SAMSUNG Research

ITU-APT Foundation of India - 5G TECH SESSIONS

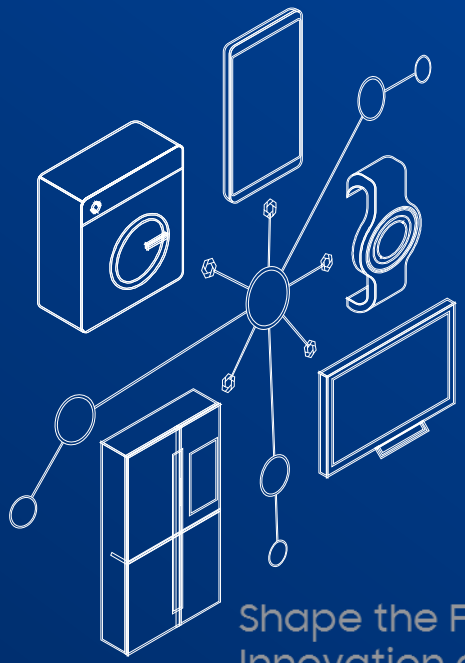
5G Security

September 27, 2018

Samsung R&D, Bengaluru

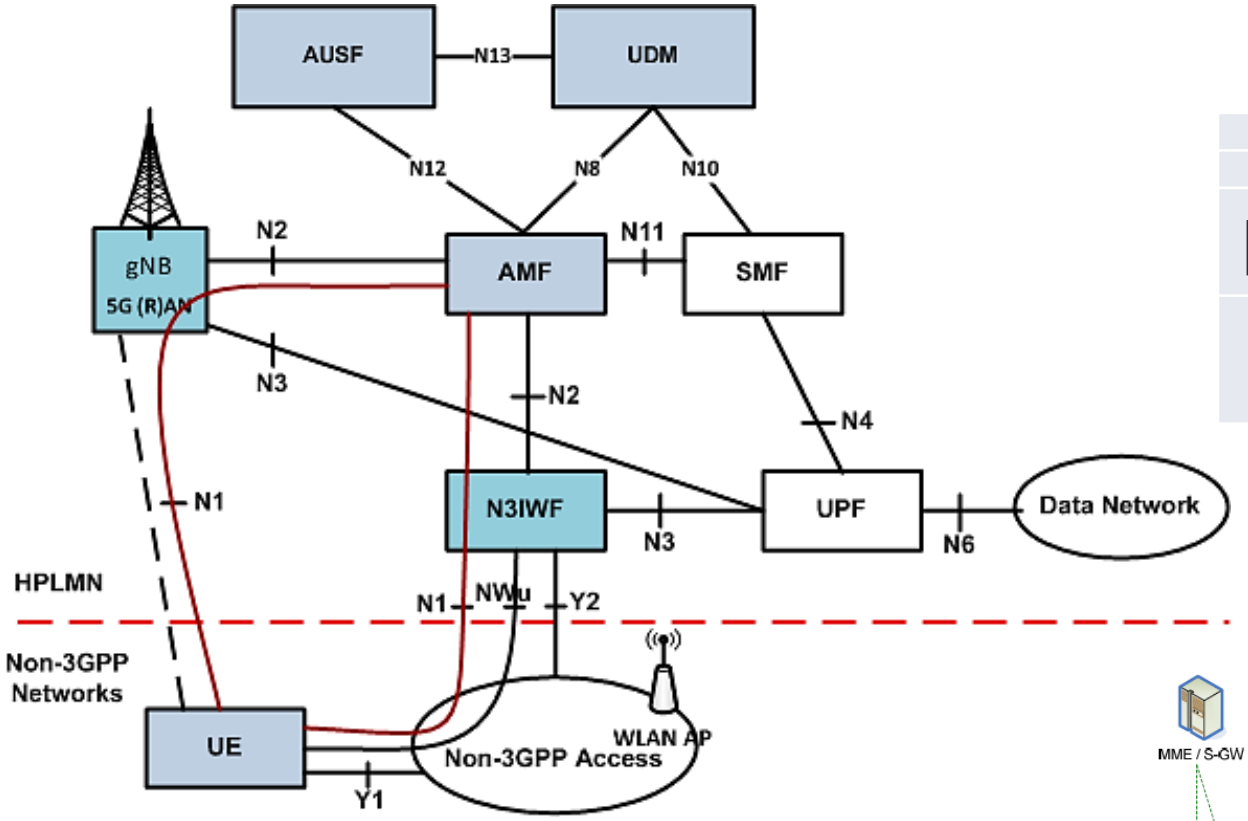
Disclaimer

Contents

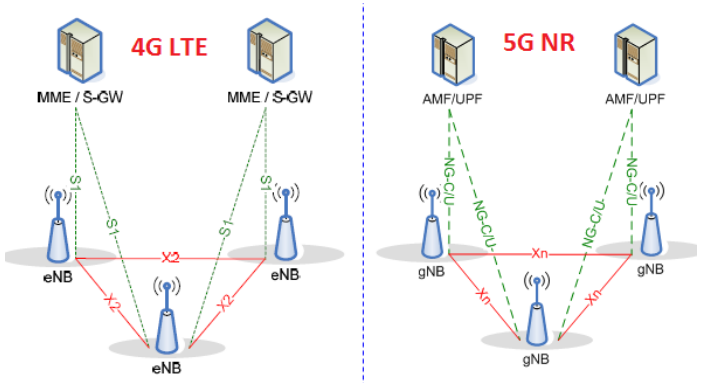


Shape the Future with
Innovation and Intelligence

5G Security Architecture



	Network Access Security
	Non-3GPP Networks
	Core network Functions to establish network access security for UE
	Access network Functions to establish network access security for UE



3GPP TS 33.501

SAMSUNG Research

Authentication Framework

5G Authentication Framework

Unified Authentication Framework

- Multiple access technologies – Manage access security in unified manner
- Unified Authentication Framework supports:
  - Security Context sharing between different access technologies
  - Reduce latency in adapting security context to different access technologies
  - Support multiple security credentials (Symmetric key (K), PKI (Certificate),..)
  - **Extensible Access Protocol (EAP)** authentication framework is one of the supported unified authentication method

Authentication Methods

- **EAP-AKA' and 5G-AKA** are mandatory to support and **EAP-TLS** is optional to support/use (Phase-1)
- **Primary authentication** shall create a unified anchor key, to protect the subsequent communication
- Support for general EAP methods for *optional* **secondary authentication** between a UE and an external data network

5G Authentication Framework

Security Functionalities

ARPF/UDM (AuC)

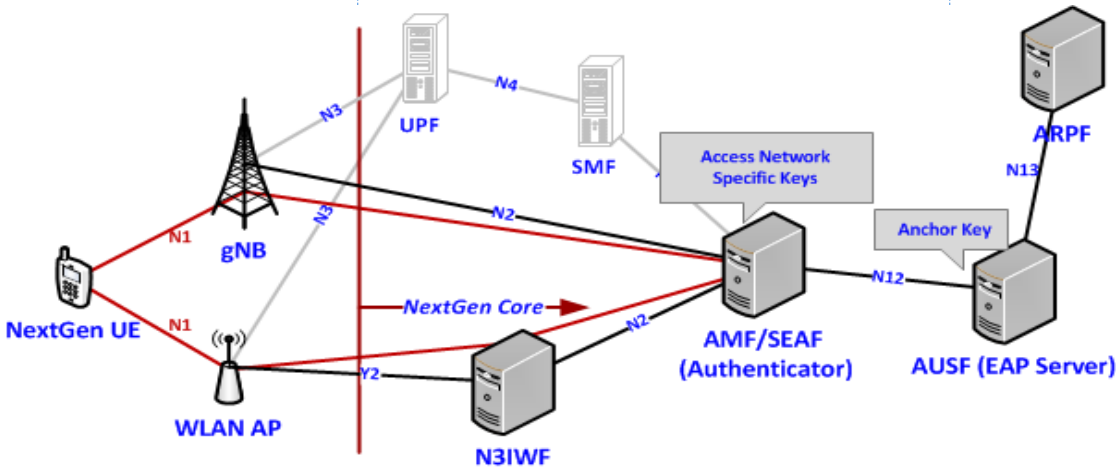
- Authentication Credential Repository and processing Function
- Stores Long term security Credentials

AUSF (HSS, EAP Server)

- Authentication Server Function
- Interacts with ARPF and terminates requests from SEAF

SEAF (Authenticator)

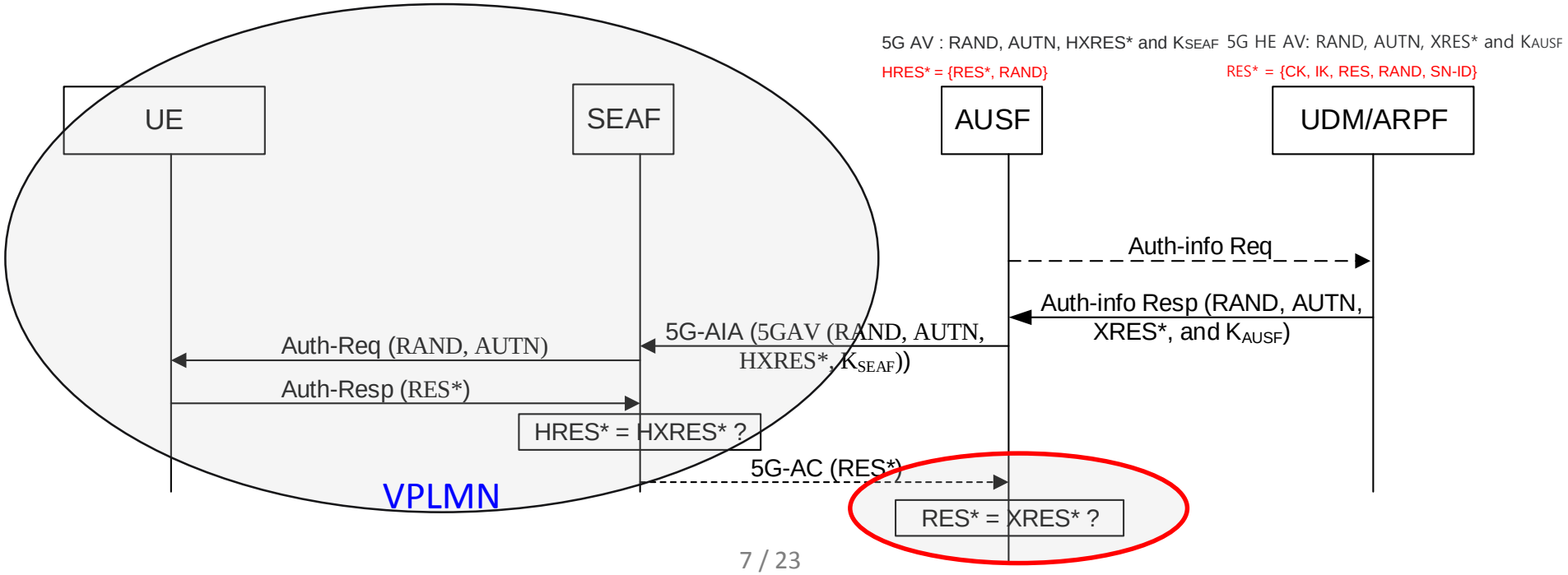
- Security Anchor Function
- Receives Intermediate Key from AUSF
- SEAF and AMF co-located
- Single anchor per PLMN for all access networks
- Derives further keys for AS.



5G AKA

Enhanced EPS AKA for more home control

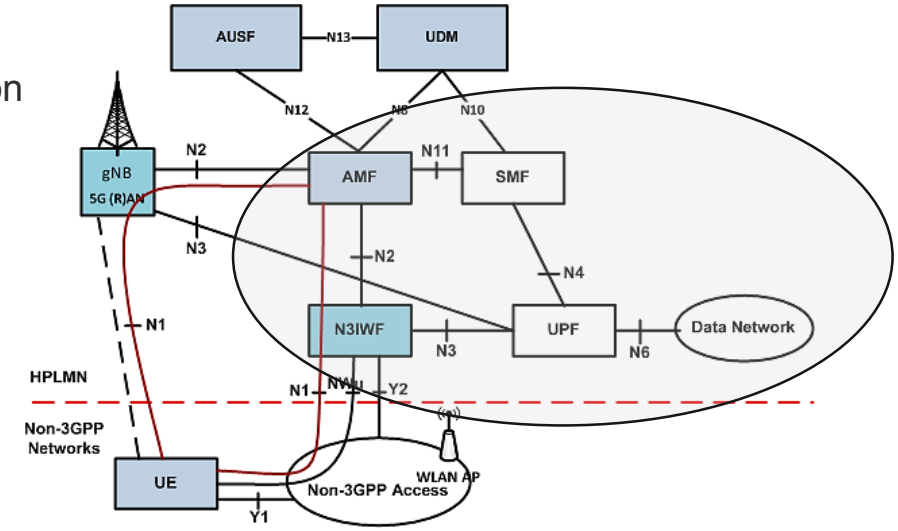
- Prevents certain frauds like *fraudulent Update Location request for subscribers that are not actually present in the visited network*
- More home control
  - 5G AKA (At AUSF, RES* = XRES*)
  - EAP-AKA' (AUSF takes "Backend Authentication Server" role)



Secondary Authentication

Between UE and external data network via 5G Network

- *Optional* to use between UE and an external data network (DN)
- EAP (RFC 3478) based authentication by external DN-AAA server
- SMF performs the role of EAP Authenticator
- Between UE and SMF - EAP messages sent in SM NAS message
- SMF (EAP authenticator) communicates with the external DN-AAA over N4 and N6 via the UPF.
- PDU Session Establishment Request may contain PDU session authorization by the external DN
  - SMF checks UE's authorization
  - Based on subscription
  - And Local policies



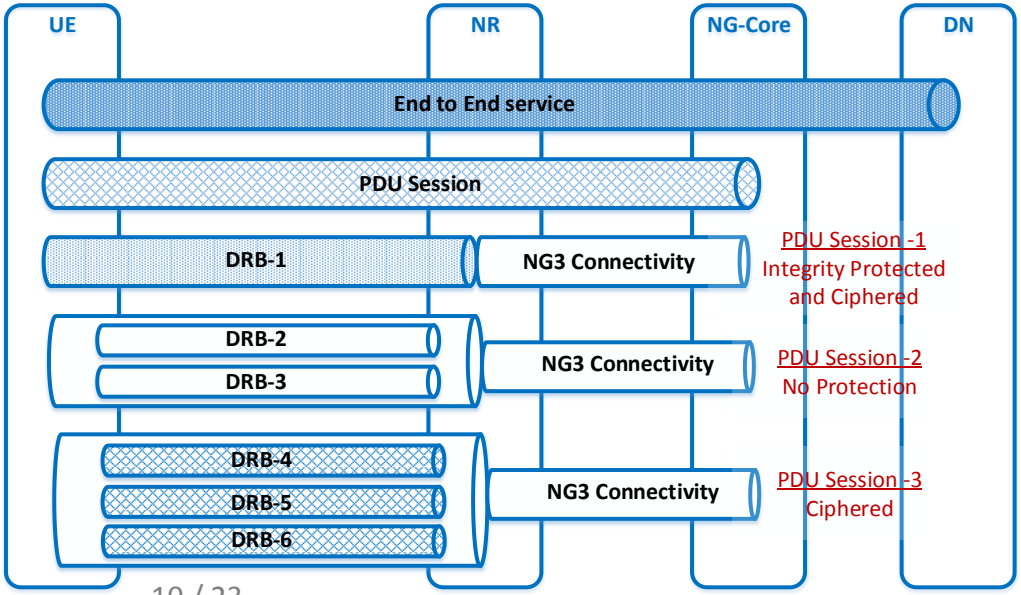
SAMSUNG Research

RAN Security

User Plane Security Aspects

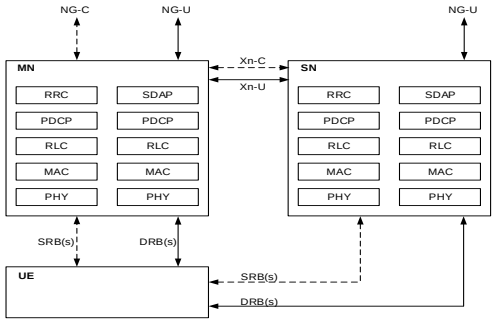
User Plane security between UE and network

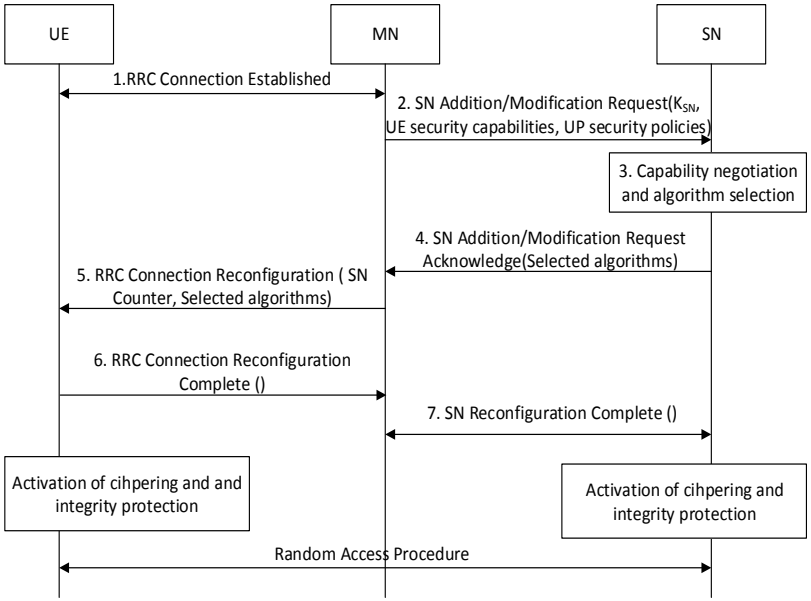
- **UP integrity/encryption** is mandatory to support and **optional to use**
  - Shall be determined by the network based on network policy.
- **The UP security termination point is in the RAN and located in the PDCP layer.**
  - Agreement should not preclude introducing a ***UP security termination point in the 5G core in phase-2***.
- The system shall determine the UP protection between UE and the RAN protection based on **PDU session**.



RAN Security – Dual Connectivity

Multi-RAT Dual Connectivity (MR-DC) with 5GC





Non-Standalone Architecture

- Similar to LTE Dual Connectivity (E-UTRAN + E-UTRAN)
- NG-RAN E-UTRA-NR Dual Connectivity (NGEN-DC)
  - MN = ng-eNB, SN = gNB
- NR-E-UTRA Dual Connectivity (NE-DC)
  - MN = gNB, SN = ng-eNB
- SN Addition / Modification
  - MN Initiated (Initial offload, Update KSN)
  - SN Initiated (PDCP Count Wrap)

Traffic protection between UE and SN

- KSN to establish RRC security context
- TS 33.401 (SN=ng-eNB), TS 33.501 (SN=gNB)
- MN generates KSN (KDF (Kng-eNB/KgNB, SN Counter))
- SN Counter
  - Freshness parameter (To UE for KSN derivation)
  - Increase for every new KSN generated.
- Integrity protection of the user plane whose PDCP terminates on the SN is not supported

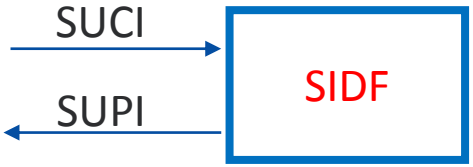
SAMSUNG Research

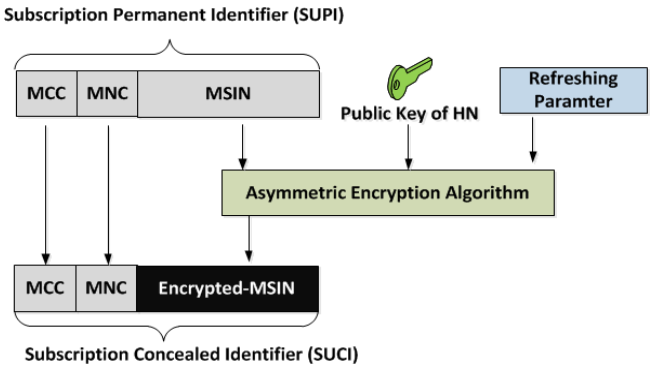
User Privacy

Subscriber Identifier Privacy

Concealing permanent or long-term subscription identifier (SUPI)

- SUPI privacy protected over-the-air using SUCI.
- Privacy preserving solution for a 5G core network (both 3GPP and non-3GPP access).
- Subscription identifier privacy shall be based upon HN asymmetric key solution in Rel-15.
- Subscription Concealed Identifier (SUCI) includes partially encrypted SUPI data
- The Subscription Identifier De-concealing Function (SIDF) is defined for obtaining SUPI out of the SUCI.
- SUCI included in NAS messages
  - Registration request to a network without 5G-GUTI
  - Response of Identity Request message from network
- SUCI in “null-scheme”
  - Unauthenticated emergency session and no 5G-GUTI to choose PLMN
  - Home network configures to use “null-scheme”
  - Home network has not provisioned public key
- 5G-GUTI – Subscription temporary identifier (From serving network after NAS security activation)





SAMSUNG Research

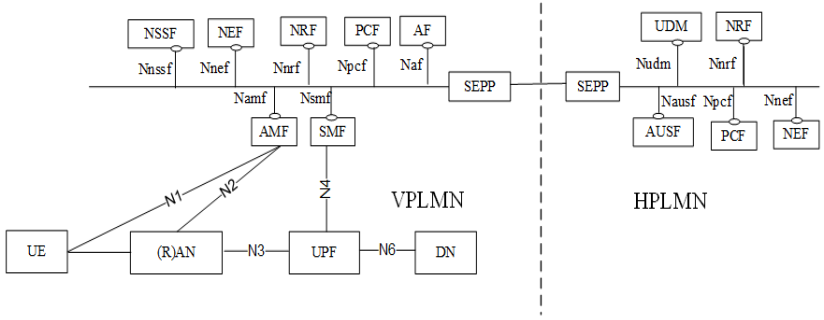
API Security

SBA Security Architecture and Key decisions

SAMSUNG Research

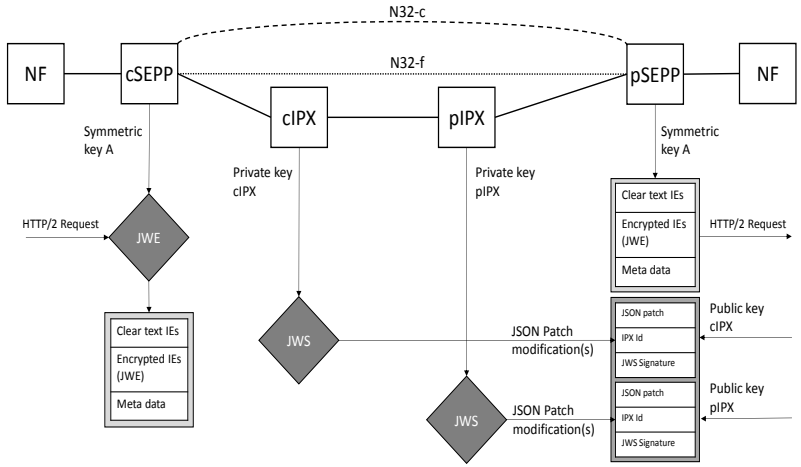
- NF Service access authorization (NF-consumer to obtain service from NF-producer)
- Transport layer security may be used between two NFs within an operator domain

- Application layer security
  - Between two NFs residing in different PLMNs
  - To protect JSON based information elements
  - Implemented at the network edge in SEPP (Security Edge Protection Proxy)
- HOP by HOP Security (NF-SEPP-IPX-SEPP-NF)
- NOT Supported - IPX operators to modify/update/add HTTP headers or payload
- Need to support service discovery across PLMNs (Topology hiding by SEPP)
- Protection for SBA traffic will include the following:
  - Integrity protection of ALL IE's
  - Confidentiality protection (Encryption) of Authentication vectors and other sensitive information like IMSI etc.



Authentication and Authorization (NF-NF, NF-NRF)

(TLS, HTTP/2, RESTFul API, JSON (IEs), OAuth)



N32 – Application Layer Security

API Security (3GPP Northbound API)

Common API Framework (3GPP Northbound API) Security

CAPIF-1/1e Security

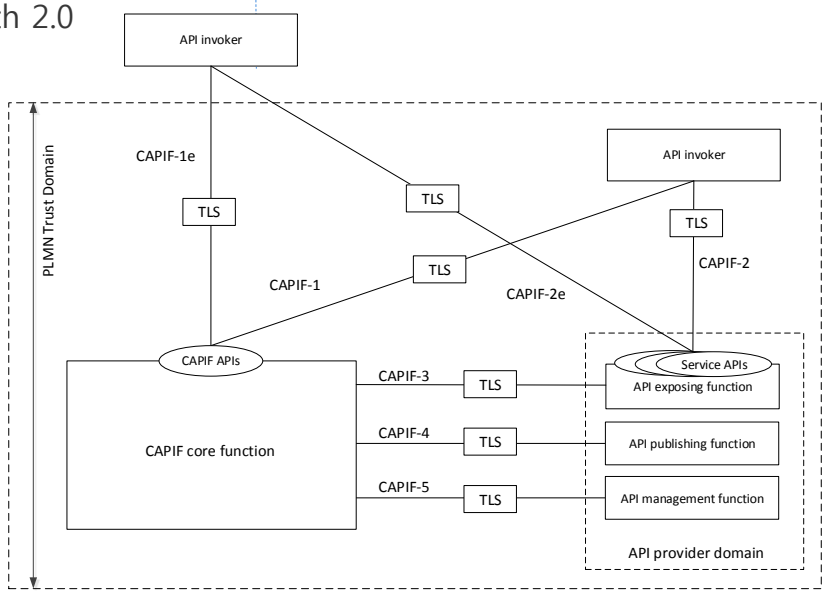
- TLS (Certificate based mutual Authentication)
- On demand Security for CAPIF-2/2e (API Invoker preference, CCF decision)
- Enables support of multiple security methods for multiple API Exposing Functions.
- API Invoker onboarding results in certificate from CCF or 3rd Party certificate.

CAPIF-2/2e Security

- Security Methods
  - TLS-PSK (CAPIF-1/1e Security bootstraps)
  - TLS-PKI (Direct)
  - TLS-OAuth 2.0

CAPIF–3/4/5 Security

- TLS (Certificate based)
- TS 33.310 profiles



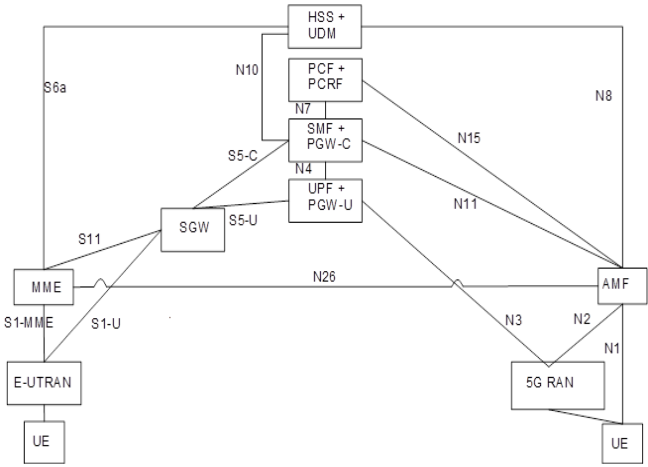
SAMSUNG Research

Security for Interworking

Security for Interworking with 4G

- **N26**
  - Inter-CN interface between the MME and AMF.
  - For context transfer between the source and target network.
  - New keys are generated (obtained via N26)
  - Avoid authentication when moving into a target network.

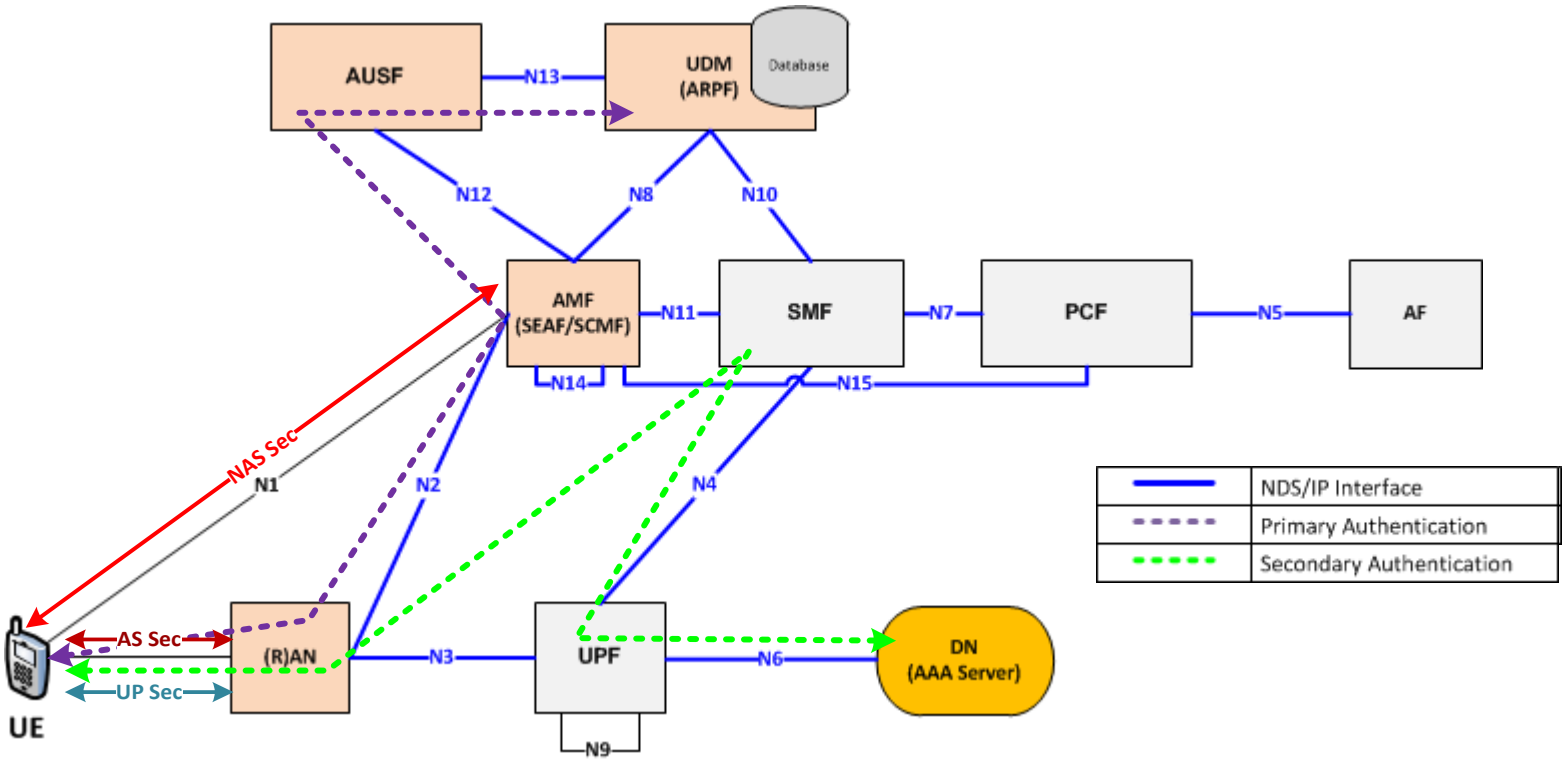
- A UE that supports both 5GC NAS and EPC NAS can operate in:
  - Single-registration mode: UE either connects to 5GC or connects to EPC. Mandatory for UEs that support both 5GC NAS and EPC NAS
  - Dual-registration mode: UE can independently register with 5GC and EPC.
- Security impacts during mobility using N26
  - Idle-mode mobility between EPC and 5GC
  - Connected-mode mobility (inter-system handover) between EPC and 5GC
- It‘s mandatory in phase 1 to support interworking with a legacy MME
  - Legacy MME sees N26 as a S10 interface, does not know that it is talking to a AMF on the other side
- No security impact for mobility scenarios without N26
  - In principle, lack of N26 means that the UE has to register with the target network with full authentication and key establishment.



SAMSUNG Research

Summary

Snapshot on 5G Security



4G vs 5G Security Aspects

Security Feature	4G	5G
Access Agnostic Authentication	Not Access agnostic	Unified Authentication for all access
Authentication Credentials	Only AKA credentials	AKA credentials Or Certificate for IoT/Private networks(optional , informative annex)
Authentication Protocol	EPS-AKA over 4G NAS	5G-AKA over 5G NAS or EAP-AKA'/EAP-TLS over 5G NAS
Security Platform for Authentication Credentials	UICC	UICC or Non-removable UICC
Home Control for authentication	Not Supported	Supported (HPLMN involves in Authentication and holds a key)
Integrity Protection of UP traffic	Not Supported	Supported (optional to use)
Security of UP traffic	Enabled/disabled for all DRBS	Per PDU session based Selective Protection
Subscription Identity protection	IMSI is not protected, if there is no security context	SUPI is always protected using Asymmetric Cryptography
Network Domain Security	IPSec (Point-to-Point Architecure)	TLS/Application layer Protection (SBA)
Steering of Roaming	OTA based (optional to support)	New native solution using control plane (mandatory to implement and optional to use) + OTA based (optional to support)
Protection of North bound APIs	Fragment security mechanism	Common API Framework Security
Security Visibility	Visibility to User	Visibility to User and Application (e.g Via API), per PDU session granularity

3GPP Security – Approved Release-16 Studies

Title	Unique Acronym
Study on evolution of Cellular IoT security for the 5G System	FS_CIoT_sec_5G
Study on Enhanced network slicing	FS_eNS-SEC
Study of KDF negotiation for 5G system security	FS_5GS_KDF
Study on 5G security enhancement against false base station	FSFBS
Study on security for 5G URLLC	FS_5G URLLC_SEC
Study on security for 5GS enhanced support for vertical and LAN services	FS_Vertical_LAN_SEC
Security Assurance specification for 5G	SCAS_5G
Study on security of enhancement of the 5G location services	FS_eLCS-Sec
Study on SECAM and SCAS for 3GPP virtualized network products	
Study on Security Aspects of the 5G Service Based Architecture	FS_SBA_Sec
Study on authentication and key management for applications based on 3GPP credential in 5G	FS_AKMA
Study on the security of the Wireless and Wireline Convergence for the 5G system architecture	FS_5WWC_SEC
Study on 256-bit algorithms for 5G	FS_256_Algo
Study on Security Aspects of PARLOS	FS_PARLOS_Sec
Mission critical Services Security Enhancements	MCXSec
Study on security aspects of single radio voice continuity from 5G to UTRAN	FS_5G_UTRAN_SEC

More Release-16 studies expected based on SA2 and SA6 conclusions

SAMSUNG Research

धन्यवाद!

Contact: Narendranath Tangudu
Email ID: n.tangudu@samsung.com