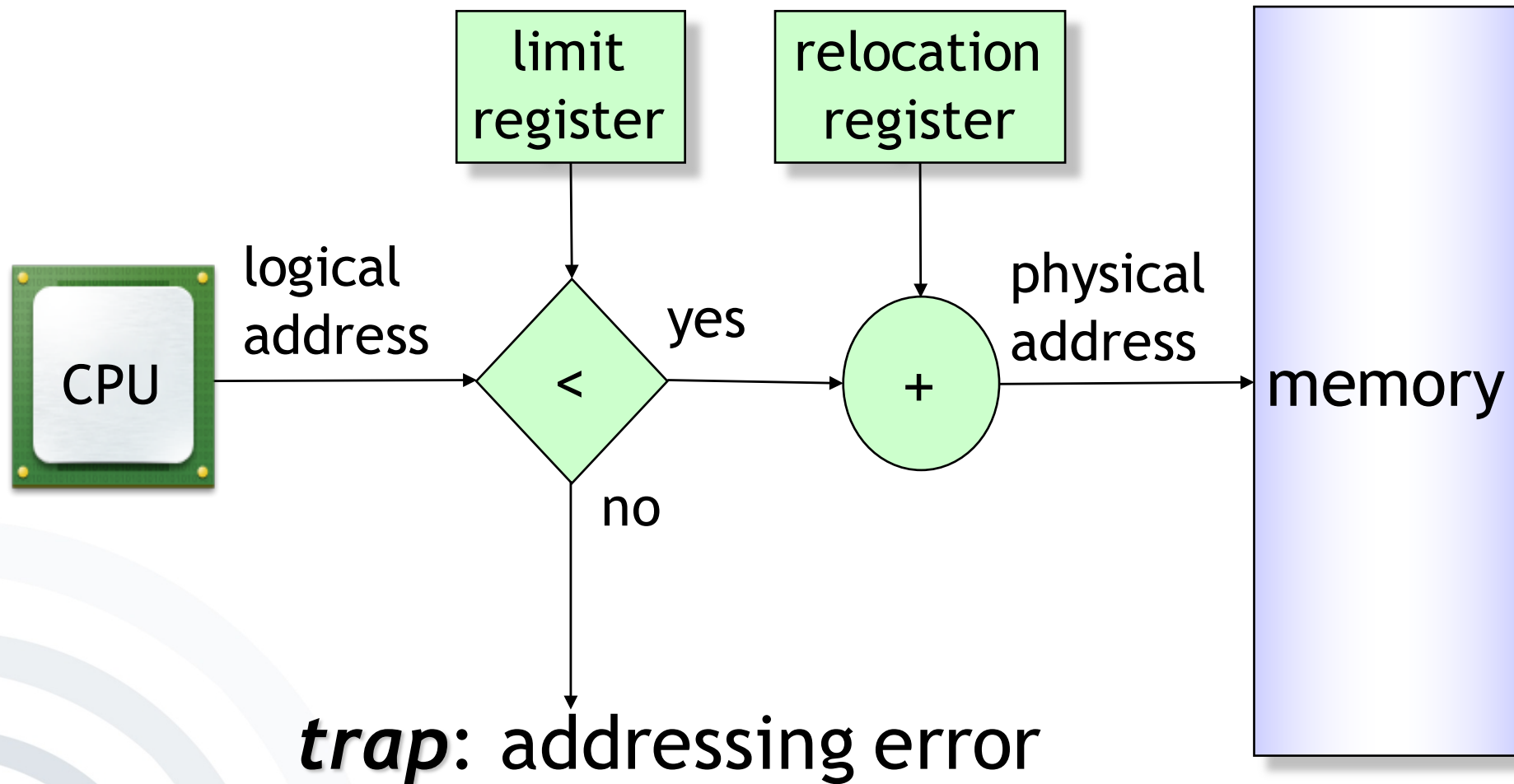
- Lecture 10, slide 30/31: Can you explain what the limit register is, please?



- Functions
- Processes
 - States and elements
 - Scheduling
 - Inter-Process-Communication (IPC)
- Memory Management
 - Mapping
 - Paging
 - Segmentation
 - Examples
- Security & Maintenance

- **Logical Addresses:**
Generated by the CPU
- **Physical Addresses:**
Sent to the memory unit

- The memory of a system also contains the actual operating system.
- The access of other processes onto the code of the operating systems needs to be prevented.
- Furthermore, the processes need to be protected against each other.
- Solution: Usage of so called „Limit Registers“



Q: (Lecture 10) In which detail do we have to know the examples on lecture 10 (slide 40-52)?

A: You should understand the logic and have an overview of this part of the lecture on memory management.

Q: (Lecture 11) Is it enough to name examples of the mobile operating systems unavailable to other device manufacturers and manufacturer-independent mobile operating systems or do we also need to know the history of all the examples mentioned in lecture 11?

A: It is useful to understand how the the Mobile OS ecosystem has evolved. We will not ask for dates, but a general overview is necessary.

Exercise 2

1d) Check if the concepts are correctly understood.

▪ „Application & System Vendors“ – Prof. Rannenbergh took the example of E-Plus, who outsourced their infrastructure, and bought the licenses for using it from the Vendor.

▪ „Content suppliers“ – Content that the Network Operator offers, such as information, apps.

▪ „Content aggregators/portals“ – Services, such as Google Play, where one downloads, e.g. apps.

▪ „Network Infrastructure“ – I could mix it with „Application & System Vendors“ – What is the difference?

- Yes, but this refers even more to Technology & equipment vendors.
- Applications for users and for managing the network.

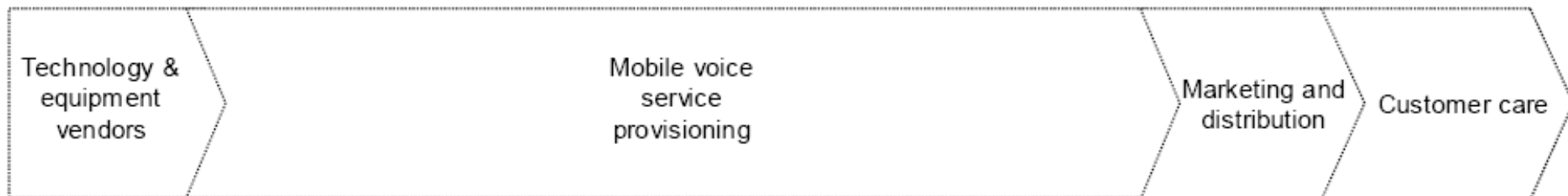
This is more the exception than the rule. This is normally a different entity from the Network Operator.

E.g. t-zones or Google maps, etc.

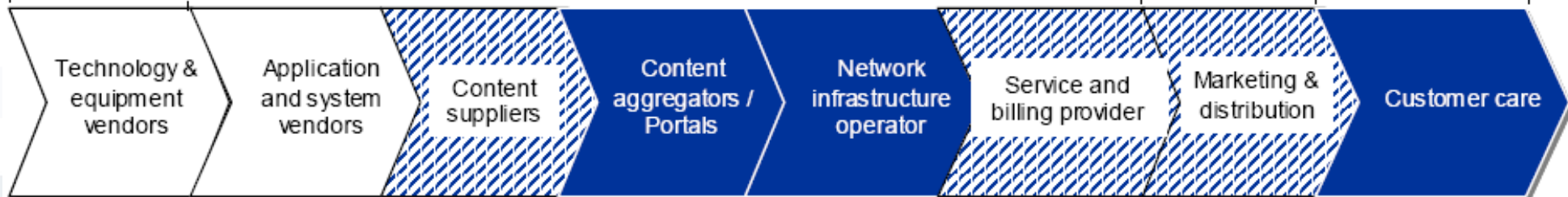
- Incomparable
- Missing “operator”?

Several market players take care of parts of the value chain

TRADITIONAL VALUE CHAIN OF MOBILE SERVICE DELIVERY



EMERGING MOBILE OPERATOR VALUE CHAIN



Primary opportunity for operator



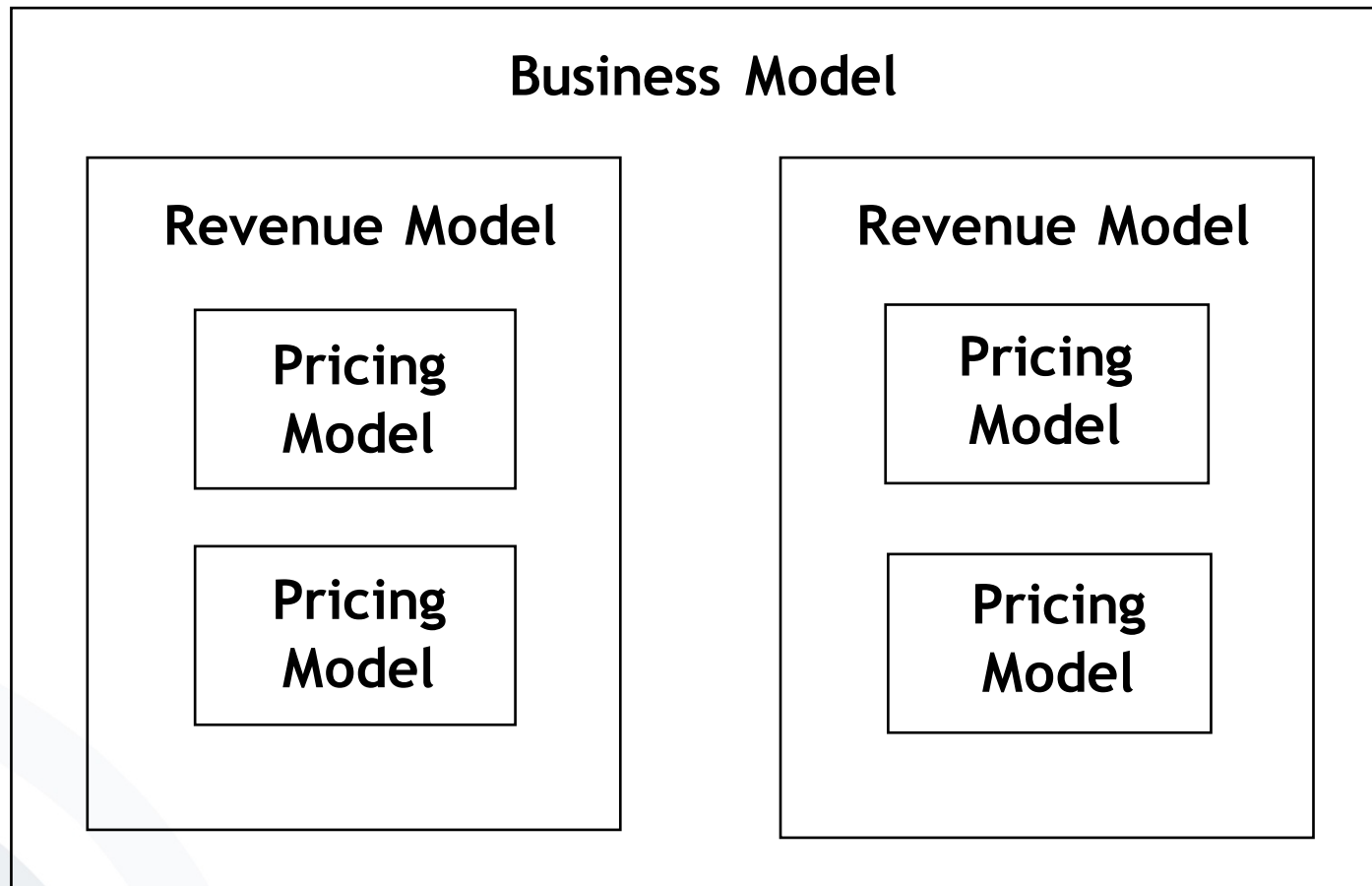
Some opportunity



Opportunity through alliances

[Passerini et al. 2004]

- Q: (6.1a) Can we describe this task as follows: “The business model contains a revenue model which can contain different pricing models.” or would it be enough to draw a simply graph (diagram) in the exam?



Example

- Q: (6.1a) Can we describe this task as follows: “The business model contains a revenue model which can contain different pricing models.” or would it be enough to draw a simply graph (diagram) in the exam?
- A: Almost correct. Except that there may be more than one revenue model.

- Q: 1b) Part (ii) applications. In the solution we only discuss about the security, but what about the relation to applications?

- b) Why are they used and what role do smartcards play with respect to
 - (i) security
 - (ii) applications?

- Used when **security** of data (e.g. for keys, signatures, physical access control, payment) is needed in **insecure environments**
- Examples:
 - Phone cards of Deutsche Telekom
 - Signature cards according to German Signature Law
 - Smartcard applications for PC
 - Smartcards for mobile communication (SIMs)

Q 2b) The question is what contents are there in the SIM card and why some of them are not protected? Can you elaborate a bit on the “why”?



- Protected data:
 - IMSI, PIN, PUK
 - A3, A8 crypto algorithms
 - List of subscribed services
 - Language used by the subscriber
- Dynamic data:
 - Cell information
 - Frequency information
 - Dynamically generated (session) keys
 - Attributes of GSM login
 - User data (address book, telephone list, SMS memory)

Q: The question here is what contents are there in the SIM card and why some of them are not protected? Can you elaborate a bit on the “why”?

A: see next slides

- Protected data:
 - IMSI, PIN, PUK
 - A3, A8 crypto algorithms
 - List of subscribed services
 - Language used by the subscriber
- Dynamic data:
 - Cell information
 - Frequency information
 - Dynamically generated (session) keys
 - Attributes of GSM login
 - User data (address book, telephone list, SMS memory)

- (Rather) static data:
 - IMSI, PIN, PUK
 - A3, A8 crypto algorithms
 - List of allocated (subscribed) services
 - Language preferred by the subscriber
- Dynamic data:
 - Cell information
 - Frequency information
 - Dynamically generated (session) keys
 - Attributes of GSM login
 - User data (address book, telephone list, SMS memory)

Q 4b) What is meant by „separation of components“? And what is a „head-mounted-display“?

- The size of a mobile terminal is considerably determined by its:
 - Input Facilities (e.g. keyboard)
 - Output Facilities (e.g. display)
- ➡ Separation of components (e.g. display in the watch, head-mounted-displays)

Q: What is meant by „separation of components“?
And what is a „head-mounted-display“?

A: A head-mounted display is a display device, worn on the head or as part of a helmet, that has a small display optic in front of one (monocular HMD) or each eye (binocular HMD).



https://en.wikipedia.org/wiki/File:Orlovsky_and_Oculus_Rift.jpg

- Q: What are the weaknesses of Bluetooth? It is generally better than Infrared.
- A: Indeed, Bluetooth improved on weaknesses of Infrared.



- Connection of periphery-devices (headsets, keyboards, mice, etc.)
- Setting up of ad-hoc networks for spontaneous data exchange
- Ad-hoc connection of different networks (e.g. laptop ↔ mobile or phone ↔ GSM ↔ net)
- Applications similar to applications based on infrared technology
- Weaknesses of infrared technology were overcome
 - Increased bandwidth (up to 865.2KBit/s)
 - No optical connection between devices necessary
 - Expanded range (up to 10m)
 - Allows setting up of ad-hoc networks instead of point-to-point connections

- Q 7c) Can you explain briefly the concept „Data section“?



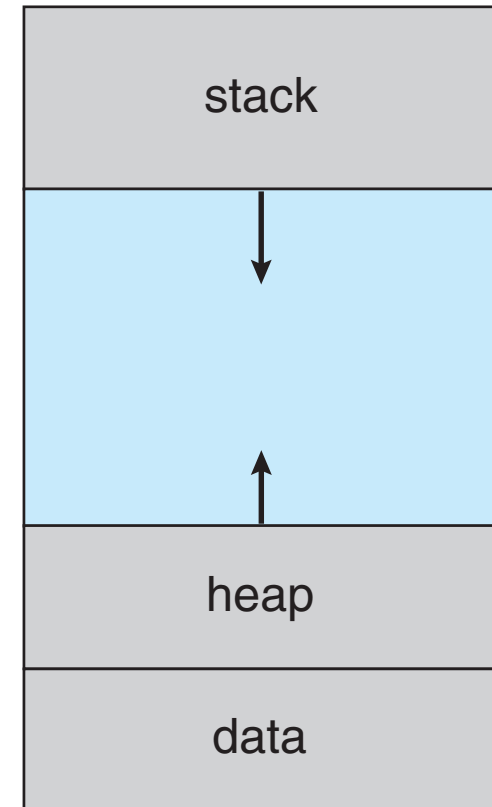
c) What is a process? What does it do, what does it use and how is the mobile operating system involved?

- A process is a program “in operation”.
- A process uses resources, such as CPU time, memory, files, and I/O devices.
- The resources of a process are allocated while it is created or when it is running.
- The operating system has to manage the process (creation, resource distribution, etc.).

Components of a Process

- More than simple code!
- Program counter: Indicates on which point in the code the process resides.
- Contents of the process registers:
 - **Stack:** Contains temporary data, such as subroutine parameters or return addresses, etc.
 - **Data section:** Contains the global variables
 - **Heap:** Dynamically allocated memory

max



Thank you!