ETSI The Standards People

Security Conference

5G Security in practice and future

Presented by: Rong Wu, Huawei

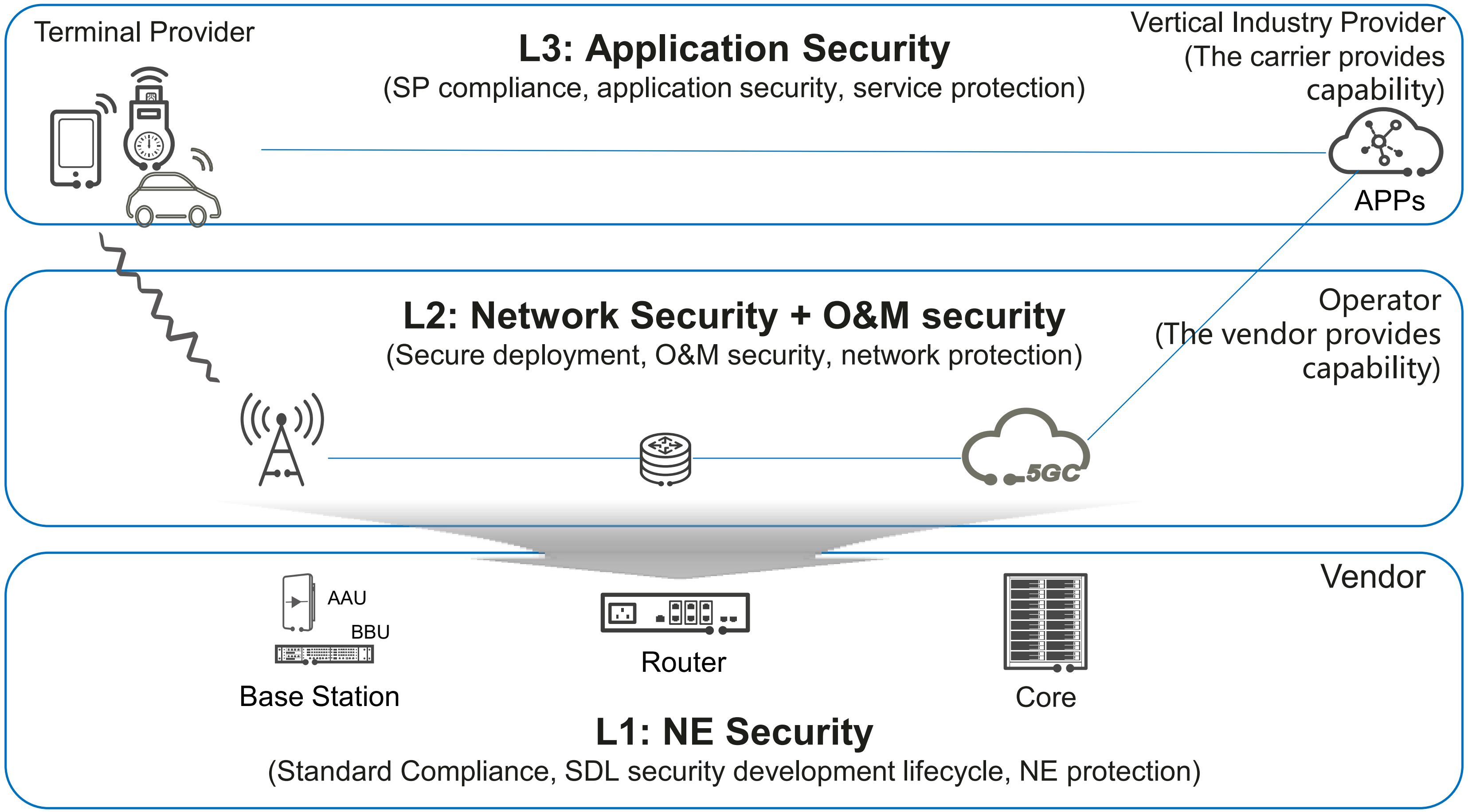
HUAWEI

26/09/2023

Outline

1. **5G Network Security Solution those we have now**
2. 5G Network Security Trend those we expect for future
3. Summary

5G Cyber Security: Layered Models Become Industry Consensus



Terminal Provider
L3: Application Security
(SP compliance, application security, service protection)
Vertical Industry Provider
(The carrier provides
capability)
APPs
L2: Network Security + O&M security
(Secure deployment, O&M security, network protection)
Operator
(The vendor provides
capability)
5GC
Vendor
AAU
BBU
Base Station
Router
Core
L1: NE Security
(Standard Compliance, SDL security development lifecycle, NE protection)

Industry Standards and Methodologies:

IEC62443 IACS, ISO/IEC 27034

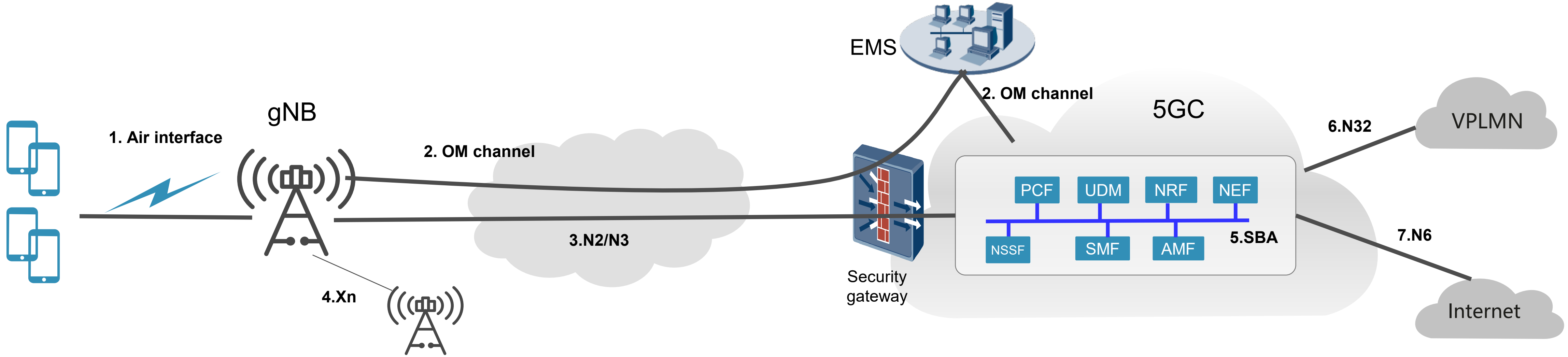
NIST CSF, NCSC CAF, 3GPP SA3, GSMA 5G CKB

ISO19600, NIST SSDF, NIST SP800-160, 3GPP, NESAS/SCAS

The 3-layer security model is widely accepted in telecom industry including 3GPP, 5GPPP etc.

5G security requires ”shared responsibility” among different stake holders.

End-to-end secure transmission ensures data confidentiality and integrity

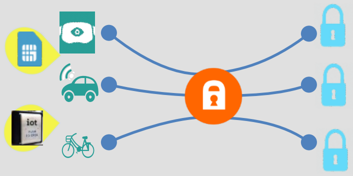
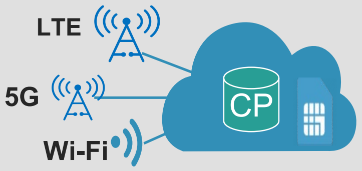
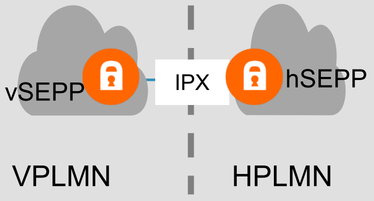
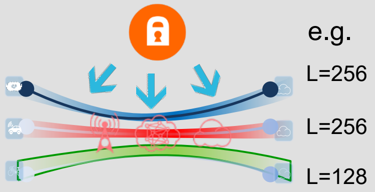


Data communication protection : identity authentication, encryption, integrity protection, and anti-replay

#	Threatened object	Security Solution
1	Air interface	• AES/SNOW3G/ZUC(128bit) encryption and integrity protection
2	O&M channel	• TLS
3	N2/N3 interface	• IPsec (N2/N3), DTLS (N2) • IPSec built-in base station; Security gateways can be deployed on the core network side.
4	Xn interface	• IPsec (Xn-C/Xn-U), DTLS (Xn-C)
5	SBA interface	• HTTPS
6	N32 Roaming Interface	• SEPP: TLS at the transport layer or PRINS at the application layer
7	N6 Internet interface	• Firewalls are deployed to protect against external network attacks.

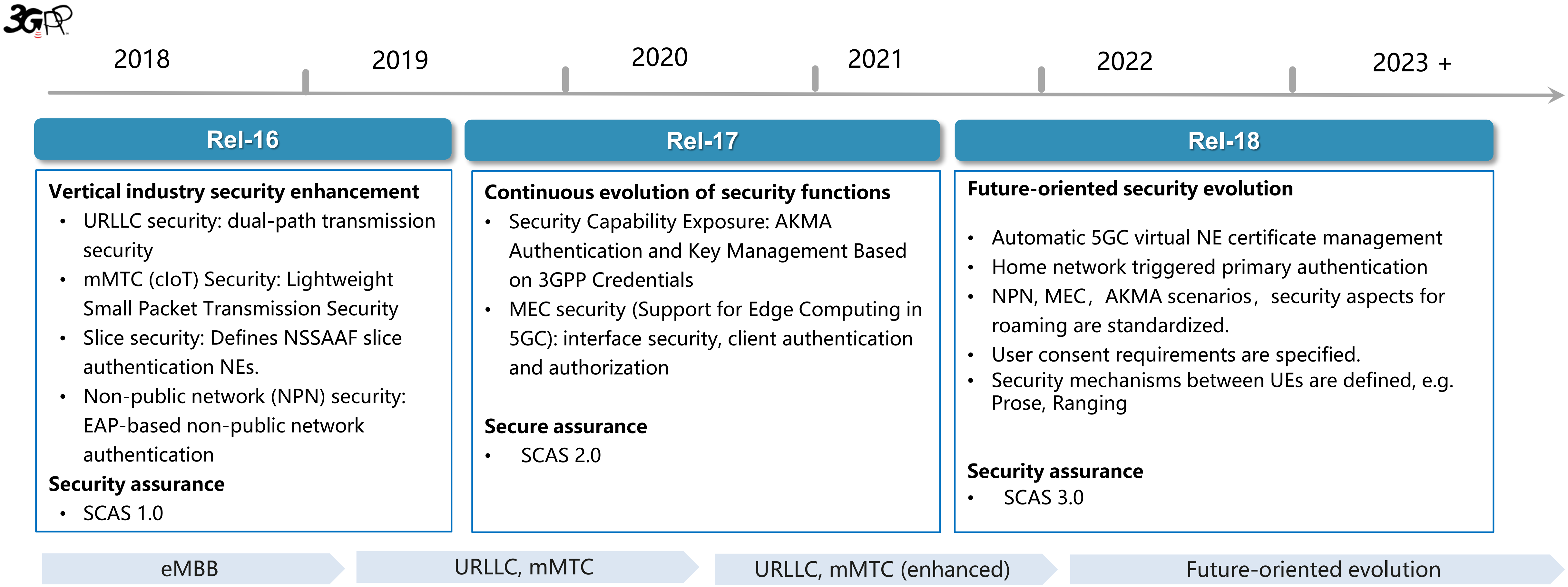
5G standard evolution: 5G Enhances Network Security Capabilities Based on 4G

- The 4G network is based on a series of security solutions and has not been attacked in a large scale in the past 10 years.
- 5G reuses the 4G security architecture and further enhances security for some known risks.

5G	**Better** **Air interface security**	**More Reliable** **User privacy protection**	**Flexible** **Security Policy**	**Unified** **User authentication experience**	**Enhanced** **Roaming security**	**Stronger** **cryptographic algorithm**
	User Plane Integrity Protection 	User privacy protection **SUCI** 	**Subscriber-level** security policy 	**Unified** authentication 	**Roaming** security **SEPP** 	**256-bits** encryption algorithm (**after R18**) 
4G	**Plaintext** transmission of roaming subscriber data	**No** integrity protection for UP	**Plaintext** transmission of IMSI	**Network-level** security policy	**Separate** Different authentication for different access	**128 bits** encryption

HUAWEI

5G standard evolution: The network architecture continuously enhanced from R15 to R18



2018 | 2019 | 2020 | 2021 | 2022 | 2023 +

Rel-16

Vertical industry security enhancement

- URLLC security: dual-path transmission security
- mMTC (cIoT) Security: Lightweight Small Packet Transmission Security
- Slice security: Defines NSSAAF slice authentication NEs.
- Non-public network (NPN) security: EAP-based non-public network authentication

Security assurance

- SCAS 1.0

Rel-17

Continuous evolution of security functions

- Security Capability Exposure: AKMA Authentication and Key Management Based on 3GPP Credentials
- MEC security (Support for Edge Computing in 5GC): interface security, client authentication and authorization

Secure assurance

- SCAS 2.0

Rel-18

Future-oriented security evolution

- Automatic 5GC virtual NE certificate management
- Home network triggered primary authentication
- NPN, MEC，AKMA scenarios，security aspects for roaming are standardized.
- User consent requirements are specified.
- Security mechanisms between UEs are defined, e.g. Prose, Ranging

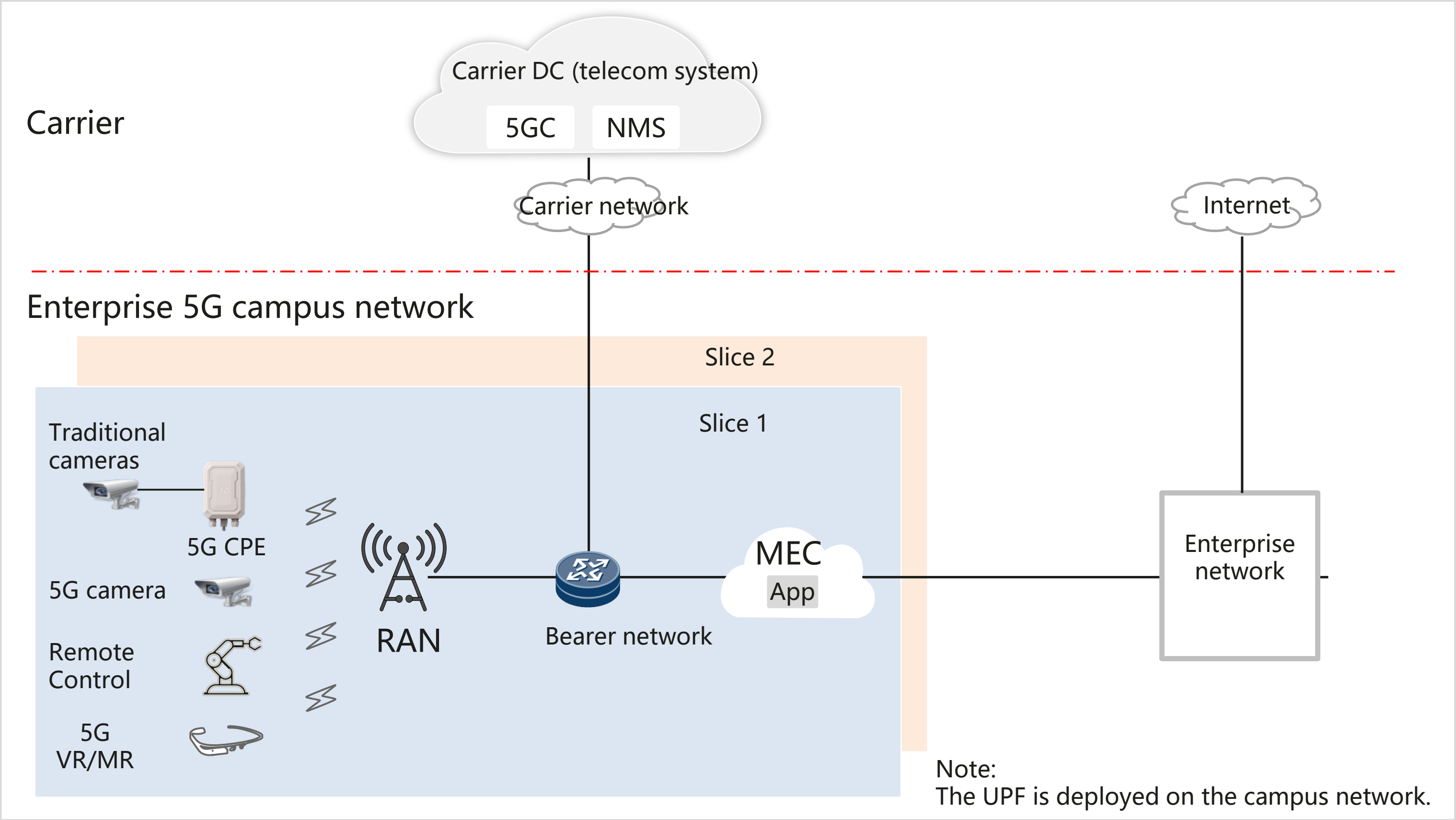
Security assurance

- SCAS 3.0

eMBB → URLLC, mMTC → URLLC, mMTC (enhanced) → Future-oriented evolution

- More URLLC and mMTC scenarios are defined in R16 to R18.

5G securely enabling vertical services: Build 5G vertical security capabilities to support higher security requirements in the industry



Note:
The UPF is deployed on the campus network.

Industry customer requirements

1. Only authorized terminals can access the campus network.
2. Enterprise service data does not leave the campus.
3. Carrier networks and campus networks are isolated from each other.
4. Third-party app security protection

Terminal access security

- Multi-access control for enterprise terminals

Data security

- User-plane data does not leave the campus

Border security

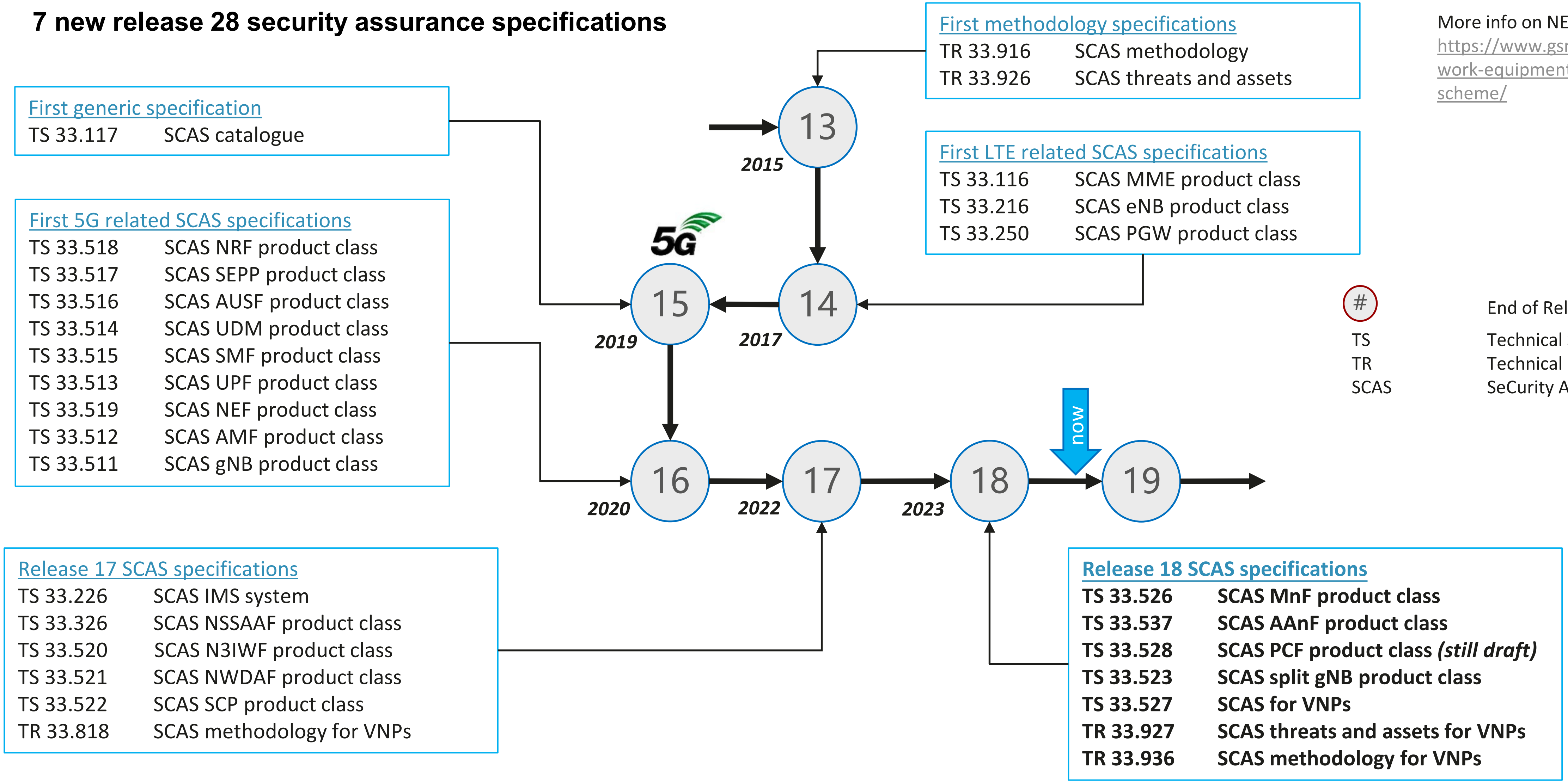
- Border protection between carrier networks and enterprise networks

MEC security

- MEC platform and interface security protection
- Third-party app security protection

NE security: Security assurance

7 new release 28 security assurance specifications



First methodology specifications

TR 33.916	SCAS methodology
TR 33.926	SCAS threats and assets

First generic specification

TS 33.117	SCAS catalogue

First LTE related SCAS specifications

TS 33.116	SCAS MME product class
TS 33.216	SCAS eNB product class
TS 33.250	SCAS PGW product class

First 5G related SCAS specifications

TS 33.518	SCAS NRF product class
TS 33.517	SCAS SEPP product class
TS 33.516	SCAS AUSF product class
TS 33.514	SCAS UDM product class
TS 33.515	SCAS SMF product class
TS 33.513	SCAS UPF product class
TS 33.519	SCAS NEF product class
TS 33.512	SCAS AMF product class
TS 33.511	SCAS gNB product class

Release 17 SCAS specifications

TS 33.226	SCAS IMS system
TS 33.326	SCAS NSSAAF product class
TS 33.520	SCAS N3IWF product class
TS 33.521	SCAS NWDAF product class
TS 33.522	SCAS SCP product class
TR 33.818	SCAS methodology for VNPs

Release 18 SCAS specifications

TS 33.526	**SCAS MnF product class**
TS 33.537	**SCAS AAnF product class**
TS 33.528	**SCAS PCF product class *(still draft)***
TS 33.523	**SCAS split gNB product class**
TS 33.527	**SCAS for VNPs**
TR 33.927	**SCAS threats and assets for VNPs**
TR 33.936	**SCAS methodology for VNPs**

More info on NESAS:
https://www.gsma.com/security/network-equipment-security-assurance-scheme/

#	End of Release number #
TS	Technical Specification
TR	Technical Report
SCAS	SeCurity Assurance Specification

HUAWEI

Outline

1. 5G Network Security Solution those we have now
2. **5G Network Security Trend those we expect for future**
3. Summary

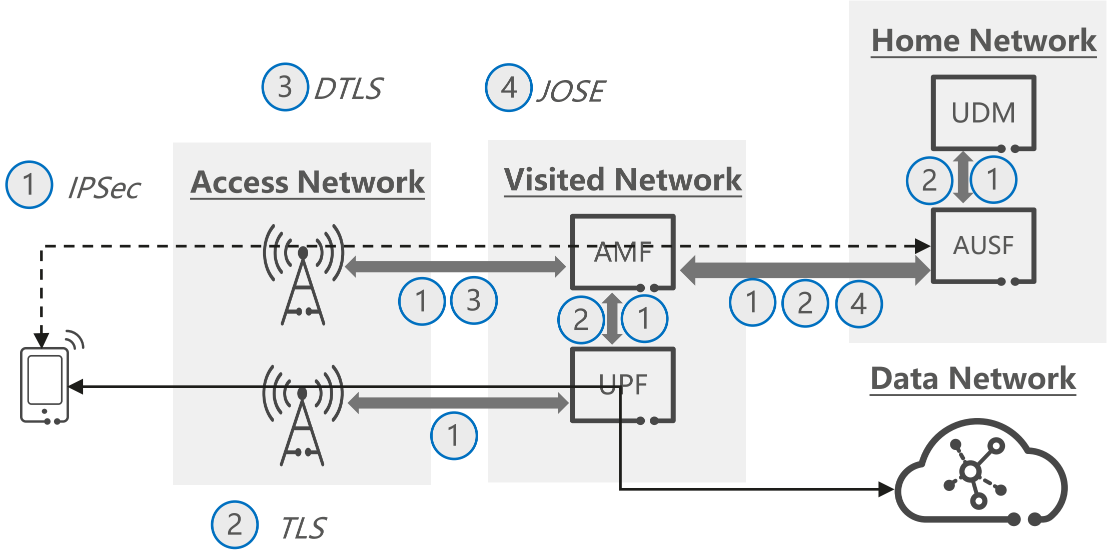
Crypto evolution

Security protocol adaptation

- Specifications include provisions for usage/support of security protocols such as IPsec, TLS, JOSE, CMPv2, X509, etc.
- SA3 maintains several profiles for all the security protocols used in 3GPP systems to ensure best practices and recommendations are followed.

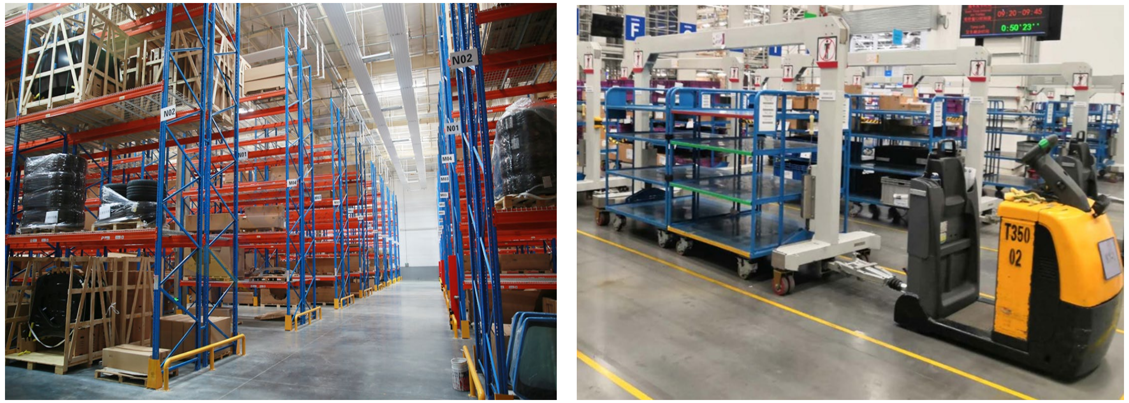
New 256-bit algs now available

- During release 18 SAGE finalized the work on the new 256-bit key algorithms
- New 256-bit key algorithms would be specified in release 19.



AMF	Access and Mobility management Function
UPF	User Plane Function
UDM	User Data Management
AUSF	AUthentication Server Function
UE	User Equipment
EAP	Extensible Authentication Protocol
JOSE	Javascript Object Signing and Encryption
TLS	Transport Layer Security
DTLS	Datagram TLS

Ambient_IoT Security



Service requirements and KPI for use of Ambient_IoT devices for intralogistics in automobile manufacturing has been defined in 3GPP SA1 and RAN.

Constrains（active tag and passive tag)

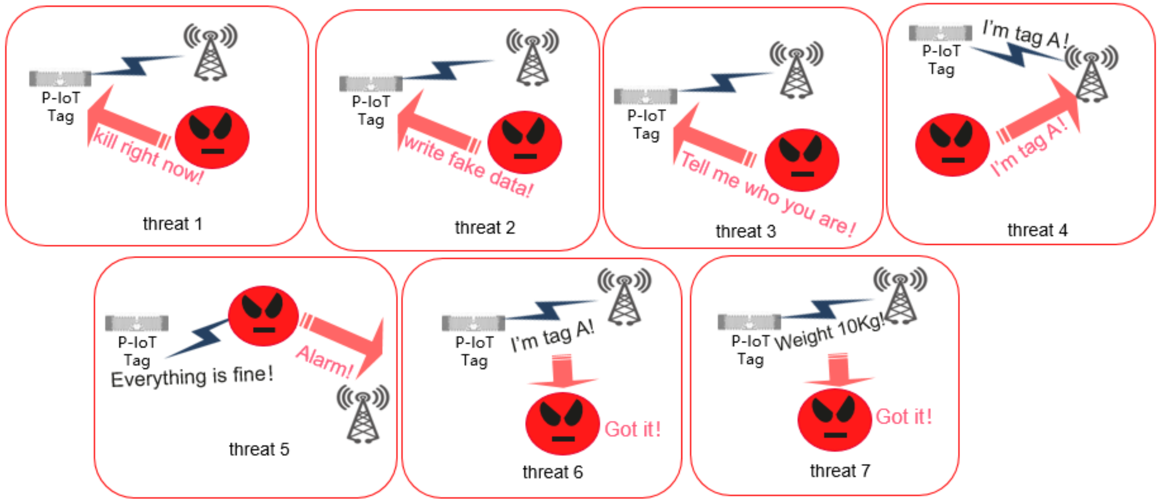
- Credentials provisioning
- Calculation capability is limited

Constrains（passive tag)

- Limited memory
- Unguaranteed memory writing

Principles of security designed for Ambient IoT

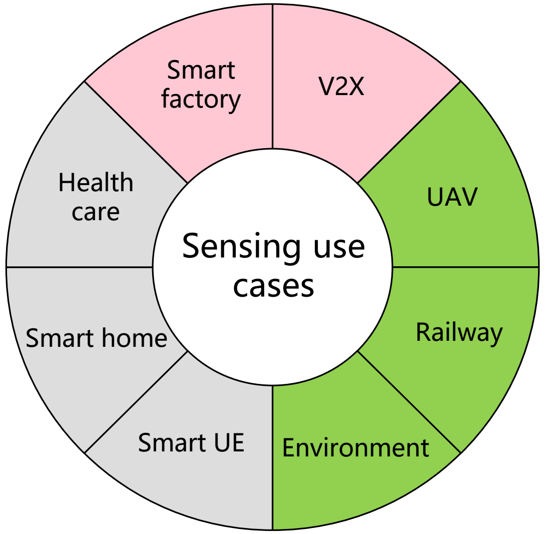
- Security on demand to meet differentiated requirements in multiple scenarios
- Security with UEs using CP CIoT optimization is considered as baseline with optimization



Num	Threat	Requirement
1	Tag is killed by attacker;	Access control in tag
2	Tag stores the invalid information from attacker	
3	Tag follows the invalid command from attacker	
4	impersonation attack	network verifies tag, anti-replay
5	The reported message is tampered	Integrity protection
6	The reported message is eavesdropped	Confidentiality Protection
7	Tag is tracked by attacker	ID privacy protection

The security mechanism for Ambient IoT shall consider the tag restriction and network load.

Integrated Sensing and Communication Security



Source of use cases:

3GPP	5GAA
IMT-2020	IEEE
Next-G	Hexa-X

RAN-based sensing

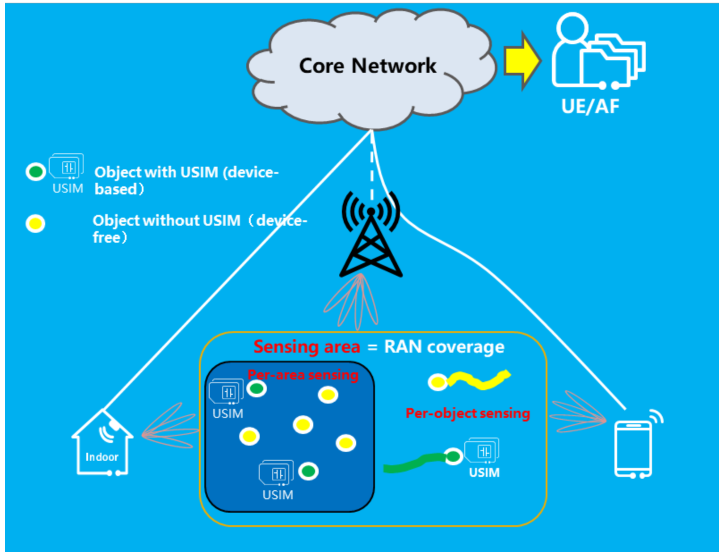
UE-based sensing

RAN & UE-based sensing

Industry information

- IMT-2020 sets up a HCS working group, and IMT-2030 takes HCS as one key technology of 6G network architecture. CCSA starts the 5G-Advanced oriented HCS research work, which helps boost the HCS industry in 5.5G.
- IEEE sets up the 802.11bf working group to study Wi-Fi enabled sensing use cases and technologies.
- Next-G and Hexa-X take sensing as a fundamental 6G technology.
- 3GPP SA1 has initiated the HCS SID for R19 in Q1 of 2022.

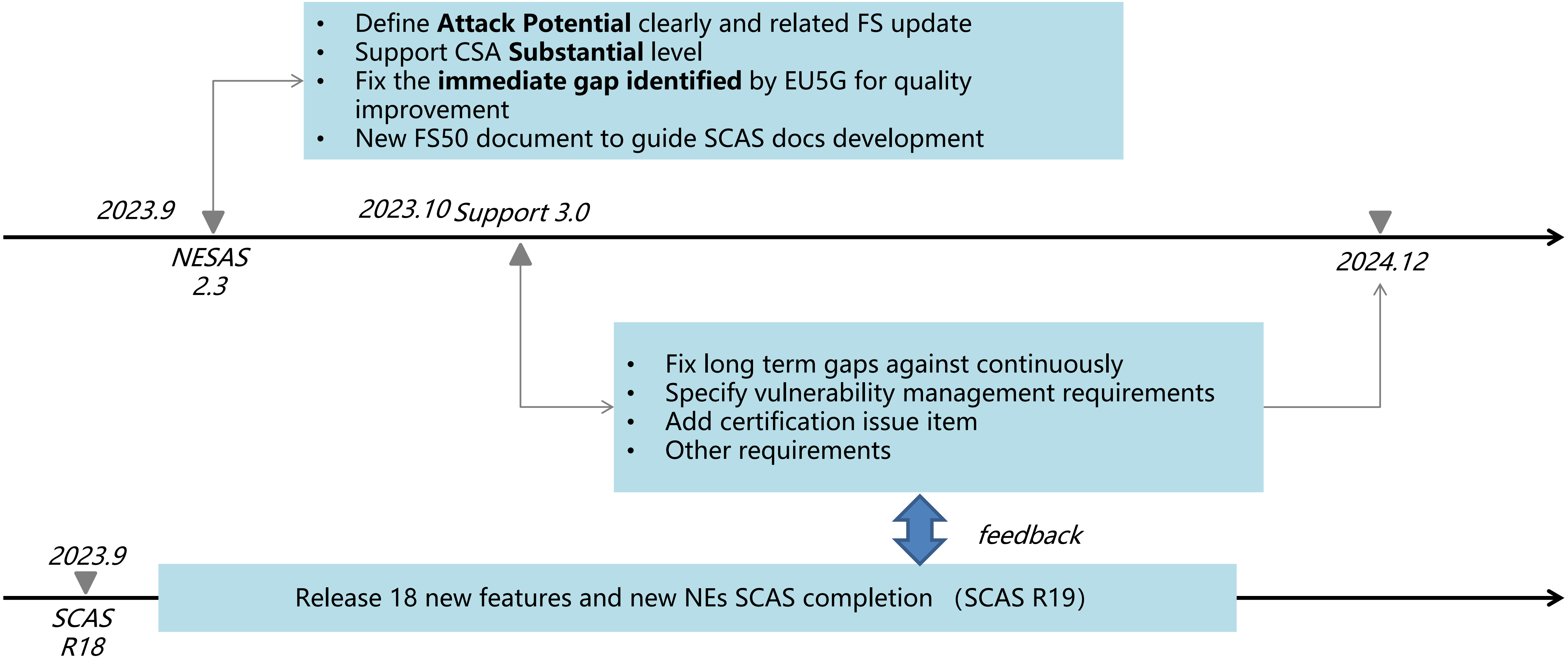
Sensing →Object detection


Core Network
UE/AF
USIM
Object with USIM (device-based）
Object without USIM（device-free）
Sensing area = RAN coverage
Per-area sensing
USIM
USIM
Per-object sensing
USIM
Indoor

Security Requirements potentially

- A mechanism to protect identifiable information
- Support encryption, integrity protection, privacy of the 3GPP sensing data, non-3GPP sensing data and sensing results, to protect the data inside the 5G system.

NESAS/SCAS: Initiate new version for gap fixing



- Define **Attack Potential** clearly and related FS update
- Support CSA **Substantial** level
- Fix the **immediate gap identified** by EU5G for quality improvement
- New FS50 document to guide SCAS docs development

- Fix long term gaps against continuously
- Specify vulnerability management requirements
- Add certification issue item
- Other requirements

Release 18 new features and new NEs SCAS completion (SCAS R19)

Outline

1. 5G Network Security Solution those we have now
2. 5G Network Security Trend those we expect for future
3. **Summary**

Summary

- 5G security needs collaboration between equipment vendors, operators, and application service providers to build a 5G security system.
- 5G inherits the security capabilities of 4G, and 5G security standards are continuously enhanced.
- 5G networks bear vertical industry services, focusing on terminal access security, data security, and border security to meet the industry's requirements for enhanced security.
- 5.5G network security would consider more about improvements about new services, e.g. Ambient IoT, Sensing, as well as crypto adaptation.

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI