mobile business

Lecture 14

Q&A Session

Mobile Business I (WS 2019/20)

Prof. Dr. Kai Rannenberg

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

mobile business

Lecture 2

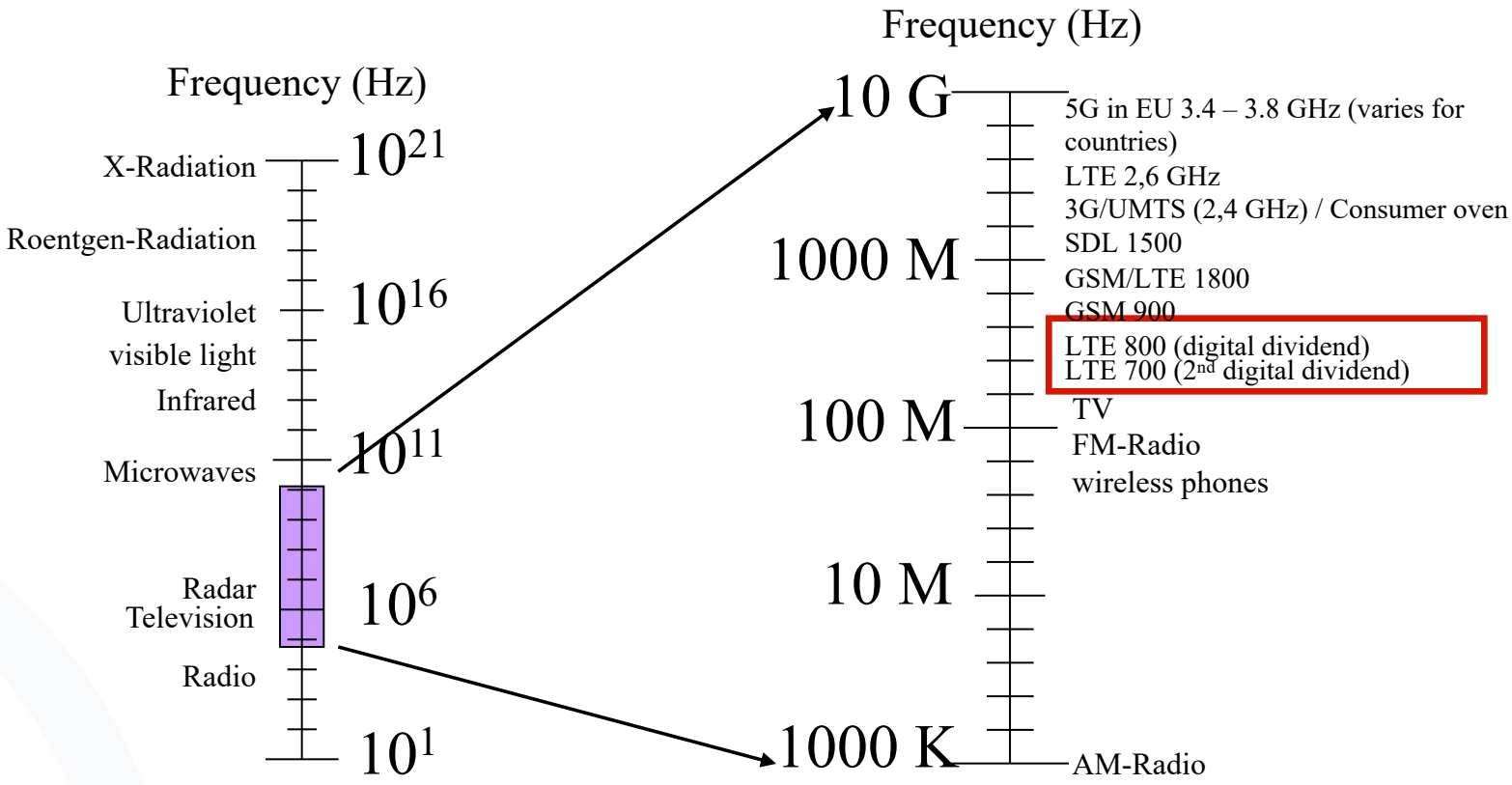
Question 1

- Slide 12: Could you please explain the term “digital dividend”?
- Could you please explain again the main idea behind slide 12?

Cell Based Communication (CBC)

Spectrum Ranges

Frequency range of instruments of entertainment and communication electronics



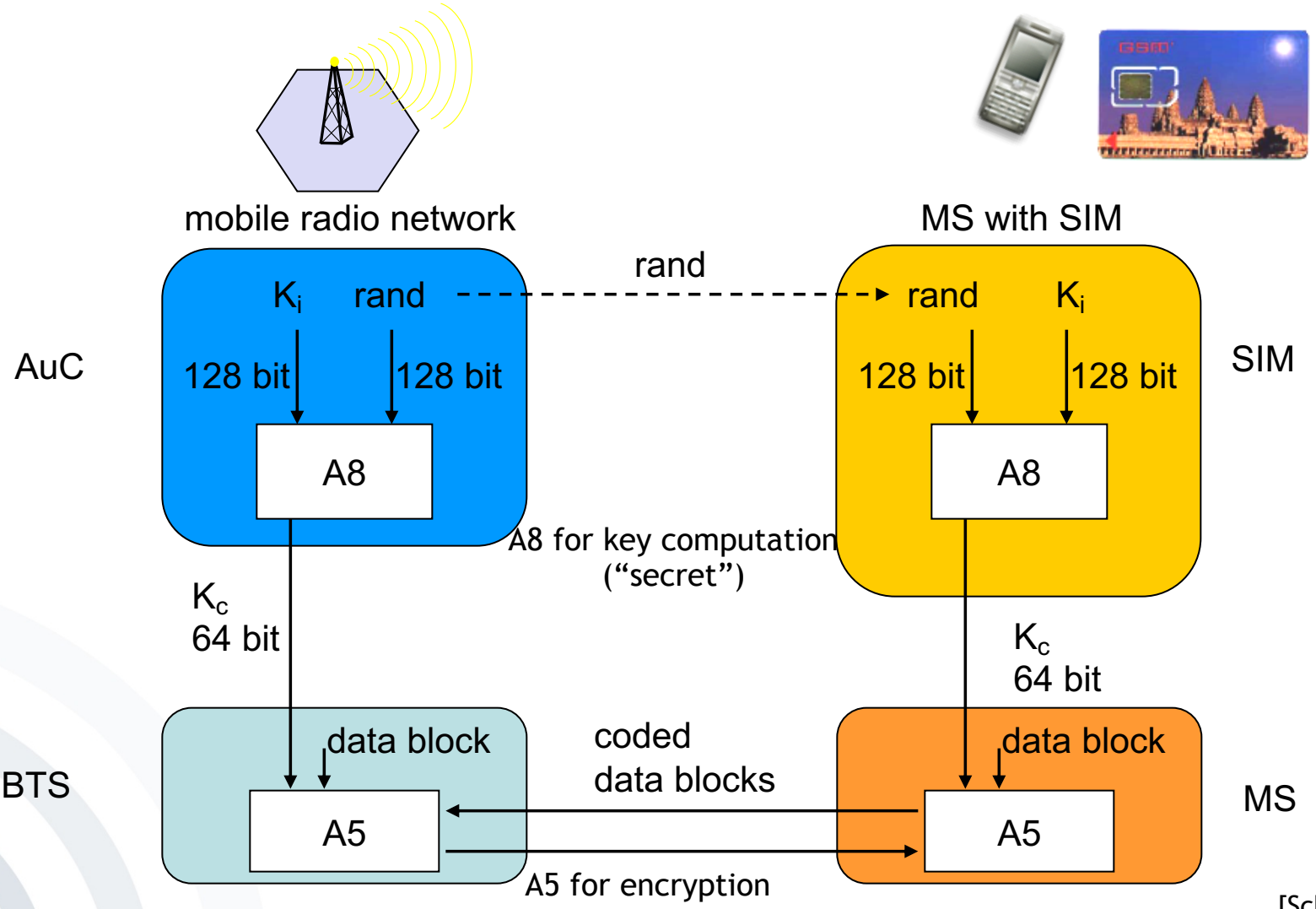
Cf. [Heise2014] for more information on discussion related to the digital dividend.

Question 2

Could you please explain again slide 34?

GSM (2G)

Security Model – Encryption



[Schiller2003]

Question 3

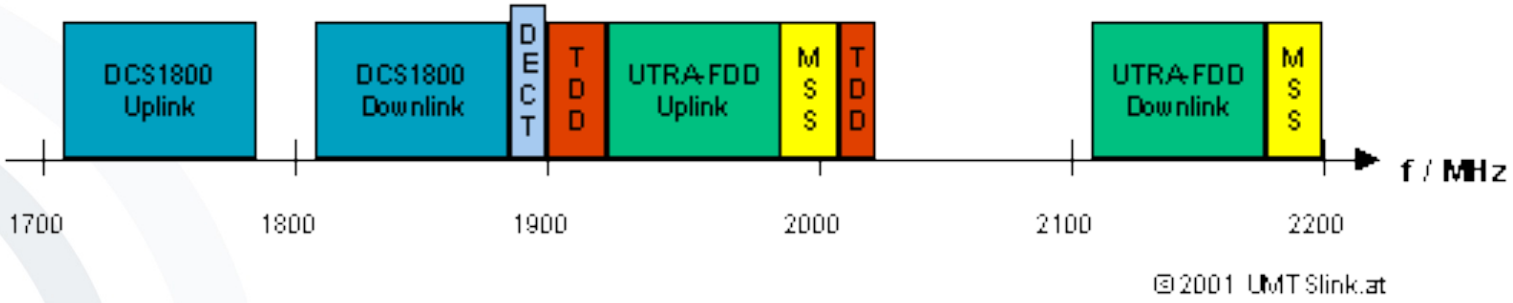
Slide 42: Please explain this slide again.

UMTS (3G)
Frequencies

- ***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:



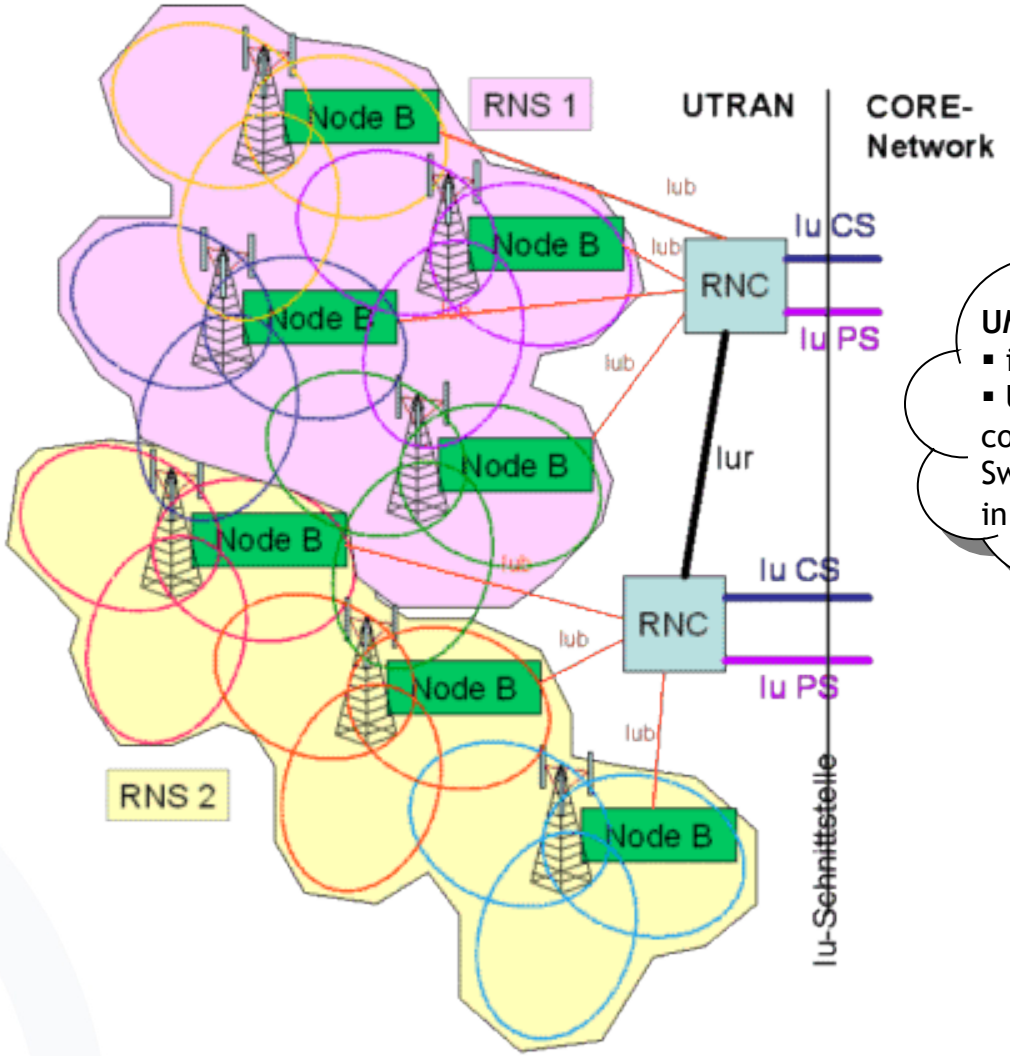
UTRA-FDD: UMTS Terrestrial Radio Access – Frequency Division Duplex [UMTSLink2006]

Question 4

Slide 43: Do we also have to know the UMTS System Architecture in detail? (in addition to the GSM System Architecture?)

UMTS (3G) System Architecture

- ***UTRAN:*** UMTS Terrestrial Radio Access Network
- ***RNS:*** Radio Network Subsystem
- ***RNC:*** Radio Network Controller (controls the Node Bs)
- ***Node B:*** UMTS base stations (equivalent to base transceiver stations (BTS) in GSM



UMTS Core network
- is not shown here in detail
- UMTS Core network corresponds to Network- & Switching Subsystem (NSS) in GSM

Source: UMTSlink.at (2011)

Question 5

Slide 53: Is a handover also defined as roaming?

Roaming
Overview

- Roaming denotes a change of network access, e.g.:
  - Change of the GSM network operator
  - Change between different network systems (UMTS, GSM, WLAN, CDMA, PDC)
  - Cell change within the GSM system (Handover)
- Roaming usually means extensive changes, e.g. of the network technique or the network operator, and with a new authentication:
  - ***Example:*** The mobile device automatically logs into an available WLAN when a hotspot is entered (e.g. airport, conferences).

Lecture 3

Question 1

To what extend do we have to study slides like slide 7? What is the main idea behind this slide?

mobile business

Wireless LAN Basics
802.11 Standard

Standard	Description
802.11	Protocol for transmission methods for wireless networks, defined in 1997 for **2 MBit/s** at 2,4 GHz
802.11a	Wireless LAN **up to 54 MBit/s** at 5 GHz
802.11b	Wireless LAN **up to 11 MBit/s** at 2,4 GHz
802.11f	Roaming between access points of different manufacturers (published in 2003 and withdrawn by IEEE in 2006) [IEEE2010]
802.11g	Wireless LAN **up to 54 MBit/s** at 2,4 GHz
802.11i	Extended security features: AES, 802.1x, TKIP
802.11n	Wireless LAN **up to 450 MBit/s** when using 3 spatial streams (3x 150 Mbit/s) at 2,4 GHz or 5 GHz *)
802.11r	Fast Roaming/Fast BSS Transition
802.11ac	Wireless LAN using 3 spatial streams at 5 GHz: **Up to 1.3 GBit/s** (3x 433 Mbit/s) or even **up to 2.6 GBit/s** (3x 867 Mbit/s, part of *802.11ac Wave2*) *) **)
802.11ad	Wireless LAN at 60 GHz: **Up to 7 GBit/s**
802.11ah	Wi-Fi HaLow for Smart Home and connected devices (900 MHz, increased distance, ~1km)
802.11aj	A rebanding of 802.11ad for use in the 45 GHz unlicensed spectrum in some regions of the world (specifically China)
802.11ax	Upcoming Standard operating in the existing 2.4 GHz and 5 GHz spectrums but incorporating additional bands between 1 and 7 GHz. Expected to achieve 4x increase to user throughput

*) 802.11n and 802.11ac data rates depend on the number of antennas and spatial streams (“parallele räumliche Inhaltsströme”) supported by the hardware. 802.11ac devices often support 3 streams at most. 802.11n specifies a maximum of 4 streams, 802.11ac a maximum of 8 streams.

**) 802.11ac is a 5 GHz-only standard, so dual-band access points and clients will probably continue to use 802.11n at 2.4 GHz in parallel.

[IEEE] [Sauter 2008]

Question 2

Slide 14/15: Which one is currently a secure pre-shared key encryption method? WPA2, although there are KRACKs against it?

Wireless LAN
State-of-the art Encryption

- **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).

Key Reinstallation Attacks (KRACKs) against WPA2

- The attack is mainly against the ***4-way handshake*** of the WPA2 protocol.
- The 4-way handshake protocol is mathematically proven, but it only assures the negotiated key remains secret, and that handshake messages cannot be forged.
- The attack doesn't leak the encryption key, but sensitive information (usernames, passwords, …) can be stolen.
- Discovered by Mathy Vanhoef – a post-doctoral researcher at *KU Leuven*
- *Background material and video on the attack via* https://www.krackattacks.com

Question 3

- Could you please explain again the graphic on slide 36?
- Slide 35/36: Could you please explain again the concept of RAN/IP RAN?

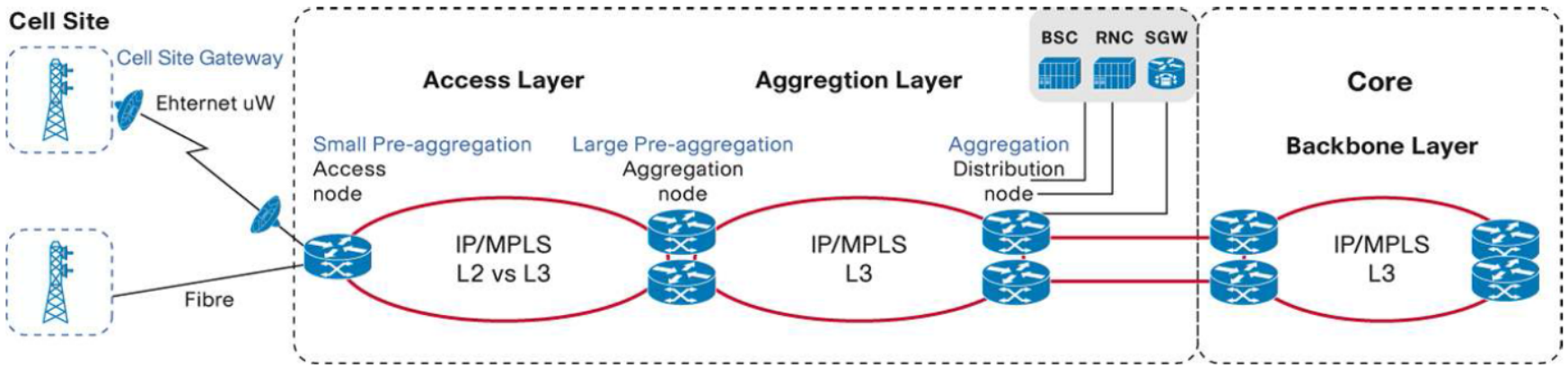
Radio Access Networks (RAN)

- Part of a mobile telecommunication system
- Provides connection between device (phone, computer, or machine) and core network
- Implements certain radio access technologies, e.g. GSM or 3G
- Examples of radio access network types are:
  - **GRAN:** GSM radio access network
  - **GERAN:** essentially the same as GRAN but specifying the inclusion of EDGE packet radio services
  - **UTRAN:** UMTS radio access network
  - **E-UTRAN:** Long Term Evolution (LTE) high speed, low latency radio access network
  - **C-RAN**: Centralized or Cloud-based radio access network
- Some handsets have capability to be simultaneously connected to multiple RANs (dual-mode handsets).

[Wiki 2014]

IP-based Radio Access Networks (IP RAN)

- All different backhaul technologies may be collapsed onto a single IP/MPLS network (MPLS = Multiprotocol Label Switching) → End-to-end IP approach
- Support for legacy services and reduced cost per bit
- 2G, 3G, and 4G radio technologies transparently supported
- Cost savings possible due to alternative transport media (such as Ethernet and DSL)



[Cisco 2011] [Cisco 2014]

Lecture 4

Question 1

Is the annex also relevant for the exam?

Slide 33: VoIP (ENUM) - how is ENUM working?

IP-based Mobile Services
Voice over IP: Overview

- In order to compensate transmission problems (lost packets, speech disruption, etc.) buffers are used.
- In VoIP systems, users can be identified by their:
  - Nicknames (e.g. Skype, Freeworlddialup)
  - Phone number (Sipgate)
  - Phone number (using ENUM – "***t**elephone **nu**mber **m**apping" for mapping telephone numbers to Internet-addresses* - RFC 3761)

Lecture 5

Question 1

Slide 34/35: Please explain again.

Multi Channel Management Possible Scenarios

Multi Channel Management of mobile applications becomes increasingly complex.

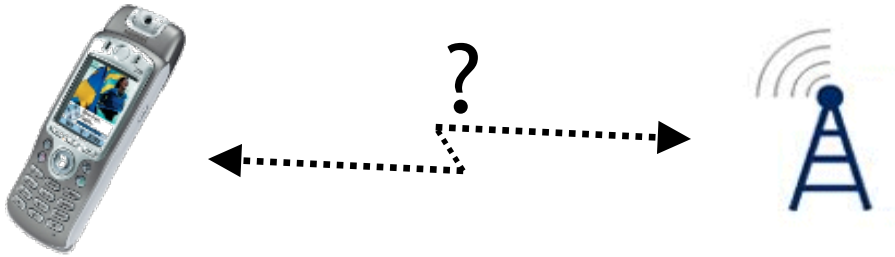
Multimedia Content	Bearer Service	User Agent	
WBMP Images	CSD	WAP Browser	
Color Images	GPRS	HTML Browser	
Multimedia Streams	UMTS	HTML Browser	
Video Telephony	LTE	Apps	

[Example Multi Channel Management Scenarios]

Technological Challenges
Multi Channel Management

- User Agent Detection can be implemented by the providers of mobile applications.

- Only network operators can identify the data transfer services used by the user (bearer detection).



Question 2

Slide 44: Please explain again.

Conclusion
E-Business vs. M-Business

- Convergence of Mobile and Fixed Networks:
  - Deutsche Telekom reintegrated T-Mobile.
  - Vodafone reintegrated Arcor and bought Kabel Deutschland and ONO.
  - O_2 (Telefónica) bought HanseNet.
  - …

→ Will E-Business and M-Business converge?

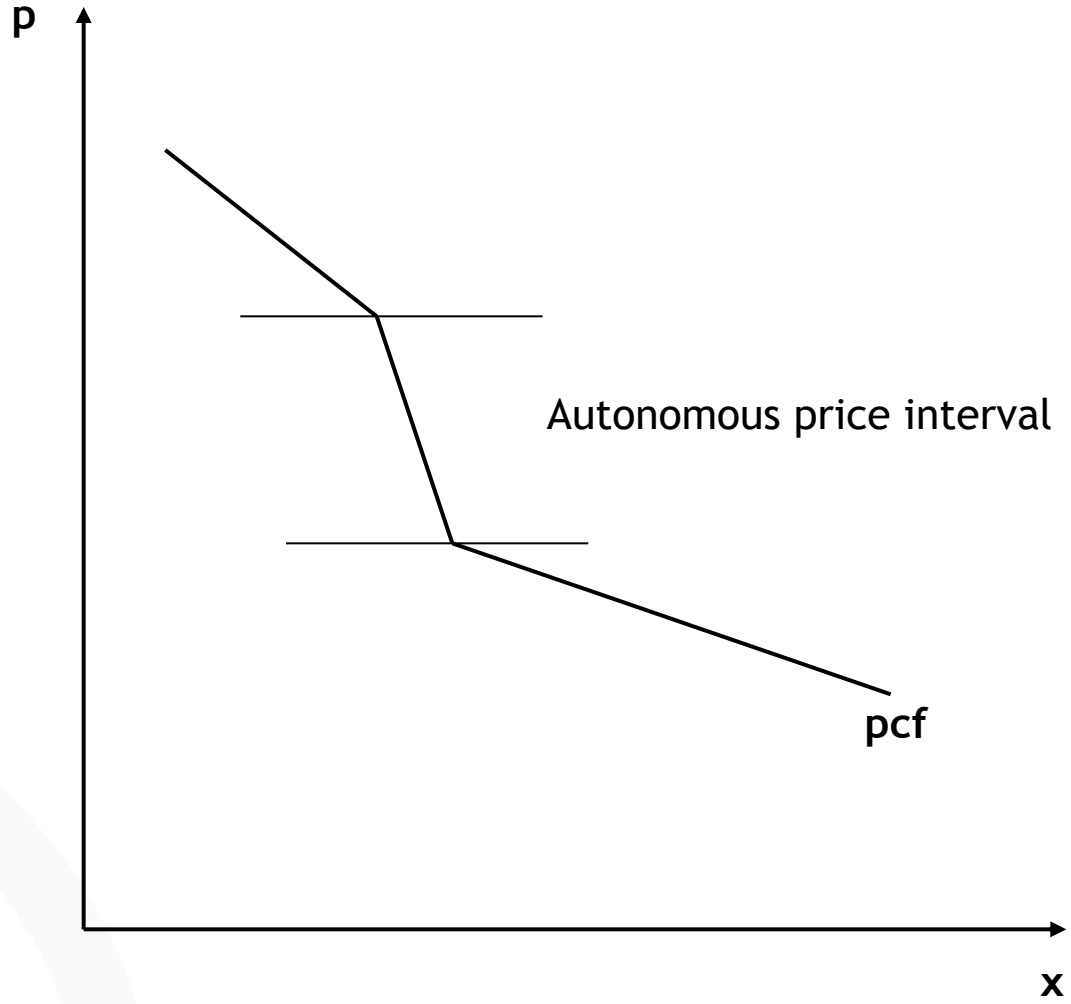
mobile business

Lecture 6

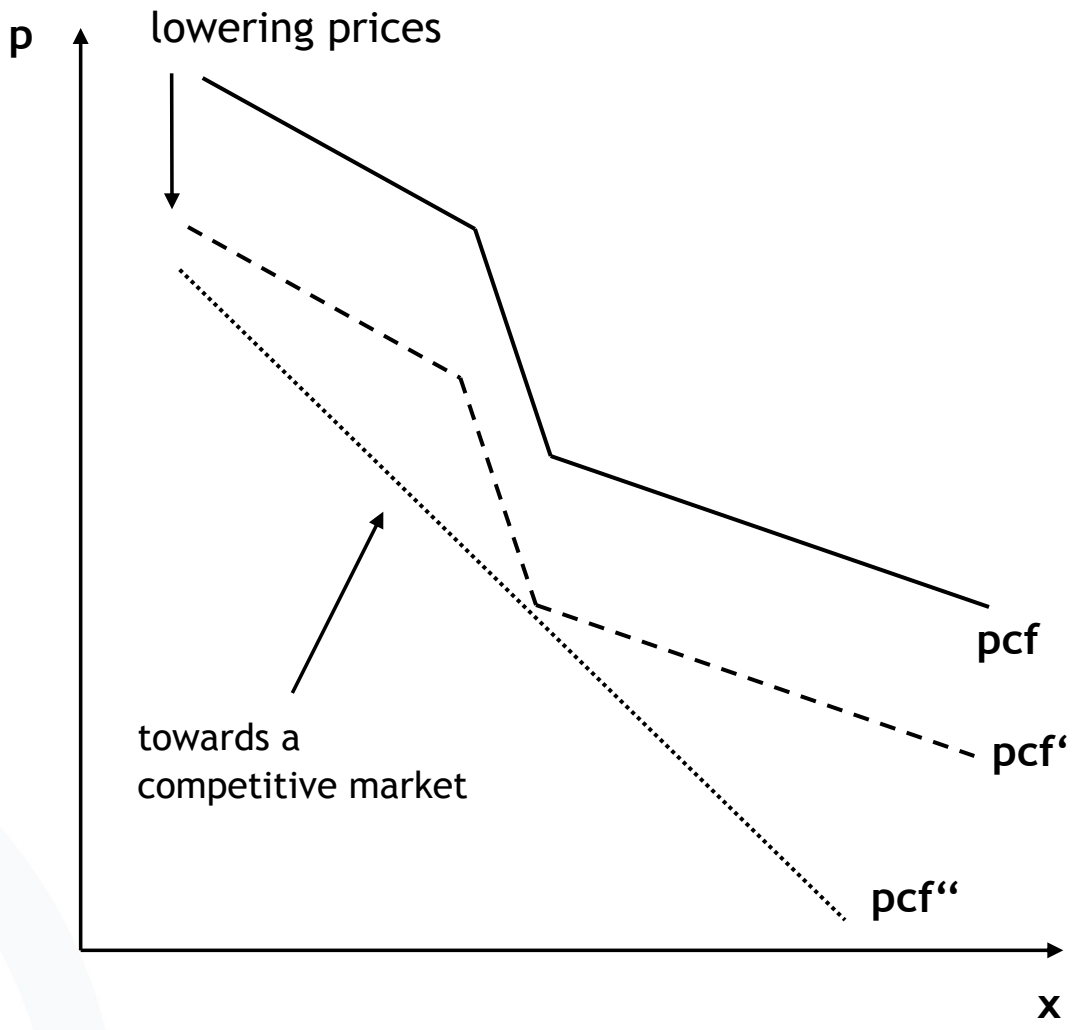
Question 1

Could you please explain again the price-consumption function (Slide 28 vs slid 33)?

Price-consumption function in a heterogeneous oligopoly (Gutenberg)



MVNO driven change of price-consumption function

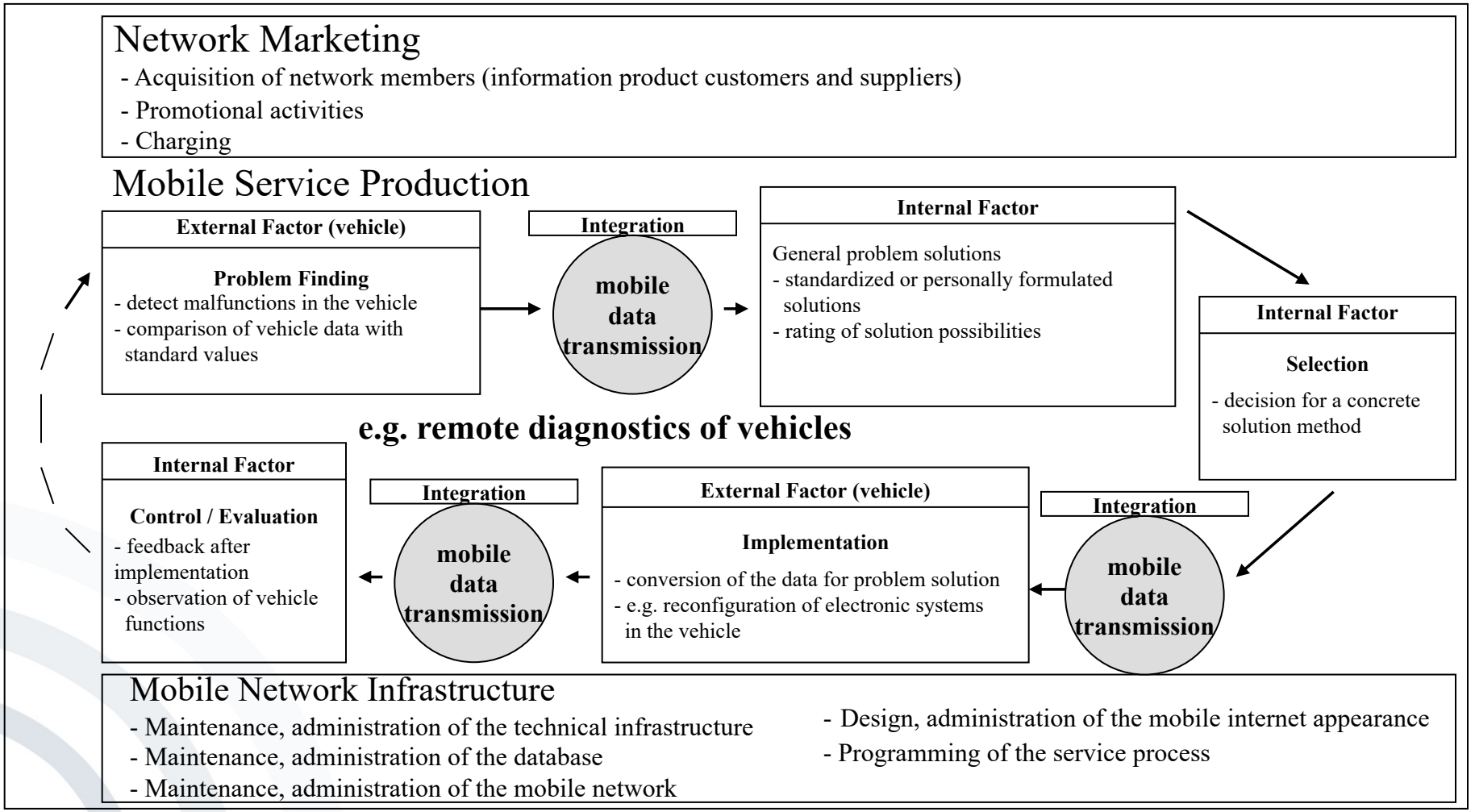


Question 2

what is the main idea behind slide 44?

Value Creation

- Value added shop [ReicMeieFrem2002]



Lecture 7

Question 1

Do you expect us to know details such as the information on Slides 31-35?

Tariff Models

T-Mobile 2007:

Prices in € including value-added tax	T-Mobile Data 5	T-Mobile Data 30	T-Mobile web' n' walk basic	T-Mobile web' n' walk medium	T-Mobile web' n' walk large
minimal runtime	24 months	24 months	3 months	3 months	3 months
monthly price of options	5,00	10,00	20,00	35,00	50,00
inclusive volume	5 MB	30 MB	200 MB	400 MB	5 GB
price of volume per started data bloc beyond the inclusive volume;	3,00	1,90	0,80	0,80	0,50
unit of account	1 MB	1 MB	1 MB	1 MB	1 MB

[T-Mobile, 9/2007]

Tariff Models

Deutsche Telekom 2013:

Prices in € including value-added tax	Mobile Data eco S	Mobile Data eco M	Mobile Data eco L	Mobile Data eco XL
minimal runtime	24 months	24 months	24 months	24 months
monthly price of options	19,95 €	29,95 €	49,95 €	69,95 €
inclusive volume	1 GB	3 GB	10 GB	30 GB
Extras	Inclusive LTE	Inclusive LTE Hotspot Flat	Inclusive LTE Plus Hotspot Flat Internet Telephony	Inclusive LTE Plus Hotspot Flat Internet Telephony

[Deutsche Telekom, 10/2013]

There are often multidimensional tariffs in mobile communications.

Tariff Models

Deutsche Telekom 2015:

	MagentaMobile			
Prices in € including VAT	S	M	L	L Plus
minimal runtime	24 months			
monthly price of options	26,95 €	35,95 €	44,95 €	71,95 €
inclusive volume	500 MB	2 GB	4 GB	10 GB
speed	LTE 150	LTE 150	LTE 300	LTE 300
Extras		VoIP	VoIP	VoIP Hotspot Flat 100 min/SMS abroad

There are often multidimensional tariffs in mobile communications.

[Deutsche Telekom, 10/2015]

Tariff Models

Deutsche Telekom 2017:

Prices in € including VAT	Data Comfort S	Data Comfort M Eco	Data Comfort L Eco
minimal runtime	24 months		
monthly price of options	14,95 €	19,95 €	29,95 €
inclusive volume	2 GB	4 GB	10 GB
speed	LTE Max	LTE Max	LTE Max
Extras	VoIP	VoIP	VoIP

[Deutsche Telekom, 10/2017]

Tariff Models

Deutsche Telekom 2018:

Prices in € including VAT	Data Comfort S	Data Comfort M Eco	Data Comfort L Eco
minimal runtime	24 months		
monthly price of options	13,45 €	17,95 €	26,95 €
inclusive volume	2 GB	4 GB	10 GB
speed	LTE Max	LTE Max	LTE Max
Extras	VoIP	VoIP	VoIP

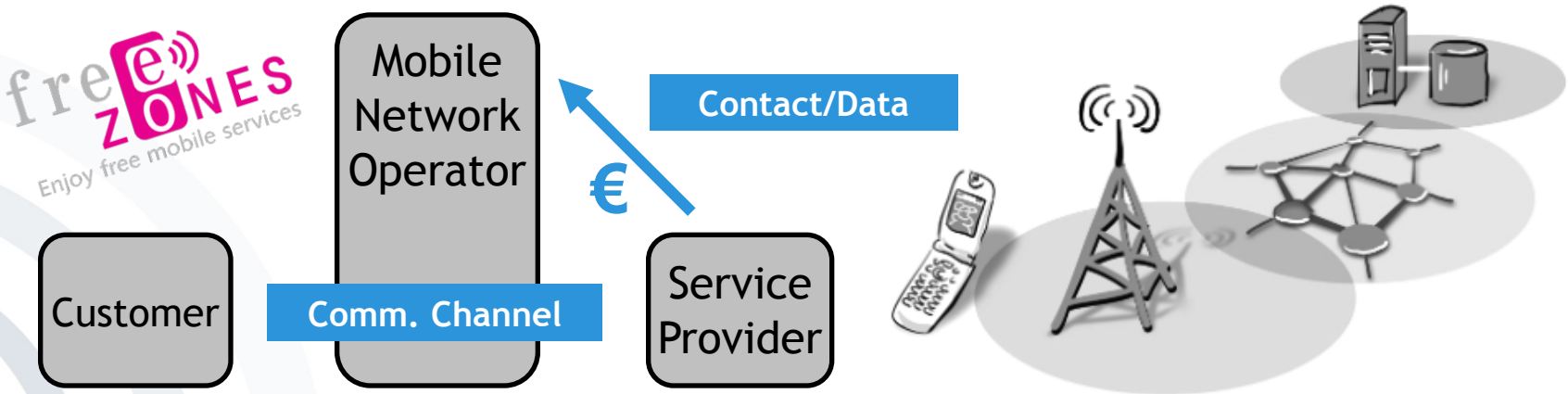
[Deutsche Telekom, 11/2018]

Question 2

Slide 47: New business model (who are service providers? - banks?)

Developing a Value Proposition: Freezones

- **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.



Question 3

- Slide 53: Could you please show the correct answer. Will there be a task like this in the exam?
- Could you provide the solution for slide 53 again?

Business Models: Revenue Models

- 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

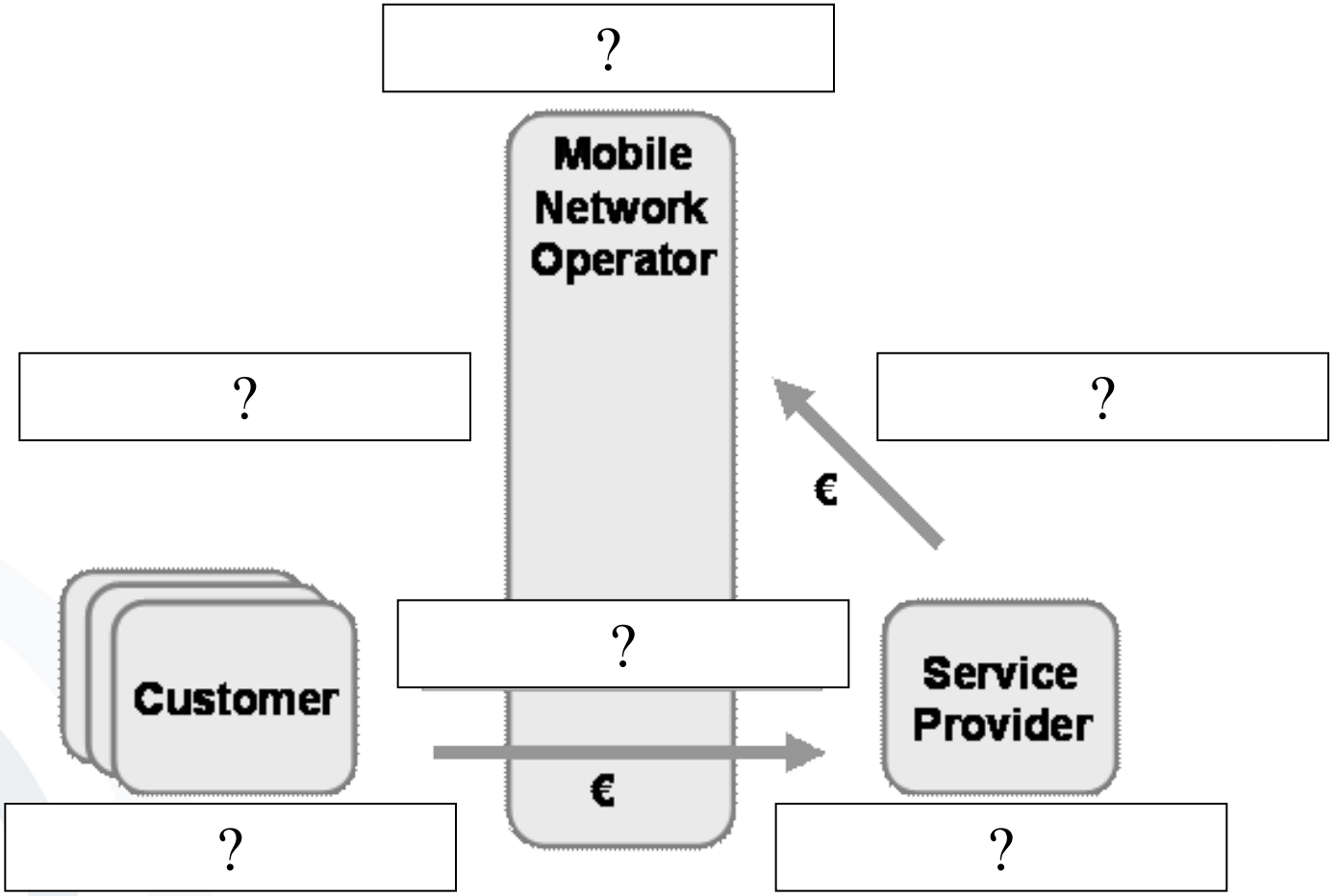
    ➲ 10€ expenditures per customer (by the service provider) and 1,8m € revenues for the operator.

    ➲ Revenues of the operator: 0m € + 1,8m € = 1,8m €

    ➲ Revenues of the service provider: 3,6m € - 1,8m € = 1,8m €

New Business Models: Revenue Models

- New revenue flows



Business Models: Revenue Models

- New revenue flows:
  - Assumptions:
    - Service provider obtains a 15% discount on data transfer: 30 MB only for 8.50 €.
    - Service provider obtains economies of scale which is just possible in this revenue model.

Business Models for Mobile Network Operators

In summary:

- Towards the customer the value proposition and the value creation architecture are the same as in classical business models.
- Towards the advertising service provider the value proposition is the offering of customer contacts.

Differences in revenue and pricing

Question 4

Slide 56: Why CPT if he pays 1,8 for our data? (ex. 52)

Business Models for Mobile Network Operators

Revenue model:

Towards customer indirect revenue model:

- Data costs are eliminated for customers.
  - ➲ Revenue via advertisements

Pricing model:

Static pricing for advertising party based on CPT (contact price per thousand)

Lecture 8

- CamWebSim: is this relevant? Do we need to study the codes?
- Slide 43-50: Please explain again.

CamWebSIM (Slide 43)

- A smaller personal security device

HTTP server (!) in the GSM SIM card

- A SIM based on the MS Smart Card can be programmed

Connection between GSM and Internet

- HTTP Requests via HTTP/SMS Gateway to mobile phone

More than a cool demo …

- Explore the relation between PDAs and Smart Cards
  - What can really be done on the Smart Card?
  - Can Smart Card encrypt info to be stored in the PDA?
- Explore the possibilities of extra interaction channels
  - SMS in parallel to Internet
- Research Authorisation vs. Authentication vs. Identification

CamWebSIM (Slide 44)

Combine Infrastructures

http://www.camwebsim.telco.com/+14253334711/dt=(Hello World)

SIM Addressing via HTTP (Slide 45)

- Website
  - http://www.camwebsim.telco.com/
- Tel-No.
  - +14253334711/
- Command (SIM AT V 2.0 ++)
  - dt=(Hello World!)
  - LOCATION INFO **`info`**
  - SELECT ITEM **`si=(title,item1,item2,…)`**
  - DISPLAY TEXT **`dt=(text)`**
  - GET INPUT **`gi=(text)`**
  - MAIL NOTIFICATION **`mail=(who,subj,phone)`**
  - SIGN CHEQUE **`cq=(who,amount)`**

Website

Tel.-No.

Command

SIM based Payment Authorisation (Slide 46)

.com.

WELCOME ADDRESS ITEMS WRAP SHIP PAY CONFIRM

- More Payment Channels
  - Telephone Bill
  - …

si=(Toys.com 3 Gimmicks, Pay $ 27.80, Cancel, Help)

Payment Authorisation live (Slide 47)

HTTP-Request

HTTP-Response

Response Data
via SMS

Internet

HTTP/SMS
Gateway

CamWebSIM

www.camwebsim.telco.com/+14253334711/
si=(Toys.com 3 Gimmicks, Pay 27.80, Cancel, Help)

What have we done in this example? (Slide 48)

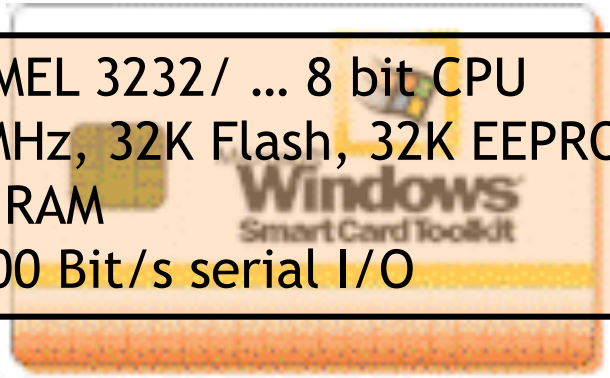
- Technologywise
  - Connected a smart card to the Internet
    Goal: transparent, uniform access to smart card services
  - Used the mobile phone as a trusted device
    Assumed a secure path between SIM and display/keyboard
    ! This might be (more) dangerous with more complex phones
  - Used the existing GSM infrastructure and security model for payment authorisation
    User authentication key is stored in the SIM
  - …

What have we done in this example? (Slide 49)

- Applicationwise
  - …
  - Used the existing GSM infrastructure and security model for payment authorisation
    User authentication key is stored in the SIM
  - *Provided a telecom with a new revenue channel based on an existing process*
    Telecoms as payment servers (the Teletext model)
  - *Enabled cash-like payment for Internet services*
    In countries where one does not need to register a name with a prepaid GSM account

Technical Details and Issues (in 2001) (Slide 50)

ATMEL 3232/ … 8 bit CPU
5 MHz, 32K Flash, 32K EEPROM, 1K RAM
9600 Bit/s serial I/O



Sagem Smart Card

SMS limits

- No guaranteed delivery times
- 140 “real” Bytes just cover a 128 Bytes signed message ...
- ... and sometimes not even that
- We look forward to GPRS.

Space limits

- More than 32K in the chip would be helpful.

Phone capability limits

- SIM Application Toolkit Support is being interpreted widely …

SIM Addressing via HTTP indication application areas
(Slide 51)

- Website
  - http://www.camwebsim.telco.com/
- Tel-No.
  - +14253334711/
- Command (SIM AT V 2.0 ++)
  - dt=(Hello World!)
  - LOCATION INFO **info**
  - SELECT ITEM **si=(title,item1,item2,…)**
  - DISPLAY TEXT **dt=(text)**
  - GET INPUT **gi=(text)**
  - MAIL NOTIFICATION **mail=(who,subj,phone)**
  - SIGN CHEQUE **cq=(who,amount)**

Website

Tel.-No.

Command

- Slide 32: Please explain again.

ISIM

IP Multimedia Services Identity Module (Slide 29)

- An **IP Multimedia Services Identity Module (ISIM)** is an application running on a UICC smart card in a 3G mobile telephone in the IP Multimedia Subsystem (IMS).
- It contains parameters for identifying and authenticating the user to the IMS.
- The ISIM application can co-exist with SIM and USIM on the same UICC making it possible to use the same smartcard in both GSM networks and earlier releases of UMTS.
- It is specified in 3GPP TS 31.103 [3GPP2016] and described in e.g. [GSM2006].

ISIM

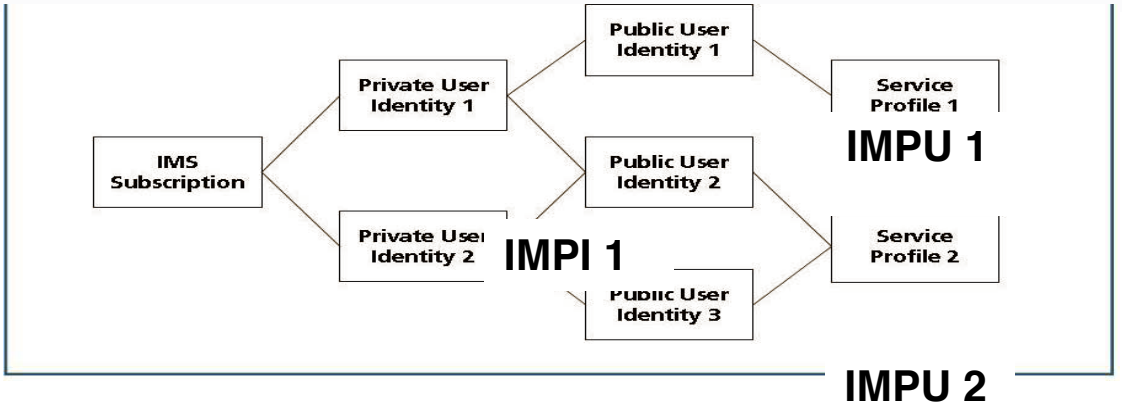
User Identifiers ("Identities") and Secret (Slide 30)

- The ISIM contains:
  - One "IM Private Identity"
  - One or more "IM PUblic Identities"
  - A long-term secret used to authenticate and calculate cipher keys
- The IM **Private** Identity (IMPI)
  - Unique global identifier per IMS subscriber: username@operator.com
  - Assigned by the home network operator
  - Used for e.g. registration, authorisation, administration, and billing
  - Not accessible to the user
  - Only visible to control nodes inside the IMS
  - One ISIM application includes only one IMPI – but an IMS user may have several UICC cards carrying an ISIM application or a UICC card with several different ISIM applications.
- IM **PUblic** Identities (IMPUs)
  - Every IMS subscriber has one or more IMPUs, e.g. user@operator.com, or tel:+1-212-555-12345.
  - Used for requesting communications to other users
  - Visible to the outside, e.g. to be shown on a business card

- Service Profile
  - identifies the services a user may currently use such as video telephony, VoIP, Presence
  - defined and maintained in the Home Subscriber Server (HSS) of the subscriber's home network
- Home domain name
  - The ISIM application stores the home domain name of the subscriber securely.
  - This can not be changed or modified.

ISIM

IMPIs, IMPUs, and Service Profiles (Slide 32)



- In case of more than one IMS subscription, there may be a many-to-many mapping of IMPIs to IMPUs.
- Each IMPU is assigned exactly one Service Profile, but a Service Profile may be assigned to more than one IMPU.

Lecture 11

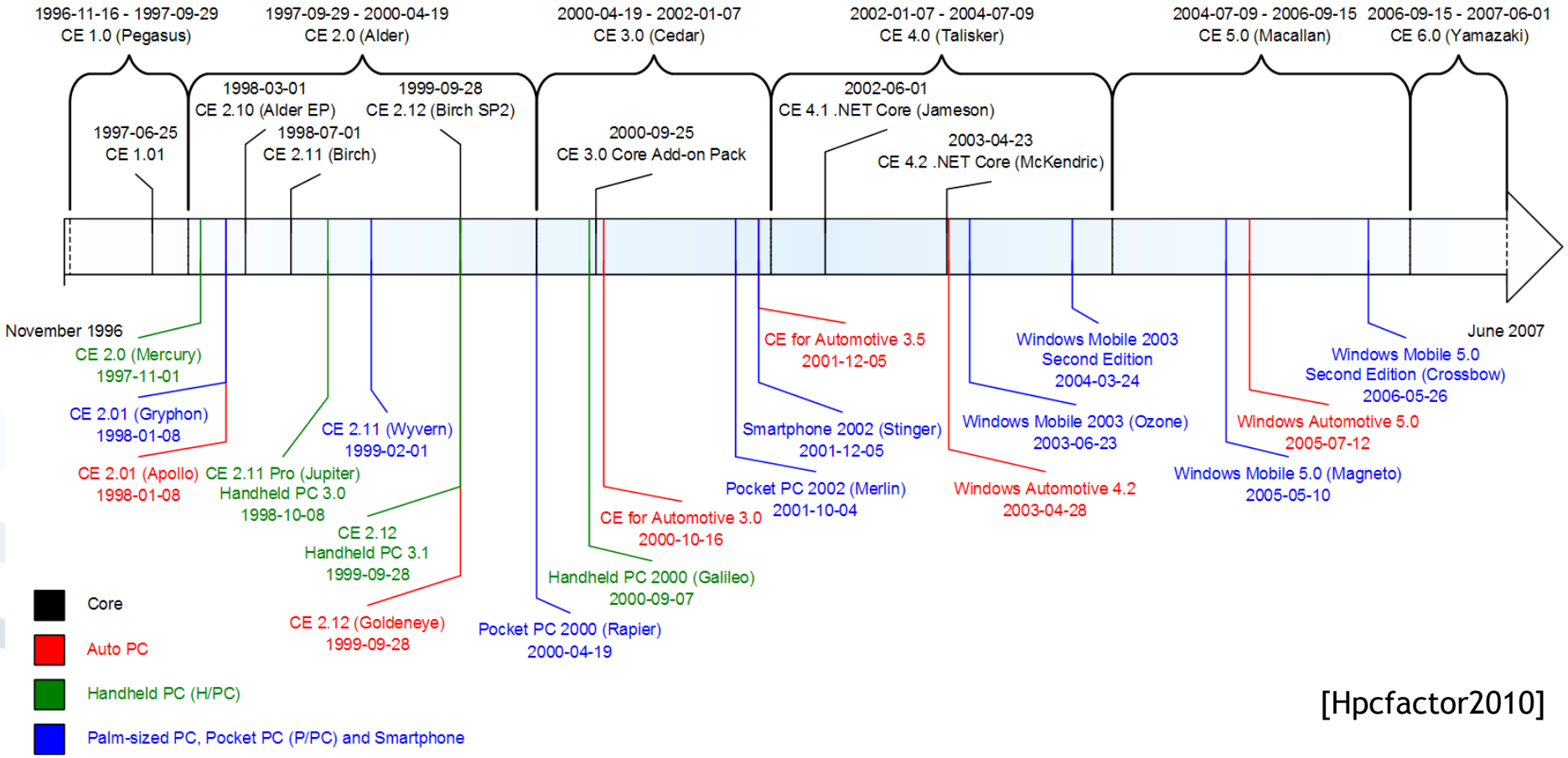
- Could you explain again what is relevant on Slide 43?

- Slide 55: do we have to study all mobile threats? Or is this just an overview?

Windows CE, Pocket PC, Pocket PC Phone Edition, Mobile History (Slide 43)

Windows CE Timeline

Source: "A Brief History of Windows CE" (http://www.hpcfactor.com/support/windowsce/), *HPC:Factor*, retrieved May 21, 2007



[Hpcfactor2010]

Timeline mobile threats 2004-2016 (Slide 55)

[Sophos2016]

Lecture 12

- Slide 21: could you please explain what the main idea is? Do we have to study things like this in detail?

mobile business

Standardisation Activities (Slide 21)

Organization/ Project	Participants	Goals	Results
Mobile Phone Work Group of the TCG (since 2005)	Nokia and a "large number of wireless vendors, component manufacturers and mobile service or content providers"	Adaptation of TCG specifications to mobile device requirements	Reference Architecture and trusted Module Specification
Trusted Mobile Platform project (2003/2004)	Intel, IBM, NTT DoCoMo	Architecture definition of a trusted execution environment at different trust levels	Hardware and Software Architecture Description, Protocol Specification
GSM Association / Mobile Application Security (since 1995)	Mobile Operators (Vodafone, Orange, T-Mobile, France Telecom)	Definition and promotion of a Mobile Application Security Framework for open operation system platforms	Application Security Terminal Requirements based on domain model and terminal security policies, Application Certification Program
OMTP Group (2004 -2010) Application Security Project Trusted Environment Project	Mobile Operators, Equipment Manufacturers, Service Providers	• Open framework for mobile device manufacturers and associated software and hardware suppliers • Definition for hardware-based security functions	Application Security Framework
Security Working Group of the Open Mobile Alliance (OMA) (since 2002)	Mobile Operators, Equipment Manufacturers, Service Providers	Specification of the operation of security mechanisms, features and services for mobile clients, servers and related entities	Specifications of Wireless Transport Layer Security, Wireless Identity Module, Wireless Public Key Infrastructure, Smartcard Web Server, and other requirements for application layer and transport layer security
GlobalPlatform (since 1999)	Mobile Operators, Payment Associations, Public Sector Organisations and Government Agencies	Creation and publishing of specifications for secure chip technology	GlobalPlatform Card Specification

Based on [PiskRannRoss2005]

Guest Lectures

Guest Lectures

- To what extend do we have to study the case studies that we worked on in class? If it is relevant is it possible to provide a specific solution for example for the digital wallet?

mobile business

Thank you!

Contact: mob1@m-chair.de

GOETHE UNIVERSITÄT
FRANKFURT AM MAIN