

# Information & Communication Security (SS 2022)

## Network Security II

**Prof. Dr. Kai Rannenber**

Chair of Mobile Business & Multilateral Security

Goethe University Frankfurt

[www.m-chair.de](http://www.m-chair.de)

- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- **Wireless / Mobile Security**
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G 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.

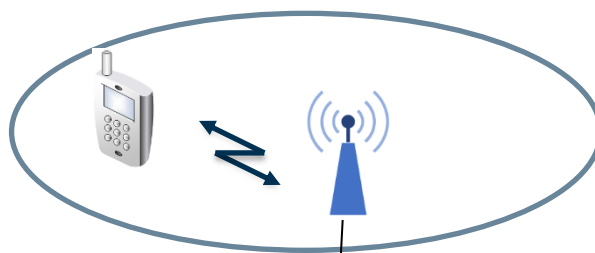
- **Access Point (AP):**  
Transmitting and receiving station which allows multiple devices to connect
- **Stations:**  
Terminals, used by AP for building a wireless network connection (Example: PCMCIA-WLAN Card in Laptops)



# Wireless LAN Basics

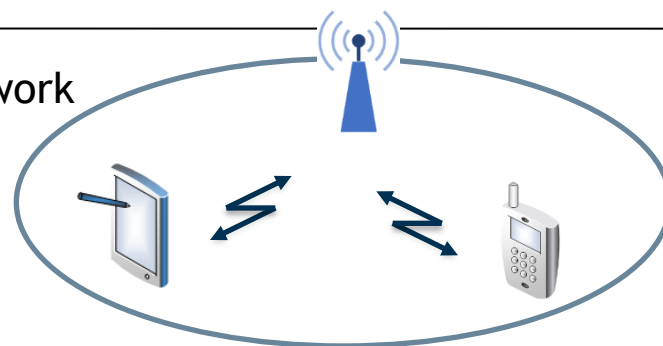
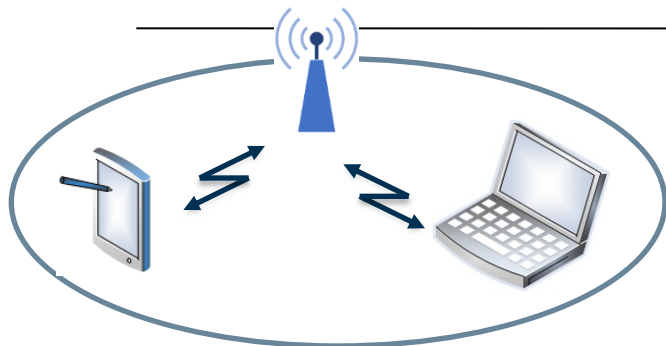
## Infrastructure and ad hoc networks

Infrastructure network

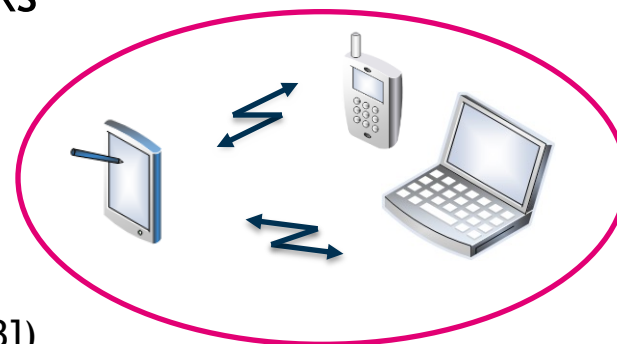
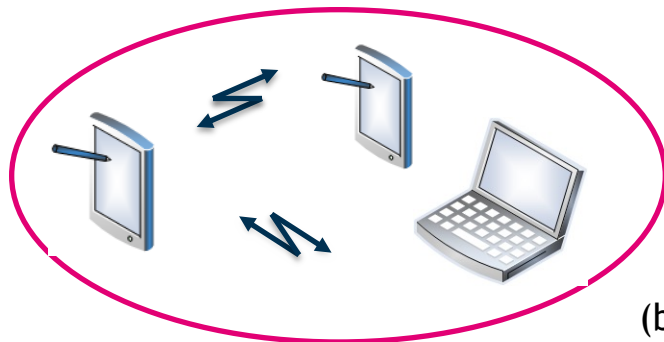


Access Point

Existing fixed network



Ad hoc networks



(based on [Schiller03])

# Wireless LAN Basics

## 802.11 Standard

Standard	Release date	Description
802.11	1997	Protocol for transmission methods for wireless networks, defined in 1997 for 2 MBit/s at 2,4 GHz
802.11a	1999	Wireless LAN <b>up to 54 MBit/s</b> at 5 GHz
802.11b	1999	Wireless LAN <b>up to 11 MBit/s</b> at 2,4 GHz
802.11g	2003	Wireless LAN <b>up to 54 MBit/s</b> at 2,4 GHz
802.11i	2004	Extended security features: AES, 802.1x, TKIP
802.11ad	2012	Wireless LAN at 60GHz: <b>Up to 7GBit/s</b>
802.11ac	2013	Wireless LAN using 3 spatial streams at 5 GHz: <b>Up to 1.3 GBit/s</b> (3x 433 Mbit/s) or even <b>up to 2.6 GBit/s</b> (3x 867 Mbit/s, part of 802.11ac Wave2) *) **)
802.11ah	2016	Wi-Fi HaLow for Smart Home and connected devices (900 MHz, increased distance, ~1km)
802.11ax	2017	This amendment defines modifications for high efficiency operation in frequency bands between 1 GHz and 7.125 GHz.
802.11ay	2021	Standard extending 802.11ad by defining a new physical layer for 802.11 networks to operate in the <b>60 GHz</b> spectrum
802.11ba	2021	Amendment of IEEE 802.11 enabling energy efficient operation for data reception without increasing latency
802.11be	-	Potential next amendment likely be designated Wi-Fi 7 building upon 802.11ax

\*) 802.11n and 802.11ac data rates depend on the number of antennas and spatial streams 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] [IEEE17]  
[Sauter 2008]

- 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

# Wireless LAN (In)Security

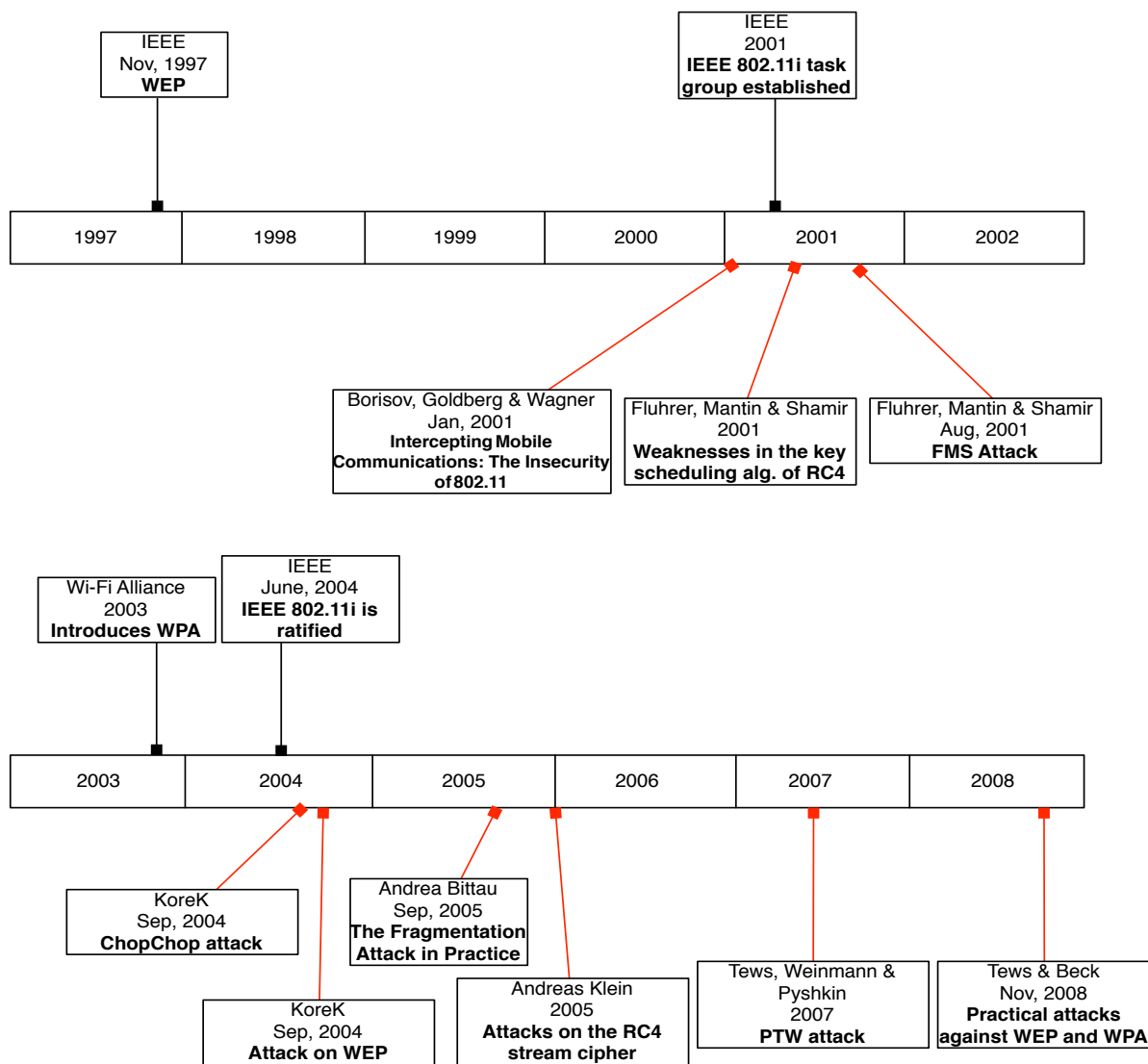
## IEEE 802.11-1997 (2): Vulnerabilities

- 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



# Wireless LAN (In)Security

## IEEE 802.11-1997 (3): Discovery of vulnerabilities



[Halvorsen09]

- 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 [Jain07]

- 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
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G Security
  - Wireless Application Protocol (WAP)
  - Personal Area Networks

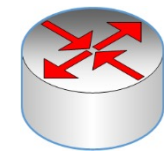
## Situation today

- 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

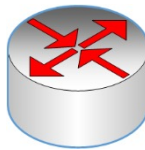
# Routing in TCP/IP



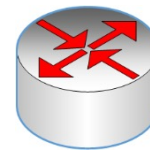
Partner B  
IP address, e.g.  
61.9.193.200



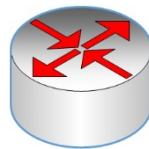
Router



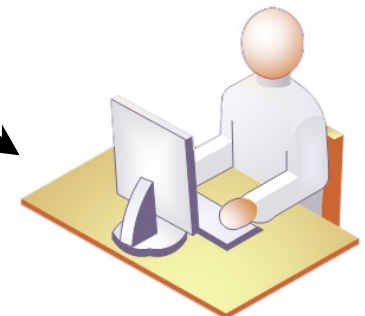
Router



Router



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



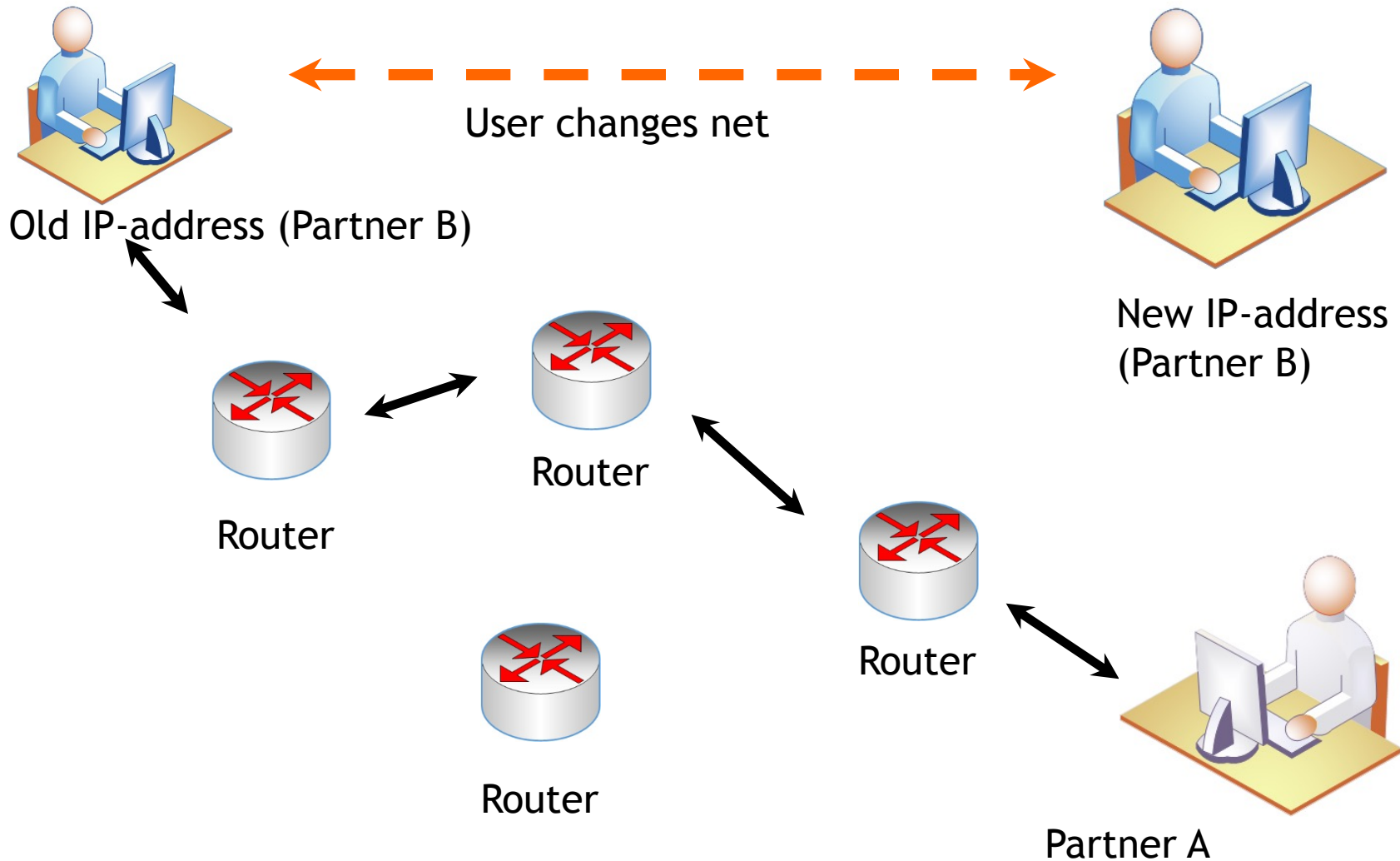
# Updating Domain Names

- 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.

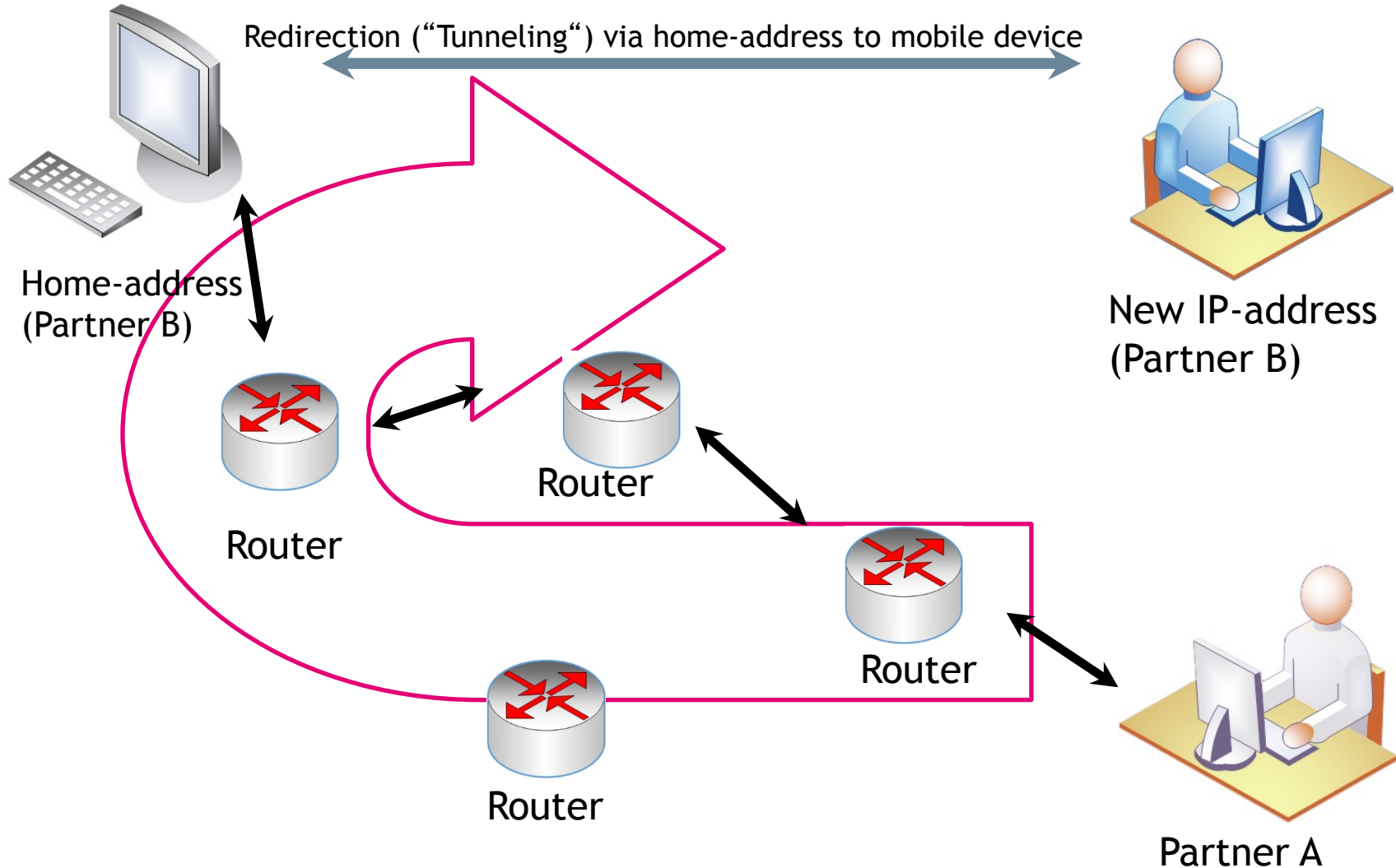
# Addressing of mobile devices

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

# Roaming problem

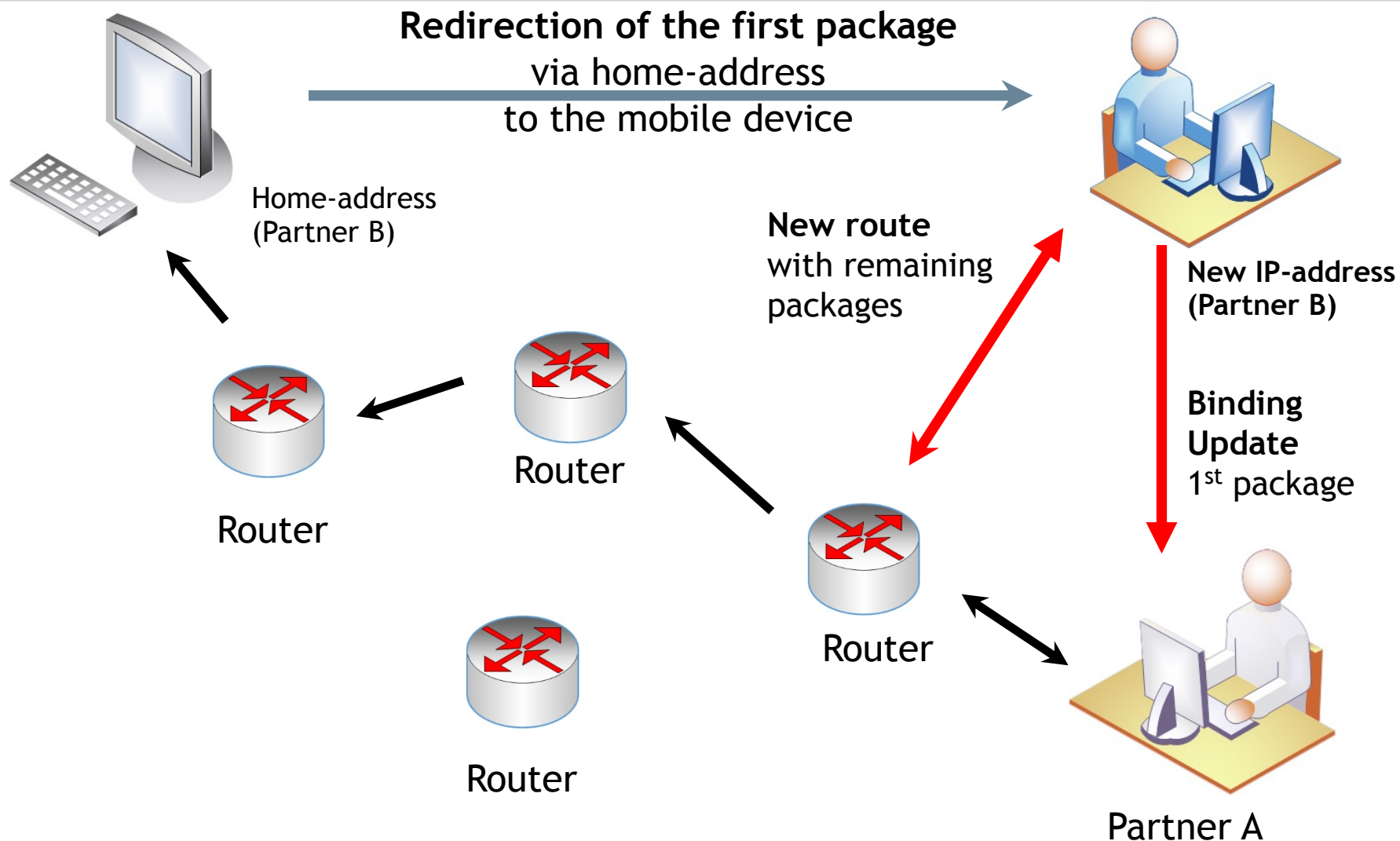


# Roaming solution Layer 3



- **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.

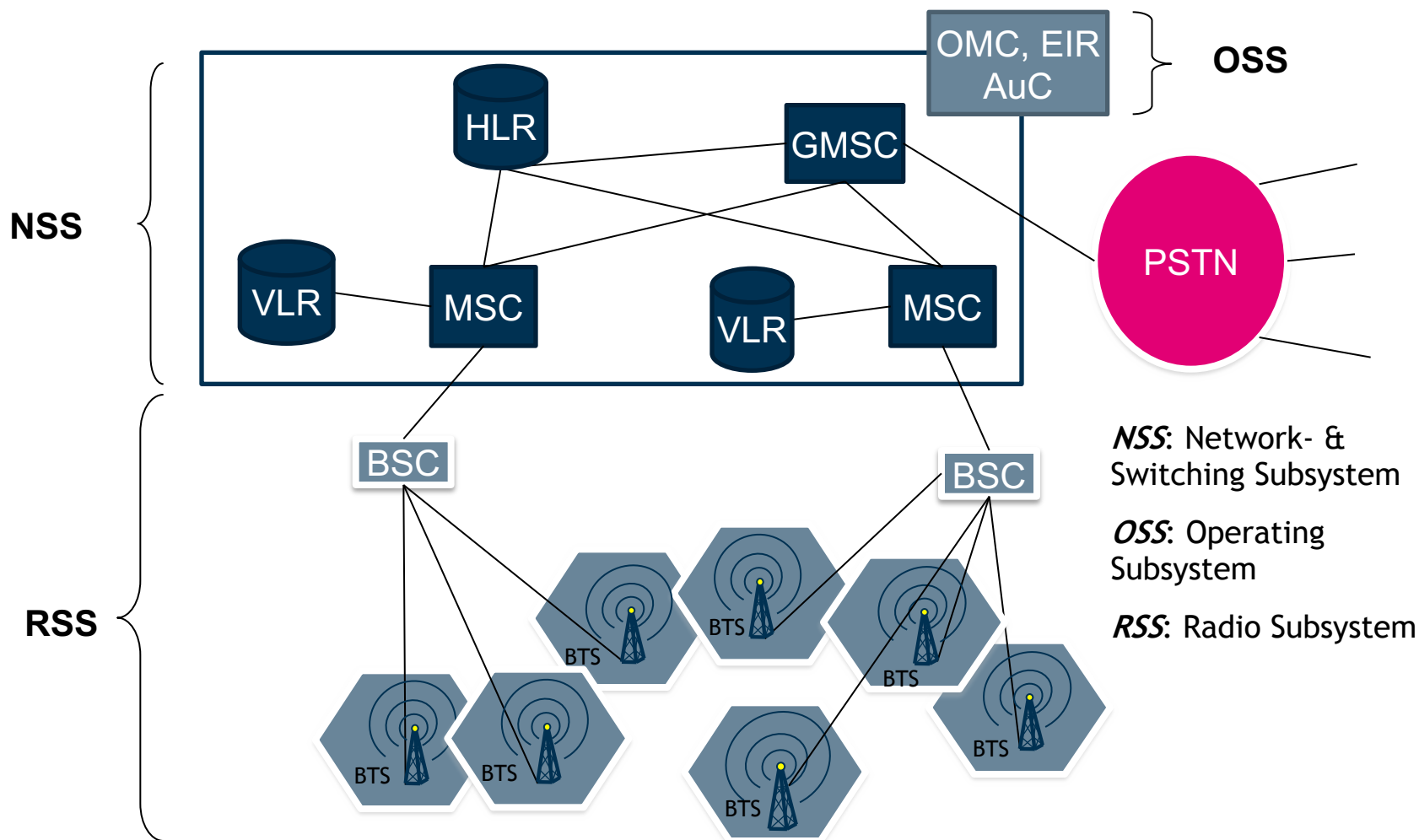
- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G 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.

# GSM (2G)

## System Architecture



Based on [Schiller03]

The GSM system offers several “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:

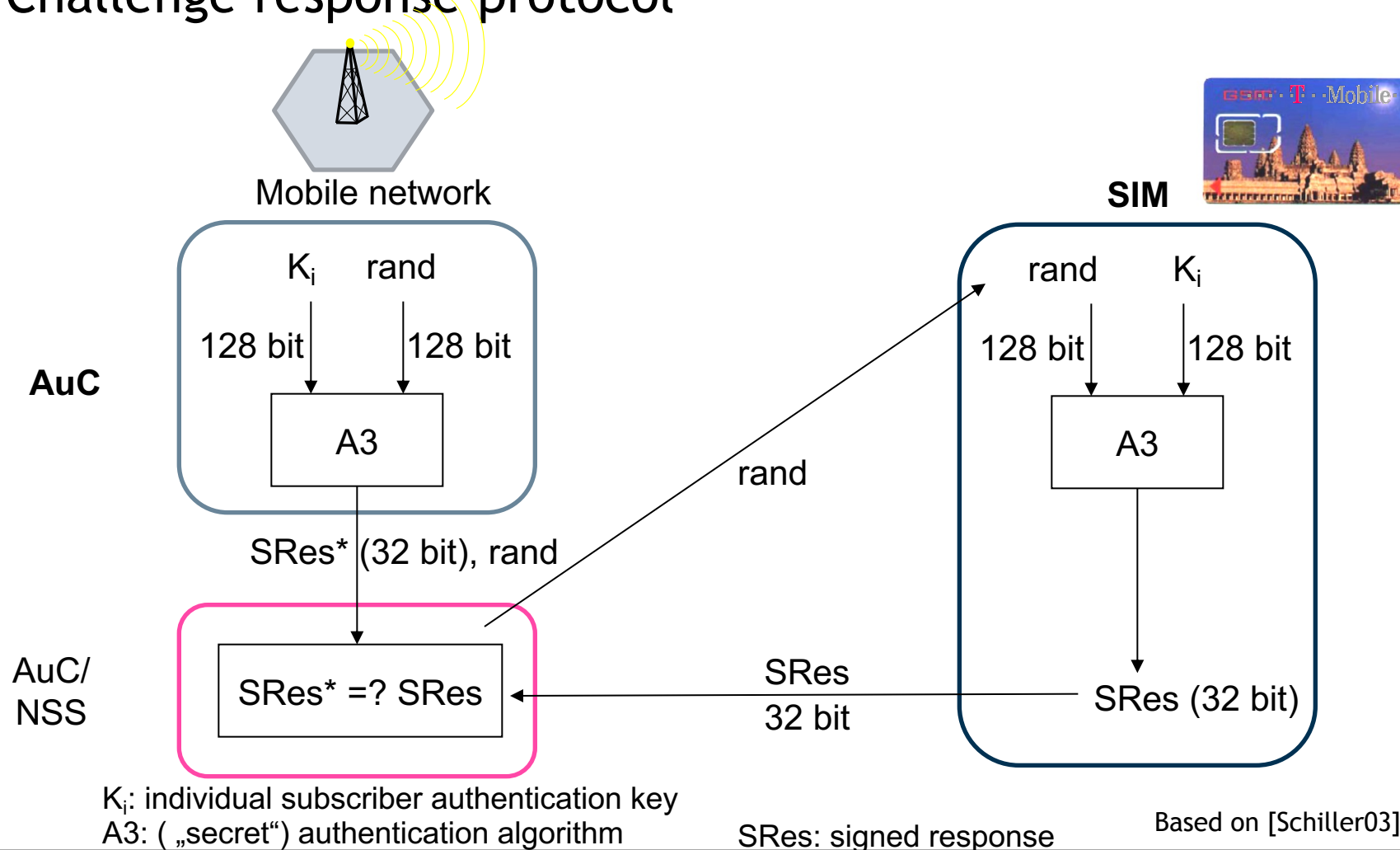
Data & voice transferred between mobile station and BTS are encrypted.

(Partial) Anonymity:

No transfer of data which can identify the subscriber via radio, instead temporary identification (Temporary Mobile Subscriber ID, TMSI)

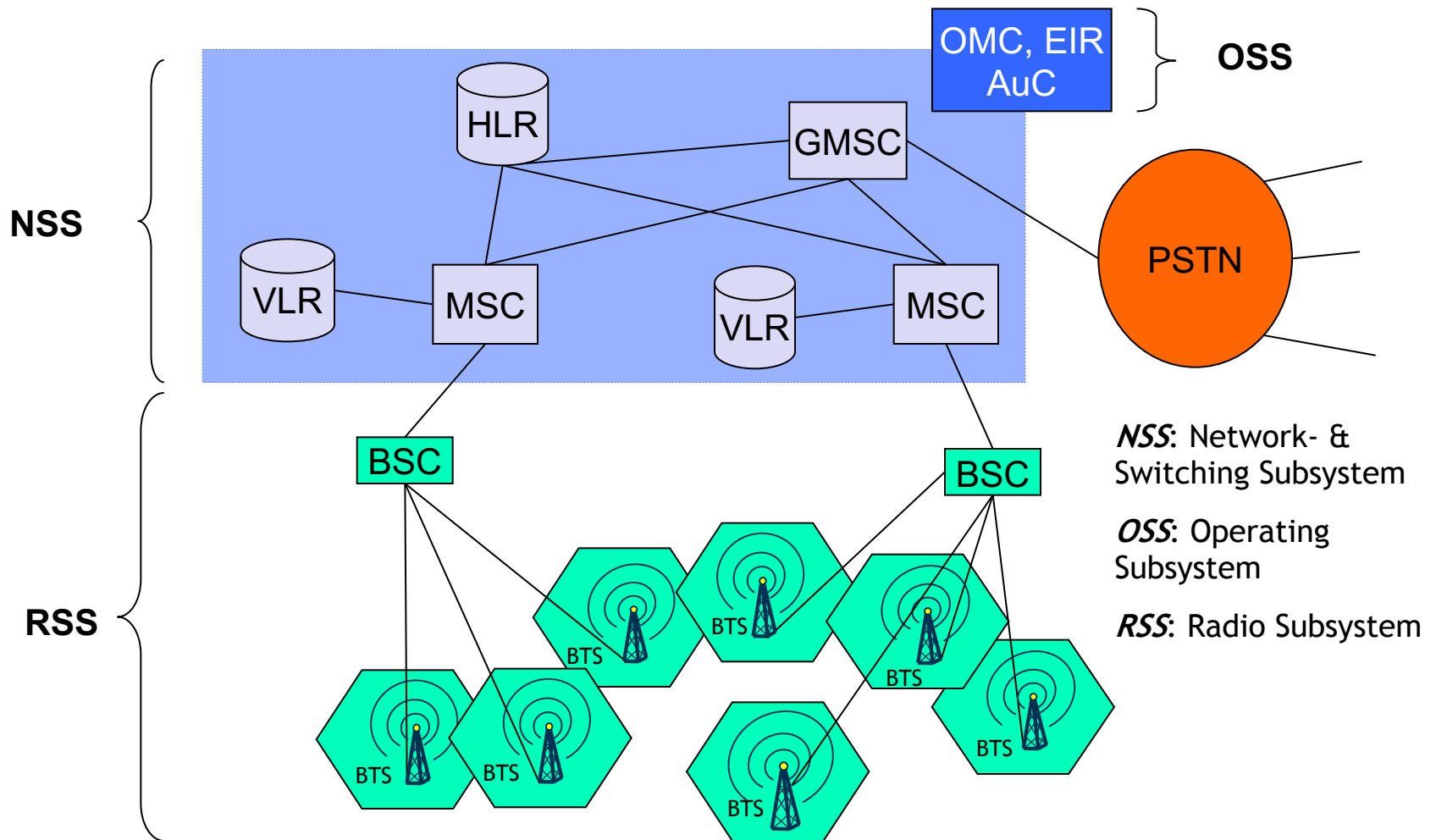
# SIM based subscriber authentication

## Challenge response protocol



# SIM based subscriber authentication

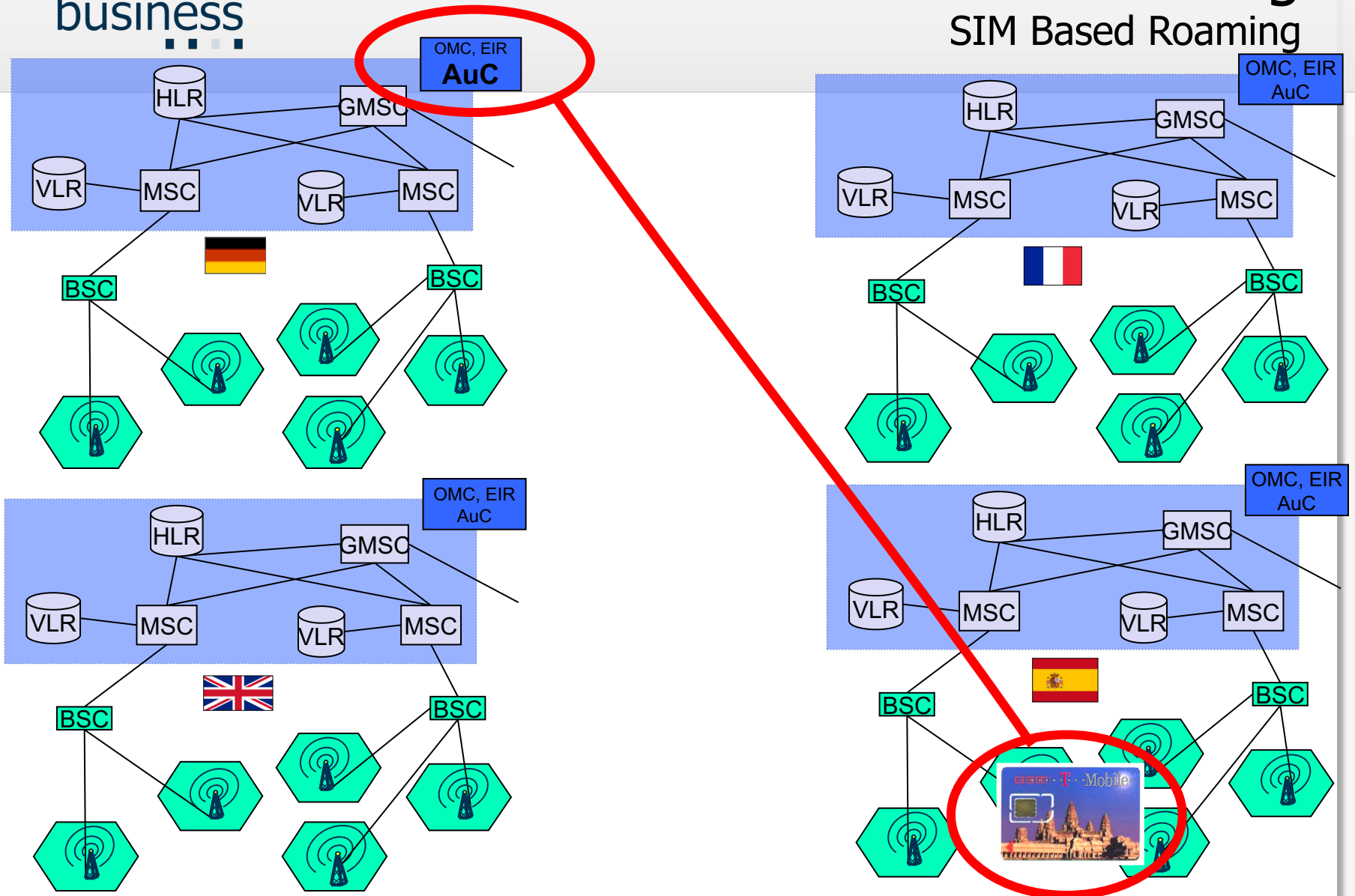
- Challenge-Response-Procedure
  - Authentication is based on the individual key  $K_i$ , the subscriber identification IMSI, and a secret algorithm A3.
  - $K_i$  and A3 are stored on the SIM and in the AuC.
- 
1. AuC creates random number *rand*.
  2. AuC encrypts *rand* and  $K_i$  via A3 (-> SRes\*).
  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.



Based on [Schiller03]

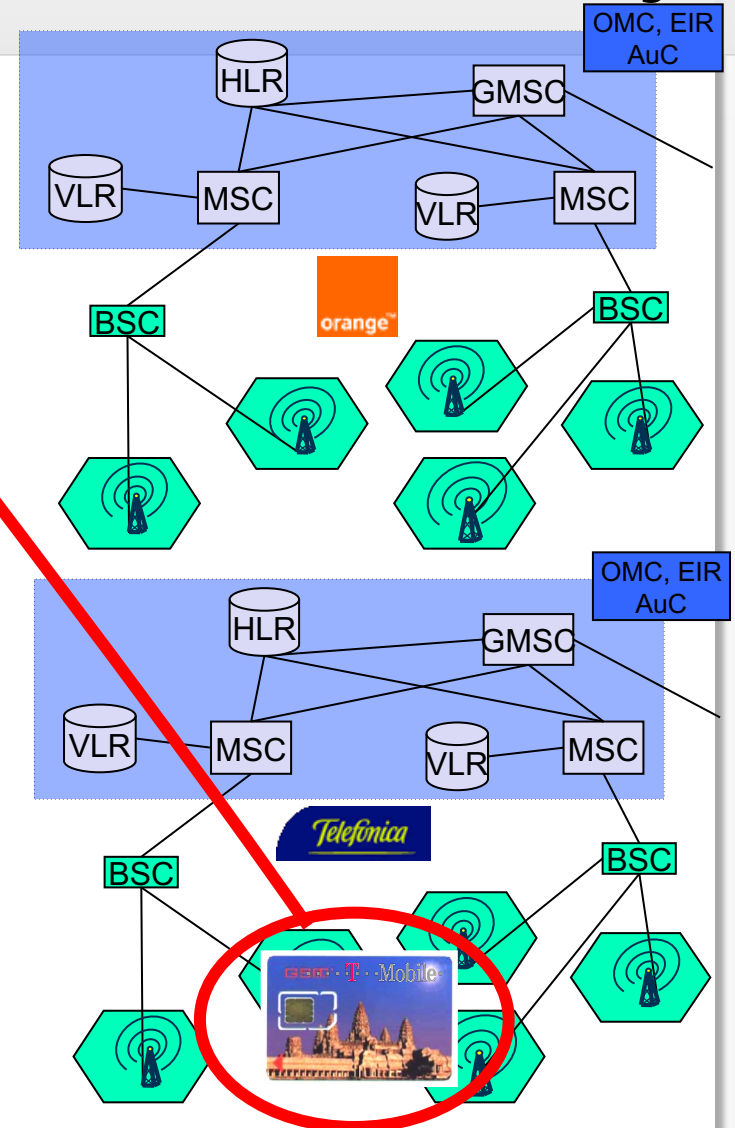
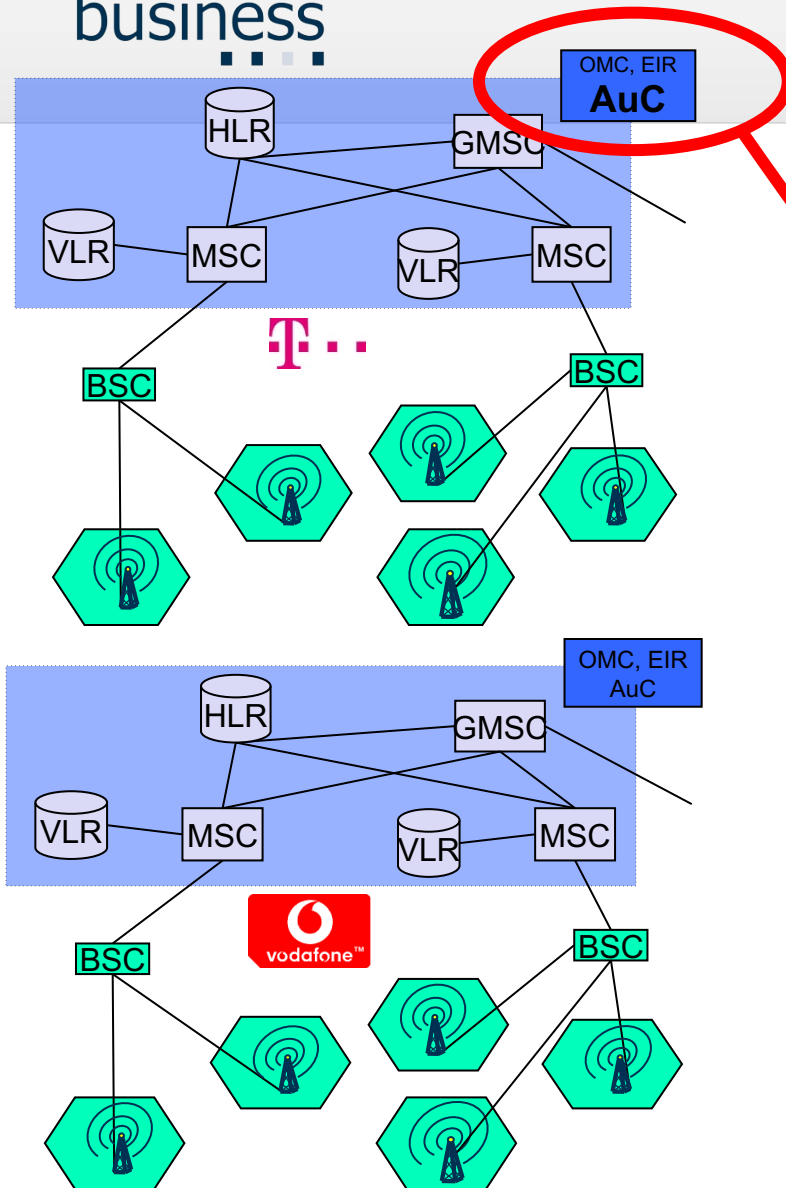
# Roaming

## SIM Based Roaming



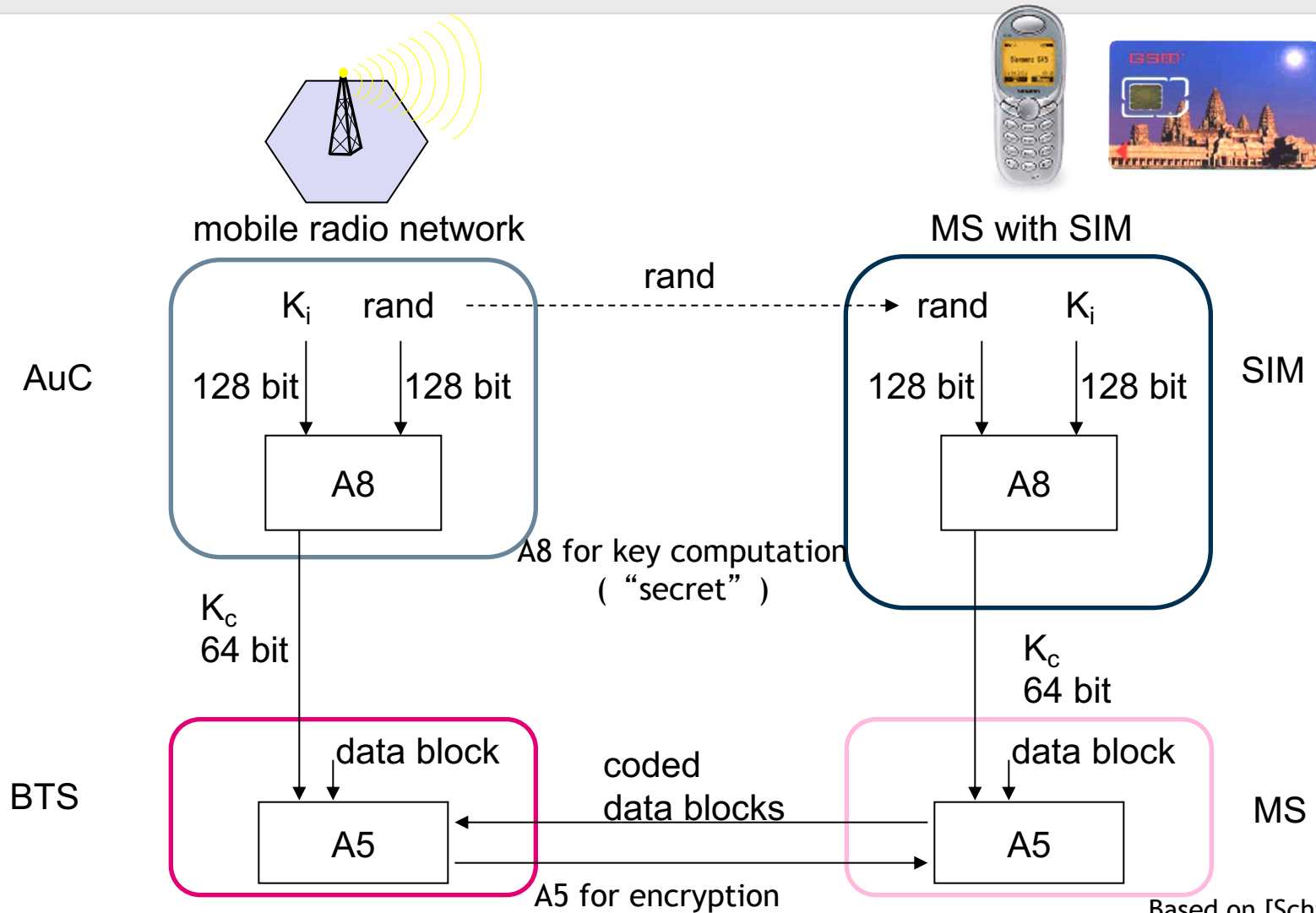
# Roaming

## SIM Based Roaming





# Content Encryption



- 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
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G 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.

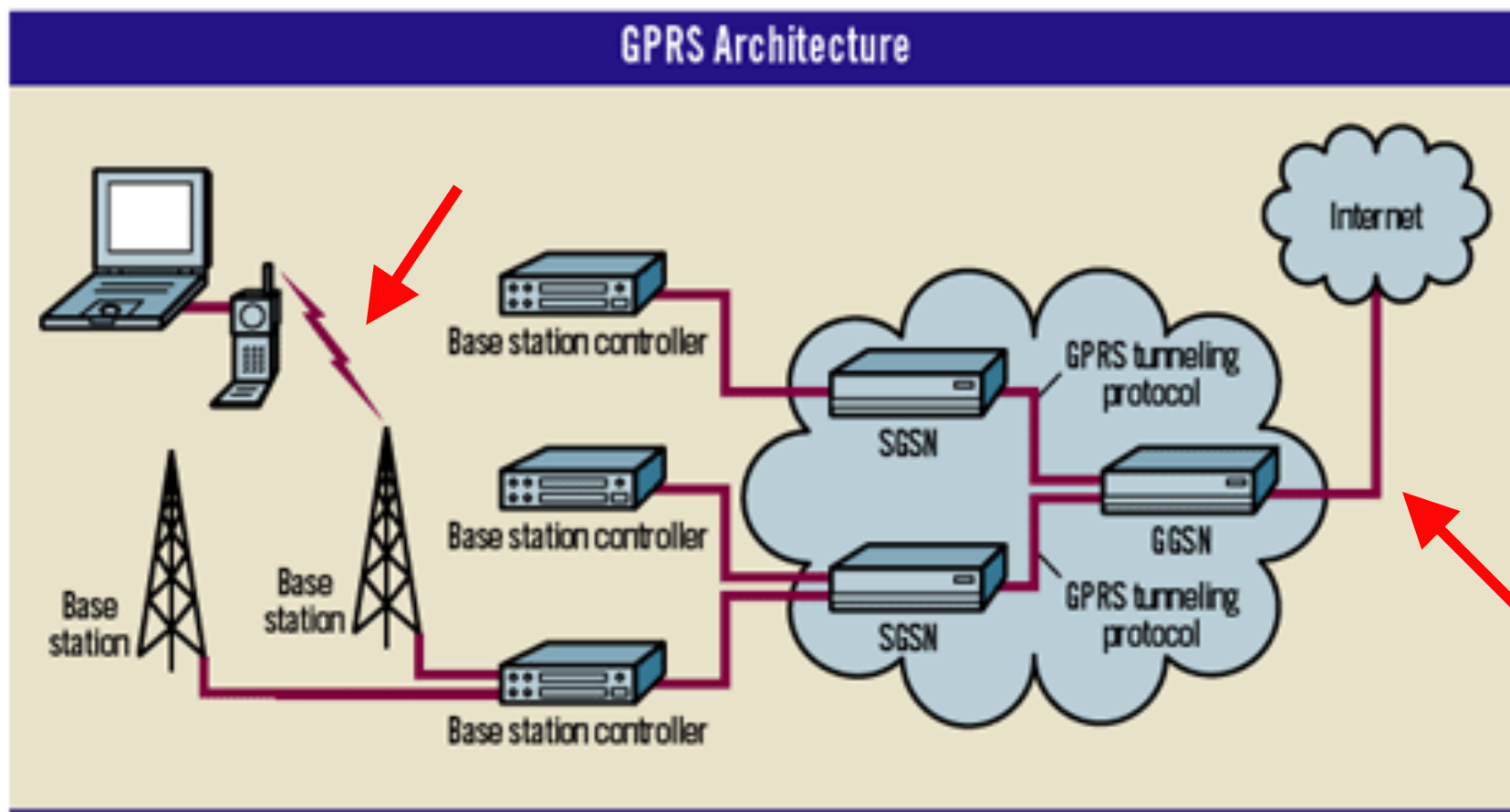
- Up to 8 time slots can be occupied per time frame (at the moment 4 in practice).
- In contrast to HSCSD the GPRS data service requires an extensive upgrade of the GSM architecture with new network components.
- In spite of better network utilization and volume based billing at the beginning the data 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.

# GPRS

## Architectural Security Issues



- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G 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.

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
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G Security
  - Wireless Application Protocol (WAP)
  - Personal Area Networks

- **Long Term Evolution (3.9G, “4G”)** standard allows for 300 Mbit/s downlink and 75 Mbit/s uplink speeds
  - First commercial LTE network launched in Scandinavia in December 2009
  - LTE was originally not named a “4G network” due to stricter naming requirements \*)
  - The technology can be named either 3.9G or 4G network today.
- **LTE Advanced (4G)** makes use of the frequency spectrum more efficiently, resulting in higher data rates (towards 1 Gbit/s) and lower latency. It remains backward compatible with LTE, uses same frequency bands.



<http://www.3gpp.org/LTE>



<http://www.3gpp.org/LTE-Advanced>

\*) A 4G service was originally defined as meeting the *IMT-Advanced* requirements issued by the ITU-R. For more information see [Parkvall2008].



## Characteristics of LTE Security

- Re-use of UMTS Authentication and Key Agreement (AKA)
- Use of USIM required (GSM SIM excluded)
- Extended key hierarchy
- Possibility for longer keys
- Greater protection for the link between the core network subnet works.
- Integrated interworking security for legacy and non-3GPP networks

[Dionisio11]

- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G Security
  - Wireless Application Protocol (WAP)
  - Personal Area Networks

# 5<sup>th</sup> Generation (5G) The Concept

## Two views of 5G

- **View 1** - The hyper-connected vision
- **View 2** - Next-generation radio access technology

## 5G technology requirements

- 1 millisecond end-to-end round trip delay (latency)
- 1-10 Gbps connections to end points in the field (i.e. not theoretical maximum)
- 1000 x bandwidth per unit area
- 10-100 x number of connected devices
- 99.999 % availability
- 100 % geographical coverage
- 90 % reduction in network energy usage
- Up to ten year battery life for low power, machine-type devices

## **Security and privacy requirements**

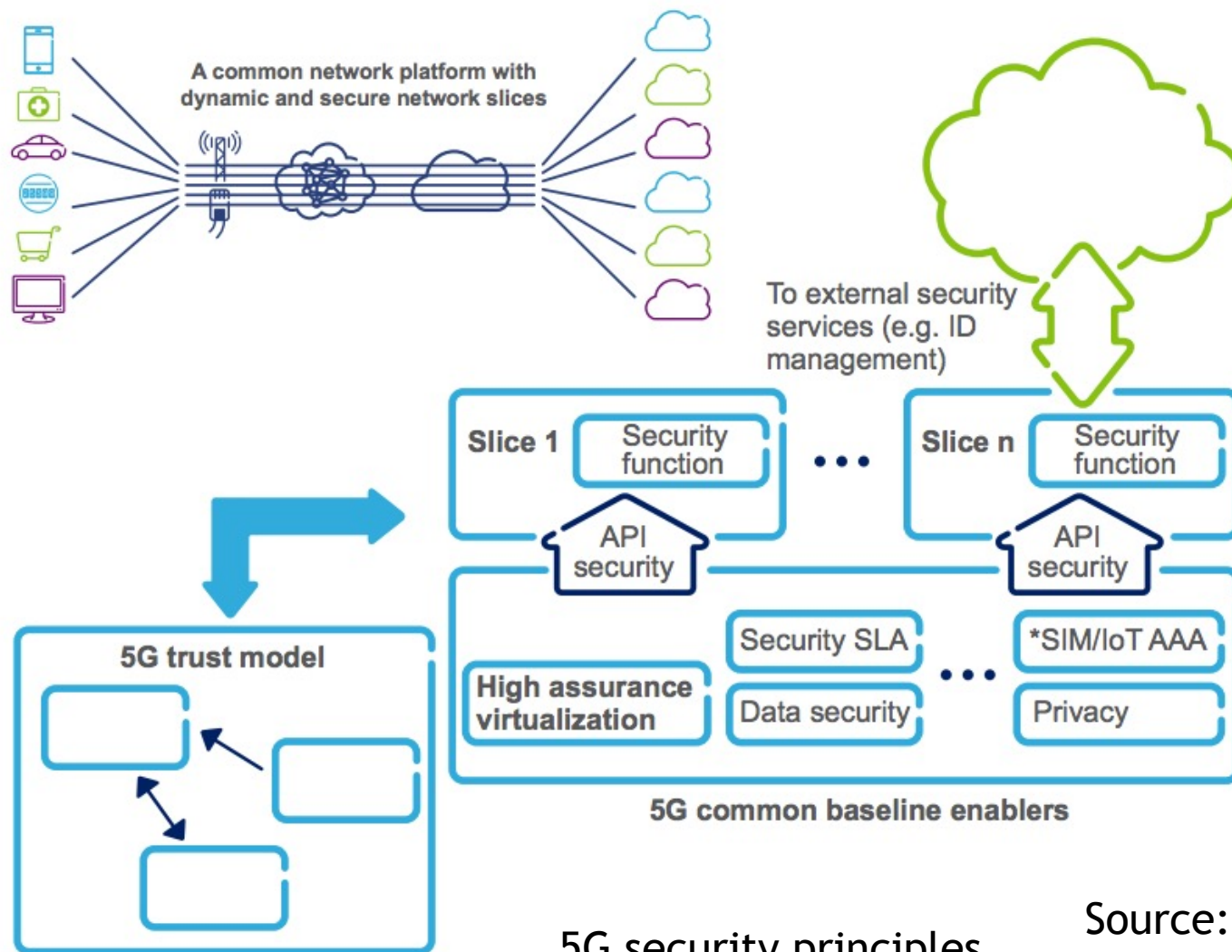
- New trust model
- Security for new service delivery models
- Evolved threat landscape
- Increased privacy concerns

## **Core 5G security concepts**

- Security assurance
- Identity Management
- 5G radio network security
- Flexible and scalable security architecture
- Energy-efficient security
- Cloud security

[5Gsec]

# 5<sup>th</sup> Generation (5G) Security II



5G security principles

Source: [5Gsec]

# 5<sup>th</sup> Generation (5G) Security Issues

- Huawei 5G switches
  - Public discussion about possible security risks due to Huawei 5G network components
  - Huawei's 5G networks were named a "trojan horse" by US officials in 2019 who also warned the NATO about the companies technology [CNBC2019]
  - In 2020, 41 members of the European Parliament labelled Chinese 5G vendors Huawei and ZTE as "high risk" companies with respect to potential security threats [Brusselstime2020]
- Main security threat: weak security of the infrastructure components could be exploited by hackers to gain access to important networks (spying) or even to disrupt internet access [BBC2020]

- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G Security
  - Wireless Application Protocol (WAP)
  - Personal Area Networks

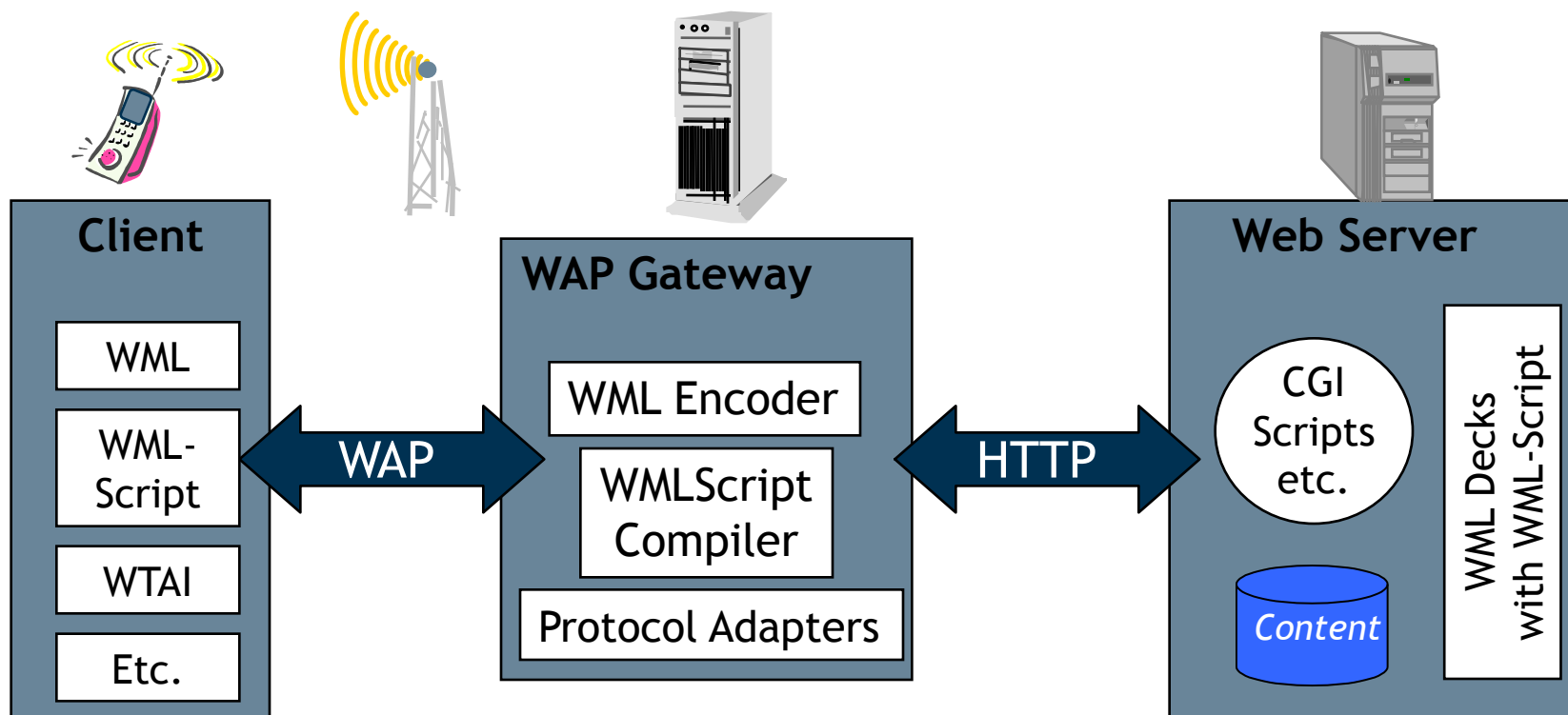
## Wireless Application Protocol (WAP)

- 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)



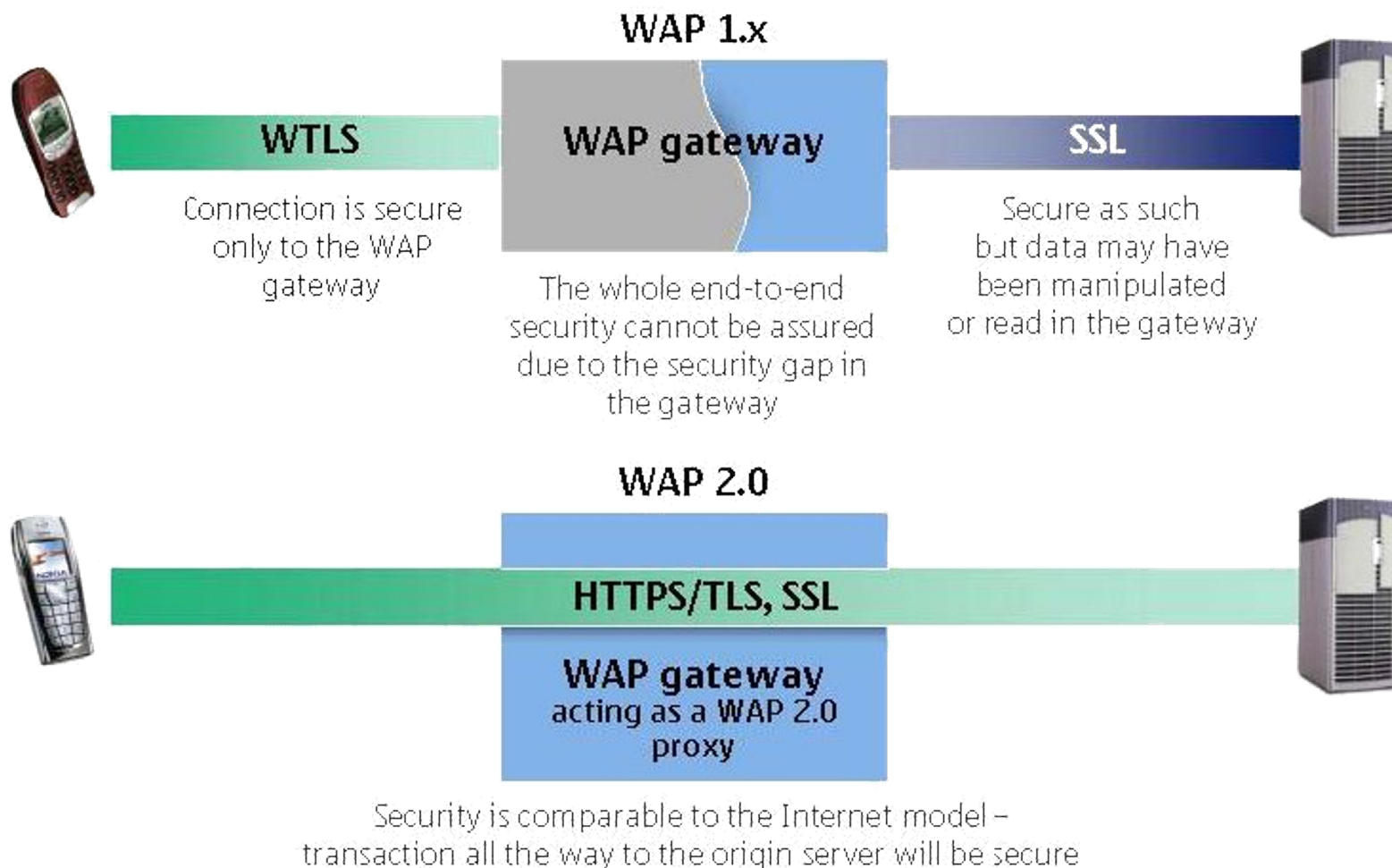


# Application environment WAP Gateway



# Comparison of Infrastructures

## WAP 1.x vs. WAP 2.0



- Introduction
- Infrastructure Security Components
- Security Protocols
- Application Layer Security
- Wireless / Mobile Security
  - Wireless Internet Security
    - Wireless LAN (WLAN)
    - Mobile IP
  - “Telco” Networks
    - GSM Security
    - GPRS Security
    - UMTS Security
    - LTE Security
    - 5G Security
  - Wireless Application Protocol (WAP)
  - Personal Area Networks

# 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 1.3: asynchronous, serial connection up to 1 Mbps
- 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
  - Using smartphones as remote controllers for TVs

## ■ Attributes:

- Wireless
- Range up to 10 meters
- Illumination-angle  $15^{\circ}$  -  $30^{\circ}$

## ■ 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. (Bluetooth Special Interest Group (Bluetooth SIG))
- Broadly supported by industry

# Bluetooth

## Popular applications

File exchange between  
mobile devices



Wireless extension of device  
features (headset for mobile)





- „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

- [BBC2020] <https://www.bbc.com/news/newsbeat-47041341>
- [Brusselstime2020] <https://www.brusselstimes.com/135929/huawei-zte-eu-european-union-5g-threat-security-high-risk-digital-network-thierry-breton-margrethe-vestager>
- [CNBC2019] <https://www.cnbc.com/2019/06/28/huawei-expansion-in-western-nations-may-be-a-trojan-horse-warns-a-top-gop-senate-leader.html>
- [Dionisio11] Dionisio Zumerle (2011), 3GPP LTE Security Aspects, [ftp://www.3gpp.org/Information/presentations/presentations\\_2011/2011\\_05\\_Bangalore/DZBangalore290511.pdf](ftp://www.3gpp.org/Information/presentations/presentations_2011/2011_05_Bangalore/DZBangalore290511.pdf)
- [IEEE] IEEE, <http://grouper.ieee.org/groups/802/11/>, accessed 2013-10-09.
- [IEEE17] IEEE SA: Standard Association, [https://standards.ieee.org/project/802\\_11ax.html](https://standards.ieee.org/project/802_11ax.html) accessed 2020-06-30
- [ETSI00] ETSI: GSM - Historical Background, 2000; <http://www.etsi.org/WebSite/Technologies/Cellularhistory.aspx>
- [GSMA5G] Understanding 5G: Perspectives on future technological advancements in mobile, December 2014GSM <https://gsmaintelligence.com/research/?file=141208-5g.pdf&download>
- [Halvorsen09] Halvorsen, Finn Michael and Haugen, Olav: Cryptanalysis of IEEE 802.11i TKIP, NTNU, Master Thesis, 2009.

- [Jain07] 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/l\\_21wpa.pdf](http://www.cse.wustl.edu/~jain/cse571-07/ftp/l_21wpa.pdf)
- [MIP02] Mobile IP: RFCs of IETF: [www.ietf.org/html.charters/mobileip-charter.html](http://www.ietf.org/html.charters/mobileip-charter.html) , especially RFC 2002.
- [OMA10] OMA Open Mobile Alliance: Wireless Application Protocol Specifications, 2010, <http://www.wapforum.org/what/technical.htm>.
- [Parkvall2008] Parkvall, S.; Dahlman, E.; Furuskär, A. - LTE Advanced - Evolving LTE towards IMT-Advanced (PDF). Vehicular Technology Conference Fall 2008,  
[http://www.ericsson.com/res/thecompany/docs/journal\\_conference\\_papers/wireless\\_access/VTC08F\\_jading.pdf](http://www.ericsson.com/res/thecompany/docs/journal_conference_papers/wireless_access/VTC08F_jading.pdf), accessed 2013-10-14.
- [Sauter08] Sauter, M. (2008): Grundkurs Mobile Kommunikationssysteme (3., erweiterte Auflage), Vieweg, Wiesbaden.
- [Schiller03] Schiller, Jochen: **Mobile Communications**, London, 2003, pp. 93-156.
- [5Gsec] 5G security: scenarios and solutions,  
<https://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf>