

Information & Communication Security (SS 15)

Network Security II

Prof. Dr. Ioannis Stamatiou
Computer Technology Institute
Patras, Greece

- Introduction
- Security Components
- Security Protocols
- Security Threats
- **Wireless / Mobile Security**
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

- Wireless communication based on radio as transport medium
- Cell based architecture
- Possible extension to a (wired) LAN
- One cell serves a circular area in which PCs, laptops, and other connected devices can move freely.

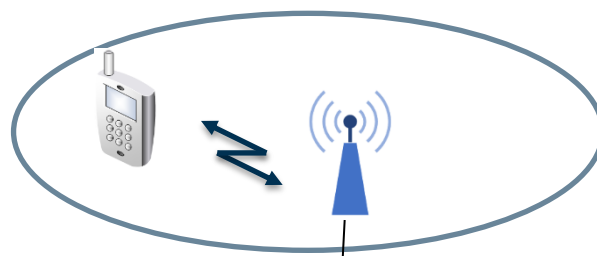
- **Access Point (AP):**
Transmitting and receiving station which allows multiple devices to connect
- **Stations:**
Terminals, used by AP for building a wireless network connection (Example: PCMCIA-WLAN Card in Laptops)



Wireless LAN Basics

Infrastructure and ad hoc networks

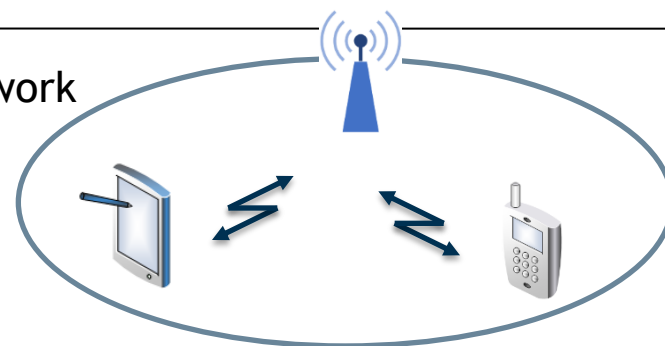
Infrastructure network



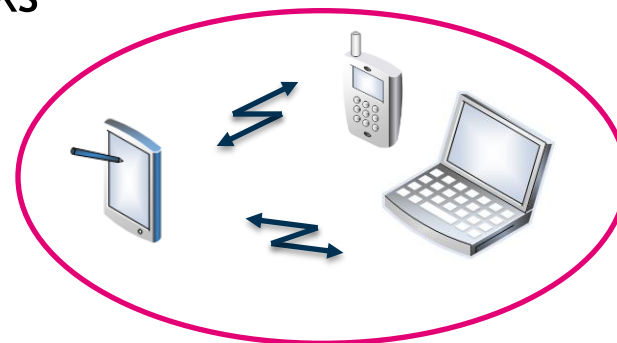
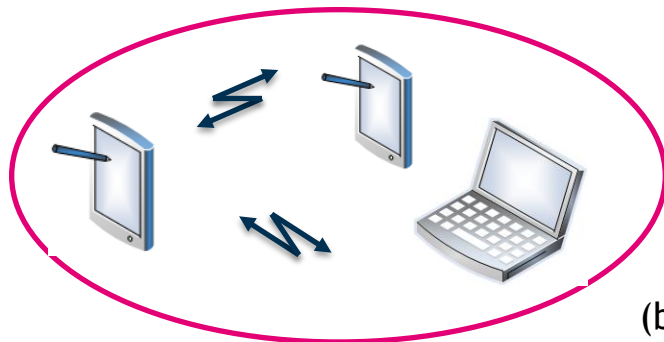
Access Point



Existing fixed network



Ad hoc networks



(based on [Sch03])

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802.11f	Roaming between access points of different manufacturers (published in 2003 and withdrawn by IEEE in 2006) [IEEE2010]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 by the year 2015) *) **) [IEEE] [Sa08]

- How IEEE 802.11-1997 aimed to provide security for Wireless LAN:
 - SSID (Service Set Identifier)
 - Name of the network
 - MAC (Media Access Control)
 - Rule based access control
 - WEP (Wired Equivalent Privacy)
 - Encryption mechanism

- Primitive access control
 - Cumbersome and easy-to-fake by use of MAC address of network card
 - No user authentication
 - Better solution: VPN on top of WLAN
- Weak encryption
 - Problems with entry parameter of RC4 algorithm
 - Challenge-response can be used to retrieve the shared key
 - Weak linear integrity check
- Cumbersome key management
 - WEP does not have a centralized key management.
 - Manual key distribution -> difficult to change keys
 - Single set of shared keys for all nodes

- Standard for authentication server:
 - Remote Authentication Dial-In User Service (RADIUS)
 - In the beginning quasi-standard developed by one company (Livingston Enterprises)
 - Since 1997 supported by The Internet Engineering Task Force (IETF) as Requests for Comments (RFCs)

- Improved security by WiFi Protected Access (WPA)
 - Access control
 - Extensible Authentication Protocol (EAP)
 - RADIUS enables individual user authentication.
 - New Message Integrity Check (MIC) algorithm - “Michael” - (to avoid MAC spoofing)
 - Encryption
 - RC4 is kept, but with increased size of the initialization vector.
 - Updated initialization algorithm to avoid using weak keys
 - Key management
 - Dynamic key exchange - TKIP (Temporal Key Integrity Protocol)
 - Derived session keys instead of a shared master key
 - Authentication key different from encryption key
- Interim solution by the WiFi Alliance (manufacturer consortium) till availability of IEEE 802.11i-2004

- Standardization of security mechanisms for 802.11 through IEEE
- Available since the end of 2004 as 802.11i
- Commercially labelled “WPA2”
- Robust Secure Network Association (RSNA)
 - New Cryptographic Mechanisms
 - AES (instead of RC4) => requires hardware support
 - CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) (instead of TKIP)
 - Key Management
 - RADIUS, EAP, 802.11X
- Transition Security Network (TSN)
 - Uses TKIP instead of CCMP
 - Backwards compatibility for devices not supporting CCMP-AES

Example: Wireless technology at Goethe University

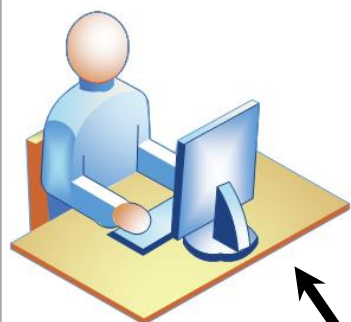
- **Eduroam and Flughafen**
 - Both WPA and WPA2 supported
 - RADIUS enables individual user authentication (university credentials used).
 - Eduroam supports the authentication method of participating institutions.
- **Freiflug**
 - Unencrypted connection
 - Login via an https-secured webpage

- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

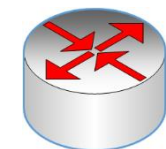
Situation today:

- Separate IP-addresses in the office and at home
- DHCP - dynamic IP assignment
- Dial-up with dynamic IPs
 - Continuous accessibility via one IP is not guaranteed.
 - Connection interruptions during access point switches

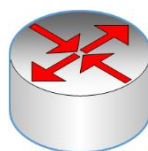
Routing in TCP/IP



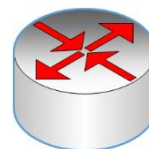
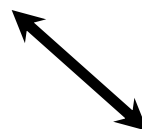
Partner B
IP address, e.g.
61.9.193.200



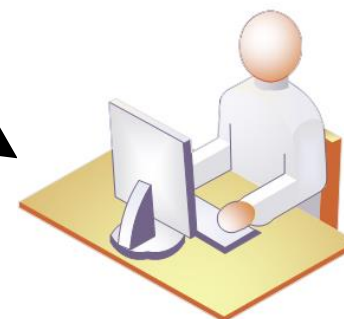
Router



Router

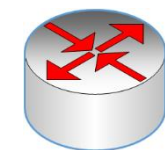


Router



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-packages by routers



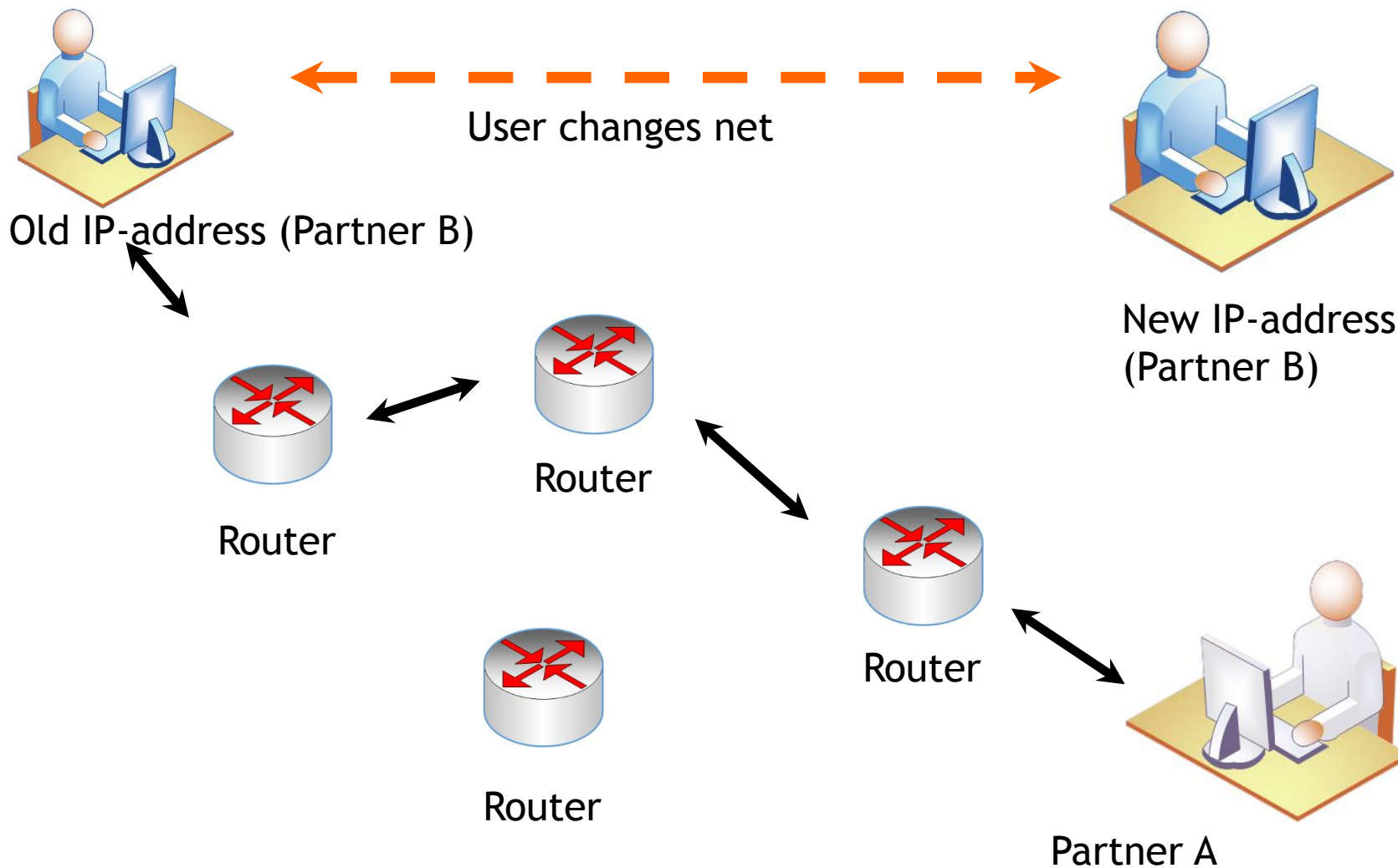
Router

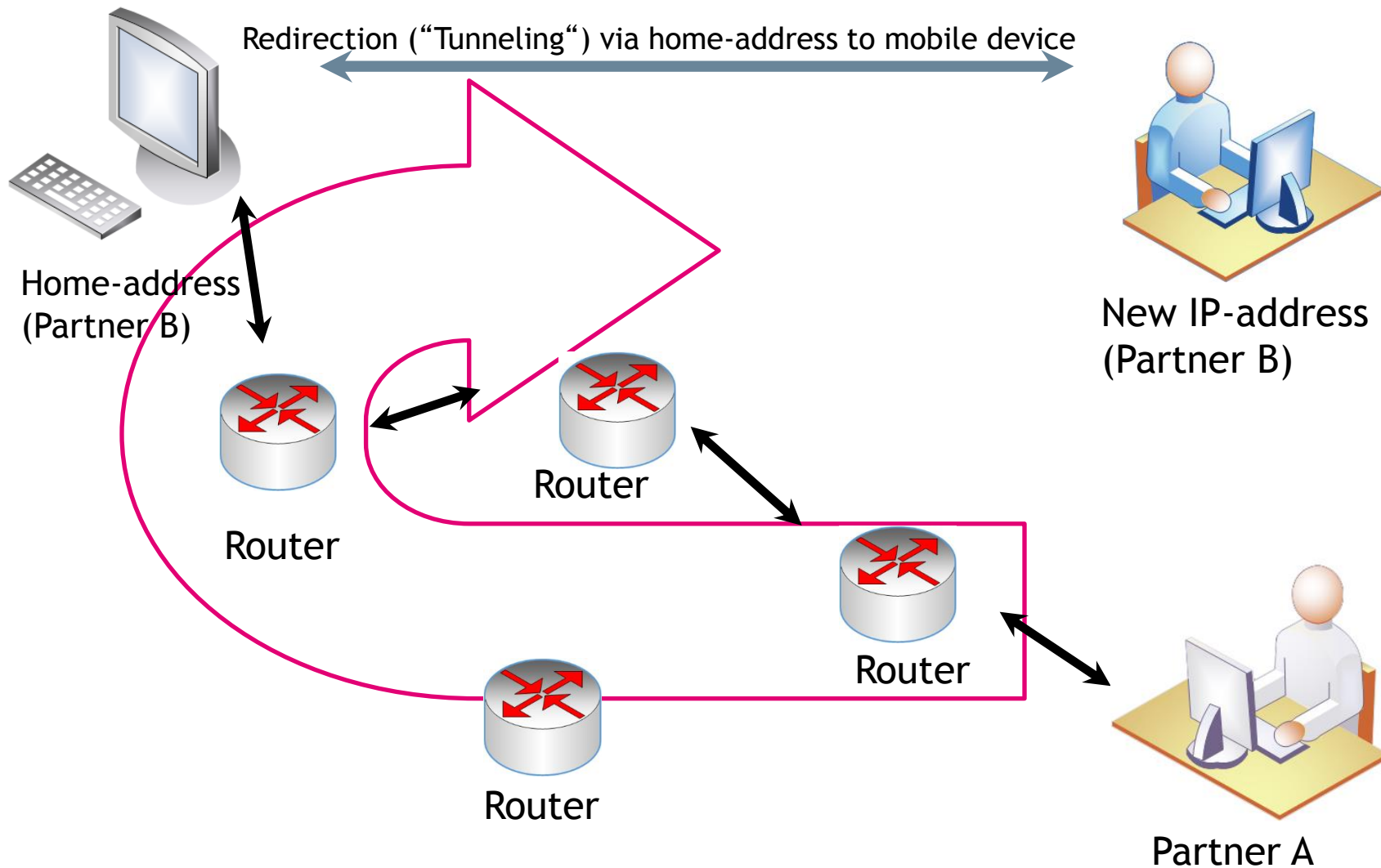
- In the **Domain Name Service** a domain-name belongs to a fixed IP-address (e.g. www.m-chair.de = 188.138.95.94).
 - **Changing** these addresses requires an update-time of several hours \Rightarrow this is no usable solution.
- **Better solution: Dynamic DNS**
 - Modification time: 15 minutes.
 - Problem: applications resolve a name just once and do not query possible address changes thereafter.

Addressing of mobile devices

- Standards
- Internet Engineering Task Force (IETF)
- RFC 2002, 3220: IP Mobility Support
- RFC 2977: Mobile IP Authentication, Authorization, and Accounting Requirements

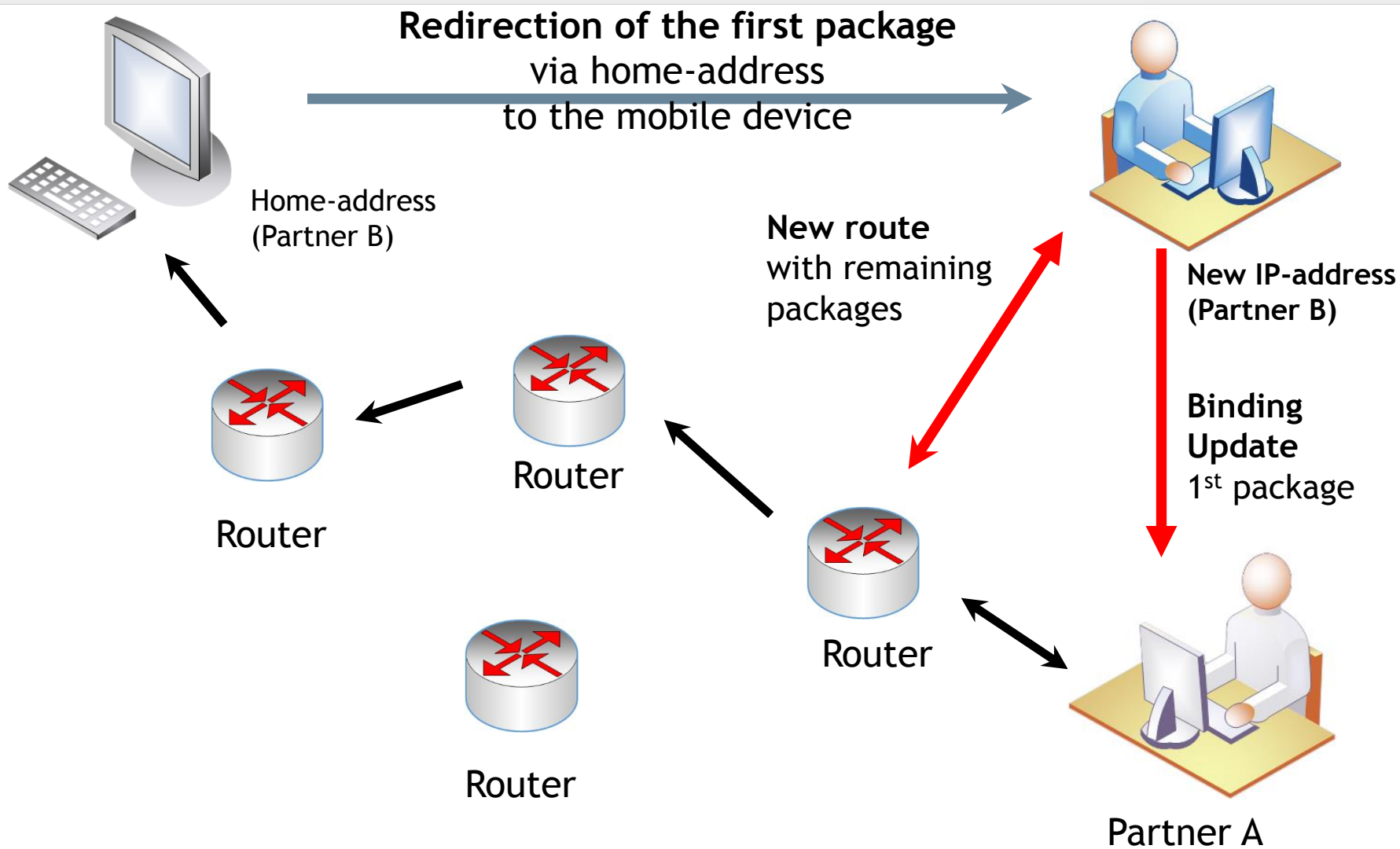
Roaming problem





- **But redirection implies**
 - A longer route than before
 - Higher runtime
 - Avoidable usage of resources

Roaming solution Binding Update



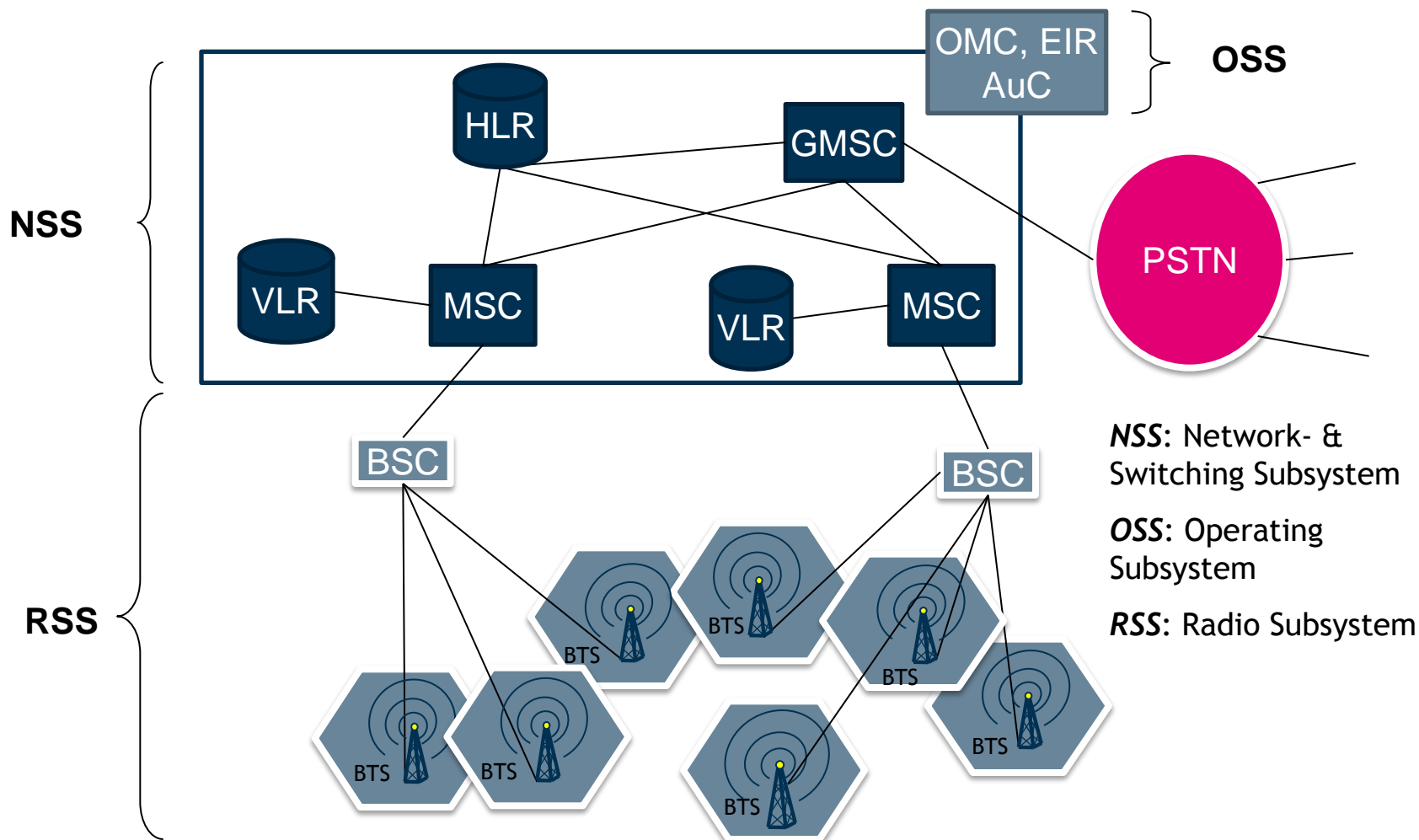
- Possible attack with illegitimate binding update:
 - **Capture the route** and redirect the TCP/IP-session.

- ⇒ **Therefore, authentication** of BU-messages and address check is required.

- Further possible attack: **Observation** of user-movements through their binding updates!
- ⇒ **Anonymous communication-channels** are necessary to protect privacy.

- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

- GSM (Global System for Mobile Communications)
 - Originally 1982 driven by *Groupe Spéciale Mobile* in order to create a cross national standard contrary to national analogue standards
 - European standard by *ETSI* (European Telecommunications Standardisation Institute) 
 - Worldwide adoption of the standard in more than 100 countries (most successful mobile radio system up to now)
- ➔ Thus, worldwide roaming among different mobile network operators became possible.



Based on [Schiller2003]

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

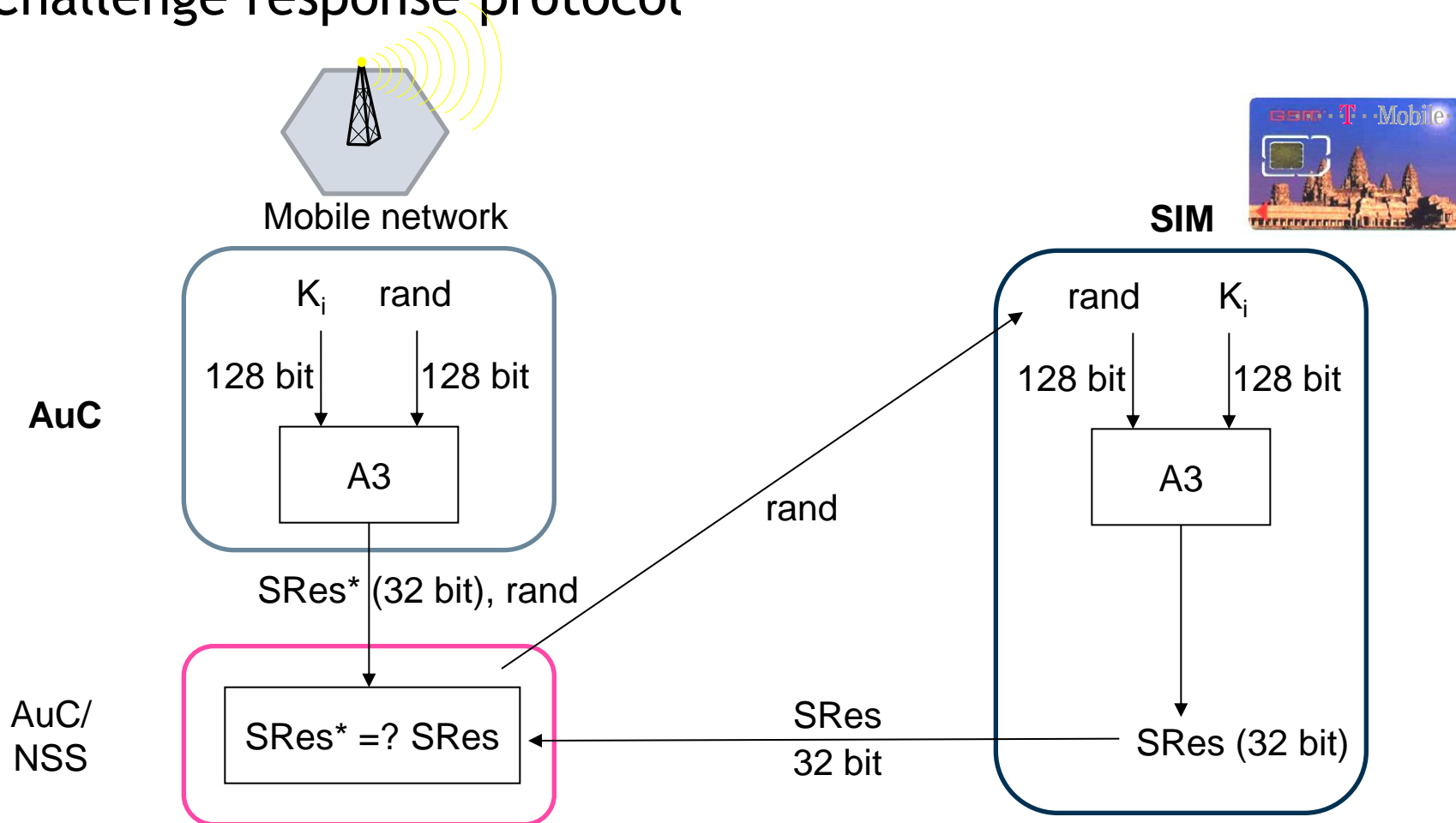
Confidentiality:

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)

Challenge response protocol



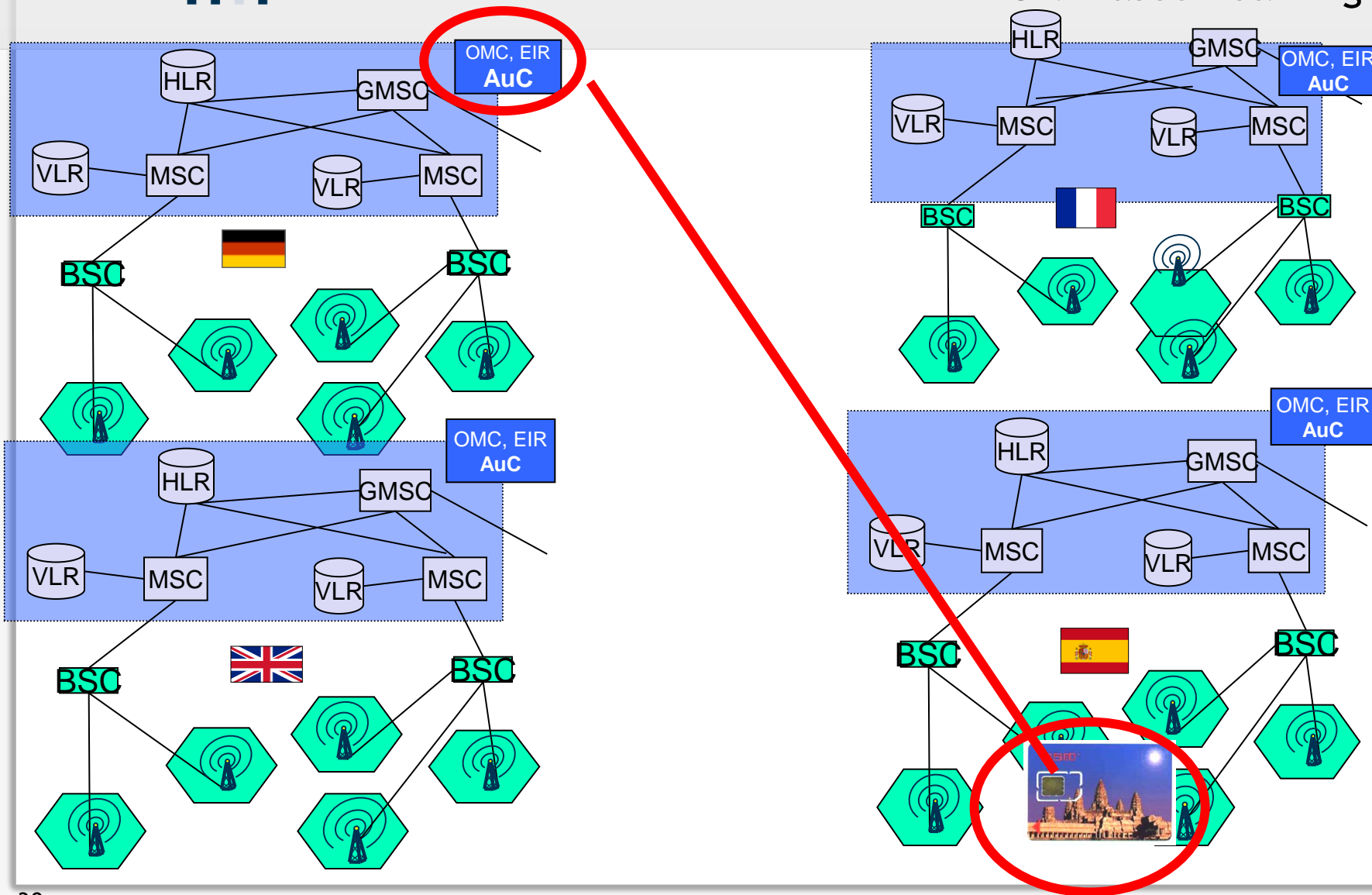
K_i : individual subscriber authentication key
 $A3$: („secret“) authentication algorithm

$SRes$: signed response Based on: Jochen Schiller

- Challenge-Response-Procedure
 - Authentication is based on the individual key K_i , the subscriber identification IMSI, and a secret algorithm A3.
 - K_i and A3 are stored on the SIM and in the AuC.
1. AuC creates random number *rand*.
 2. AuC encrypts *rand* and K_i via A3 (-> SRes*).
 3. AuC transfers *rand* and SRes* to NSS.
 4. NSS transfers *rand* to SIM.
 5. SIM computes with “own” K_i and A3 Signed Response SRes.
 6. The SRes computed by the SIM is transmitted to the NSS and is compared with SRes*.
 7. If SRes* and SRes are equal the subscriber is authenticated successfully.

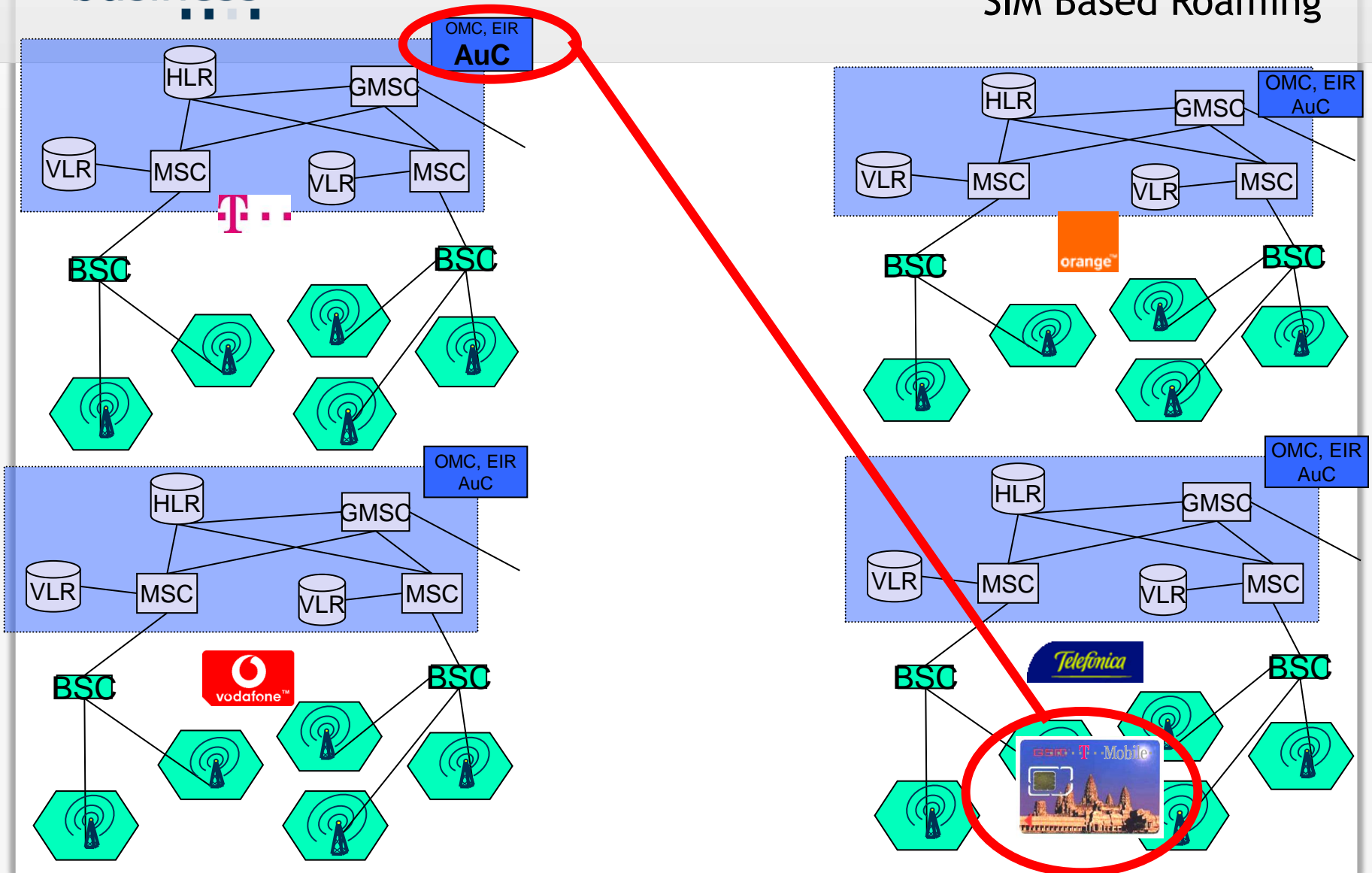
Roaming

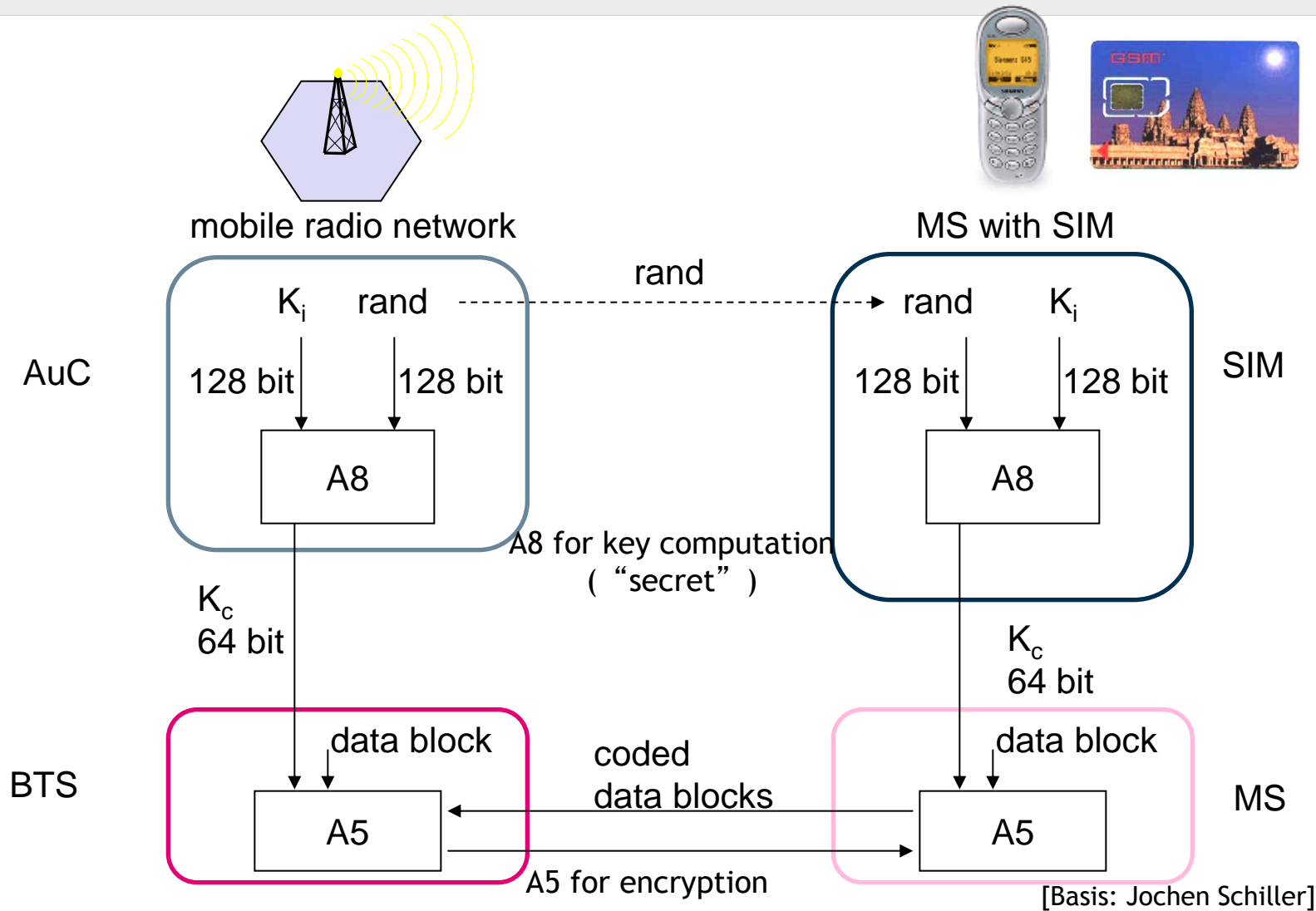
SIM Based Roaming



Roaming

SIM Based Roaming





[Basis: Jochen Schiller]

- GSM provides encryption of voice and data transferred via the air interface:
 1. AuC creates random number *rand*.
 2. AuC generates the key K_c for the encryption of the transferred data using *rand*, K_i and A8.
 3. AuC sends *rand* to SIM.
 4. SIM locally computes key K_c using *rand* received, as well as (local) K_i and A8.
 5. Mobile station (MS) and mobile radio network (BTS) use K_c and algorithm A5 for encryption and decryption of sent and received data.

- In order to guarantee the anonymity of the users temporary subscriber identification (TMSI) is used.
- TMSI is updated automatically from time to time or on demand.
- Data which identify users are not transmitted.
- Anonymous charging is (technically) possible via prepaid card.

- Authentication only by the terminal/subscriber towards 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 positioning is almost exclusively controlled by the network.
 - Centralized movement tracking is possible.
 - To avoid positioning 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-standard algorithms.
- No encryption from terminal to terminal but only over the air interface
 - Encryption deactivation by the network possible
- Encryption comparatively “weak” because of key length (64 bit)
 - Sometimes the real key length is shorter.

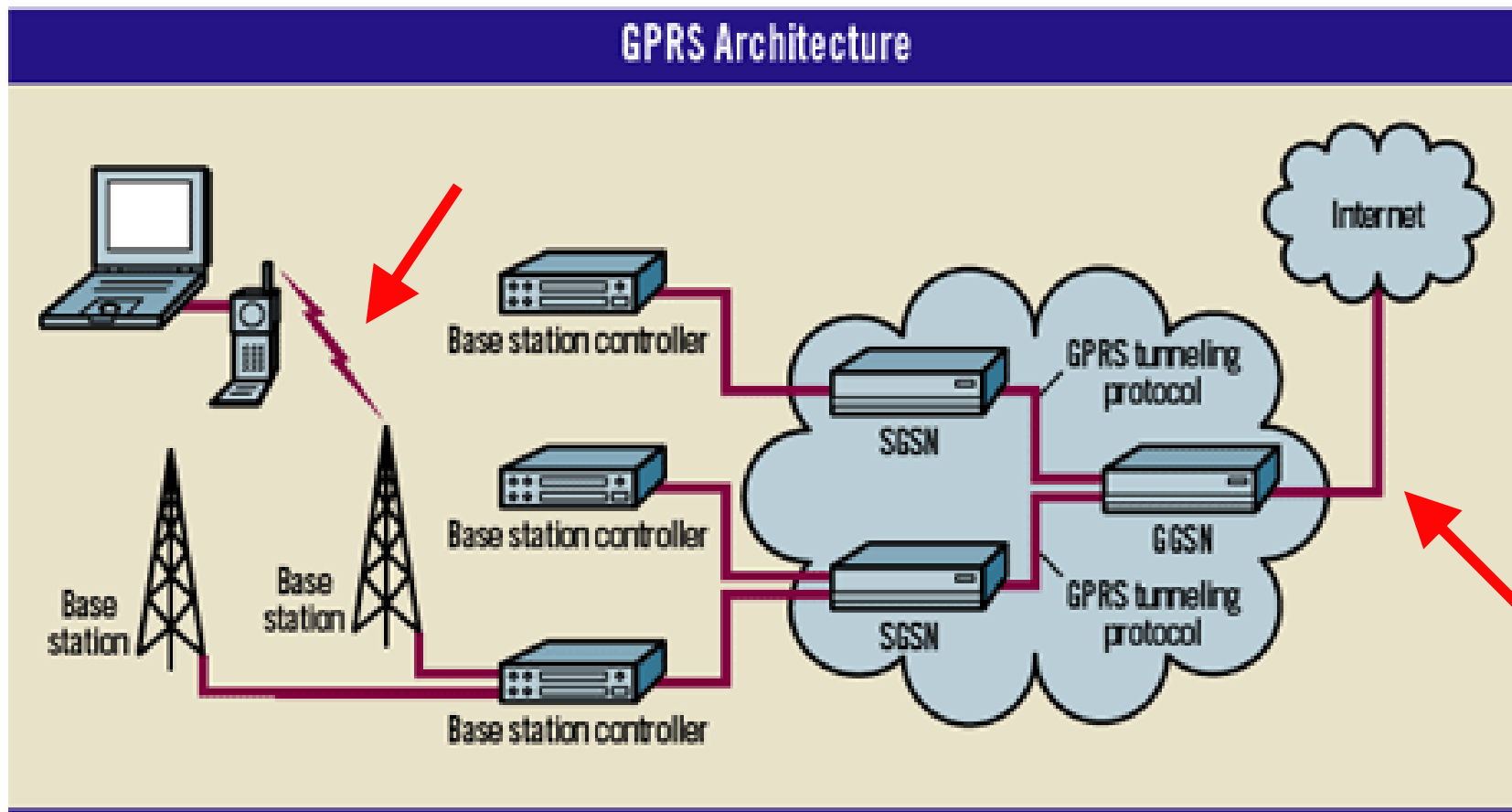
- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

General Packet Radio Service (GPRS)

- First packet-based data service
 - Employment of time multiplex procedure for data services
 - Dynamic allocation of radio channels among the subscribers in a radio cell
 - Channels are only blocked when data is actually transferred.
- ➔ Packet orientation implies the introduction of new billing methods.

- Up to 8 time slots can be occupied per time frame (at the moment 4 in practice).
- In contrast to HSCSD the GPRS data service requires an extensive upgrade of the GSM architecture with new network components.
- In spite of better network utilization and volume based billing at the beginning the data transfer costs were much higher than those of connection oriented data services (c't 9/2002, p.100).
- The data transfer costs of GPRS data services have been lowered through new price models (especially free volume with higher basic charge).

- Authentication possible via SIM
- Mobile device is „always on“ and connected directly to the Internet without specific protection (e.g. firewall)
- Encryption algorithm is analog to GSM.
- Encryption can be disabled by the GSM/GPRS-Network.



- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

- Universal Mobile Telecommunications System (UMTS):
 - ***Status of 2G-Networks:*** Different standards in some different continents avoid worldwide roaming
 - ***Demand for 3G-Networks:*** Globally uniform standard

➔ Voting of regional & national regulation offices (e.g. ETSI, ARIB, ANSI) via the International Telecommunication Union (ITU)



- Common approach: worldwide reservation of frequencies in the 2GHz range
- Competing technologies: Existing national networks and installed network technologies in different regions compete for the standard.
- ➔ The specification of 3G-Networks, introduced by the ITU, leaves room for national, partly incompatible implementations.

Coverage obligations (in Germany)

- The licensees are contractually obliged to guarantee certain degrees of coverage:
 - 25% of the population till 2003-12-31
 - 50% of the population till 2005-12-31
- Theoretical coverage degree at Q1/2009 between 59% and 81% depending on operator. But only 26 Mio. capable devices at end of 2009.

- At least 144 kbit/s in the countryside (target: 384 kbit/s)
- At least 384 kbit/s in suburbs (target: 512 kbit/s)
- Up to 2 Mbit/s in urban areas / city centers

But: Bandwidth decreases if terminal is moving or if there are many participants in one radio cell.

➔ Bandwidths enable multimedia services.

UMTS complements the security mechanisms known by GSM:

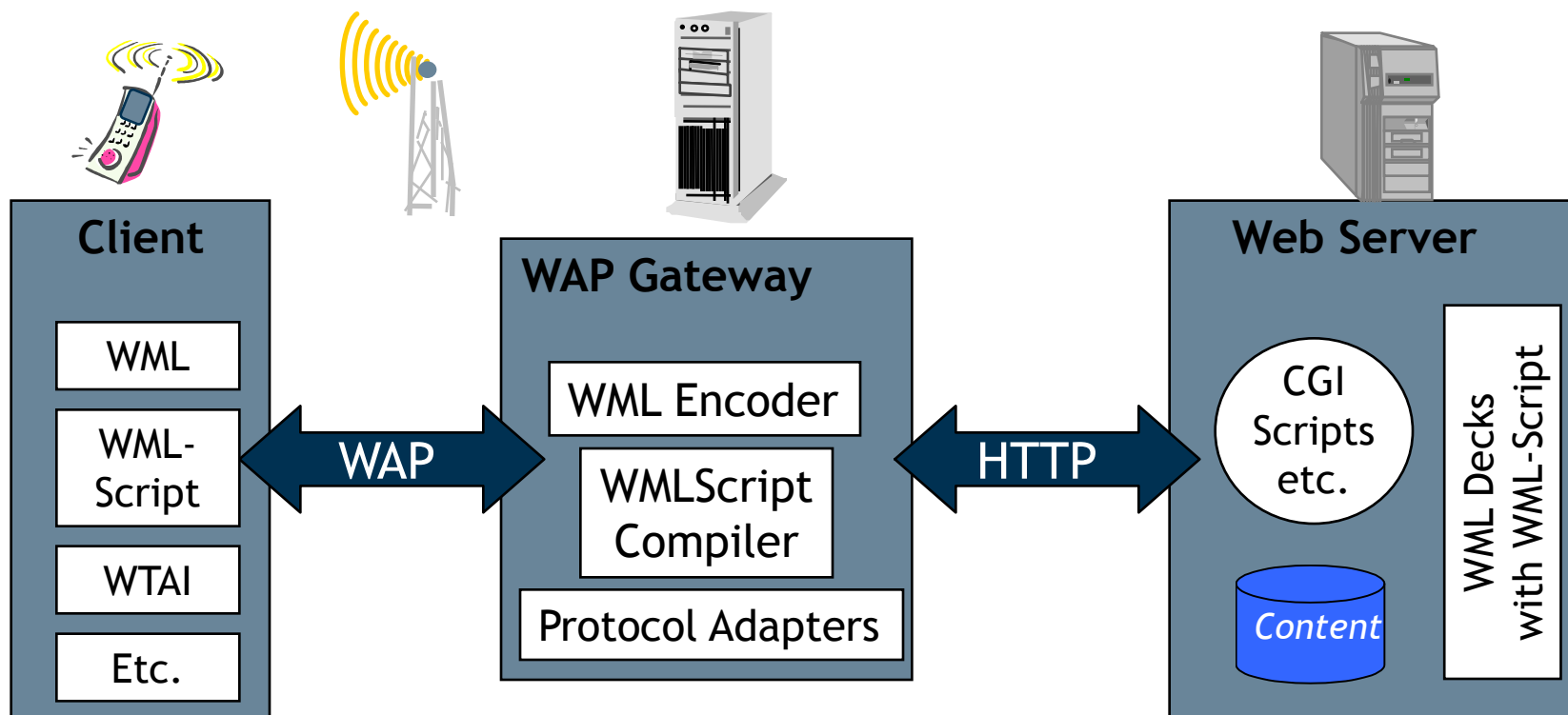
- Enhanced participant authentication (EMSI)
- Network authentication
- Integrity protection of data traffic
- Transferred security keys are also encrypted in the fixed network (e.g. between HLR and VLR).
- Increased key length
- End-to-End encryption is possible.

- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

Wireless Application Protocol (WAP)

- In 1997, Ericsson, Motorola, Nokia and Unwired Planet founded the WAP-Forum.
- The WAP-Forum is a non-profit-organization with the objective to establish an open standard (protocol) for wireless data-communication.
- More than 300 members worldwide: Manufacturers, software industry, computer and telecommunication companies & network-operators
- Meanwhile consolidated into the Open Mobile Alliance (OMA)





- Introduction
- Security Components
- Security Protocols
- Security Threats
- Wireless / Mobile Security
 - Mobile Internet Security
 - Wireless LAN (WLAN)
 - Mobile IP
 - “Telco” Networks
 - GSM Security
 - GPRS Security
 - UMTS Security
 - Wireless Application Protocol (WAP)
 - Personal Area Networks

- “PAN“: Personal Area Network
- Personal environment, short range
- Purpose: Connection of devices in short range, for example PDAs and printers (IrDA, Bluetooth)
- Replaces cable-connections



- IrDA: Infrared Data Association (1993):
 - Standardized infrared-protocols
 - IrDA Version 1: asynchronous, serial connection up to 115 kbps
 - Point-to-Point
 - Protocol-family for various purposes
 - New specification: up to 4 Mbit/s
- Exemplary applications:
 - Transmission of mobile business cards
 - Sales data extraction from cigarette vending machines
 - Connection between mobile and laptop
 - Wireless printing



- **Attributes:**
 - Wireless
 - Range up to 10 meters
 - Illumination-angle 15° - 30°

- **Disadvantages:**
 - Sounding: if the infrared-ray misses the target
 - Optical connection required
 - Short interruption of the optical connection e.g. between laptop and mobile phone in the trains leads to complete network-interruption



- Frequency range of 2.4 GHz
- Simple and cheap possibility to set up ad-hoc networks of limited range (up to 10 meters)
- No official standard, but de-facto-standard
- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba, etc.
- Broadly supported by industry

- „Bonding“ of devices:
 - Exchange of IDs (48 bit, globally unique (!), public)
 - Agreement on key for protected communication
- Access control for devices and singular services possible (3 security modes)
- **Sufficient** for „own“ devices when they are introduced to each other in a secure environment
- **Problematic** when ad hoc networks are initiated in unknown environments
- **Dangerous** when devices are configured to
 - Search (“inquire”) for other devices and connect
 - Be open and detectable for other devices

- Bundesnetzagentur (RegTP): Rules for the Award of Licences for UMTS/IMT-2000;
<http://www.bundesnetzagentur.de/cae/servlet/contentblob/39016/publicationFile/2767/RegelnzurLizenzvergabeld353pdf.pdf>
- ETSI: **GSM - Historical Background, 2000**;
<http://www.etsi.org/WebSite/Technologies/Cellularhistory.aspx>
- Federrath, Hannes: **Protection in Mobile Communications**, in: Günter Müller, Kai Rannenberg (Ed.): *Multilateral Security in Communications*, Addison-Wesley-Longman 1999, pp. 349-364.
- Halvorsen, Finn Michael and Haugen, Olav: *Cryptanalysis of IEEE 802.11i TKIP*, NTNU, Master Thesis, 2009.
- Jain, Raj: *Wireless LAN Security II: WEP Attacks, WEP Attacks, WPA and WPA2*, Washington University in Saint Louis, 2007.
http://www.cse.wustl.edu/~jain/cse571-07/ftp/I_21wpa.pdf
- IEEE, <http://grouper.ieee.org/groups/802/11/>, accessed 2013-10-09.
- Mobile IP: RFCs of IETF: www.ietf.org/html.charters/mobileip-charter.html , especially RFC 2002.
- OMA Open Mobile Alliance: **Wireless Application Protocol Specifications, 2010**, <http://www.wapforum.org/what/technical.htm>.
- Sauter, M. (2008): *Grundkurs Mobile Kommunikationssysteme (3., erweiterte Auflage)*, Vieweg, Wiesbaden.
- Schiller, Jochen: **Mobile Communications**, London, 2003, pp. 93-156.