T-ISAC EVENTS

5G SECURITY EVOLVES

Jyrki Penttinen

GSMA North America Technology Team

Thursday 27 May 2021 | 15:00 – 16:00 CEST

Online Webinar

Jyrki Penttinen
Senior Technology Manager, GSMA

Assists operator members with the adoption, design, development, and deployment of GSMA specifications and programmes ensuring interoperability and standardisation is met

Author of telecom books such as *5G Explained* and *Wireless Communications Security*

in linkedin.com/in/jypen

✉ jpenttinen@gsma.com

@jyrki_penttinen

Blog amazon.com/author/jype

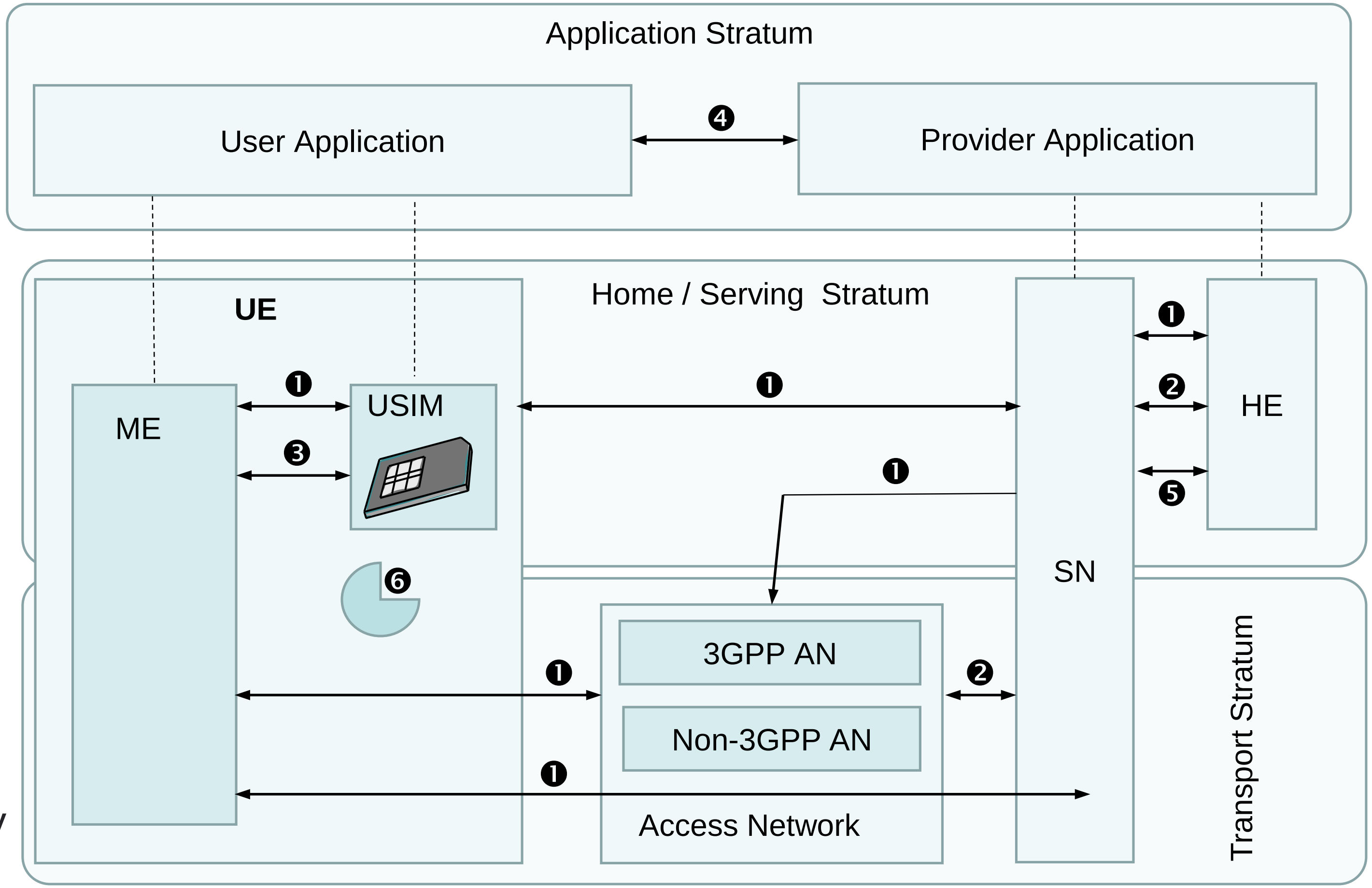
5G SECURITY EVOLVES

Contents

1. 5G security architecture
2. Functions of the 3GPP Release 15
3. Additional aspects of the Release 16
4. What the specifications mean in a practical environment including financial verticals

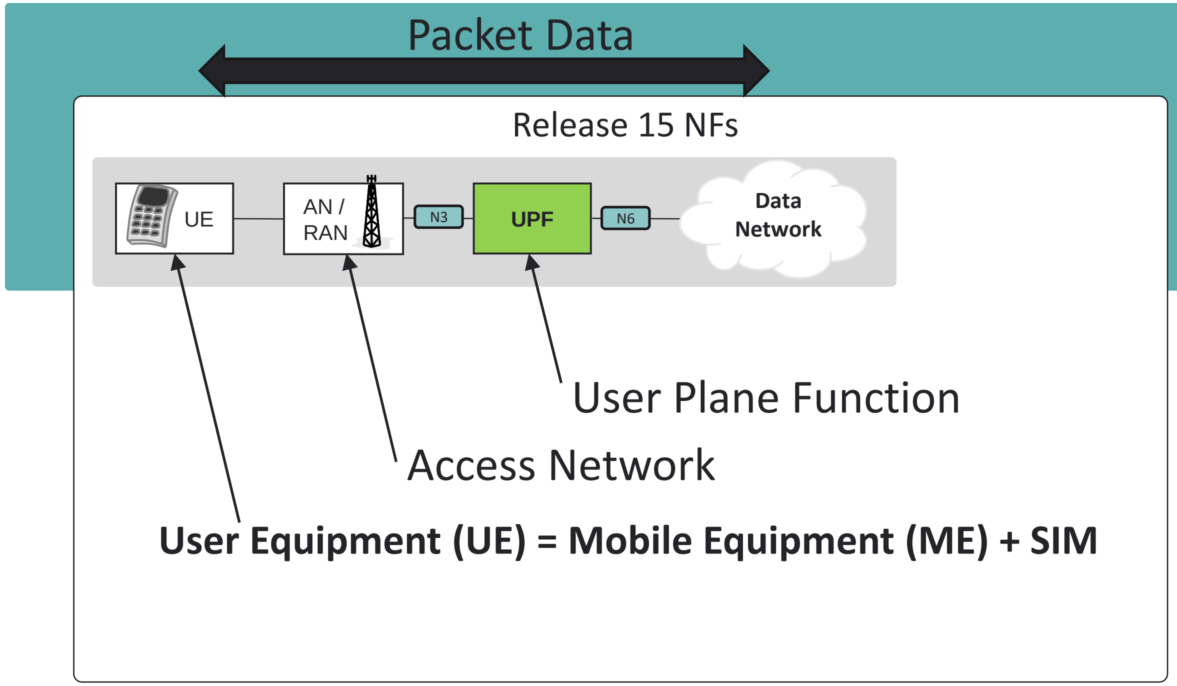
5G security architecture

1. **Network access security** (UE authentication and service access)
2. **Network domain security** (network nodes exchange data and signaling)
3. **User domain security** (user's ME access)
4. **Application domain security** (message exchange of user / provider application)
5. **Service-Based Architecture** (SBA) domain security (communication within the serving and other network domains)
6. **Visibility and configurability** of security features (information for the user)



Interpreted from: 3GPP TS 33.501, Release 16

Network Functions of the 3GPP Release 15 and 16



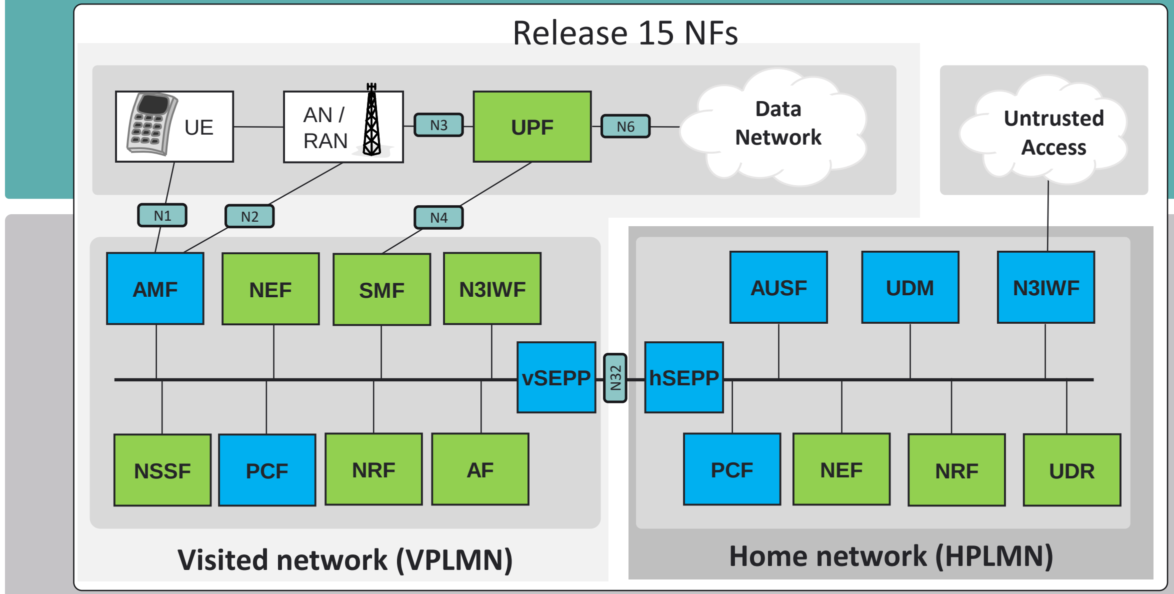
User Plane Function

Access Network

User Equipment (UE) = Mobile Equipment (ME) + SIM

User Plane for data connection

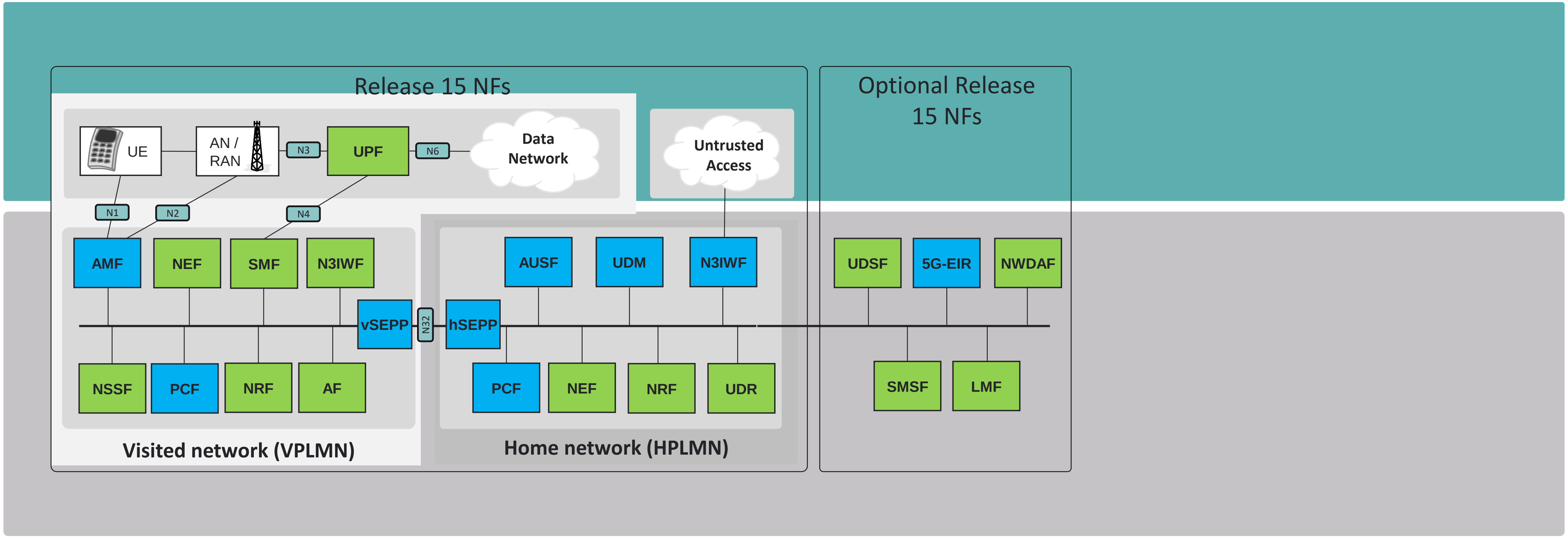
Network Functions of the 3GPP Release 15 and 16



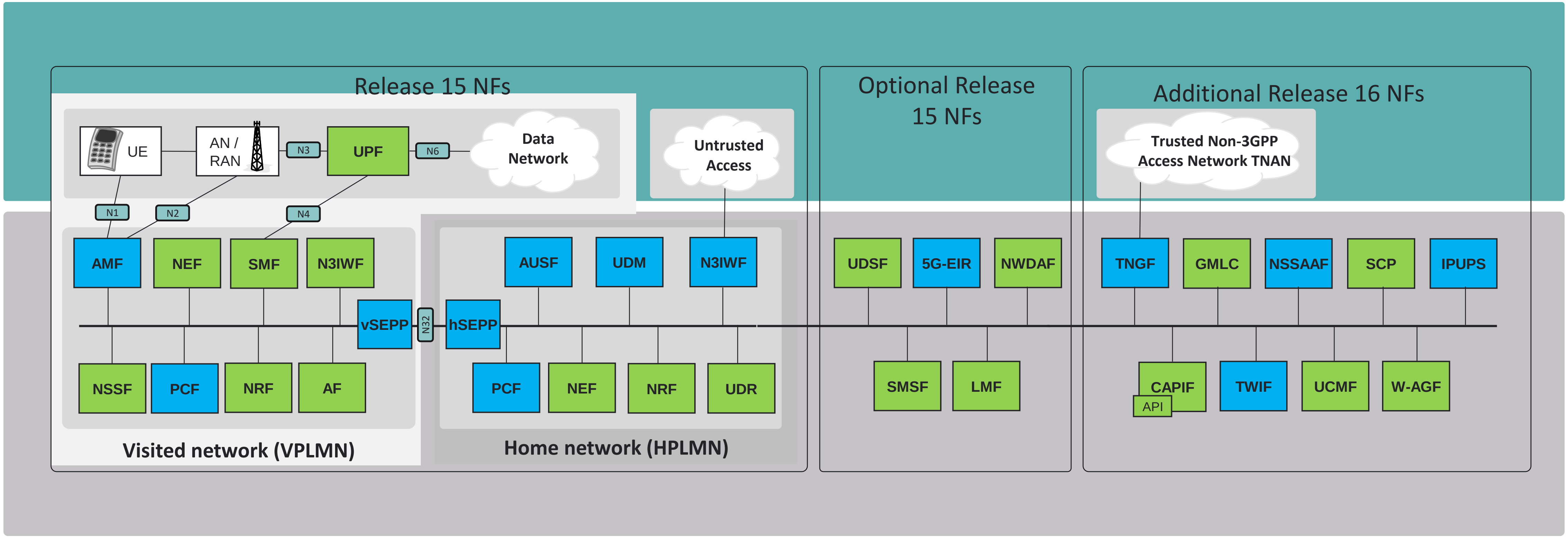
User Plane for data connection

Control Plane for signaling

Network Functions of the 3GPP Release 15 and 16



Network Functions of the 3GPP Release 15 and 16



Release 15 Network Functions

5G-EIR 5G Equipment Identity Register checks the listing status of the Permanent Equipment Identity (PEI).

AF Application Function provides services such as application influence on traffic routing, access to the Network Exposure Function (NEF), and interaction with the policy framework.

AMF 5G Access and Mobility Management Function handles signaling, access authentication and authorization.

AUSF 5G Authentication Server Function supports authentication for the 3GPP access and untrusted non-3GPP access.

LMF Location Management Function determinates the UE location.

N3IWF Non-3GPP Interworking Function handles untrusted access (Wi-Fi).

NEF 5G Network Exposure Function assists in storing and retrieving exposed capabilities and events of the Network Functions (NF).

NRF 5G Network Function Repository Function supports service discovery function.

NSSF 5G Network Slice Selection Function selects set of Network Slice instances.

NWDAF Network Data Analytics Function provides slice-specific network data analytics to the Network Functions which are subscribed to it.

PCF 5G Policy Control Function offers policy rules.

SEPP 5G Security Edge Protection Proxy interconnects 5G networks.

SMF 5G Session Management Function handles session establishment, modification, and release.

SMSF Short Message Service Function supports the Short Message Service (SMS) over a 5G Non-Access Stratum (NAS).

UDM Unified Data Management generates 3GPP AKA (Authentication and Key Agreement) credentials for users, performs user identification including storage and management of the Subscription Permanent Identifier (SUPI) and de-concealing of the Subscription Concealed Identifier (SUCI).

UDR 5G Unified Data Repository stores and retrieves subscription, policy, structured, and application data; “Master Database”.

UDSF 5G Unstructured Data Storage Function stores and retrieves information in a form of unstructured, dynamic state data by NFs

UPF 5G User Plane Function takes care of the user data ad is anchor point for intra- and inter-RAT (Radio Access Technology) mobility. It also is the external PDU session point to interconnect Data Network (DN) and it takes care of packet routing and forwarding.

Release 16 Network Functions

CAPIF Common API Framework for 3GPP northbound APIs provides exposure of the NEF for external entities. It facilitates standardized integration of services with diverse service providers for interaction at the application layer.

CHF Charging Function is specified in 3GPP TS 32.255. It considers various configurations and functionalities the SMF supports.

GMLC The Gateway Mobile Location Centre extends the functionality of the LMF defined in the Release 15, adding also roaming cases.

I-SMF Intermediate SMF. During mobility events such as Hand-Over or AMF change, if the service area of the SMF does not include the new UE location, then the AMF selects and inserts an I-SMF which can serve the UE location and the S-NSSAI.

I-UPF Intermediate UPF supports redundant transmission on N3/N9 interfaces.

NSSAAF Network Slice Specific Authentication and Authorization Function.

SCP Service Communication Proxy is a decentralized solution and composed of control plane and data plane. It provides routing control, resiliency, and observability to the core.

TNGF Trusted Non-3GPP Gateway Function connects trusted non-3GPP access networks to the 5G Core Network. This extends the Release 15 Non-3GPP Interworking Function (N3IWF) which connects the untrusted non-3GPP access network to the 5G Core Network.

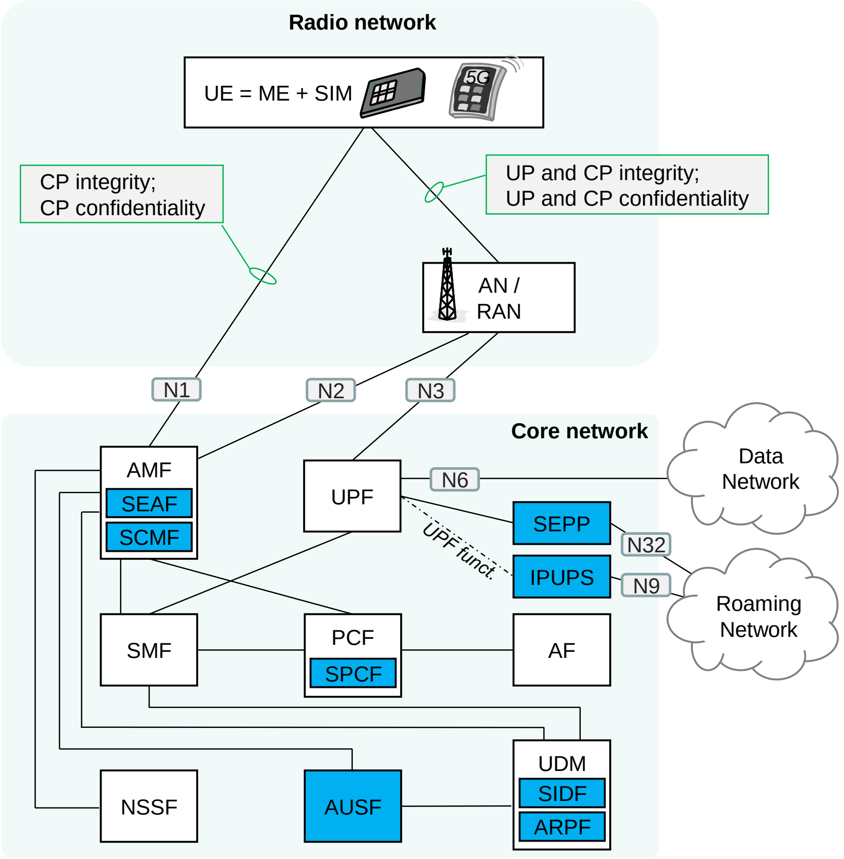
TWIF Trusted WLAN Interworking Function enables “Non-5G-Capable over WLAN” (N5CW) devices to access 5GC via trusted WLAN access networks.

UCMF UE radio Capability Management Function serves for storing dictionary entries related to PLMN-assigned or Manufacturer-assigned UE Radio Capability IDs.

W-AGF Wireline Access Gateway Function is a Network Function in W-5GAN that provides connectivity to the 5G Core, 5G-RG (5G-Residential Gateway), and FN-RG (Fixed Network Gateway).

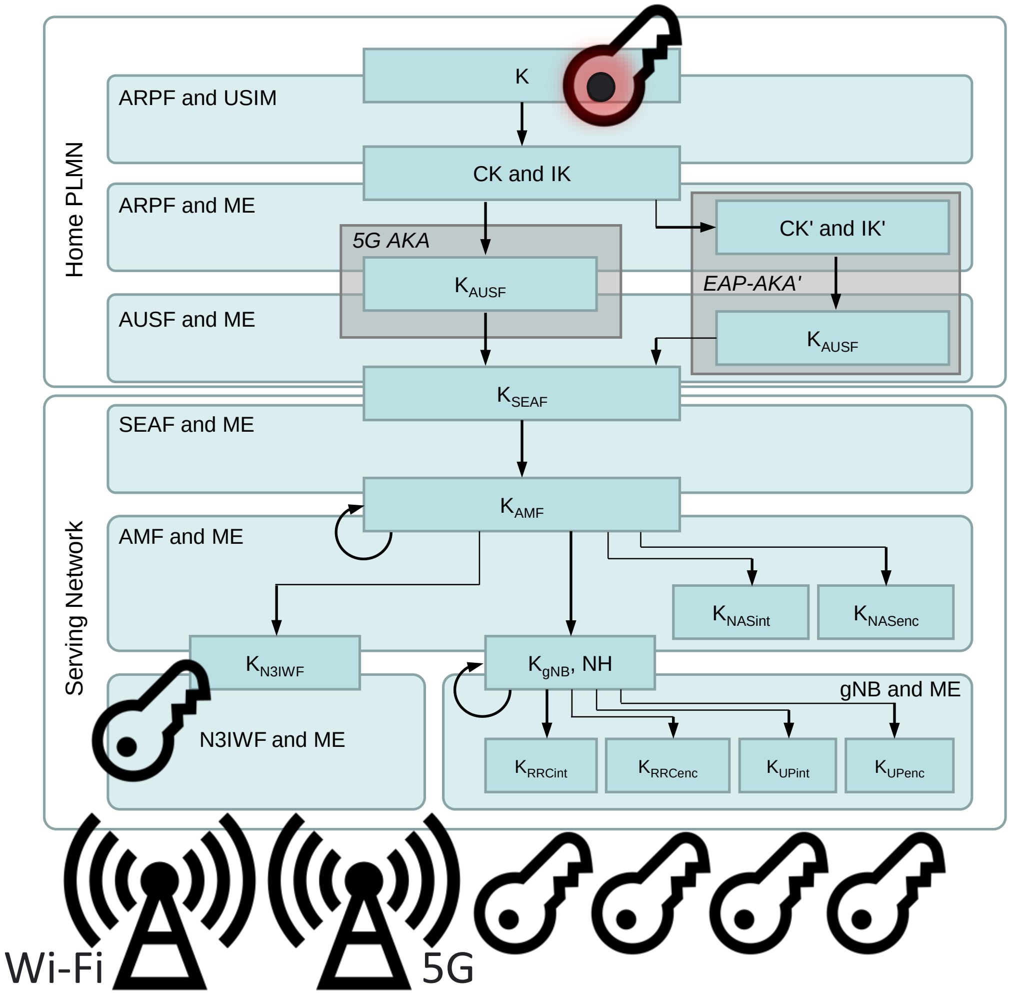
Security-related 5G Network Functions

- **AUSF**: The *Authentication Server Function* terminates requests from the SEAF and interacts with the ARPF.
- **ARPF**: The *Authentication Credential Repository and Processing Function* stores *K,* executes cryptographic algorithms, and it creates authentication vectors.
- **IPUPS**: The *Inter-PLMN UP Security* is Release 16 function located at the perimeter of the PLMN for protecting user plane messages.
- **SCMF**: The *Security Context Management Function* retrieves the key from the SEAF, which is used to derive further keys.
- **SIDF**: The *Subscription Identifier De-Concealing Function* de-conceals the SUPI (Subscription Permanent Identifier) from the SUCI (Subscriber Concealed Identifier).
- **SEAF**: The *Security Anchor Function* forms, as an outcome of the primary authentication, the unified, common anchor key K_{SEAF} for all the access scenarios.
- **SEPP**: The *Security Edge Protection Proxy* protects control plane messages at the perimeter of the PLMN, and it enforces inter-PLMN security.
- **SPCF**: The *Security Policy Control Function* provides policies related to the security of network functions such as AMF, SMF and UE.



Key derivation

- ARPF and USIM house the permanent secrets (K) that are the base for the short term keys
- Mobile Equipment takes care of the rest of the key derivation procedures with multiple 5G network functions
  - 5G network keys via 5G AKA, and other keys (for Wi-Fi access) via EAP-AKA’
  - The intermediate keys are stored in AUSF (K_{AUSF}), SEAF (K_{SEAF}), AMF (K_{AMF}), and finally in access elements (Non-3GPP Interworking Function for Wi-Fi access and gNB for 5G access)
  - The already utilized mutual authentication has been extended to cover also roaming scenarios, that is, the system recognizes if the roaming network has active connection with the home network’s customer, preventing spoofed base stations.
- The 5G keys protect both signaling and data in terms of encryption and integrity



The elemental security enhancements

- **Primary authentication** and key agreement in 5G establish mutual authentication between the UE and the serving network providing keying material such as an anchor key K_{SEAF}. The home network's AUSF provides it to the SEAF of the serving network.

- **Initiation of authentication** and selection of authentication method refers to the ability of the SEAF to perform authentication with the UE during any signaling procedure. The registration request of the UE is based on SUCI (subscription concealed identifier) or 5G-GUTI (globally unique temporary UE identity).

- **Authentication procedures** involve intermediate key K_{AUSF} and resulting anchor key K_{SEAF}. The AUSF can securely store the K_{AUSF}.

- **5G enhances authentication** and key agreement protocols fortifying security compared to 4G EPS AKA.

- 5G core network functions support **mutually authenticated TLS** (Transport Layer Security) **and HTTPS** (HyperText Transport Protocol Secure). This takes place by client-server certificates protecting control plane signaling.

Security Aspects of Network Slicing

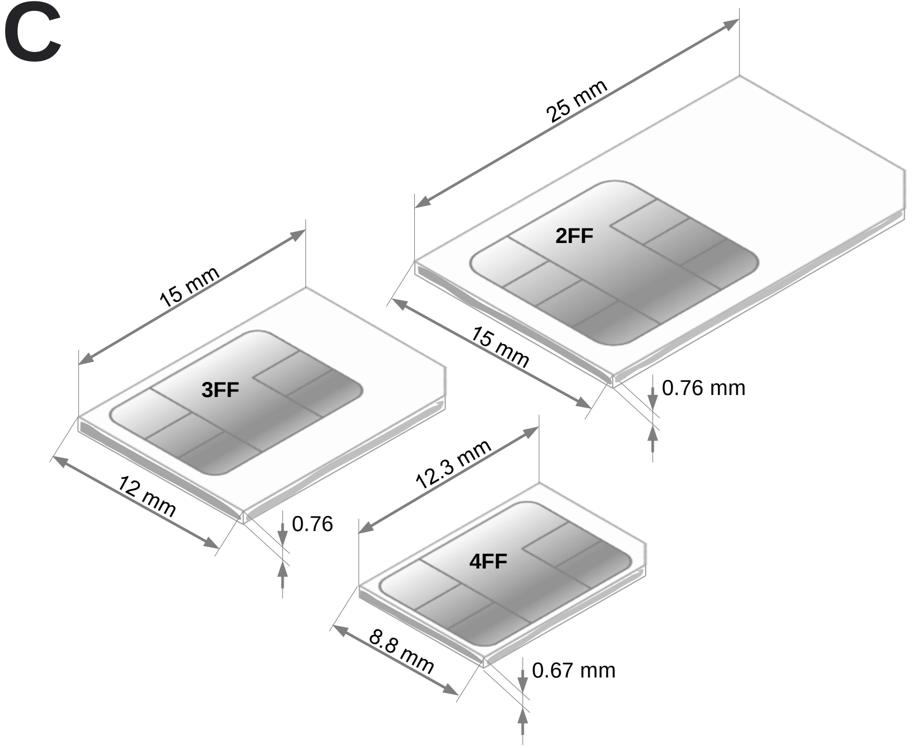
- **Network Slice** refers to a logical end-to-end network. An operator can create network slices to provide different service types to a set of customers.

- The network slice can involve the user and control plane of 5G core network, the radio access network, and the interworking functions to other non-3GPP access networks.

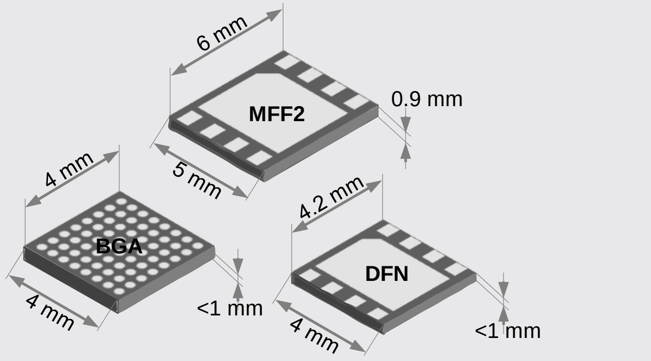
- The AMF manages the network slices, connecting the UE in one or more network slices. The UE is capable of connecting a maximum of eight parallel slices.

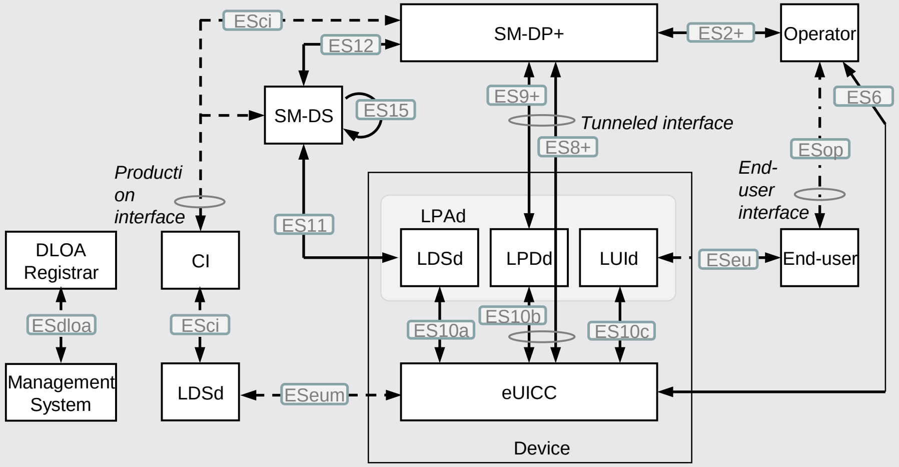
- The Release 16 3GPP TS 23.502 defines the **Network Slice-Specific Authentication and Authorization procedure** (NSSAA) for an S-NSSAI requiring it with an AAA Server (AAA-S). Either a Home PLMN (H-PLMN) operator or 3rd party can host the server.

UICC



- 5G can use “traditional” SIM form factors, or evolving embedded and integrated products.
- The latter requires solutions for Remote SIM Provisioning of consumer and M2M devices.
- GSMA PRDs detail the architectural and technical solutions, as well as the production security assurance at https://www.gsma.com/esim/esim-specification/





How verticals benefit from 5G?

- 5G fortifies the security of mobile communications, including end-to-end environment involving interconnected 5G core networks.
- Within the mobile network involving access, transport, and core segments, 5G provides extra layer of security for critical communications, financial institutes, as well as less critical environment such as massive IoT sensor networking.
- The up-to-date security that is a result of native design can be assumed to prevent well attacks – so the bad actors may prefer selecting easier ways to compromise the communications outside of the 5G infrastructure. Thus, critical communications outside the 5G network infrastructure needs to be shielded, e.g. by applying appropriate application-level security.

Conclusion: 5G in Practical environment

- 5G security controls address threats that have occurred in 2G-4G networks.
- 3GPP has designed 5G based on Secure by Design principles, including *enhanced mutual authentication* (ensuring trust and end-to-end relationship), *open network model* (removing assumption of safety from overlaid products and processes), and *encryption of inter- and intra-network traffic* (ensuring the encrypted information is worthless when intercepted).
- Nevertheless, the new solutions can also open up unknown threats. As an example, use of new architectures and features such as network slicing, network functions virtualization and cloud-based execution and storage can introduce new threats that require updated controls.

https://www.gsma.com/security/securing-the-5g-era/

References

1. J. Penttinen. 5G Second Phase Explained. Wiley 2021.
2. 3GPP TS 23.501, 5G Security Architecture.
3. GSMA PRD SGP.21, eSIM Architecture Specification V2.2, 1 September 2017.
4. GSMA PRD SGP.22, eSIM Technical Specification V2.2.2, 5 June 2020.
5. Example of SEPP in practice: https://www.broadforward.com/security-edge-protection-proxy/
6. Examples of roaming security: https://www.mpirical.com/blog/5g-security-when-roaming-part-1
7. Examples of 3GPP security standards: https://www.sdxcentral.com/5g/definitions/5g-security-standards/