3GPP TR 33.813 V0.3.0 (2019-03)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Security Aspects;

Study on Security Aspects of Enhanced Network Slicing

(Release 16)

 ** 

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 Report 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.



Keywords

<keyword[, keyword]>

***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.

© 2018, 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 5

1 Scope 6

2 References 6

3 Definitions, symbols and abbreviations 7

3.1 Definitions 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Background 7

5 Requirements, assumptions and constraints 7

6 Key Issues 7

6.1 Introduction 7

6.2 Key Issue #1 Authentication for access to specific Network Slices 7

6.2.1 Key issue detail 7

6.2.2 Security threats 8

6.2.3 Potential security requirements 8

6.3 Key Issue #2: AMF Key separation 8

6.3.1 Key issue details 8

6.3.2 Security threats 9

6.3.3 Potential security requirements 9

6.4 Key Issue #3: Security features for NSaaS 9

6.4.1 Key issue details 9

6.4.2 Security threats or disadvantages 9

6.4.3 Potential Security requirements 9

6.5 Key Issue #4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization 9

6.5.1 Description 9

7 Solutions 12

7.1 Solution #1Slice Specific Authentication and Authorization 12

7.1.1 Introduction 12

7.1.2 Solution details 13

7.1.3 Evaluation 14

7.2 Solution #2 Slice Authentication 15

7.2.1 Introduction 15

7.2.2 Solution details 15

7.2.3 Evaluation 16

7.3 Solution #3 Security features for NSaaS 16

7.3.1 Introduction 16

7.3.2 Solution details 16

7.3.3 Evaluation 16

7.4 Solution #4 Solution for Slice Specific Authentication and Authorization with multiple registrations in the same PLMN 16

7.4.1 Introduction 16

7.4.2 Solution details 17

7.4.3 Evaluation 18

7.5 Solution #5 Privacy for Slice Authentication 18

7.5.1 Introduction 18

7.5.2 Solution details 18

7.5.3 Evaluation 20

8 Conclusions 20

9 Recommendations 20

Annex <X>: Change history 21

# 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.

# Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

# Scope

The scope of this Technical Report 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,

o Inter-slice security isolation

o Slice-specific security in the roaming scenarios.

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

o 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 modes

# 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] RFC 3748: "Extensible Authentication Protocol (EAP)"

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

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP 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 3GPP TR 21.905 [1].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

# 4 Background

# 5 Requirements, assumptions and constraints

Editor’s note: This section holds Enhanced Network Slice security requirements, assumptions and constraints which have to be considered or addressed by any of the proposed solution.

# 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 3GPP 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 3GPP 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 3GPP 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 TS28.530 [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 TS33.501 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 authentication by 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 3GPP 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 3GPP 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 shall 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.

Editor's Note: Key issue details have to be updated to reflect the decision in editor's note in 6.6.3

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.

Editor's note: this can be solved by configuration and doesn't require additional security mechanism.

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.

# 7 Solutions

## 7.1 Solution #1Slice 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, shall be 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 RFC 4282 [x]), 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 Secondary Authentication and Authorisation or not. If the Slice specific Authentication security capability is not included in the registration request, the AMF shall not allow UE to access to any Network Slice for which Slice-specific authentication is required.

The assumption is that the Slice specific authentication is performed as a secondary authentication 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

AMF

AUSF

Slice Specific AAA

4d. EAP Request-Response Messages

3. AMF checks subscription data and UE security capability for Slice specific secondary authentication, for each NSSAI

5. UE and AMF knows the list of authorized and subscribed NSSAIs

4. Slice specific secondary Authentication

4e. EAP-SUCCCESS

1. REG-REQ (NSSAI,) etc)

4c. Authentication Request (EAP Identity Response, S-NSSAI, GPSI )

4a. NAS Message (EAP Identity Request, S-NSSAI)

2. Primary Authentication using 3GPP credentials

UE

4f. NAS Message (EAP SUCCCESS, S-NSSAI)

4b. NAS Message (EAP Identity Response, S-NSSAI)

Step 1-2: Regular Registration Request and Authentication of the UE. Primary Authentication is complete and NAS Security is established.

Step 3: The AMF checks the UE Subscription data received in the primary Authentication process, whether Slice Specific Authentication is enabled for any of the S-NNSAIs requested by the UE.

Step 4a-4f: If Slice Specific Authentication is enabled for the UE, AMF initiates Slice specific Authentication using EAP, by requesting the EAP User ID for the specific Slice S-NSSAI. The NAS message to the UE includes the S-NSSAI value so the right Network Slice authentication is executed and so the corresponding User ID and credentials are used by the UE. The AMF may start in parallel several such authentication and Authorisations procedures if more than one S-NSSAI is enabled for Secondary Slice-Specific Authentication and Authorisation.

Editor Note: The acceptability of nesting EAP authentication during the Registration Procedure approach is FFS with assistance of CT1 and SA2 if needed

Editor Note: Performance and correlation implications due to parallel EAP runs, if more than one S-NSSAI is subject to Slice-Specific Authentication and Authorisation is FFS.

Step 5: At the completion of Slice Specific authentication, the UE and AMF will have a set of allowed NSSAIs already authenticated for service. The AMF proceeds with PDU session setup for each of the authenticated S-NSSAIs.

### 7.1.3 Evaluation

## 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 RFC 3748 [6].

Editor’s Note: The acceptability of nesting EAP authentication during the Registration Procedure approach is FFS with assistance of CT1 and SA2 if needed.

### 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 7.2.1. The procedure is based on the registration procedure in TS23.502.

 Figure 7.2.1 Registration overview when slice authentication is performed

Steps 1 indicates the registration steps the same as 1-7 as in TS23.502 [4].

Steps 2 indicates the same Primary Authentication procedure as in TS33.501 [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.

Editor’s note: UE skipping Primary Authentication if it has a security context and then doing Slice specific authentication needs to be described and verified with Initial attach procedure.

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

Step 4: 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 Slice Authentication Assistance Function (SAAF), 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 RFC 3748 [6]. The number of messages exchanged is dependent on the EAP method used.

Step 5: The slice registration is completed after slice authentication is completed.

### 7.2.3 Evaluation

## 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 shall be able to ignore 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 [x] respectively

### 7.3.3 Evaluation

N.A.

## 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 (SSA) in TS 23.502 [4]. SSA 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 SSA 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 SSA is performed after the Registration procedure. After the SSA 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 3GPP first and then over non-3GPP (the reverse scenario is also possible). The UE sends over 3GPP access a Registration Request which includes in the Requested NSSAI an S-NSSAI subject to SSA. Then, the UE includes the same S-NSSAI in the Registration Request over non-3GPP access. The UE waits for the completion of the SSA procedure for the S-NSSAI over the 3GPP access before performing the Registration over non-3GPP access. The AMF may decide to skip a new SSA run for the S-NSSAI for which the UE was already authenticated over 3GPP access.

### 7.4.2 Solution details

The solution shown in Figure 7.x.1 illustrates a UE performing multiple registrations with the same serving PLMN while requesting the same S-NSSAI subject to SSA in each Registration Request. The Registration and SSA procedural steps over 3GPP are as specified in TS 23.502 [4]. The solution can be applied in the reverse scenario where the UE registers over non-3GPP access prior to registering over 3GPP access. The UE waits for SSA over 3GPP to complete before performing a Registration procedure over non-3GPP access.



Figure 7.4.1 Multiple Registration with the same PLMN with same S-NSSAI subject to SSA

Step 1: UE and network performs a standard Registration procedure over 3GPP 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 SSA 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 and include an indication of a pending SSA for the S-NSSAI.

Step 2: UE and network perform a standard SSA procedure over 3GPP. 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.

Step 4: UE checks that SSA is completed over 3GPP before starting the Registration procedure over non-3GPP e.g. S-NSSAI is included in the Allowed NSSAI for 3GPP.

Step 5-6: UE sends a Registration Request over non-3GPP protected using the available common NAS security context. UE may indicate a preference (e.g. in the security capabilities) to skip the SSA for the S-NSSAI over non-3GPP access if the UE is already authenticated for that S-NSSAI over 3GPP access. AMF decides to skip a new Primary authentication over the non-3GPP access.

Step 7: AMF determines that S-NSSAI is subject to SSA and that the UE is already authenticated for S-NSSAI following the previous Regitration over 3GPP. The S-NSSAI authentication result (e.g. success/failure) from previous SSA run over 3GPP may be included in the common NAS security context. AMF may decide to skip SSA run over non-3GPP for the S-NSSAI.

Step 8: AMF sends a Registration Accept to the UE including S-NSSAI in the Allowed NSSAI for non-3GPP

Step 9: UE may start using the S-NSSAI over any access, e.g. it may establish a PDU Session using S-NSSAI over non-3GPP 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 SSA 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 SSA over that AMF selected access e.g. SSA 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 UCU procedure for each access.

Editor's Note: Call flow and terminology need to be aligned with TS 23.501 [3] and TS 23.502 [4].

Editor’s Note: Further justification for the dependency of this solution on the type of access is needed.

### 7.4.3 Evaluation

TBD

## 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.Y.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 interfdace with external service provider via the NEF is utilized in order to provision the NSSAI and public kery 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.

# 8 Conclusions

# 9 Recommendations

Annex <X>:
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 |

Change history of this template:

|  |  |  |
| --- | --- | --- |
| 2001-07 | Copyright date changed to 2001; space character added before TTC in copyright notification; space character before first reference deleted. | 1.3.3 |
| 2002-01 | Copyright date changed to 2002. | 1.3.4 |
| 2002-07 | Extra Releases added to title area. | 1.3.5 |
| *2002-12* | *“TM” added to 3GPP logo* | *1.3.6* |
| *2003-02* | *Copyright date changed to 2003.* | *1.3.7* |
| *2003-12* | *Copyright date changed to 2004. Chinese OP changed from CWTS to CCSA* | *14.0* |
| *2004-04* | *North American OP changed from T1 to ATIS* | *1.5.0* |
| *2005-11* | *Stock text of clause 3 includes reference to 21.905.*  | *1.6.0* |
| *2005-11* | *Caters for new TSG structure. Minor corrections.* | *1.6.1* |
| *2006-01* | *Revision marks removed.* | *1.6.2* |
| *2008-11* | *LTE logo line added, © date changed to 2008, guidance on keywords modified; acknowledgement of trade marks; sundry editorial corrections and cosmetic improvements* | *1.7.0* |
| *2010-02* | *3GPP logo changed for cleaner version, with tag line;LTE-Advanced logo line added; © date changed to 2010;editorial change to cover page footnote text;trade marks acknowledgement text modified;additional Releases added on cover page;proforma copyright release text block modified* | *1.8.0* |
| *2010-02* | *Smaller 3GPP logo file used.* | *1.8.1* |
| *2010-07* | *Guidance note concerning use of LTE-Advanced logo added.* | *1.8.2* |
| *2011-04-01* | *Guidance of use of logos on cover page modified; copyright year modified.* | *1.8.3* |
| *2013-05-15* | 1. *Changed File Properties to MCC macro default*
2. *Removed R99, added Rel-12/13*
3. *Modified Copyright year*
4. *Guidance on annex X Change history*
 | *1.8.4* |
| *2014-10-27* | *Updated Release selection on cover. In clause 3, added "3GPP" to TR 21.905.* | *1.8.5* |
| *2015-01-06* | *New Organizational Partner TSDSI added to copyright block.Old Releases removed.* | *1.9.0* |
| *2015-12-03* | *Provision for LTE Advanced Pro logo Update copyright year to 2016* | *1.10.0* |
| *2016-03-08* | *Standarization of the layout of the Change History table in the last annex.(Unreleased)* | *1.11.0* |
| *2016-06-15* | *Minor adjustment to Change History table heading* | *1.11.1* |
| *2017-03-13* | *Adds option for 5G logo on cover* | *1.12.0* |
| *2017-05-03* | *Smaller 5G logo to reduce file size* | *1.12.1* |