|  |
| --- |
| 3GPP TR 33.813 V16.0.0 (2020-07) |
| *Technical* *Report* |

|  |
| --- |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Security aspects;  Study on security aspects of network slicing enhancement  **(Release 16)** |

|  |  |
| --- | --- |
|  | |
| *5G-logo_175px* | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 7

1 Scope 8

2 References 8

3 Definitions of terms, symbols and abbreviations 9

3.1 Terms 9

3.2 Symbols 9

3.3 Abbreviations 9

4 Background 9

5 Requirements, assumptions and constraints 9

6 Key Issues 9

6.1 Introduction 9

6.2 Key Issue #1 Authentication for access to specific Network Slices 9

6.2.1 Key issue detail 9

6.2.2 Security threats 10

6.2.3 Potential security requirements 10

6.3 Key Issue #2: AMF Key separation 10

6.3.1 Key issue details 10

6.3.2 Security threats 11

6.3.3 Potential security requirements 11

6.4 Key Issue #3: Security features for NSaaS 11

6.4.1 Key issue details 11

6.4.2 Security threats or disadvantages 11

6.4.3 Potential Security requirements 11

6.5 Key Issue #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization 11

6.5.1 Description 11

6.5.2 Security threats 12

6.5.3 Potential security requirements 12

6.6 Key issue #5: Access token handling between Network Slices 12

6.6.1 Key issue detail 12

6.6.2 Security threats 13

6.6.3 Potential security requirements 13

6.7 Key Issue #6: Confidentiality protection of NSSAI and home control 13

6.7.1 Key issue details 13

6.7.2 Security and privacy threats 13

6.7.3 Potential Security requirements 13

6.7 Key Issue #7 Cancellation of rejected S-NSSAIs 13

6.7.1 Key issue detail 13

6.7.2 Security threats 14

6.7.3 Potential security requirements 14

7 Solutions 14

7.1 Solution #1 Slice Specific Authentication and Authorization 14

7.1.1 Introduction 14

7.1.2 Solution details 16

7.1.3 Evaluation 17

7.2 Solution #2 Slice Authentication 17

7.2.1 Introduction 17

7.2.2 Solution details 17

7.2.3 Evaluation 19

7.3 Solution #3 Security features for NSaaS 19

7.3.1 Introduction 19

7.3.2 Solution details 19

7.3.3 Evaluation 19

7.4 Solution #4 Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN 19

7.5 Solution #5 Privacy for Slice Authentication 21

7.5.1 Introduction 21

7.5.2 Solution details 22

7.5.3 Evaluation 23

7.6 Solution #6 Slice Authentication with user ID privacy but network aware 23

7.6.1 Introduction 23

7.6.2 Solution details 23

7.6.3 Evaluation 24

7.7 Solution #7: Solution to protect user ID 25

7.7.1 Introduction 25

7.8 Solution #8 Protecting NSSAI for transmission on the AS layer 25

7.8.1 Introduction 25

7.8.2 Solution details 25

7.8.3 Evaluation 27

7.9 Solution #9: Slice specific authorization 27

7.9.1 Introduction 27

7.9.2 Solution details 28

7.9.3 Evaluation 28

7.12 Solution #12 Privacy protection of NSSAI 32

8 Conclusions 34

8.1 Key issue-solution mapping 34

8.2 General conclusions 35

8.2.1 Conclusions for key issues 35

9 Recommendations 35

Annex A: Change history 36

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Scope

The scope of the present document is:

- To address the network slicing open security issues which are left over from Rel-15, specifically:

- Study security and privacy aspects related to the solution for Network Slice specific access authentication and authorization using a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and that takes place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorization and authentication, developed in the FS-eNS study led by SA2.

- Identify and study the open security issues from R15 Network Slices particularly the aspects such as:

- Inter-slice security isolation.

- Slice-specific security in the roaming scenarios.

- Slice-specific security features that can be offered as part of Network Slice as a Service (NSaaS) (Slice management).

- Slice-specific security features that can be made visible or monitored in the slice management (Slice management).

- Study the security aspects of architectural solutions in SA2 for the enhanced Network Slicing in R16.

- Study the possible security aspects of the Network Slicing interworking with EPC for Connected and Idle mes.

# 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 33.501: "Security architecture and procedures for 5G system".

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

[4] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[5] 3GPP TR 23.740: "Study on Enhancement of Network Slicing".

[6] IETF RFC 748: "Extensible Authentication Protocol (EAP)"

[7] 3GPP TS 28.531: " Management and orchestration Provisioning".

[8] IETF RFC 4282: " The Network Access Identifier".

[9] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

# 4 Void

# 5 Void

# 6 Key Issues

## 6.1 Introduction

This clause details the key issues identified for security aspects related to the enhanced Network Slices. Each key issue defines the background to the issue, defines the threats related to the issue and proposes requirements that resolve the key issue.

## 6.2 Key Issue #1 Authentication for access to specific Network Slices

### 6.2.1 Key issue detail

This key issue will study how to perform Network Slice Access authentication and authorization specific for the Network Slice Access authentication that uses User Identities and Credentials different from the 3GPP SUPI and that takes place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorization and authentication.

In particular, the key issue will address: Access control to Network Slices that require additional authorization and authentication:

- How do the UE and the Network know that additional authorization and authentication is required for a Network Slice?

- How is the additional authorization and authentication triggered and performed? E.g. which procedures are used and when.

### 6.2.2 Security threats

If Slice specific authentication is not performed, unauthorized UEs may access the Slice which those UEs are not entitled to access. The unauthorized UEs may consume resources of the Network Slice and they may cause DoS to legitimate UEs.

The unauthorized UEs may be any regular UE, which may have successfully completed the primary authentication using 3GPP credentials, but do not have credentials for access the specific Network Slice. Hence such UEs need to be prevented from accessing the Network Slice.

Without slice authentication, operators may not meet the service demands from industry efficiently. Without standardized slice-authentication mechanisms, it will be costly for operators to develop proprietary workarounds or subject to potential security risks when interacting with third party networks.

### 6.2.3 Potential security requirements

It should be possible to perform Network Slice Access authentication and authorization specific Network Slice, in addition to primary authentication if the Slice is configured for such additional authentication.

It should be possible to perform the additional authentication after primary authentication using credentials other than credentials used for primary authentication used for 3GPP access.

## 6.3 Key Issue #2: AMF Key separation

### 6.3.1 Key issue details

The TR 23.740 [5] contains a key issue on the support of Mutually Exclusive Access to Network Slices (MEANS) in clause 5.1. The use cases include, but are not limited to, UEs being restricted to one of two modes of operations. For example, a Public Safety UE being either in an off-duty or an on-duty mode but not simultaneously in both modes. So that the said UE, when on-duty, can be directed to a dedicated Public Safety slice while when in off-duty mode, it is directed to the mainstream one. Whilst this is certainly a beneficial feature for performance and resource optimization, there might be deployment aspects related to tenancy and ownership that require further strengthening the access restriction to prevent access to the signalling and user data communicated between the UE and such mutually exclusive slices.

The TS 33.501 [2] already supports features for backward and forward security during AMF change. When AMF relocation takes place, and based on a local operator policy, the source AMF may derive a new AMF key for the target and the target AMF may trigger a new authentication run. A new authentication run refreshes the whole key hierarchy and totally shield the communication between the UE and the network from the source AMF. It is worth mentioning that in TR 23.740 [5], another key issue in clause 5.3 addresses the support of an additional slice-specific authentication. This additional authentication is expected to take place after the primary authentication when UE is redirected to another slice.

In the current solution, assuming that a new authentication procedure is endorsed for slice authentication, realizing forward security requires yet another run of the primary authentication following or preceding the new slice authentication procedure run. Observe that a primary authentication run always involves the HPLMN. This might be acceptable, but it is not very efficient. Therefore, it is worth investigating how to improve the existing mechanism to meet the forward security requirements in 5G Systems.

### 6.3.2 Security threats

Without key separation between mutually exclusive slices controlled by different AMFs, a potential key leakage in one slice would expose the signalling and the user data between the UE and the next slice the UE is redirected to, which could be a restricted slice owned and managed by a different party, e.g. Public Safety or government organization.

### 6.3.3 Potential security requirements

The system shall support forward security between mutually exclusive slices.

## 6.4 Key Issue #3: Security features for NSaaS

### 6.4.1 Key issue details

Operators may offer customised services through management services to the service consumers based on the Network Slice as a Service (NSaaS) model, as described in TS 28.530 [x1, x2]. The services offered are characterized by the network slice's properties, e.g. radio access technology, bandwidth, latency, reliability, guaranteed/non-guaranteed QoS, and security level etc. However, the security related properties are not identified. This KI will address: offering slice-specific security features as NSaaS including:

- Which security features can be offered as a service to be exposed and managed?

- How to expose and manage the security features and specify the related network functions?

In addition, some of security properties in TS 33.501 are optional, but network resources need to be allocated if provided. It is beneficial for the operators to know, in terms of resource optimization, which optional features are not necessary for every slice.

### 6.4.2 Security threats or disadvantages

N.A.

### 6.4.3 Potential Security requirements

N.A.

## 6.5 Key Issue #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization

### 6.5.1 Description

In Rel-16, after mandatory primary authentication performed by MNO which is to control the access to MNO's network, slice authentication may be needed to control the access to the specific slice service and to support User centric identifier and authentication:

- Access control on slice service or slice resource: TR 23.740 [2] on enhancement of Network Slicing includes studies on how to provide additional Network Slice Access authentication and authorization specific for the Network Slice. Network Slice Access may need to be controlled by entities besides MNO.

- User centric identifier and authentication: TR 22.904 [1] aims to study the introduction of an optional, user-centric authentication layer on top of the existing subscription authentication, supporting various authentication mechanisms and interactions with external authentication systems as well as a degree of confidence. It gives some use cases including: Slice authenticationby 3rd party. It mentions slice authentication can support user centric identifier and authentication apart from the MNO credential and authentication and thus allows users to have access to the specific slice service (e.g., different tires of gaming services) regardless of device used based on the user's subscription to the slice service.

The access control to Network Slices requires additional authorization and authentication uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and that takes place after the primary authentication which is still required between the UE and the 5GS for PLMN access authorization and authentication.

This KI will address: Security and privacy aspects related to access control to Network Slices that require additional authorization and authentication including:

- How to protect the security of the User ID and credentials in UE storage, transition and network storage?

- As the Network Slice Access may be controlled by entities besides MNO, how to protect the security of the interaction between the 3rd party entities and the network functions performing slice authorization and authentication. As well as the interaction between the network functions performing slice authorization and authentication and the related MNO NFs such as AMF, SMF or NSSF?

### 6.5.2 Security threats

Without confidentiality or integrity protection of the User ID and corresponding credentials, sensitive information may leak, and user data may be obtained by attackers.

### 6.5.3 Potential security requirements

- User ID shall be privacy protected.

Editor's Note: clarification on who shall not have access to User ID information or from whom to protect.

## 6.6 Key issue #5: Access token handling between Network Slices

### 6.6.1 Key issue detail

As described in TS 23.501 [3], an NRF which takes the role of OAuth 2.0 Authorization server can be deployed at different levels:

- PLMN level (the NRF is configured with information for the whole PLMN);

- shared-slice level (the NRF is configured with information belonging to a set of Network Slices);

- slice-specific level (the NRF is configured with information belonging to an S-NSSAI).

Hence, an NRF deployed at the PLMN level or the shared-slice level can manage the access of NF service producers belong to different Network Slices.

Furthermore, according to TS 33.501 [2], upon receiving the access token request, an NRF can generate an access token with appropriate claims included for the NF service consumer. The claims in the token include the NF Instance Id of NRF (issuer), NF Instance Id of the NF Service consumer (subject), NF type of the NF Service producer (audience), expected service name(s) (scope) and expiration time (expiration).

Consequently, with the same access token authorized by the NRF deployed at the PLMN level or the shared-slice level, an NF service consumer may access the services provided by the same type of NF service producers belong to different Network Slices.

However, network slices may differ for supported features and have different access rights. The access tokens for these network slices should be different (separated). In the cases where a group of network slices have similar access rights sharing the same access token, the access token should be restricted to a specific list of network slices, not for all network slices.

### 6.6.2 Security threats

Without access token separation between slices, an access token may be used to access all Network Slices managed by the same NRF which means a compromised NF service consumer can maliciously access services provided by NF service producers belong to all Network Slices.

### 6.6.3 Potential security requirements

It should be possible to perform access token authorization for a specific Network Slice or a list of Network Slices.

## 6.7 Key Issue #6: Confidentiality protection of NSSAI and home control

### 6.7.1 Key issue details

NSSAI may contain sensitive information that causes privacy concerns when transmitted in clear. For example, a particular NSSAI may be linked to a slice instance exclusively for UEs serving police officers. It has been concluded in Rel-15 that S-NSSAI is not transmitted in initial NAS messages, until security context is established. Besides S-NSSAI is by default not transmitted in AS messages, unless a serving PLMN instructs the UE to do so. These tentative decisions leave following open issues needed to be addressed.

1) Fulfil the requirement to send protected S-NSSAI.

The objective of this key issue is to investigate complete solutions, to address above issues, in the meantime to address potential backward compatibility issue, if any, to R15.

### 6.7.2 Security and privacy threats

If an S-NSSAI is sent in the cleartext during the RRC connection establishment procedure, then the user privacy is lost. In case the S-NSSAI is related to the critical services (e.g. MCPTT) then the man in the middle may disrupt the services by targeting the user using these services.

In addition, A non-compliant serving PLMN may transmit NSSAI in clear, leading to a leak of NSSAI.

### 6.7.3 Potential Security requirements

5G system shall provide confidentiality protection for NSSAI transmission. This key issue will only study solutions where:

- Cryptographic key material is available from an earlier authentication run.

- Existing NAS or AS security contexts can be used.

## 6.7 Key Issue #7 Cancellation of rejected S-NSSAIs

### 6.7.1 Key issue detail

This key issue wdeals with how to perform the revocation of an already rejected S-NSSAI, else there will not be a possibility for the UE to use the S-NSSAI even with a renewed valid.

There is no policy defined in the UE for re-attempt to request a rejected S-NSSAI and allowing the UE to delete Rejected S-NSSAI(s) internally may result in undesirable and non-deterministic behaviour, i.e. the UE can directly renew it is subscription on application layer with the service provider but the NAS layer removed the rejected S-NSSAI. Since in Rel-15 and Rel-16 the UE can autonomously remove a Rejected S-NSSAI for a whole PLMN or a registration area, there would be no chance to re-register to the S-NSSAI even the UE re-newed the subscription on application layer.

Another problem is that the context is stored in the AMF, i.e. a rejected S-NSSAI will be directly rejected by the AMF even without performing any slice authentication with the AAA.

Editor's Note: It is FFS how the AMF updates the UE context for a rejected S-NSSAI.

### 6.7.2 Security threats

TBD

### 6.7.3 Potential security requirements

TBD

# 7 Solutions

## 7.1 Solution #1 Slice Specific Authentication and Authorization

### 7.1.1 Introduction

The solution described in this clause addresses key issue#1 Authentication for access to specific Network Slices and key issue#4 Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization.

This solution is based on the agreed Solution #3.2 in the SA2 TR 23.740. The architecture assumes Authentication, Authorisation and Accounting Server (AAA-S) deployed in a PLMN or in a third-party network that allows Slice-Specific authentication and authorisation of users who have the right of access to certain slices. A AAA proxy function (AAA-F) is also defined to provide a single point of interaction from the PLMN with the third parties. Slice specific User IDs and credentials, separate from those used for the primary authentication, are used in the Slice specific authentication.

During the primary authentication, whether the UE requires a slice specific authentication is detected by the UDM by checking a flag for this extra authentication against the NSSAI corresponding to the Slice. The IP address or FQDN/realm of the AAA Server that would perform the authentication and authorisation may be stored in the AAA-F per S-NSSAI. Alternately, the User ID in the third party could be defined as a NAI (see IETF RFC 4282 [8]), i.e. the User ID is in the form user@domain.

When a UE performs a registration request which includes S-NSSAI(s) in the Requested NSSAI which needs Slice-Specific Authentication and Authorisation, after the successful completion of the primary authentication, the AMF and SMF triggers, an Authentication with the AAA of specific S-NSSAI(s). If multiple Slices need slice specific authentication, one such authentication is needed for each S-NSSAI.

The UE needs to be provisioned with the credentials necessary to authenticate itself with the Slice AAA Server corresponding to the NSSAI of the Slice. The UE includes a Slice-Specific Authentication and Authorisation indicator in the 'UE security capabilities' in the registration request message, for the AMF to determine whether it can execute Slice-Specific Authentication and Authorisation or not. If the Slice specific Authentication security capability is not included in the registration request, the AMF does not allow the UE to access to any Network Slice for which Slice-specific authentication is required.

The assumption is that the Slice specific authentication is performed after primary authentication using one of the EAP authentication methods.

Once the slice specific authentication is executed, authentication status is kept by the AMF in the UE context, so extra authentication is not repeated at subsequent registrations until a re-authentication is required by the AAA Server or the PLMN, based on policy.

The Slice AAA server may re-authenticate the UE or decide to revoke the authorization, in this case the AAA proxy routes to the serving AMF, based on the binding between the User id and the GPSI of the UE established when the UE was authorized for the Slice.

Once the slice specific authentication is complete, SM procedures to the authorised slices takes place for the UE.

### 7.1.2 Solution details



Figure 7.1.2-1

Step 1: UE sends Registration Request to the network. UE will include the list of NSSAIs corresponding to the network slices it is interested in to get authenticated for access.

Step 2: UE and network completes Primary authentication of the UE, either using the 5G AKA procedure or EAP-AKA' procedure. At the end of a successful primary authentication, the AMF will have a list of allowed NSSAIs for the UE in the AMF form the AUSF, based on the subscription information available in the UDM.

Step 3: At the end of a successful primary authentication procedure, AMF sends Registration Accept message to the UE. Based on the subscription information received from the UDM/AUSF, the message will contain all the allowed NSSAIs except the ones which require Slice specific authentication.

Step 4: UE sends Registration Accept message, indicating the successful completion of primary authentication.

Steps 5-10: If the UE had indicated its support for Network Slice-Specific Authentication and Authorization Procedure in the UE MM Core Network Capability in Registration Request, based on the subscription information received from AUSF/UDM, the AMF initiates slice specific authentication, for all the slices which require slice specific authentication.

Step 5: AMF sends EAP Identity Request to the UE corresponding to the NSSAI of the network slice, to initiate slice specific authentication.

Step 6: UE responds with EAP Identity Response message for the requested NSSAI.

Step 7: AMF sends Authentication Request to the AAA server of the network slice to authenticate the UE. The message will contain the EAP Identity received from the UE.

Step 8: UE and AAA exchanges EAP Request/Response messages for the authentication via AMF. There may be multiple exchanges based on the particular configuration of the AAA.

Step 9: AAA sends EAP success for the EAP user identity, if the verification succeeds.

Step 10: AMF records the success of the EAP authentication for the Slice represented by the NSSAI, and forwards the EAP Success to the UE.

Step 11: AMF completes the Slice specific authentication for all network slices for which there is subscription indication that a slice specific authentication is required for the UE to access these slices.

Step 12: Once the Slice-Specific Authentication is completed for all S-NSSAIs, depending on the result of Slice-Specific Authentication, the AMF may trigger a UE Configuration Update procedure to deliver a new list of Allowed NSSAIs.

### 7.1.3 Evaluation

This solution addresses key issue#1 Authentication for access to specific Network Slices. Slice specific authentication is enabled based on the UEs subscription information received from the AUSF/UDM upon successful primary authentication. Slice specific authentication is initiated only if the UE also indicated its capability for the procedure in the UE capability indication. Since the AMF is initiating the EAP procedure for the slice specific authentication one by one, there are no timing issues associated with the procedure. Also, since the primary authentication has been completed before initiating the slice specific authentication, it is possible to set up AS security and protect the NSSAI in the RRC message if the UE initiates a Service Request related to an allowed NSSAI, before it goes to Idle state. Since NAS and AS security is established by the primary authentication procedure, the EAP identity used for the Slice specific authentication is protected at these layers. Hence this solution provides protection of User ID for the slice authentication between UE and serving network.

## 7.2 Solution #2 Slice Authentication

### 7.2.1 Introduction

This solution addresses the Key Issue #1 Authentication for access to specific Network Slices.

The slice authentication is performed between a UE and an AAA server, which may reside in the PLMN domain or outside the PLMN domain. It is based on subscription identifiers that are different from SUPI, e.g. DN subscription identifiers or user ID registered at DN.

The slice authentication is performed after Primary Authentication and based on the EAP framework, where SEAF/AMF takes the role of the Authenticator. Various EAP methods are supported and can be negotiated between the UE and the AAA server, following the EAP framework as described in IETF RFC 3748 [6].

### 7.2.2 Solution details

This solution presents the registration procedure between UE and the network when slice authentication is performed. A general overview is shown in figure 7.2.2-1. The procedure is based on the registration procedure in TS 23.502.



Figure 7.2.2-1: Registration overview when slice authentication is performed

Steps 1 indicates the registration steps the same as 1-7 as in TS 23.502 [4].

Steps 2 indicates the same Primary Authentication procedure as in TS 33.501 [2], where the UE and the PLMN are mutual authenticated. The user subscription ID for slice authentication can be included in the N2 messages exchanged with the AMF. In case the UE has valid security context, the primary authentication is skipped.

Step 3: AMF obtains the subscription information of the user from UDM, which provides necessary information to AMF whether slice authentication is required.

Step 4: Registration accept is sent to UE, including allowed NSSAI as in TS 23.502 [4], after Primary Authentication is successful. The S-NSSAI in the Requested NSSAI that require slice authentication, e.g. authenticated previously, can also be included.

Step 5: UE sends Registration Complete corresponding to the allowed S-NSSAI in step 4.

Step 6: EAP based Slice authentication is performed, and AMF should make sure the link between AMF and AAA server is established. The link can be routed through a Proxy of Slice Authentication Server (AAA Proxy), as illustrated in the figure.

The slice authentication is based on the EAP framework, where AMF/SEAF takes the role of Authenticator. Various EAP methods can be supported and UE can negotiate with AAA server on the EAP method based on IETF RFC 3748 [6]. The steps 6a and 6b and the number of messages exchanged in step 6d are dependent on the EAP method used.

Step 7: The UE Configuration Update is sent with allowed NSSAI after slice authentication is completed.

### 7.2.3 Evaluation

In this solution, slice authentication is performed after Primary authentication. The well-established EAP mechanism is chosen for the Slice Authentication and can accommodate various authentication methods and credentials, chosen between AAA and UE.

It addresses KI#1 Authentication for access to specific Network Slices and meet both security requirements of KI#1.

## 7.3 Solution #3 Security features for NSaaS

### 7.3.1 Introduction

This solution addresses the Key Issue #3 Security features for NSaaS.

### 7.3.2 Solution details

Whether a network slice requires slice-specific authentication can be configured for a slice during network slice provisioning. UP security policy (i.e. confidentiality protection and integrity protection) can also be configured for a slice for NSaaS, however PLMN ignores that request (e.g. if it goes against its policy on UP protection).

Note: the management services and procedure for network slice provisioning are specified in clauses 6 and 7 of TS 28.531 [7] respectively.

### 7.3.3 Evaluation

This solution addresses the key issue #3. It has identified two security features for NSaaS that can be addressed through configuration.

## 7.4 Solution #4 Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN

7.4.1 Introduction

This solution addresses KI#1, Authentication for access to specific Network Slices.

This solution is based on the normative solution for Slice-Specific Authentication and Authorization (SSAA) in TS 23.502 [4]. SSAA is performed with a AAA Server (AAA-S) which may be hosted by the H-PLMN operator or a trusted third party. A AAA proxy (AAA-P) may be involved in the serving PLMN. The SSAA is performed between the UE and the AAA-S based on the EAP framework where the AMF/SEAF acts as the EAP authenticator. The EAP authentication messaging for SSAA is performed after the Registration procedure. After the SSAA procedure is completed successfully for an S-NSSAI, the Allowed NSSAI is updated to include that S-NSSAI in the AMF and in the UE.

The scenario described here is for a UE that aims to register over 3GPP and over non-3GPP in the same serving PLMN. The UE registers over a first RAT (e.g., 3GPP) and then over another RAT (e.g., non-3GPP). RAT#1 is the name used for the first RAT that the UE uses to Register for an S-NSSAI subject to SSAA, and RAT#2 is used for the other access (e.g., RAT#1 may be 3GPP and RAT#2 non-3GPP, or vice-versa). The UE sends over RAT#1 a Registration Request which includes in the Requested NSSAI an S-NSSAI subject to SSA. The UE waits for the completion of the SSAA procedure for the S-NSSAI over RAT#1 before performing the Registration over RAT#2. Since the UE is registered over RAT#1 and UE context exists with allowed NSSAIs for the UE, the AMF decides to skip a new SSAA run during Registration over RAT#2

7.4.2 Solution details

The solution shown in figure 7.4.2-1 illustrates a UE performing multiple registrations with the same serving PLMN while requesting the same S-NSSAI subject to SSAA in the Registration Request. The Registration and SSAA procedural steps over 3GPP are as specified in TS 23.502 [4]. Note that the solution below can apply regardless of the RAT order used by the UE to register (i.e. 3GPP or non-3GPP first). Upon receiving a Registration Accept over a first access indicating a pending SSAA run, the UE refrains from Registering over the other access until the completion of SSAA over the first access (i.e. perform associated UE Configuration Update procedure).



Figure 7.4.2-1: Multiple Registration with the same PLMN with same S-NSSAI subject to SSA

Step 1: UE and network performs a standard Registration procedure over RAT#1 including primary authentication and establishment of the NAS security context. The AMF determines from the subscription data that the S-NSSAI included in the Requested NSSAI is subject to SSAA which is to be performed after sending the Registration Accept message to the UE. The Allowed NSSAI returned in the Registration Accept message does not include the S-NSSAI. The Rejected NSSAI in the Registration Accept message includes the S-NSSAI with a cause value indicating a pending SSAA for the S-NSSAI.

Step 2: UE and network perform a standard SSAA procedure over RAT#1. The EAP based authentication run is performed over secure NAS transport messages.

Step 3: Following the successful authentication of the UE for the S-NSSAI, the Allowed NSSAI is updated to include S-NSSAI using a UE Configuration Update procedure.

Step 4: UE checks that SSAA is completed over RAT#1 before starting the Registration procedure over RAT#2

Step 5-6: UE sends a Registration Request over RAT#2 protected using the available common NAS security context. AMF decides to skip a new Primary authentication over the RAT#2 access.

Step 7: AMF determines that S-NSSAI is already authorized by SSAA and that the UE is already authenticated for S-NSSAI following the previous Registration over RAT#1. The S-NSSAI authentication result (e.g. success/failure) from previous SSAA run over RAT#1 may be included in the common NAS security context. AMF may decide to skip SSAA run over RAT#2 for the S-NSSAI.

Step 8: AMF sends a Registration Accept to the UE including S-NSSAI in the Allowed NSSAI for RAT#2

Step 9: UE may start using the S-NSSAI over any access, e.g. it may establish a PDU Session using S-NSSAI over RAT#2 access.

The AAA-S may decide to re-authenticate and re-authorize the UE at any time. The re-authentication and re-authorization procedure is based on the solution specified in TS 23.502 [4]. In that procedure, the AAA-S sends a request to re-authenticate and re-authorize the UE for a given S-NSSAI to the serving AMF via the AAA-F. Then the AMF triggers an SSAA over the access used to register for that S-NSSAI. The difference in this solution, is that AMF needs to select one of the accesses used to register for that S-NSSAI and trigger an SSAA over that selected access e.g. SSAA may be run on an access where UE may be CM-Connected while being CM-Idle on the other.

The AAA-S may decide to revoke the authorization of the UE at any time. The revocation procedure is based on the solution specified in TS 23.502 [4]. In that procedure, the AAA-S sends a request to revoke the authorization of the UE for a given S-NSSAI to the serving AMF via the AAA-F. Then the AMF updates the UE configuration to remove the S-NSSAI from the Allowed NSSAI for the access used to register for that S-NSSAI. The difference in this solution is that AMF needs to update the UE configuration to remove the S-NSSAI from the Allowed NSSAI for both accesses i.e. trigger a UE Configuration Update procedure for each access.

7.4.3 Evaluation

Key Issue #1 in the present document is about enabling Slice Specific Authentication and Authorization (SSAA). This solution addresses KI#1 in the context of a UE performing multiple registrations in the same PLMN over different access types.

The solution builds on top of the adopted solution in TS 23.501 [2] and TS 23.502 [3] for a single registration over a single access type where the SSAA is performed after the primary authentication (i.e. after the Registration procedure) and EAP messages exchanged during the SSAA procedure are transported over secure NAS messages.

When the UE registers with a PLMN over a given access type for a network slice that is subject to SSAA, it postpones registration with that PLMN for that same network slice over another access type until the completion of the SSAA procedure. This avoids potential race conditions and unnecessary signalling as a new SSAA procedure may be triggered over the second access type while such a procedure is already ongoing over the first access type.

This solution is complimentary to either solution #1 or solution #2 as they deal with a single registration scenario.

The proposed solution meets the requirement of key issue #1.

## 7.5 Solution #5 Privacy for Slice Authentication

### 7.5.1 Introduction

This solution addresses the Key Issue #4: "Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization".

A public key is provisioned form the service provider to the UDM and bound with the corresponding NSSAI. If a UE requests service for a NSSAI, then the UDM provisions the public key to the AMF and further to the UE in order to use it for concealing the User ID in the EAP Identification response.

### 7.5.2 Solution details

The following figure shows the procedure for public key provisioning and User ID concealment in the UE.

UE

AMF

UDM/

AUSF

AAA

Serving Network

HPLMN

3

rd

Party/Internet

1. Registration Req. (NSSAI)

NEF

0.a AAA Registration (Pub Key)

0.b AAA Registration ACK

4a. NAS Message (EAP Identity Request,

S

-

NSSAI, Pub Key)

4c.

NAS Message (EAP Identity

Response with concealed User ID

-

)

4d.

Authentication Request (EAP Identity

Response with concealed User ID

,

-

,

GPSI)

4e.

EAP Request

-

Response Messages

4f.

EAP

-

SUCCCESS

4g.

NAS Message (EAP SUCCCESS,

-

)

5. UE and AMF knows the list of authorized

and subscribed NSSAIs

2. Primary Authentication using 3GPP credentials

3. AMF checks subscription data

(including Pub Key) and security

context for slice specific

authentication for each NSSAI

4b. UE uses Pub Key

to

conceal the User ID

Figure 7.5.2-1: Procedure for public key provisioning and User ID concealment

Step 0 is not further described here but it is assumed that the normal interface with external service provider via the NEF is utilized in order to provision the NSSAI and public key binding to the UDM.

The procedure is in general the same as described in solution#1, clause 7.1.2 with the following differences:

Step 3: The AMF retrieves the subscription data from the UDM, including the public key for each NSSAI where slice authentication is required. Based on operator policy the UDM provides the public key at any request or only when requested by the UE or the key is changed in the UDM.

Step 4a: The AMF initiates the slice authentication and sends an EAP Identity Request to the UE including the S-NSSAI and the corresponding public key.

Step 4b: The UE stores the public key and binds it with the S-NSSAI. It uses the Public Key to encrypt the User ID for the S-NSSAI.

Step 4c: The UE sends the NAS message with the EAP Identity Response with the concealed User ID.

Step 4d: the AMF sends an Authentication Request with the concealed User ID to the AAA server, which has the corresponding private key and is able to de-conceal the User ID.

Step 4e - 5: The normal related EAP message exchange for authentication of this User ID is performed now and slice authentication is carried out.

Editor's Note #1: Whether user ids used for slice authentication is within the scope of 3GPP is FFS;

Editor's Note #2: EAP framework assumes that privacy is handled by the EAP methods. It is FFS whether this creates any issues;

Editor's Note #3: It is FFS whether using a public key of an external entity to encrypt the user id is appropriate;

### 7.5.3 Evaluation

TBD.

## 7.6 Solution #6 Slice Authentication with user ID privacy but network aware

### 7.6.1 Introduction

This solution addresses the Key Issue #4: "Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization".

This solution is to provide privacy protection to the user identify used during slice authentication. In the meantime, the network should be aware of the user in order to support multiple users using one device to access DN services. The use cases have been described in TR 22.904, which motivates the current study.

### 7.6.2 Solution details

If user ID privacy is required, it is protected by the EAP method.

The following figure shows the procedure for the UE to register to the network where slice authentication is required. The User ID concealment is provided by the EAP method itself. In order for the network to be aware of the user, AMF will store the user's ID. The steps of the procedure are as follows:



Figure 7.6.2-1

Steps 1-3: AMF starts EAP based slice authentication procedure after Primary Authentication.

Step 4: AMF, as Authenticator, sends ID Request to UE.

Step 5: UE responses with ID requested. The ID will be concealed depending on the EAP method used.

Step 6: AMF stores the user ID.

Step 7: AMF sends slice authentication request to AAA server and the message may be routed by AAA prox8.

Step 8: EAP based Slice authentication continues with message exchange between AAA and UE via AMF.

Step 9: AAA informs AMF Slice authentication successful.

Step 10: AMF continues with other steps of slice authentication.

### 7.6.3 Evaluation

This solution addresses the KI #4.

This solution relies on ID privacy protection mechanism provided by EAP methods and does not introduce a new mechanism.

This solution can provide the user ID protection between UE and the AAA server.

## 7.7 Solution #7: Solution to protect user ID

### 7.7.1 Introduction

This security solution is related to the Key Issue #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization.

According to the agreed solution present in clause 6.3.2 of TR 23.740 [5] the slice specific authentication takes place after the UE has been authenticated by the 3GPP system for PLMN access. Therefore, the necessary key material needed for the network to configure AS security with the UE using AS Security Mode Command is available. Key material needed for setting up NAS security with NAS Security Mode Command is also available.

7.7.2 Solution details

This solution proposes that any message exchange after the primary authentication will be confidentiality protected after successful activation of AS and NAS security.

7.7.3 Evaluation

This solution addresses Key Issue #4 and protects the User ID over the air interface between UE and serving network relying on the activation of AS and NAS security. The solution combines NDS IP and EAP methods in tunnel mode to protect the user ID between the AAA server and serving network.

## 7.8 Solution #8 Protecting NSSAI for transmission on the AS layer

### 7.8.1 Introduction

This solution addresses the Key Issue #6 Confidentiality protection of NSSAI and home control.

This solution aims to provide a method of protecting the S-NSSAIs that will be transmitted on the AS layer in a way that is compatible with Rel-15 UEs. In this solution, UE and RAN are offered a temporary NSSAIs (T-S-NSSAIs) instead of cleartext S-NSSAIs in registration procedure. After that, the T-S-NSSAIs will be used in the AS layer.

This temporary NSSAI needs to be updated frequently to preserve the privacy.

### 7.8.2 Solution details

Figure 7.8.2-1 illustrates this solution.



Figure 7.8.2-1: NSSAI protection during the RRC connection establishment

0. The UE has registered successfully to a PLMN and 5G NAS security context has been created.

1. In the registration procedure, core network first generates a fresh number RAND, and then calculates UE-specific T-S-NSSAIs according to allowed S-NSSAIs and RAND using a 128-NEA as in Annex D 2.1.2 [2]. At last, CN stores the {allowed S-NSSAIs, T-S-NSSAIs} tuple.

2. In the registration/service accept message, {allowed S-NSSAIs, T-S-NSSAIs} tuple will be sent to UE instead of cleartext S-NSSAIs.

3. CN sends RAND to NG-RAN with N2 message.

4. In a registration request message, UE transmit T-S-NSSAIs in RRC message.

5. RAN is able to restore allowed S-NSSAIs according to T-S-NSSAIs and RAND using 128-NEA1 as in step 1.

The T-S-NSSAIs are generated and assigned by the AMF during the initial and subsequent registration procedures. The T-S-NSSAIs are sent to UE and the serving gNB. Whether the T-S-NSSAIs are sent to additional gNBs, e.g. under the same TA, are implementation dependent and based on the operator's policy (e.g. AMF configuration).

For example, AMF may be configured to send to the serving gNB only.

In another example, AMF is configured to send to the serving gNB and adjacent gNBs within the same TA.

The UE and the receiving gNBs will store these T-S-NSSAIs to be used later in the subsequent registration process. T-S-NSSAIs are updated periodically based on the operator's policy.

When UE moves to a new cell (different gNB) while in an idle mode, whether a T-S-NSSAI is available in the target cell depending on whether the T-S-NSSAI has been stored. In case T-S-NSSAI is not available, the UE will be routed to an AMF the same way as that S-NSSAI is not present. This is reasonable since the presumption of this key issue is that the security context is available (Security context is released when UE is in an idle mode). In general, the more gNBs storing a T-S-NSSAI, the less likely that S-NSSAI is not present. The trade-off is that more T-S-NSSAI storage is needed at gNBs. As to congestion control, only the serving gNB is storing T-S-NSSAIs.

Different UEs have different T-S-NSSAIs. For a specific UE, the T-S-NSSAI is the same across Ng-RAN under the same AMF.

### 7.8.3 Evaluation

This solution addresses the key issue #6, the solution is able to protect the privacy of NSSAI in air interface. Besides, the solution introduces no extra message exchanges to the existing procedures, and there is no extra computation in UE. Instead, it increases complexity at gNB. A new IE in the service accept message is needed when T-S-NSSAI is transmitted at RRC in the service registration procedure.

The key proposal is to use temporary NSSAIs in the RRC signaling. These T-S-NSSAIs are generated and assigned by the AMF during the initial and subsequent registration procedures, as part of Initial context set up in the base station. The UE and the gNB need to store these T-S-NSSAI values to be used later in the subsequent registration process. If these values remain static, then based on the characteristic of communication, these values could be mapped to their real slice types and thereby to the NSSSAI. Also, the T-S-NSSAIs need to be individually different, otherwise mapping to the Slice becomes very easy.

## 7.9 Solution #9: Slice specific authorization

### 7.9.1 Introduction

This solution addresses Key Issue#5 by identifying how to handle the access token between network slices. This solution is based on the following authorization procedures (see TS 33.501, V15.3.1, clause 13.4.1):



Figure 7.9.1-1: NF service consumer obtaining access token before NF service access

The following figure and procedure describe service access request based on token verification.



Figure 7.9.1-2: NF service consumer requesting service access with an access token

According to the figure above, if the slice specific authorization is needed, the access token authorization and verification considers the slice information.

### 7.9.2 Solution details

All the procedures described in TS 33.501 [2], clause 13.4.1 are applied in the proposed solution with some additional description as follows:

In the first step, if the NF service consumer is limited to access NF service producers belonging to specific slice, it requests an access token from the NRF using the Nnrf\_AccessToken\_Get request operation with additional slice information compared to the existing IEs, e.g., S-NSSAI and NSI ID(s) defined in TS 23.501 [3].

In the second step, the NRF then generates an access token with additional slice information included in the claim e.g., S-NSSAI and NSI ID(s).

During the verification procedure, the NF service producer additionally checks that the slice information claim in the access token matches its own slice information.

### 7.9.3 Evaluation

Key Issue #5 in the present document is about malicious service access between network slices, resulting from malicious NFs with access token authorized by the NRF deployed at the PLMN level or the shared-slice level. The solution addresses the key issue by introducing slice specific information for the expected NF producer in token requests, token claims and token verification.

The proposed solution meets the requirement of key issue #5 .

7.10 Solution #10 Protecting S-NSSAI for transmission on the AS layer

7.10.1 Introduction

This solution addresses the Key Issue #6 Confidentiality protection of NSSAI and home control.

This solution aims to provide a method of protecting the S-NSSAIs that will be transmitted on the AS layer in a way that is compatible with Rel-15 UEs.

7.10.2 Solution details

7.10.2.1 General

This configuration of S-NSSAIs in the serving network follows the SA2 procedures, i.e. HPLMN allocates some S-NSSAIs to the UE which uses these S-NSSAIs initially to request access to a slice in a serving PLMN. The serving PLMN may allocate its own local S-NSSAI (as a configured S-NSSAI) for each requested S-NSSAI. The UE will use the configured S-NSSAIs to indicate its interest in the particular slices in the serving PLMN.

Hence an S-NSSAI value that the UE sends on the AS layer may be allocated by the serving network as part of the existing procedures. This means that the serving network can assign different S-NSSAIs that are mapped (or resolved) to the same S-NSSAI, to different UEs. Therefore, for S-NSSAI privacy, the AMF provides "encrypted S-NSSAI" to a UE that would be sent on the AS layer, where the encryption incorporates a UE specific parameter such as 5G-GUTI. The UE can directly return this 'encrypted S-NSSAI' to the network. The AMFs and NG-RAN nodes across the whole network will need to be co-ordinated on which actual S-NSSAI each 'encrypted S-NSSAI' will resolve to. If these 'encrypted S-NSSAI' further depend on the part of the 5G-GUTI supplied by the UE to the NG-RAN node at RRC set-up, it would mean that the same 'encrypted S-NSSAI' value that is used by different UEs would not necessarily indicate the same actual S-NSSAI.

7.10.2.2 Format and content of the 'encrypted S-NSSAI'

The format for the 'encrypted S-NSSAI' is as follows:

- Key ID | Random number | S-NSSAI Identifier XOR E(Key, Random Number, S-TMSI)

where

- E(Key, Random Number, S-TMSI) is an encryption function to produce key stream with Key as the key and Random Number and S-TMSI as input;

- Key ID identifies the key and the algorithm used in E(Key, Random Number, S-TMSI);

- Random Number is just a random number so that different 'encrypted S-NSSAI' can be used for the same actual S-NSSAI; and

- S-NSSAI Identifier allows the NG\_RAN and AMF to understand which S-NSSAI the UE is requesting

Each Key ID is associated with a key, choice of algorithm and any other information (e.g. MSB of counter input for AES in counter mode) needed by the AMF or NG-RAN node to create or parse an 'encrypted S-NSSAI'. Each AMF in a serving network needs to be provisioned with the current Key ID and associated information. The NG-RAN nodes can either be provisioned with this information or could request it from the AMF when they receive a Key ID that is currently unknown to them.

Since the 'encrypted S-NSSAI' carries a Key ID and a random number, it is not possible to send a complete S-NSSAI in an 'encrypted S-NSSAI'. Hence, an instead of the S-NSSAI, an S-NSSAI identifier, which can be mapped to the corresponding S-NSSAI, is used to construct 'encrypted S-NSSAI''. A mapping between S-NSSAI identifiers and S-NSSAI is configured by AMF to NG-RAN nodes.

7.10.2.3 Creating an 'encrypted S-NSSAI'

When the AMF creates a new 'encrypted S-NSSAI' to send as a configured S-NSSAI, it calculates the 'encrypted S-NSSAI' using the Key ID, the S-NSSAI identifier of the slice that is to be configured, the UE's S-TMSI and a random number. The AMF can use any key and method that is provisioned locally. Those key and method are also made available in the NG-RAN nodes. When calculating each 'encrypted S-NSSAI', a fresh random number is chosen and this together with the S-TMSI provides the freshness for the input to the ciphering algorithm.

7.10.2.4 Resolving an 'encrypted S-NSSAI'

When the UE sends such an 'encrypted S-NSSAI' to the NG-RAN, the NG-RAN calculates the S-NSSAI Identifier and from this the NG-RAN gets the S-NSAAI the UE is requesting. This is done by using the Key ID in the 'encrypted S-NSSAI' to know the key and encryption method. This allow the S-NSSAI identifier to be decrypted and the mapping to the actual S-NSSAI requested by the UE to be resolved. If this procedure fails, i.e. the NG-RAN does not get a S-NSSAI Identifier it recognises, then the AMF can be selected based on the UE identity supplied at the AS layer or the default AMF can be selected.

7.10.2.5 Updating the 'encrypted S-NSSAI'

The 'encrypted S-NSSAI's sent to a UE will need to change when the S-TMSI changes in order not to provide a longer-term identifier of the UE than the S-TMSI. This can already be done with the specified procedures. Since when a GUTI (including the S-TMSI) is allocated to the UE using the Registration Accept or the UE Configuration Update message, there is space in each of these messages to update the configured S-NSSAI at the same time.. This means that it is not easier to track the UE based on the values in the S-NSSAI IE sent on the AS layer than to do it based on the S-TMSI. A new 'encrypted S-NSSAI' has to be calculated for each S-NSSAI that the UE is allowed to access when the update is performed.

Editor's note: Clarification for supporting idle mode mobility is needed.

7.10.3 Evaluation

The solution satisfies to the key issue as it encrypts the data that identifies the S-NSSAI over the air (in effect the data is encrypted in the AMF and decrypted in the RAN node with the UE just passing the received information on without changing it).

The NG-RAN nodes need to have the mapping of S-NSSAI Identifiers of S-NSSAIs and also the Key\_ID, Key and encryption method used by the AMF when creating the 'encrypted S-NSSAI'.

The 'encrypted S-NSSAI' need to be updated every time the GUTI changes which is more frequent than normal S-NSSAI would be updated, although no new message is needed to perform the update.

The solution reduces the possible number of S-NSSAIs. With a 4-bit Key ID and 16-bit Random Number, there are still 12 bits available for S-NSSAI (i.e. 4096 different S-NSSAIs can be used) in the 4-bytes used to carry an S-NSSAI in the NAS protocol (see clause 9.11.2.28 of TS 24.501 [9]).

The solution works with Rel-15 UEs as the UE does not need to process the 'encrypted S-NSSAI'.

The solution protects against UEs who may access the same slice from knowing what slice is being requested. The solution does not require every S-NSSAI to be protected if so desired by the operator.

Editor's Note: Further evaluation is FFS.

7.11 Solution #11: Protection of S-NSSAI transmitted in the AS layer using T-S-NSSAI

7.11.1 Introduction

This solution addresses Key Issue #6: Confidentiality protection of NSSAI and home control.

The following solution builds on a similar notion of temporary S-NSSAI (T-S-NSSAI) as in solution #8. The UE obtains the T-S-NSSAI from the AMF over NAS in a Registration accept message during the registration procedure similar to solution #8. The NG-RAN obtains a list of T-S-NSSAI and associated S-NSSAI tuples supported by the PLMN from the AMF in a NG Setup Response during an NG Setup procedure. In this solution, the T-S-NSSAI are generated/maintained per PLMN. The UE transmits requested T-S-NSSAIs as hash values (instead of cleartext T-S-NSSAI) in the AS layer during AS connection establishment. The T-S-NSSAI hash values are computed using the S-TMSI as one of the hash function arguments. The NG-RAN identifies the corresponding slices requested by the UE (indicated by S-NSSAIs) by matching each hashed T-S-NSSAI requested by the UE and received in the AS layer with the hash value computed from the T-S-NSSAI and the associated S-NSSAI from the tuple provided to the NG-RAN by the 5GC.

One of the weakness of any pseudonym-based solution is the need to manage pseudonyms and change them frequently to protect entities from trackability and linkability attacks. The addition of hashing of temporary identifiers allows to minimize the overhead and reduce the complexity of pseudonym changes.

7.11.2 Solution details

The solution shown in figure 7.11.2-1 illustrates a UE performing an AS connection establishment while transmitting T-S-NSSAIs as hash values in the AS layer.



Figure 7.11.2-1: Hashed T-S-NSSAI transmission during AS connection establishment

1. The NG-RAN sends to the AMF in a NG\_SETUP\_REQUEST a list of supported S-NSSAI per TA (as per TS 38.300 [1]) and, additionally, T-S-NSSAI.

2. The NG-RAN obtains in a NG\_SETUP\_RESPONSE the list of supported NSSAIs from the AMF (as per TS 38.300 [1]), and additionally a corresponding list of supported T-S-NSSAIs.

3. The UE performs an initial Registration procedure with the network. The UE obtains a list of Allowed T-S-NSSAIs in the Registration Accept message over NAS. Optionally, the UE can obtain a RAND. If a RAND is not provided by the AMF the UE generates a RAND itself in the following step.

4. The UE computes the hash values of its requested T-S-NSSAIs using its S-TMSI and RAND. The UE transmits the T-S-NSSAIs hash values (instead of cleartext T-S-NSSAIs) in the AS layer in the RRCConnectionSetupComplete message. The UE may also include an indication about the nature of the slice assistance information in the AS layer (i.e. hashed T-S-NSSAI) to assist the NG-RAN in distinguishing the UEs capable of NSSAI privacy protection according to Rel-15.

By using its S-TMSI and a RAND in computations of T-S-NSSAI hashes, UEs requesting the same T-S-NSSAI will transmit different T-S-NSSAI hash values. It is assumed that the likelihood of the same S-TMSI being eventually re-allocated to a new UE using the same slice over time is negligible for any practical linkability attack. In addition, the UE will automatically transmit fresh T-S-NSSAI hash values during AS connection establishment after a new S-TMSI has been allocated as per existing procedures. By including RAND as a salt in the T-S-NSSAI hash computation, this solution supports the resistance to offline dictionary attacks that mounted with the knowledge of S-TMSI.

5. The NG-RAN does not "learn" but rather computes the hash using S-TMSI and RAND for each of the supported T-S-NSSAI received from the AMF. The NG-RAN has obtains T-S-NSSAI, S-NSSAI tuples from step 1 and by matching the T-S-NSSAI hash value received from the UE in step 4 to the hash value of a supported T-S-NSSAI from the AMF, NG-RAN is able to obtain the associated S-NSSAI directly from the tuple. When the complete list of requested S-NSSAIs from the UE is determined, the NG-RAN selects the appropriate AMF based on the list of requested S-NSSAIs as per current mechanisms. Matching hash values of T-S-NSSAI from the UE to the hash values of supported T-S-NSSAI from AMF adds moderate complexity to NG-RAN.

Note that in the idle mobility scenario, the new gNB computes the T-S-NSSAI hash values in a manner that is consistent with the gNB handling of T-S-NSSAI hash values during the Initial Registration procedure.

6. The NG-RAN routes the UE initial NAS message to the selected AMF.

NOTE: The NG-RAN may receive at any time an AMF Configuration Update message including an updated list of T-S-NSSAIs (e.g., following an update of the list of S-NSSAIs supported by the PLMN). In this solution, the network needs only to maintain one set of T-S-NSSAI per PLMN, i.e. with direct one-to-one mapping of S-NSSAI to T-S-NSSAI.

7.11.3 Evaluation

The Solution #11 addresses Key Issue #6: Confidentiality protection of NSSAI and home control.

It builds on a similar notion of temporary T-S-NSSAIs as introduced in existing Solution #8. The UE transmits hashed T-S-NSSAI in the AS layer instead of cleartext T-S-NSSAI while alleviating UE privacy/linkability attacks in addition to providing confidentiality protection for NSSAI transmission.

Solution 11 is an hybrid approach where actions for S-NSSAI privacy protection are performed in both the UE and the network. As such, it can also complement existing Solutions #8 and #10 as it would minimize the need for the network to provision the UE with new S-NSSAI pseudonyms every time an update is required.

Since T-S-NSSAI and random salt are provisioned and maintained on a per PLMN basis, the solution supports the case where the UE connects with a new gNB (under the same AMF). In an idle mobility scenario, the new gNB computes the T-S-NSSAI hash values the same way as the old gNB that handled the initial registration connection.

Solution 11 does not prevent passive attacks from UEs that have the same T-S-NSSAI and are using their knowledge of T-S-NSSAI.

## 7.12 Solution #12 Privacy protection of NSSAI

7.12.1 Introduction

This solution addresses the Key Issue #6 Confidentiality protection of NSSAI and home control.

This solution is based on the notion of temporary S-NSSAI (T-S-NSSAI) as in solution #8. In this solution, the AMF generates the T-S-NSSAIs based on the S-NSSAIs supported by the PLMN and stores the list of mapping between the S-NSSAIs and the T-S-NSSAI in the AMF. The NG-RAN gets and stores a list of mapping of S-NSSAI and T-S-NSSAI supported by the PLMN from the AMF in a NG Setup Response during an NG Setup procedure. UE are offered a temporary NSSAIs (T-S-NSSAIs) instead of cleartext S-NSSAIs in registration procedure. After that, to preserve the privacy, when UE use the T-S-NSSAI to access the slice, AMF will generate a new T-S-NSSAI for the allowed S-NSSAI and allocate for the UE.

The T-S-NSSAI needs to be updated based on predefined policies when it is used to ensure the privacy.

7.12.2 Solution details

Figure 7.12.2-1 illustrates this solution.



Figure 7.12.2-1: Privacy protection of NSSAI

The AMF generates the T-S-NSSAIs based on the S-NSSAIs supported by the PLMN and stores the list of mapping of the S-NSSAIs and the T-S-NSSAI in the AMF.

1. The UE has registered successfully to a PLMN and 5G NAS security context has been created, and NG-RAN gets and stores a list of mapping of S-NSSAI and T-S-NSSAI supported by the PLMN from the AMF in a NG Setup Response during an NG Setup procedure.

2. In the registration procedure, AMF identifies T-S-NSSAIs according to allowed S-NSSAIs based on the mapping of S-NSSAIs and T-S-NSSAIs. Then, AMF obtains the {allowed S-NSSAIs, T-S-NSSAIs} tuple.

3. In the registration/service accept message, {allowed S-NSSAIs, T-S-NSSAIs} tuple will be sent to UE instead of cleartext S-NSSAIs.

4. In a slice registration request message, UE transmits T-S-NSSAI to NG-RAN, NG-RAN identify the allowed S-NSSAI from the T-S-NSSAI based on the mapping of the NSSAI and T-NSSAI in the NG-RAN, and select the target AMF.

5. AMF calculates a new T-S-NSSAI according to the allowed S-NSSAI based on the predefined policies. Then AMF cancel the old T-S-NASSAI, and stores the {allowed S-NSSAI, new T-S-NSSAI} tuple.

6. In the Slice registration Accept message, the new T-S-NSSAI will be sent to UE.

7. AMF indicate NG-RAN to update the stored mapping of NSSAI and old T-NSSAI with the new mapping of NSSAI and new T-NSSAI.

Editor's Note: Idle mode mobility need to be addressed and solved.

7.12.3 Evaluation

The solution #12 addresses the key issue #6, the solution introduce a notion of temporary T-S-NSSAI similar as introduced in existing Solution #8. The AMF generates the T-S-NSSAIs based on the S-NSSAIs supported by the PLMN and stores the list of mapping between the S-NSSAIs and the T-S-NSSAI in the AMF. The NG-RAN gets and stores a list of mapping of S-NSSAI and T-S-NSSAI supported by the PLMN from the AMF. The UE gets and maintains a list of mapping between allowed S-NSSAIs and T-S-NSSAIs. The T-S-NSSAI will be updated based on the predefined policies when it is used, and accordingly the allowed S-NSSAI and T-S-NSSAI mapping relationship will also be updated. This solution will allow UE to use the updated T-S-NSSAI based on the predefined policies, thus achieving enhanced privacy protection.

# 8 Conclusions

## 8.1 Key issue-solution mapping

The present document contains six key issues and six solution proposals to solve them. A comparison of solution proposals against the key issues which they address is shown here below. Solutions address only some of the key issues.

Table 8.1: Solution mapping

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Key issue | Solution1 | Solution2 | Solution3 | Solution4 | Solution5 | Solution6 | Solution7 | Solution8 | Solution 9 | Solution 10 |
| #1 Authentication for access to specific Network Slices | Yes | Yes | NA | Evaluation pending | NA | NA | NA | NA | NA | NA |
| #2: AMF Key separation | NA | NA | NA | NA | NA | NA | NA | NA | NA | NA |
| #3: Security features for NSaaS | NA | NA | Evaluation pending | NA | NA | NA | NA | NA | NA | NA |
| #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization | Evaluation pending | NA | NA | NA | Evaluation pending | Evaluation pending | Evaluation pending | NA | NA | NA |
| #5: Access token handling between Network Slices | NA | NA | NA | NA | NA | NA | NA | NA | Evaluation pending | NA |
| #6: Confidentiality protection of NSSAI and home control | NA | NA | NA | NA | NA | NA | NA | Evaluation pending | NA | Evaluation pending |
| NA: Not Applicable | | | | | | | | | | |

## 8.2 Conclusions

### 8.2.0 General conclusions

- Slice specific authentication is optional to use.

- Slice specific authentication uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication.

- AMF confirms, locally or based on ARPF/UDM, whether slice authentication is required for each S-NSSAI.

- Slice specific authentication is based on EAP framework where AMF takes the role of the passing through Authenticator.

### 8.2.1 Conclusions for key issues

For Key Issue #1 Authentication for access to specific Network Slices, a merge of Solution#1, solution#2 and Solution#4 are recommended as the basis for the normative work.

For Key Issue#2, AMF key separation, it is concluded not to consider in the present document, since the use case that this key issue is addressing, is not concluded in TR 23.740 [5].

For Key Issue #4, it is recommended that no normative work is required.

For Key Issue #5, it is recommended that Solution #9 is used as the basis for normative work.

For Key issue#7, it is concluded that no normative work is needed.

# 9 Recommendations

For Key Issue #1 Authentication for access to specific Network Slices, a merge of Solution#1, solution#2 and Solution#4 are recommended as the basis for the normative work.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
|  |  |  |  |  |  |  |  |
| 16/11/18 | SA3#93 | S3-183333, |  |  |  | TR Skeleton |  |
| 16/11/18 | SA3#93 | S3-183807 |  |  |  | Tdocs S3-183808, S3-183802, S3-183810, S3-183531 | V0.1.0 |
| 01/02/19 | SA3#94 | S3-190539 |  |  |  | Tdocs S3-190533, S3-190534, S3-190535, S3-190536, S3-190537, S3-190538 | V0.2.0 |
| 15/03/19 | SA3#94-adhoc | S3-190948 |  |  |  | Tdoc S3-191002, S3-191007, S3-191034 | V0.3.0 |
| 05/09/19 | SA3#95 | S3-191731 |  |  |  | Tdocs S3-191730, S3-191732, S3-191733, S3-191734, S3-191735, S3-191736, S3-191737, S3-191738, S3-191739, S3-191008, S3-191009 | 0.4.0 |
| 06/27/19 | SA3#95Bis | S3-192346 |  |  |  | Tdocs S3-192363, S3-192260, S3-192367, S3-192369, S3-192370, S3-192371, S3-192372, S3-192374, S3-192375, S3-192376, S3-192373, S3-192366. | 0.5.0 |
| 08/30/19 | SA3#96 | S3-193119 |  |  |  | Tdocs S3-182852, S3-193121, S3-193122, S3-193123, S3-192124, S3-193125, S3-193201 | 0.6.0 |
| 10/18/210 | SA3#96 ad-hoc | S3-193732 |  |  |  | Tdocs S3-193301, S3-193354, S3-193731, S3-193734, S3-193735, S3-193736, S3-193819, S3-193820, S3-193821, S3-193822, S3-193823, S3-193824, S3-193825. | 0.7.0 |
| 22/11/19 | SA3#97 | S3-194543 |  |  |  | Tdocs S3-193964, S3-194542, S3-194547, S3-194544, S3-194545, S3-194546, | 0.8.0 |
| 18/05/2020 | SA3#99-e | S3-201360 |  |  |  | Tdoc S3-201261, S3-201978, S3-201061, S3-201159 | 0.9.0 |
| 2020-06 | SA#88-e | SP-200382 |  |  |  | EditHelp/MCC review  Presented for information and approval | 1.0.0 |
| 2020-07 | SA#88-e |  |  |  |  | Upgrade to change control version | 16.0.0 |