4G and 5G networks security techniques and algorithms

ITU PITA Workshop on
Mobile network planning and security

Sami TABBANE
23-25 October 2019 – Nadi, Fiji Islands
Introduction

A. 4G LTE Security

B. 5G Release 15 Security
Introduction
Security features in mobile cellular networks:

1. Access security: Authentication
2. Confidentiality: Ciphering
3. Identity protection
4. Information protection: Integrity
<table>
<thead>
<tr>
<th>Security Dimension</th>
<th>Brief Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Protects against unauthorized use of network resources. It also ensures that only authorized persons or devices access the network elements, services, stored information and information flows.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Confirms identities of communicating entities, ensures validity of their claimed identities, and provides assurance against masquerade or replay attacks.</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>Provides means for associating actions with entities or user using the network and that an action has either been committed or not by the entity.</td>
</tr>
<tr>
<td>Data Confidentiality</td>
<td>Protects data from unauthorized disclosure, ensures that the data content cannot be understood by unauthorized entities.</td>
</tr>
<tr>
<td>Communication security</td>
<td>Ensures that information flows only between the authorized end points and is not diverted or intercepted while in transit.</td>
</tr>
<tr>
<td>Data integrity</td>
<td>Ensures the correctness or accuracy of data, and its protection from unauthorized creation, modification, deletion, and replication. It also provides indications of unauthorized activities related the data.</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensures that there is no denial of authorized access to network resources, stored information or its flow, services and applications.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Provides protection of information that might be derived from the observation of network activities.</td>
</tr>
</tbody>
</table>
## ITU Recommendations

<table>
<thead>
<tr>
<th>RECOMMENDATION</th>
<th>TITLE</th>
<th>PUBLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.1087</td>
<td>A guideline to technical and operational countermeasures for <strong>telebiometric applications</strong> using mobile devices</td>
<td>2016</td>
</tr>
<tr>
<td>X.1121</td>
<td>Framework of security technologies for <strong>mobile end-to-end data communications</strong></td>
<td>2004</td>
</tr>
<tr>
<td>X.1122</td>
<td>Guideline for implementing secure mobile systems based on PKI</td>
<td>2004</td>
</tr>
<tr>
<td>X.1123</td>
<td>Differentiated security service for <strong>secure mobile end-to-end data communication</strong></td>
<td>2007</td>
</tr>
<tr>
<td>X.1124</td>
<td><strong>Authentication</strong> architecture for mobile end-to-end data communication</td>
<td>2007</td>
</tr>
<tr>
<td>X.1125</td>
<td>Correlative <strong>Reacting System</strong> in mobile data communication</td>
<td>2008</td>
</tr>
<tr>
<td>X.1126</td>
<td>Guidelines on mitigating the negative effects of <strong>infected terminals in mobile networks</strong></td>
<td>2017</td>
</tr>
<tr>
<td>X.1127</td>
<td>Functional security requirements and architecture for mobile <strong>phone anti-theft measures</strong></td>
<td>2017</td>
</tr>
<tr>
<td>X.1143</td>
<td>Security architecture for <strong>message security in mobile web services</strong></td>
<td>2007</td>
</tr>
<tr>
<td>X.1147</td>
<td>Security requirements and framework for <strong>Big Data analytics in mobile Internet services</strong></td>
<td>2018</td>
</tr>
<tr>
<td>X.1158</td>
<td><strong>Multi-factor authentication</strong> mechanisms using a mobile device</td>
<td>2014</td>
</tr>
<tr>
<td>X.1196</td>
<td>Framework for the downloadable <strong>service and content protection system</strong> in the mobile Internet Protocol Television (IPTV) environment</td>
<td>2012</td>
</tr>
<tr>
<td>X.1247</td>
<td>Technical framework for countering <strong>mobile messaging spam</strong></td>
<td>2016</td>
</tr>
<tr>
<td>X.1249</td>
<td>Technical framework for countering mobile <strong>in-application advertising spam</strong></td>
<td>2019</td>
</tr>
<tr>
<td>X.tsfp</td>
<td>Technical security framework for the <strong>protection of users' personal information while countering mobile messaging spam</strong></td>
<td>[2020]</td>
</tr>
<tr>
<td>X.Suppl.30</td>
<td>ITU-T X.805 – Security guidelines for <strong>mobile virtual network operators</strong></td>
<td>2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work item</th>
<th>Subject / Title</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.5Gsec-q</td>
<td>Security guidelines for applying quantum-safe algorithms in 5G systems</td>
<td>2020-03</td>
</tr>
<tr>
<td>X.5Gsec-t</td>
<td>Security framework based on trust relationship in 5G ecosystem</td>
<td>2021-03</td>
</tr>
<tr>
<td>X.5Gsec-ecs</td>
<td>Security Framework for 5G Edge Computing Services</td>
<td>2021-03</td>
</tr>
<tr>
<td>X.5Gsec-guide</td>
<td>Security guideline for 5G communication system based on ITU-T X.805</td>
<td>2021-09</td>
</tr>
</tbody>
</table>
A. 4G LTE Security
Main changes and additions in LTE / 3G:

- Introduction of a **hierarchical key system** in which keys can be changed for different purposes (e.g., HO),
- **Separation** of the security functions for the NAS,
- Introduction of the concept of **forward security**: limits the security issues when a disclosed key is used
Security Aspects and parameters in LTE

Main characteristics

- Re-use of UMTS Authentication and Key Agreement (AKA)
- Use of USIM required (GSM SIM excluded)
- Extended key hierarchy
- Longer keys

Security distribution
Access security
• **Access Security Management Entity (ASME)** is assumed by the MME.

• It receives the top-level keys in an access network from the HSS or HLR.

• The MME invokes the AKA procedures by requesting authentication vectors to the HE (Home environment). The HE sends an authentication response back to the MME that contains a fresh authentication vector, including a base-key named KASME
Authentication and Key Agreement Algorithm

AKA procedure

- NAS attach request (IMSI)

- NAS auth request (AUTN, RAND, KSIasme)

- NAS auth response (RES)

- NAS SMC (confidentiality and integrity algo)

- NAS Security Mode Complete

- S1AP Initial Context Setup

- RRC SMC (confidentiality and integrity algo)

- RRC Security Mode Complete

- AUTH data request (IMSI, SN_id)

- AUTH data response (AV=[AUTN, XRES, RAND, Kasme])
Authentication and Ciphering procedure

LTE: Initial Attach

- Does AUTN come from HSS?
- Have I seen it before?

1. Check $II(AES_1(K, RAND), SQN, AUTN))$
2. RES = AES_2(K, RAND)
3. $(C_k, I_k) = AES_3(K, RAND)$

RES, $C_k, I_k$

- Verify "OK"
- Switch "on" security

"OK", SELECTED_ALG, SUPPORTED_ALGS

"OK"

K_{eNB}

Protected signaling
Protected traffic

MME

HSS

ATTACH REQUEST
(IMSI, SUPPORTED_ALGS)

AUTH VECT REQUEST
(IMSI)

RAND, AUTN

$RAND = RANDOM()$
$SQN = SQN + 1$
$AUTN = AES_1(K, RAND, SQN)$
$RES = AES_2(K, RAND)$
$(C_k, I_k) = AES_3(K, RAND)$
$K_{ASME} = F(C_k, I_k, ...)$

K_{eNB}

F

KeUP-enc KeRRC-Int KeRRC-enc

K_{eNB}

KN-enc

KN-int

F

Ke
User identity privacy
User Identities

• **International Mobile Subscriber Identity** (IMSI) allocated to each mobile subscriber in every (GSM, UMTS, and EPS) system.

• VLRs, SGSNs and MMEs may allocate **Temporary Mobile Subscriber Identities** (X-TMSI) for subscriber identity confidentiality.

• An MS may be allocated three TMSIs through the:
  - VLR (TMSI)
  - SGSN (P-TMSI)
  - MME (S-TMSI, M-TMSI, part of GUTI, *Globally Unique Temporary UE Identity*).
**User Identities**

**Temporary Mobile Subscriber Identity (TMSI)** structure and coding is chosen by agreement between operator and ME manufacturer in order to meet local needs. TMSI = 4 bytes.

**Globally Unique Temporary UE Identity (GUTI):** unambiguous identification of the UE that does not reveal the UE or the user's permanent identity in the *Evolved Packet System (EPS)*. It allows the identification of the MME and network.

\[ GUTI = GUMMEI + M-TMSI, \]

where

- \( GUMMEI = MCC + MNC + MME \) Identifier
- \( MME \) Identifier = MME Group ID + MME Code
- MCC and MNC shall have the same field size as in earlier 3GPP systems.
- \( M-TMSI \) shall be of 32 bits length.
- MME Group ID shall be of 16 bits length.
- MME Code shall be of 8 bits length.
GUTI for UE identity protection

- **Temporary identity** used instead of the permanent identity IMSI.
- GUTI may be transferred from the **MME to the UE** via:
  - *Attach Accept* message as an answer to an Attach Request message,
  - *Tracking Area Update Accept* message as an answer to a Tracking Area Update Request message,
  - *Update Request* message,
  - *GUTI Re-allocation Command* message.
User data confidentiality and integrity
Security Aspects and parameters in LTE

• Security concerns:
  • UE authentication (USIM: 128 bits key);
  • Internal signaling protection (integrity), signaling and traffic encryption;
  • Signaling encryption for RRC and NAS.

• Safety is enhanced by protecting all entities
  • Hierarchical protection (UE, eNB, ASME, HSS, AuC);
  • Transport security on all interfaces.
• Encryption is performed at the eNodeB.
• MSPs (Mobile Services Provider) to support encryption within the transport network, especially if using third-party backhaul transport providers or public Internet transport.
• **IPSec tunneling** between the eNodeB and the security gateway used to secure data and provide QoS to manage the security centrally.
NAS security

- NAS messages, **UE** and **MME** scope.
- NAS message communication between UE and MME are **Integrity** protected and **Ciphered** with extra NAS security header.

AS security

- RRC and user plane data, **UE** and **eNB** scope.
- PDCP layer in UE and eNB side responsible for ciphering and integrity.
- RRC messages integrity protected and ciphered but U-Plane data is only ciphered.
Different Security algorithms (integrity/ciphering)

• **Integrity** (EIA: EPS Integrity Algorithm)
  - “0000” EIA0 Null Integrity Protection algorithm
  - “0001” 128-EIA1 SNOW 3G
  - “0010” 128-EIA2 AES

• **Ciphering** (EEA: EPS Encryption Algorithm)
  - “0000” EEA0 Null ciphering algorithm
  - “0001” 128-EEA1 SNOW 3G based algorithm
  - “0010” 128-EEA2 AES based algorithm


### Key/parameters distribution in LTE nodes

<table>
<thead>
<tr>
<th></th>
<th>UE</th>
<th>eNB</th>
<th>MME</th>
<th>HSS/Au</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre Shared keys</strong></td>
<td>UE Security Key (K)</td>
<td></td>
<td></td>
<td>UE Security Key</td>
</tr>
<tr>
<td></td>
<td>AMF</td>
<td></td>
<td>AMF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>OP</td>
<td></td>
<td>OP</td>
<td></td>
</tr>
<tr>
<td><strong>Generated keys</strong></td>
<td></td>
<td></td>
<td>SQN</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RAND</td>
<td></td>
</tr>
<tr>
<td><strong>Derived Auth vectors</strong></td>
<td>IK</td>
<td>CK</td>
<td>IK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CK</td>
<td></td>
<td>CK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ak</td>
<td></td>
<td>AK</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RES</td>
<td></td>
<td>XRES</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XMAC</td>
<td></td>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td><strong>Derived Keys</strong></td>
<td>KASME</td>
<td></td>
<td>KASME</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knas-int</td>
<td></td>
<td>Knas-int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knas-enc</td>
<td></td>
<td>Knas-enc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>KeNB</td>
<td></td>
<td>KeNB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Krrc-int</td>
<td></td>
<td>Krrc-int</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Krrc-enc</td>
<td></td>
<td>Krrc-enc</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kup-enc</td>
<td></td>
<td>Kup-enc</td>
<td></td>
</tr>
</tbody>
</table>

*AMF* (Authentication Management Field) – *SQN* (Sequence Number)
Key hierarchy

- Faster handovers and key changes, independent of AKA
- Added complexity in handling of security contexts
Security Aspects and parameters in LTE

Security aspects in LTE

- Confidentiality and integrity for signalling and confidentiality for user plane (RRC & NAS)
- Confidentiality and integrity for signalling only (NAS)
- Optional user plane protection (IPsec)
Security Aspects and parameters in LTE

LTE Ciphering and Integrity Algorithms

Ciphering

 Sender

 Plaintext Block

 Keystream Block

 Ciphertext Block

 Receiver

 Integrity

 Sender

 MAC-I/NAS-MAC

 Receiver

 XMAC-I/XNAS-MAC
Security Aspects and parameters in LTE

• Security keys for AS (Access Stratum)
  • User data and control
  • Different from those used in EPC.

• eNodeB keys:
  • $K_{\text{eNB}}$: Derived by the UE and the MME from $K_{\text{ASME}}$ (‘Master Key’) and issued by the MME in eNodeB
  • $K_{\text{eNB}}$: used to derive the AS traffic keys and handover key $K_{\text{eNB}^*}$
  • $K_{\text{eNB}^*}$: Derived from the UE and the source from eNodeB $K_{\text{eNB}}$ or valid NH (Next Hop) ⇒ During the handover, the terminal and the target eNodeB derive a new $K_{\text{eNB}^*}$ from $K_{\text{eNB}}$
Security Aspects and parameters in LTE

- $K_{\text{UPenc}}$: Derived from $K_{\text{eNB}}$ and used to **encrypt the user plane**
- $K_{\text{RRCint}}$: Derived from $K_{\text{eNB}}$ and used to ensure **the integrity of** RRC message
- $K_{\text{RRCenc}}$: Derived from $K_{\text{eNB}}$ and used to **encrypt** RRC messages
- Next Hop (NH): Intermediate key used to derive $K_{\text{eNB}}$ during **intra-LTE handover security**
- The NCC (*Next Hop Chaining Counter*) determines if the next $K_{\text{eNB}}$ must be based on a current $K_{\text{eNB}}$ or fresh NH:
  - If no fresh NH available $\Rightarrow$ target PCI (*Physical Cell Identity*) + $K_{\text{eNB}}$
  - Fresh NH $\Rightarrow$ Target PCI + NH
Security Aspects and parameters in LTE

Keys derivation scheme
Security Aspects and parameters in LTE

Different Keys Scheme
Security Aspects and parameters in LTE

1. NCC
2. Fresh NH available
   - Yes: $K_{eNB}^* = \text{Target PCI} + NH$
   - No: $K_{eNB}^* = \text{Target PCI} + K_{eNB}$

$K_{eNB}^*$ determination
Handover key chaining

NCC: Next Hop Chaining Counter

NCC = 0

NCC = 1

NCC = 2
Synthesis
Security Aspects and parameters in LTE

Security related message flow

1. **Authentication**
   - Attach Request (IMSI, UE Security Capability, K5EAA=111)
   - Authentication Request (RAND, AUTN, K5EAA=111) [not ciphered; not integrity protected]
   - Authentication Response (RES) [not ciphered; not integrity protected]
   - Authentication Data Request (IMSI, SNID, Network Type)
   - Authentication Data Response (AVs [1,...,n])

2. **NAS Security Setup**
   - NAS Security Mode Command (K5EAA=111, Replayed UE Security Capability, NAS Ciphering Algorithm=EAA1, NAS Integrity Algorithm=EAA1, NAS-MAC)
   - NAS Security Mode Complete (NAS-MAC) [NAS ciphered and integrity protected]
   - Select encryption/integrity algorithm
   - KDF
   - KDF
   - NAS Security Uplink Counter
   - Compute K5EAA

3. **AS Security Setup**
   - AS Security Mode Command (Ciphering Algorithm=EAA1, Integrity Algorithm=EAA1, MAC-1)
   - AS Security Mode Complete (MAC-1) [AS integrity protected]
   - Select encryption/integrity algorithm
   - KDF
   - KDF

4. **UE Network Capability** (24.301)
   - EPS encryption algorithm (EAA)
   - EEAO: NO encryption
   - 22E: EAA1 SDOW 3G
   - 22E: EAA2 128-bit AES
   - EEA3=EAA7 NOT Defined
   - EPS integrity algorithm (EIA)
   - 22E: EAA1 SDOW 3G
   - 22E: EAA2 128-bit AES
   - EEA3=EAA7 NOT Defined

5. **UE Security Capability** (Supported encryption/integrity algorithm)
   - EEAO=on, EEA1=on, EAA2=on, ...
   - EEAO=on, EEA1=on, EAA2=off, ...
   - EAA1=on, EEA2=on, ...

   Alg-ID
   - EEAO 00
   - EEA1 01
   - EEA2 02
   - EEA3 03
   - EAA1 01
   - EAA2 02
   - UEA1=off, EEA2=off, ...

   Alg Distinguisher
   - NAS-enc-alg 01
   - NAS-int-alg 02
   - RRC-enc-alg 03
   - RRC-int-alg 04
   - UP-enc-alg 05
B. 5G Release 15 Security
Simplified 5G reference network architecture
Security threat landscape in 5G networks

1. Illegal Intercept
2. DoS Attacks
3. Flash Traffic
4. Privacy Breach
5. Fake BS
6. Slice/Resource Theft
7. Threats Originating from Internet
8. Security Policy Conflicts
Main attacks in 5G wireless networks

- Eavesdropping
- Jamming
- DDoS
- MITM
Elements in a 5G security architecture

Authentication/authorization; Key agreement

Security negotiation;
Key hierarchy;
Enhanced control plane;
Robustness;
Enhance subscriber privacy

NFV/SDN security;
Network slicing security

Crypto algorithms;
Physical layer security;
Jamming protection

Security management and orchestration;
Security assurance for NFV environments;
Self-adaptive, intelligent security controls
<table>
<thead>
<tr>
<th>Security threats</th>
<th>Potential targets</th>
<th>Affected network segments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>HetNet Access</td>
</tr>
<tr>
<td>DoS attack on signaling plane</td>
<td>Centralized control elements</td>
<td></td>
</tr>
<tr>
<td>Hijacking attacks</td>
<td>SDN controller, hypervisor</td>
<td>✓</td>
</tr>
<tr>
<td>Signaling storms</td>
<td>5G core network elements</td>
<td></td>
</tr>
<tr>
<td>Un-authorized access</td>
<td>Low-power access points</td>
<td></td>
</tr>
<tr>
<td>Configuration attacks</td>
<td>Low-power access points</td>
<td></td>
</tr>
<tr>
<td>Saturation attacks</td>
<td>Ping-pong behavior in access points, and MME</td>
<td>✓</td>
</tr>
<tr>
<td>Penetration attacks</td>
<td>Subscriber information</td>
<td></td>
</tr>
<tr>
<td>User identity theft</td>
<td>User information data bases</td>
<td></td>
</tr>
<tr>
<td>Man-in-the middle attack</td>
<td>Un-encrypted channels, e.g. in IoT</td>
<td></td>
</tr>
<tr>
<td>TCP level attacks</td>
<td>Gateways, router and switches</td>
<td></td>
</tr>
<tr>
<td>Key exposure</td>
<td>Radio interfaces</td>
<td></td>
</tr>
<tr>
<td>Session replay attacks</td>
<td>Session keys in non-3GPP access</td>
<td></td>
</tr>
<tr>
<td>Reset and IP spoofing</td>
<td>Control channels</td>
<td></td>
</tr>
<tr>
<td>Scanning attacks</td>
<td>Radio interfaces interfaces</td>
<td></td>
</tr>
<tr>
<td>IMSI catching attacks</td>
<td>Roaming and UE</td>
<td></td>
</tr>
<tr>
<td>Jamming attacks</td>
<td>Wireless channels</td>
<td></td>
</tr>
<tr>
<td>Channel prediction attacks</td>
<td>Radio interfaces</td>
<td></td>
</tr>
<tr>
<td>Active eavesdropping</td>
<td>Control channels</td>
<td></td>
</tr>
<tr>
<td>Passive eavesdropping</td>
<td>Control channels</td>
<td></td>
</tr>
<tr>
<td>NAS signaling storms</td>
<td>Bearer activation in core network elements</td>
<td></td>
</tr>
<tr>
<td>Traffic bursts by IoT</td>
<td>Saturation of GTP end-points</td>
<td></td>
</tr>
</tbody>
</table>
5G security overview

Service based architecture security

Service Based Interface (SBI)

Network Domain Security (NDS)
Primary authentication
Secondary authentication

CP Confidentiality/Integrity
UP Confidentiality/Integrity
Synthesis
LTE Security Algorithms

More security aspects: Mobility (key separation in handovers), Home eNB, Relay Node, non-3GPP access, dual connectivity (LTE, LTE/WiFi), proximity services (incl. device-to-device communication), security assurance methods, ...
5G Security Architecture and Entities
5G security architecture (AN–Access Network, HE–Home Environment, ME–Mobile Equipment, SN–Serving Network)

- **Network access security** (I): features and mechanisms to enable a UE to authenticate and securely access network services. UEs exchange protocol messages through the access network with the serving network (SN) and leverage the PKI, where keys are stored in the USIM and the home environment (HE).

- **Network domain security** (II): features and mechanisms to enable network nodes to securely exchange.

- **User domain security** (III): features and mechanisms at the UE that secure the access to UE and mobile services. It establishes hardware security mechanisms to prevent the UEs and USIMs from being altered.

- **Service-Based Architecture (SBA) domain security** (IV): network features and mechanisms for network element registration, discovery and authorization, for protecting the service-based interfaces. It allows new 5GC functions, which may be implemented as virtual network functions, to be securely integrated. Enables secure roaming, which involves the SN as well as the home network (HN)/HE.

- **Visibility and configurability of security**: features and mechanisms to allow informing users whether a security feature is in operation. Can be used to configure security features. As the 3GPP 5G security specifications establish optional security features and degrees of freedom for implementation and operation, 5G users may encounter different security context.
5G architecture and security domains

DU: Distributed Unit of gNodeB
CU: Central Unit of gNodeB
AMF: Access Management Function
SMF: Session Management Function
UPF: User Plane Function
UDM: Unified Data Management
ARP: Authentication and Portfolio Function
Repository and Processing Function

Radio Access Network

Access Stratum Security
Network Domain Security
Non-Access Stratum Security

Core Network

Other Network(s)
5G security architecture

Authentication credential Repository and Processing Function (ARPF): keeps the authentication credentials

SEcurity Protection Proxy (SEPP) for the control plane of the internetwork interconnect

SEcurity Anchor Function (SEAF): holds the root key (known as anchor key) for the visited network
2 trust domains:

1. The tamper proof universal integrated circuit card (UICC) on which the Universal Subscriber Identity Module (USIM) resides as trust anchor

2. The Mobile Equipment (ME)

The USIM and the ME form the UE.
DU and CU in the RAN

• RAN is separated into:
  ➢ **Distributed Units** (DU): does not have any access to customer communications. May be deployed in unsupervised sites
  ➢ **Central Units** (CU): terminates the AS security. Deployed in sites with restricted access to maintenance personnel

• DU and CU form the **gNB**
Core network security

- **Access and Mobility Management Function (AMF)** serves as termination point for NAS security.

- AMF is collocated with the **SEcurity Anchor Function (SEAF)** that holds the **root key** (known as **anchor key**) for the visited network.

- The security architecture allows separation of the **security anchor** from the **mobility function** in a future evolution of the system architecture.

- The **ARPF (Authentication Credential Repository and Processing Function)** is collocated with the UDM and stores the long-term security credentials like the key **K** (EPS AKA) or **EAP-AKA** for authentication.
Identity protection
**MAJOR CHANGES IN 5G – SUBSCRIBER PRIVACY**

**Solution:**
- SUPI encrypted with home network public key on initial attach (SUCI)
- Complete authentication
- Then, send SUPI from HPLMN to VPLMN
- Finally, confirm SUPI by binding into a key

**Further details:**
- Encryption can be done on UE or USIM
- Two algorithms standardized on UE side
- Algorithms on the USIM can be controlled by operators

*Note:* In order to fight against IMSI catchers, 5G introduces the **Subscriber Permanent Identifier (SUPI)**, as replacement of the IMSI, and a PKI for the encryption of the SUPI into the **Subscriber Concealed Identifier (SUCI)**.
4G
• Initial attach with permanent identity
• Response to identity request in clear

5G improvements
• Encryption of SUPI with public key of home operator (SUCI)
• Routing information (home network ID) in clear
• SUPI revealed to VPLMN only after authentication
• Binding of SUPI into key
• UE and HPLMN have to use the same SUPI: requested for lawful intercept purposes
• Respond to identifier request with SUCI
• No SUPI based paging
Access Security
4G AKA protocol

SMC (Security Mode Command)
5G AKA protocol
5G AKA protocol

User Equipment - UE

K, IMSI, SQN_{UE}

ID_{Req} → ID_{Resp}, ID

Serving Network - SN

ID

Home Network - HN

K, IMSI, SQN_{HN}

new random R
AK ← f_5(R, K)
MAC ← f_1((SQN_{HN}, R), K)
CONC ← SQN_{HN} @ AK
AUTN ← (CONC, MAC)
CK, IK ← f_3(R, K), f_4(R, K)
xRES ← f_2(R, K)
SQN_{HN} ← SQN_{HN} + 1

If (i) and (ii)
SQN_{UE} ← SQN_{HN}
xCK, xIK ← f_3(R, K), f_4(R, K)

Auth_{Resp}, RES

if RES complies with xRES then continue

If (i) and (ii)

MAC_{Failure}

If (i) and (ii)

MAC* ← f_1^*(SQN_{UE}, R, K)
AK* ← f_2^*(R, K)
CONC* ← SQN_{UE} @ AK*
AUTS ← (CONC*, MAC*)

Sync_Failure, AUTS

Mobile Phone

Authentication for serving network

SEAF

Secure

Insecure

AUSF

Secure

ARPF

Credential Store for home network

Authentication for home network
MAJOR CHANGES IN 5G – AUTHENTICATION HOME CONTROL IN 5G AKA

Based on EPS AKA
- New authentication confirmation
- New RES* and H(X)RES*

Calculation of RES*:
- KDF(CK, IK, SN name, RAND, RES)
- Calculated in ARPF and UE

Calculation of HRES*:
- HASH(RAND, RES*)
- Calculated in SEAF and AUSF
- Used for authentication by the SEAF
Key Hierarchy

Authentication Credential Repository and Processing Function

Security Anchor Function
Authentication and registration

5GC

New AMF  Old AMF  AUSF

NAS Authentication and Security

UDM

1: Nudm_UERegistration_Get_Request
   SUCI: Subscription Concealed Identifier

2: Authentication Vector Generation

3: Nudm_UERegistration_Get_Response
   Authentication method and data

Register with the UDM and obtain the subscription data

4: Nudm_UERegistration_Management_Registration_Request
   PUT,
   Amf_3Gpp_Access_Registration = { AMF Instance Id, Supported Features, PEI, dereg Callback Uri, ...}

5: Nudm_UERegistration_Management_Registration_Response
   204 No Content
Secondary Authentication Call Flow

1. N4 Session Establishment
2. Authentication/Authorization Request
3a. Authentication/Authorization Request
3b. Namf_Communication_N1N2MessageTransfer
3c. NAS SM Transport (Authentication Message)
3d. NAS SM Transport (Authentication Message)
3e. Nsmf_PDUSession_UpdateSMContext(N1SM message)
3f. Authentication/Authorization Response
4. Authentication/Authorization Response
5. Continuation and completion of PDU Session establishment
6. Notification of IP Address allocation
Data and Signaling protection
Key distribution

![Key distribution diagram](image-url)

- Key distribution process:
  - K
  - CK
  - IK
  - KASME
  - KeNB
  - NASenc
  - NAS int
  - RRCenc
  - RRC int
  - UPenc

TCP/IP Stack:
- App
- NAS
- TCP UDP
- RRC
- IP
- PDCP
- RLC

Cellular Stack
5G key hierarchy

Key hierarchy extended:
- $K_{AUSF}$ at home network
- $K_{SEAF}$ at visited network

Reasons for $K_{AUSF}$
- Quick reauthentication
- Protecting home to UE traffic, e.g. steering of roaming under discussion

Reasons for $K_{SEAF}$
- Separate security anchor from mobility anchor
- Pre-empts AMF at insecure locations
5G key hierarchy when roaming
Integrity
Integrity protection

Split of gNB into Central and Distributed Unit (CU/DU)
  • CU performs security functions (confidentiality/integrity)
  • Can be located closer to the core

Visibility
  • Requirement to enable applications to check security being applied to the connection
Slice security
Network slice security

Network Slice Isolation
• Virtual machine isolation
• Physical network function isolation
• Virtual network function isolation

Tenant Isolation
• Identification, authentication, authorization and delegation (Tokenization technique)
• Network resources provisioning platform isolation (e.g., multi-factor authentication and tokenization)
• Tenant data isolation (many-to-one synchronization)

Virtual Network Infrastructure Visibility
• Virtual machine introspection to reduce the semantic gap
• Proactive Tenant’s Network Slice Service Chain Behaviour Detection

Network Slice Communication Confidentiality and Integrity
• Intra- and Inter-Network Slice Communications Model

Trust Model
• Stakeholder trust model and network entities trust
Conclusions
Main security enhancements with 5G

- Security anchor in the SEAF co-located with the AMF. The SEAF creates the **primary authentication** a unified anchor key $K_{SEAF}$ (common for all accesses)
- Access agnostic **primary authentication** with home control
- Protection **SUPI** (*Subscriber Permanent Identifier 5G IMSI-equivalent*) of the air with a public key encryption
- **Security key** establishment and management
- **Security for mobility**
- **Service based** architecture security
- Inter-network security, privacy and security for services provided over 5G with **secondary authentication** (for ex. between an enterprise and the UE to authenticate access to a corporate APN)
Thank You