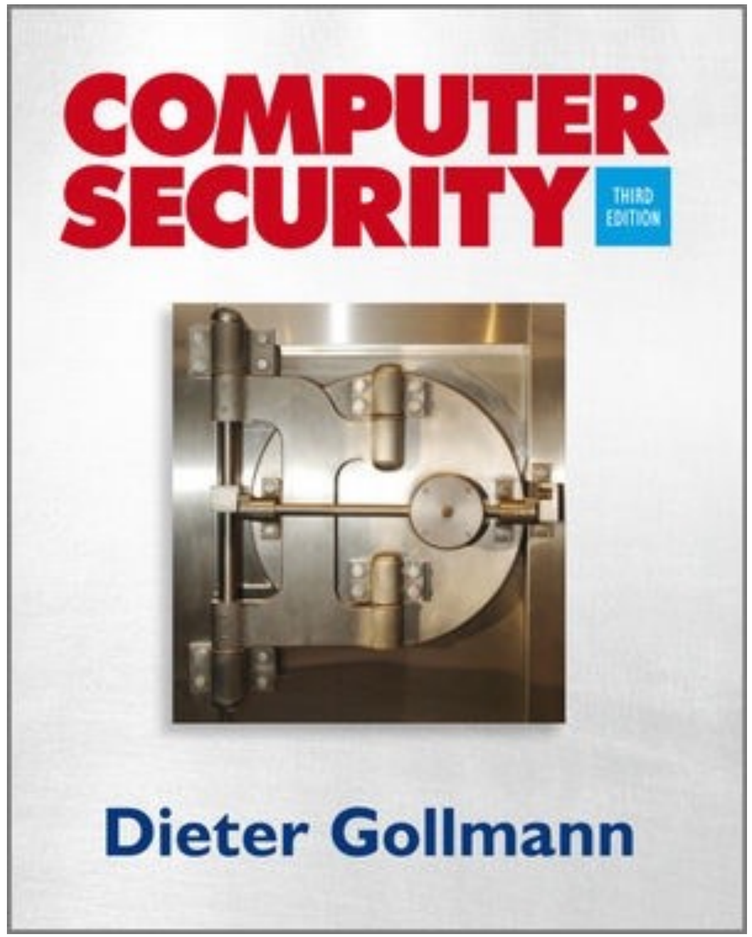
UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

L10 - Mobile Security and Key Handling

based on D. Goldman, “Computer Security”, Chapter 19



Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

Objectives

- Examine new security challenges and attacks specific to mobile services.
- Give an overview of the security solutions adopted for different mobile services.
- Show some novel ways of using of cryptographic mechanisms.
- Discuss the security aspects of location management in TCP/IP networks.

Agenda (slides 1-50)

- Security Architecture
- From PSTN to GSM
- GSM security
- UMTS authentication
  - What do we mean by “mutual authentication”
- ➡ LTE Security architecture
- ~~Mobile IPv6 security~~
  - ~~Secure binding updates~~
- ~~Cryptographically generated addresses~~
- ~~WLAN security~~
  - ~~WEP~~
  - ~~WPA~~
  - ~~Bluetooth~~

Public Switched Telephone Networks

- The “plain old telephone system” (with additional functionality)
- Provided (worldwide) telephone service
  - Government owned telephone companies
- Main driver telco: Availability service (postulation)
  - Limited (none?) focus on security services
  - Results in practice: No security mechanisms at all
- Stable service: 99.999% uptime
- Main driver for early attacks: Get free calls!

[source: Lars Strand, 2011]

Attack: Blueboxing

- Signaling sent in-band
- Could be emulated and manipulated by user
- Bluebox: Dedicated devices did the work for you

[source: Lars Strand, 2011]

Attack: Clip-on

- Physically attaching a phone to someone else's line to steal their service

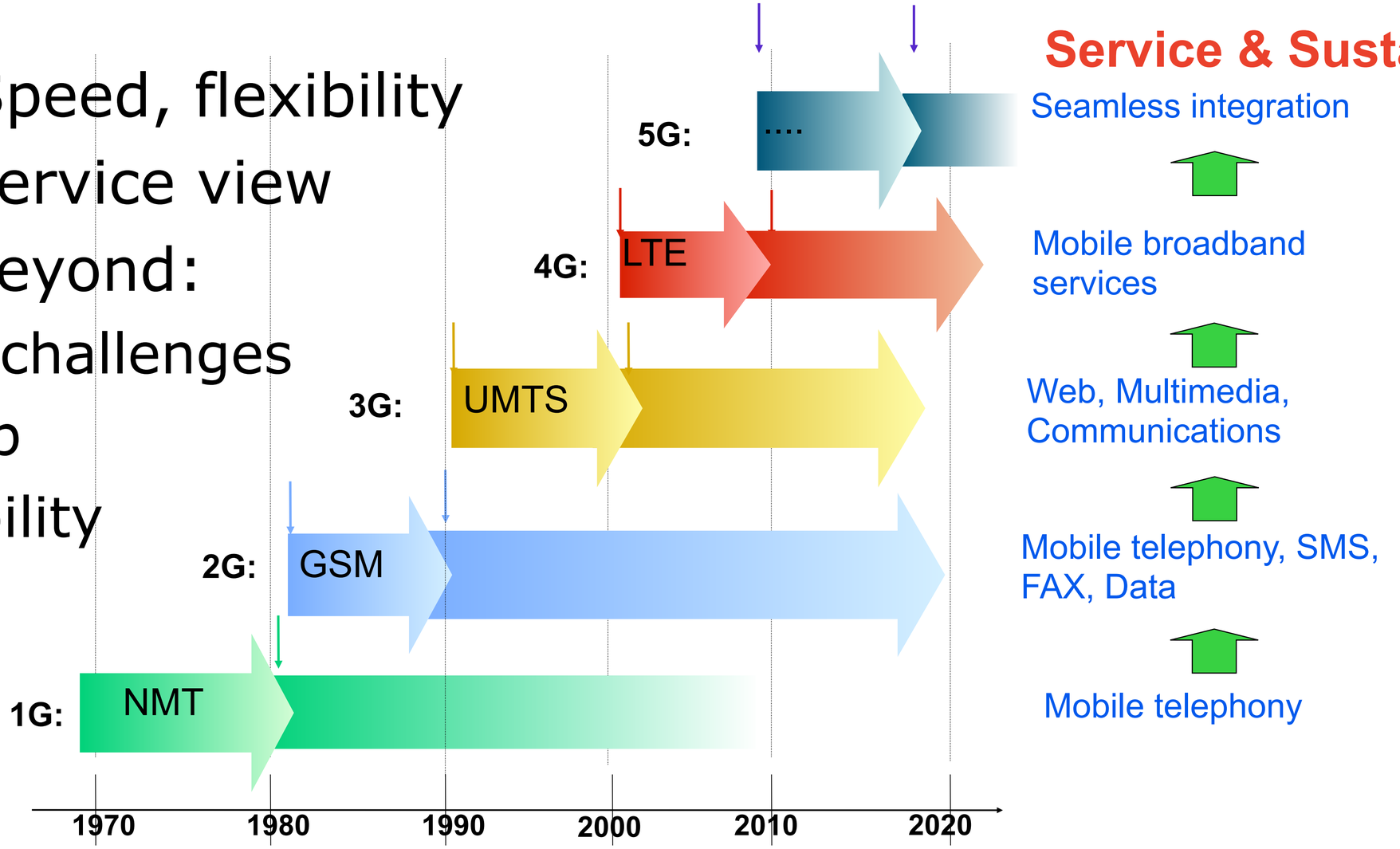
- Results:
  - Customer billed incorrectly
  - Hard to prove innocent

- Telco incentives to follow up low:
  - State owned (no competition)
  - Increased usage = increased revenue (except international calls)

[source: Lars Strand, 2011]

5G: Speed, Bandwidth, latency and

- 1G-3G: Speed, flexibility
- 3G-4G: service view
- 5G and beyond:
  - Business challenges
  - ownership
  - sustainability

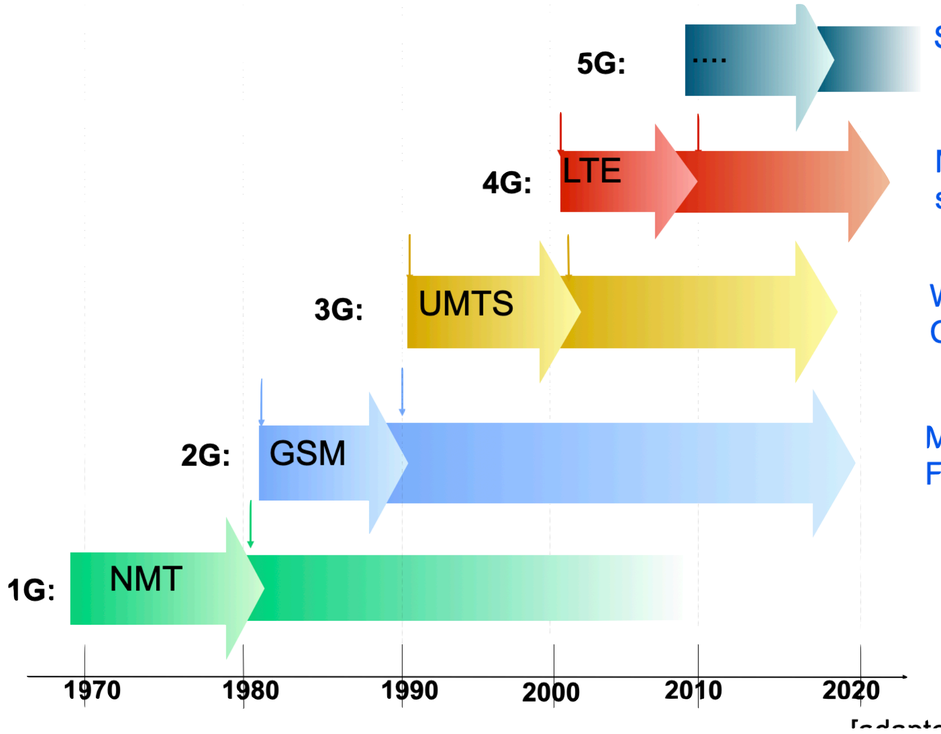


[adapted from Per Hjalmar Lehne, Telenor, 2000]

GSM & UMTS security

GSM: Threat environment

1. Vulnerability: Cloning
   - GSM security service: Authentication
   - GSM security mechanism: Authentication mechanism
2. Vulnerability: Content (voice) sent in clear
   - GSM security service: Call content confidentiality
   - GSM security mechanism: A5/1, A5/2, A5/3, A5/4
3. Vulnerability: Spying (subscriber location tracking)
   - GSM security service: Identity confidentiality
   - GSM security mechanism: Location security (TMSI)



[source: Lars Strand, 2011]

Security Goals

- Protect against interception of voice traffic on the radio channel:
  - Encryption of voice traffic.
- Protect signalling data on the radio channel:
  - Encryption of signalling data.
- Protections against unauthorised use (charging fraud):
  - Subscriber authentication (IMSI, TMSI).
- Theft of end device:
  - Identification of MS (IMEI), not always implemented.

GSM: Problems

- Focus on *access security*
  - Confidentiality terminated at the base stations
  - Weak operator network protection
  - Example: Traffic to/from BS and AuC should be protected!
- *"Security through obscurity"* - A3/A5/A8 eventually leaked
- Algorithms not resistant to cryptanalysis attack
  - A5/1 can "easily" be broken – in 2021 gradually replaced by A5/3
  - No public scrutiny during development
- Lack of user visibility
  - User do not know if/what encryption is used
- Difficult to upgrade cryptographic algorithms
  - But not in theory? Resides on the SIM card
- Authentication: One-way authentication only
  - Only MS to BS and not BS to MS.
- + many more..

[source: Lars Strand, 2011]

Cryptography in GSM

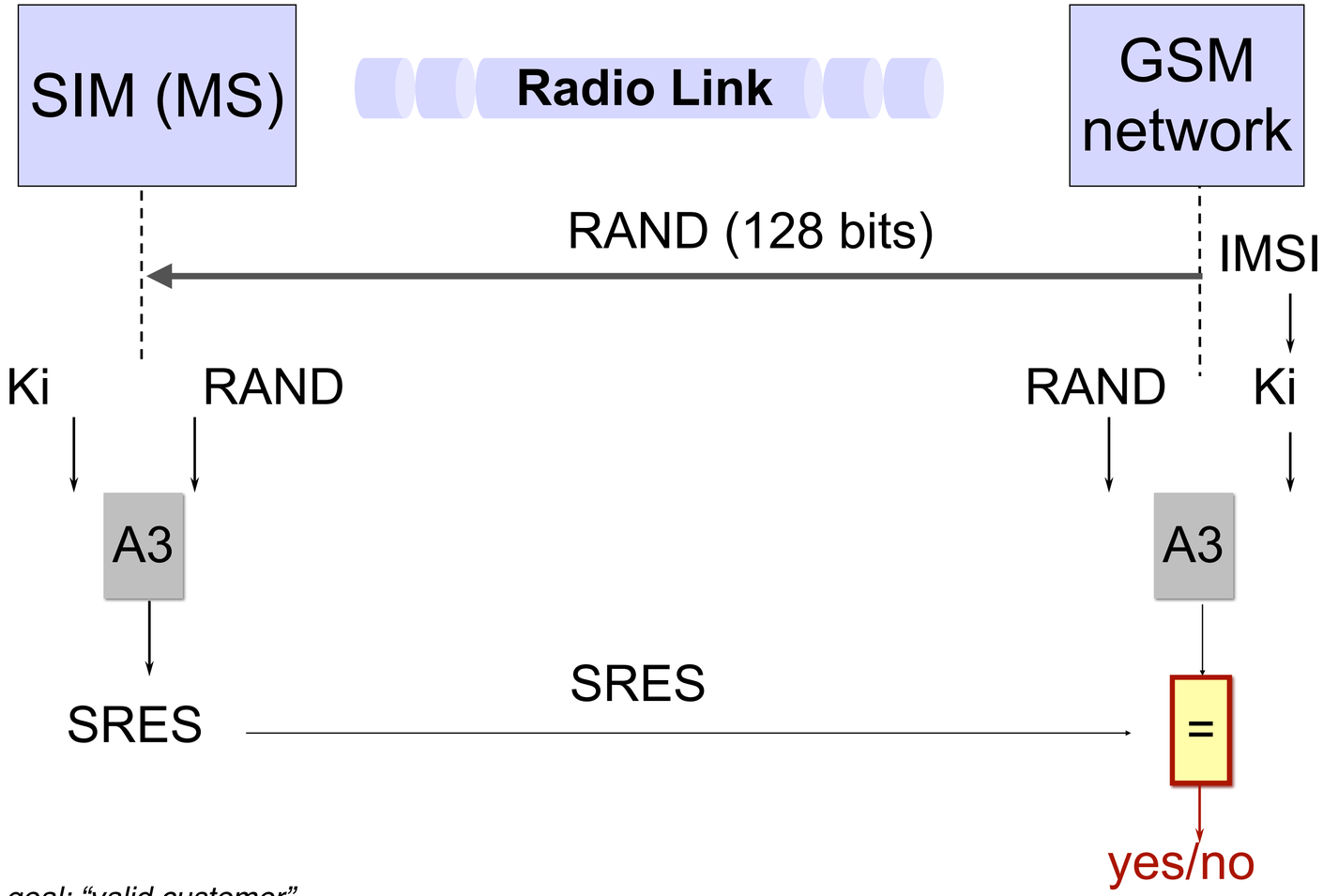
- A3 authentication algorithm
- A5 signalling data and user data encryption algorithm
- A8 ciphering key generating algorithm

- Symmetric key crypto algorithms (public key cryptography was considered at the time – 1980s – but not considered mature enough)

- *GSM/MoU: Memory of Understanding*
- *PLMN: Public Land Mobile Network*

GSM Subscriber Authentication

- Smart card (processor chip card) in MS:
  - **Ki** Secret subscriber key (128 bits)
  - Algorithms A3 and A8
  - **IMSI - International Mobile Subscriber ID**
  - **TMSI - Temporary ID**
  - Kc Current encryption key (64 bits)
- **A3 authentication** algorithm
- A5 signalling data and user data encryption algorithm
- A8 ciphering key generating algorithm



goal: "valid customer"

https://link.springer.com/content/pdf/10.1007/11872153_15.pdf

User Authentication in Mobile Equipment (ME)

- User Authentication Authentication is initiated by the fixed network, and is based upon a simple challenge-response protocol.
- When a MS attempts to access the system, the network issues it a 128-bit random challenge RAND.
- The MS computes the 32-bit signed response (SRES) based on the encryption of the random number RAND with the authentication algorithm (A3) using the individual subscriber authentication key Ki.
- The key Ki is unique to the subscriber, and is shared only by the subscriber and an authentication center, which serves the subscriber's home network.
- The value SRES computed by the MS is signaled to the network, where it is compared with a pre-computed value. If the two values of SRES agree, the mobile subscriber has been authenticated, and the call is allowed to proceed.
- The subscriber authentication key is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the HLR and VLR databases[9][10].

https://link.springer.com/content/pdf/10.1007/11872153_15.pdf

TMSI

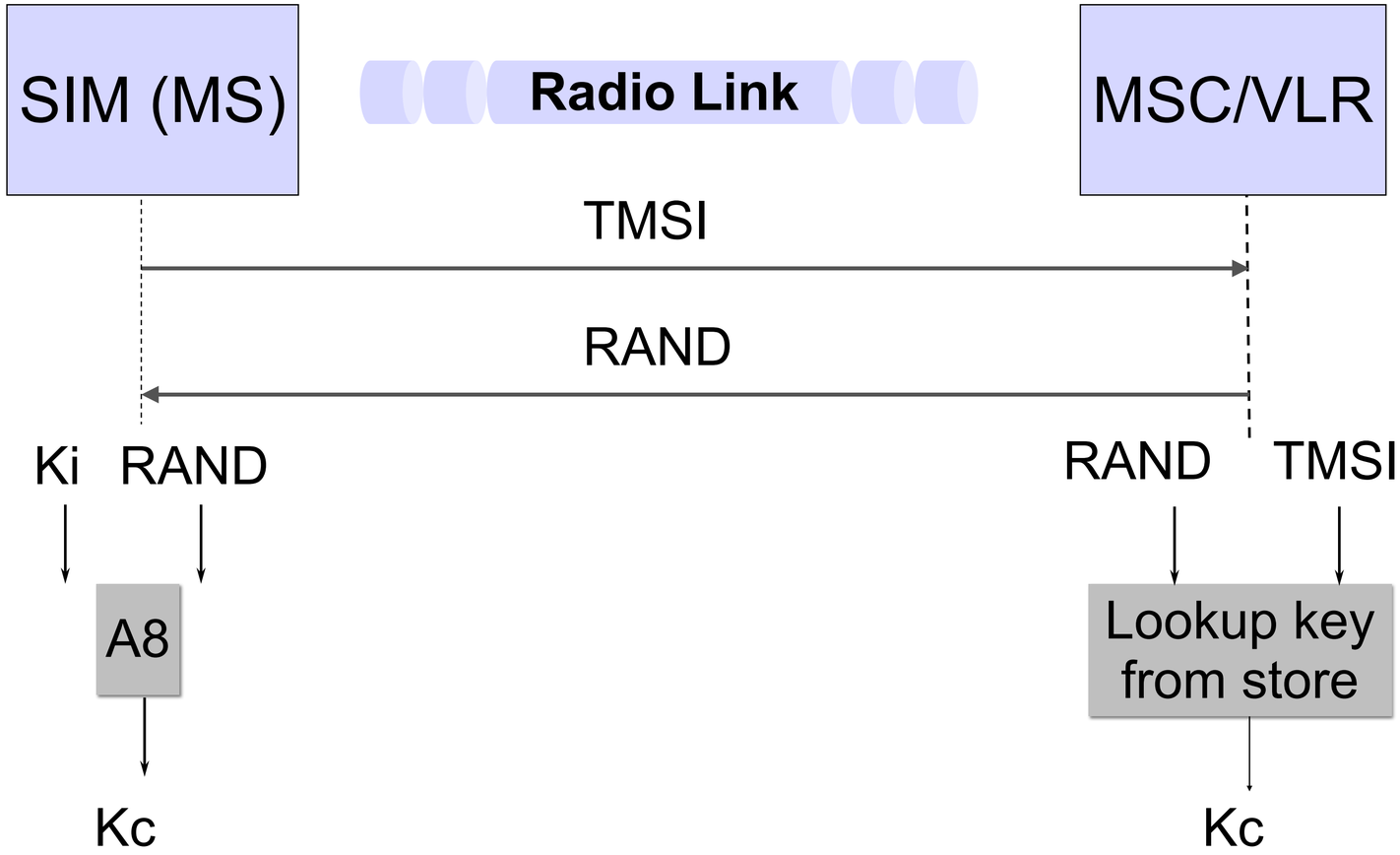
- When a MS makes initial contact with the GSM network, an unencrypted subscriber identifier (IMSI) has to be transmitted.
- The IMSI is sent only once, then a temporary mobile subscriber identity (TMSI) is assigned (encrypted) and used in the entire range of the MSC.
- When the MS moves into the range of another MSC a new TMSI is assigned.

GSM 02.09: Encryption

- Encryption normally applied to all voice and non-voice communications.
  - The infrastructure is responsible for deciding which algorithm to use (including the possibility not to use encryption, in which case confidentiality is not applied).
  - When necessary, the MS shall signal to the network indicating which of up to seven ciphering algorithms it supports. The serving network then selects one of these that it can support (based on an order of priority preset in the network), and signals this to the MS.
  - The network shall not provide service to an MS which indicates that it does not support any of the ciphering algorithm(s) required by GSM 02.07.

GSM Subscriber Authentication

- Smart card (processor chip card) in MS:
  - **Ki** Secret subscriber key (128 bits)
  - Algorithms A3 and A8
  - IMSI - International Mobile Subscriber ID
  - **TMSI - Temporary ID**
  - Kc Current encryption key (64 bits)
- A3 authentication algorithm
- A5 signalling data and user data encryption algorithm
- **A8 ciphering key** generating algorithm



Cryptographic Algorithms: A3/A8

- Algorithms A3 and A8 shared between subscriber and home network; thus each network could choose its own algorithms.
  - Algorithms A3 and A8 at each mobile operator's discretion.
  - GSM 03.20 specifies only the formats of their inputs and outputs; processing times should remain below a maximum value (A8: 500 msec).
- COMP128: one choice for A3/A8; attack to retrieve Ki from the SIM (→ cloning) possible; not used by many European providers.

GSM – Summary

- Voice traffic encrypted over the radio link (A5)
  - but calls are transmitted in the clear after the base station.
- Optional encryption of signaling data
  - but ME can be asked to switch off encryption.
- Subscriber identity separated from equipment identity.
- Some protection of location privacy (TMSI).
- Security concerns with GSM:
  - No authentication of network: IMSI catcher pretend to be BTS and request IMSI.
  - Undisclosed crypto algorithms.

Security architecture: GSM

Threats/attacks	Security services	Security mechanisms
Cloning	Authentication	Authentication mechanism (challenge-response with a shared secret)
Eavesdropping (voice sent in clear)	Confidentiality	Encryption of call content (A5/1, A5/2, A5/3)
Spying (identity tracking)	Confidentiality	Location security (TMSI)

Conclusion: GSM had a security architecture from the start

* Well defined threats and security services (at the time)
* Security mechanisms implemented poorly
  - missing public scrutiny
  - hard to replace components
  - not adaptive to future changes

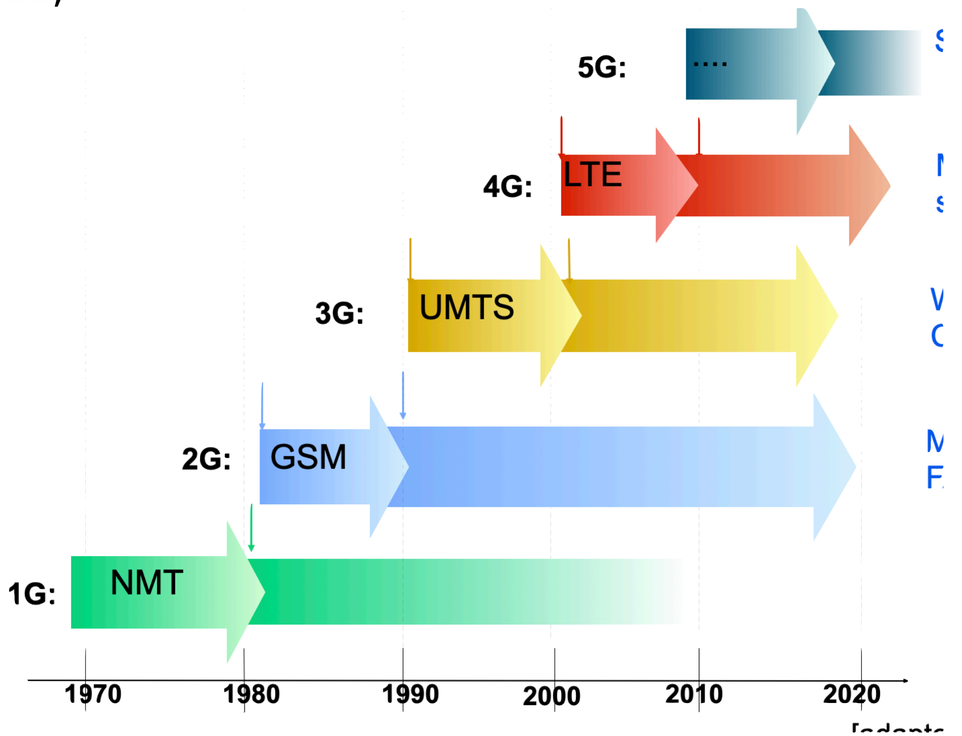
[source: Lars Strand, 2011]

UMTS – Introduction

- Universal Mobile Telephony System (UMTS) on 3G; developed from 1990s; first specs 1999.

Main tasks of the security architecture (Køien, 2004):

1) Authentication
   - GSM vulnerability: False BST
   - UMTS: Mutual authentication, new algorithm (MILENAGE)
2) Replace algorithms/New key generation
   - GSM vulnerability: Inadequate algorithm
   - UMTS: New algorithm (KASUMI)
3) Encryption/integrity protection
   - GSM vulnerability: Cipher keys and auth data sent in clear in operator network
   - UMTS: Extend confidentiality and integrity service to the operator network

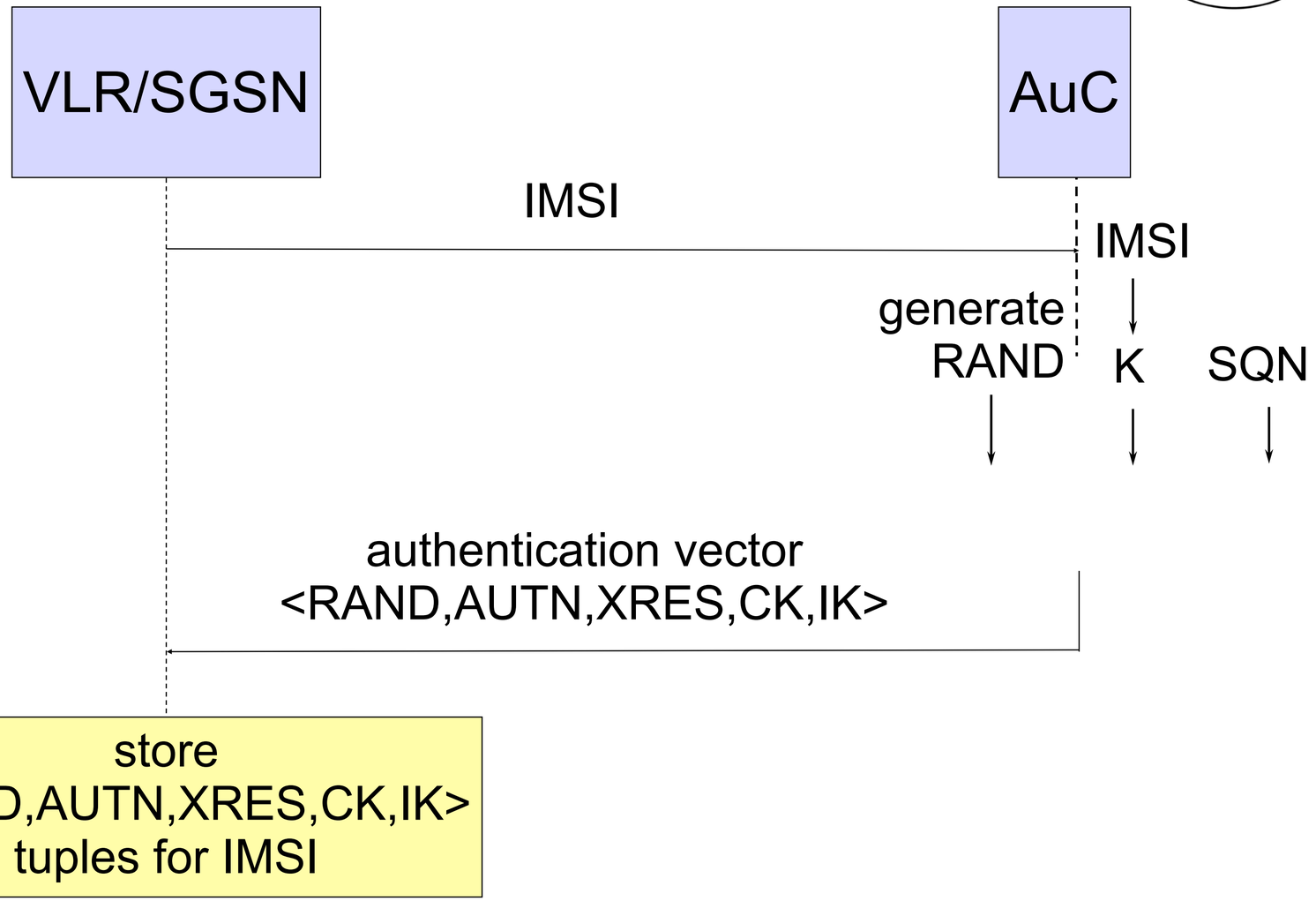


UMTS AKA
"Authentication and Key Agreement"

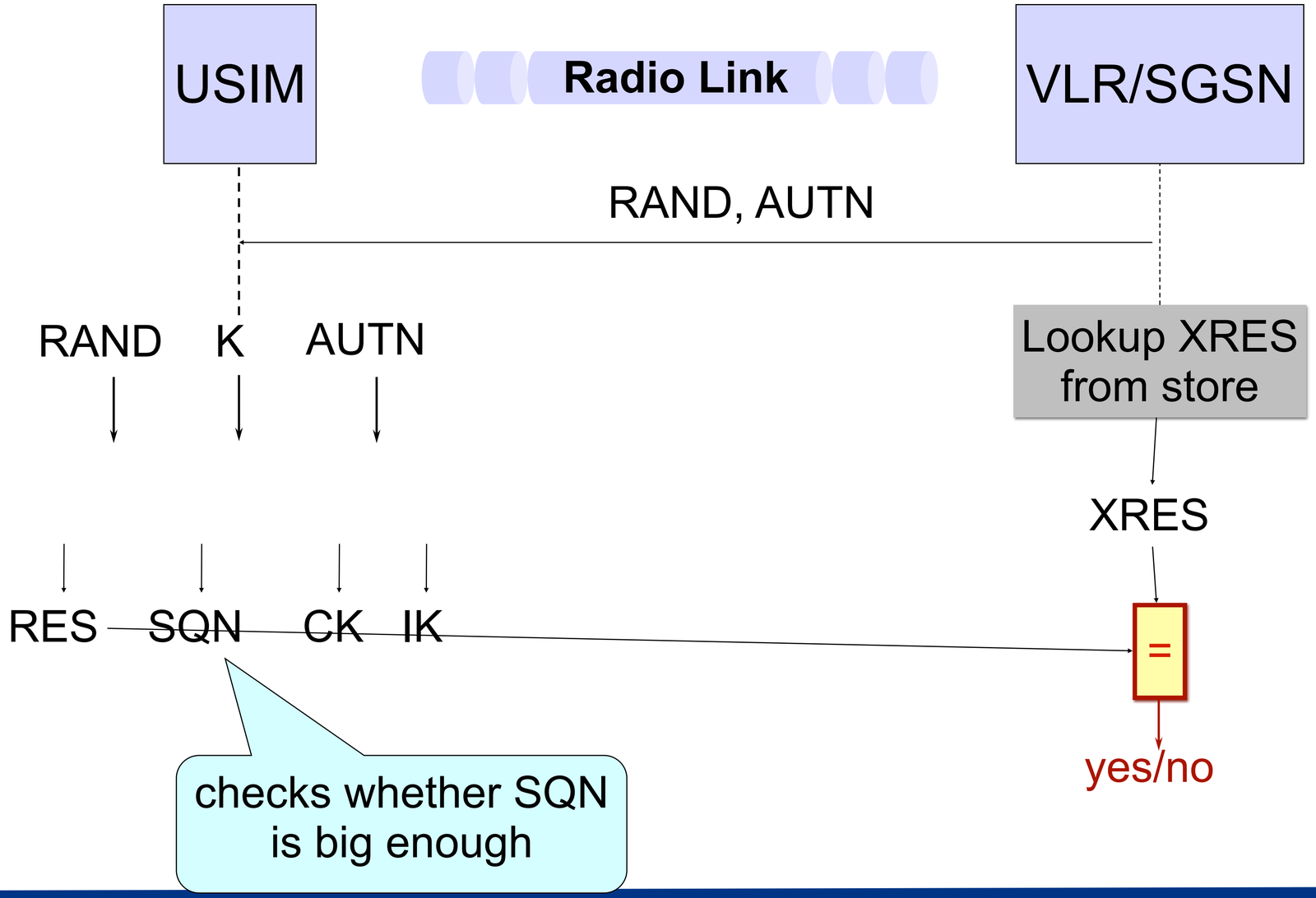
- Home network (AuC) and USIM (Universal Subscriber Identity Module) in user equipment (UE) share secret 128-bit key K.
- AuC can generate random challenges RAND.
- USIM and AuC have synchronized sequence numbers SQN available.
- Key agreement on 128-bit cipher key CK and 128-bit integrity key IK.
- AMF: Authentication Management Field.

UMTS Authentication Center (AuC) ↔ Visiting Location Register (VLR)

- Home network (AuC) and USIM (Universal Subscriber Identity Module) in user equipment (UE) share secret 128-bit key K.
- AuC can generate random challenges RAND.
- USIM and AuC have synchronized sequence numbers SQN available.
- Key agreement on 128-bit cipher key CK and 128-bit integrity key IK.
- AMF: Authentication Management Field.



UMTS Authentication (AKA): USIM ↔ VLR



UMTS AKA – Discussion

- Checks at USIM:
  - Compares MAC received as part of AUTN and XMAC computed to verify that RAND and AUTN had been generated by the home AuC.
  - Checks that SQN is fresh to detect replay attacks.
- Checks at VLR:
  - Compares RES and XRES to authenticate USIM.
- False base station attacks prevented by a combination of key freshness and integrity protection of signalling data, not by authenticating the serving network.

UMTS: Crypto Algorithms

- Confidentiality:
  - MISTY1: block cipher, designed to resist differential and linear cryptanalysis
  - KASUMI: eight round Feistel cipher, 64-bit blocks, 128-bit keys, builds on MISTY1
- Authentication and key agreement
  - MILENAGE: block cipher,128-bit blocks, 128-bit keys
- All proposals are published and have been subject to a fair degree of cryptanalysis.

Security architecture: UMTS

Threats/attacks	Security services	Security mechanisms
False BST	Authentication	Mutual authentication mechanism (challenge-response with a shared secret)
Eavesdropping (Poor GSM encryption)	Confidentiality	Encryption of signaling and call content
Data sent in clear in the operator network	Confidentiality	Encryption and integrity protection of data, to also cover operator network

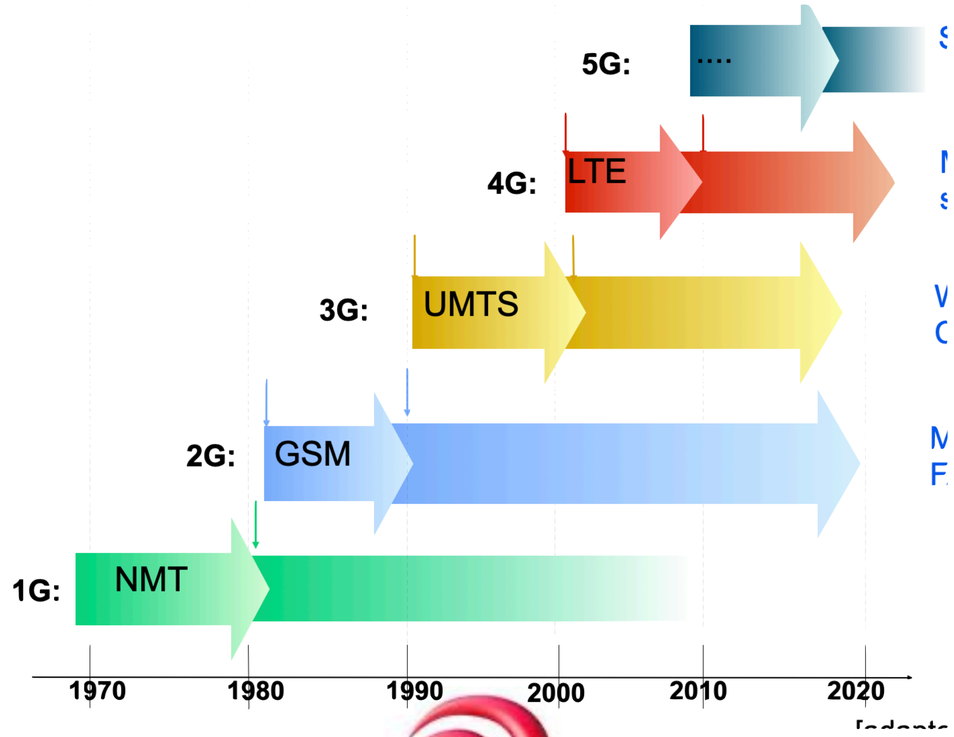
Conclusion: UMTS has a decent security architecture

* Extensive threat and attack analysis
* Open development
* Modular ("flexible") security mechanisms
  - "cryptographic core" can be replaced by operator
* Target: End-user, Operators and law enforcements

[source: Lars Strand, 2011]

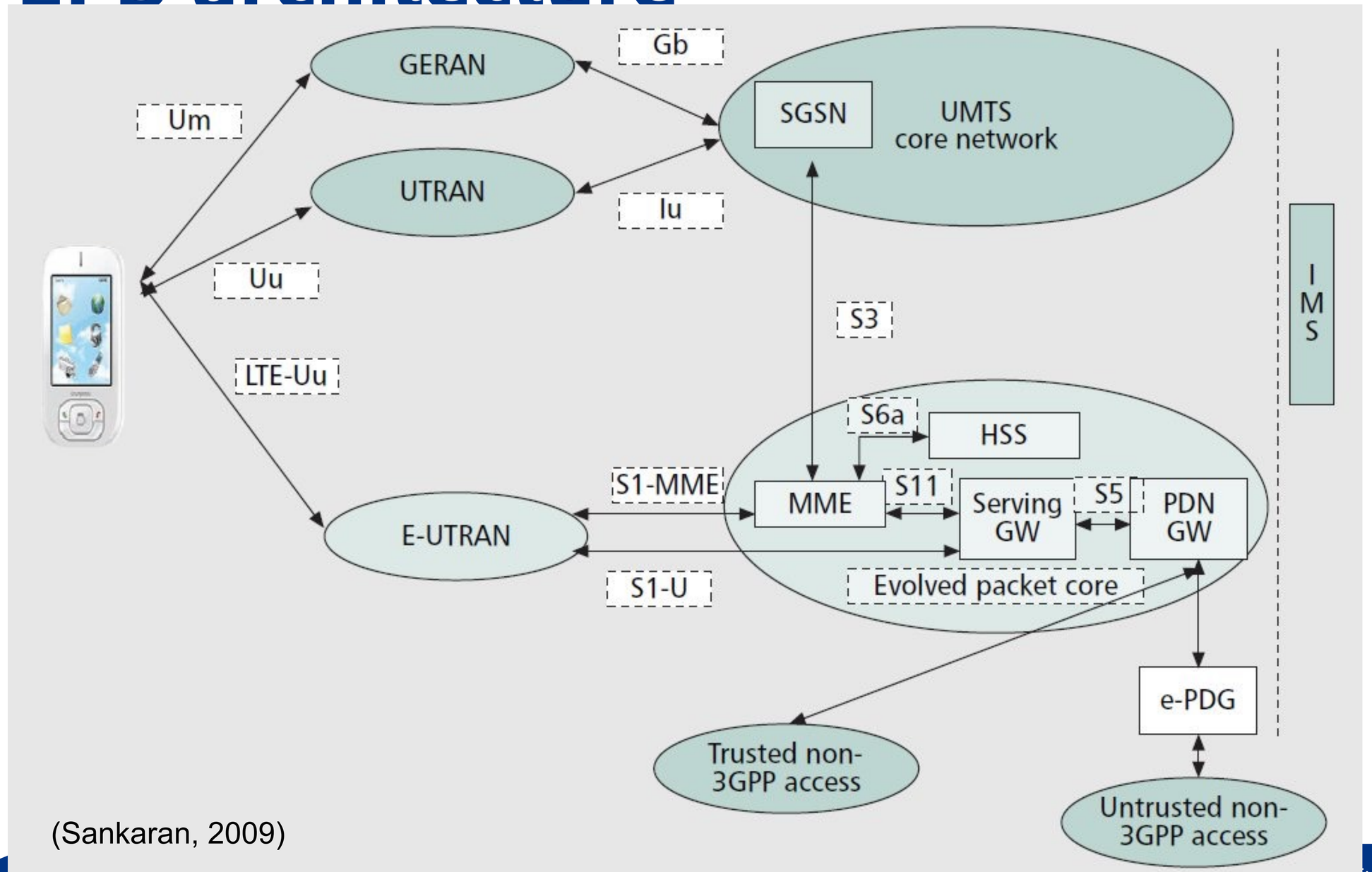
LTE Advanced (4G)

- Long Term Evolution (LTE)
- Overall architecture of Evolved Packet System (EPS) consists of:
  1) Access network
  2) Evolved Packet Core (EPC) network
     - IP Multimedia Subsystem (IMS)
- *"Improved overall security robustness over UMTS"*
- Major changes from UMTS:
  - All IP network
  - Higher bandwidth



[source: Lars Strand, 2011]

LTE: EPS architecture



(Sankaran, 2009)

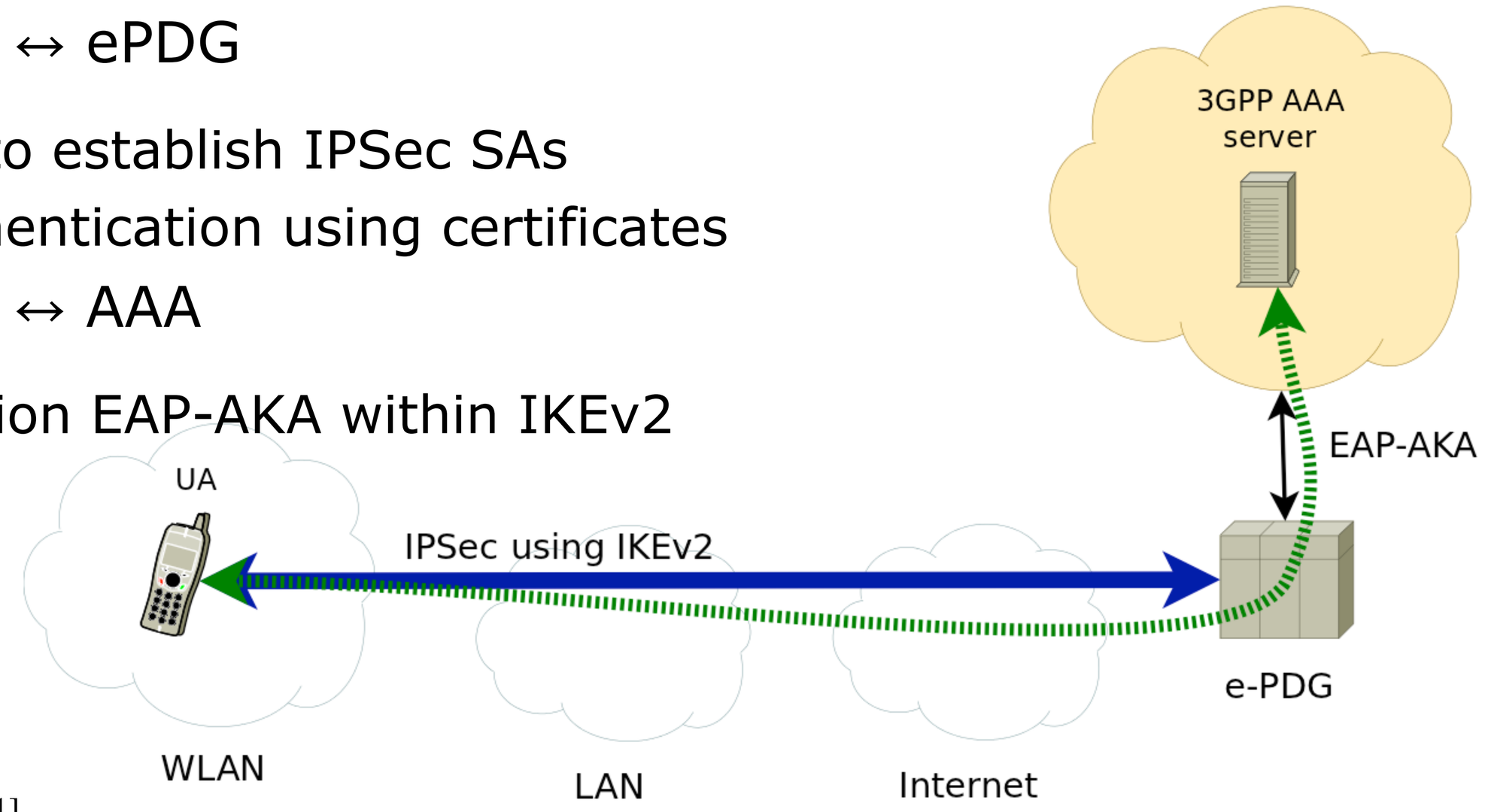
LTE: Heterogeneous networks

- Non-3GPP access network include:
  - cdm2000, WiFi (WLAN), fixed networks (Internet)
- Two classes of network access defined:
  1) Trusted access – has direct access to the operator network
     - Network operator decide which access technology is trusted
     - Can use EAP-AKA
  2) Untrusted access – everything else
     - Require IPSec with IKEv2 + EAP-AKA
     - Challenges: New threats (Internet), performance!

[source: Lars Strand, 2011]

LTE: Non-3GPP untrusted access

- Session: UA ↔ ePDG
  - Use IKEv2 to establish IPSec SAs
  - Mutual authentication using certificates
- Session: UA ↔ AAA
  - Authentication EAP-AKA within IKEv2



[source: Lars Strand, 2011]

Security architecture: LTE

Threats/attacks	Security services	Security mechanisms
Eavesdropping	Data confidentiality	IPSec
Modification of content	Data integrity	IPSec
Impersonation	Authentication	EAP-AKA
Denial of service, roaming, performance	Availability service	fast re-authentication? different access network?

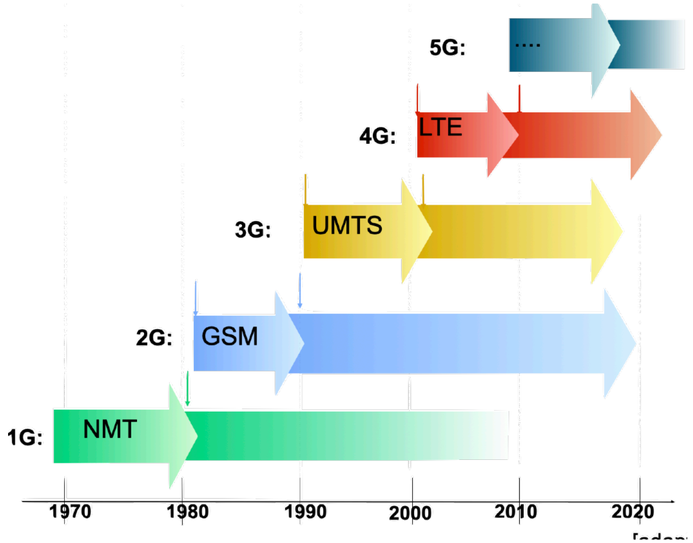
Conclusion: LTE has a decent security architecture

* Built on and improved over UMTS
* All-IP architecture a challenge
* Untrusted non-3GPP access a challenge
* Performance might be an issue

[source: Lars Strand, 2011]

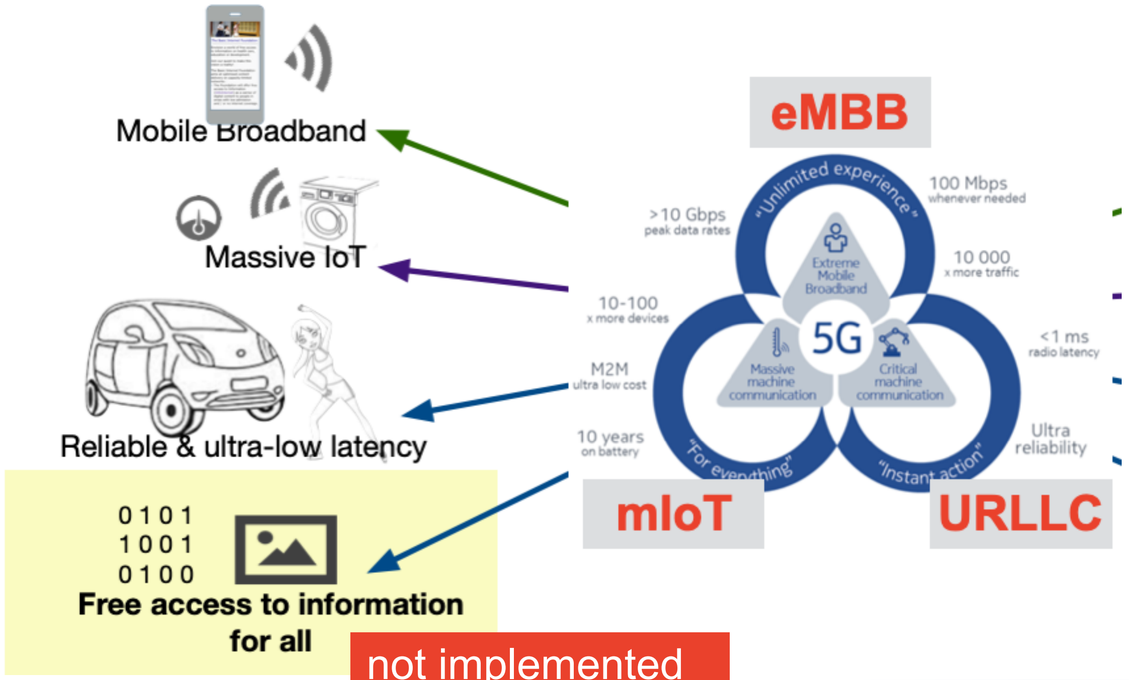
5G and Security

- enhanced mobile broadband (eMBB)
- massive IoT (mIoT)
- ultra reliable, low latency communication (URLLC)



Security aspects

- Cloud computing (virtualisation)
- Distributed Edge
- State attacks

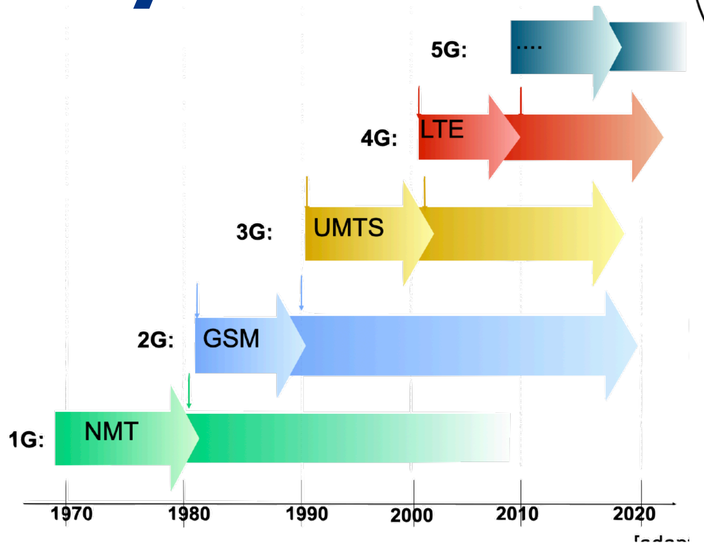


5G security aspects
“zero-trust architecture in network security”

Security-by-design mindset

- Strong access control
- encryption protocols
- up-to-date software
- network segmentation
- intrusion detection (real-time)
- incident response plan & training

Take away from L10 Mobile Security



- Key characteristics of mobile systems
  - 1G - analog - voice
  - 2G - digital - voice & SMS
  - 3G - voice & mobile data
  - 4G - mobile broadband (MBB)
  - 5G - eMBB, massive IoT, URLLC (reliable, low latency)
- Security considerations
  - 2G - IMSI catcher (mobile authenticates to network)
  - 3G - mutual authentication
  - 4G - all IP security
  - 5G - increased attack surface (cloud computing, IoT devices)