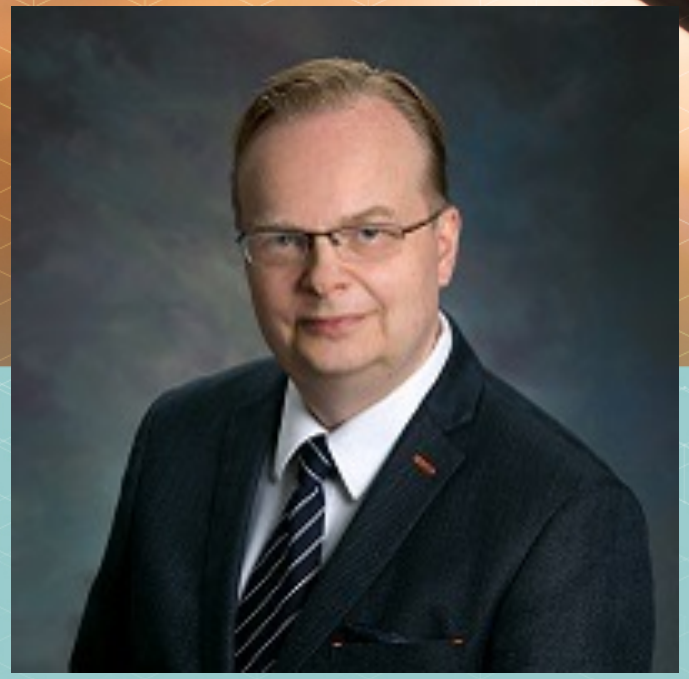
T-ISAC
Telecommunication
Information Sharing and Analysis Center

5G Security:
Use Cases & Best Practices

Welcome

Thursday 25 November 2021



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 Second Phase Explained*** and ***Wireless Communications Security***

linkedin.com/in/jypen

jpenttinen@gsma.com

@jyrki_penttinen

Blog amazon.com/author/jype

5G Security: use cases and best practices

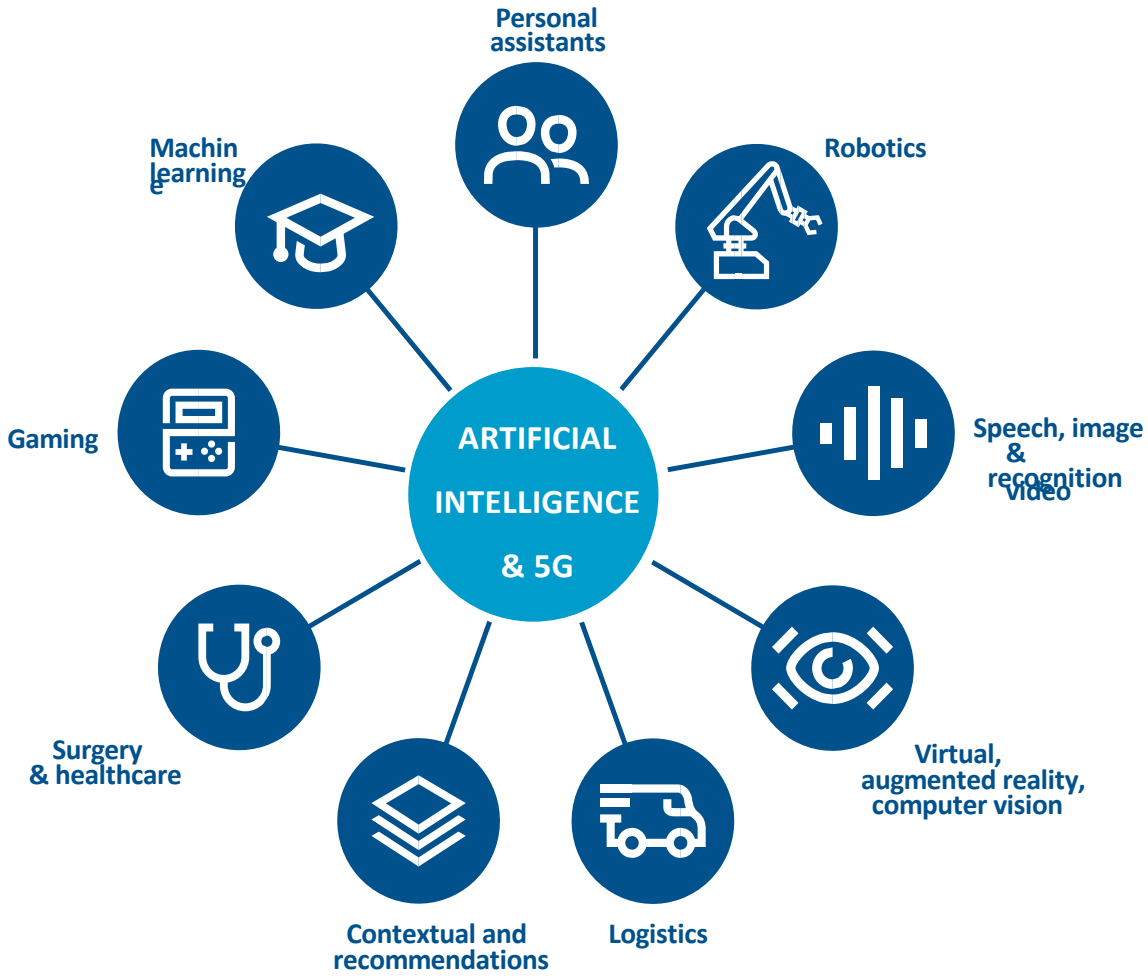
Contents

5G and Intelligent Connectivity

5G is developing in parallel with rapid advancements in AI and IoT.

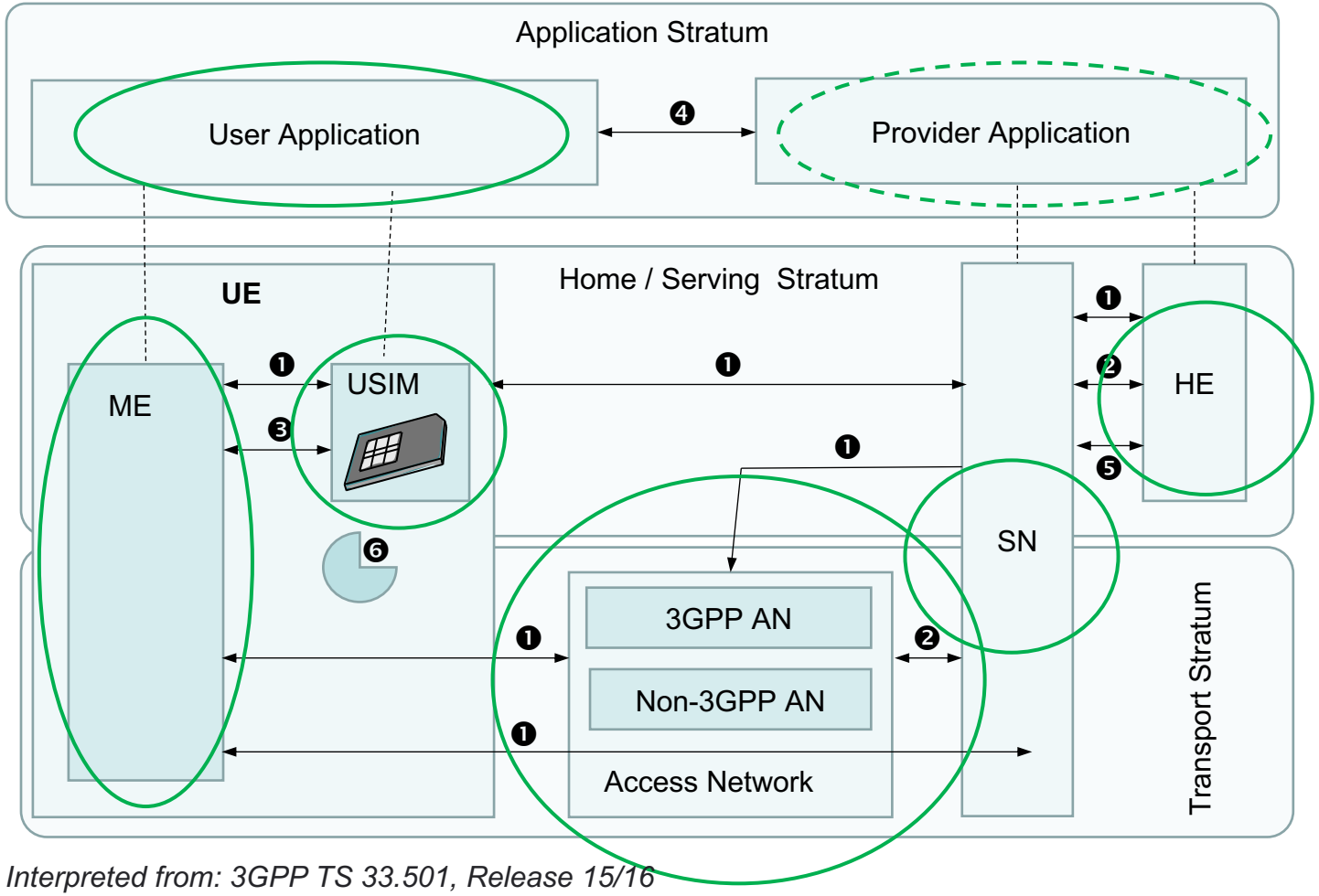
The combination of flexible, high-speed 5G networks with AI and IoT will underpin the new age of Intelligent Connectivity.

Along the advances of the functions, enablers, and performance, 5G also has uplifted the security architecture.



1. 5G Security Architecture

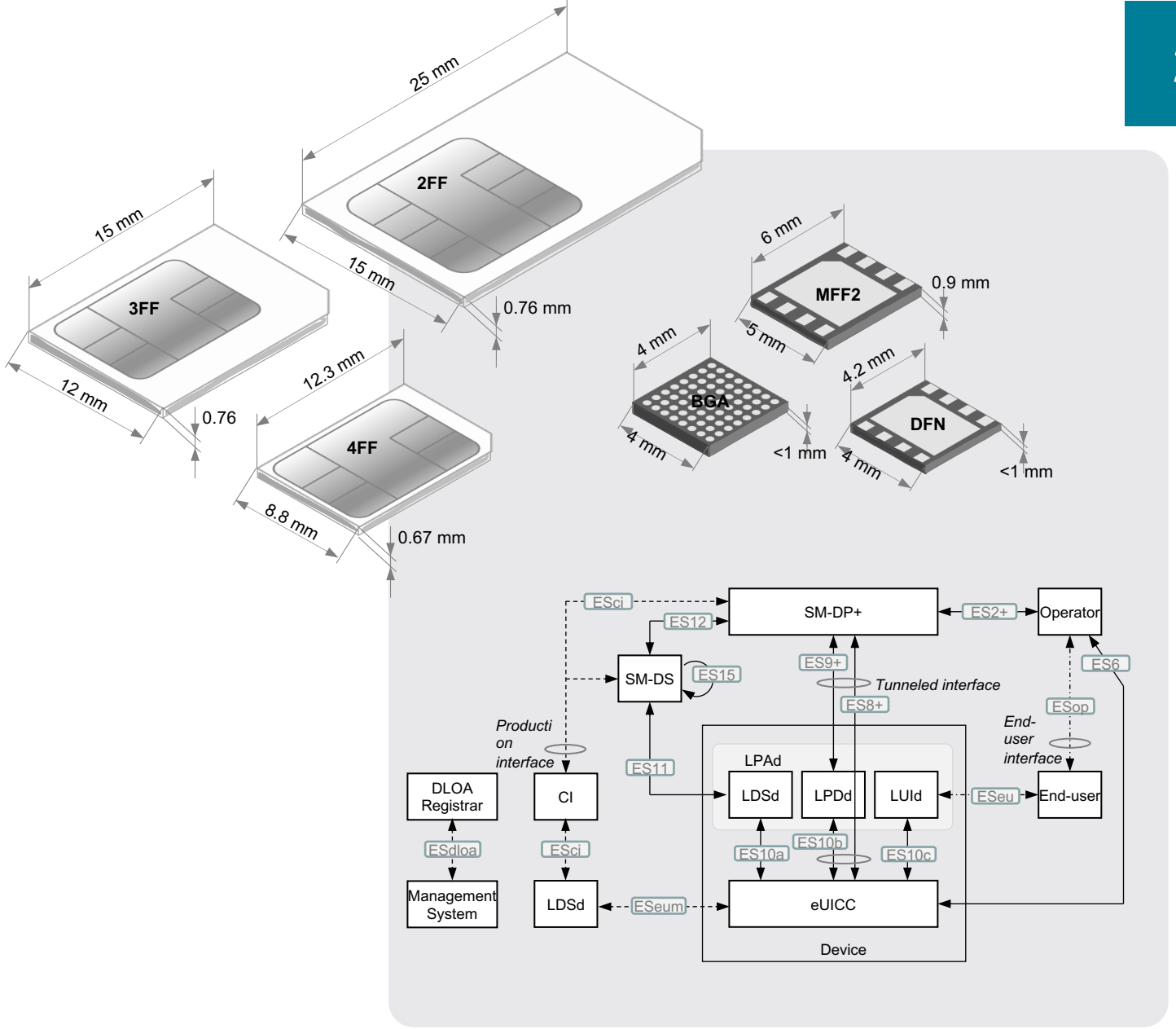
1. **Network access security** (UE authentication and service access)
2. **Network domain security** (network nodes exchange data and signaling)
3. **User domain security** (user's ME access)
4. **Application domain security** (message exchange of user / provider application)
5. **Service-Based Architecture** (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 15/16

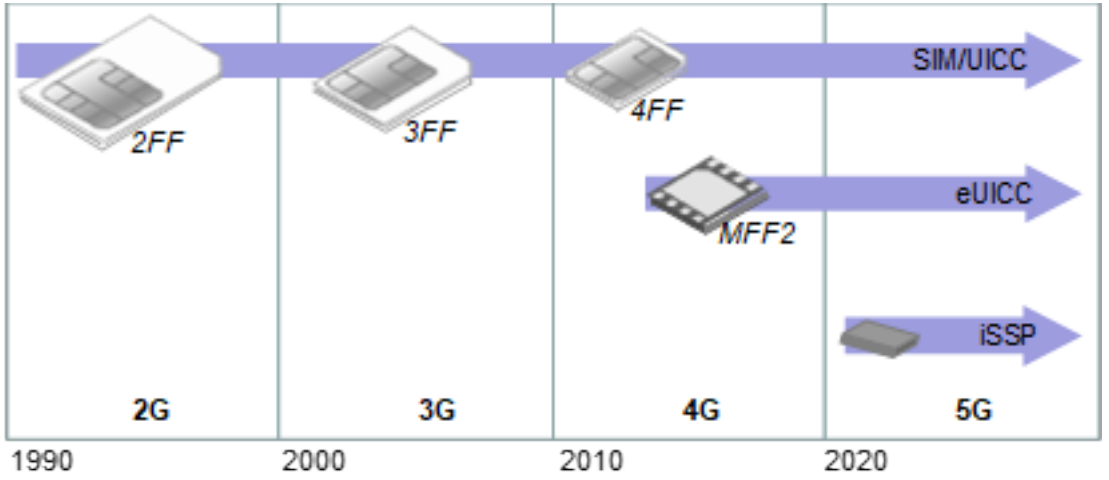
SIM in 5G era

- 5G can use “traditional” USIM (Universal Subscription Identity Module) form factors or embedded and integrated products.
- The latter ones require 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/



5G SIM

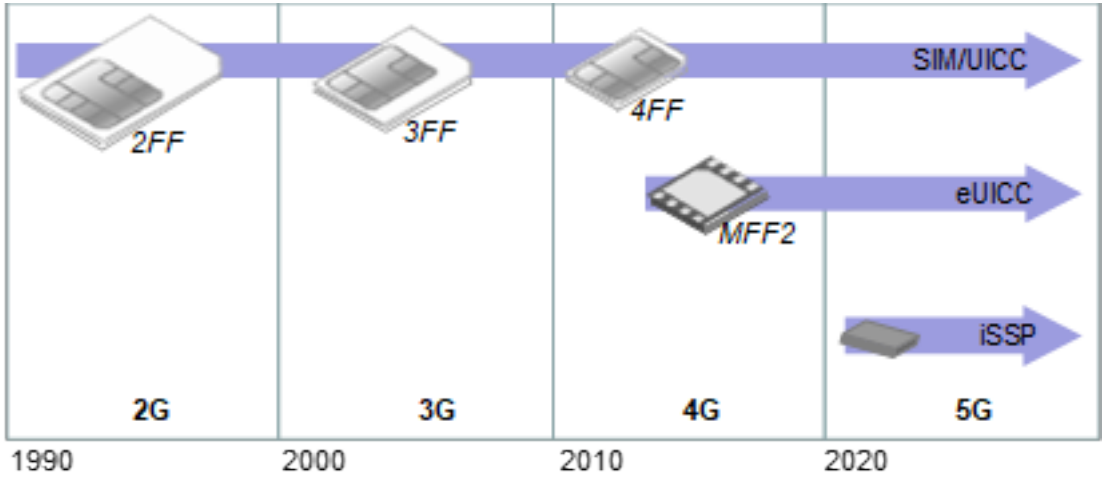
- 3GPP defines the new 5G subscription credentials as a set of values in the USIM and the Authentication Credential Repository and Processing Function (ARPF).
- These credentials refer to a long-term key or set of keys K, unique for each user, and the Subscription Permanent Identifier (SUPI) which uniquely identifies a subscription.
- The K and SUPI are designed to mutually authenticate the subscriber and 5G core.



- The eSIM principles designed for the UICC profile management apply to 5G, too, for consumer, application providers, etc., to provide a security anchor requiring security in the end-points.
- There is convergence path to support both consumer and M2M devices by a common platform.

5G SIM

- 3GPP defines the new 5G subscription credentials as a set of values in the USIM and the Authentication Credential Repository and Processing Function (ARPF).
- These credentials refer to a long-term key or set of keys K, unique for each user, and the Subscription Permanent Identifier (SUPI) which uniquely identifies a subscription.
- The K and SUPI are designed to mutually authenticate the subscriber and 5G core.



- The eSIM principles designed for the UICC profile management apply to 5G, too, for consumer, application providers, etc., to provide a security anchor requiring security in the end-points.
- There is convergence path to support both consumer and M2M devices by a common platform.

eSIM

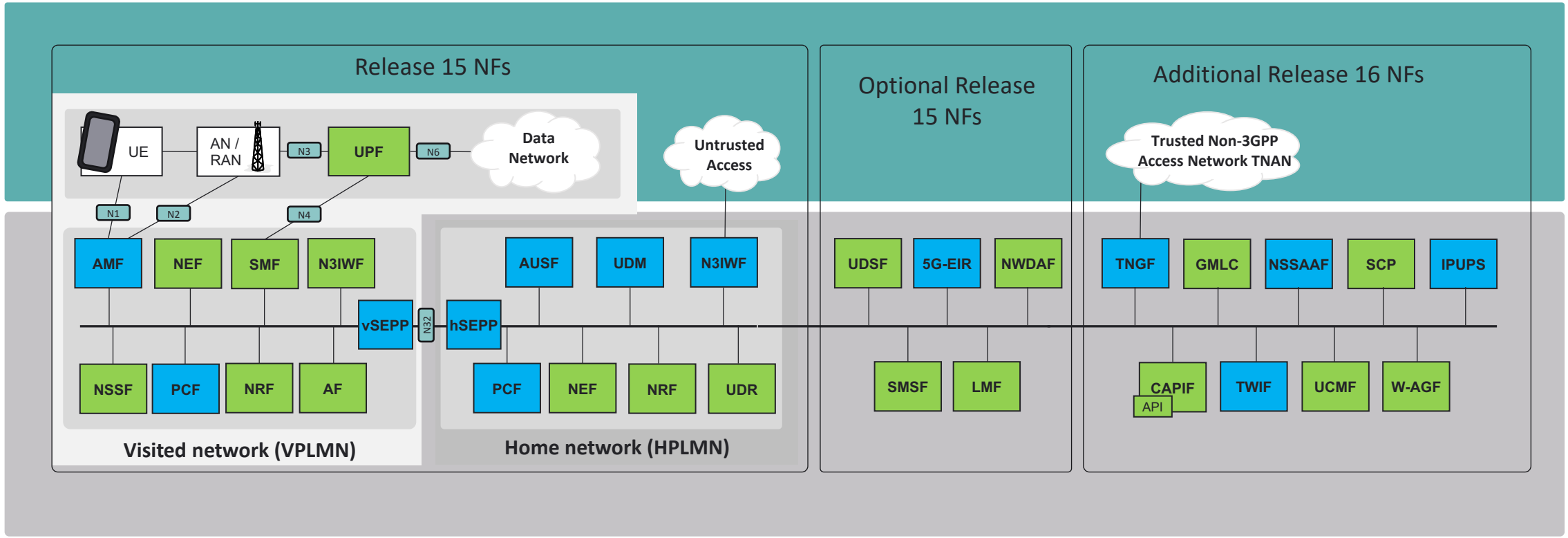
- The eSIM (Embedded SIM) refers to the extension of the “traditional” SIM.
- The original SIM has been evolved ever since to cope with the new requirements of the 3G, 4G and 5G
  - UICC, Universal Integrated Circuit Card, for HW.
  - USIM, Universal SIM, for operating system and files.
- The eSIM can be based on SIM, embedded into the device, (e.g., MFF2, M2M Form Factor), or it can be integrated even deeper into the processor.
- In all these cases, the same physical SIM can be utilized for managing the subscription, including the change of the Mobile Network Operator.

eSIM

- The **ETSI** (European Telecommunications Standards Institute) recognizes the embedded and integrated UICCs in their SSP (Smart Secure Platform).
- The **3GPP** will refer them to include the remote SIM provisioning aspects.
- As an example, as defined by ETSI, an iSSP is an integrated SSP confined in a dedicated sub-system within a SoC (System on Chip). The SoC is usually soldered in the terminal so the SSP is an integral part of the terminal.
- The **GSMA** complements the eSIM architectural and technical aspects:
  - eSIM Architecture Specification SGP.21 V2.3, 2021.
  - eSIM Technical Specification SGP.22 V2.2.2, 2020.

- https://www.gsma.com/esim/resources/sgp-21-architecture-specification-v2-3/
- https://www.gsma.com/esim/resources/sgp-22-v2-2-2/

Network Functions of the 3GPP Release 15 and 16



Further Releases

- 3GPP Release 17 schedule is currently set to complete the work in 2022 (freeze in March 2022, and implementation guides in June 2022).
- Some examples of the Release 17 items are:
  - Ultra-reliable low latency communications (URLLC) for industrial IoT
  - Integrated access and backhaul (IAB)
  - Radio access network slicing for NR
  - NR sidelink
  - Support for multi-SIM devices for LTE/NR
- Also the security-related specifications are updated, e.g. clarifying the usage of TLS and PRINS (Protocol for N32 Interconnect Security) between SEPPs. For more information, please refer to the principal 5G security specification TS 33.501 (Security architecture and procedures for 5G System).

- https://www.3gpp.org/release-17
- https://www.3gpp.org/news-events/1975-sec_5g

NFs form the SBA

- The Service-Based Architecture (SBA) of 5G is based on web technology and protocols. It provides flexible and scalable deployment thanks to virtualization, containers and cloud processing platforms.
- The SBA supports adequate security required by the increased number of use cases as well as the virtualized environment and cloud processing.
- In SBA, NFs can intercommunicate by request/response or subscribe/notify interactions between **NF service consumers** and **service producers**.
- This requires planning for the NF service API protection and authorization. The underlying protocol stack is based on web protocols such as HTTP and JSON and security protocols for interactions.

- https://www.ericsson.com/en/blog/2020/8/security-for-5g-service-based-architecture
- 3GPP TS 23.501, SBA
- 3GPP TS 33.501, 5G security

NS communications protection

- Adequate security mechanisms are needed for the NF communications:
  - **Authentication** for communication endpoints (to protect against spoofing of messages)
  - **Authorization** of the requests (to protect against elevation of privileges)
  - **Transport data protection** for confidentiality, integrity, and replay protection (to protect against tampering and message / information capture)
- Methods provided as of the Release 15
  - **Security for NF direct communication** without proxies used in between
  - TLS 1.2/1.3 for **mutual authentication** and **transport security** for the NF traffic
  - OAuth 2.0 (token authorization) for NF service consumers to **authorize access** services of NF service producers

Secure NF Communications

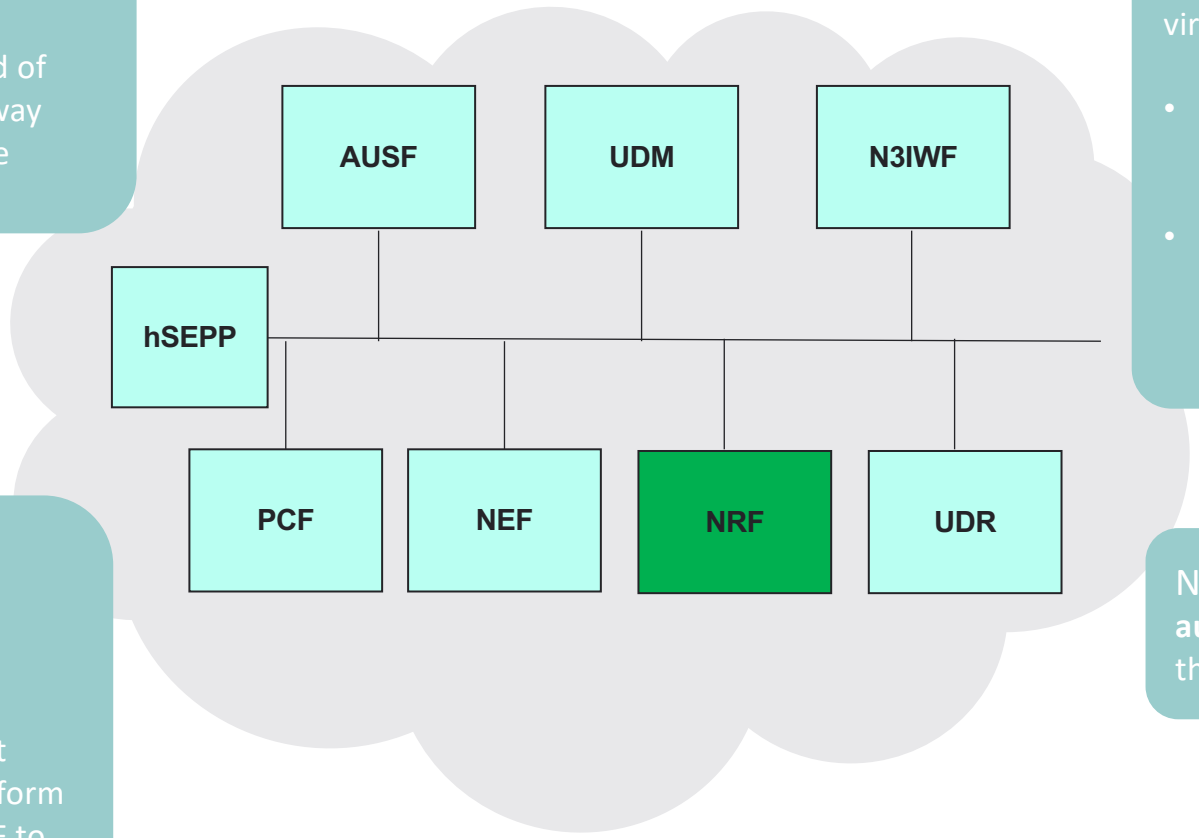
TLS 1.2 / 1.3 secures Internet communications replacing IPsec.

- TLS suits well in virtualized SBA to terminate security in the NF instead of relying on a separate security gateway (SEG) that typically secure complete network domain.

Transport TSL protection protects tokens against interception and fraudulent use.

Network Function Repository Function (NFRF) supports service discovery function.

- It acts as authorization server.
- Token-authorization and authentication are coupled so that NRF and NF service consumer perform mutual TSL-authentication for NRF to issue access token.



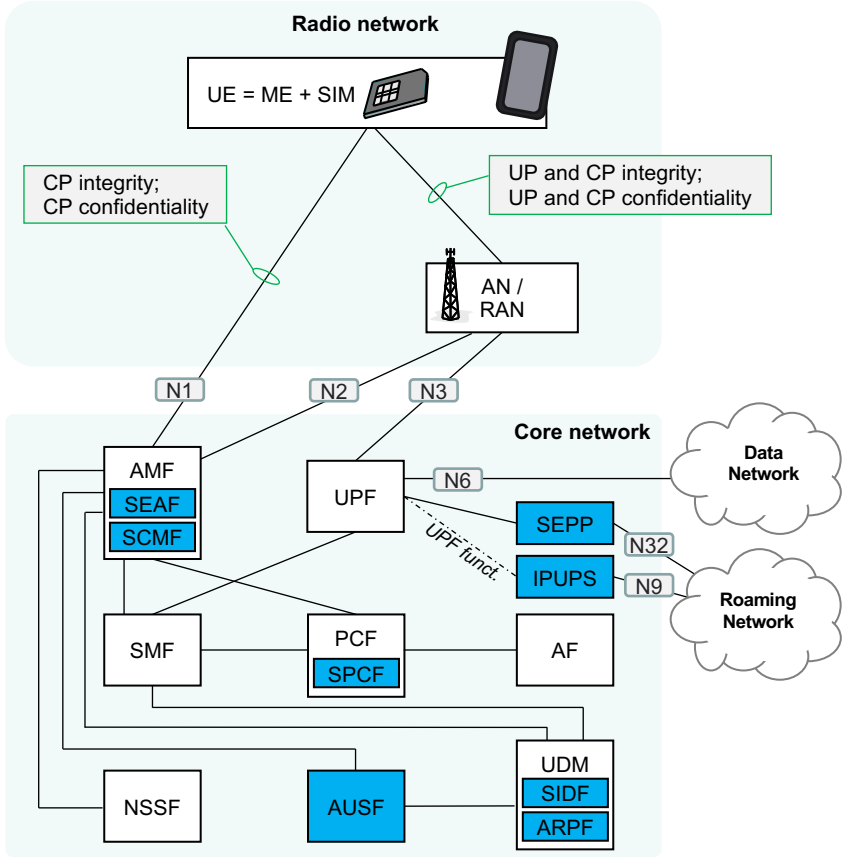
OAuth 2.0 works well in a dynamic, virtualized environment.

- It uses central authorization server to grant access tokens to NF service consumer after it authentication.
- Upon invoking a service, the client presents the access token to the NF service producer for its validation and service access.

NF service producers may provide **authorization rules** during registration at the NRF.

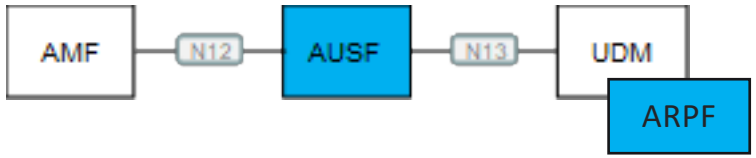
Security-related 5G Network Functions

- **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.



AUSF and ARPF

- The 5G Authentication Server Function replaces the LTE MME/AAA. It supports authentication for 3GPP access and untrusted non-3GPP access as per the 3GPP TS 33.501. It has interfaces towards AMF and ARPF (UDM).

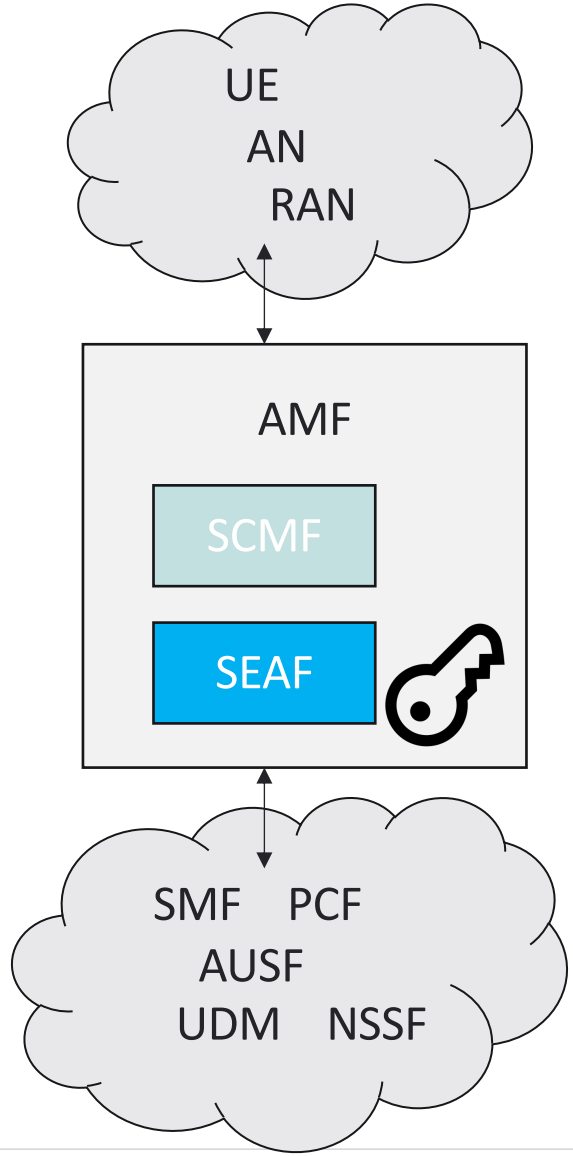


- **AUSF**: The Authentication Server Function terminates requests from the SEAF and interacts with the ARPF. The AUSF and the ARPF could be collocated and form a general EAP server for EAP-AKA and EAP-AKA'.

- **ARPF**: The Authentication Credential Repository and Processing Function is collocated with the UDM (Unified Data Management). It stores the long-term security credentials such as user's key K. Based on those, it executes cryptographic algorithms, and it creates authentication vectors.

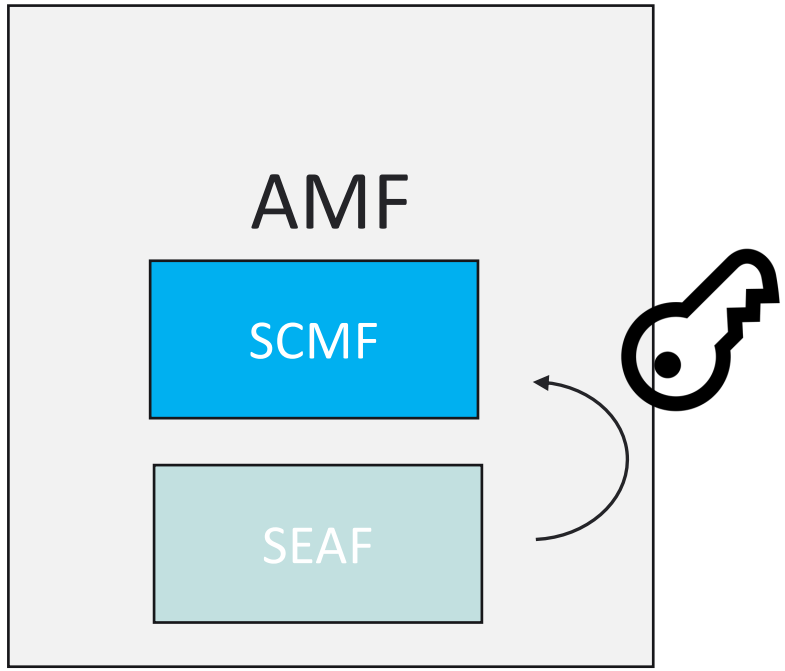
SEAF

- SEAF is the Security Anchor Function that forms, as an outcome of the primary authentication, the unified, common anchor key KSEAF for all the access scenarios.
- KSEAF protects the communications of the UE and the serving network, and it resides in the visited network in roaming scenario.
- There may be separate KSEAF keys for the same UE connected to a 3GPP and a non-3GPP (such as Wi-Fi) access networks.
- SEAF is collocated with the AMF in 3GPP Release 15.



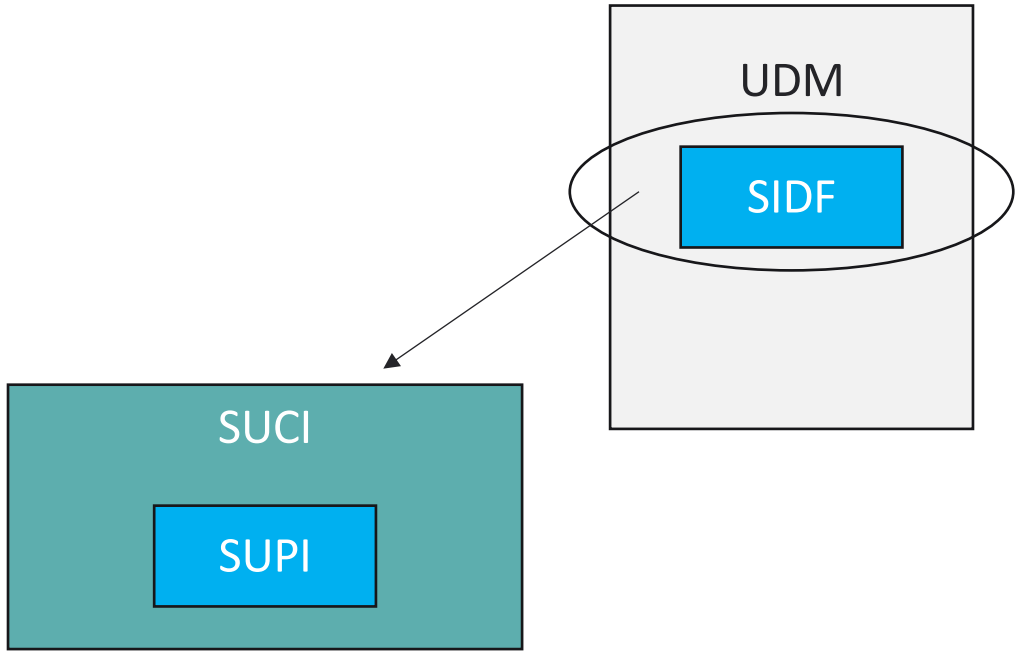
SCMF

- SCMF is the Security Context Management Function.
- It retrieves the key from the SEAF (Security Anchor Function), which is used to derive further keys.
- The SCMF may be collocated with the SEAF in the same AMF (Access and Mobility Management Function).



SIDF

- SIDF is the Subscription Identifier De-Concealing Function.
- It is a service offered by the UDM Network Function of the home network of the subscriber.
- It **de-conceals the SUPI** (Subscription Permanent Identifier) from the SUCI (Subscriber Concealed Identifier).



SIDF for SUCI & SUPI

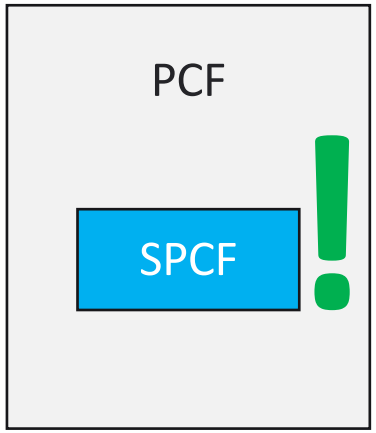
- There are two new identifiers in 3GPP 5G network: SUPI and SUCI.
- **SUPI** - Subscription Permanent Identifier.
  - **Primary identifier** in 5G in foundation for all the key derivation together with the subscribers' unique K key.
  - Serving network authenticates SUPI via authentication and key agreement procedure of UE-network.
  - Serving network authorizes the UE through the **subscription profile** obtained from the home network basing on the authenticated SUPI.
- **SUCI** - Subscription Concealed Identifier
  - As defined in 3GPP TS 33.501, SUCI is a one-time use subscription identifier.
  - It contains the concealed subscription identifier, e.g., MSIN (Mobile Subscriber Identification Number).
  - The SUCI is an **optional** mechanism managed from the UICC.
  - Its aim is to provide **further security** in hiding the permanent user identification information.
  - It is a privacy-preserving identifier and it contains the concealed SUPI.

SIDF for SUCI and SUPI

- SUCI is a **one-time use subscription identifier**, which contains the concealed subscription identifier such as the MSIN portion of the SUPI, and additional non-concealed information needed for home network routing and protection scheme usage.
- UE generates SUCI using a protection scheme with the raw public key that has already been securely provisioned beforehand in control of the home network.
- Based on the indication of USIM, dictated by the MNO, the calculation of SUCI can be done either by the USIM or the ME.
- The UE then builds a scheme-input from the part containing subscription identifier of the SUPI and executes the protection scheme.
- The UE would not conceal the home network identifier though, such as Mobile Country Code (MCC) or Mobile Network Code (MNC).
- Please note that there is no requirement for protecting the SUPI in case of unauthenticated emergency call.

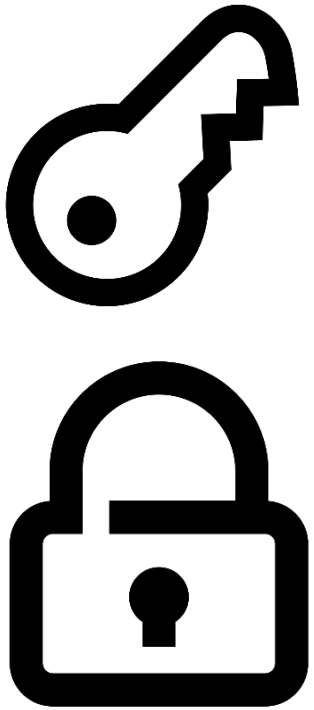
SPCF

- SPCF is the Security Policy Control Function.
  - It provides policies related to the security of network functions such as AMF, SMF and UE.
  - The AF dictates the elements involved for each policy scenario.
  - The SPCF may be collocated with the PCF, or it can be a stand-alone element.
  - SPCF contributes to the confidentiality and integrity protection algorithms, key lifetime and length, and the selection of the AUSF.
- Via mobile edge computing and virtualization, 5G network functions and contents are moving closer to the consumer.
  - The functions and contents are often replicated and exposed in potentially less protected environments.
  - To make contents available to the user with reduced latency, the edges need to cache it via 3rd party content provider, so there needs to be adequate security measures in place, respectively, which SPCF can control.



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.



5G Roaming and Interconnection Scenarios

- SEPP and IPUPS interconnect 5G networks.
- 3GPP defines SEPP in Release 15 and additional UP Security in Release 16.
- 3GPP defines the security for the traffic between SEPP components.
  - Nevertheless, in practical environment, there is a need for further definitions for a fluent solutions.
  - These aspects should take into account also stakeholders beyond mobile network operators, e.g., when roaming takes place via IPX or roaming hubs, as well as value added service (VAS) providers in the roaming environment.
  - This additional work takes place currently at GSMA's roaming and security -related groups.

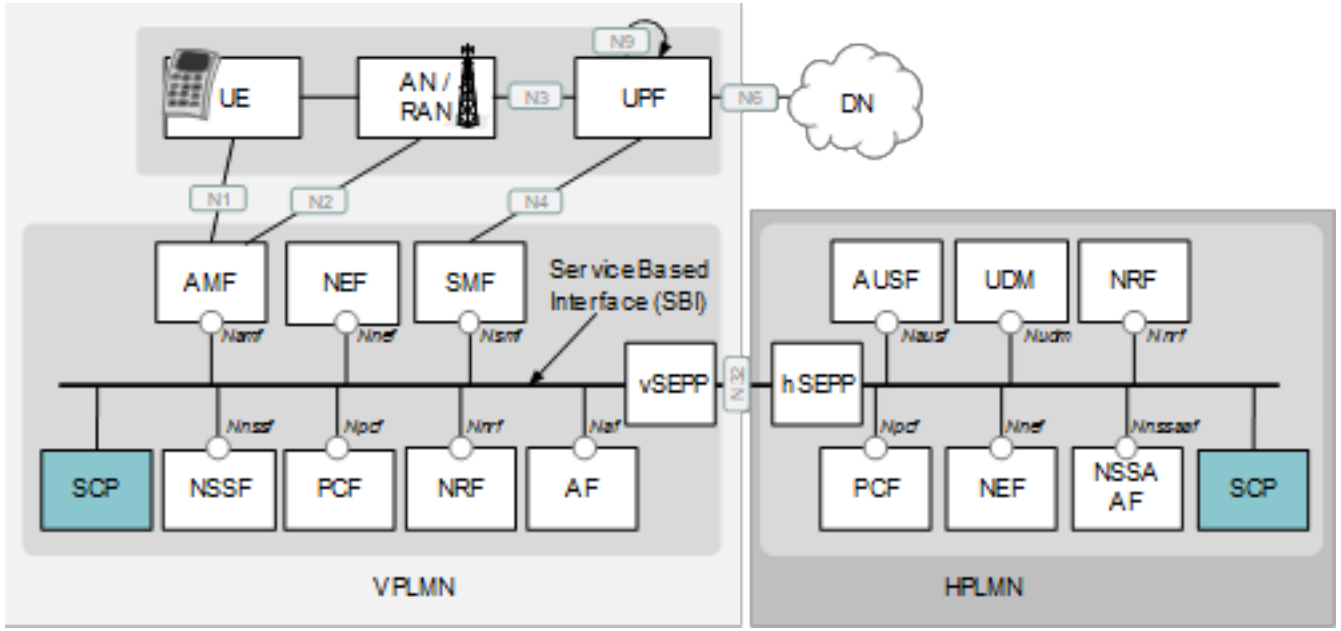
Protection between SEPPs as defined by 3GPP

- TLS must be used for N32-c connections between the SEPPs. Scenarios:
  - **No IPX providers between the SEPPs**: TLS for N32-f connections between the SEPPs.
  - **IPX providers offering merely IP routing service between SEPPs**: TLS or PRINS (application layer security) shall be used for protection of N32-f connections between the SEPPs.
  - **IPX providers for IP routing and services requiring modification or observation of the information and/or additions to the information sent between the SEPPs**: PRINS shall be used for protection of N32-f connections between the SEPPs.
- If PRINS is used on the N32-f interface, one of the following additional transport protection method should be applied between SEPP and IPX provider for confidentiality and integrity protection:
  - NDS/IP (as per 3GPP TS 33.210 and TS 33.310), or
  - TLS VPN with mutual authentication (as per TS 33.210 and TS 33.310); The identities in the end entity certificates shall be used for authentication and policy checks, but it shall be compliant with the profile given by HTTP/2 (as per RFC 7540).

- 3GPP TS 33.501 V17.3.0, Security architecture and procedures for 5G system, Release 17

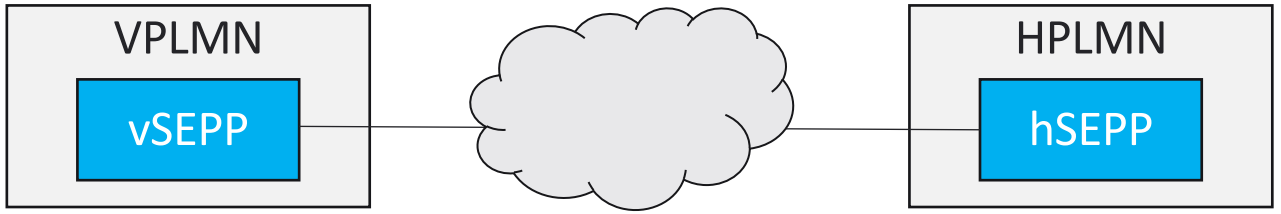
Roaming scenarios – SEPP and IPUPS

- This is an example of a 5G roaming case for a roaming basing on Local Breakout (LBO) as interpreted form the TS 23.501.
- In the LBO scenario VPLMN (Visited Public Land Mobile Network) controls the SMF and all UPF components involved with the PDU session.



Roaming scenarios – SEPP and IPUPS

- In this scenario:
  - The UE, which is roaming in visited network (VPLMN), establishes connection to the Data Network (DN) of the VPLMN.
  - Meanwhile, the Home Public Land Mobile Network (HPLMN) enables the connectivity basing on the user's subscription information on the UDM, subscriber authentication via the AUSF, and policies via the PCF for this specific UE.
- The interworking between HPLMN and VPLMN is protected by home Security Edge Protection Proxy (hSEPP) and visited network's Security proxy (vSEPP).
- The SEPP is **non-transparent proxy** and supports message filtering and policing on inter-PLMN control plane interfaces, and topology hiding



5G Roaming Scenarios – SEPP and IPUPS

- In this example:
  - The visited network provides functions for the **network slice selection** via NSSF, **network access control and mobility management** via AMF, **data service management** via SMF, and **application functions** via AF.
  - 5G applies the same principles for the **separate user and control planes** managed by the user plane via UPF as in 4G.
- In the LBO architecture of 5G, the PCF residing in the VPLMN is able to interact with the AF to generate PCC rules for the services the VPLMN delivers.
  - In that case, the PCF relies on the locally configured policies based on the roaming agreement between the VPLMN and HPLMN operators.
  - Nevertheless, the PCF of the VPLMN has no access to subscriber policy information from the HPLMN.
- In this example, the Release 16 brings along the new **SCP**, Service Communication Proxy.
  - It can communicate indirectly between NF components and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN.
  - 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.

The role of IPUPS

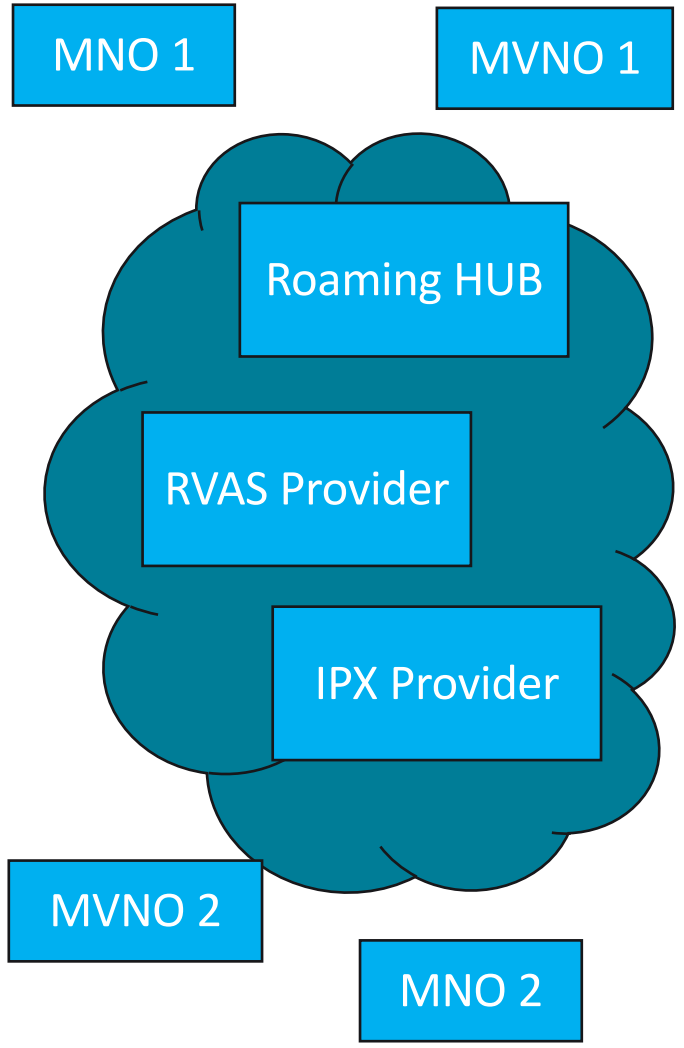
- IPUPS provides the Inter-PLMN User Plane (UP) security.
- It is a new 5G functionality introduced in the Release 16.
- It is located at the perimeter of the PLMN for protecting user plane messages.
- It is an UPF functionality that enforces GTP-U (GPRS Tunnelling Protocol User Plane) **security between UPF elements** of the visited and home PLMN via the **N9 interface**.
- Please note that it is possible to activate the IPUPS with other functionality in a UPF, and it can be activated in a UPF dedicated for IPUPS functionality.

The role of IPUPS

- The TS 23.501 presents various scenarios for 5G for both home network as well as for the roaming such as the roaming architecture in the case of home routed scenario which involves the new NSSAAF component in the HPLMN.
  - In that case the UPF components in the home routed scenario can be used to support also the optional IPUPS functionality (Inter PLMN UP Security).
  - The 3GPP TS 33.501 and Section 5.8.2.14 of the TS 23.501 specify the IPUPS.
- The IPUPS functionality is housed at the border of the operators' networks, and it protects the network from invalid inter-PLMN N9 traffic in home routed roaming scenarios.
  - This solution allows the UPF to terminate GTP-U N9 tunnels.
  - The UPFs that support the IPUPS in both VPLMN and HPLMN are controlled by the V-SMF and the H-SMF of the respective PDU session.
  - In practice, operators could deploy the IPUPS functionality as a separate Network Function from the UPF. In that case, the IPUPS serves as a transparent proxy that is capable of reading transparently the N4 and N9 interfaces.
- Please refer to the TS 23.501 for more architectural scenarios of the IPUPS.

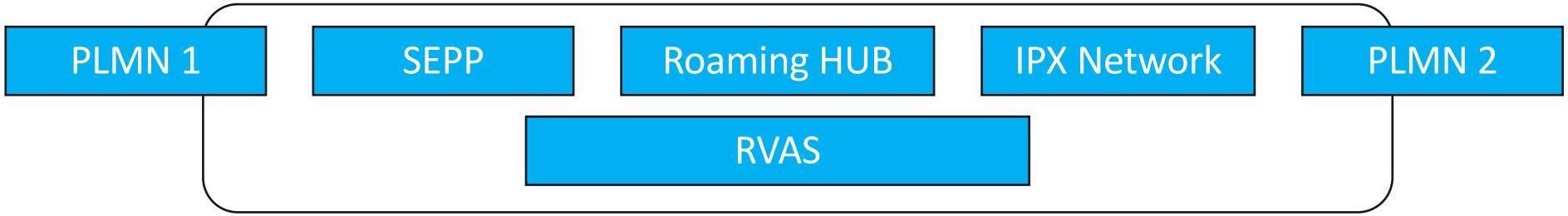
Practical roaming aspects in 5G

- The 3GPP defines SEPP TLS security for 5G roaming.
- Roaming Value Added Service (RVAS) can be offered to MNO. This service processes signaling messages that MNOs exchange for easing the international roaming.
- Now, to provide fluent transition, and if an MNO prefers to use RVAS, is partnering with MVNO, or uses SCP, there should be no impacts.
- The roles on the roaming scenarios may involve also IPX Provider and Roaming Hub, and each one of these have their own, non-overlapping task.
- Decoupling RVAS from the N32 interface seems to be the solution. The practical realization of this is discussed at GSMA work groups.



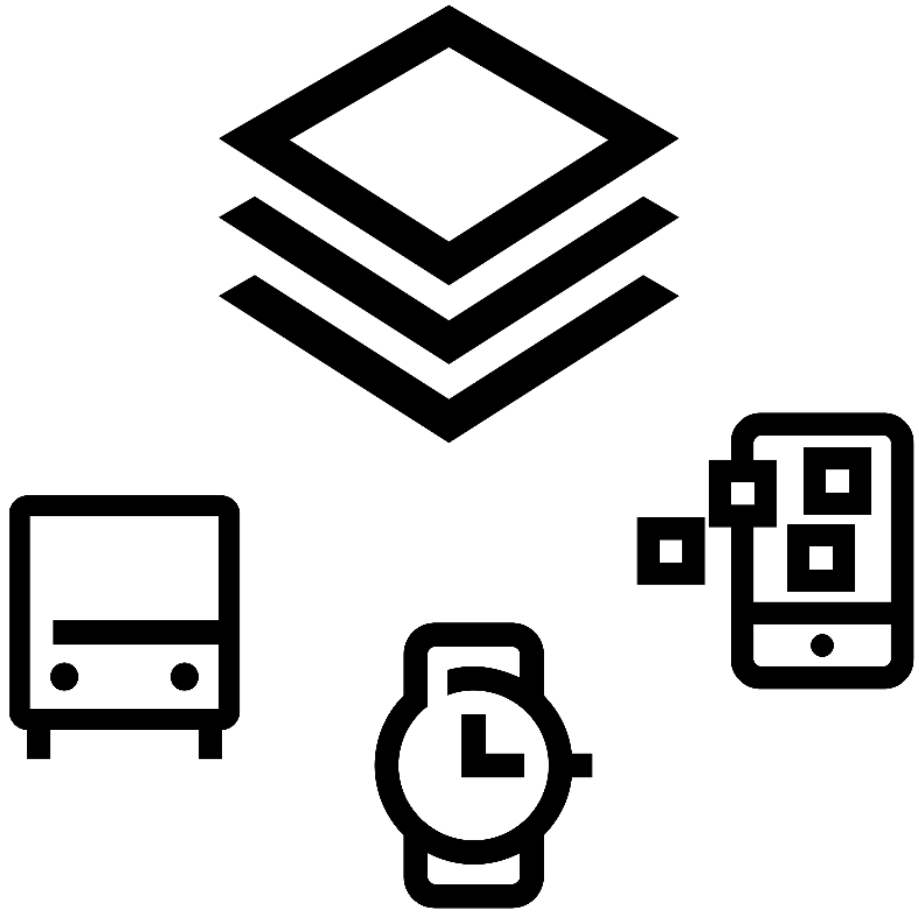
Examples of practical roaming scenarios

Scenario description	SEPP comms	RVAS	Roaming HUB	IPX
A: no RVAS , no roaming hub	PLMNs have their own	No	No	Optional transport, or direct connection
B: RVAS in PLMN, no roaming hub	SEPP – RVAS comm can include routing of all or selected messages; request / response for selected content	In PLMN; RVAS in SEPP or interacting with external RVAS function.	No	Optional transport, or direct connection
C: MVNO, no roaming agreements	MVNO does not have SEPP	No	No	Bilateral agreement; no impact on PLMNs
D: RVAS and Roaming hub	PLMN can have SEPP at RH, and also direct connections to other PLMNs using their own SEPP.	PLMN may delegate RVAS to their Roaming Hub	Yes, to one or each PLMN	Optional transport, or direct connection
E: RVAS and SEPP delegated to IPX	PLMN can delegate SEPP to IPX.	PLMN can delegate also RVAS to IPX.	No	Bilateral agreement for PLMN NF/SCP - IPX comms.



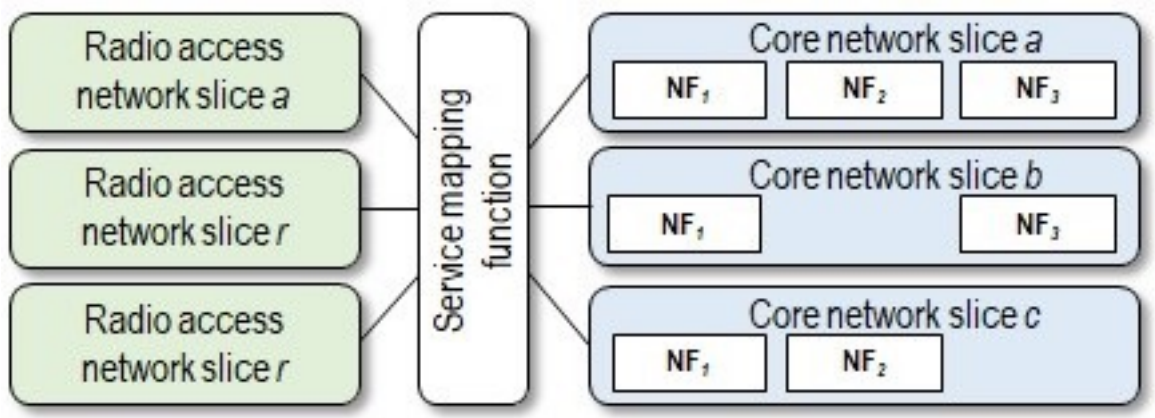
5. Security Aspects of Network Slicing

- **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.



Security of Network Slicing

- The network slicing is an essential function of the Standalone 5G networks.
- It provides means for operators to adjust their service level per vertical in terms of attributes such as data speed, latency, and capacity.
- Another important aspect of the network slicing functionality is its capability to **isolate the slices** to provide adequate security level between the users.



- https://www.linkedin.com/pulse/network-slicing-5g-jyrki-penttinen/
- https://www.gsma.com/newsroom/resources/ng-130-network-slicing-north-americas-perspective/attachment/ng-130-white-paper-network-slicing-na-perspective-3/

Security of Network Slicing

- The 3GPP TS 23.501 and TS 23.502 describe the **Network Slice-Specific Authentication and Authorization** procedure.
- The 5G system triggers it for an S-NSSAI requiring Network Slice-Specific Authentication and Authorization with an AAA Server (AAA-S).
- Either a Home PLMN (H-PLMN) operator or 3rd party can host the server; in the latter scenario, the 3rd party needs to have a business relationship with the H-PLMN by relying on an EAP framework.
- If the AAA Server belongs to a third party, the H-PLMN operator can apply an AAA Proxy (AAA-P).

Security of Network Slicing

- As stated in the 3GPP TS 23.502, the **AMF triggers the network slicing procedure** during a registration procedure as soon as any network slices require Slice-Specific Authentication and Authorization.
  - This triggering can also take place when the AMF determines that Network Slice-Specific Authentication and Authorization is required for an S-NSSAI in the Allowed NSSAI; this scenario happens, e.g., in the event of a subscription change.
  - The procedure takes place when the AAA Server that authenticated the Network Slice triggers a re-authentication.
- The AMF works as an EAP Authenticator communicating with the AAA-S via the Network Slice Specific Authentication and Authorization Function (NSSAAF).

GSMA resources

- The GSMA is supporting the mobile security ecosystem through the following Programmes and services:
  - The Fraud and Security Group (FASG) who acts as the GSMA home of 5G Security, building and sharing industry best practice on 5G fraud risks and security controls.
  - The Future Network Programme supports the industry with 5G implementation guidance.
  - The GSMA CVD programme successfully manages disclosures into the 5G standards, cooperating with 3GPP this research has been used to create more secure 5G standards prior to deployment.
  - The GSMA IoT Security Project which develops resources specifically targeted at addressing IoT security risks.
  - The Networks Group (NG) who define network architecture guidance and functionality, including SEPP configuration and network slicing templates, for 5G.

5G Security Guidelines & Services

- Securing the 5G Era
  - https://www.gsma.com/security/securing-the-5g-era/
  - https://www.gsma.com/security/resources/t-isac-5g-security-evolves-catch-up/
- T-ISAC
  - https://www.gsma.com/security/t-isac/
- GSMA IMEI database / SG.18 Device Registry Specification/Access Policy
  - https://imeidb.gsma.com/imei/index#
  - https://devicecheck.gsma.com/sg18/SG.18_v7.0

Example: GSMA Security Controls

- The GSMA document FS.31 presents baseline security controls.
- The latest version V2.0 by February 2020 presents a set of practical aspects on business and technological controls, including controls for UE and ME, UICC and eUICC management, IoT, RAN, roaming and interconnect, core network management and network operations, and security operations.
- The document serves as a guideline for specific set of security controls that the mobile telecommunications industry should consider deploying.
- It is important to note that the presented security controls do not override local regulations or legislation in any territory, but merely supplement security levels within the mobile telecommunications industry.

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/

Further references

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

- A guide to 5G security by Ericsson
  - https://www.ericsson.com/en/security/a-guide-to-5g-network-security

- Cybersecurity aspects and guidelines
  - https://www.cisa.gov/5g
  - https://semiengineering.com/the-growing-risk-of-5g-security/