Mobile Security – 5G

Network Security - Lecture 9

Ruxandra F. Olimid

Faculty of Mathematics and Computer Science, University of Bucharest

Outline

- Arhitecture
- EPS AKA
- Key hierarchy
- Cryptographical aspects
- New concepts

5G Security

Figure 1: Standardisation organisations of relevance for 5G security

https://www.3gpp.org/

https://www.ieee.org/

https://www.etsi.org/

https://www.itu.int

https://www.ietf.org/

[ENISA – Security in 5G Specifications – Controls in 3GPP
Available at: https://www.enisa.europa.eu/publications/security-in-5g-specifications]

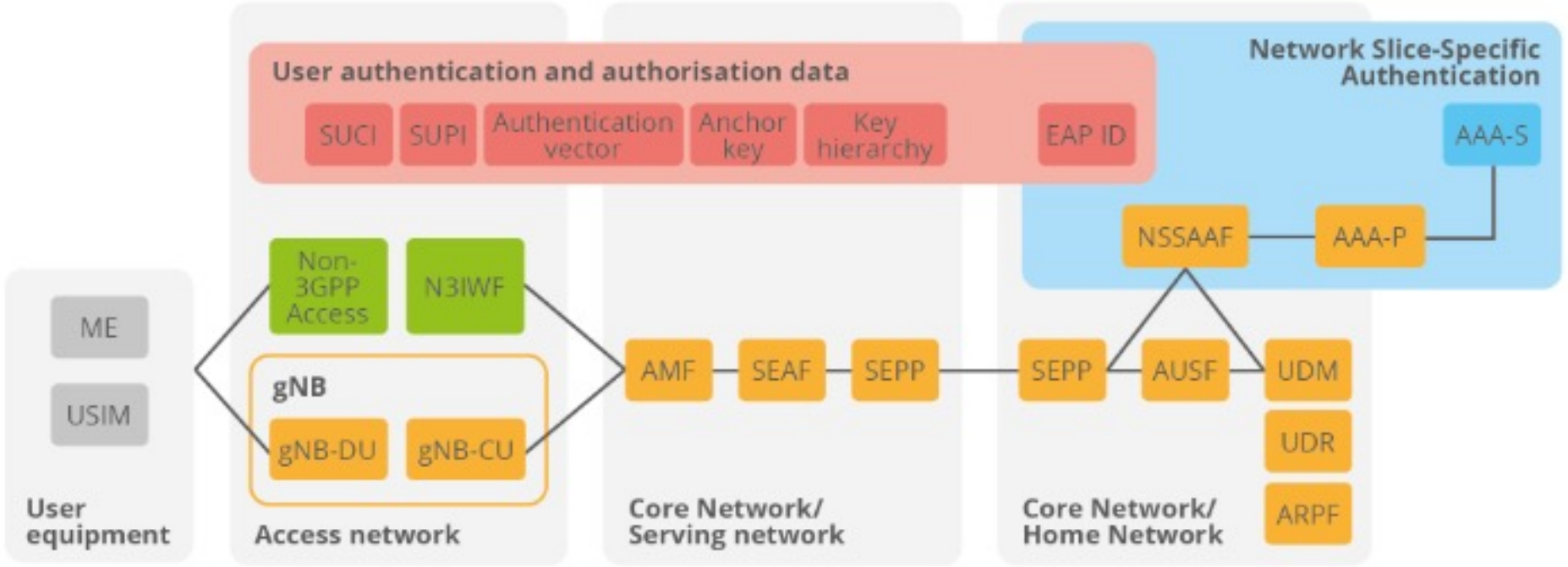
3GPP Security Standards

TS 33.501	Security architecture and procedures for 5G System
TS 33.511	Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
TS 33.512	5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)
TS 33.513	5G Security Assurance Specification (SCAS); User Plane Function (UPF)
TS 33.514	5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class
TS 33.515	5G Security Assurance Specification (SCAS) for the Session Management Function (SMF) network product class
TS 33.516	5G Security Assurance Specification (SCAS) for the Authentication Server Function (AUSF) network product class
TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class
TS 33.518	5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class
TS 33.519	5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class
TS 33.520	5G Security Assurance Specification (SCAS); Non-3GPP InterWorking Function (N3IWF)
TS 33.521	5G Security Assurance Specification (SCAS); Network Data Analytics Function (NWDAF)
TS 33.522	5G Security Assurance Specification (SCAS); Service Communication Proxy (SECOP)
TS 33.535	Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)

[Source: https://www.3gpp.org/DynaReport/33-series.htm]

Security Architecture

Figure 8: Security architecture zoom-in from the ENISA 5G Threat Landscape 2020



[ENISA – Security in 5G Specifications – Controls in 3GPP
Available at: https://www.enisa.europa.eu/publications/security-in-5g-specifications]

UE Privacy

SUCI: Subscription Concealed Identifier
SUPI: Subscription Permanent Identifier
GUTI: Globally Unique Temporary UE Identity

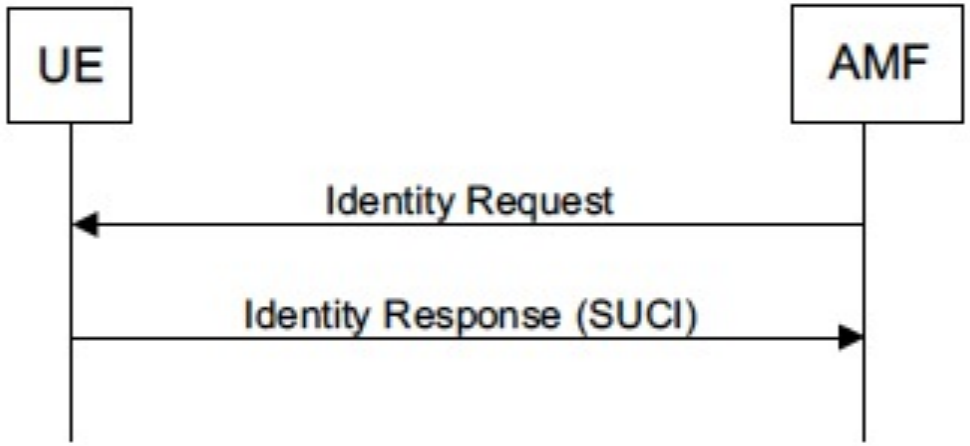


Figure 6.12.4-1: Subscription identifier query

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI - SUCI

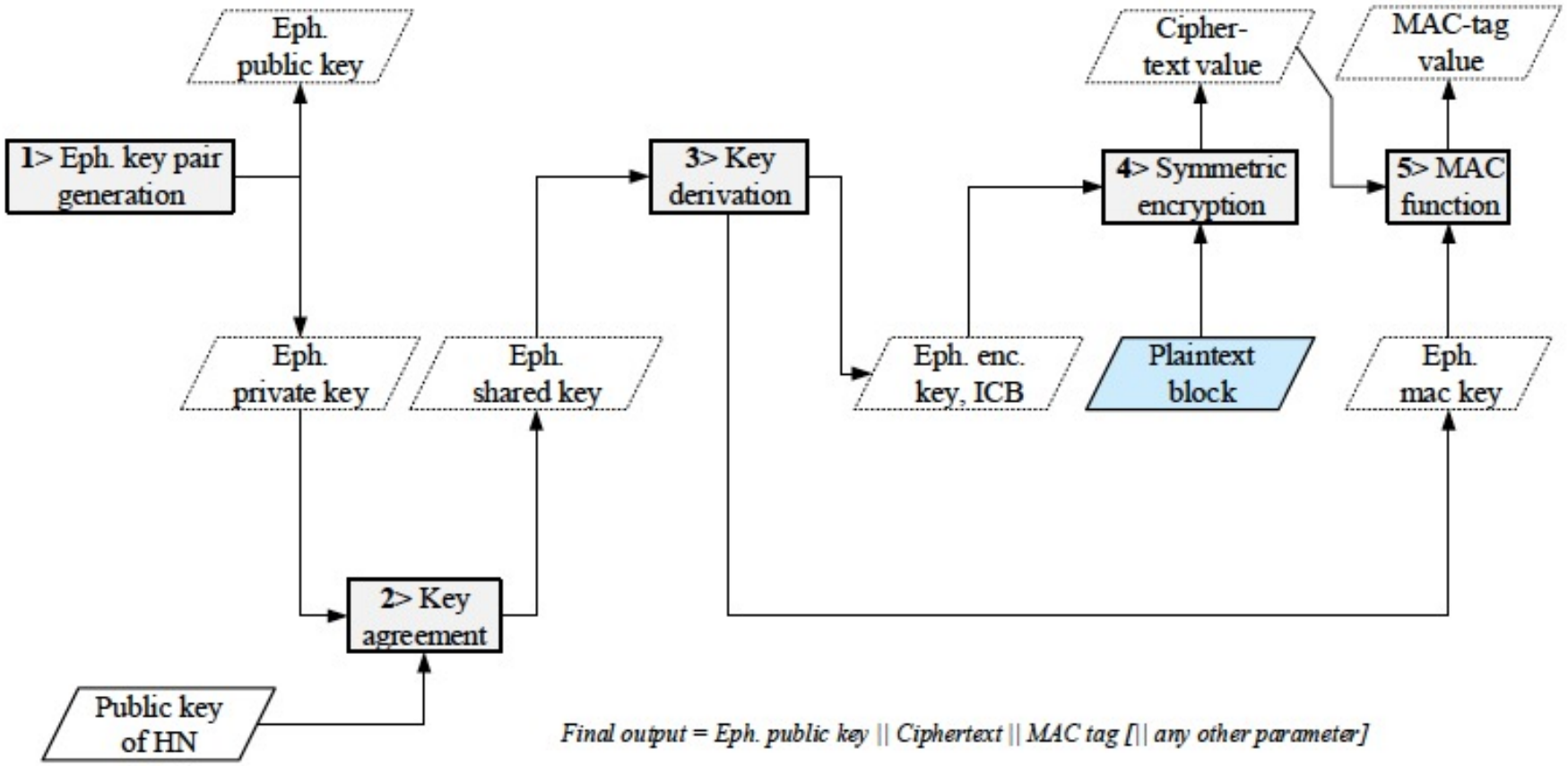


Figure C.3.2-1: Encryption based on ECIES at UE

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Protection of SUPI - SUCI

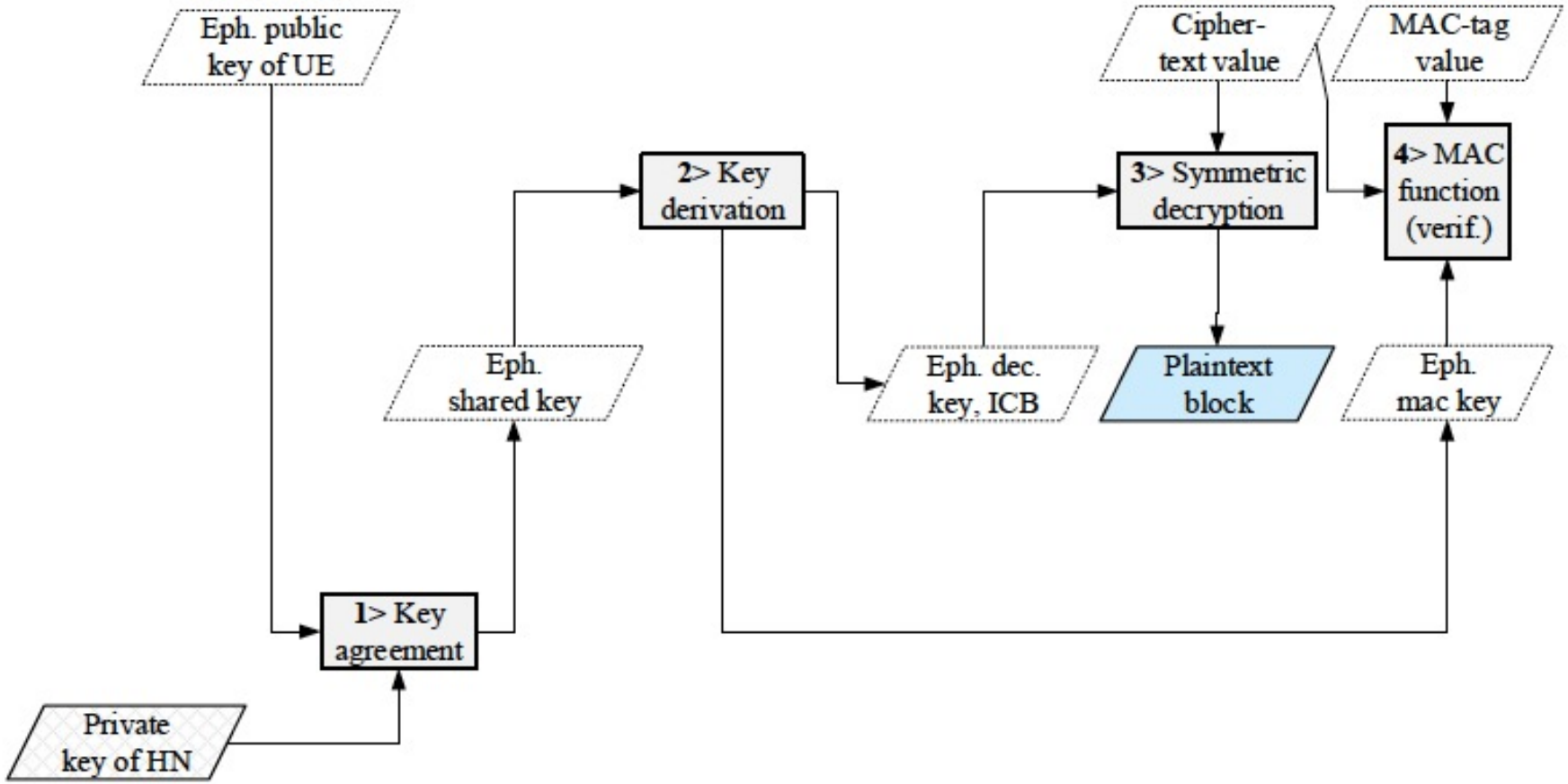


Figure C.3.3-1: Decryption based on ECIES at home network

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

5G-AKA

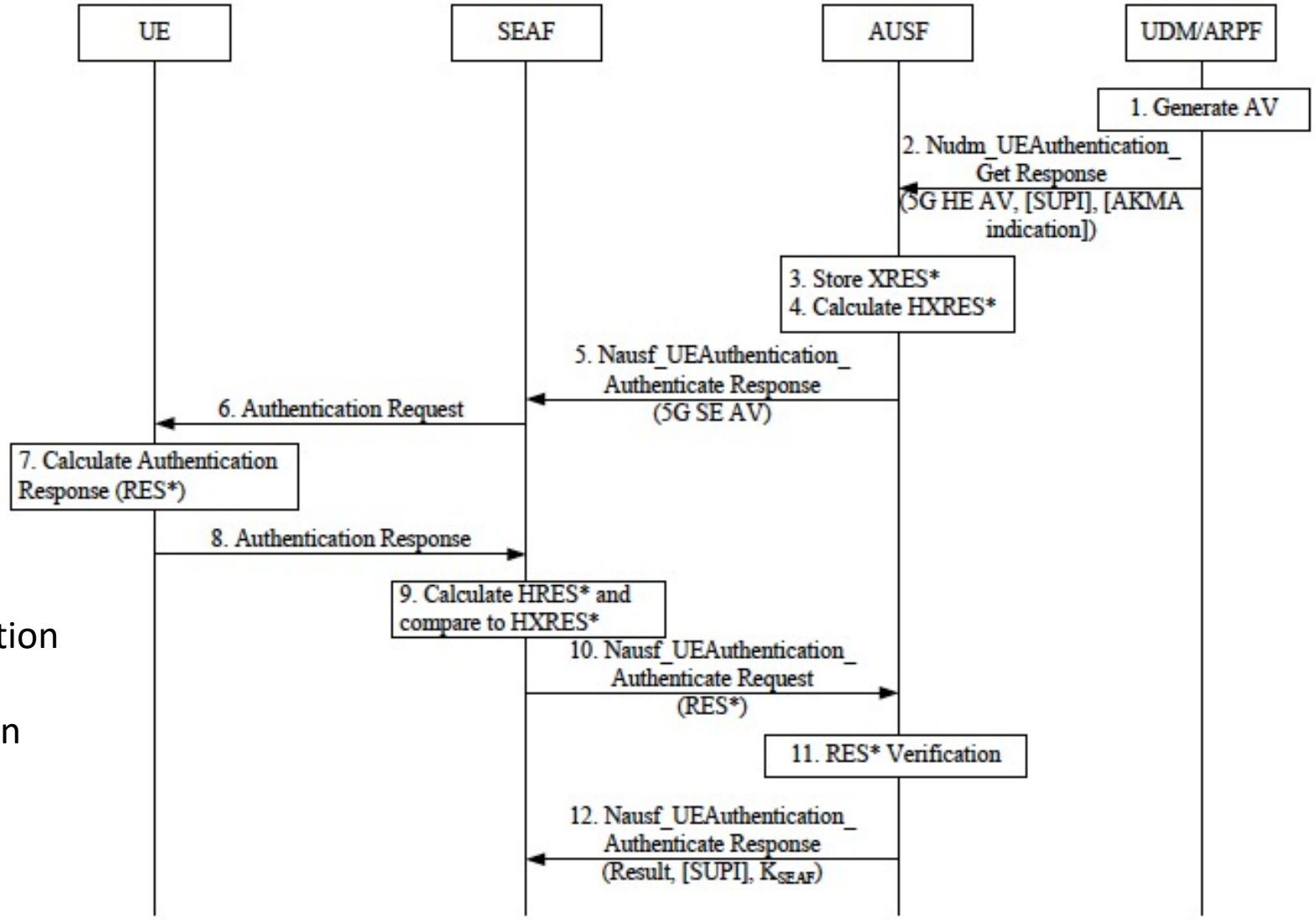


Figure 6.1.3.2-1: Authentication procedure for 5G AKA

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

AUSF: AUthentication Server Function
ARPF: Authentication credential Repository and Processing Function
SIDF: Subscription Identifier De-concealing Function
SEAF: SEcurity Anchor Function

Key Hierarchy

AUSF: AUthentication Server Function
ARPF: Authentication credential Repository and Processing Function
SEAF: SEcurity Anchor Function
AMF Access and Mobility Management Function

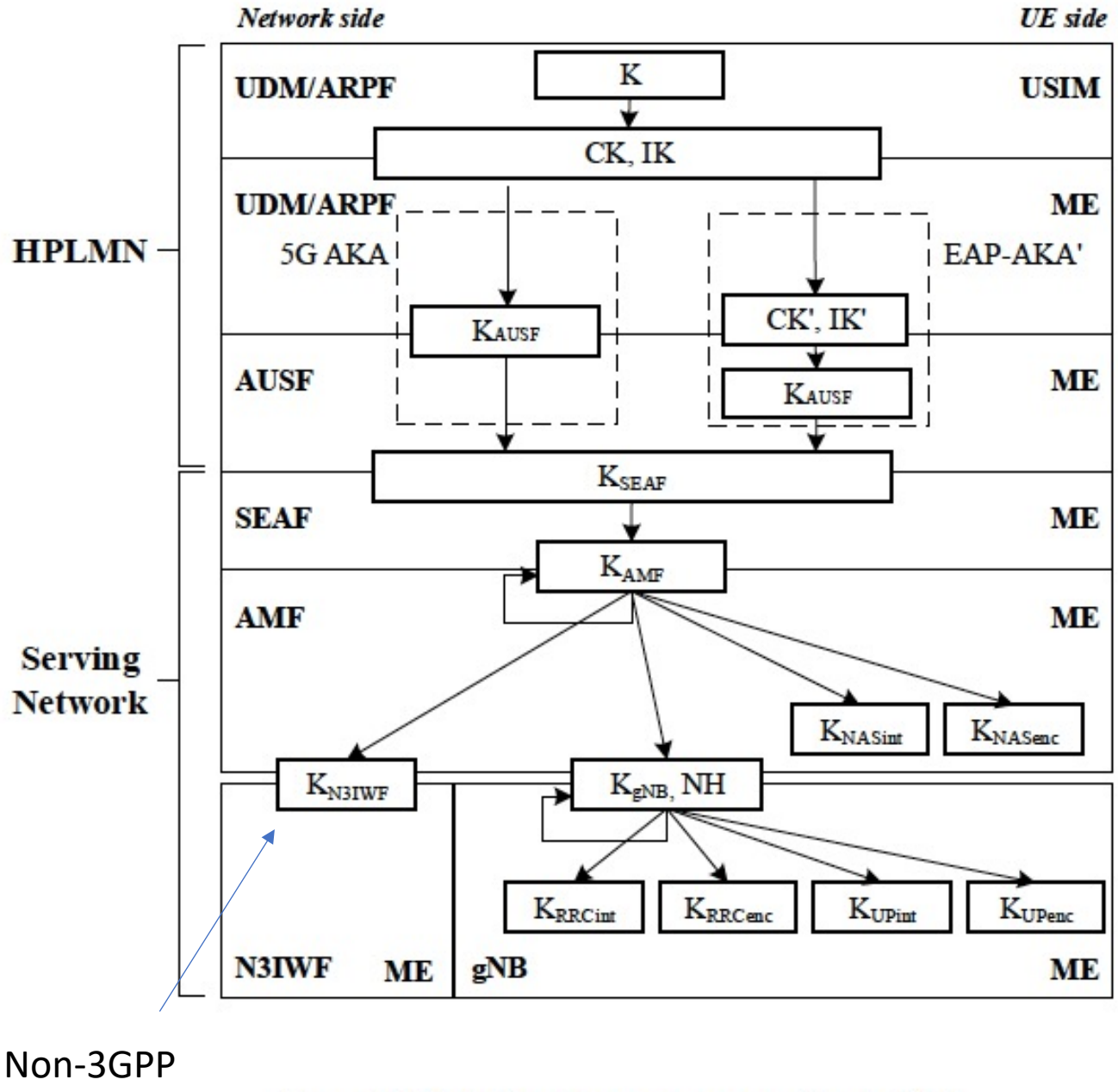


Figure 6.2.1-1: Key hierarchy generation in 5GS

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Cryptographical Aspects

"0000_2"	NEA0	Null ciphering algorithm;
"0001_2"	128-NEA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NEA2	128-bit AES based algorithm; and
"0011_2"	128-NEA3	128-bit ZUC based algorithm.

5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

Cryptographical Aspects

"0000_2"	NIA0	Null Integrity Protection algorithm;
"0001_2"	128-NIA1	128-bit SNOW 3G based algorithm;
"0010_2"	128-NIA2	128-bit AES based algorithm; and
"0011_2"	128-NIA3	128-bit ZUC based algorithm.

5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

[Source: 3GPP TS 33.501 V17.1.0 (2021-03)]

New Concepts

- SDN
- NFV
- MEC
- Slicing
- Virtualisation
- … … …

To remember!

1. Improvements over 4G security

2. New concepts