5G Security: Standard and Technologies

Dr. Haiguang Wang, Senior Researcher， Huawei International

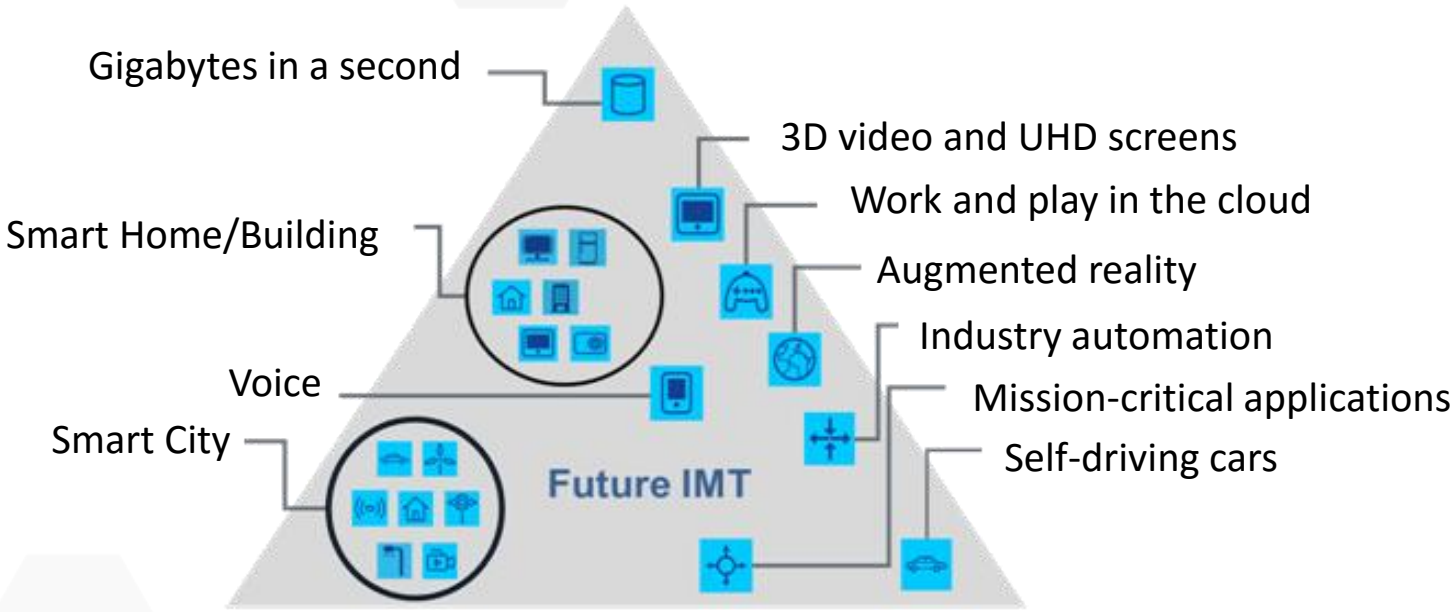
Oct 18, 2017

www.huawei.com

Contents

5G: Diverse Use Cases

Enhanced Mobile Broadband

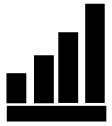
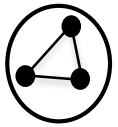


Massive Machine Type Communications

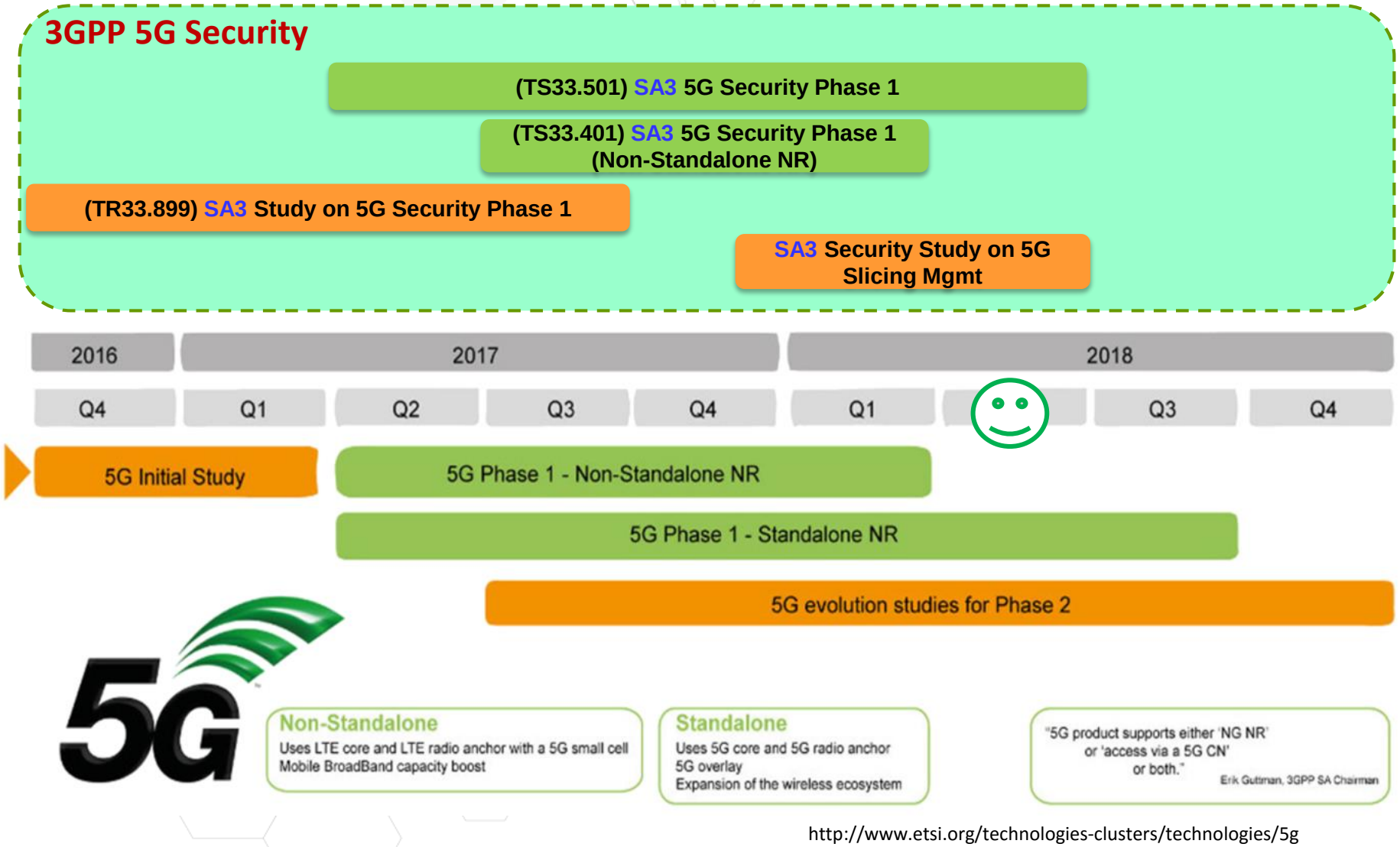
Ultra-Reliable and Low-Latency Communications

Source: ITU-R M.[IMT.VISION]

5G: Stringent Requirements

	Latency	Throughput	Connections	Mobility	Flexibility
5G	1 ms end-to-end latency	10 Gbit/s per connection	1M per square kilometer	500 km/h for express trains	Slicing Flexible and on demand
					
	30–50x	100x	100x	1.5x	NaaS
LTE	30–50ms	100 Mbit/s	10,000	350 km/h	Inflexible

5G Security Timelines in 3GPP



http://www.etsi.org/technologies-clusters/technologies/5g

3GPP SA3 5G Security

1. **TR 33.899**
   Study Item: Technical Report on 5G Security Architecture and Functions, Frozen
2. **TS 33.401**
   Work Item: System Architecture Evolution (SAE); Security architecture
3. **TS 33.501**
   Work Item: Standard on 5G Security Architecture and Functions
4. **NEW TR**
   Study Item: Network Slicing Security Management， SBA，IPX

5G Security Technologies

	TS 33.501
1	**Security Architecture**
2	**Security requirement and features**
3	Security procedure between UE and 5G Network Functions
4	Security for non-3GPP Access
5	Security of interworking
6	Security procedures for non-service based interfaces
7	Security aspects of IMS emergency session handling
8	Security procedures between UE and external data networks
9	Security aspects of network exposure function
10	Service Based Interfaces
Annex	For key derivation and authentication procedures

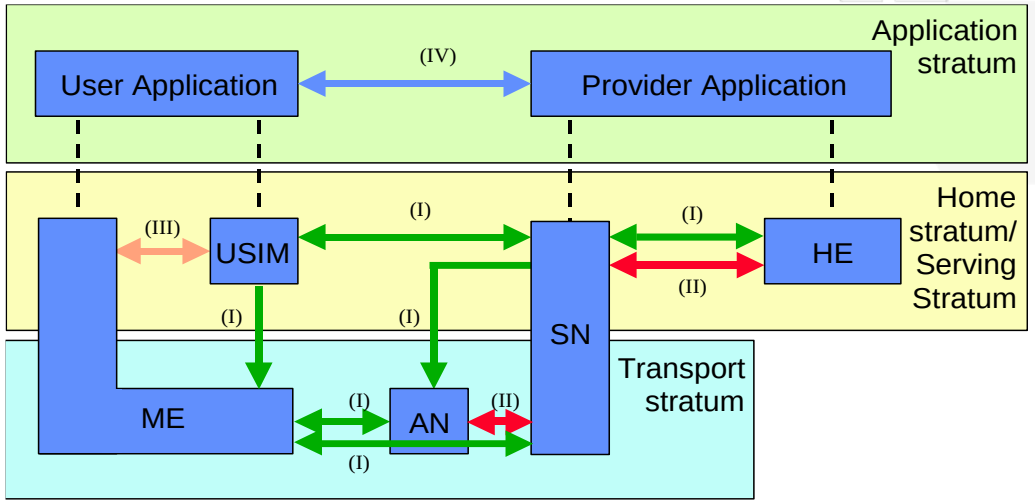
Technologies Specified as of March 2018

- Security architecture
- Primary authentication
  - Unified authentication framework with EAP support: 5G-AKA and EAP-AKA’, EAP-TLS
- Secondary Authentication
  - Authentication with DN: EAP methods
- Security context management
- Mobility support
- Multiple registration
- Non-3GPP access
- Security for Service based architecture
- Privacy Protection
  - Public key encryption of subscription permanent identifier (SUPI)

Contents

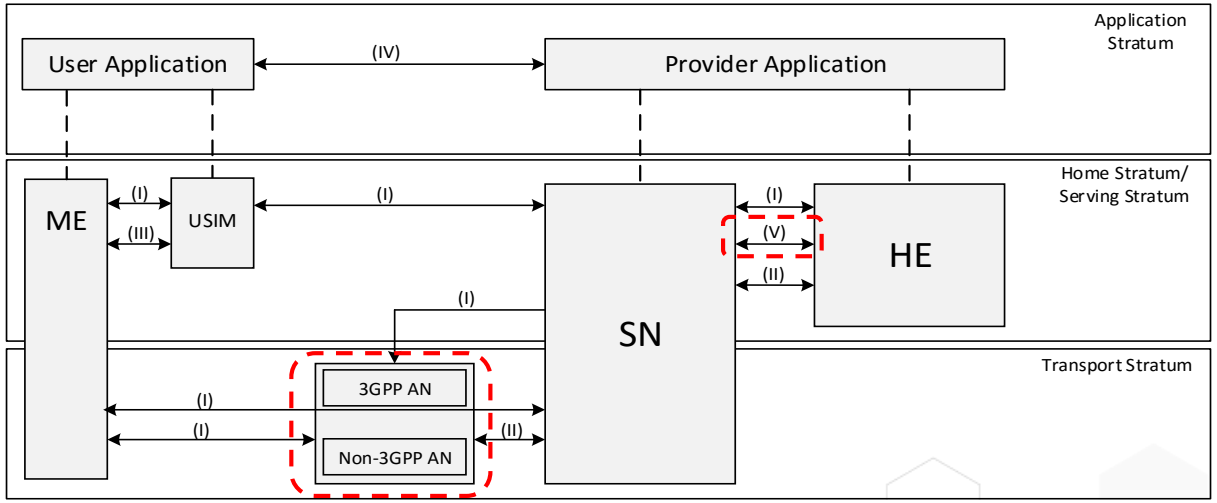
Security Architecture

4G Security Architecture (TS 33.401)



I. Network access security (I)
II. Network domain security (II)
III. User Domain Security (III)
IV. Application domain security (V)
V. Visibility and configurability of security (VI)

5G Security Architecture (TS 33.501)



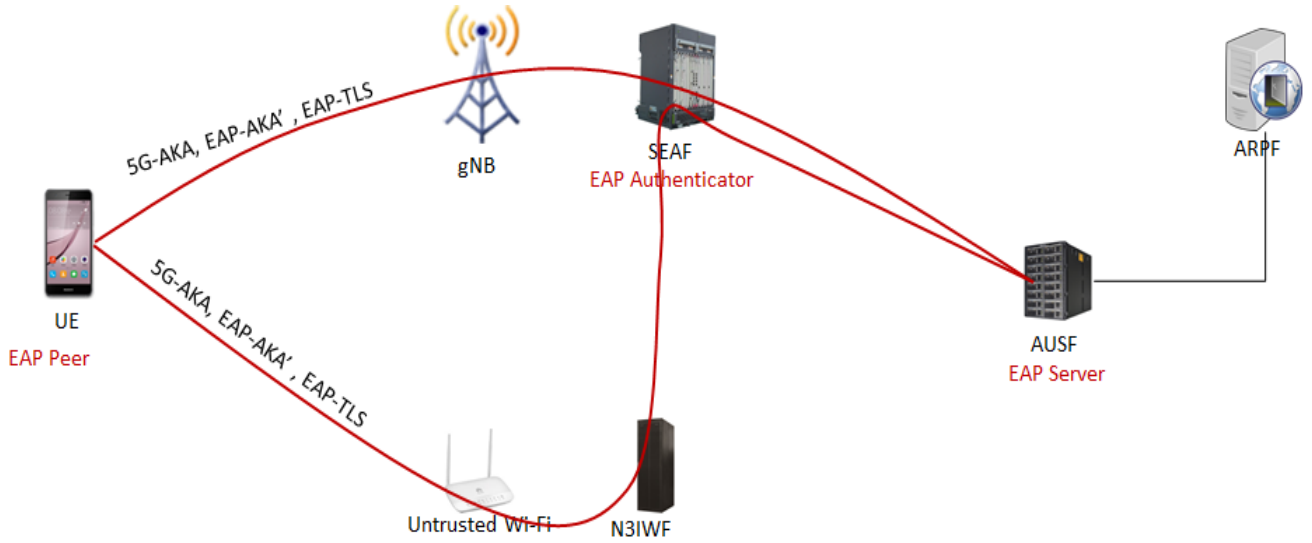
I. Network access security (I)
II. Network domain security (II)
III. User Domain Security(III)
IV. Application domain security (V)
V. SBA domain security (V)
VI. Visibility and configurability of security (VI)

Enhancement

1. AN : 3GPP and non-3GPP access network treated more equally in access network.
2. SN←→ HE(V) : interface for Service-based Architecture

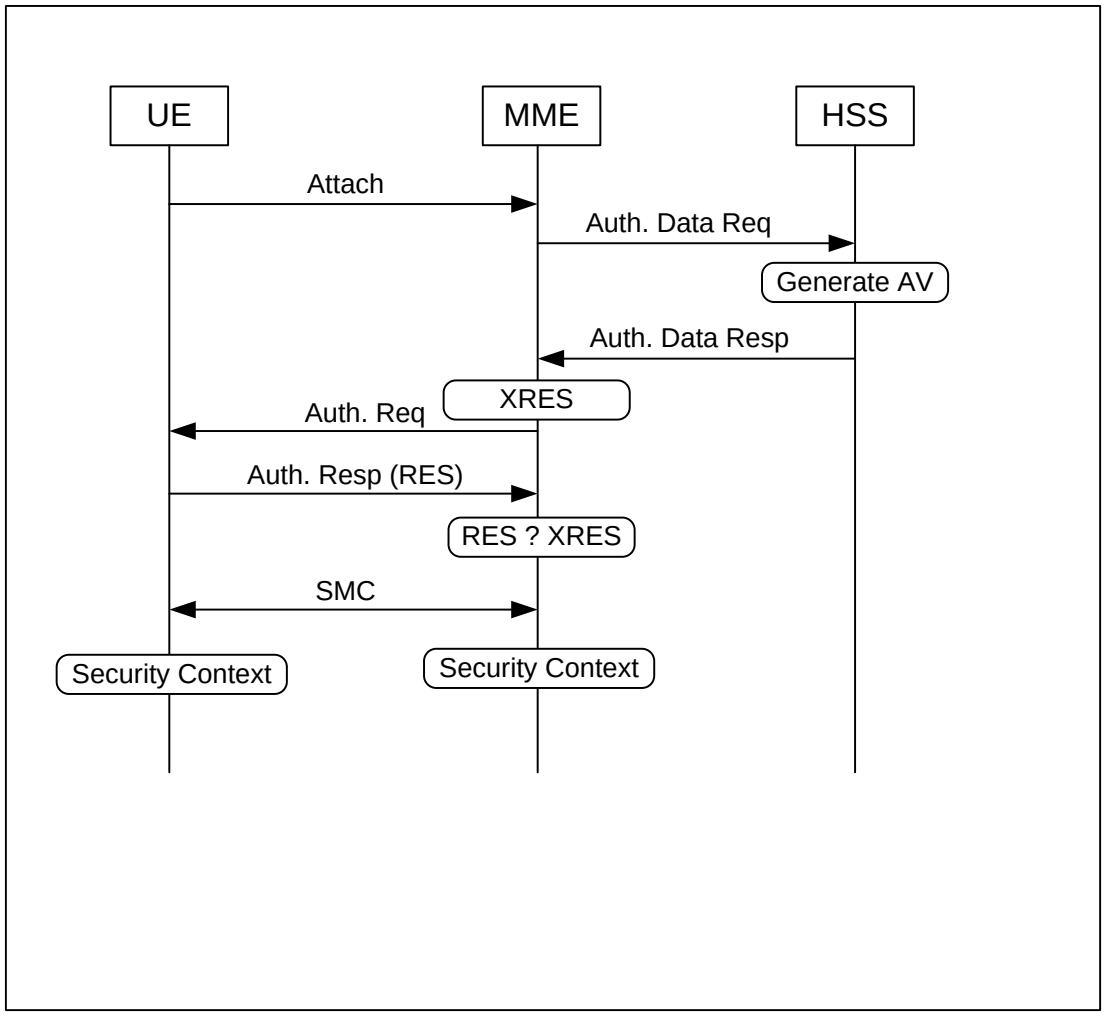
Unified Authentication Framework

- Build up an unified authentication framework for different access technology, enable security context sharing among different access technology:
  - ARPF: credential repository
  - AUSF: authentication server
  - SEAF: security anchor
  - EAP framework are supported, a critical step for 5G to become an open network platform
  - EAP extended type, EAP-5G, is used to carry the NAS signaling over untrusted N3GPP link
    - EAP-5G is an vendor specific message format to carry NAS signaling between UE and N3IWF.

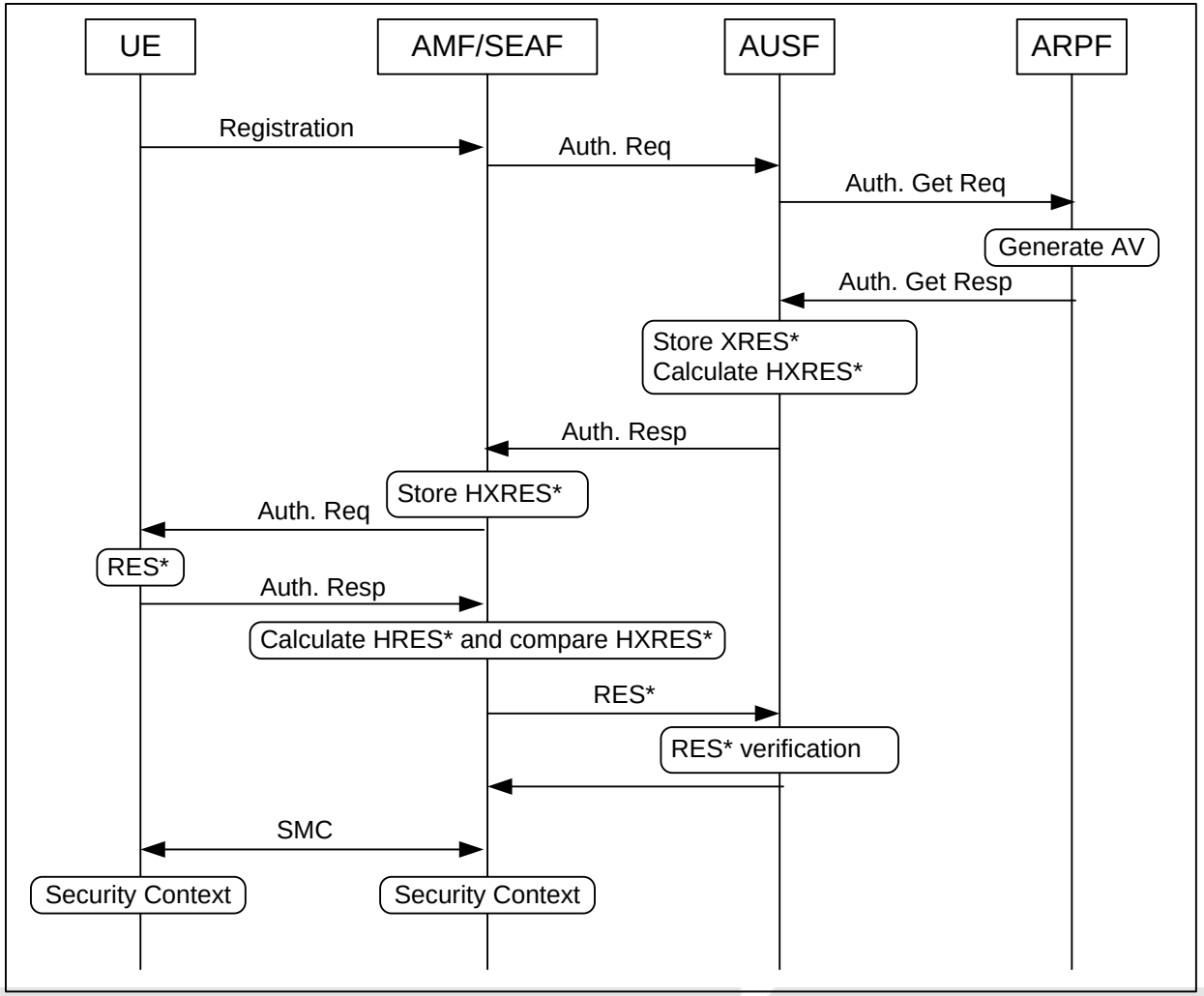


Authentication Protocols： EPS-AKA vs. 5G-AKA

4G: EPS-AKA



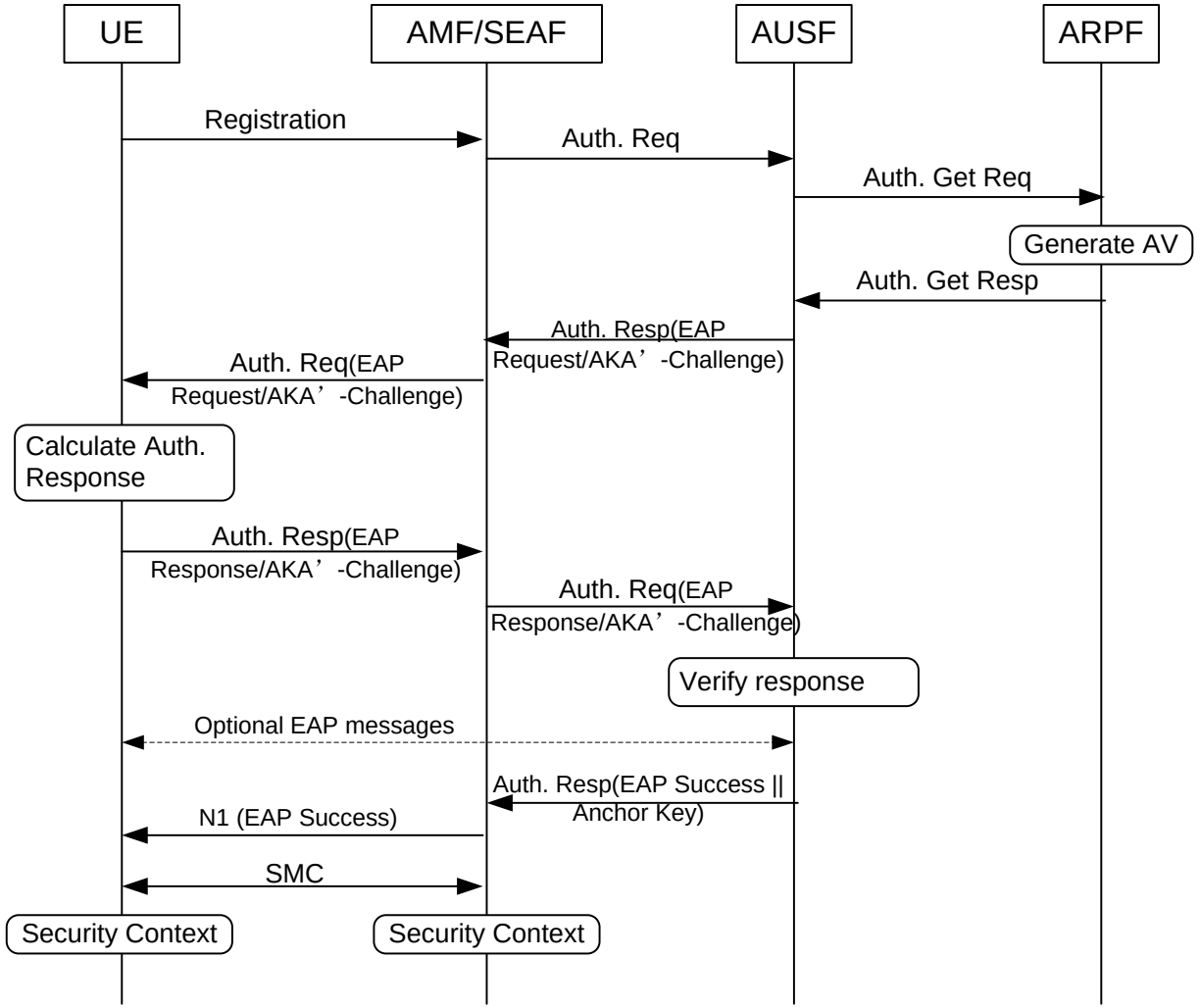
5G: EPS-AKA



EAP-AKA’ in 5G

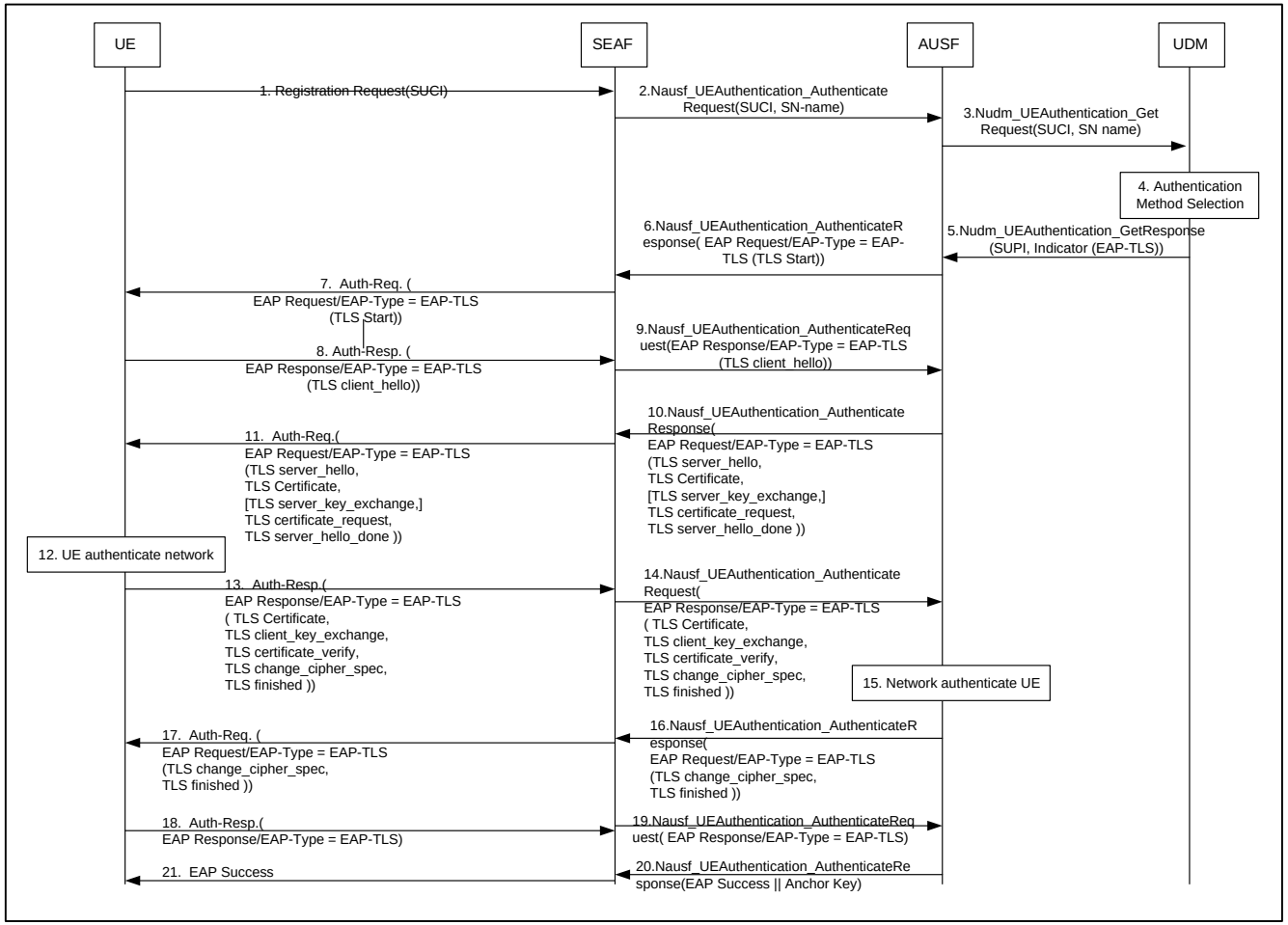
Basic procedure:

1. UE send registration request to AUSF and ARPF
2. ARPF decide authentication method
3. AUSF start EAP-AKA’
4. UE and AUSF perform mutual authentication
5. AUSF send anchor key to SEAF/AMF for further key derivation
6. UE derive keys for communication.



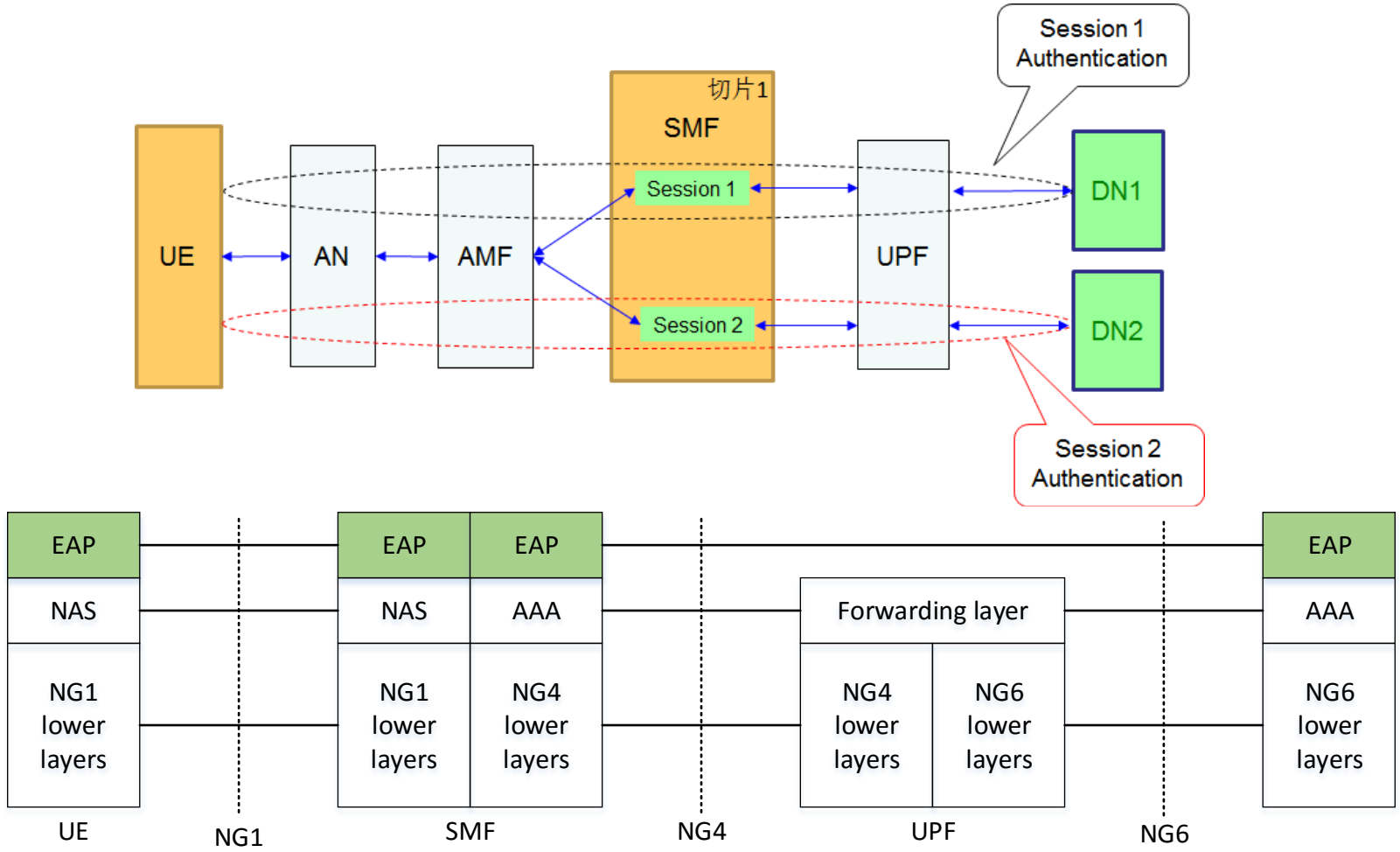
Authentication for Private and IoT Networks

- **5G support to use EAP methods other than EAP-AKA' for private and IoT networks.**
  - An example procedure for EAP-TLS using with 5G authentication framework is given.
  - Key derivation and privacy protection issues are similar to EAP-AKA'



Secondary Authentications

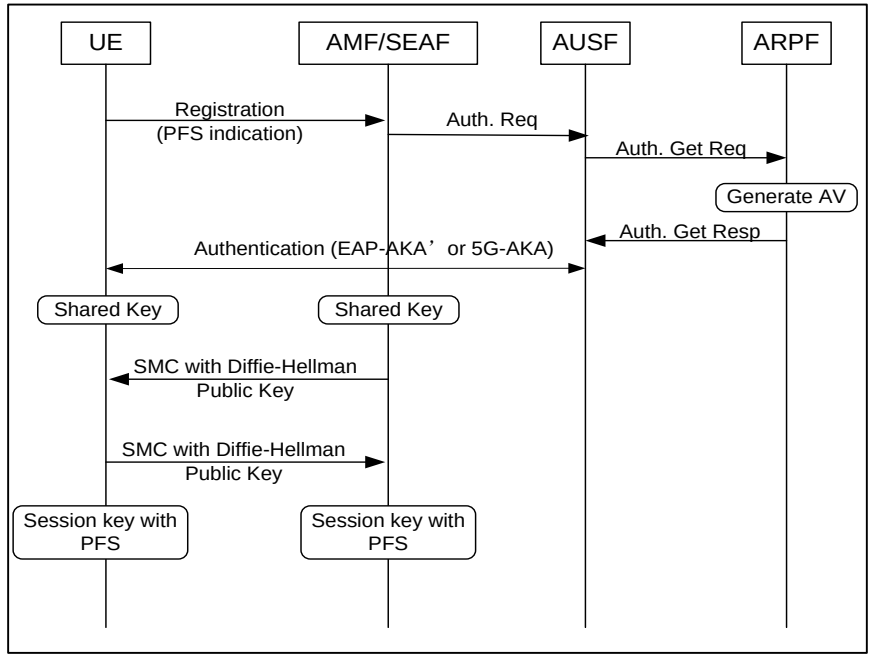
Secondary authentication is used by UE authenticate with outside data network and get authorization on establishing data path from operator network to outside data networks.

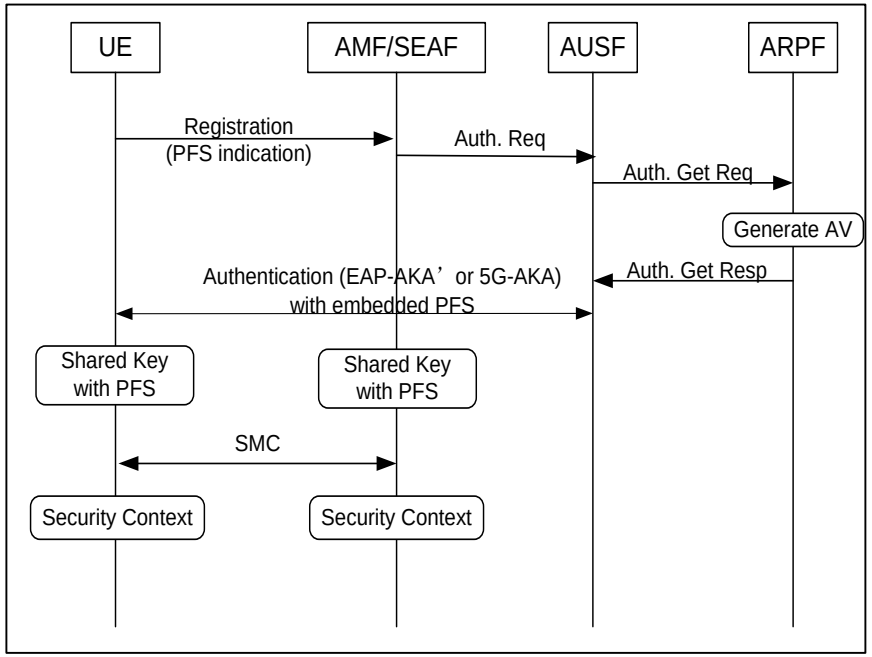


Long Term Key Leakage and Perfect Forward Secrecy for 5G

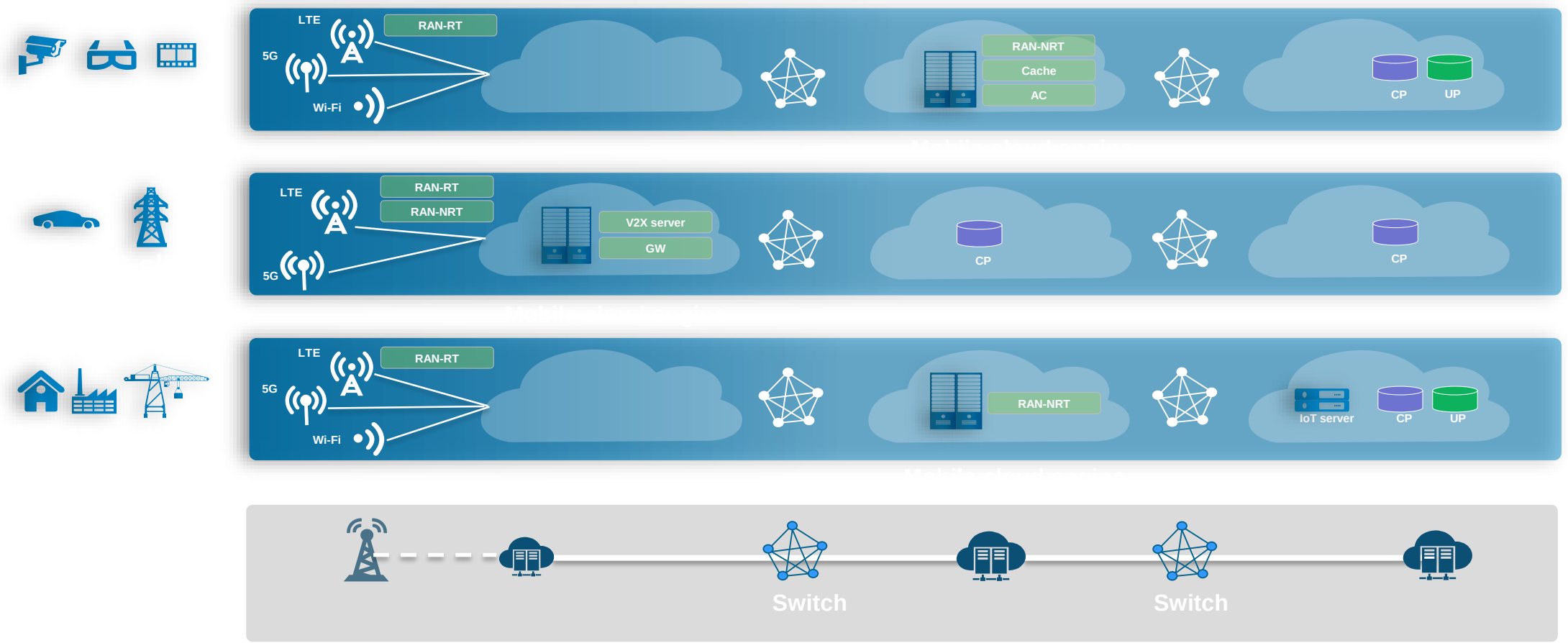
- **According to the study of TR 33.899, Long Term Key might be leaked due to following reasons:**
  - hacking at the factory (SIM vendor or subscription manager) where Ki is generated
  - hacking of the communication channel over which Ki is transported from SIM vendor or subscription manager to mobile operator
  - hacking into the mobile operators
  - insider attack (mobile operator or SIM vendor)
  - local attack (e.g. side channel) on the SIM card in the supply chain
  - local attack (e.g. side channel) on the SIM card while temporarily "borrowed" from the customer

Build in Perfect Forward Secrecy for 5G networks





5G Network Architecture: A View from Slicing



Industry Defined Network Slicing

Service oriented cloud-formation

Internet architectural operation

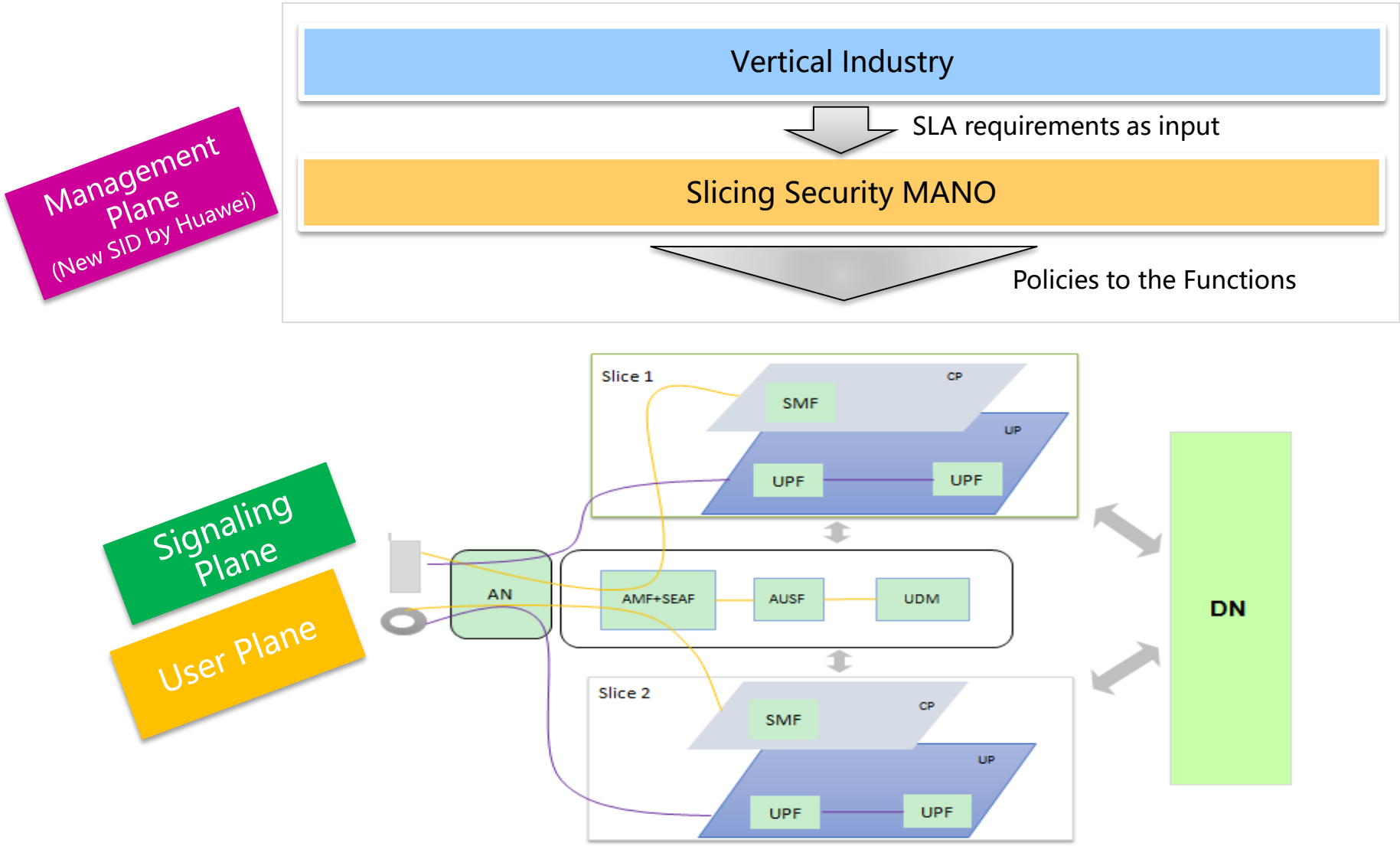
Slice security

Management Plane : Configure and manage the slicing security policies for MANO.

A new Study Item proposed by Huawei was approved in August 2017. The study results will be captured in a separate Technical Report.

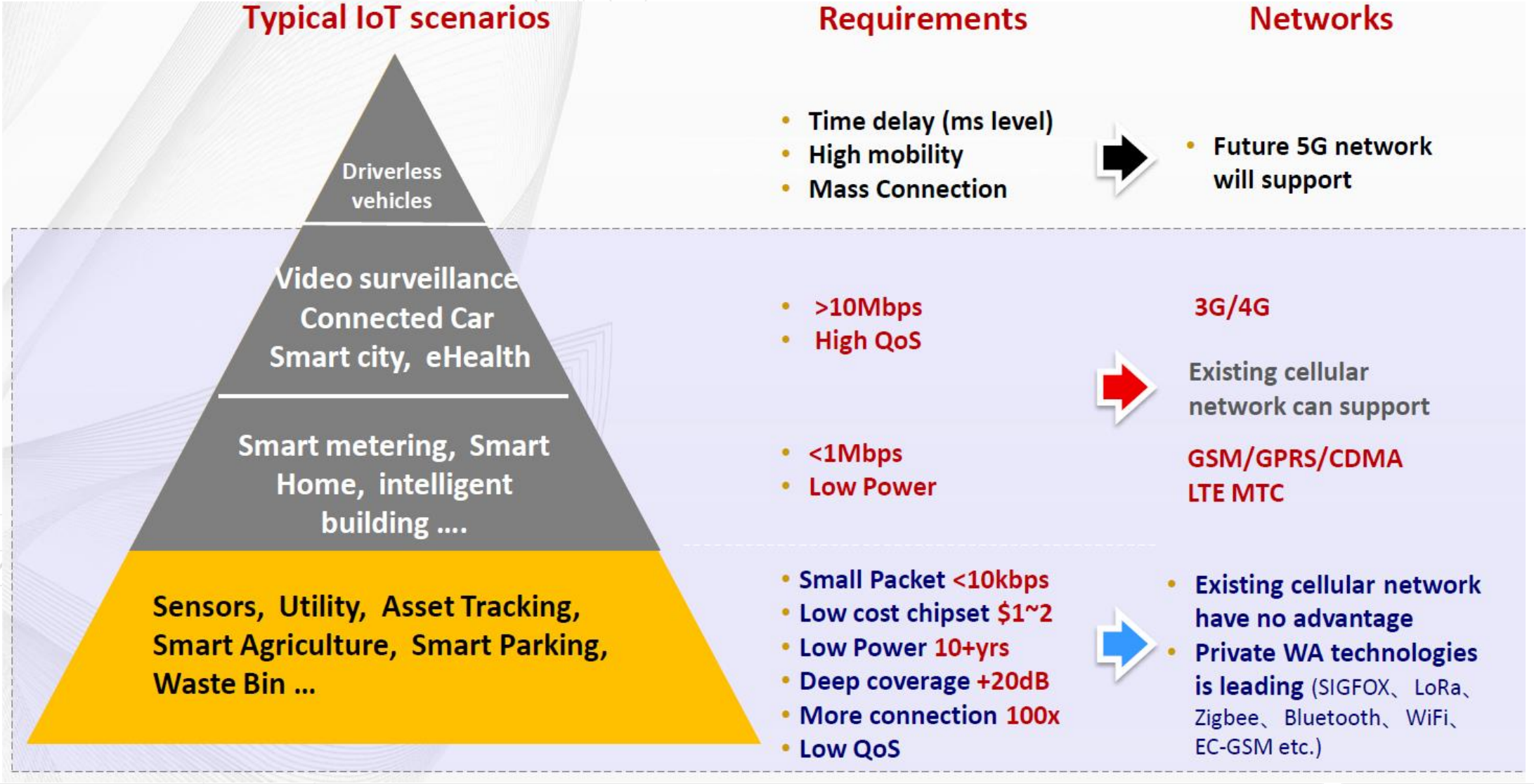
Signaling Plane: Execute the slicing accessing security procedure and release the security enablers

User Plane: Execute the protection solution by analyzing the flowing map of data.



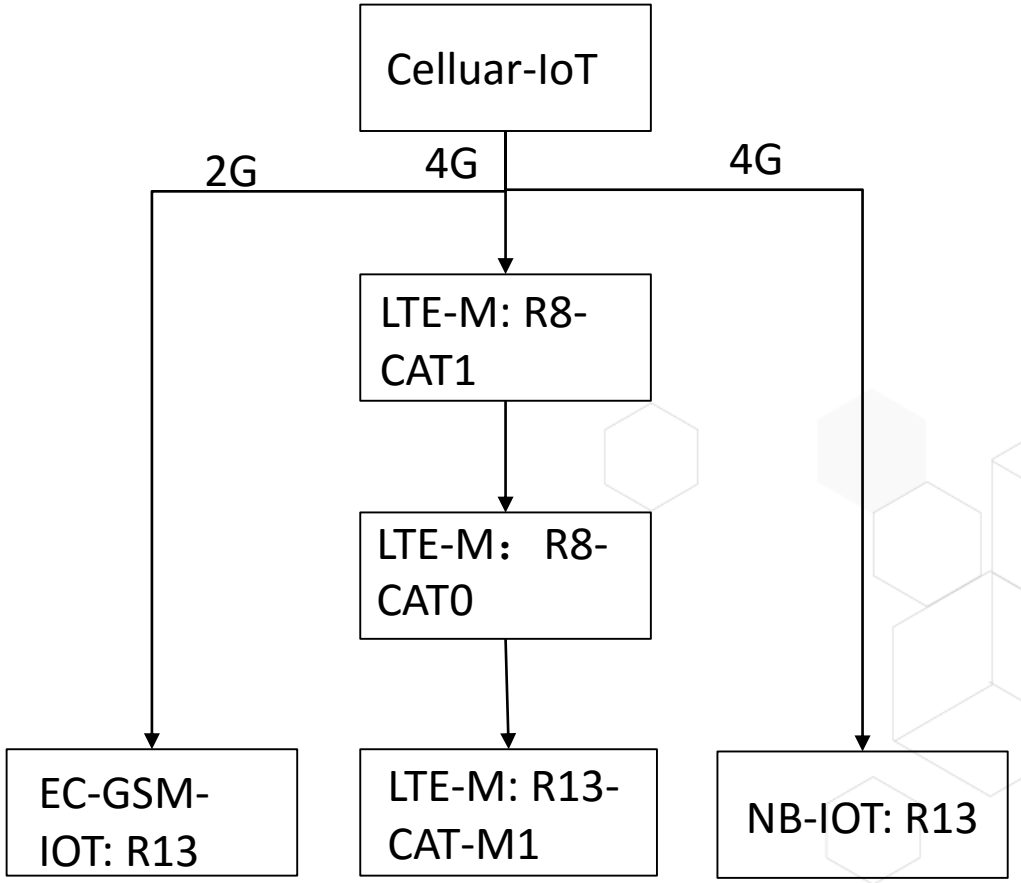
Contents

IoT Usages Scenarios and Its Requirement on Cellular Networks



Evolution of Cellular IoT in the Past a Few Years

	LTE Rel-8 Cat-1	LTE Rel-8 Cat-0	LTE Rel-13 Cat-M1	NB-IoT Rel-13	EC-GSM-IOT Rel-13
DL Peak Rate	10 Mbps	1 Mbps	1 Mbps	~0.2 Mbps	~0.5 Mbps
UL Peak Rate	5 Mbps	1 Mbps	1 Mbps	~0.2 Mbps	~0.5 Mbps
Duplex	Full Duplex	Full/Half Duplex	Full/Half Duplex	Half Duplex	Half Duplex
Channel Bandwidth	20 MHz	20 MHz	1.4 MHz	0.18 MHz	0.2 MHz
Tx Power	23 dBm	23 dBm	23 dBm	23 dBm	23/33 dBm
Complexity	100%	50%	20-25%	10%	unkown



Communication Networks are Facing Restructuring, and New Principles for Security Design are Expected

Communication Networks

Service Support：
Network slicing support vertical industry customize the application and simplify the deployment

Network Coverage：
Fully exploit the potentials of cellular and short range communication networks, and build a new network with properties of low power, low cost and deep coverage

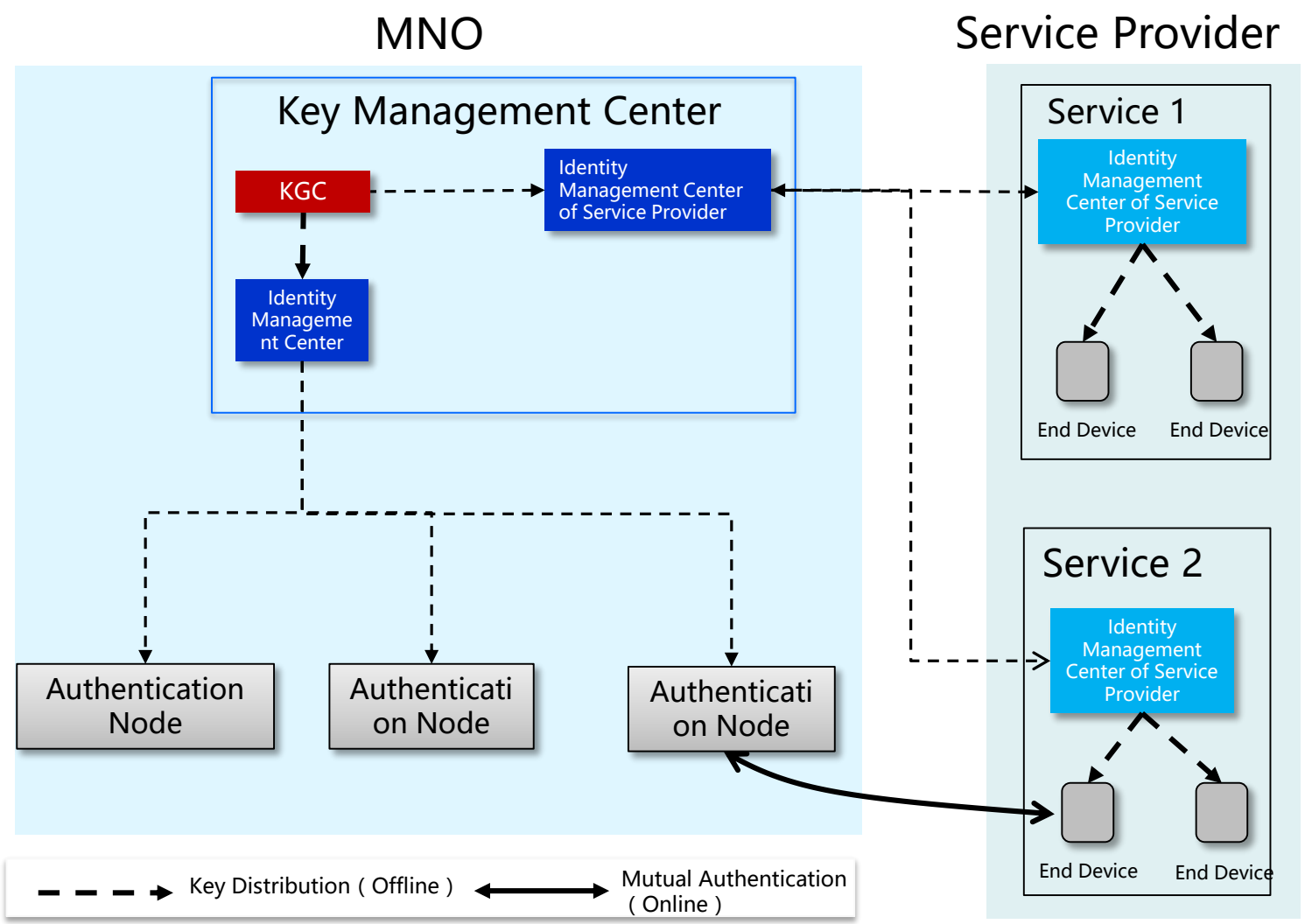
Network Access：
Massive number of devices with features of random network access, flexible online schedule, and fast deployment, requiring network provide capability of fast discovery and association, and extremely simplified network deployment procedure. ***Like V2V connection.***

Security

Light Weighted Architecture
Lower down the key management cost, shorten the authentication chain.

Agile Security Association
Avoid the bottleneck caused by centralized authentication node.

Distributed Authentication Method—Example

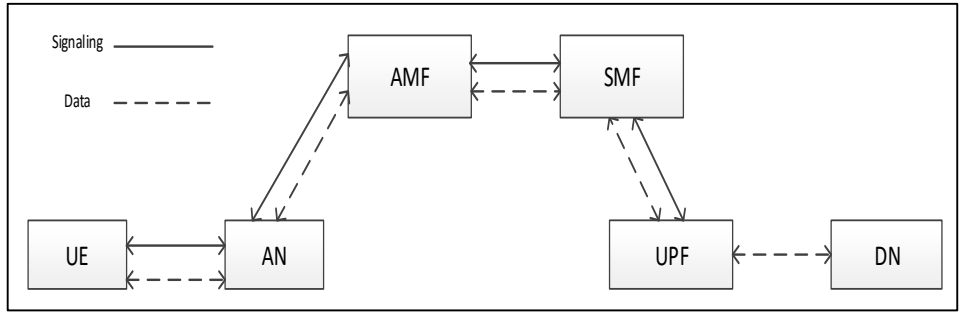


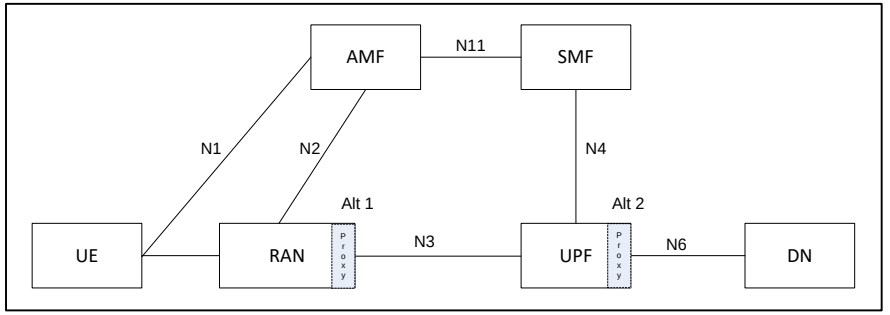
- Key Management Center
  - Key Generation Center: Generates keys for network elements and end device; Do not involve in the authentication procedure; Do not storage keys for network elements and end device
  - ID Management Center of Service Provider: Manage the identity and distribute key for its users
  - Network Element Identity Management Center: Distribute key for network elements
- Authentication Node: Authentication node at the network side; store the key of network element; perform mutual authentication with device
- Identity Management Center of Service Provider: Belongs to each vertical; Manage vertical its own devices identity and keys, including key distribution and etc.
- End Device：Store its own key; perform mutual authentication with the network

Small Data Protection for Massive IoT Devices

- **5G networks need to support massive IoT devices, i.e. 1 million devices within 1 km^2.**
  - Many devices sends data with very low frequency
  - Communication context, including security context, may cause heavy system resource pressure for core networks nodes. This may increase both CAPEX and OPEX
  - Both network architecture and security group need put in effort to solve the issue.

Example Solutions: data transmission



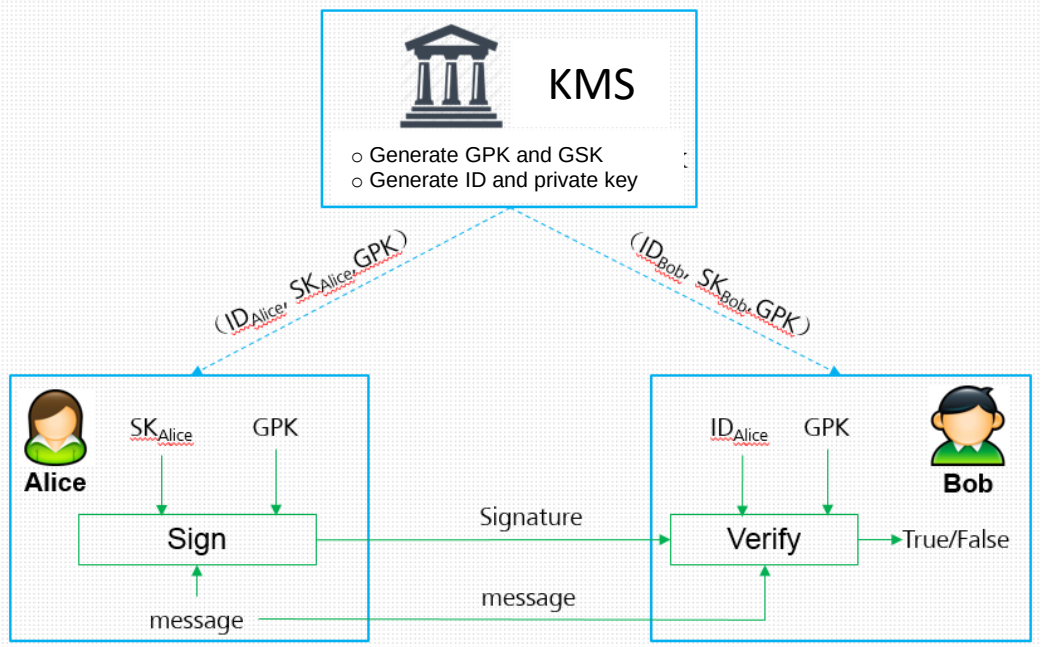


Security ?
Legacy Method or New?

Identity-Based Cryptography, IBC

- IBC(Identity-Based Cryptography):
  - Includes IBS and IBE；
  - Each user has its own public and private key pairs, and its public key is its own identity, such as Email, Mobile Number;
  - User's private key is generated by PKG based on User's ID and PKG's Global Secret Key (GSK);
  - The signing procedure do not involve the PKG；To verify the signature, we only need the signature, message, id, and the Global Public Key (GPK)
- Difference between PKI and IBC:
  - In PKI, the public key of a user is a random sequence, which needs the CA issuing a certificate to the user to prove the public key indeed belongs to the user；the certificate needs to be verified during the signing and encryption procedure
  - A classic algorithm for PKI is RSA, which is developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977, widely used 20 years later

ID-based Signature Framework



IBS is first proposed by Adi Shamir in 1984

In 2001，Boneh and Franklin proposed bi-linear map。In 2002，Hess designed the first IBS based on a bi-linear pariing.

Bellare proposed a transformation method from normal identity based algo. to IBS.

1984 2001-2002 2004

Progress on Using IBC in IoT Networks

- **3GPP**
  - An open EAP authentication framework with EAP-TLS supporting
- **IETF**
  - 2017.7: Amend TLS with IBC public key
  - 2018.3: A second draft has been submitted to TLS group
- **ITU-T SG-17**
  - 2017.9: new work item on x.ibc-iot
    - China Telecom, Huawei etc.
    - With Support from CMCC

Contents

Summary

- The first phase of 5G security standard is approaching its closing stage and technology details are available in TS 33.501. It not only inherits some good security features from previous generations, but also provide some significant new features to make the 5G system more secure and open to meet the new stringent system requirement.

- Comparing to the LTE security standard (TS 33.401), 5G security system provides an open authentication platform with better protection over privacy.

- More advanced security features will be provided in the next phase of 5G standard, including Perfect Forward Secrecy, Credential Remote Provisioning, and possible new authentication and data protection scheme for massive IoT devices.

Security Level:

www.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI