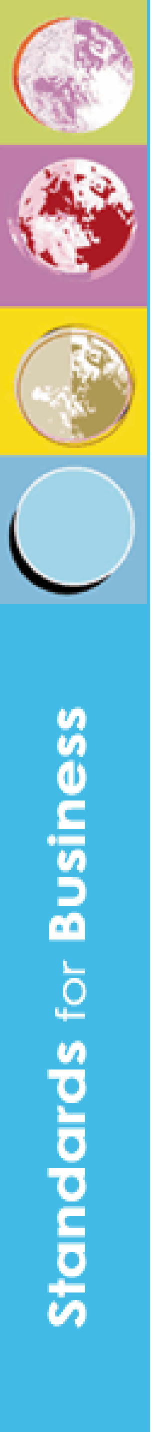
3GPP security

Valtteri Niemi
3GPP SA3 (Security) chairman
Nokia

Some history and background



Some history 1/2

- ❑ SA3 took over the responsibility of specifications created by ETSI SMG10, e.g. TS 43.020 “Security-related network functions”
- ❑ For 3GPP Release 99, WG SA3 created 19 new specifications, e.g. TS 33.102 “3G security; Security architecture”
  - ➢ 5 specifications (out of these 19) originated by ETSI SAGE, e.g. TS 35.202 “KASUMI specification”
- ❑ For 3GPP Release 4, SA3 was kept busy with GERAN security, MAP security (later to be replaced by TCAP security) and various extensions to Rel-99
  - ➢ ETSI SAGE originated again 5 new specifications, e.g. TS 35.205-208 “MILENAGE algorithm set”

Some history 2/2

- ❑ 3GPP Release 5: SA3 added 3 new specifications:
  - ➢ TS 33.203 “IMS security”
  - ➢ TS 33.210 “Network domain security: IP layer”
  - ➢ TS 33.108 “Handover interface for Lawful Interception” (created by SA3 LI subgroup)
- ❑ Release 6: SA3 added 17 new specifications, e.g.:
  - ➢ TS 33.220-222 “Generic Authentication Architecture”
  - ➢ TS 33.234 “WLAN interworking security”
  - ➢ TS 33.246 “Security of MBMS”
  - ➢ TS 33.310 “Network domain security: Authentication Framework”
  - ➢ TR 33.978 “Early IMS security”
  - ➢ TS 55.205 “GSM-MILENAGE algorithms: An example algorithm set for A3 and A8” (originated by SAGE)
  - ➢ TS 55.216-218 “A5/3 and GEA3 specifications” (originated by SAGE)

More recent history: Releases 7 and 8

- ❑ Key establishment between a UICC and a terminal (TS 33.110)
- ❑ Network Domain Security; Transaction Capabilities Application Part (TCAP) user security (TS 33.204)
- ❑ GAA extensions:
  - ➢ HTTPS connection between a UICC and a Network Application Function (NAF) (see TR 33.918)
  - ➢ SIM card based GBA (see TR 33.920)
  - ➢ GBA Push (TS 33.223)
- ❑ Specifications of UEA2 & UIA2 (incl. SNOW 3G spec) (TS 35.215-218)
- ❑ LTE/SAE security
  - ➢ Threats and Rationale for design decisions (TR 33.821)
  - ➢ Security of mobility between 3GPP and non-3GPP access networks (TR 33.922)
- ❑ Co-existence between TISPAN and 3GPP authentication schemes (TR 33.803)
- ❑ Access security review (TR 33.801)
- ❑ Trust recommendations for open platforms (TR 33.905)
- ❑ Liberty Alliance and 3GPP security interworking (TR 33.980)

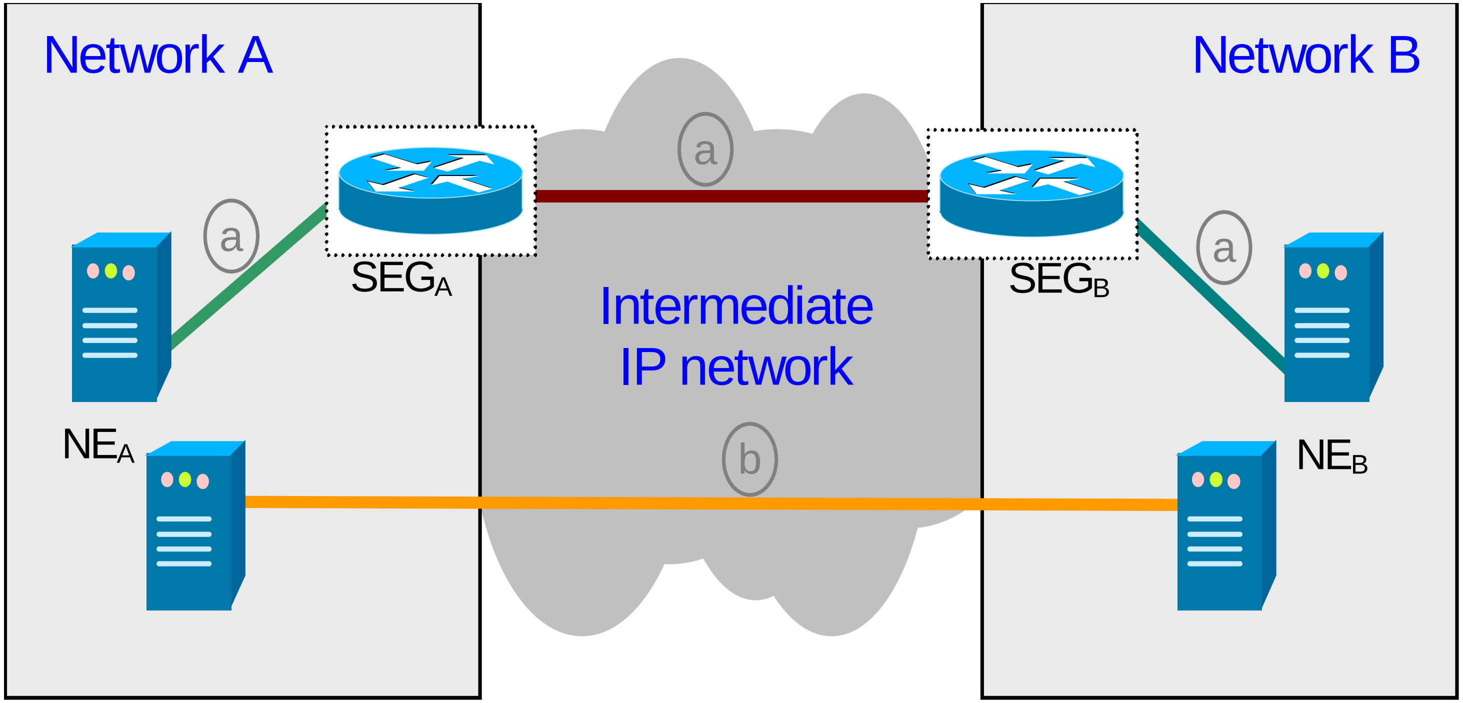
3G security background

- ❑ **Leading principles:**
  - ➢ Move useful 2G security features to 3G
  - ➢ Add countermeasures against real weaknesses in 2G
- ❑ **Main security characteristics in GSM (= 2G) :**
  - ➢ User authentication & radio interface encryption
  - ➢ SIM used as security module
  - ➢ Operates without user assistance
  - ➢ Requires minimal trust in serving network
- ❑ **Main weaknesses in GSM:**
  - ➢ Active attacks are possible (false BS etc.)
  - ➢ Authentication data (e.g. cipher keys) sent in clear inside one network and between networks
  - ➢ Cipher keys too short (in the near future)
  - ➢ Secret algorithms do not create trust

Some release 5 highlights

Security gateways for IPsec

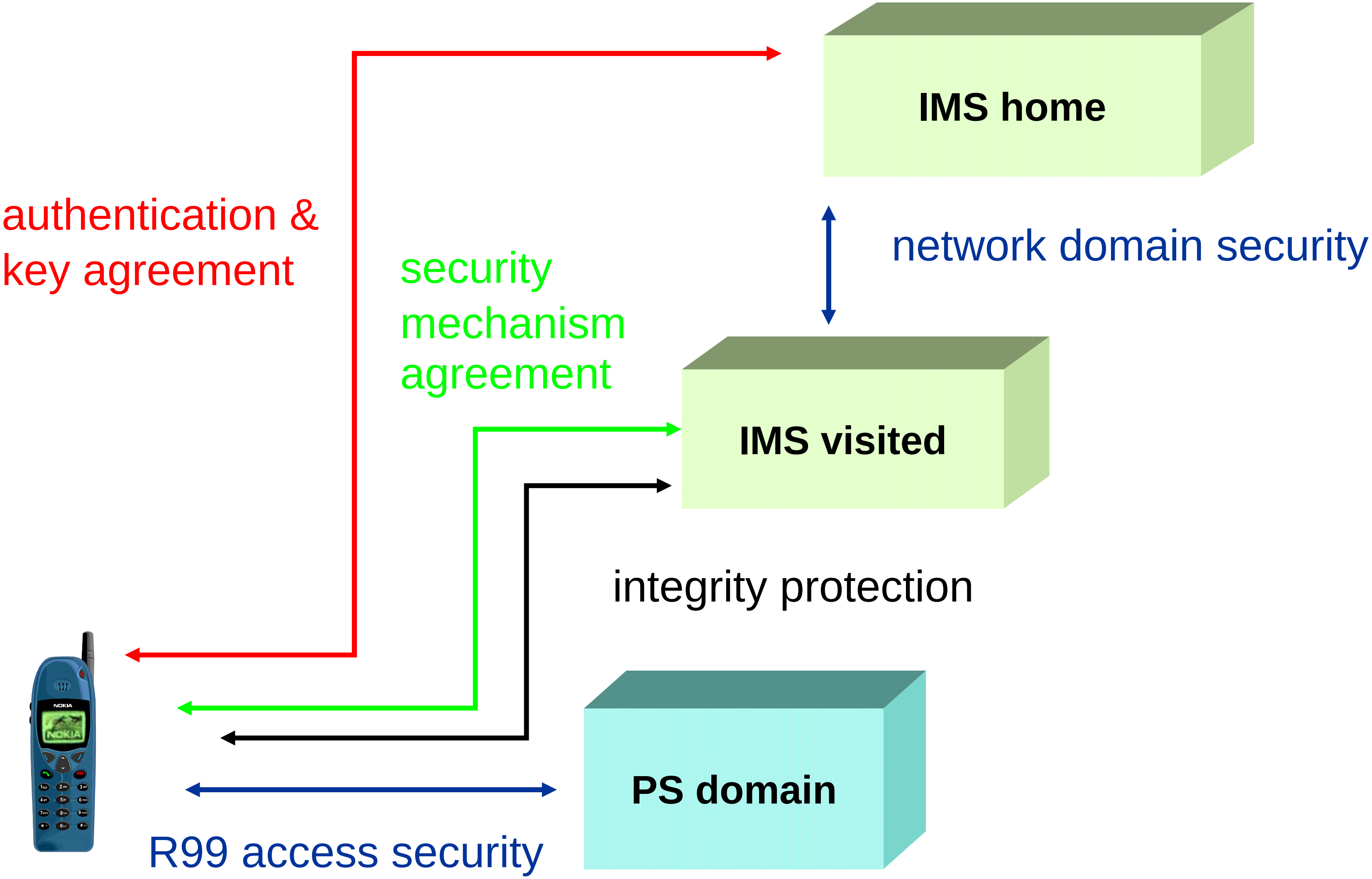
- Inter-operator signaling is done via security gateways (a)
- End-to-end security (b) can be added after key management evolves towards PKI



Challenge with phased introduction of security mechanisms

- An example case: introduction of Security Gateways in network-to-network communications
- Now: communication works well without this additional security
- Problem #1: Assume 10 % of networks have been upgraded to support security gateways → Only ~ 1 % of the total communication is protected
- Problem #2: Assume 99 % of networks have been upgraded to support security gateways
- Then ~ 98 % of total communication is protected
- But certainly an active attacker masquerades as one of the remaining 1% of networks

IMS (SIP) security



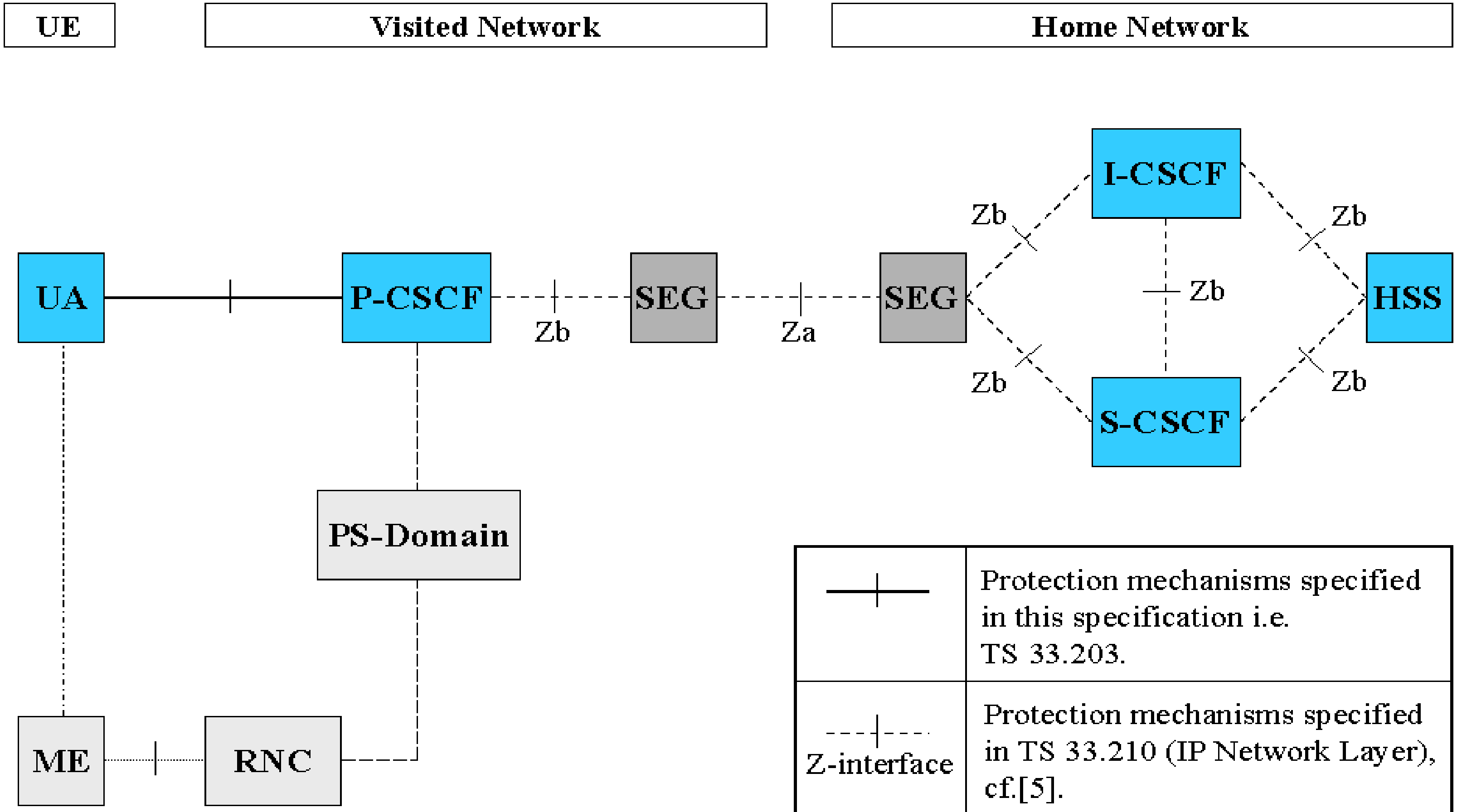
Authentication in the IMS access domain

- ❑ Strong mutual authentication needed
- ❑ Re-use of UMTS AKA protocol
  - ➢ Based on secret key cryptography
  - ➢ Typically implemented on a tamper-resistant UICC (ISIM application)
- ❑ UMTS AKA integrated into HTTP Digest
  - ➢ According to RFC3310

Message protection in the access domain

- SIP entities must be able to communicate using integrity and replay protection
  - 3GPP Rel-5 relies on bearer network confidentiality
  - 3GPP Rel-6 introduced SIP message confidentiality
  - 3GPP Rel-7 introduced NAT traversal
- Must be possible to provide protection on a per hop basis as some proxies need to read bodies

IMS security builds on network domain security



—┼—	Protection mechanisms specified in this specification i.e. TS 33.203.
--┼-- Z-interface	Protection mechanisms specified in TS 33.210 (IP Network Layer), cf.[5].
┈┼┈	Protection mechanisms specified in TS 33.102, cf. [1].

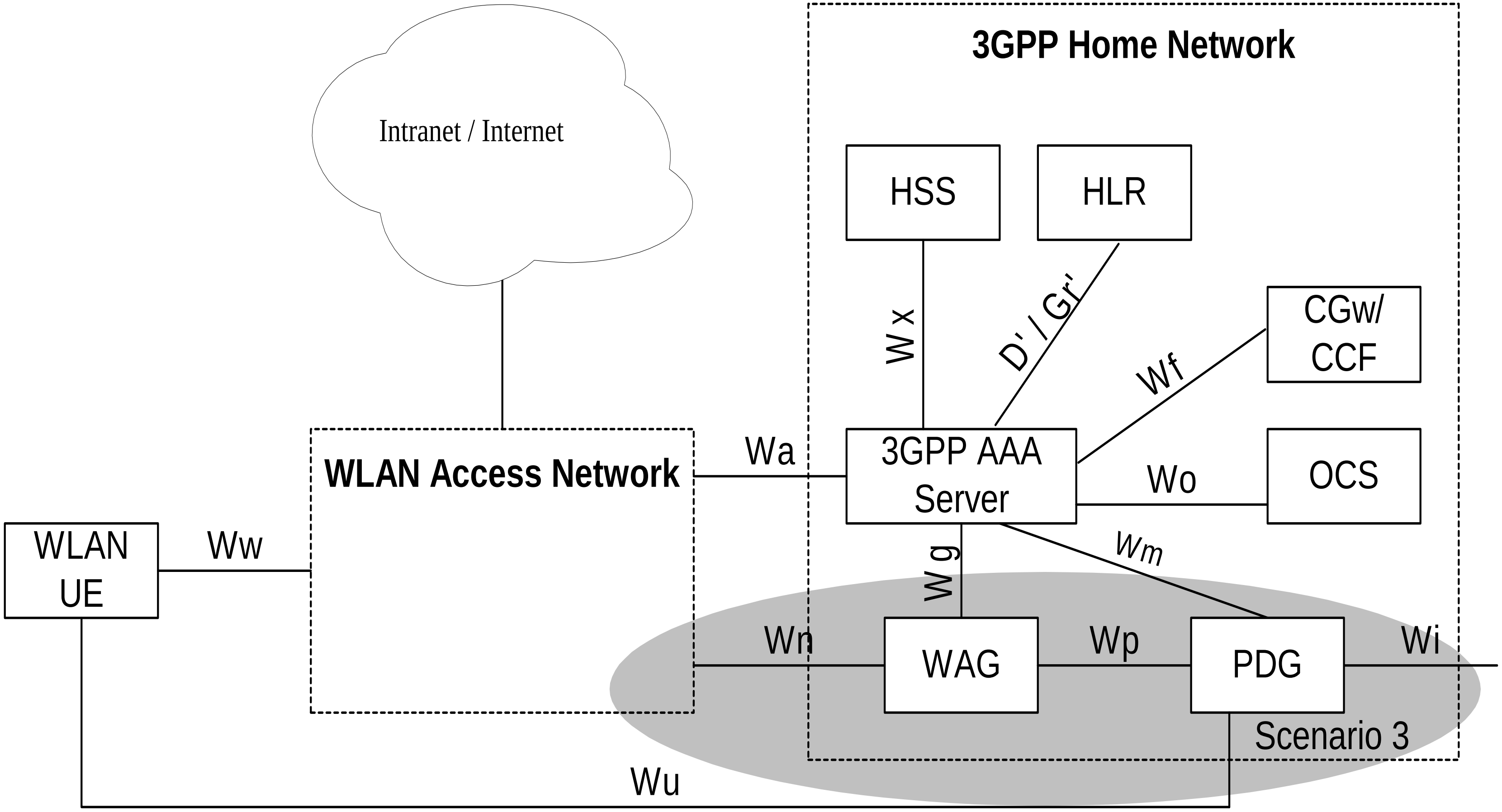
Source: 3GPP TS 33.203

Release 6 highlights

WLAN interworking in 3GPP

- ❑ WLAN access zone can be connected to cellular core network
- ❑ Shared subscriber database & charging & authentication (WLAN Direct IP access)
- ❑ Shared services (WLAN 3GPP IP Access)
- ❑ Service continuity is the next step

WLAN interworking – non-roaming case



Source: 3GPP TS 33.234

WLAN Direct IP access security

- Authentication methods
  - between WLAN-UE and 3GPP AAA server
  - based on EAP (RFC3748)
  - EAP-SIM: based on GSM AKA and network authentication (RFC4186)
  - EAP-AKA: based on UMTS AKA (RFC4187)
- Identity privacy
  - user’s identity (IMSI) encrypted within pseudonym
  - AAA server generates and delivers pseudonym to UE as part of authentication
  - UE shall not interpret pseudonym, it uses received identifier at next authentication
  - if AAA server can’t identify user by its pseudonym -> AAA server requests permanent identity

WLAN 3GPP IP access 1/2

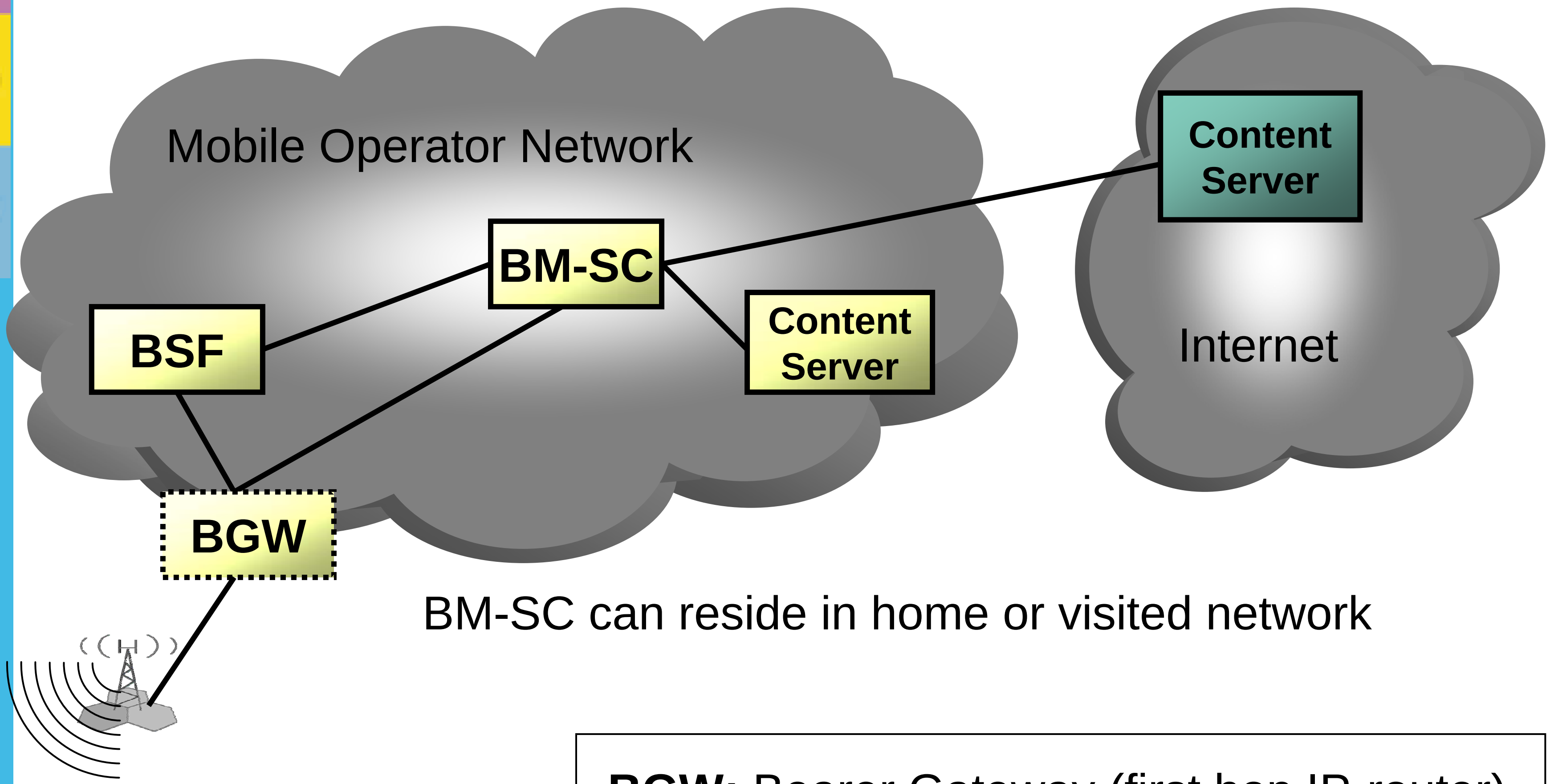
- ❑ Goal is to provide access to 3GPP system PS based services for the user through WLAN
  - ➢ IMS and corporate network
- ❑ Most of security requirements of Direct IP access are also applicable for this case
  - ➢ level of security of the 3GPP system shall not be compromised by deployment of the 3GPP-WLAN IW system
  - ➢ access control for users accessing WLAN shall have the same level of security as 3GPP system authentication procedure

Standards for Business

WLAN 3GPP IP access 2/2

- ❑ Security is provided by IPsec tunnel between UE and PDG
- ❑ WLAN-UE uses IKEv2 for tunnel establishment
- ❑ EAP messages carried over IKEv2 terminate in AAA server.
- ❑ PDG extracts EAP messages received from the WLAN-UE over IKEv2, and sends them to the AAA server over Diameter/RADIUS.

MBMS Security Architecture (node layout)



BM-SC can reside in home or visited network

BGW: Bearer Gateway (first hop IP-router)
BM-SC: Broadcast/Multicast Service Center
BSF: Bootstrapping Server Function

Summary of MBMS Security

- ❑ Service protection, not content protection in DRM-sense
- ❑ Application layer solution which is bearer agnostic
- ❑ Based on IETF and OMA protocols (cover all MBMS user services)
    - ➢ MIKEY for key delivery
    - ➢ SRTP for streaming protection
    - ➢ DCF for download protection
- ❑ GBA used for mutual authentication and distribution of shared secret
- ❑ Three level key hierarchy for data protection
- ❑ Allows two trust models for key management:
    - ➢ ME is trusted; or
    - ➢ Only UICC is trusted
- ❑ Specified in TS 33.246

Generic Authentication Architecture (GAA)

- GAA consists of three parts (Rel-6):
- *TS 33.220 Generic Bootstrapping Architecture* (GBA) offers generic authentication capability for various applications based on shared secret. Subscriber authentication in GBA is based on HTTP Digest AKA [RFC 3310].
- *TS 33.221 Support of subscriber certificates:* PKI Portal issues subscriber certificates for UEs and delivers an operator CA certificates. The issuing procedure is secured by using shared keys from GBA.
- *TS 33.222 Access to Network Application Function using HTTPS* is also based on GBA.

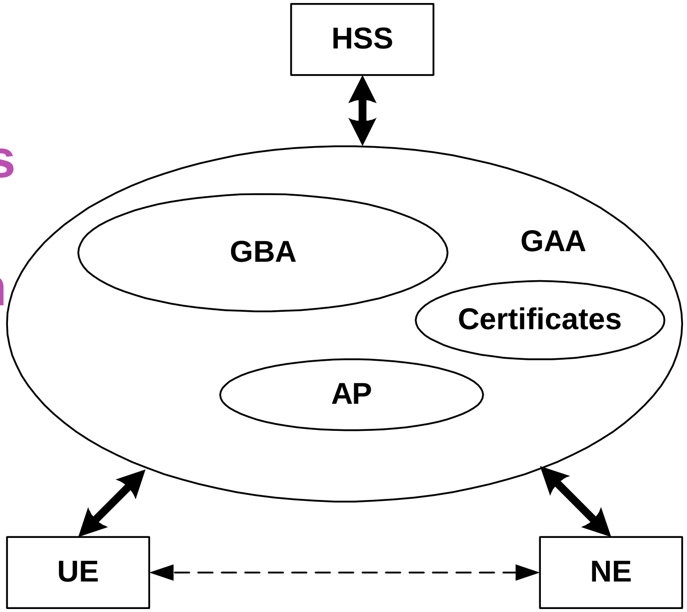
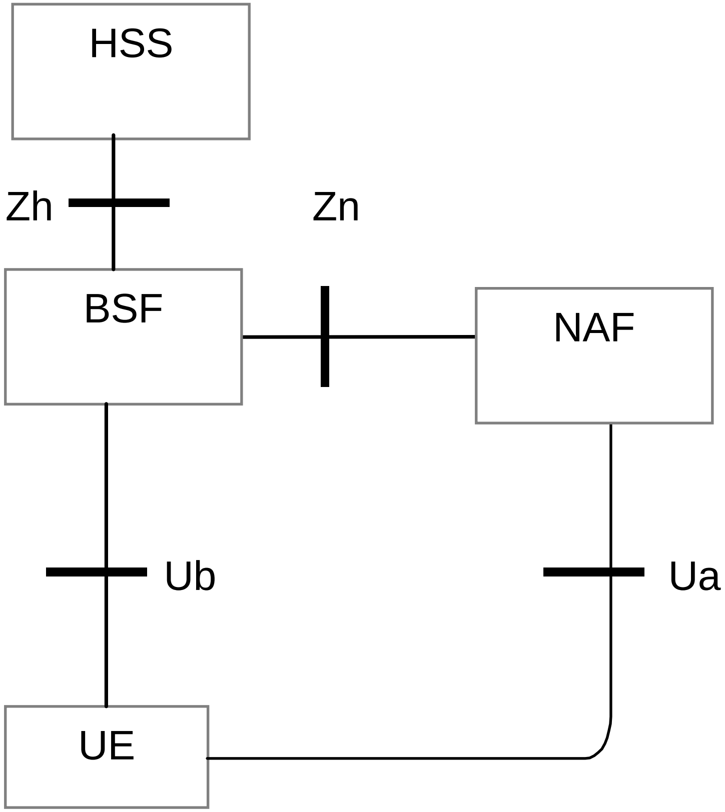


Figure from 3GPP TR 33.919

GBA: Generic Bootstrapping



- ❑ Zh and Zn are based on DIAMETER
- ❑ Ub uses HTTP Digest AKA
- ❑ Ua is application-specific

- ❑ Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and an operator-controlled Network Application Function (NAF).
- ❑ After the bootstrapping, the UE and NAF can run some application-specific protocol where the authentication / encryption of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

GBA_U

- ❑ GBA establishes session keys between the ME and the NAF
- ❑ An enhanced version called GBA_U allows session keys to be established between UICC and NAF
  - ➢ The session keys are not revealed outside the UICC
  - ➢ The application-specific NAF protocol is implemented on the UICC
  - ➢ This enhancement offers a higher level of security which is needed for certain applications like MBMS

Summary of standardized GBA use cases

	Uses
Web browsing (3GPP Rel-6)	**Digest, PSK TLS**
Subscriber certificates (3GPP Rel-6)	**Digest**
Authentication Proxy (3GPP Rel-6)	**Digest (PSK TLS)**
MBMS (3GPP Rel-6)	**Digest, MIKEY**
Aggregation Proxy (OMA XDM 1.0)	**Digest**
OMA SUPL 1.0	**PSK TLS**
Web Single Sign-On (3GPP Rel-7)	**Digest (PSK TLS)**
OMA Common Security Functions 1.0	**Digest, PSK TLS, …**
OMA BCAST Smartcard profile 1.0	**Digest, MIKEY**

Release 7 (and beyond) highlights

Rel-7: 2G-GBA

- In Release 6, GAA requires USIM
- As an *early implementation feature* it is possible to use SIM cards in Rel-7
- Adds a TLS channel between UE and BSF
- Some key requirements:
  - not to reduce security for USIM / ISIM users.
  - minimise the changes to the USIM / ISIM based GBA.
  - provide measures to mitigate known vulnerabilities of GSM.
- BSF informs NAF if subscriber uses 2G-GBA
- NAF may decide not to serve 2G subscribers

Rel-7: Support for https between UICC and NAF

- Adds the possibility to use GBA-U key KS_int_NAF for https (TLS protected http)
- Feature is useful if e.g. web server inside UICC
- *Early implementation feature* in Rel-7

SAE/LTE: some key threats

- ❑ User plane packet injection/modification/ eavesdropping
- ❑ Physical attack threat on eNodeB
- ❑ (D)DoS attacks against eNodeB from the network/UE's
- ❑ Mobility Management threats
  - ➢ Unauthorized access to the control plane data
  - ➢ Privacy (disclosure of user location)
  - ➢ Unauthorized manipulation of control plane data
  - ➢ Disturbing or misusing network service
  - ➢ Unauthorized access to network service

SAE = System Architecture Evolution

LTE = Long Term Evolution (of radio networks)

SAE/LTE: some recent discussion items

- ❑ User Plane Ciphering Termination End-Point
- ❑ Common or separate eNodeB keys
- ❑ EAP AKA versus UMTS AKA
- ❑ User plane integrity protection
- ❑ UICC required for LTE access

IMS enhancements

- Release 7: IMS security TS 33.203 expanded to support NAT traversal for fixed broadband access
- Rel-7: 3GPP TR 33.803 created to show how different authentication mechanisms may co-exist in one single IMS system (with several different access systems)
  - IMS access with UICC (3GPP)
  - “Early” IMS access with SIM (3GPP)
  - NASS-bundled authentication (TISPAN)
  - HTTP Digest as defined by TISPAN
  - Other mechanisms (e.g. from packet cable industry) may be included later
- Rel-8: Media security requirements gathered (together with TISPAN and IETF)

Other Release 7 security enhancements

- Key establishment for secure UICC-terminal channel (TS 33.110)
  - Applies, e.g. for secure UICC-terminal channel specified by ETSI SCP
  - Built on top of GBA
- Liberty-3GPP security interworking
- GBA push (TS 33.223, probably Rel-8)
  - Applies to several OMA specified features (e.g. BCAST)
- Network domain security: Authentication Framework (TS 33.310) enhanced for TLS support
- Withdrawal of A5/2 algorithm
- Key establishment between UICC hosting device and a remote device (probably Rel-8)

For more information:

www.3gpp.org