

Lecture 14

Questions & Answers

Mobile Business I (WS 2024/25)

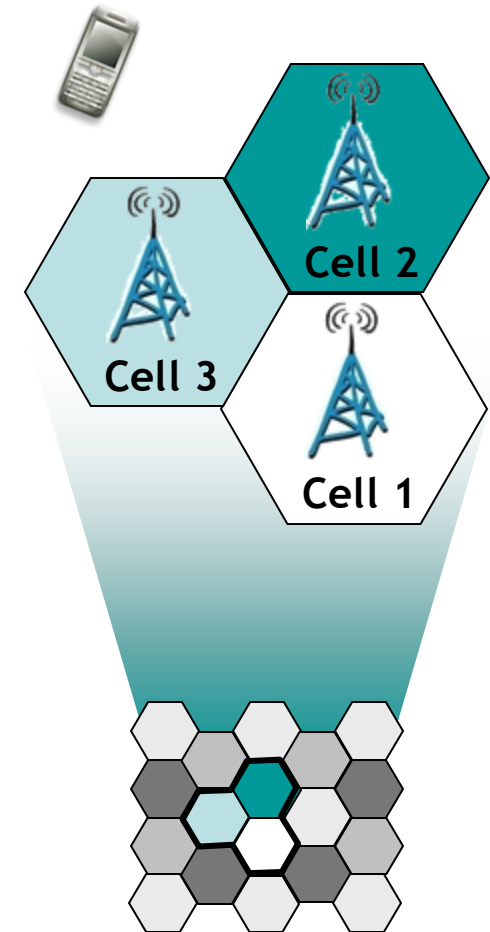
Prof. Dr. Kai Rannenber

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

- Could you please give us some advice on how to study for the exam? It is a lot of information and I am really struggling with learning facts by heart. For example, do we need to know every detail on the slide about every topic, or is it enough to focus on the general idea? Are there topics that are especially relevant?
- Will there be all lectures, guest lectures and exercises be relevant for the exam? → Yes
- Will the exam be like the mock exams or the old exams?
- **E04:** Other models (e.g. UTAUT and APCO) were mentioned in the exercise, but these were not part of the lecture. Do we also need to know these in detail for the exam? → Not in detail. Understanding the general academic concepts of different models in enough.

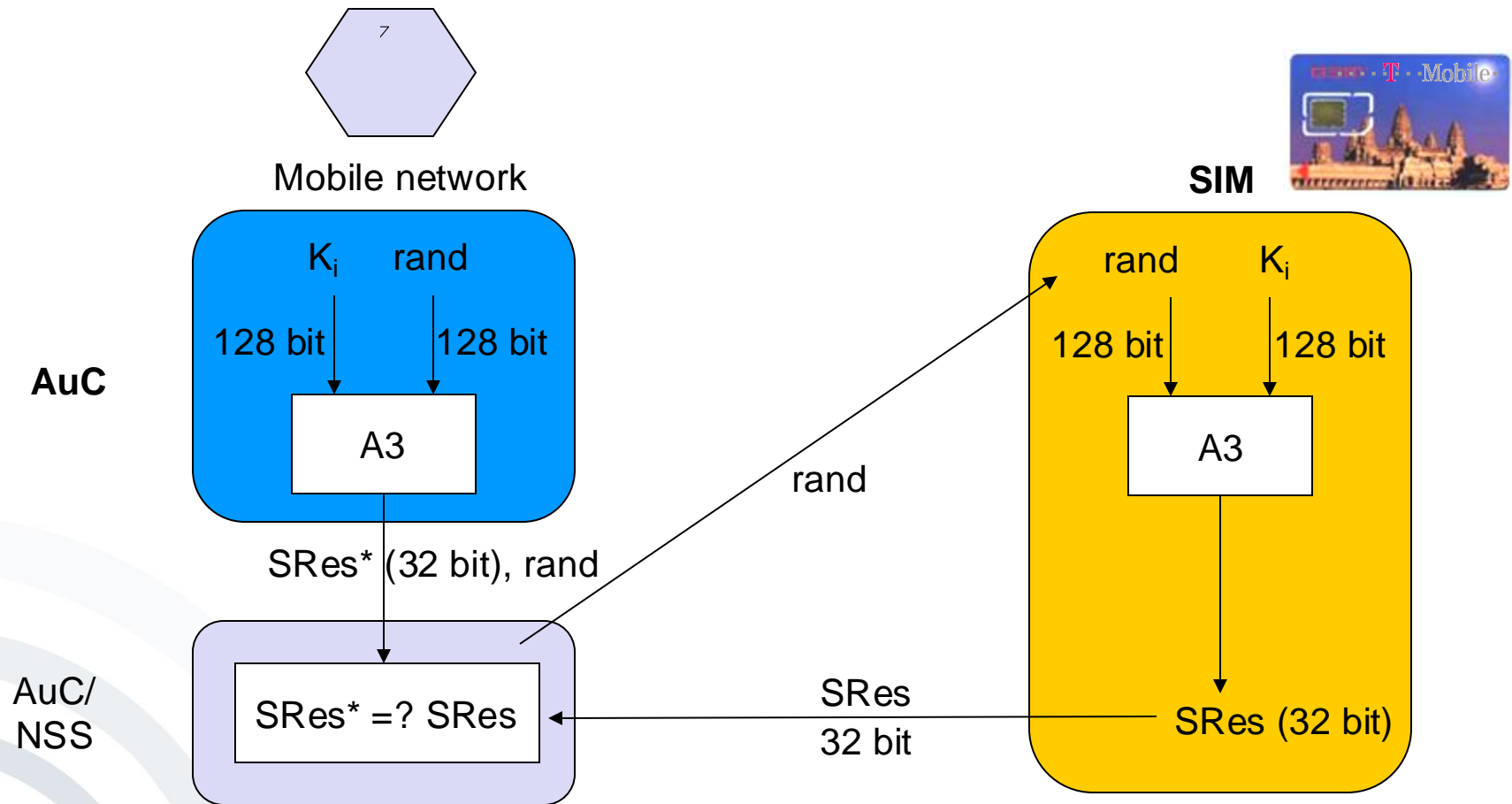
- L02:
 - Slide 8: how exactly is high capacity provided?
 - Slide 36: schema is unclear
 - Slide 48: last Sentence on the slide is not clear

- Cellular networks are radio networks consisting of several transmitters.
- Each transmitter or base station, covers a certain area ➔ *a cell*.
- Cell radii can vary from tens of meters to several kilometres.
- The shape of a cell is influenced by the environment (buildings, etc) and usually neither hexagonal nor a perfect circle, even though this is the usual way of drawing them.



- Cellular networks offer a number of advantages compared to centralised radio systems:
 - **Higher capacity:** Cells offer the possibility to “reuse” the transmission frequencies assigned to mobile devices (e.g. by multiplexing). In order to do so, the networks need a thorough planning of the position of base stations and their frequencies.
 - ➔ More users can use the infrastructure
 - **Reduced transmission power:** Reduced power usage for the mobile device, due to the fact that only a limited amount of transmission power is needed in a small cell, compared to a far away base station.
 - ➔ Reduced power consumption for mobile devices

- Challenge-response procedure



K_i : individual subscriber authentication key
 A3: („secret“) authentication algorithm

SRes: signed response

- 3G UMTS/HSPA/HSPA+ bandwidths
 - UMTS: 384 kbit/s downlink/uplink
 - High Speed Packet Access (HSPA) provides higher data speeds for downlink and uplink, e.g.
 - 7.2 or 14.0 Mbit/s downlink speed (HSDPA)
 - 1.4 or 5.7 Mbit/s uplink speed (HSUPA).
 - Evolved HSPA (HSPA+) using either *Multiple Input Multiple Output (MIMO)* or *Dual-Cell* technology provides
 - downlink speeds of e.g. 21,1 or 42,2 Mbit/s and
 - a maximum uplink speed of 11.5 Mbit/s.
 - But: Available bandwidth per user decreases if terminal is moving or if there are many participants in one radio cell.
- ➔ Bandwidths enable multimedia services

- L03:
 - We had the slides of “Key Reinstallation Attacks (KRACKs) against WPA2” & “WPA2-PSK- Handshake Protocol” (with the graph attached). At which point does the Key Reinstallation Attack take place? I assume that it will most likely occur during Message 3 or after Message 4.
- - L03 p. 38: Could you explain this slide again and state the key message?

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

[Wi-Fi 2010]

- There are three versions of **Wi-Fi Protected Access, WPA, WPA2 and WPA3:**



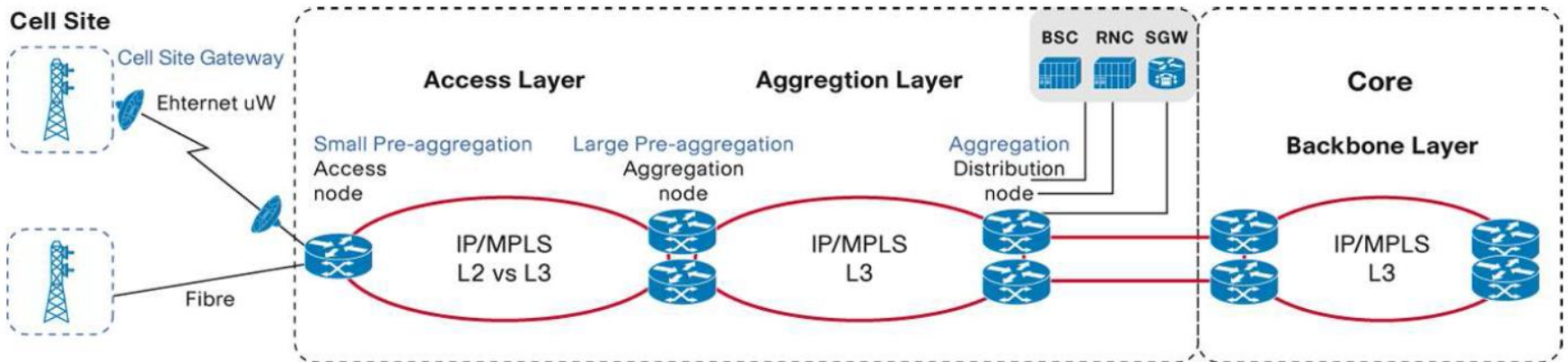
- **WPA** includes most of the 802.11i standard, but is **outdated and insecure** as it has various weaknesses:
 - Vulnerability to dictionary attacks when using a weak PSK
 - Other weaknesses inherited from earlier standards [ArsT 2008]
[ArsT 2008]
- **WPA2** includes **802.11i** to its full extent and also the Advanced Encryption Standard (AES).
- **WPA3** replaces pre-shared key (PSK) exchange with Simultaneous Authentication of Equals (SAE) exchange (IEEE 802.11s)

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>*

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)



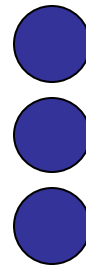
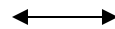
- - L06, p. 37: Here you talk about a 1st-tier and 2nd-tier structure.
Could you explain again what exactly is meant by this and put this slide in context with the previous slides?
- L07: -why the transaction independent and direct revenues has as example „in app subscription sales“?

- Also many providers in the second row (e.g. content providers)

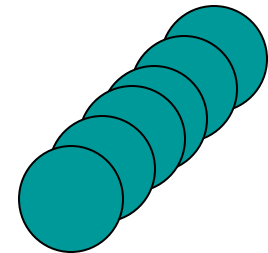
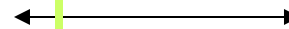
Considered oligopolistic market



Many
customers



Few (mobile)
network
providers

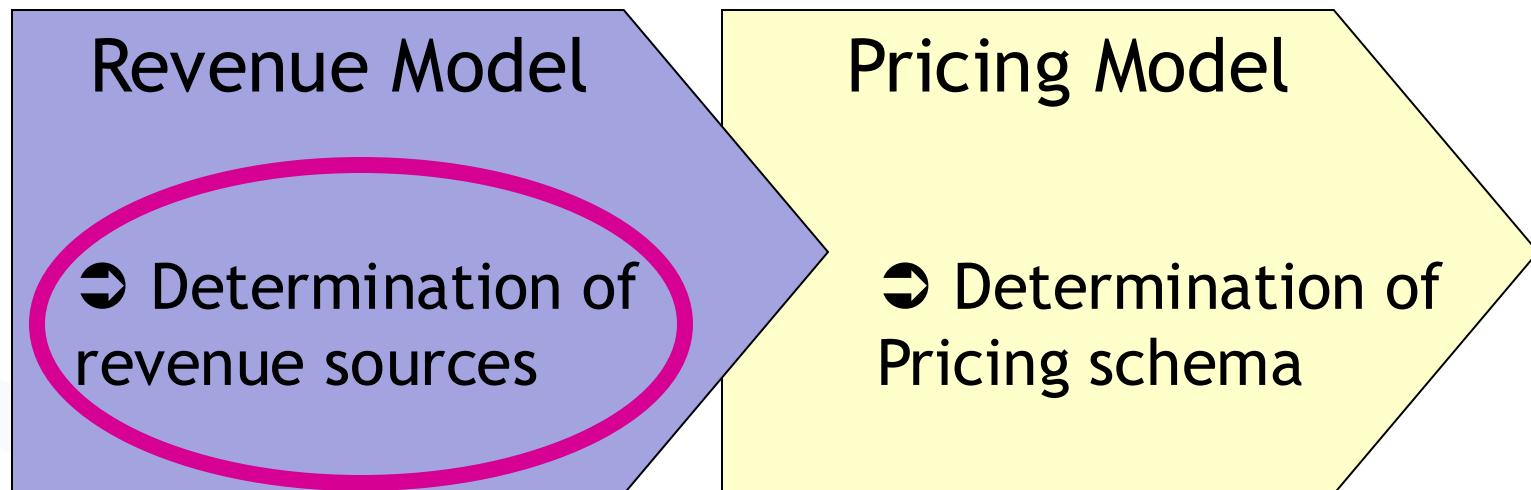


Many content
providers

- Interesting disintegration of 1st-tier-, 2nd-tier-structure
- Increasing contact between 2nd-tier and customer
- “Diversification” of MNO market now?

- - L06, p. 37: Here you talk about a 1st-tier and 2nd-tier structure.
Could you explain again what exactly is meant by this and put this slide in context with the previous slides?
- L07: -why the transaction independent and direct revenues has as example „in app subscription sales“?

- Two-tier determination of revenue



- Revenue types

	direct revenues	indirect revenues
transaction dependent	1	3
transaction independent	2	4

- Type 1: transaction dependent / direct revenues

Single transactions:

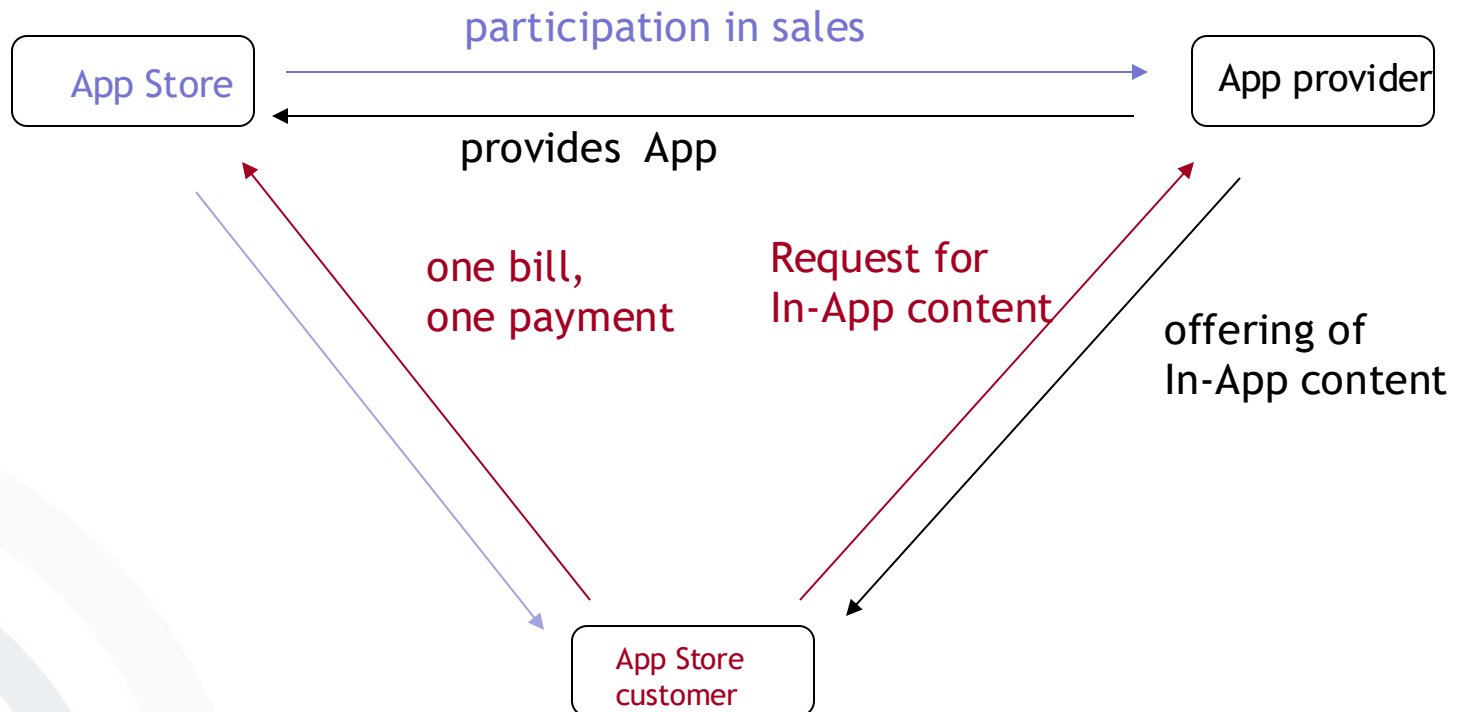
- Volume based: books, ring-tone downloads, data packages (GPRS).
- Time based: calls, communication links (HSCSD, CSD).

- Type 2: transaction independent / direct revenues
 - One-time: Installation fees
 - Recurring: Subscriptions

- Type 3: transaction dependent / indirect revenues
 - Reverse revenue streams - supplier specific
 - Advertising
 - Commissions (e.g. revenue participation)

- Type 4: transaction independent / indirect revenues
 - Reverse revenue streams
 - Advertising
 - Commissions (e.g. listing fee)

- Example: (Apple) App Store

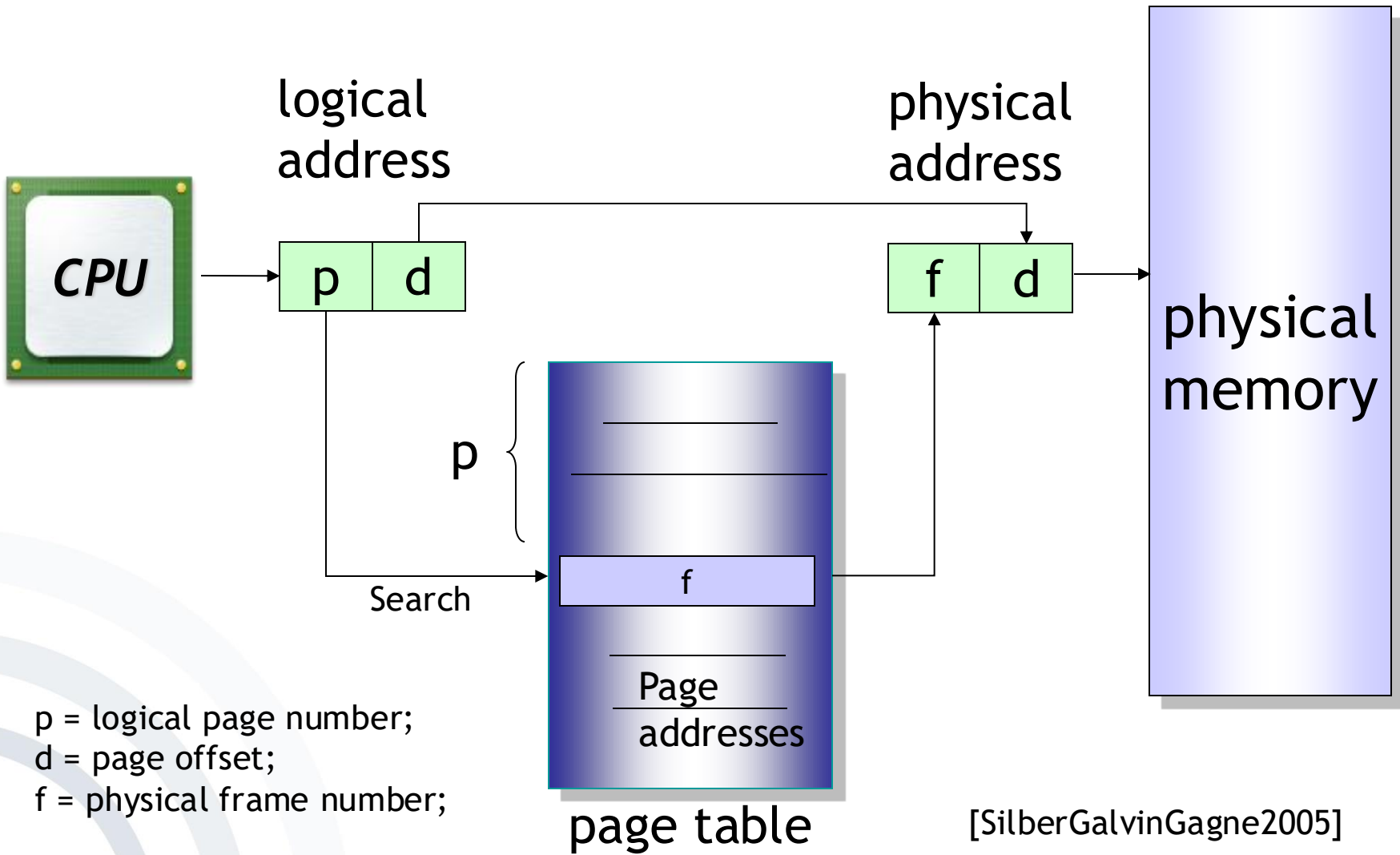


- App Provider revenue model

	direct revenues	indirect revenues
transaction dependent	In-App sales	In-App Advertising
transaction independent	In-App subscription sales	Commission from App Store

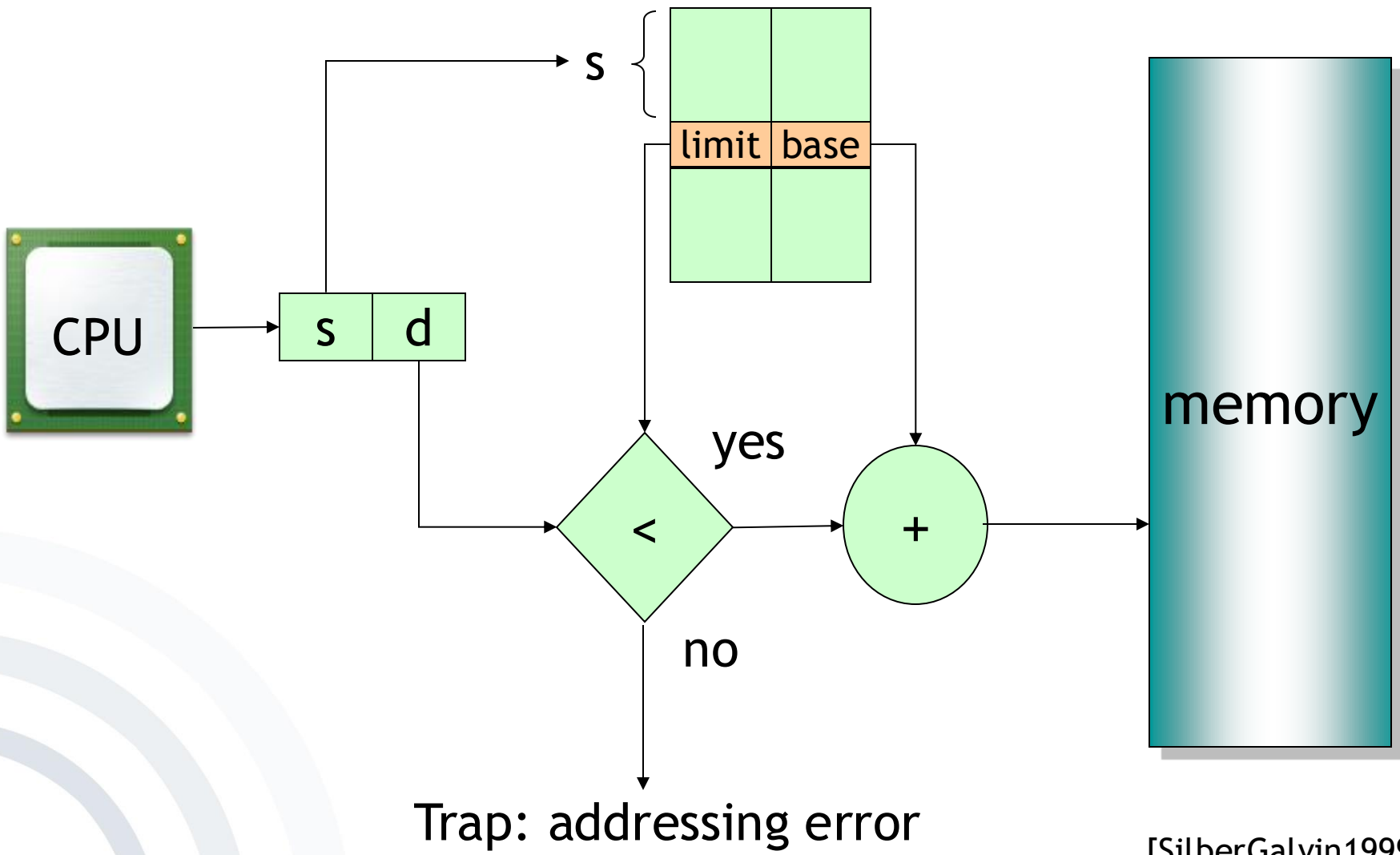
- Moreover, regarding Lecture 10, could you please briefly explain the concepts **paging** (Slide 36) and **segmentation** (Slide 39) again? (-How paging works and what is it's practical advantage?)
- L10 p. 43-55: Could you explain the **memory management** example again? To what extent is it relevant to the exam?
- How exactly **sandboxing** helps to provide security of a mob device?

- The *physical memory* is divided into blocks of a defined size, the so called *frames*.
- The *logical memory* gets divided into blocks of the same size, the so called (memory) *pages*.
- Every address created by a CPU is divided into a *page number* [p] and an *offset* [d].
- The page number is used as the index for the page table, containing the base address for all (memory) pages.
- The base address is combined with the offset resulting in the physical address.



p = logical page number;
d = page offset;
f = physical frame number;

[SilberGalvinGagne2005]

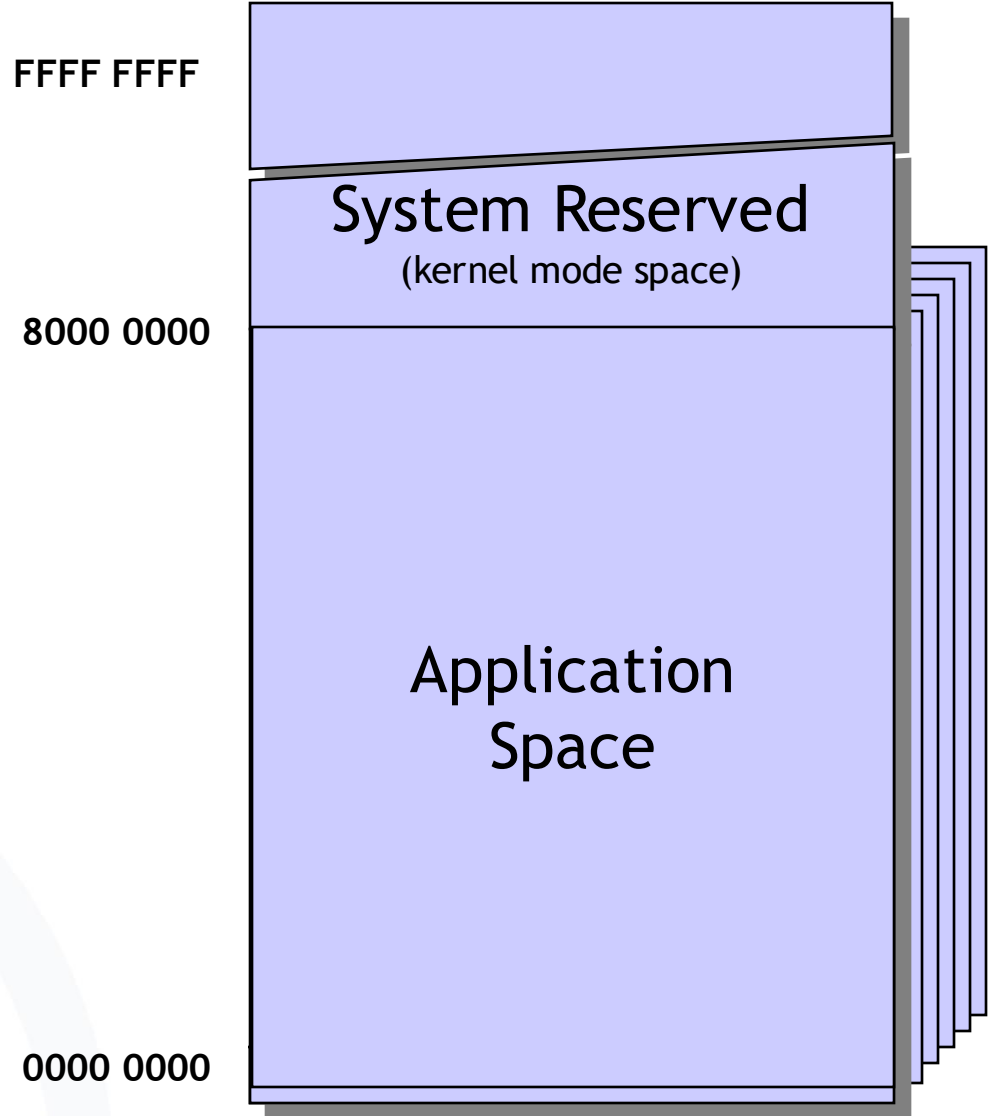


- The memory is partitioned into segments of variable length.
- Every segment has a name and a defined length.
- A segment table is used to store the base address and the limit of the segments.
- The logical address consists of a segment number $[s]$ and the offset $[d]$.

- Moreover, regarding Lecture 10, could you please briefly explain the concepts paging (Slide 36) and segmentation (Slide 39) again? (-How paging works and what is it's practical advantage?)
- L10 p. 43-55: Could you explain the **memory management** example again? To what extent is it relevant to the exam?
- How exactly **sandboxing** helps to provide security of a mob device?

Memory Management Examples

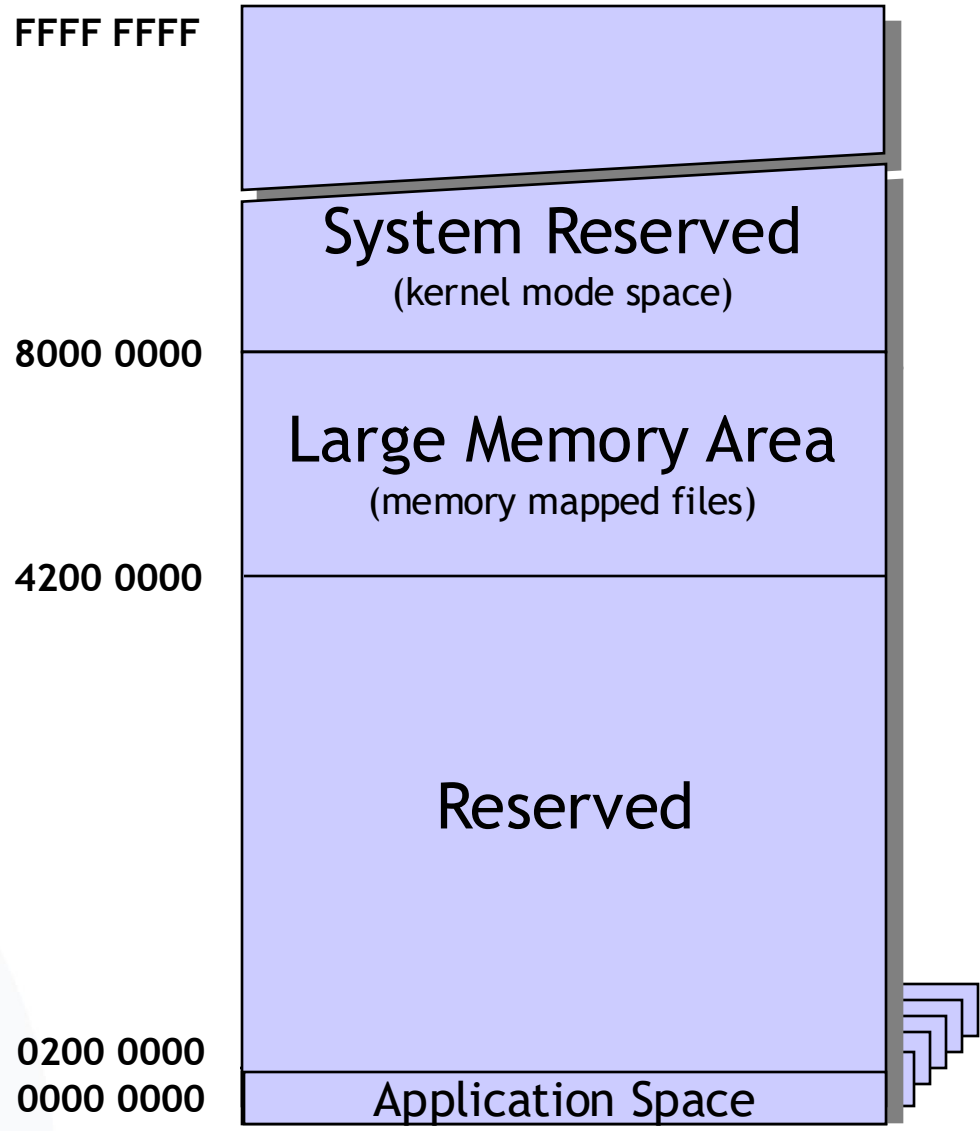
Windows XP Memory Map



[Hall2002]

Memory Management Examples

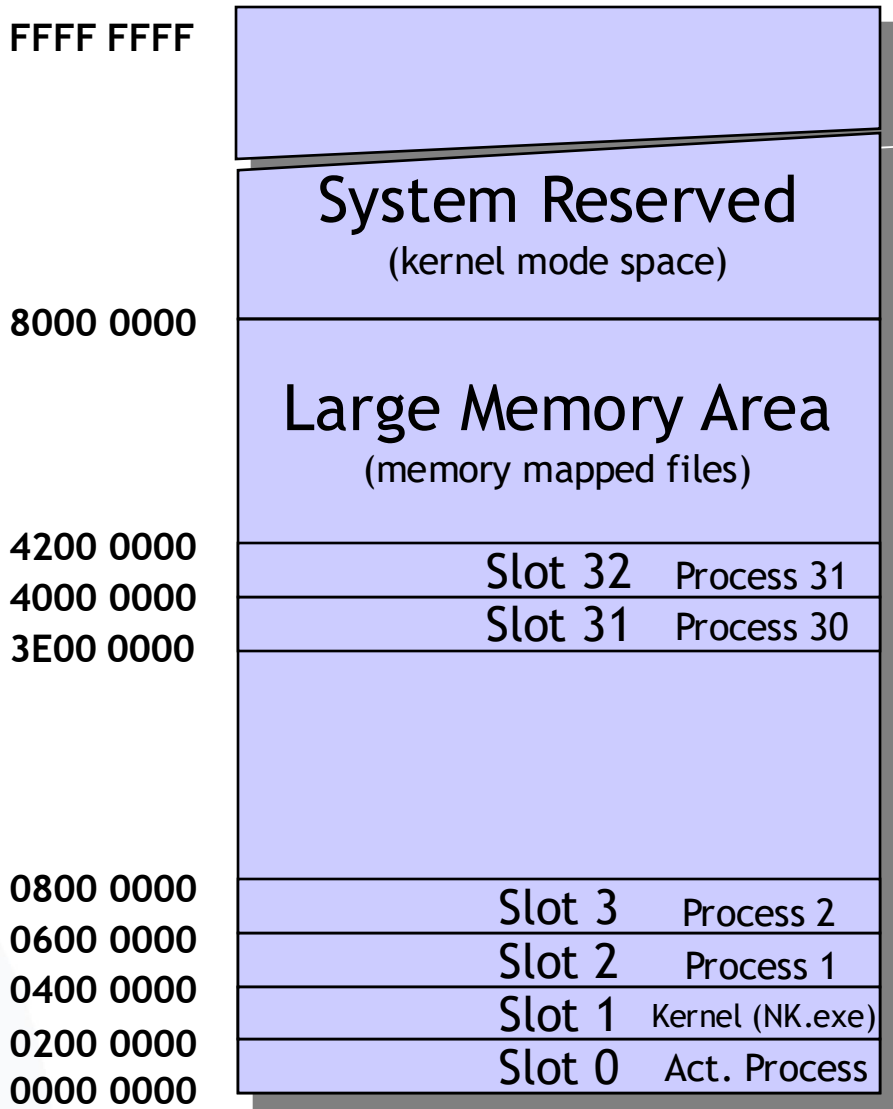
Windows CE Memory Map



[Hall2002]

Memory Management Examples

Windows CE Memory Map



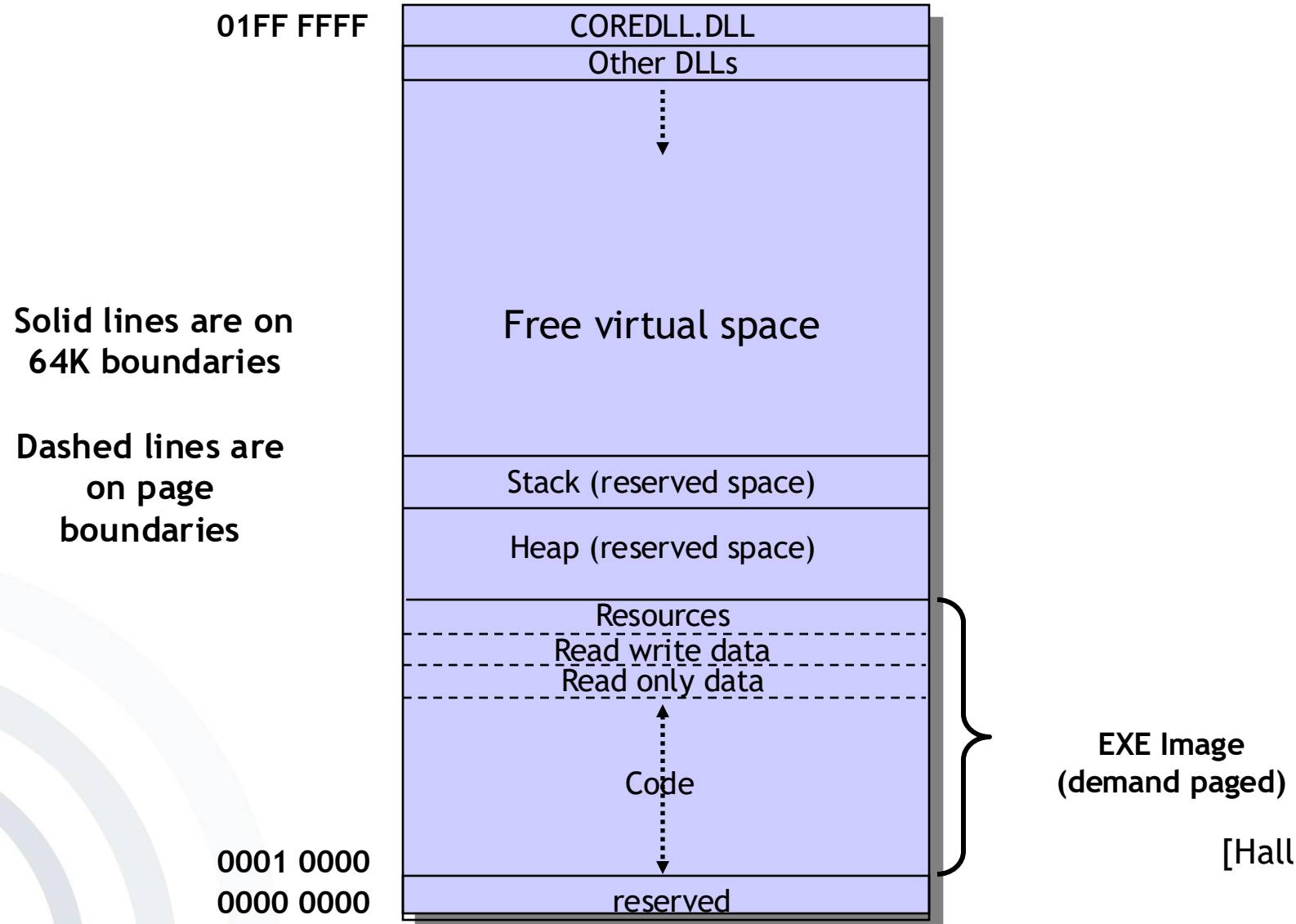
Detailed View

[Hall2002]

- Memory (RAM) is divided into 33 slots.
- One process per slot
 - Slot 2 to Slot 32
 - A process only has access to his own slot
 - ... and to slot 0, when it is active.
- Active process is placed into Slot 0.
- Kernel (NK.exe) is placed into Slot 1.
- Remaining memory is shared.

Memory Management Examples

Application Memory Map (Slot 0)



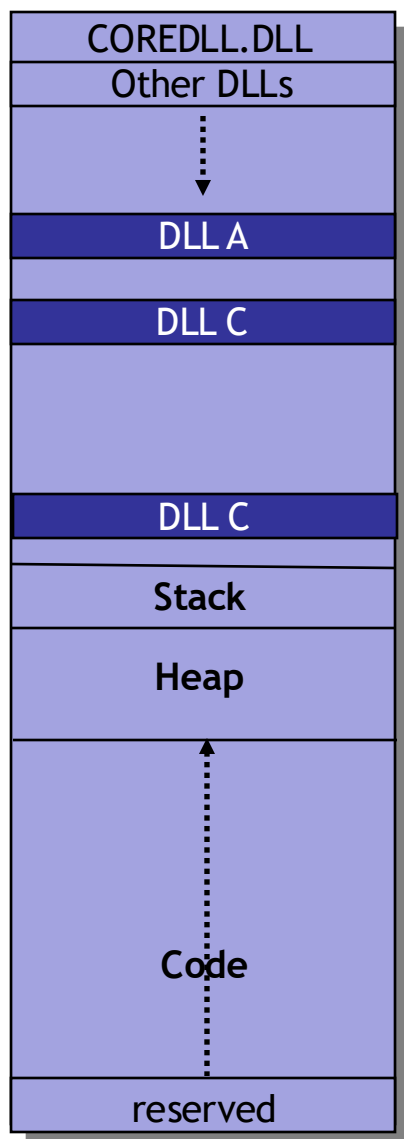
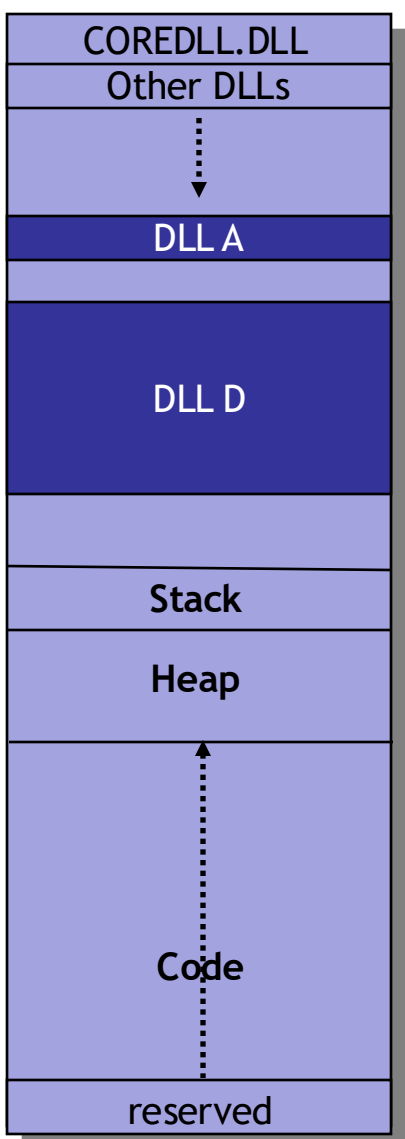
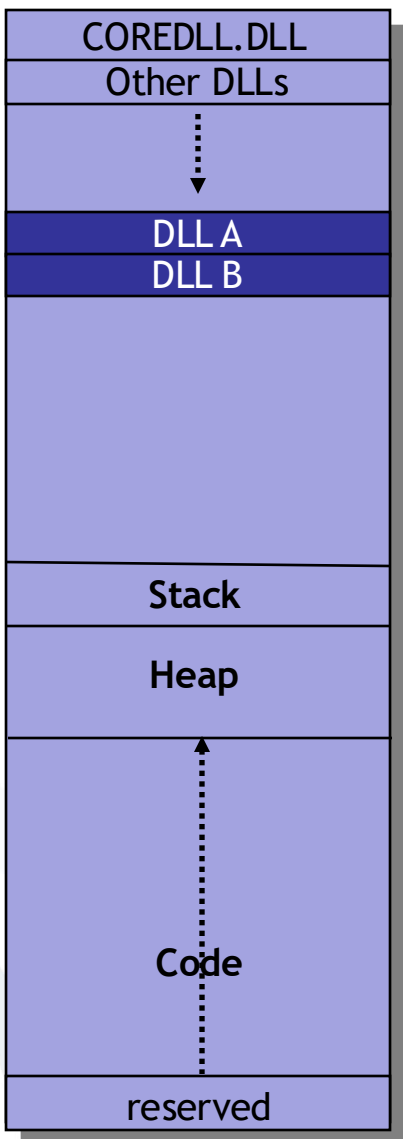
[Hall2002]

- Maximum of 32 MB for virtual memory
 - Virtual memory is used for the code and the data.
- Memory is:
 - Allocated on the basis of pages
 - Reserved in blocks of 64 KB

- Software library, containing a collection of functions and sub-programs that can be used by other independent programs.
- This methodology offers the following advantages:
 - Reutilisation of existing code
 - Distribution of the development process
 - Etc.

Memory Management Examples DLL Load Positioning

01FF FFFF



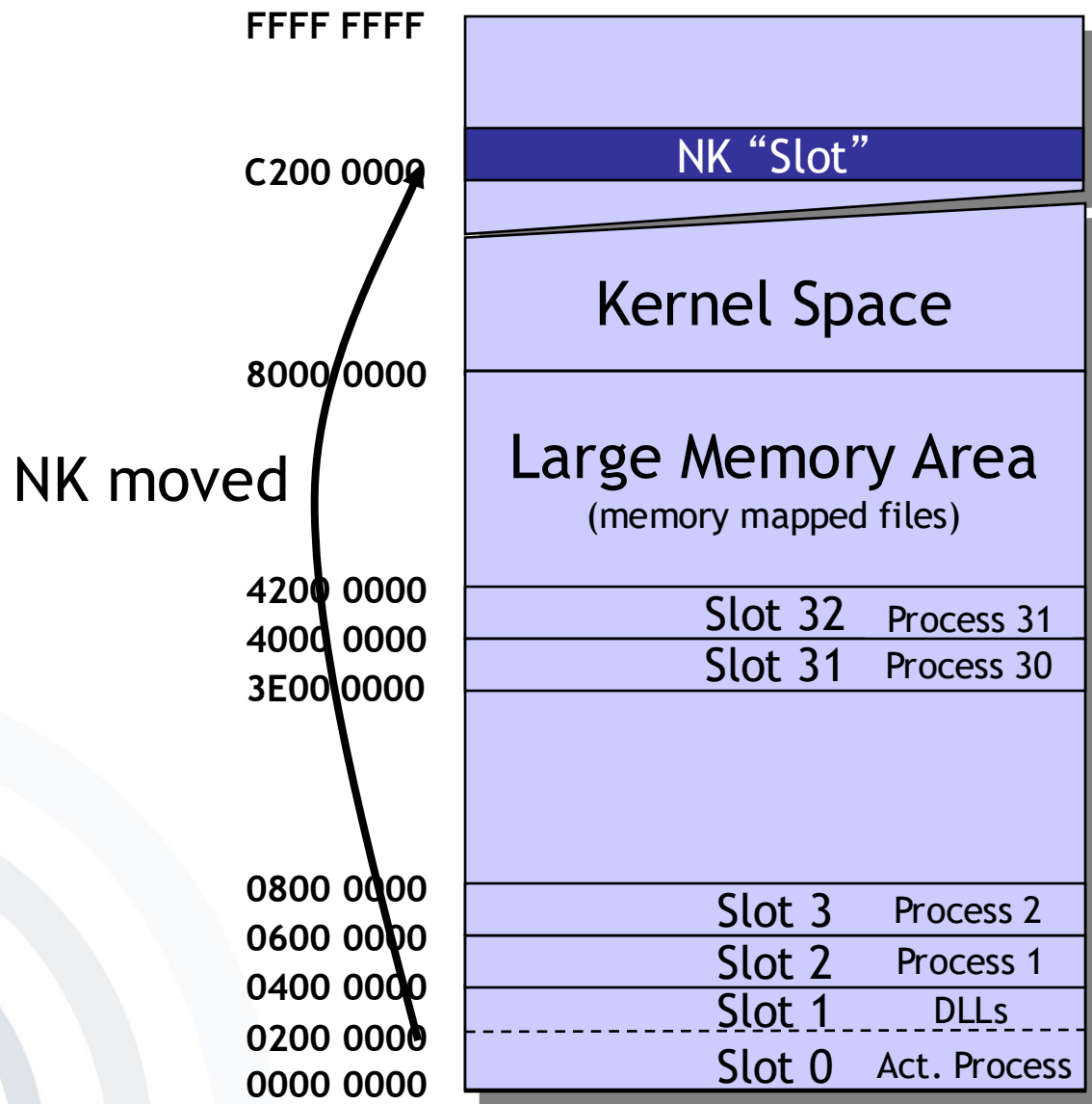
0001 0000
0000 0000

- Any DLL being loaded by any process allocates memory of other processes, regardless if the DLL is used by other processes or not.
- The address the DLL is loaded to is dependent on the other DLLs being loaded by other processes.
- All DLLs are loaded/stored into memory blocks of 64K.
- ➔ The more DLLs loaded, the bigger the problem

- Windows CE .NET solves the DLL load problem by modifying the memory map.
- The kernel (NK.EXE) is relocated from Slot 1 into the kernel space starting from address 0xC200 0000.
- Slot 1 is used for the DLLs:
 - Is connected with all applications for Slot 0

Memory Management Examples

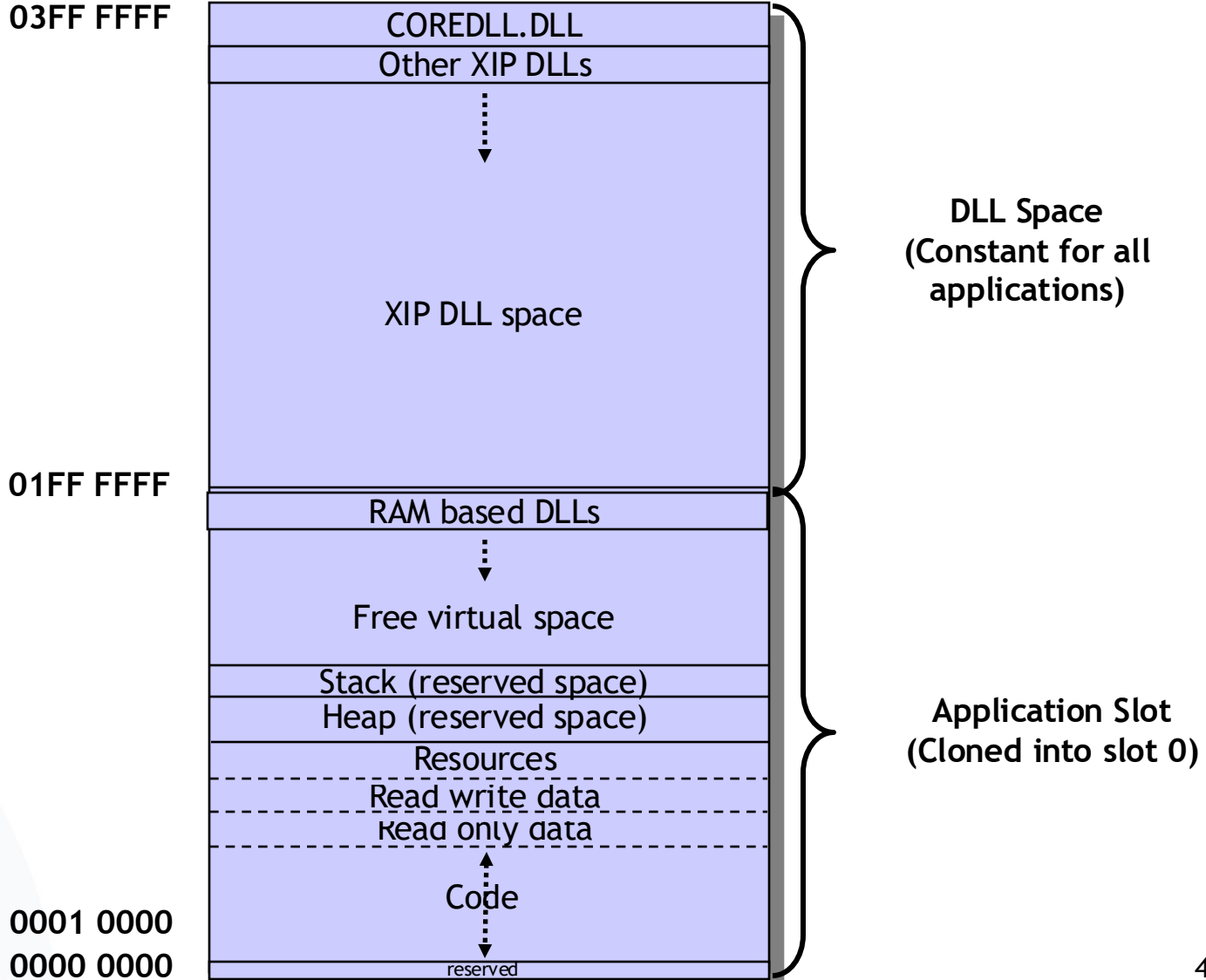
Windows CE .NET Memory Map



[Hall2002]

Memory Management Examples

Windows CE .NET Application Memory Map



- Windows CE .NET Application Memory Map
 - Application memory is now extended to 64 MB (from 0000 0000 up to 03FF FFFF).
 - DLLs are loaded into the upper 32 MB (from 0200 0000 up to 03FF FFFF).
 - Executable (EXE) code, heaps and stacks are using the lower 32 MB (from 0000 0000 up to 01FF FFFF).
 - There is no possibility for loaded applications to allocate memory above 32 MB.

- Moreover, regarding Lecture 10, could you please briefly explain the concepts paging (Slide 36) and segmentation (Slide 39) again? (-How paging works and what is it's practical advantage?)
- L10 p. 43-55: Could you explain the memory management example again? To what extent is it relevant to the exam?
- How exactly **sandboxing** helps to provide security of a mob device?

- Security mechanism provided by all mobile operating systems
 - Separation of running programs
 - Memory Management allocates well-defined memory areas for every sandboxed application at runtime.
 - Protection of device's resources from mobile applications in the sandbox
 - Untested (program) code cannot cause damage to the outside from within the sandbox.
- Examples
 - Network-access restrictions
 - Restricted file system access



- Could you please address the question on slide 33 again?
("Who knows the user's identity and interprets the user's behaviour?")
Was a definite answer given during the lecture or is it rather meant for discussion?
- Furthermore, on Slide 37: What part do network operators play in the IT world? Does this refer to them providing a connection to the Internet?
Also: Would a SIM card in a laptop count towards the GSM world or the IT world?
- L12 p. 59: Could you briefly explain again what you mean by mobile wallets and give reasons/arguments why mobile wallets are relevant for the respective players mentioned in the table?

(Mobile) Equipment Identifier

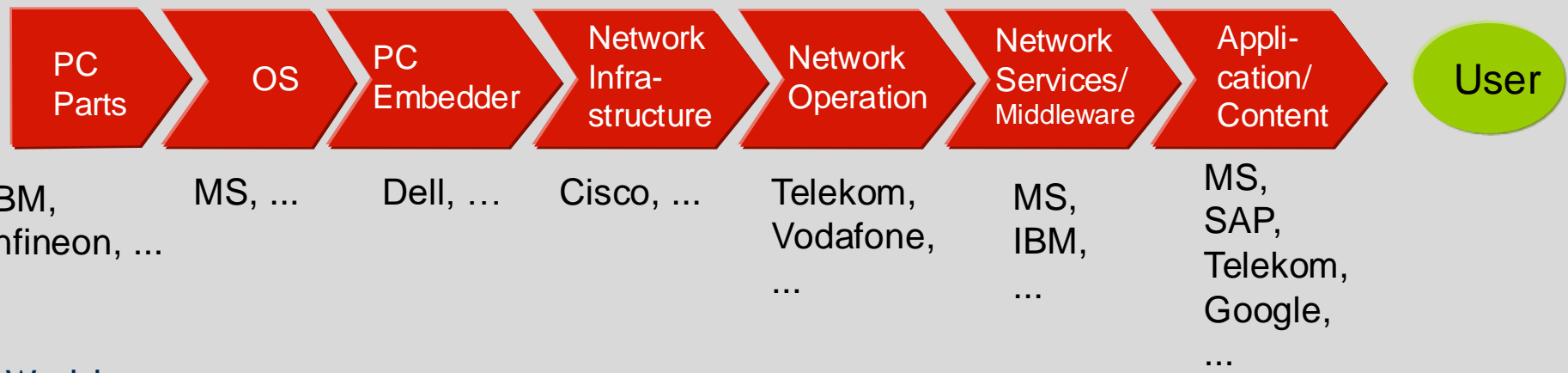
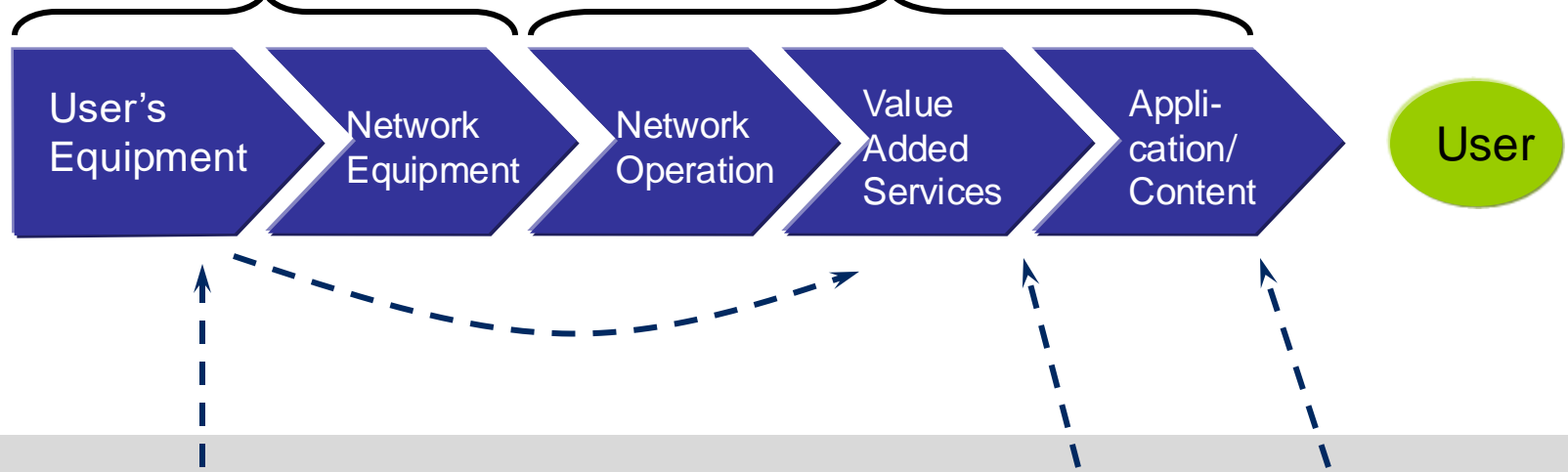
- IMEI, IMSI, UDID, Android ID, TPM:
Who knows the user's identity and
interprets the user's behaviour?



GSM World

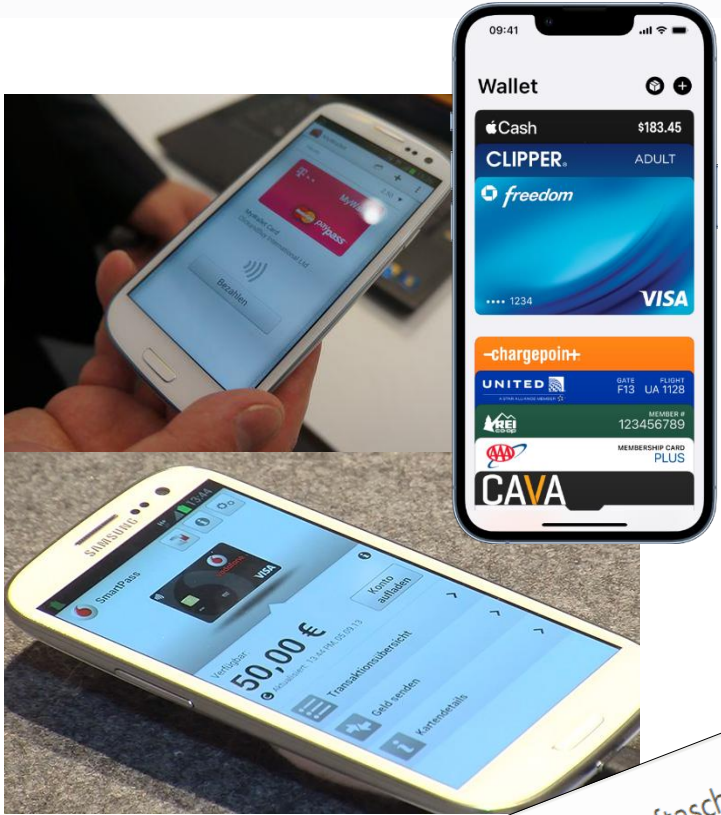
Equipment Manufacturers
(Apple, Samsung, Microsoft/Nokia, Lenovo, Huawei, ...)

Telcos
(Telekom, Vodafone, Telefónica...)

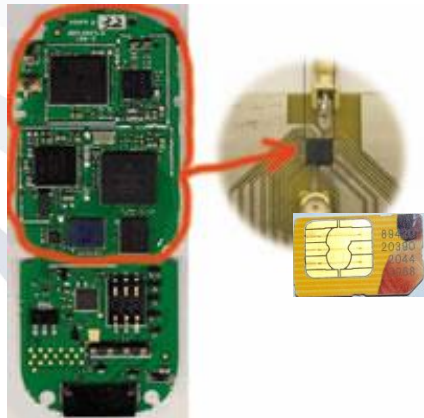


- (NFC) Mobile Wallets
 - contain virtual payment cards and other cards, e.g. customer loyalty cards
 - use the UICC/SIM-based Secure Element (SE)
 - Licensed by Deutsche Telekom, Vodafone, Telefónica and E-Plus independently in 2014.

- Mobile Wallet application “runs” in non-secure memory of the mobile device whereas a UICC payment application runs within the SE.



https://support.apple.com/de-de/guide/iphone/iphco5dbd539/ios



Telefónica O2 to begin beta testing NFC payments in Germany
 By Sarah Clark | January 21st, 2013

"Soon, children will only know from history books what a wallet and hard cash are," says René Schuster, CEO of Telefónica Germany, as the carrier prepares to make payments available to customers from...

E-Plus Mobile Wallet – das Smartphone als Brieftasche

Die Mobile Wallet ermöglicht mehr als Zahlungen

4. November 2013 [Manuela Mirzadeh](#) [Marken, Produkte & Flatrates, über uns,](#)
 Unternehmen [Kommentar schreiben](#)

Mit der „Mobile Wallet“-App macht die E-Plus Gruppe das Smartphone zur digitalen Brieftasche. Die Lösung wird ab Frühjahr 2014 bei den Marken und Partnern des Unternehmens an den Start gehen. Im Bus das Ticket vorzeigen, Rabattaktionen im Kaufhaus nutzen, in das Studio einchecken, beim Einkauf im Drogeriemarkt zahlen und gleichzeitig Bonuspunkte sammeln. Zukünftig ist das buchstäblich alles aus einer Hand möglich. Mit der App können Kunden- und Bank-Karten, die das Portmonee sprengen, ist...

Usage Scenarios and Players

Players and security features they are especially interested in

Usage Scenarios/ Players	Mobile Equipment manufacturers	Mobile operators	MVNOs	Content providers	Appl. Service providers	Private customers	Corp. buyers	Corp. users	Intelligence Agencies
Secure OS	++	++	++		+	+	++	+	
Digital Rights Management	+	+	+	++					
Device misuse prevention						+	++	+	
Storage of additional credentials	+				+	+	+		
Secure corporate network interaction		+			+		++	+	
Mobile Wallet	++	++				+			

Lecture 13

Questions & Answers

Mobile Business I (WS 2024/25)

Prof. Dr. Kai Rannenber

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