**3GPP TSG-WG SA2 Meeting #140E e-meeting *S2-200xxxx***

**Elbonia, August 19 – September 1, 2020 (revision of S2-200xxxx)**

**Source: Huawei, HiSilicon**

**Title: KI#1, update Sol#4, 8, 10 to address the ENs**

**Document for: Approval**

**Agenda Item: [Agenda Item]**

**Work Item / Release: [FS\_eNPN] / [Rel-17]**

*Abstract: This contribution introduces…*

# 1. Introduction/Discussion

This contribution aims at address the ENs of Solution #4, #8 and #10.

**For Solution #4: External Authentication and Authorization:**

Editor's note: Whether a domain name based SO ID can be broadcast in SIB is FFS. It is FFS whether the support of EAA indication is needed or not.

Refer to MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1.1), MFA TS MF.202, https://www.multefire.org/, Release 1.1, the subscription owner can use the domain name as a SO ID. A valid domain name is issued according to ICANN regulations or be free form complying with a domain name format. The domain name has a short form and a long form. The short form domain name is calculated from the long form domain name by calculating the SHA-256 has value of the long form and then extract and use the 24 most significant bits as the short from domain name. The short form domain name may be broadcast in SID.

The EAA indication is needed to prevent the unauthorized UEs from attempting to register the SNPN, it is used to indicate the support of “access using credentials of SO separate from the SNPN”, and so the UEs only attempt to connect to an SNPN using credentials of SO separate from the SNPN when this indication is advertised.

**Proposal 1**: remove this EN with the justification above.

Editor's note: It is FFS what interface/protocol is used between the AMF and the AAA-P.

AAA-P can be a new 5GC NF or collocated with AUSF or NSSAAF, it is responsible to interact with the AAA-S. The interface between AMF/SMF and AAA-P is assumed to be service based interface.

**Proposal 2**: remove this EN with the justification above.

Editor's note: It is FFS what is the content of UE subscription and how to deliver the appropriate UE subscription data to SNPN AMF/SMF, and what interface/protocol is used between the SMF and the AAA-P.

UE subscription data delivered to AMF may contain the information on DNN, S-NSSAI, UE-AMBR, dedicated SMF, etc. This can help AMF to perform UE’s access and mobility management, optionally SMF selection.

UE subscription data delivered to SMF may contain the information on DNN, S-NSSAI, session-AMBR, service flow template, UE address, etc. This can help SMF to perform PDU session management, optionally control the traffic allowed within the PDU Session.

In the case of AAA-P provides the UE subscription data to AMF/SMF, the AAA-P can acquire the data from AAA-S as individual UE subscription or acquire the local configuration per SO as common UE subscription. External UE ID or SO ID is used to index the UE subscription data.

In the case of UDM provides the UE subscription data to AMF/SMF, the UE subscription data can be per individual UE or common subscription shared by a group of UEs. Internal UE ID is used to index the UE subscription data. Internal UE ID can be generated based on external UE ID and configured at UDM. Alternatively, the Internal UE ID can be separate from the external UE ID.

**Proposal 3**: remove this EN and update the solution with the justifications above.

Editor's note: Need to perform secondary authentication with the same AAA-S as was used for primary authentication is FFS.

Remove the case where secondary authentication and authorized procedure is used to acquire UE subscription data from SMF.

**Proposal 4**: remove this EN and update the solution to delete the aspects related to this EN.

**For Solution #8: SNPN access using 3rd party credentials via external Credential Provider:**

Editor's note: Impacts to security architecture and key derivation resulting from the above architecture need to be evaluated by SA WG3.

Editor's note: It is FFS whether the SNPN needs to provide the UE subscription data at UDM/UDR. If this is required, it is FFS the content in UE subscription data that indexed by SUPI/SUCI generated based on CdP-UE ID. It is FFS how to correlate the UE subscription data in SNPN and UE credentials in CdP.

In the case of SNPN UDM/UDR provides the common subscription data per CdP, the AMF/SMF can retrieve the data using CdP IP, which can be derived from UE’s SUPI/SUCI generated based on CdP-UE ID since SUPI provisioned by the CdP is on NAI format and includes the CdP ID in the domain part of the NAI, e.g. UEID@CdPID.

In the case of SNPN UDM/UDR provides the individual subscription data per UE, as typically CdP corresponds with an already existing credential management system, so it requires generating SUPI based on CdP-UE ID and provision the individual subscription indexed by this SUPI into the SNPN UDM/UDR. However if the individual subscription data is not indexed by SUPI generated based on CdP-UE ID, then the UE shall be pre-configured with one SUPI assigned by the SNPN, once the SNPN UDM/AUSF determines that primary authentication is executed towards a certain CdP, then SNPN AMF/AUSF asks the UE to provide the CdP-UE ID to continue the primary authentication.

In the case of the SNPN does not provide UE subscription, then the CdP should provide the subscription data, this case can refer to Sol#4.

**Proposal 5**: remove this EN and update the solution with justifications above.

Editor's note: It is FFS whether CdP is a 5GC NF since the CdP can use the SUPI in step 5.

AUSF map SUPI (if generated based on CdP-UE ID) to CdP-UE ID or AUSF/AMF asks the UE to provide the CdP-UE ID when AUSF interacts with CdP.

**Proposal 6**: remove this EN and update the solution with justifications above.

**For Solution #10: UE external subscription data stored in the SNPN:**

Editor's note: It is FFS whether and how the (external) UE-ID can be also used in the Serving SNPN instead of the SI.

Editor's note: This clause lists impacts to services, entities and interfaces.

The SI is used to index the UE subscription in SNPN, it MUST be a SUPI, and should not be known to the SP.

In the case of the SI is generated based on (external) UE-ID per agreements between SNPN and SP. the SI should be provided by UE during registration.

In the case of the SI has no relation with (external) UE-ID, then SI should be configured at UE, the SI is provided by UE during registration. The UDM subscription/local configuration indicates the primary AA to the AAA-server, and then the AUSF/AMF can ask UE to provide the (external) UE-ID to proceed the primary AA towards the AAA-server.

**Proposal 7**: remove this EN and update the solution with justifications above.

# 2. Text Proposal

It is proposed to capture the following changes vs. TR 23.xxx.

\* \* \* \* First change \* \* \* \*

## 6.4 Solution #4: External Authentication and Authorization

### 6.4.1 Introduction

This solution addresses the key issue #1: Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN. This solution allows the UE using subscription or credentials owned by an entity separate from the desired SNPN to register and request connectivity at the desired SNPN.

This solution assumes that the AAA Server is the separate entity that owns and authenticates UE's SNPN security related subscription (non-3GPP identities e.g. non-IMSI and credentials). In addition, there are several ways to provide the mobility related subscription, e.g., information on DNN, S-NSSAI, UE-AMBR, dedicated SMF, etc. to enable AMF perform UE’s access and mobility management, optionally SMF selection, or the service related subscription, e.g., information on DNN, S-NSSAI, session-AMBR, service flow template, UE address, etc. to enable SMF perform PDU session management:

* AAA-S owns the mobility related subscription and service related subscription as individual UE subscription and provides them to AMF or SMF via AAA-P; or
* AAA-P is pre-configured with the mobility related subscription and service related subscription as common UE subscription per SO, and provides them to AMF or SMF; or
* UDM/UDR owns the mobility related subscription and service related subscription as individual or common UE subscription, the UE subscription is indexed by a SUPI generated based on External UE ID, i.e., UE ID assigned as part of the subscription owned by the AAA-S.

NOTE: It is assumed that the SNPN supports the SUPI generated based on External UE ID, the UE subscription indexed by the SUPI is provisioned at the SNPN UDM/UDR per agreements between SNPN and the SO.

* UDM/UDR owns the mobility related subscription and service related subscription as individual or common UE subscription, the UE subscription is indexed by a SUPI assigned by the SNPN and this SUPI has no relation with the External UE ID.

This applies for the cases where:

- SNPN is deployed as an incremental enhancement or supplementary to the existing communications (e.g. Ethernet, WLAN) infrastructure to leverage the benefits of reliable, low latency wireless communications to meet specialized and stringent requirements for industries. The existing user account (e.g. identities/credentials) management server is used as the AAA Server; or

- SNPN is deployed as an ad-hoc communication infrastructure to support audio/video applications (includes television and radio studios, private events, medical operating). An entity separate from the SNPN provides the user account (e.g. identities/credentials) management server as the AAA Server and the ad-hoc SNPN allows UE access with the non-3GPP identities/credentials (e.g. user name/password).

### 6.4.2 Functional Description

#### 6.4.2.1 Architecture and Concept



Figure 6.4.2.1-1: Architecture in case separate entity that owns the subscription is AAA-S

NOTE: For the sake of simplicity, the figures above do not show all NFs and interfaces.

**Subscription Owner (SO):** The entity that provides the AAA-S and the services to the end user.

**AAA-Server (AAA-S):** Entity separate from the desired SNPN but owns UE's desired SNPN subscription. It is also responsible to authenticate/authorize the UE based on the UE's SNPN subscription. It is deployed by the SO.

**AAA Proxy (AAA-P):** It acts as the relay for interactions between SNPN and the AAA-S and undertakes any AAA protocol interworking with the AAA protocol supported by the AAA-S. The AAA-P uses towards the AAA-S an AAA protocol message of the same protocol supported by the AAA-S. It is deployed per SNPN. AAA-P can be a new 5GC NF or collocated with AUSF or NSSAAF.

**Nx:** Reference point between AAA-P and AAA-S that support AAA protocol, e.g. Diameter.

**SO-ID:** SO Identity, it is used to uniquely identify a SO. SO-ID can be domain name. The AAA-P can address the AAA-S with the SO-ID. The subscription owner can use the domain name as a SO-ID. A valid domain name is issued according to Internet Corporation for Assigned Names and Numbers - ICANN regulations or be free form complying with a domain name format. A domain name based SO-ID has a short form and a long form. The short form domain name based SO-ID is calculated from the long form domain name by calculating the SHA-256 hash value of the long form and then extract and use the 24 most significant bits as the short from domain name based SO-ID. The short form domain name based SO-ID may be broadcast. Refer to MFA TS MF.202 [x].

**External Subscription (E-Sub):** UE's SNPN subscription (credential/identity), which is stored in AAA-S. It can be non-3GPP identities (e.g. non-IMSI) and credentials. E-Sub is used to authenticate and authorize UE's access to the desired SNPN that provides connectivity to services of the SO.

**External Authentication and Authorization (EAA):** Authentication/Authorization executed by the AAA-S based on UE's E-Sub, in particular the security related subscription.

#### 6.4.2.2 EAA for the UEs with E-Sub

This clause applies when the UE is provisioned with the E-Sub (subscription stored at entity separate from the desired SNPN):

- UE that is provisioned with E-Sub also contains the network configuration, which is used for SNPN discovery and selection; the network configuration contains the following information for each desired SNPN:

- PLMN ID+NID; and

- Priority; and optionally

- Subscribed SO ID.

- SNPN broadcasts the following information:

- PLMN ID+NID; and

- support of EAA, and optionally

- Supported SO-ID list.

NOTE: The EAA indication is used to indicate the support of “access using credentials of SO separate from the SNPN”, and the UEs only attempt to connect to an SNPN using credentials of SO separate from the SNPN when this indication is advertised, thus to prevent the unauthorized UEs from attempting to register the SNPN.

- UE discovers and selects the desired SNPN based on network configuration and the broadcast information. When the UE receives the broadcast from the network that supports the EAA, the UE in order of the priority in network configuration checks the first desired SNPN that is supported in the broadcast, i.e. the PLMN ID+NID of the desired SNPN is equal to the PLMN ID+NID received in broadcast, and the Subscribed SO ID of the desired SNPN is present in the Supported SO-ID list received in broadcast.

- UE using E-Sub performs registration to the SNPN. The SUPI provided at Registration request message is generated based on External UE ID of E-Sub. Alternatively, the SUPI provided at Registration request message is pre-configured at the UE and has no relation with the E-Sub.

- Based on local policy or UDM indication the SNPN triggers the EAA for the UE. The EAA is performed between the UE and the AAA-S via SNPN.

- SNPN and UE establishes the PDU Session to access to SP services.

### 6.4.3 Procedures

In this case, E-Sub is used to authenticate and authorize the UE for access to the desired SNPN that provides connectivity to services of the SO.

In this case, UE selects and registers to the desired SNPN using network configuration in E-Sub and received broadcast system information. Instead of Authentication/Security at AUSF/UDM of SNPN during the registration, the AMF triggers the EAA for UEs using E-Sub based on local policy, or the UDM triggers the EAA for UEs using E-Sub based on UE subscription stored at UDM/UDR. The SNPN establishes security context and decides whether to accept the registration based on EAA results.



Figure 6.4.3-1: AMF triggered EAA of UEs with E-Sub

In this procedure AAA-S owns the mobility related subscription and service related subscription as individual UE subscription and provides them to AMF or SMF via AAA-P; or AAA-P is pre-configured with the mobility related subscription and service related subscription as common UE subscription per SO, and provides them to AMF or SMF. This mobility related subscription and service related subscription are used during UE’s access and mobility management, session management procedure.

1. Steps 1-7 in clause 4.2.2.2.2 of TS 23.502 [6] are performed with the following changes:

 In Step 1, the UE includes the support for EAA in the AN message and "EAA" Registration Type value in Registration Request message. The UE generates the SUPI based on the UE Identity in E-Sub and include this SUPI in the Registration Request message.

 In Step 2, the RAN selects an AMF that supports for EAA.

 The Registration Type indicates that the UE desires to use the E-Sub to register to the SNPN, then AMF needs to select the AAA-P that supports interactions with the AAA-S, the AMF needs to contact with the selected AAA-P when the AMF needs to perform primary authentication/authorization.

2. The AMF decides to trigger EAA based on UE request and local policy, the AMF may ask the UE to start EAA procedure, and selects an AAA-P that supports for exchange of EAA signalling between UE and AAA-S.

3. Based on the UE Identity that contains the SO-ID, the AAA-P addresses the AAA-S. The EAA is performed between the UE and the AAA-S via SNPN and the AMF receives the EAA results. Besides that, AAA-S provides the anchor key to AAA-P, AAA-P further provides it to AMF, and the AMF generates the security context with that anchor key.

NOTE: The details of this EAA procedure will be defined by SA WG3.

4. AMF retrieves the UE subscription from AAA-P, which obtains the UE subscription from AAA-S as individual UE subscription or obtain the local configuration per SO as common UE subscription. The UE subscription data may include, e.g., information on DNN, S-NSSAI, UE-AMBR, dedicated SMF, etc. to enable AMF perform UE’s access and mobility management, optionally SMF selection. Then steps 21-22 in clause 4.2.2.2.2 of TS 23.502 [6] are performed.

5. When SMF receives the PDU Session Establishment request, the SMF may retrieve the UE subscription from AAA-P, which obtains the UE subscription from AAA-S as individual UE subscription or obtain the local configuration per SO as common UE subscription. The UE subscription data may include, e.g., information on DNN, S-NSSAI, session-AMBR, service flow template, UE address, etc. to enable SMF perform PDU session management.



Figure 6.4.3-2: UDM triggered EAA of UEs with E-Sub

In this procedure, UDM/UDR owns the mobility related subscription and service related subscription as individual or common UE subscription, and provides them to AMF or SMF during UE’s access and mobility management, session management procedure. The SUPI that used to index the subscription is generated based on the UE Identity in E-Sub or the SUPI has no relation with the UE Identity in E-Sub and is pre-configured at the UE.

In the case of a SUPI generated based on UE Identity in E-Sub is provided during registration procedure, the subscription in UDM indicates that the primary authentication and authorization should be performed towards the AAA-S server, and the AUSF/AAA-P initiates the authentication and authorization towards the AAA-S based on the SO-ID extracted from the SUPI and the UDM indication.

In the case of a SUPI which has no relation with UE Identity in E-Sub is provided during registration procedure, the subscription in UDM indicates that the primary authentication and authorization should be performed towards the AAA-S server, and before the AUSF/AAA-P initiates the authentication and authorization towards the AAA-S, the AUSF/AAA-P should first ask UE to provide the UE Identity in E-Sub based on UDM indication. Alternatively, the AMF may first try to use the primary authentication procedure as defined in TS 33.501, consequently the UDM/AUSF sends to AMF the Authentication method (primary authentication towards AAA-S), and then AMF triggers the primary network authentication, asks UE to provide the UE Identity in E-Sub and selects the AAA-P that supports interactions with the AAA-S.

### 6.4.4 Impacts on services, entities and interfaces

Impacts on UE:

 Provisions with the E-Sub owned by the SO, as well as the corresponding network configuration for discovery and selection of the available desired SNPN that connects to the AAA-S.

 Selects the desired SNPN based on network configuration and the received broadcast information.

 Indicates the support of EAA to RAN and the EAA Registration Type to AMF.

Impacts on RAN:

 Broadcasts the support for EAA and the supported SO-ID list.

 Selects the AMF that supports for EAA based on UE's EAA indication.

Impacts on AMF:

 Triggers the EAA based on "EAA" Registration Type or UDM indication and Selects the AAA-P that supports for EAA.

 Receives UE subscription from AAA-P.

Impacts on SMF:

 Receives UE subscription from AAA-P.

Impacts on UDM:

 Determines to trigger the primary authentication and authorization towards the AAA-S server and indicate to AAA-P/AUSF.

AAA-P:

 Addresses the AAA-S with UE Identity.

 Interacts with the AAA-S to obtain the EAA results and UE subscription.

 Relays EAA messages towards AAA-S and performs related protocol conversion based on AMF indication or UDM indication.

\* \* \* \* Second change \* \* \* \*

## 6.8 Solution #8: SNPN access using 3rd party credentials via external Credential Provider

### 6.8.1 Introduction

This solution addresses key issue 1 "Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN".

The solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN 5GS.

### 6.8.2 Functional Description

#### 6.8.2.1 Definitions

The following definitions apply to this solution:

**SNPN:** An SNPN which enables access for UEs using credentials owned by an entity separate from the SNPN.

**Credentials Provider (CdP):** An entity, separate from the SNPN that supports that its credentials are used to access an SNPN.

**CdP-ID:** Identifies the CdP that issued the credentials that a UE is using to access an SNPN.

NOTE: Appropriate terminology regarding Credential Provider can be decided in normative phase.

#### 6.8.2.2 Architecture

Figure 6.8.2.2-1 depicts the architecture for the solution, i.e. the SNPN includes a complete 5GS SNPN network and the CdP provides credential management type of functionality.



Figure 6.8.2.2-1: Access to SNPN services using credentials from Credential Provider (CdP) for authentication in the SNPN

Editor's note: Impacts to security architecture and key derivation resulting from the above architecture need to be evaluated by SA WG3.

#### 6.8.2.3 High level principles of the solution

This solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN. The credential management functionality provided by the CdP includes handling of identifiers and corresponding security material used to identify the devices used within the SNPN and to mutually authenticate these devices and the SNPN 5GS. The credential provider will typically correspond with an already existing credential management system owned by the vertical owner of the SNPN 5GS.

The UE is provisioned with non-AKA credentials managed by the CdP, which include an identifier and related security information and the CdP Identifier. The UE initiates registration in the SNPN using a SUPI containing a network-specific identifier, provided by the CdP and provisioned in the UE.

The AMF initiates primary authentication, registration and subscription management procedures for the UE towards the AUSF and UDM of the SNPN based on existing procedures defined in TS 33.501 [7]. It is assumed that there are AUSF and UDM instances within the SNPN supporting the SUPIs of the CdPs (e.g. SUPI ranges or CdP ID) the SNPN has agreements with. Alternatively, the SNPN may use the SUPIs separate from the CdPs.

For the primary authentication procedure, the UDM allows the UE to run primary authentication with non-AKA credentials owned by a certain CdP. The UDM indicates to the AUSF to proceed with primary authentication involving the corresponding CdP.

One possibility is for the SNPN to delegate the authentication server role to the CdP (i.e. the CdP supports AAA functionality). In this case, the AUSF acts as EAP authenticator and interacts with the CdP to execute the primary authentication procedure using the CdP credentials. The AUSF uses a AAA-P/IWF to interact with the CdP. The AAA-P/IWF undertakes any AAA protocol interworking between SBI services used by the AUSF and the AAA protocol supported by the CdP. This allows the AUSF to remain a full SBA entity within the 5GC architecture.

For the registration and subscription management procedures, it is assumed that the SNPN has provisioned in the UDM/UDR individual subscriptions for the UEs that use non-AKA credentials from the CdP. Alternatively, the SNPN may use common subscription profiles per CdP for these UEs.

- In the case of SNPN UDM/UDR provides the individual subscription data, the AMF/SMF can retrieve the data using a SUPI. It is assumed that the SUPI may be generated based on CdP-UE ID and provisioned at the UDM/UDR as part of the individual subscription data or the SUPI may not relate with the CdP-UE ID and is provisioned at the UDM/UDR and UE.

- In the case of SNPN UDM/UDR provides the common subscription data, the AMF/SMF can retrieve the data using CdP IP, which can be derived from UE’s SUPI/SUCI generated based on CdP-UE ID.

- In the case of SNPN UDM/UDR doesn’t provide the common subscription data nor individual subscription data, refer to solution #4 for subscription handling for registration and session management procedure.

### 6.8.3 Procedures

This clause shows the interactions to enable UEs to access an SNPN which makes use of a credential management system managed by a Credential Provider external to the SNPN proposed in this solution.



Figure 6.8.3-1: UE registration in SNPN using CdP as authentication server and CdP-UE ID for SUPI derivation

0. The UE is configured with non-AKA credentials from the CdP e.g. SUPI containing a network-specific identifier, CdP ID and security information, and optionally a list of SNPNs that the CdP has an agreement/SLA with.

 It is also assumed that there are AUSF and UDM instances within the SNPN that support the SUPIs of the CdPs (e.g. SUPI ranges or CdP ID) the SNPN has agreements with. The AMF selects these AUSF/UDM instances based on information locally configured in the AMF or provided by the SNPN NRF.

1. The UE selects the SNPN and initiates UE registration in the SNPN. The UE creates a SUCI/SUPI based on the CdP-UE ID provided by the CdP and provisioned in the UE.

NOTE 1: It is assumed that the SUPI is on NAI format and includes also the CdP ID in the domain part of the NAI, e.g. UEID@CdPID. Whether the SUPI within the SUCI is encrypted is FFS in SA WG3.

2. The AMF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF as currently specified in TS 33.501 [7]. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [4].

3. The AUSF checks with UDM within the SNPN for the authentication method to be executed for the UE using a Nudm\_UEAuthentication\_Get service operation as currently specified in TS 33.501 [7]. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [4]. The UDM resolves the SUCI to the SUPI before checking the authentication method applicable for the UE. The UDM can obtain the common subscription data or individual subscription data based on the SUPI.

4. The UDM provides the AUSF with the UE SUPI and the applicable authentication method for the UE. In this case, the UDM indicates to the AUSF to run primary authentication with non-AKA credentials owned by a certain CdP. The UDM provides the AUSF also with the address of the CdP if required.

NOTE 2: The SNPN may support credentials managed by different CdPs.

5. Based on the indication from the UDM, the AUSF interacts with the CdP to execute the primary authentication procedure. The AUSF derives the CdP-UE ID from the SUPI. The AUSF uses a AAA-P/IWF to interact with the CdP. The AAA-P/IWF undertakes any AAA protocol interworking between SBI services used by the AUSF and the AAA protocol supported by the CdP.

NOTE 3: In this case, the AUSF is not exposing primary authentication services externally to the SNPN 5GS but rather the AUSF is consuming primary authentication service from an authentication server external to the SNPN based on SNPN configuration.

6. The UE executes the applicable authentication method with the CdP.

7. After successful authentication, the AMF is provided with the successful indication together with the SUPI of the UE and the resulting security key.

NOTE 4: Details of the authentication procedure are for FFS in SA WG3. This includes potential impacts on key hierarchy and how UE is aware of key hierarchy to be used.

8. After successful authentication, the AMF continues with the registration procedure for the UE in the SNPN. The AMF selects a UDM based on the UE's SUPI to perform AMF registration and subscription management procedures with UDM. The SNPN may have provisioned individual subscriptions for the UEs that use non-AKA credentials from the CdP in the UDM/UDR. Alternatively, the SNPN may use common subscription profiles for these UEs.

NOTE 5: The details of how subscriptions for UEs that use credentials from the CdP are provisioned/managed within the UDM/UDR are Out of Scope of this solution.

9. The AMF completes the registration procedure in the SNPN. The security keys result from the primary authentication procedure using CdP non-AKA credentials are used for subsequent security procedures within the SNPN (i.e. Security Mode Command).



Figure 6.8.3-2: UE registration in SNPN using CdP as authentication server and an SUPI not related with CdP

In this procedure, the UE and SNPN/UDM is configured with the SUPI, which has no relation with the CdP. Compared to procedure in figure 6.8.3-1, the following differences are captured:

0. UE is configured with a SUPI that has no relation with CdP-UE ID. The UDM/UDR is also provisioned with this SUPI.

1. The SUPI/SUCI used in this step is the SUPI configured at step 0.

5. Based on the indication from the UDM, the SNPN AUSF asks the UE to provide the CdP-UE ID via AMF before initiating the primary authentication and authorization towards CnP.

### 6.8.4 Impacts on services, entities and interfaces

UE impacts:

- Possible impact on key hierarchy (to be confirmed by SA WG3).

AMF impacts:

- Ask UE to provide the CdP-UE ID as requested by AUSF.

AUSF impacts:

- Delegation of authentication server role to the CdP; possible impacts on key hierarchy need to be analysed by SA WG3.

UDM impacts:

- Possible impact on SUCI to SUPI de-concealment (to be confirmed by SA WG3).

- Indication of authentication method using non-AKA credentials from applicable CdP to the UE.

AAA-IWF/P impacts:

- New NF supporting protocol interworking with CdP acting as e.g. external EAP server.

\* \* \* \* Third change \* \* \* \*

## 6.10 Solution #10: UE external subscription data stored in the SNPN

### 6.10.1 Introduction

This solution is for Key Issue #1, "Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN". The solution is based on the following principles:

- The UE the security-related data (e.g. UE Keys) are stored in the SO domain (e.g. AAA server).

- The subscription data for the UE is either a) pre-provisioned in the SNPN, or b) provisioned on-demand to the SNPN.

- The UDM/UDR in the SNPN generates a UE subscription identifier (SI, i.e., SUPI) for the provisioned subscription data. The SI is used in the Serving SNPN to identify the Subscription Data (without security credentials). The SI is configured at UE and is sent to AMF and used internally in the SNPN during the UE is served by the SNPN. The SI may or may not related to the External UE ID.

- The AMF uses both UE identities: External UE-ID (from the Registration Request message) and the SI as follows:

- The External UE-ID is used for security procedures (e.g. key derivation in the AMF, signaling exchange with the AUSF).

- The SI is used for subscription data retrieval from the UDM/UDR.

- The AMF populates the SI to the other NFs (SMFs, PCF, etc.) during various procedures.

Figure 6.10.1-1 shows the architecture assumed for this solution. The AAA server stores the UE security data (for authentication and authorisation) and also the UE service subscription which is valid for the UE (e.g. type of service, allowed bitrate, spending allowance, mobility restrictions, etc.). The red path shows the signalling flow exchange for the primary network access authentication and authorization. The eAUSF (enhanced Authentication Server Function) can be a known AUSF function, but can be also considered as enhanced AUSF implementing additional functionality (e.g. AAA proxy functionality, AAA message translation to SBI, etc.). The blue path shows the signaling flow exchange for the UE subscription data provisioning in the SNPN's UDM/UDR. The signaling flow between UDM and AAA server can be sent directly or traversing through the eAUSF.



Figure 6.10.1-1: Architecture for storing the UE subscription data in the SNPN while the security signalling is performed to the SO

### 6.10.2 Functional Description

The solution uses the principles from clause 6.10.1.

### 6.10.3 Procedures

Two different procedures are shown below.

#### 6.10.3.1 UE subscription data pre-stored in the SNPN



Figure 6.10.3.1-1: Registration and PDU Session establishment procedures when the UE subscription data is pre-stored in the SNPN

0a. The UE has a subscription with service provider (SP). The subscription is identified by an External UE-ID.

0b. The SNPN can store one or more subscription data sets for different groups of UEs, which are SP subscribers. The subscription data set is generated and stored based on the SLA with the SP. Each subscription data/profile/set is associated with a unique subscription identifier (SI). The SI can be generated internally by the SNPN or based on External UE-ID.

1. The UE selects the SNPN as suitable serving network and sends Registration Request message. The UE includes its SI. For example, the SI can be in form of NAI, where the "realm"-part of the NAI identifies the UE's subscription owner (SO).

2a. The AMF triggers the primary network authentication procedure for network access based on local configuration. Alternatively, the AMF may first try to use the primary authentication procedure as defined in TS 33.501, consequently the UDM/AUSF sends to AMF the Authentication method (primary authentication towards AAA-server), and then AMF trigger the primary network authentication. The AMF may select a specific AUSF (e.g. eAUSF) in the own network based on the SO identifier (e.g. "realm" part of the SI). If the UE-ID can not be derived from the SI, the AMF may ask the UE to provide the UE-ID before initiating the authentication towards the eAUSF/AAA-server.

2b. The UE is authenticated by the AAA server. Any EAP authentication method may be used.

2c. The AAA server sends the authentication result (Success or Failure) to the AMF. In case the authentication is successful, the message may also contain Key material (e.g. Kseaf for deriving further keys for NAS or AS) and SI (used to identify the UE subscription data in the SNPN).

3. The AMF performs NAS security mode command (SMC) with the UE to setup the NAS security with the UE. The AMF uses the Key material received in step 2c to derive the further security keys.

4a. The AMF uses 2 identifiers for the UE the UE-ID and the SI. The SI is used for internal network operations to retrieve subscription data from UDM/UDR (e.g. AM/SM subscription retrieval from UDM). The UE-ID is used for security procedures, e.g. deriving of (NAS or AS) security keys for the UE, communication towards the eAUSF during (re-)authentication/authorization procedure.

4b. The AMF may register with the UDM using Nudm\_UECM\_Registration for the access to be registered using the SI. The AMF retrieves the UE subscription data from the UDM, by using the SI as a subscription identifier for this UE towards the UDM, whereas the UE-ID used to identify the UE in the UDM for the UE-context (not to identify the UE subscription data).

5. The AMF completes the registration procedure as per specification TS 23.502 [6].

6a. The UE may request PDU Session establishment.

6b. The AMF selects an appropriate SMF. In the N11 message to the SMF, the AMF includes an additional information of the SI.

7. The SMF uses the SI to retrieve the UE's Session Management (SM) subscription data from the UDM. The UE-ID is used in the SMF to uniquely identify the UE context.

8. The SMF completes the PDU Session establishment procedure with the UE.

The benefit of this solution is that the UE-specific signalling exchange between the SNPN and the SP is reduced to the UE (primary) authentication and authorization procedure. Once the primary authentication is successfully completed, the SNPN can serve the UE without further interaction with the SP.

#### 6.10.3.2 UE subscription data sent on-demand to the SNPN



Figure 6.10.3.2-1: Registration procedures when the UE subscription data is sent on-demand to the SNPN

0a. The UE has a subscription with service provider (SP). The subscription is identified by an UE-ID.

0b. - 0c. The SNPN and SO has an SLA in place and may have agreed how to handle SO UEs in the SNPN.

1. – 2b. Same as steps 1 – 2b in Figure 6.10.3.1-1.

2c. The AAA server sends the authentication result (Success or Failure) to the AMF. In case the authentication is successful, the message may also contain Key material (e.g. Kseaf for deriving further keys for NAS or AS) and Subscription Retrieval Parameters. The Subscription Retrieval Parameters may include an Access Token (e.g. for authorization at the AAA server), Subscription-Data-URI (for uniquely find the UE's subscription data in the SO domain).

3. Same as step 3 in Figure 6.10.3.1-1.

4. The AMF initiates UE subscription data retrieval with the UDM. The AMF sends Nudm\_SDM\_Get Request which may contain the UE-ID and the Subscription Retrieval Parameters.

5. The UDM initiates a procedure to retrieve the UE service subscription data with the AAA server. For example, the UDM may use the HTTP GET (Subscription-Data-URI, Authorization: Access Token).

6. The AAA server replies, e.g. sending "200 OK" message and including the UE Service Subscription, validity time.

6b. The AAA server keeps track that the UE service subscription data has been sent to the SNPN and may start a validity timer. The UDM may start a validity timer with a value 'Cache time' as received from the AAA server.

7. The UDM/UDR creates subscription data based on received Service Subscription for the UE. The UDM/UDR generates a subscription identifier for this UE (e.g. SI).

8a. The UDM responds to step 4 sending the UE subscription data to the AMF. The UDM also sends the subscription identifier for the subscription data.

8b. The AMF stores the received UE subscription data. The AMF uses both UE-ID and SI. The use of both parameters is as described in step 4a in Figure 6.10.3.1-1.

9. The AMF completes the registration procedure as per specification TS 23.502 [6].

10. - 11. The UDM and AAA server can perform one of the following procedures: renewal, update or removal of the UE subscription data. The procedures can be triggered either in the UDM towards AAA server, or in the AAA server towards the UDM, e.g. upon expiration of the validity timer in step 10a or 10b.

The benefit of the UE subscription data sent on-demand to the SNPN is that the UE Service Subscription data can be updated dynamically.

### 6.10.4 Impacts on services, entities and interfaces

Editor's note: This clause lists impacts to services, entities and interfaces.

\* \* \* \* Fourth change \* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for next generation new services and markets".

[3] 3GPP TS 22.263: " Service requirements for Video, Imaging and Audio for Professional Applications (VIAPA)".

[4] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[5] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station in idle mode".

[6] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[8] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[9] Internet Assigned Numbers Authority (IANA): "Private Enterprise Numbers"; https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers (retrieved March 26, 2020).

[10] 3GPP TS 24.502: "Access to the 3GPP 5G System (5GS) via non-3GPP access networks; Stage 3".

[11] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[12] 3GPP TS 33.203: "3G Security; Access Security for IP-based services".

[13] 3GPP TS 23.632: "User Data Interworking, Coexistence and Migration; stage 2".

[14] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[15] 3GPP TS 23.003: "Numbering, addressing and identification".

[16] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[17] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".

[18] 3GPP TS 22.101: "Service aspects; Service principles".

[19] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[20] SP-191038: "IMS emergency support for SNPN" (IESNPN).

[21] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[22] GSMA SGP.01: "Embedded SIM Remote Provisioning Architecture", Version 4.0.

[23] GSMA SGP.02: "Remote Provisioning Architecture for Embedded UICC Technical Specification", Version 4.0.

[24] GSMA SGP.21: "eSIM Architecture Specification", Version 2.2.

[25] GSMA SGP.22: "eSIM Technical Specification", Version 2.2.1.

[26] 3GPP TS 31.115: "Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications.

[27] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM), Application Toolkit (USAT)".

[28] 3GPP TR 23.716: "Study on the Wireless and Wireline Convergence for the 5G system architecture".

[29] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[30] 3GPP TS 24.587: " Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3".

[31] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes; Stage 3".

[32] IETF draft: "Remote Attestation Procedures Architecture" ( draft-ietf-rats-architecture-04).

[33] IETF draft: "The Entity Attestation Token (EAT)" (draft-ietf-rats-eat-03).

[x] MulteFire Alliance (MFA), Architecture for Neutral Host Network Access Mode Stage 2 (Release 1.1), MFA TS MF.202, https://www.multefire.org/, Release 1.1.

\* \* \* \* Fifth change \* \* \* \*

\* \* \* \* End of changes \* \* \* \*