5G System Security

TP00005-V-1701 V0 - S04M04 Ed1

Learning Objectives

Upon completion of this module, you should be able to:

Describe 5G System Security Architecture.
Explain 5G System Security procedures.

Table of Contents

5G System Security Architecture

5G System Security Procedures

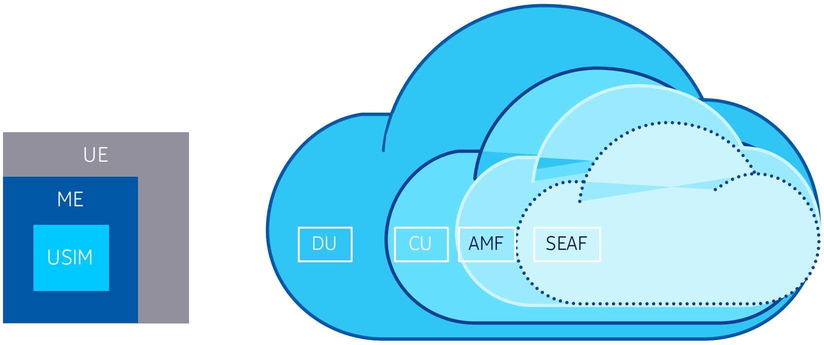
Wrap-up

5G System Security Architecture

Nokia Confidential

5G System Security Architecture

Overview of the Security Architecture



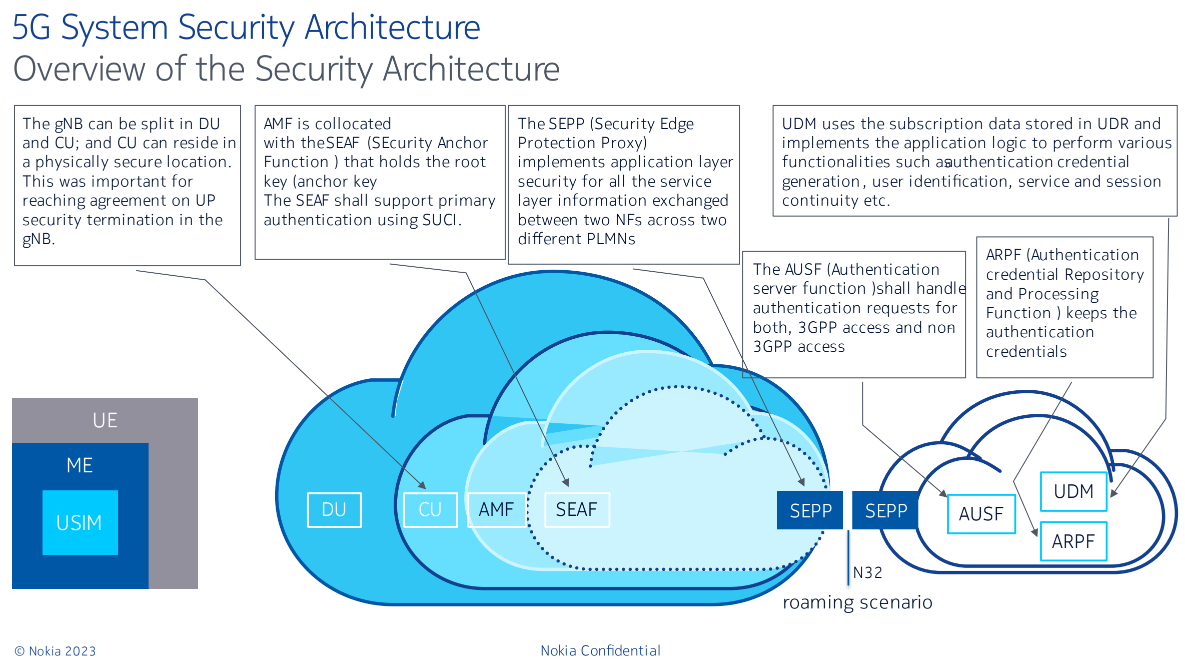
Trust model for non-roaming scenario

3GPP technical work groups have specified and standardized mobile wireless industry security features and mechanisms for 3G, 4G and 5G technologies

The SA3 Working Group is responsible for security and privacy in 3GPP systems, a role that is set to determine the security and privacy requirements and specifying the security architectures and protocols.

3GPP also ensures the availability of algorithms with ciphering and encryption capabilities which need to be described as part of the specifications.

3GPP TS 33.501 is the specification published by SA3 which describes the System Security Architecture for 5G.



5G System Security Architecture

Overview of the Security Architecture

The gNB can be split in DU and CU; and CU can reside in a physically secure location. This was important for reaching agreement on UP security termination in the gNB.

AMF is collocated with theSEAF (SEcurity Anchor Function) that holds the root key (anchor key
The SEAF shall support primary authentication using SUCI.

The SEPP (Security Edge Protection Proxy) implements application layer security for all the service layer information exchanged between two NFs across two different PLMNs

UDM uses the subscription data stored in UDR and implements the application logic to perform various functionalities such asauthentication credential generation, user identification, service and session continuity etc.

The AUSF (Authentication server function)shall handle authentication requests for both, 3GPP access and non 3GPP access

ARPF (Authentication credential Repository and Processing Function) keeps the authentication credentials

Nokia Confidential

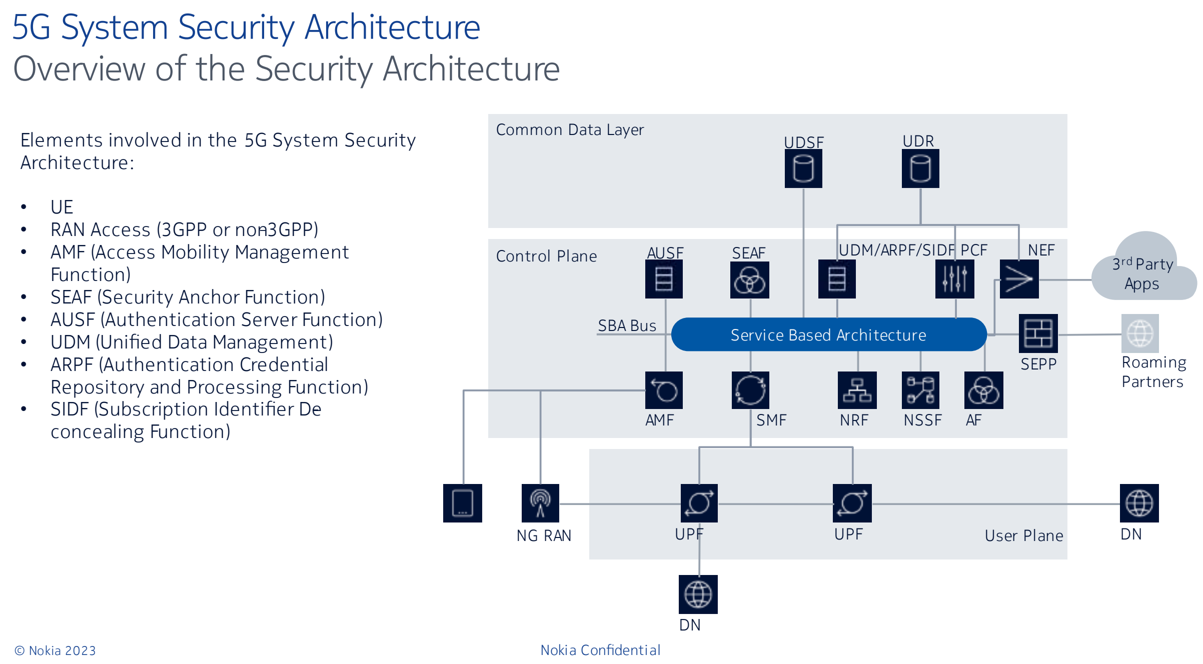
This Figure shows the Network Functions involved in 5GS Security. The gNodeB can be split into Distributed Units (DU) and Central Units (CU); and a CU can reside in a physically secure location. This was important for reaching agreement on User Plane security termination in the gNodeB.

The AMF is collocated with the SEcurity Anchor Function (SEAF) that holds the root key (anchor key) for the visited network: The SEAF forwards Extensible Authentication Protocol (EAP) messages between the UE and the EAP server in the Authentication Server Function (AUSF), where AMF/SEAF acts as an EAP authenticator. It receives from the AUSF and holds the Master Key that serves as anchor key for protecting further communication between the UE and the serving network. This anchor key is common for all accesses.

To protect messages that are sent over the N32 interface, the 5G System architecture introduces the Security Edge Protection Proxy (SEPP) as the entity sitting at the perimeter of the PLMN network. The SEPP implements application layer security for all the service layer information exchanged between two NFs across two different PLMNs.

The Authentication Server Function (AUSF) shall handle authentication requests for both 3GPP access and non-3GPP access. And the Authentication credential Repository and Processing Function (ARPF) keeps the authentication credentials.

The subscriber information is stored in the Unified Data Repository (UDR). The Unified Data Management (UDM) uses the subscription data stored in UDR and implements the application logic to perform various functionalities such as authentication credential generation, user identification, service and session continuity, etc. The long-term keys used for authentication and security association setup purposes shall be protected from physical attacks and shall never leave the secure environment of the UDM.



5G System Security Architecture

Overview of the Security Architecture

Elements involved in the 5G System Security Architecture:

- UE
- RAN Access (3GPP or non-3GPP)
- AMF (Access Mobility Management Function)
- SEAF (Security Anchor Function)
- AUSF (Authentication Server Function)
- UDM (Unified Data Management)
- ARPF (Authentication Credential Repository and Processing Function)
- SIDF (Subscription Identifier De concealing Function)

The **Security Anchor Function (SEAF)** is present in the serving network, and it is a “middleman” during the authentication process between a UE and its home network. It can reject an authentication from the UE, but it relies on the UE’s home network to accept the authentication.

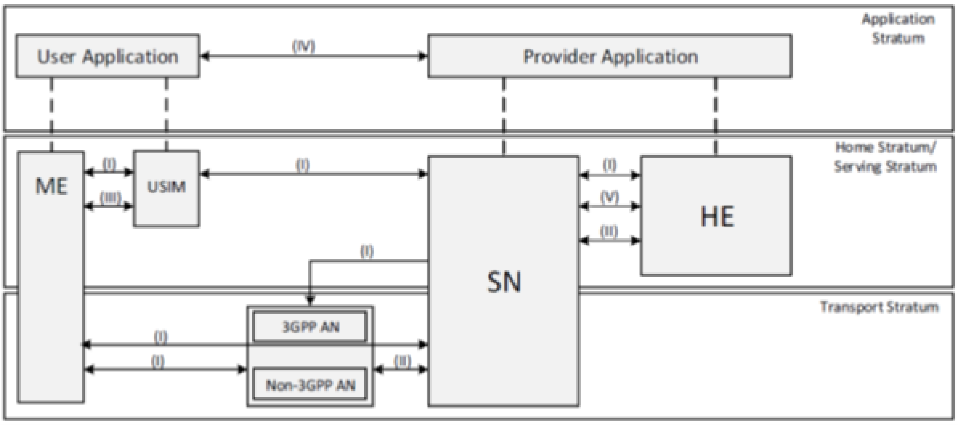
The **Authentication Server Function (AUSF)** is in a home network and performs authentication with a UE. It makes the decision on UE authentication, but it relies on backend service for computing the authentication data and keying materials when 5G-AKA or EAP-AKA’ is used.

Unified data management (UDM) is an entity that hosts functions related to data management, such as the Authentication Credential Repository and Processing Function (ARPF), which selects an authentication method based on subscriber identity and configured policy and computes the authentication data and keying materials for the AUSF if needed.

The **Subscription Identifier De-concealing Function (SIDF)** decrypts a Subscription Concealed Identifier (SUCI) to obtain its long-term identity, namely the Subscription Permanent Identifier (SUPI), e.g., the IMSI. In 5G, a subscriber long-term identity is always transmitted over the radio interfaces in an encrypted form. More specifically, a public key-based encryption is used to protect the SUPI. Therefore, only the SIDF has access to the private key associated with a public key distributed to UEs for encrypting their SUPIs.

The **ARPF (Authentication Credential Repository and Processing Function)** is a functional element of the UDM, responsible for generating 5G HE AV (5G Home Environment Authentication Vectors) based on the subscriber’s shared secret key.

5G System Security Architecture
Overview of the Security Architecture



The figure illustrates the following security domains:

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.

- Network domain security (II): the set of security features that enable network nodes to securely exchange signaling data and user plane data.

- User domain security (III): the set of security features that secure the user access to mobile equipment.

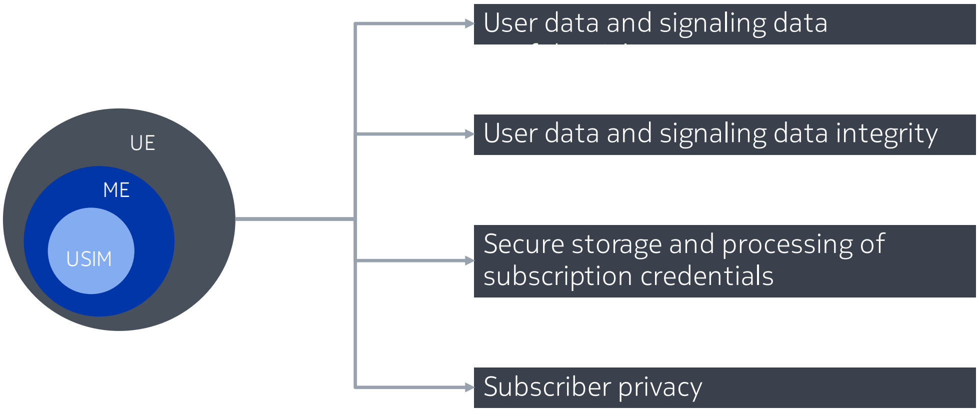
- Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Application domain security is out of scope of the present document.

- SBA domain security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains . Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401.

- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.

5G System Security Architecture

Requirements on the UE



User data and signaling data

User data and signaling data integrity

Secure storage and processing of subscription credentials

Subscriber privacy

User data and signaling 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-based signaling.

The UE shall implement the following ciphering algorithms: NEA0, 128-NEA1, 128-NEA2.

User data and signaling 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-signaling.

The UE shall implement the following integrity protection algorithms: NIA0, 128-NIA1, 128-NIA2.

Secure storage and processing of subscription credentials

The following requirements apply for the storage and processing of the subscription credentials used to access the 5G network:

The subscription credential(s) shall be integrity protected within the UE using a tamper resistant secure hardware component.

The long-term keys of the subscription credentials (K) shall be confidentiality protected within the UE using a tamper resistant secure hardware component.

The long-term keys of the subscription credentials shall never be available in the clear outside of the tamper resistant secure hardware component.

The authentication algorithms that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.

It shall be possible to perform a security evaluation / assessment according to the respective security requirements of the tamper resistant secure hardware component.

Subscriber privacy

The UE shall support 5G-GUTI.

The SUPI should not be transferred in clear text over NG-RAN except routing information, such as the Mobile Country Code (MCC) and Mobile Network Code (MNC).

The Home Network Public Key shall be stored in the USIM.

The protection scheme identifier shall be stored in the USIM.

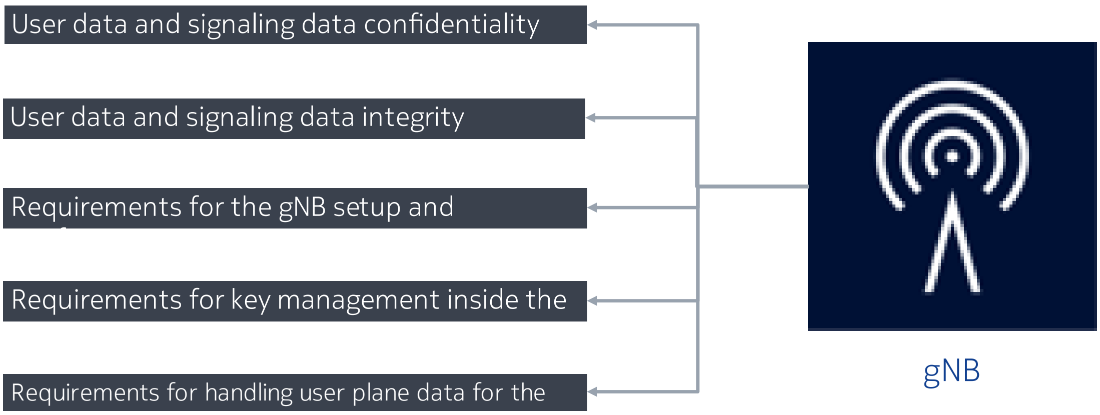
The Home Network Public Key Identifier shall be stored in the USIM.

The SUCI calculation indication, either USIM or ME calculating the SUCI, shall be stored in USIM.

The ME shall support the null-scheme. If the home network has not provisioned the Home Network Public Key in USIM, the SUPI

5G System Security Architecture

Requirements on the gNB



User data and signaling data confidentiality

User data and signaling data integrity

Requirements for the gNB setup and

Requirements for key management inside the

Requirements for handling user plane data for the

User data and signaling data confidentiality

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

The gNB shall activate ciphering of user data based on the security policy sent by the SMF.

The gNB shall support ciphering of RRC signaling.

The gNB shall implement the following ciphering algorithms: NEA0, 128-NEA1, 128-NEA2.

The gNB may implement the following ciphering algorithm: 128-NEA3.

User data and signaling data integrity

The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

The gNB shall activate integrity protection of user data based on the security policy sent by the SMF.

The gNB shall support integrity protection and replay protection of RRC signaling.

The gNB shall support the following integrity protection algorithms: NIA0, 128-NIA1, 128-NIA2

The gNB may support the following integrity protection algorithm: 128-NIA3.

Requirements for the gNB setup and configuration

The certificate enrolment mechanism specified in TS 33.310 [5] for base station should be supported for gNBs. The decision on whether to use the enrolment mechanism is left to operators.

Communication between the O&M systems and the gNB shall be confidentiality, integrity and replay protected from unauthorized parties. The security associations between the gNB and an entity in the 5G Core or in an O&M domain trusted by the operator shall be supported. These security association establishments shall be mutually authenticated. The security associations shall be realized according to TS 33.210 [3] and TS 33.310 [5].

The gNB shall be able to ensure that software/data change attempts are authorized.

The gNB shall use authorized data/software.

Sensitive parts of the boot-up process shall be executed with the help of the secure environment.

Confidentiality of software transfer towards the gNB shall be ensured.

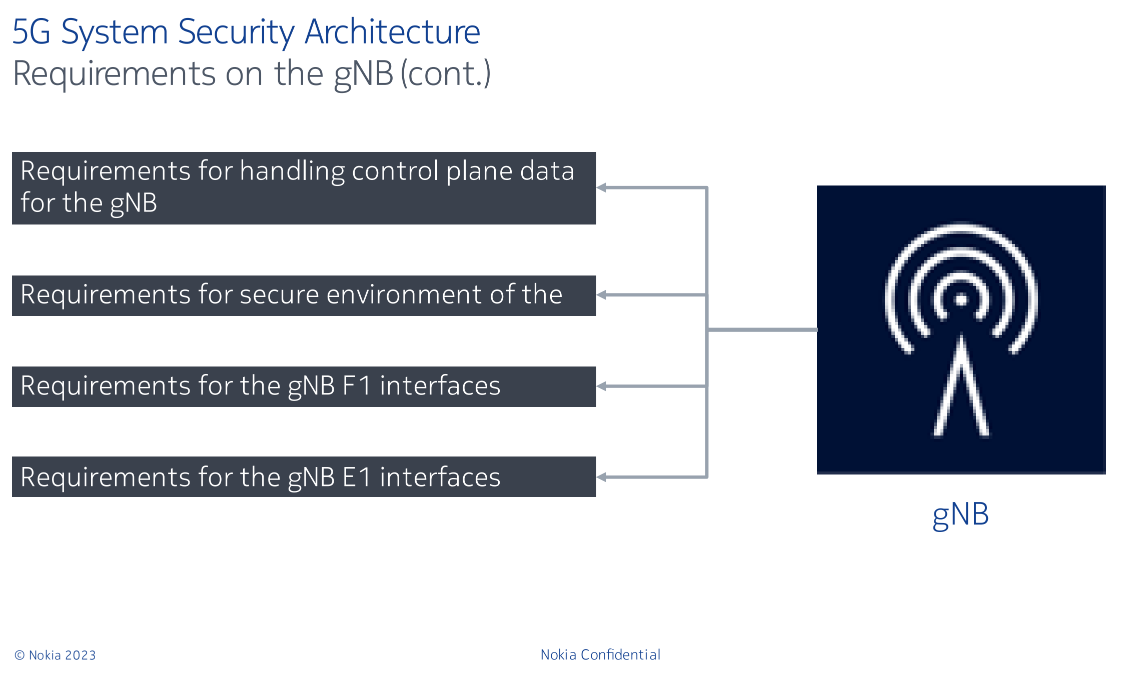
Integrity protection of software transfer towards the gNB shall be ensured.

Requirements for key management inside the gNB

Any part of a gNB deployment that stores or processes keys in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then keys in cleartext shall be stored and processed in a secure environment. Keys stored inside a secure environment in any part of the gNB shall never leave the secure environment except when done in accordance with this or other 3GPP specifications.

Requirements for handling user plane data for the gNB

Any part of a gNB deployment that stores or processes user plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then user plane data in cleartext shall be stored and processed in a secure environment.



5G System Security Architecture

Requirements on the gNB (cont.)

Requirements for handling control plane data for the gNB
Requirements for secure environment of the
Requirements for the gNB F1 interfaces
Requirements for the gNB E1 interfaces
gNB

Requirements for handling control plane data for the gNB

Any part of a gNB deployment that stores or processes control plane data in cleartext shall be protected from physical attacks. If not, the whole entity is placed in a physically secure location, then control plane data in cleartext shall be stored and processed in a secure environment.

Requirements for secure environment of the gNB

The secure environment shall support secure storage of sensitive data, for instance, long-term cryptographic secrets and vital configuration data.

The secure environment shall support the execution of sensitive functions, e.g., en-/decryption of user data and the basic steps within protocols which use long term secrets.

The secure environment shall support the execution of sensitive parts of the boot process.

The secure environment's integrity shall be assured.

Only authorized access shall be granted to the secure environment, i.e., to data stored and used within it, and to functions executed within it

Requirements for the gNB F1 interfaces

F1-C interface shall support confidentiality, integrity and replay protection.

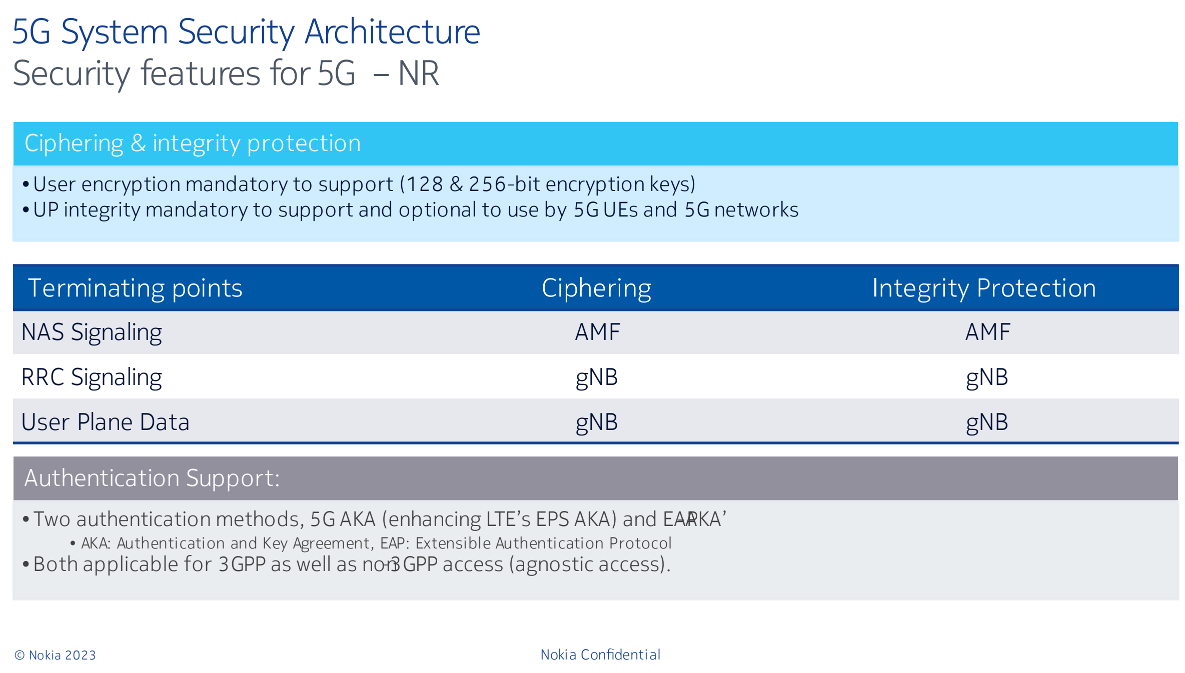
All management traffic carried over the CU-DU link shall be integrity, confidentiality and replay protected.

The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane.

F1-C and management traffic carried over the CU-DU link shall be protected independently from F1-U traffic.

Requirements for the gNB E1 interfaces

The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected.



5G System Security Architecture
Security features for 5G – NR

Ciphering & integrity protection

- User encryption mandatory to support (128 & 256-bit encryption keys)
- UP integrity mandatory to support and optional to use by 5G UEs and 5G networks

Terminating points	Ciphering	Integrity Protection
NAS Signaling	AMF	AMF
RRC Signaling	gNB	gNB
User Plane Data	gNB	gNB

Authentication Support:

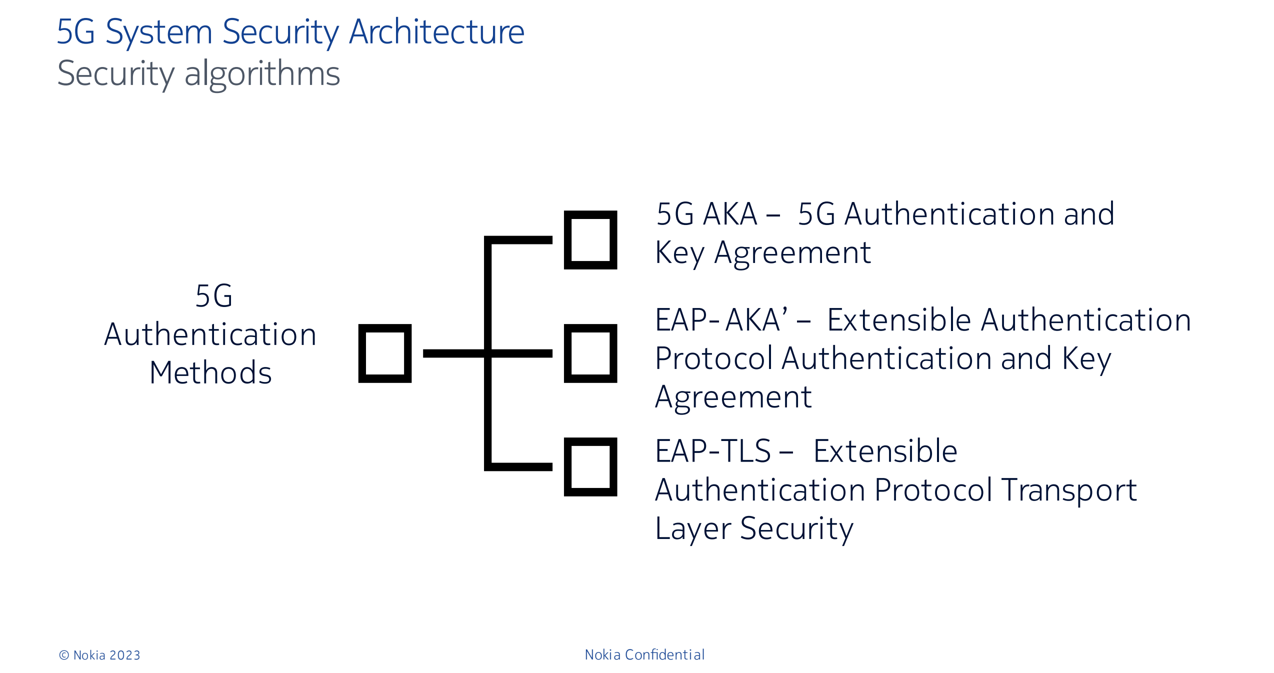
- Two authentication methods, 5G AKA (enhancing LTE’s EPS AKA) and EAP-AKA’
  - AKA: Authentication and Key Agreement, EAP: Extensible Authentication Protocol
- Both applicable for 3GPP as well as non-3GPP access (agnostic access).

Security aspects include:

- Authentication of the UE by the network and vice versa
- Security context generation and distribution.
- User Plane data confidentiality and integrity protection.
- Control Plane signaling confidentiality and integrity protection.
- User identity confidentiality.

User plane data is encrypted and can be integrity protected. User plane integrity protection is a new feature (not present in 4G) that thwarts attacks against modification of encrypted addresses and content. It is valuable for small data transmissions, particularly for constrained IoT devices. It is worth noting that this feature is mandatory to support in the User Equipment and the gNB, but optional to use.

For the authentication between the UE and the network, there are two authentication methods as shown in this table. Both are applicable for 3GPP as well as non-3GPP access.



5G System Security Architecture
Security algorithms

5G Authentication Methods

5G AKA – 5G Authentication and Key Agreement

EAP-AKA’ – Extensible Authentication Protocol Authentication and Key Agreement

EAP-TLS – Extensible Authentication Protocol Transport Layer Security

5G AKA

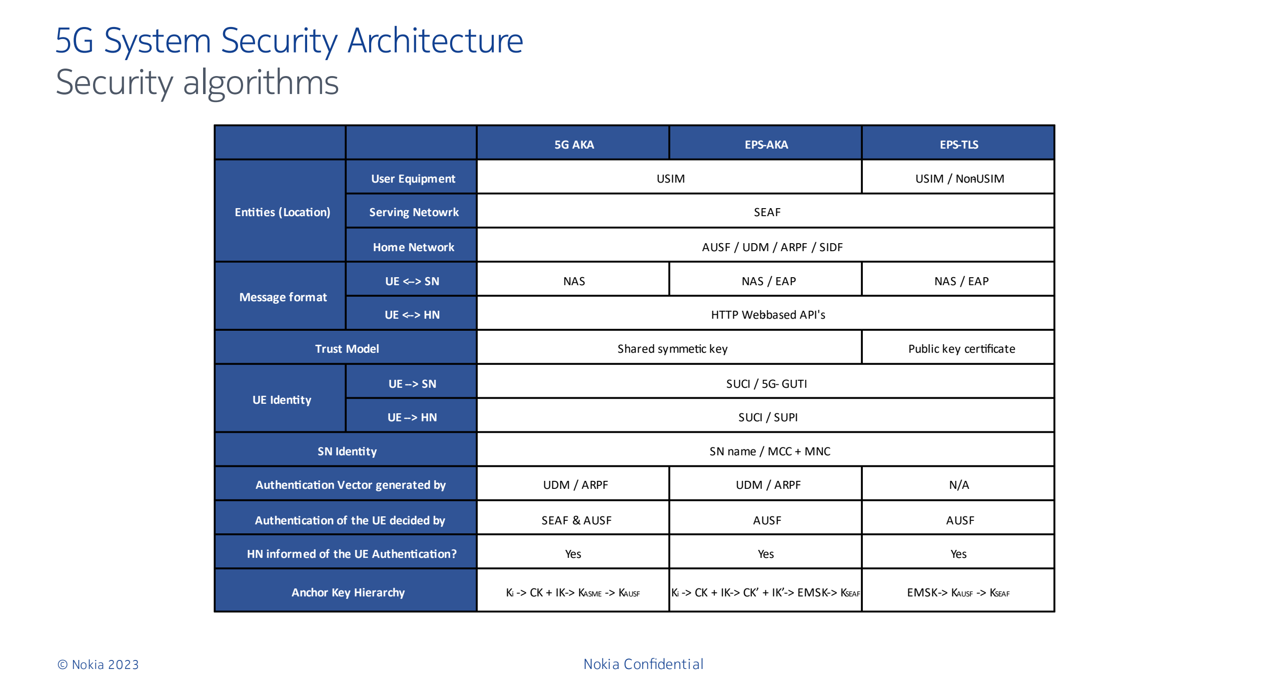
5G introduces new authentication-related services. The AUSF creates the authentication service via Nausf_UEAuthentication, and the UDM provides its authentication service through Nudm_UEAuthentication. In 5G-AKA, the SEAF may start the authentication procedure after receiving any signaling message from the UE. Please note that the UE should send the SEAF a temporary identifier (a 5G-GUTI) or an encrypted permanent identifier (a SUCI) if a 5G-GUTI has not been allocated by the serving network for the UE. The SUCI is the encrypted form of the SUPI using the public key of the home network. Thus, a UE’s permanent identifier, e.g., the IMSI, is never sent in clear text over the radio networks in 5G.

EAP-AKA’

EAP-AKA’ is another authentication method supported in 5G. It is also a challenge-and-response protocol based on a cryptographic key shared between a UE and its home network. It accomplishes the same level of security properties as 5G-AKA, e.g., mutual authentication between the UE and the network. Because it is based on EAP, its message flows differ from those of 5G-AKA. Note that EAP messages are encapsulated in NAS messages between the UE and the SEAF and in 5G service messages between the SEAF and the AUSF.

EAP-TLS

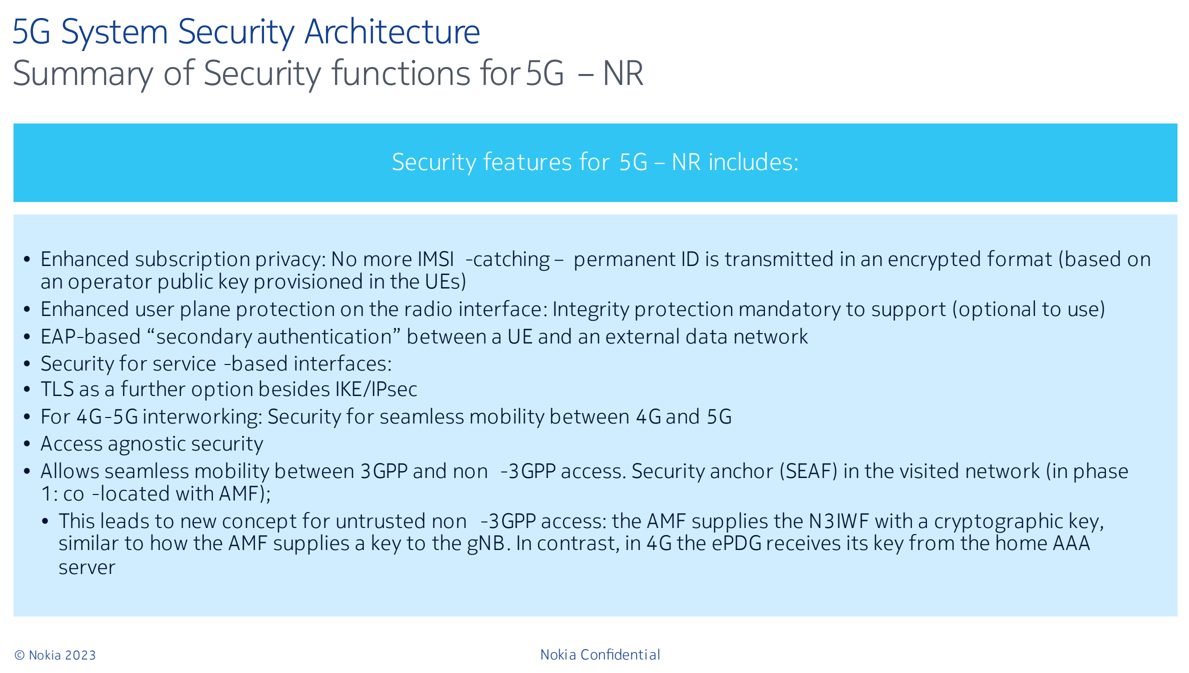
EAP-TLS is defined in 5G for subscriber authentication in limited use cases such as private networks and IoT environments. When selected as the authentication method by UDM/ARPF, EAP-TLS is performed between the UE and the AUSF through the SEAF, which functions as a transparent EAP authenticator by forwarding EAP-TLS messages back and forth between the UE and the AUSF. To accomplish mutual authentication, both the UE and the AUSF can verify each other’s certificate or a pre-shared key (PSK) if it has been established in a prior Transport Layer Security (TLS) handshaking or out of band.



5G System Security Architecture
Security algorithms

		5G AKA	EPS-AKA	EPS-TLS
Entities (Location)	User Equipment	USIM		USIM / NonUSIM
	Serving Netowrk	SEAF		
	Home Network	AUSF / UDM / ARPF / SIDF		
Message format	UE <–> SN	NAS	NAS / EAP	NAS / EAP
	UE <–> HN	HTTP Webbased API's		
Trust Model		Shared symmetic key		Public key certificate
UE Identity	UE –> SN	SUCI / 5G- GUTI		
	UE –> HN	SUCI / SUPI		
SN Identity		SN name / MCC + MNC		
Authentication Vector generated by		UDM / ARPF	UDM / ARPF	N/A
Authentication of the UE decided by		SEAF & AUSF	AUSF	AUSF
HN informed of the UE Authentication?		Yes	Yes	Yes
Anchor Key Hierarchy		K_i -> CK + IK-> K_{ASME} -> K_{AUSF}	K_i -> CK + IK-> CK' + IK'-> EMSK-> K_{SEAF}	EMSK-> K_{AUSF} -> K_{SEAF}

Table comparing the 3 different authentication methods in 5G.

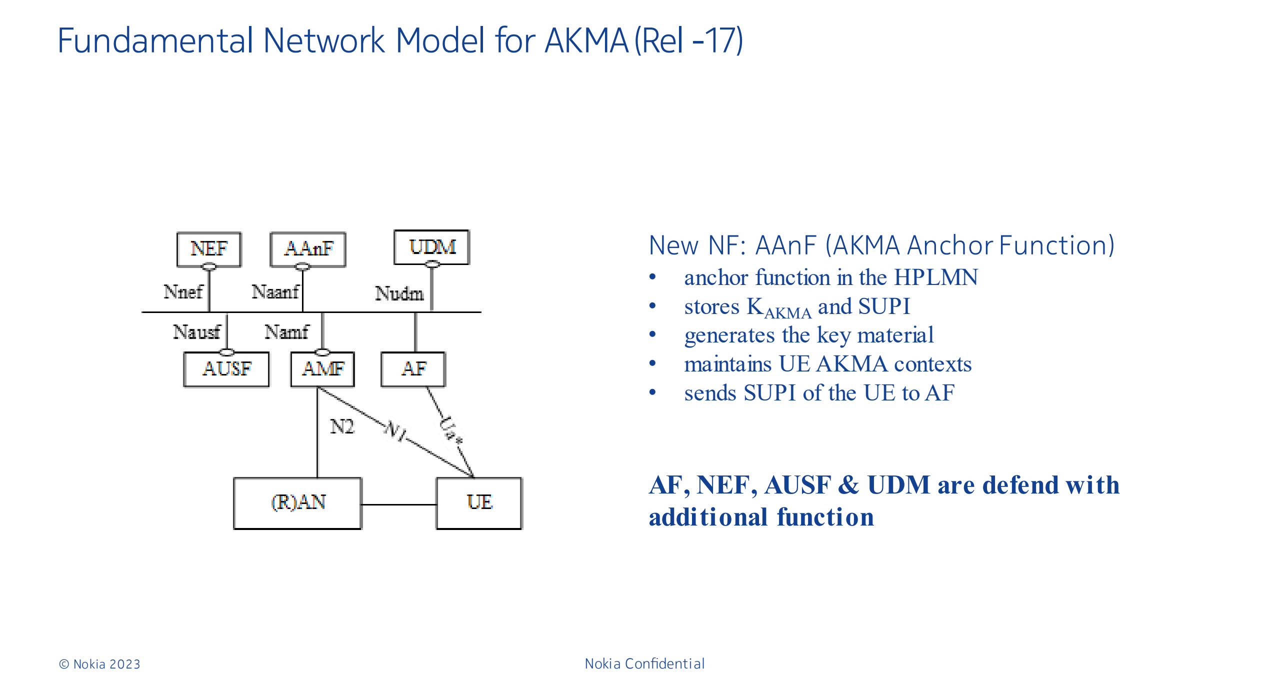


5G System Security Architecture
Summary of Security functions for 5G – NR

Security features for 5G – NR includes:

- Enhanced subscription privacy: No more IMSI-catching – permanent ID is transmitted in an encrypted format (based on an operator public key provisioned in the UEs)
- Enhanced user plane protection on the radio interface: Integrity protection mandatory to support (optional to use)
- EAP-based “secondary authentication” between a UE and an external data network
- Security for service-based interfaces:
- TLS as a further option besides IKE/IPsec
- For 4G-5G interworking: Security for seamless mobility between 4G and 5G
- Access agnostic security
- Allows seamless mobility between 3GPP and non-3GPP access. Security anchor (SEAF) in the visited network (in phase 1: co-located with AMF);
  - This leads to new concept for untrusted non-3GPP access: the AMF supplies the N3IWF with a cryptographic key, similar to how the AMF supplies a key to the gNB. In contrast, in 4G the ePDG receives its key from the home AAA server

Apart from the enhanced user plane protection on the radio interface outlined in the previous slide, other important 5G security enhancements are given in this table such as access agnostic primary authentication with home control, security key establishment and management, security for mobility, service based architecture security, inter-network security, privacy and security for services provided over 5G with secondary authentication.



Fundamental Network Model for AKMA (Rel -17)

New NF: AAnF (AKMA Anchor Function)

- anchor function in the HPLMN
- stores K_{AKMA} and SUPI
- generates the key material
- maintains UE AKMA contexts
- sends SUPI of the UE to AF

AF, NEF, AUSF & UDM are defend with additional function

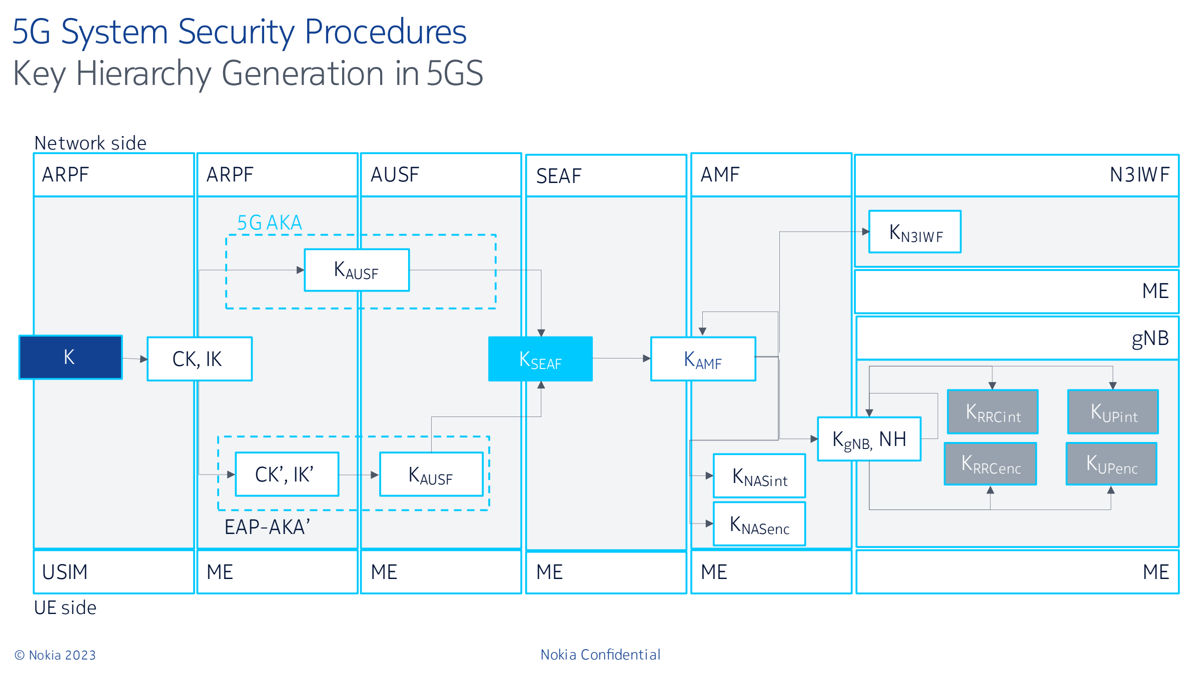
Authentication and Key Management for Applications based on 3GPP credential in 5G (AKMA) is a cellular-network-based delegated authentication system specified for the 5G system, helping establish a secure tunnel between the end user and the application server. Using AKMA, a user can log in to an application service only based on the 3GPP credential which is the permanent key stored in the user's tamper-resistant smart card UICC. The application service provider can also delegate the task of user authentication to the mobile network operator by using AKMA.

The AKMA Anchor Function (AAnF) is the anchor function in the HPLMN. The AAnF stores the AKMA Anchor Key (K_{AKMA}) and SUPI for AKMA service, which is received from the AUSF after the UE completes a successful 5G primary authentication. The AAnF also generates the key material to be used between the UE and the Application Function (AF) and maintains UE AKMA contexts. The AAnF sends SUPI of the UE to AF located inside the operator's network according to the AF request or sends to NEF.

Ref: TS 33.535

5G System Security Procedures

Nokia Confidential



5G System Security Procedures
Key Hierarchy Generation in 5GS

© Nokia 2023 Nokia Confidential

The long term secret key (K) provisioned is in the USIM and the 5G core network. It is used as the primary source of security context in the same way as in LTE.

After a successful primary authentication between the UE and the network, the serving network specific anchor key (KSEAF) is derived from K. From the anchor key, confidentiality and integrity protection keys are derived for Non Access Stratum signaling and the Access Stratum consisting of control plane, i.e.. radio resource control (RRC) messages, and user plane (UP).

Key generation and authentication in 5G

- **access agnostic**

2 mandatory authentication methods

- EAP-AKA'
- 5G AKA.

Both methods can be used for both

- untrusted non-3GPP access (e.g. Wifi)
- trusted 3GPP access.

AUSF (**Authentication Server Function**)

- introduced in 5G, functioning as EAP server

for EAP-AKA' and a pass-through for 5G-AKA.

K_{SEAF} is the anchor key

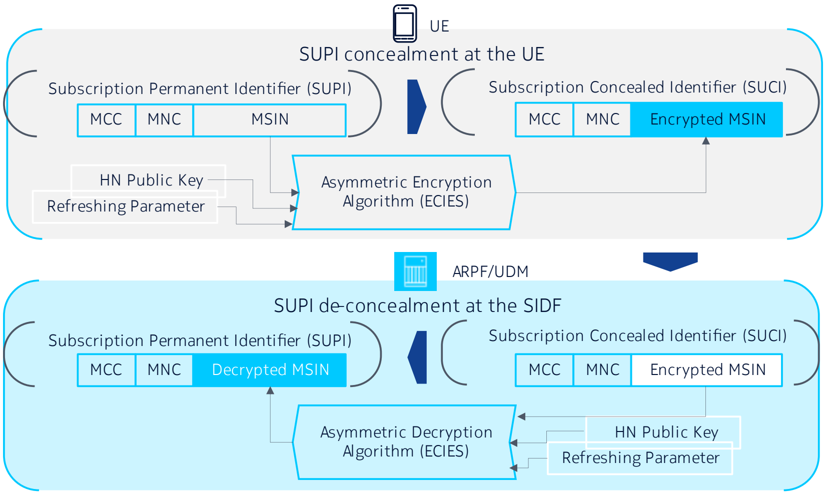
- to derive AS and NAS security context.

5G System Security Procedures

Subscriber Privacy

Enhanced privacy

- Encryption of subscriber identifier
- IMSI catcher attacks no longer possible; IMSI is never sent in clear.
- Only SUCI (encrypted SUPI (IMSI)) sent over air.
- Temporary ID reallocated to protect it from Temp ID catchers



UE

SUPI concealment at the UE

Subscription Permanent Identifier (SUPI)

MCC	MNC	MSIN

Subscription Concealed Identifier (SUCI)

MCC	MNC	Encrypted MSIN

HN Public Key

Refreshing Parameter

Asymmetric Encryption Algorithm (ECIES)

ARPF/UDM

SUPI de-concealment at the SIDF

Subscription Permanent Identifier (SUPI)

MCC	MNC	Decrypted MSIN

Subscription Concealed Identifier (SUCI)

MCC	MNC	Encrypted MSIN

Asymmetric Decryption Algorithm (ECIES)

HN Public Key

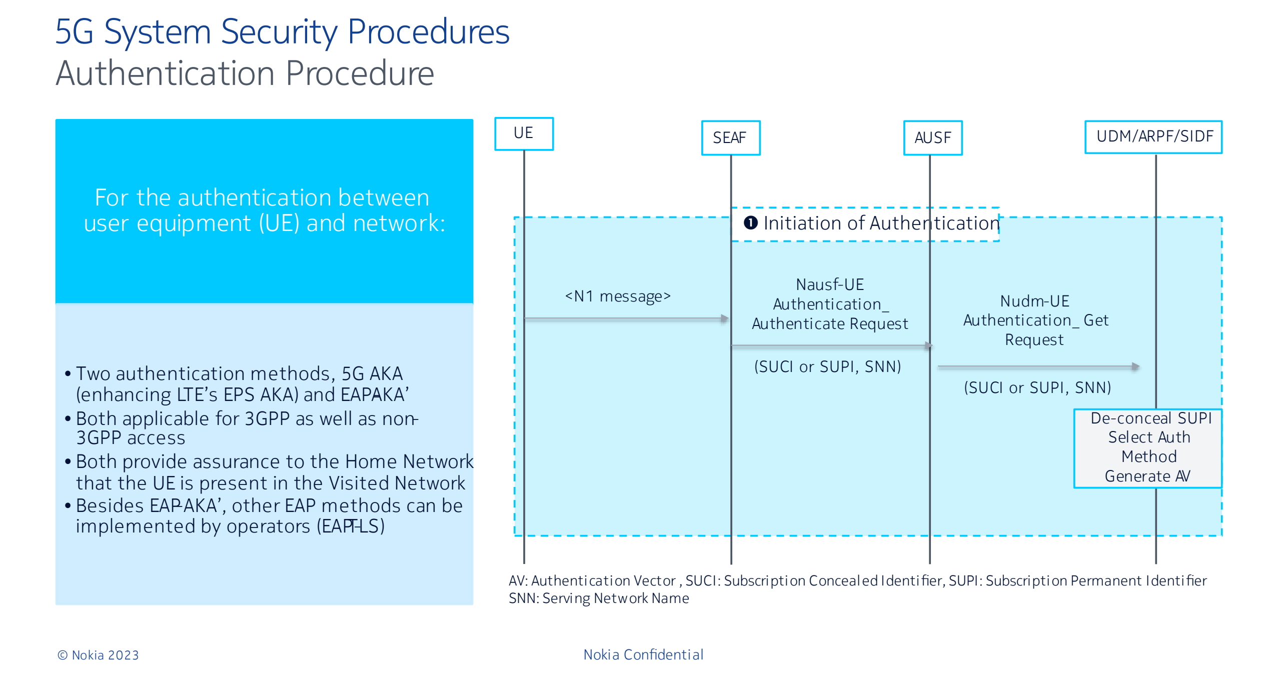
Refreshing Parameter

The subscription identifier SUPI, contains sensitive subscriber as well as subscription information thus it should not be transferred in clear text. The SUbscription Concealed Identifier, called SUCI, is a privacy preserving identifier containing the concealed SUPI.

The UE shall generate a SUCI using a protection scheme with the raw public key that was securely provisioned in control of the home network.

Further, the SUCI will contain routing information in the clear; that is to say, the UE shall not conceal the home network identifier, e.g. Mobile Country Code (MCC) or Mobile Network Code (MNC).

At the home network de-concealment of the SUPI from SUCI is done by the Subscription Identifier De-concealing Function (SIDF) which is located at the ARPF/UDM.



5G System Security Procedures

Authentication Procedure

For the authentication between user equipment (UE) and network:

- Two authentication methods, 5G AKA (enhancing LTE's EPS AKA) and EAPAKA'
- Both applicable for 3GPP as well as non-3GPP access
- Both provide assurance to the Home Network that the UE is present in the Visited Network
- Besides EAP-AKA', other EAP methods can be implemented by operators (EAPTLS)

UE

SEAF

AUSF

UDM/ARPF/SIDF

❶ Initiation of Authentication

<N1 message>

Nausf-UE Authentication_ Authenticate Request

(SUCI or SUPI, SNN)

Nudm-UE Authentication_ Get Request

(SUCI or SUPI, SNN)

De-conceal SUPI
Select Auth Method
Generate AV

AV: Authentication Vector , SUCI: Subscription Concealed Identifier, SUPI: Subscription Permanent Identifier
SNN: Serving Network Name

In 5G (unlike LTE) there are 2 types of authentication, primary authentication that all devices have to perform for accessing the 5GS services, and secondary authentication to an external data network.

Primary authentication procedure can be split into 2 steps: First step is the initiation of 5G authentication and authentication method selection.

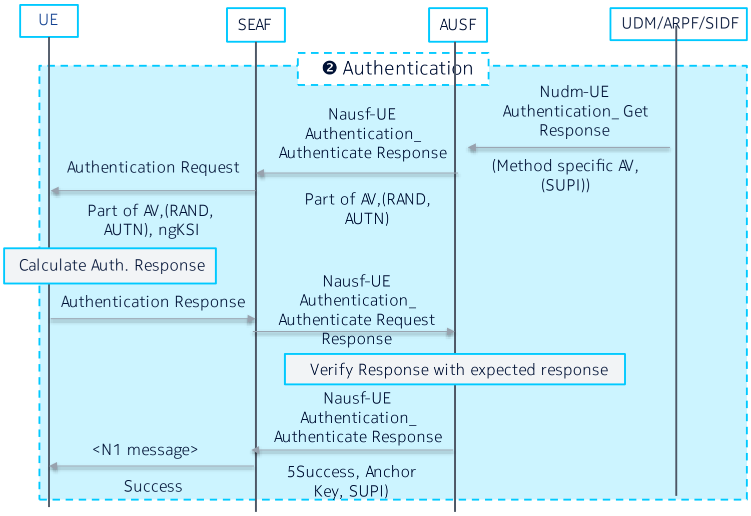
As shown in this diagram, the UE initiates the Authentication procedure be sending a registration request (N1 message) to the SEAF that contains a concealed identifier SUCI or 5G-Globally Unique Temporary UE Identity (5G-GUTI) where, as the name suggests, 5G-GUTI is a temporary identity assigned by the network during a previous session. On receiving a registration request from the UE the SEAF sends an authentication request message to the AUSF. Upon receiving the authentication request, the AUSF checks whether the requesting SEAF is authorized to use the SNN which is a form of home control in 5G. Then, SIDF is invoked to de-conceal the SUPI from SUCI. Based on SUPI and the subscription data, the UDM/ARPF choose the authentication method to be used.

5G System Security Procedures

Authentication Procedure

For the authentication between user equipment (UE) and network:

- Two authentication methods, 5G AKA (enhancing LTE’s EPS AKA) and EAPAKA’
- Both applicable for 3GPP as well as non3GPP access
- Both provide assurance to the Home Network that the UE is present in the Visited Network
- Besides EAP-AKA’, other EAP methods can be implemented by operators



UE

SEAF

AUSF

UDM/ARPF/SIDF

❷ Authentication

Nudm-UE Authentication_ Get Response

(Method specific AV, (SUPI))

Nausf-UE Authentication_ Authenticate Response

Part of AV,(RAND, AUTN)

Authentication Request

Part of AV,(RAND, AUTN), ngKSI

Calculate Auth. Response

Authentication Response

Nausf-UE Authentication_ Authenticate Request Response

Verify Response with expected response

Nausf-UE Authentication_ Authenticate Response

5Success, Anchor Key, SUPI)

<N1 message>

Success

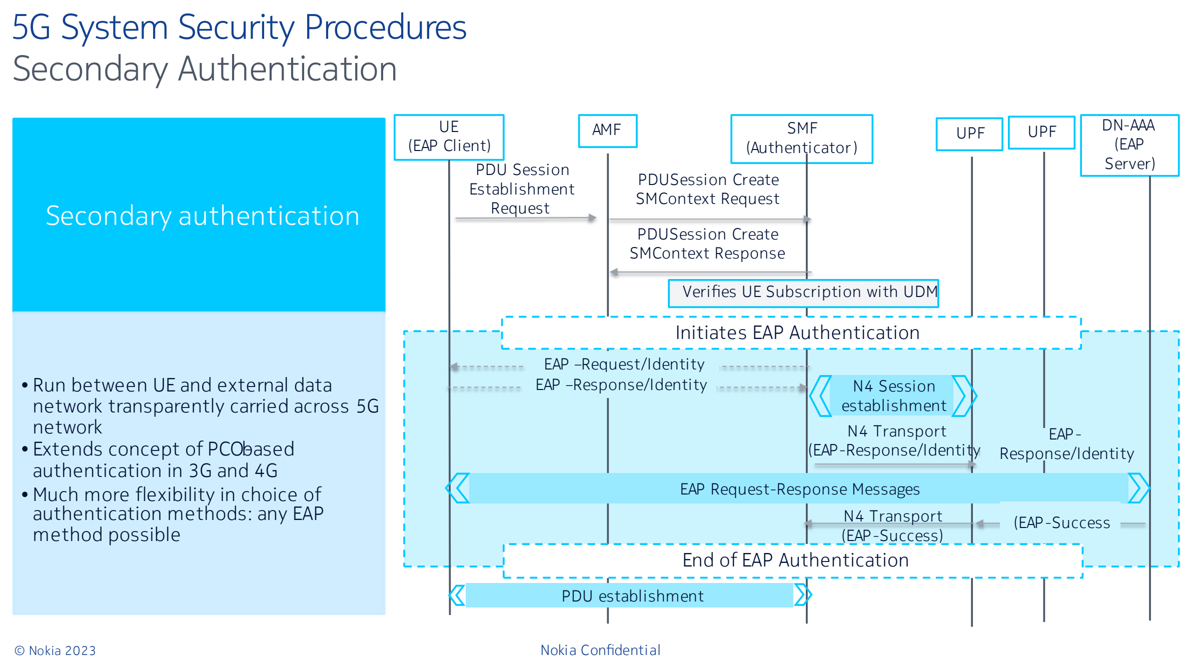
The second step is mutual authentication between the UE, subscription, and the network.

The authentication procedure involved in 5G, is briefly explained in the following steps: The UDM/ARPF first generates an Authentication Vector (AV). Then, the AUSF derives the KSEAF (anchor key) from KAUSF and sends

the Challenge message to the SEAF. At receipt of this message, the USIM computes a response RES and returns RES, CK, IK to the UE. The UE then sends the Challenge Response message to the SEAF in a NAS message Authentication Response message.

The SEAF forwards the Response Challenge message to the AUSF. The AUSF verifies the message to support increased home control and if the verification is successful, the AUSF acts according to the authentication method.

The SEAF sends the Success message to the UE in the N1 message.



5G System Security Procedures
Secondary Authentication

Secondary authentication

- Run between UE and external data network transparently carried across 5G network
- Extends concept of PCObased authentication in 3G and 4G
- Much more flexibility in choice of authentication methods: any EAP method possible

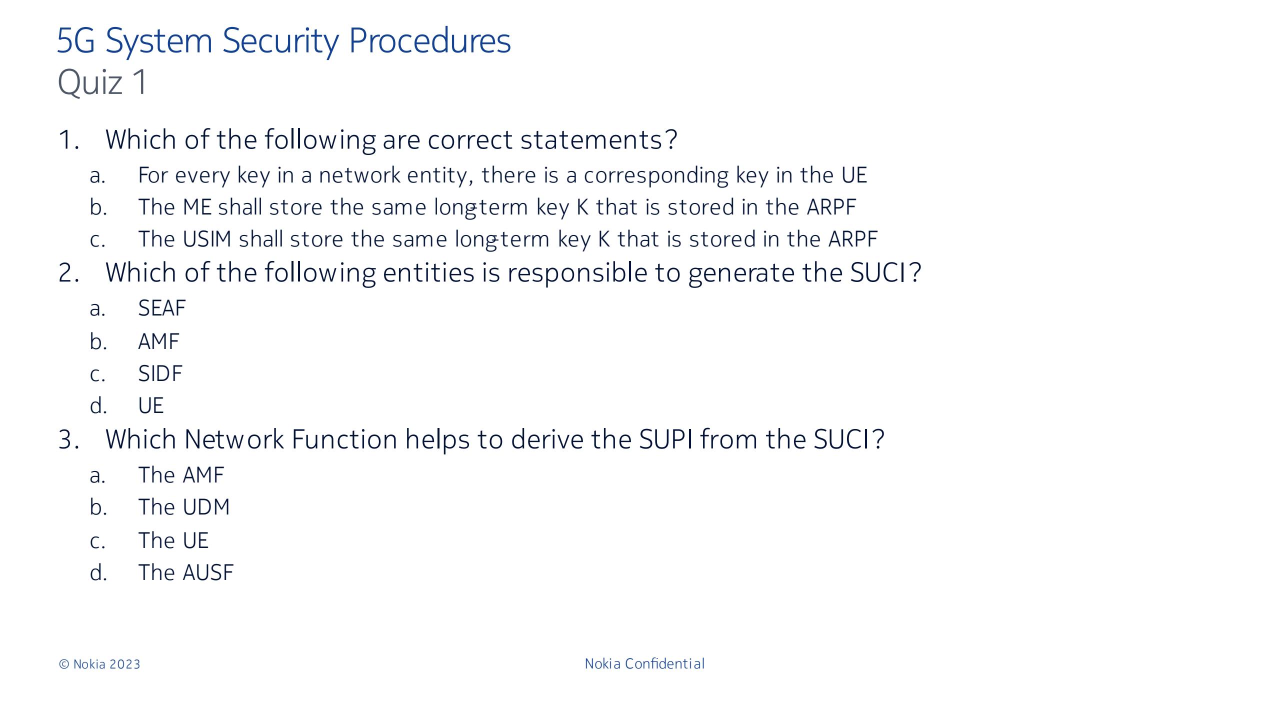
UE (EAP Client)
AMF
SMF (Authenticator)
UPF
UPF
DN-AAA (EAP Server)
PDU Session Establishment Request
PDUSession Create SMContext Request
PDUSession Create SMContext Response
Verifies UE Subscription with UDM
Initiates EAP Authentication
EAP –Request/Identity
EAP –Response/Identity
N4 Session establishment
N4 Transport (EAP-Response/Identity
EAP-Response/Identity
EAP Request-Response Messages
N4 Transport (EAP-Success)
(EAP-Success
End of EAP Authentication
PDU establishment

© Nokia 2023

Nokia Confidential

In addition, in 5G there is a secondary authentication to an external data network.

5G supports optional Extensible Authentication Protocol (EAP) based secondary authentication between the UE and an external data network (DN). The procedure is depicted in this protocol flow . Session Management Function (SMF) performs the role of the EAP Authenticator and relies on an external server to authenticate and authorize the UE’s request for the establishment of a PDU sessions.



5G System Security Procedures
Quiz 1

1. Which of the following are correct statements?
   a. For every key in a network entity, there is a corresponding key in the UE
   b. The ME shall store the same long-term key K that is stored in the ARPF
   c. The USIM shall store the same long-term key K that is stored in the ARPF
2. Which of the following entities is responsible to generate the SUCI?
   a. SEAF
   b. AMF
   c. SIDF
   d. UE
3. Which Network Function helps to derive the SUPI from the SUCI?
   a. The AMF
   b. The UDM
   c. The UE
   d. The AUSF

Wrap-up

In this module we have covered the following items:

Describe 5G System Security Architecture.
Explain 5G System Security procedures.