|  |  |
| --- | --- |
| 3GPP TR 33.875 V0.3.0 (2021-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on enhanced security aspects of the 5G Service Based Architecture (SBA);  (Release 17) | |
|  | |
|  |  |
|  | |
| 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.  © 2021, 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 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 8

3.3 Abbreviations 8

4 Trust model 8

4.0 General 8

4.1 Actors 8

4.2 Deployment options 9

4.3 Description of the trust assumptions 9

4.3.1 Trust within one PLMN 9

4.3.2 Trust in Inter-PLMN communication 10

5 Key issues 11

5.1 Key issue #1: Authentication of NRF and NF Service Producer in indirect communication 11

5.1.1 Key issue details 11

5.1.2 Security threats 11

5.1.3 Potential security requirements 11

5.2 Key issue #2: SCP security domains 11

5.2.1 Key issue details 11

5.2.2 Security threats 12

5.2.3 Potential security requirements 12

5.3 Key Issue #3: Service access authorization in the "Subscribe-Notify" scenarios 12

5.3.1 Key issue details 12

5.3.2 Security threats 13

5.3.3 Potential security requirements 13

5.4 Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP 13

5.4.1 Key issue details 13

5.4.2 Security threats 13

5.4.3 Potential security requirements 13

5.5 Key issue #5: End-to-end integrity protection of HTTP messages 13

5.5.1 Key issue details 13

5.5.2 Security threats 14

5.5.3 Potential security requirements 14

5.6 Key issue #6: Access token usage by all NFs of an NF set 14

5.6.1 Key issue details 14

5.6.2 Security threats 15

5.6.3 Potential security requirements 15

5.X Key issue #X: <distinct KI name> 15

5.X.1 Key issue details 15

5.X.2 Security threats 15

5.X.3 Potential security requirements 16

6 Solutions 16

6.0 Mapping of solutions to key issues 16

6.1 Solution #1: Verification of the entity sending the service response in indirect communication without delegated discovery 16

6.1.1 Introduction 16

6.1.2 Solution details 17

6.1.3 Evaluation 18

6.2 Solution #2: Authorization between NFs and SCP 19

6.2.1 Introduction 19

6.2.2 Solution details 19

6.2.3 Evaluation 20

6.3 Solution #3: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer 20

6.3.1 Introduction 20

6.3.2 Solution details 20

6.3.2.1 Request of access token on behalf of the consumer 20

6.3.3 Evaluation 21

6.4 Solution #4: Service request authenticity verification in indirect communication 22

6.4.1 Introduction 22

6.4.2 Solution details 22

6.4.3 Evaluation 23

6.5 Solution #5: End-to-end integrity protection of HTTP body and method 23

6.5.1 Introduction 23

6.5.2 Solution details 24

6.5.3 Evaluation 24

6.6 Solution #6: Verification of Service Response from a NF Service Producer at the expected NF Set 25

6.6.1 Introduction 25

6.6.2 Solution details 25

6.6.3 Evaluation 25

6.7 Solution #7: Access token request for NF Set 25

6.7.1 Introduction 25

6.7.2 Solution details 26

6.7.3 Evaluation 26

6.Y Solution #Y: <distinct solution name> 26

6.Y.1 Introduction 26

6.Y.2 Solution details 26

6.Y.3 Evaluation 27

7 Conclusions 27

7.X <distinct KI name> 27

Annex A (informative): Change history 28

**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.

# 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.

# Introduction

The 5G core network introduced a Service-Based Architecture (the so-called SBA). This brought fundamental impacts on the way new services are created and how the individual Network Functions (NF) communicate. A more open and adaptable system design necessitated to study different approaches to enforce the security requirements of 3GPP systems, whilst not impeding flexible service creation and future innovations. Along with these architectural challenges, SBA further introduced changes to the protocol stack and serialization format of the 5G core network.

The SBA was set on providing solutions for authentication and authorization in direct communication scenarios as well as the N32 security. Later on enhancements were introduced for indirect communication scenarios as well as the concept of Client Credential Assertion to allow NRF/NF Service Producer to directly authenticate a NF Service Consumer.

While the SBA provides a good level of security, several additional aspects have been identified that may bring new potential threats. This will be documented by the present document.

# 1 Scope

The present document studies enhanced security aspects of the 5G Service Based Architecture. It will analyse potential threats, study necessary security enhancements, and document decisions of solutions to be adopted or not adopted after evaluating the risks versus the complexity.

In particular, the following topics are addressed:

- Need and mechanism of enabling end to end authentication in roaming case if no cross-certification between operators is enabled;

- Need and mechanism of enabling NF Service Consumer authentication of NRF and the NF Service Producer;

- Need for addressing potential security impact of different deployment scenarios including the several SCPs;

- Verification of URI in subscription/notification;

- Dynamic authorization between SCPs or NF and SCP;

- End-to-End Critical HTTP headers/body parts integrity protection;

- Security of NRF service management.

# 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 (5GS); Stage 2".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms 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].

Definition format (Normal)

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 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].

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

# 4 Trust model

## 4.0 General

With introduction of the service-based architecture and moving at the same time to cloud deployments, new attack vectors such as that for NFs deployed in clouds give ground to vulnerabilities and, thus, can impact the mobile operator domain. As more important it is to assure the trust also within one operator's network. For this, security concepts have been introduced.

A service request requires mutual authentication, thus all network functions support mutually authenticated TLS and HTTPS. After registration and discovery, any service request of a network function needs also to be authorized by an authorization server (NRF) before a NF Service Consumer can consume the services of a NF Service Producer. For this 5G introduces the concept of authorization token utilizing the OAuth 2.0 authorization framework.

With Rel-16 indirect communication via a Service Communication Proxy (SCP) is possible. SCPs can be operated in a fully service-meshed environment or as standalone entity.

In the following the trust relationships between the entities of an operator network are described.

## 4.1 Actors

The following actors within one PLMN are considered: NF, NRF, SCP.

- NFs can provide services or consume services.

- NRF is a repository capturing NF profiles of NFs offering its services to other NFs. It receives discovery requests from NF instances, maintains NF profiles and acts as an authorization server. NRF responds to authorization requests by NF Service Consumers by providing OAuth 2.0 access tokens to authorize a NF Service Consumer for gaining access to a service from a NF Service Producer.

- SCP is a service communication proxy used in indirect communication to interact with NFs and other SCPs within the PLMN. SCP also communicates with the SEPP.

The following types of actors when requesting services from another PLMN are considered: SEPP.

- SEPP sits at the edge of one operator's network to allow for a secured communication with the other operator's network’s SEPP.

## 4.2 Deployment options

The following deployment options need to be considered:

- Direct communication within the same PLMN vs direct communication in Inter-PLMN scenario, i.e. without SCP behind SEPP.

- Indirect communication in the same PLMN vs indirect communication in Inter-PLMN scenario: For both, SCP standalone and service mesh need to be considered.

SEPP to SEPP communication is secured on N32-c via TLS and on N32-f via TLS (i.e. transport layer security) or PRINS (i.e. application layer security on top of NDS/IP or TLS). TLS provides for authentication between two entities. Thus, securing at transport layer provides hop-by-hop security between two SEPPs. PRINS provides end-to-end application layer security between two SEPPs.

Hop-by-hop security introduces the additional risk of allowing an entity on the path to gain full access to signalling messages exchanged. An intermediary node can read, hide, or modify the originator information.

## 4.3 Description of the trust assumptions

### 4.3.1 Trust within one PLMN

This clause describes the existing trust relationships within one PLMN. This trust is required whether the NF Service Consumer (NFc) and NF Service Producer (NFp) are within the same PLMN or not. The trust relationships described here can be replaced by security mechanisms.

NOTE: Whether the list of existing trust relationships described below is complete, depends on deployment choices.

NRF is the core entity handling registration, discovery and authorization requests by NFs or SCP. The operator needs to apply necessary security measures to secure these operations. It is assumed that there is only one NRF, or all NRFs are within the same trust domain, i.e. all NRFs are in the same security domain and the same entity(-ies) are responsible for all NRFs.

**Registration:**

An NF Service Provider needs to trust the NRF that no other NF can register with the identity of NFp.

The following applies only when there is no direct connection between NF and NRF.

If there is no direct communication between NF and NRF, an NF Service Provider needs to trust that the SCPs forward NFp profiles unmodified.

If there is no direct communication between NF and NRF, an NF Service Provider needs to trust the SCPs that no other NF can impersonate the identity of NFp towards the SCP, thus enticing the SCP to register an NF with the false identity.

**Discovery:**

An NF Service Consumer needs to trust NRF to provide profiles of authenticated NF Service Providers that offer their services to the requesting consumer.

An NF Service Consumer needs to trust SCP to forward correctly the profiles of authenticated NF Service Providers that offer their services to the requesting consumer.

**Access token request:**

Trust in direct communication between NFs, NFs and SCP/SEPP, as well as SCP and SEPP is assumed per 33.501 with mandatory mutual authentication using TLS.

An NF Service Provider needs to trust NRF to provide access tokens for consumption of its services only to those NF Service Consumers that have requested for it and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

Authentication and confidentiality protection in indirect communication is only achieved between NF and SCP, (potentially between multiple SCPs), SCP and NRF as well as SCP and SEPP, but additional considerations are needed for achieving trust between NFs, NF and NRF, as well as NRF and SEPP, NF and SEPP, when an SCP is on the path. This is because all traffic in indirect communication passes through SCPs, and TLS terminates at SCPs.

Thus, the SCP needs to be trusted by NFc and NFp, to only forward authentication tokens or CCA with the original request, as well as to forward information only between the legitimate endpoints of the communication.

An NF Service Provider needs to trust NRF to provide access tokens for consumption of its services only to those SCPs that are authorized by the NF Service Consumers that have requested for it and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

It also needs to be distinguished if SCP is collocated to NFs (service mesh) or standalone.

Editor's note: Further analysis on the trust model concerning different deployments of SCP is ffs.

### 4.3.2 Trust in Inter-PLMN communication

With 5G, a new element has been introduced. The SEPP, i.e. the Secure Edge Protection Proxy acting as perimeter of PLMN, is responsible to secure signalling with the SEPP of another PLMN via the Internet.

The SEPP of the sending PLMN needs to trust the SEPP of the receiving PLMN that no other entity on the path has unauthorized access or can modify signalling messages if not permitted to do so by policy.

**Discovery:**

The NRF in the NF Service Consumer PLMN needs to trust the cSEPP to route the request to the pSEPP representing the target PLMN and apply the correct protection policies to the discovery request.

The NRF in the NF Service Provider PLMN needs to trust the pSEPP to authenticate the origin network of the discovery request and ensure that this origin network is correctly represented in the request arriving at the pNRF.

**Access token request:**

When requesting an access token from the NRF in another PLMN, there is always an indirect communication involving the cSEPP and pSEPP. In addition, SCPs can be involved in either network.

An NF Service Provider needs to trust pNRF to provide access tokens for consumption of its services only to those NF Service Consumers in another PLMN and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

An NF Service Provider needs to trust cNRF to provide access tokens for consumption of its services only to those NF Service Consumers in another PLMN that have requested for it and only for those services that are allowed by the registered NRF policy and the registered NF Service Provider policy.

An NF Service Provider needs to trust SCP in the Service Consumer PLMN to only forward authentication tokens or CCA with the original request, as well as to forward information only between the legitimate endpoints of the communication.

**Service request:**

An NF Service Provider needs to trust pSEPP to authenticate and verify the NFc's PLMN included in the request in order to be able to perform dynamic authorization.

A pSEPP needs to trust that the cSEPP is not forwarding requests on behalf of foreign PLMNs.

# 5 Key issues

## 5.1 Key issue #1: Authentication of NRF and NF Service Producer in indirect communication

### 5.1.1 Key issue details

When SCP is present, the TLS between an NF Service Consumer and NRF/NF Service Producer can be split into at least two segments (NFc-SCP, SCP-NRF or SCP-NFp). In this case, the NF Service Consumer and NRF/NF Service Producer do not directly authenticate each other via TLS.

Client Credentials Assertion (CCA) has been specified to allow NRF or another NF to directly authenticate an NF Service Consumer in the presence of an SCP, but direct authentication of the NRF/NF Service Producer by the NF Service Consumer has not been addressed in indirect communication. The key issue will investigate solutions allowing the NF Service Consumer to directly authenticate the NRF/NF Service Producer in indirect communication.

### 5.1.2 Security threats

Editor’s note: The threats need to be further clarified and studied

An NF Service Consumer could send service requests to an unintended NF.

An NF Service Consumer could receive service responses from an unintended NF.

### 5.1.3 Potential security requirements

The 5GS should provide a mechanism that allows an NF Service Consumer to authenticate an NRF or an NF Service Producer during an indirect communication with them via an SCP.

## 5.2 Key issue #2: SCP security domains

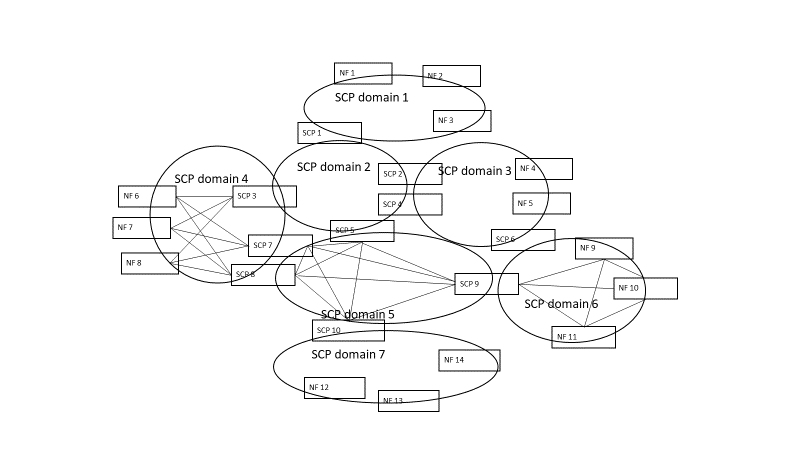
### 5.2.1 Key issue details

Editor’s note: SCP security domains to be defined.

TS 23.501 [3] addresses the aspects of handling multiple SCPs in indirect communication without and with delegated discovery and introduced SCP domains, which comprises multiple SCPs. NF Service Consumers or/and SCPs need to request NRF to discover the next hop SCP to route a service request from the NF Service Consumer to a NF Service Producer via multiple SCPs. 23.502 describes in the SCP profile SCP domain registration details about interconnected SCPs to and thus also identifies SCPs that interconnect domains.

The primary purpose of SCP domains is to describe the connectivity topology within a network. All SCPs within an SCP domain can directly interconnect. One SCP can be part of multiple SCP domains. In fact, the primary purpose of intermediate SCPs in the path is to interconnect SCP domains, thus, there are boundaries between SCP domains at each SCP in the path.

PLMN-wide trust between NFs and SCPs is an option, but more restrictions could be desirable in complex networks with SCP domains, e.g. if SCPs are operated in different regions/provinces. There can be several technical domains within a PLMN, where equipment with different capabilities is deployed and signalling also varies in some respects, e.g., if equipment upgrade is performed in a stepwise manner. Such technical domains can be defined based on computer centre boundaries, based on operators of subnetworks, based on regions/provinces, etc.

Figure 5.2.1-1: Illustration of SCP domains connecting via dedicated SPCs

This key issue is to study whether there is a need of one or several SCP domains becoming regions of trust of finer granularity than PLMN and whether there is a necessity of trust and policing of communication within or among such domains, i.e. for the case that request messages traverse a boundary between trust domains.

### 5.2.2 Security threats

Editor's Note: FFS. Maybe not applicable if only architectural security requirements are specified.

### 5.2.3 Potential security requirements

Editor's Note: FFS. Maybe not applicable if only architectural security requirements are specified.

## 5.3 Key Issue #3: Service access authorization in the "Subscribe-Notify" scenarios

### 5.3.1 Key issue details

"Subscribe-Notify" NF Service illustration 1 specified in TS 23.501, clause 7.1.2, allows one NF (e.g. NF\_A) to subscribe to notifications of NF producer (e.g. NF\_B). The subscription request includes the notification endpoint (e.g. the notification URL) of the NF Service Consumer. In this scenario, NF\_A subscribes the service of NF\_B for itself.



Figure 5.3.1-1: "Subscribe-Notify" NF Service illustration 1

"Subscribe-Notify" NF Service illustration 2 specified in TS 23.501, clause 7.1.2, allows one NF (e.g. NF\_A) to subscribe the service of NF producer (e.g. NF\_B) on behalf of another NF (NF\_C), in which the notification URI of NR\_C is included. It means the NF\_C will receive the notification message even though the subscribe request is sent by NF\_A.



Figure 5.3.1-2: "Subscribe-Notify" NF Service illustration 2

For instance, as defined in TS 23.502 clause 4.15.3.2.2, UDM could send subscribe request including the UDM URI and NEF URI to the AMF to subscribe service on behalf of the NEF, i.e. Namf\_EventExposure\_subscribe request. If the monitored event occurs, the AMF will send the event report to the associated notification URI endpoint of the NEF.

### 5.3.2 Security threats

TBD

### 5.3.3 Potential security requirements

TBD

## 5.4 Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP

### 5.4.1 Key issue details

This key issue is about authorization of SCP to request services on behalf of an NF or of another SCP and how this authorization is verified by the NRF or NF Service Producer.

### 5.4.2 Security threats

If the NRF cannot verify if the SCP has been authorized by the NF Service Consumer, the SCP can send a service request and receive a valid service response on behalf of NF Service Consumer, even though the NF Service Consumer has not authorized the SCP.

If the NF Service Producer cannot verify if the SCP has been authorized by the NF Service Consumer, the NF Service Producer can provide a service response to an unauthorized entity.

### 5.4.3 Potential security requirements

The 5GS should provide a mechanism for how an NRF or NF Service Producer can verify an SCP has been authorized by an NF Consumer to request access tokens or services on behalf of the consumer.

## 5.5 Key issue #5: End-to-end integrity protection of HTTP messages

### 5.5.1 Key issue details

Currently, in the case of indirect communication with an SCP in the path between an NF Service Consumer and an NF Service Producer, the integrity protection of the HTTP messages is provided by TLS for each hop but not end-to-end between the NF Service Consumer and the NF Service Producer. Since an SCP may need to change the content of an HTTP message, this KI is to investigate how end-to-end integrity protection of HTTP messages can be achieved while at the same time continue to allow the SCP to perform necessary mediation of HTTP messages.

NOTE: Potential issues with backwards compatibility with existing procedures are to be considered during the study.

### 5.5.2 Security threats

Critical elements of an HTTP message that are not end-to-end integrity protected could be modified by an attacker. In more detail, a service request in indirect communication could lead to attacks by Man in the Middle, which for instance can intercept the service request and try to modify the content of the message or HTTP (custom) header. This could cause communication failure, lead to DoS attacks.

### 5.5.3 Potential security requirements

In the case of indirect communication with an SCP in the path between an NF Service Consumer and an NF Service Producer, the 5GS should support end-to-end integrity protection of critical elements of an HTTP message while allowing the SCP to continue to perform necessary HTTP message mediation.

Editor's Note: Collaboration with CT4 is needed in identifying critical HTTP elements that need not be mediated by an SCP.

The NF Service Producer should be able to verify that critical elements of a service request of the NF Service Consumer received via the SCP have not been modified.

## 5.6 Key issue #6: Access token usage by all NFs of an NF set

### 5.6.1 Key issue details

SBA introduces the concepts of NF Set and NF Service Set, i.e. sets of functionally equivalent and inter-changeable NFs or NF services. 5G SBA architecture design further allows for the concept of stateless NFs, where by binding indication the NF Service Resource owner can indicate to the NF Service Consumer, for a particular resource, whether it is to an NF Service Instance, NF Instance, NF Service Set or NF Set.

**Access token usage for NF Service Producer Set:**

As specified in Rel-16, an access token can be provided by NRF for consuming a service from a dedicated producer with a distinct NF Instance Id or a specific NF type or a NF Set Id for a NF Set of NF Service Producer instances. Thus, if the NF Service Producer belongs to a NF Set, the access token can be consumed by a NF Service Consumer from any of the NF Service Producers within the set.

**Stateless NFs:**

NF Set concept supports stateless NF implementations i.e. an NF Service Producer or NF Service Consumer in a NF Set can take over at any time the control of respectively resource contexts (e.g PDU session contexts) or session contexts to receive notifications. NFs typically produce and consume services (e.g. an SMF producing the PDUSession service to establish PDU session also needs to consume services to render its PDU session service, e.g. it consumes PCF and CHF services), taking over the control at any time allows for reliability of NF instances within the same NF Set (e.g. when an NF instance fails or is scaled-in).

If an access token is granted to a specific NF Service Consumer instance, other NF Service Consumer instances in the same NF Set currently need to request always a new access token, whenever a request is sent by a different NF Service Consumer instance.

For example, a connection is released since the NF Service Consumer is stateless, then another NF Service Consumer of the NF Set can be assigned to continue subsequent communication. This optimization is part of 23.501/29.500 specifications, but the related security aspects of using such optimization have not been addressed in 33.501 Rel-16. Thus, any NF in NF Set issuing a service request targeting an existing context need to request a new access token. Further, any subsequent request may be sent to any other NF than the initiator NF of the NF Set; and also in this case, a new access token is needed.

**Examples:**

The following examples show, why it is useful to have an access token also be valid/usuable for any NF in the NF Set during its validity time.

1) A SMF instance can wish to remain the SMF (binding to itself), but at end of procedure, i.e. non-moving UEs anymore foreseen. Thus, this SMF gets stateless because it considers it is a long time before next SMF involvement. Thus, if another SMF than the service request originating SMF would get involved later, it would either need a new token or it could re-use the non-expired access token, the other SMF instance of the NF Set received earlier.

2) In stateless UDM, the binding within UDM set can be used. When UDM instance of UDM Set initially creates an AMF event subscription, it has to request an access token to be able to access the corresponding AMF service. However, the UDM instance that created the subscription may be a completely different UDM instance of the UDM Set that is later deleting the subscription. Thus, the same token within the NF Set should be usuable for achieving this. Otherwise we end up at massive access token requests that are used in the same context of service consumption.

If an access token canot be used by any ND in the NF Set during its validity time, the need for access token requests is multiplied, because every time there is a different NF instance in the NF Set that is requesting from the existing resource would need a new access token, while this is not necessarily required.

**Key issue scope:**

This key issue proposes to study the advantages and disadvantages from security perspective that any NF in a NF Set targetting a service of an existing resource can use an access token provided to a NF Set.

If acceptable from security point of view, the benefit of this concept would be that it maps with the 5G SBA architecture design, the concept of stateless NF, and the binding level of NF Set, where any NF instance can serve subsequent request without everytime requesting a new access token.

Thus, this key issue studies the security implications of a stateless NF Service Consumer belonging to a NF Set requesting an access token on behalf of and for usage by all NF instances of the NF Set.

### 5.6.2 Security threats

Not applicable, since concept of access token is already in place.

Editor's Note: possibly threats resulting of the usage of the same access token by different NFs of the same NF set can be captured here.

### 5.6.3 Potential security requirements

All NF Service Consumers of an NF Set shall be authorized to use the access token requested by one NF Instance of the NF Set, if the access token is issued for NF Set.

The 5GS may provide means to authorize a NF Service Consumer of the NF Set to request and/or use an access token requested by another NF Service Consumer of the same NF Set.

## 5.X Key issue #X: <distinct KI name>

### 5.X.1 Key issue details

TBD

### 5.X.2 Security threats

TBD

### 5.X.3 Potential security requirements

TBD

# 6 Solutions

## 6.0 Mapping of solutions to key issues

**Table 6.0-1: Mapping of solutions to key issues**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Solutions** | **Key Issues** | | | | | | | |
|  | #1 | #2 | #3 | #4 | #5 | #6 |  |  |
| #1: Service response verification in indirect communication without delegated discovery | X |  |  |  |  |  |  |  |
| #2: Authorization between NFs and SCP |  |  |  | X |  |  |  |  |
| #3: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer |  |  |  | X |  |  |  |  |
| #4: Service request authenticity verification in indirect communication |  |  |  |  | X |  |  |  |
| #5: End-to-end integrity protection of HTTP body and method |  |  |  |  | X |  |  |  |
| #6: Verification of Service Response from a NF Service Producer at the expected NF Set | X |  |  |  |  |  |  |  |
| #7: Access token request for NF Set |  |  |  |  |  | X |  |  |

## 6.1 Solution #1: Verification of the entity sending the service response in indirect communication without delegated discovery

### 6.1.1 Introduction

This solution is addressing KI#1.

This solution allows the NF Service Consumer (NFc) to verify the genuineness of the NF Service Producer (NFp), which is sending the response, when an SCP is used in between and the discovery of NFp has not been delegated to the SCP (see 3GPP TS 33.501 [X] Annex R, model C). I.e. The deployment scenario addressed is indirect communication (via SCP) without delegated discovery.

The solution counters a malicious SCP or a Man in the Middle (MitM) that could forward the service request to a malicious or unauthorized NF Service Producer, i.e. a NFp that was not intended to provide a response. Especially where multiple SCPs are involved, and the NF Service Consumer does not know whether the right entity or some malicious entity is responding its request, this situation can occur.

Currently there is no means to prevent a malicious SCP or Man in the Middle to forward the service request to a different NF Service Producer.

Editor’s Note: Applicable deployment scenarios to be clarified.

The example shows a Service request with a token for service consumption from NFp that has been redirected by a malicious MitM to a different NF Service Producer, which can be a rogue NF cooperating with the MitM.



**Figure** 6.1.1-A**:** Example of a potential attacking scenario

Editor's Note: It is ffs in which deployment scenarios the solution is applicable and whether re-selection of the producer could be a desired property (see 23.502, clause 4.17.11 and TS 23.501 Table 6.3.1.0-1).

This solution avoids that a service response is returned back to the NF Service Consumer by an unauthenticated and/or unauthorized MitM.

### 6.1.2 Solution details

NFc discovers NFp at NRF and requests an access token for a specific NFp Instance ID for consuming a service from NFp.

If indicated by NFc in the service request, the NFp provides back its CCA\_NFp. Thus, the NFc can compare the NFp instance ID in the CCA\_NFp with the selected NF instance ID when NFc requested the service. I.e. NFc can check if the NFp ID that the access token was provided for by NRF is matching the NFp ID present in the subject of CCA\_NFp. Since NFp provides its CCA\_NFp, this comparison is even possible if the response is sent via SCP.

If the NFp includes its own CCA\_NFp in the service response, NFc can verify that the sender of the service response is the one that NFc's service request was sent to.

Editor's Note: It is ffs if the CCA\_NFp ensures that the NFc can verify that the service response received from the specific NFp was requested in the original service request from this producer.

This allows authentication of NFp by NFc, i.e. by NFc verifying the CCA\_NFp against the original NFp Instance ID, for which NRF provided the access token. NFp is authenticated, if the certificate NFp used to sign CCA has been verified by NFc. In case of failure, error messages can be triggered and reported to the operator.

In the following, the steps are described in detail.



Figure 6.1.2-1: Flow chart for allowing verification of NF sending the service response

Step1,2: NFc selects NFp to send a service request along with the token. To allow NFc to validate the service response, it will require validation of the producer's identity via CCA as part of the response.

Step 3: SCP intends to forward the service request to further SCPs. If SCP or some proxy is malicious (or MitM), it forwards the service request to a rouge NFp instead.

Step 4,5: A rouge NF can try to send the service response without performing the authorization. As the service request requires validation, the NFp has to add its CCA header, CCA\_NFp.

Step 6: SCP will relay back the response to NFc including the CCA\_NFp.

Step 7: NFc compare the NFp instance ID received and Set ID (if present) in the CCA\_NFp with the one used for service request. If it is the same, then NFc is assured the service response is received from a genuine NFp.

Step 8: If it does not match, the NFc can also raise an alarm and revert the transaction at NFc.

Editor's Note: How does the service response received from the NFp was requested in the original service request is FFS.

### 6.1.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

## 6.2 Solution #2: Authorization between NFs and SCP

### 6.2.1 Introduction

This potential solution addresses KI#4.

### 6.2.2 Solution details

Authorization between NF Service Consumer and SCP, when sending the service request to SCP in delegated discovery, may be explicit by enhancing the CCA by inserting either the SCP Instance ID or the SCP Domain Info in CCA\_NFc, and therefore the NF Service Consumer can authorize SCP.

NOTE: Since in model D the NF Service Consumer is delegating the discovery, as well as access token request, service request and receiving service response to SCP, the NF Service Consumer authorizes the SCP to perform these actions on its behalf.

The SCP also generate its own enhanced CCA\_SCP including its Instance ID and/or its Domain Info and sends it along with access token request and the enhanced CCA\_NFc as received from NF Service Consumer.



Figure 6.2.2-1: Authorization of SCP by NFc in indirect communiation

NFc

SCP

NRF

1. Service Request (optionally includes enhanced CCA')

**\* CCA' additionally includes Authorized SCP ID**

2. Nnrf\_AccessToken\_Get\_Request (**includes CCA' and CCA,**

CCA contains the SCP Instance ID in the subject parameter)

3. NRF analyzes the request, and authorizes the SCP

4. Nnrf\_AccessToken\_Get Response

(access token)

The NRF verifies that the Target SCP Instance ID and/or SCP Domain info present in the CCA\_NFc matches the Instance ID/Domain Info of SCP as also being part of the subject of the CCA\_SCP. A successful verification of CCA(s) by NRF ensures that the SCP has been authorized by the NF Service Consumer.

Thus, the NRF needs to know the SCP Instance ID. One way for the NRF to learn the SCP instance ID is to use direct TLS between SCP and NRF, this requires SCP ID in the SCP TLS certificate which is currently not specified in TS 33.310. Another way for the NRF to learn the SCP instance ID is by CCA\_SCP.

If authentication was successful and the NF Service Consumer is authorized based on the NRF policy and the SCP requesting the access token has been explicitly authorized by NF Service Consumer, the NRF issues an access token.

A similar solution is also applicable for authorizing SCP by NFc to request a service and receive a response from NFp on its behalf. The NFp then may perform similar verification and, in case of successful verification, can send the service response to SCP.

However, even if the TLS certificate of the NFc would mandate the usage of NFc Instance ID, another problem still needs to be solved in case the SCP selects another SCP. This is because if the NRF or the NF Service Producer do not know the SCP domain, to which the SCP belongs to, the SCP\_CCA included by NFc does not help NRF. Thus, for this reason it is suggested that the TLS certificate needs in addition to SCP Instance Id also to hold the SCP domain identifier for allowing NRF to verify that NFc authorized one SCP of a SCP domain.

If the SCP, that NF Service Consumer delegated the authorization token request to, is not serving the NF Service Consumer request by itself, but demands another SCP' to do so, then the same procedure is needed between SCP and SCP'. Hence, SCP forward the service request to SCP' with its own CCA\_SCP including into it the SCP' ID.

Editor's Note: How the producer verifies the different CCAs is to be explained.

### 6.2.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

This solution fulfils requirement on KI#4. The SCP can be authorized to act on behalf of an NF Service Consumer and to request access tokens by NFc, because the NFc is including the SCP ID or SCP Domain ID into CCA\_NFc. With NFc providing the SCP ID in the CCA, authorization of that particular SCP is given, because NRF or NF Service Producer can with assurity verify that the SCP, which provides CCA\_NFc, is indeed the one SCP to which the NF Service Consumer sent its CCA and has authorized that SCP to request services and receive response on its behalf.

Thus, this solution counters a potential attack of SCP stealing a CCA and using it for requesting an access token without being requested by a NF Service Consumer.

Editor's Note: Impact of the solution on NFs, NRFs and SCPs is ffs.

## 6.3 Solution #3: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer

### 6.3.1 Introduction

This solution addresses Key Issue #4 "Authorization of SCP to act on behalf of an NF or another SCP". It explains how token-based authorization and CCAs as currently specified in TS 33.501 [2] can be used to authorize the SCP to act on behalf of an NF Consumer, i.e. to request access tokens or services on behalf of the consumer.

### 6.3.2 Solution details

#### 6.3.2.1 Request of access token on behalf of the consumer

The SCP requests access tokens on behalf of the consumer in Scenario D (indirect communication with delegated discovery) and in Scenario C (indirect communication without delegated discovery) without mutual authentication between NF and NRF at the transport layer. The following procedure describes token requests for Scenario D, and particularly how CCAs are used to authorize the SCP to request access tokens on behalf of the NF Consumer. For Scenario C without mutual authentication between NF and NRF at the transport layer, the same principles hold.



Figure 6.3.2.1-1: Access token request of SCP on behalf of an NF Consumer

1. The NF Service Consumer sends a service request to the SCP. The consumer includes a CCA signed by the consumer. The CCA includes the NF Instance ID of the consumer. The consumer's certificate used for signing the CCA also contains the consumer's NF Instance ID.

2. The SCP sends an access token request to the NRF. The SCP includes the CCA received by the consumer in step 1.

3. The NRF verifies the CCA as described in clause 13.3.8.3 of TS 33.501 [2] and thus obtains the NF Instance ID of the consumer that signed the CCA. Besides authentication of the consumer, the CCA also implicitly authorizes the SCP to act on behalf of the NF Service Consumer.   
  
The NRF authorizes the NF Service Consumer as described in TS 33.501 [2].

4.-8. The remaining steps of the access token request and service request procedure are exactly as described in TS 33.501 [2].

### 6.3.3 Evaluation

The solution addresses the threats and requirements of Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP.

The solution relies on token-based authorization and CCAs as currently specified in TS 33.501 [2].

It proposes that authorization of the SCP by the CCA is implicit by sending the CCA to the SCP, i.e. by presenting the CCA\_NFc received by the NF Service Consumer, the SCP shows it is authorized to act on behalf of the Consumer and to request access tokens on behalf of it. However, authorization is not explicitly stated in the CCA. Hence an entity that is not authorized by the NF Service Consumer but somehow has obtained a valid CCA signed by the consumer could use it to request access tokens on behalf of the consumer. Thus, in this case the NRF or the NFp can provide the service response to an unauthorized consumer.

## 6.4 Solution #4: Service request authenticity verification in indirect communication

### 6.4.1 Introduction

This solution addresses the KI#5.

### 6.4.2 Solution details

This solution allows the NF Service Producer to verify that a service request of the NF Service Consumer received via SCP has not been modified.

In case of CCA is used for authentication, the service request received by NRF or NF Service Producer can be verified as the one to be originally sent by the NF Service Consumer. This would guarantee that in indirect communication no intermediary can modify the service request unrecognized.

Editor's Note: Backwards compatibility with Rel-16 NF producers supporting only existing CCA is ffs.

For this, the CCA is enhanced with a new payload value for 'service request verification' and a protected header list.

- The 'service request verification' (SRV) includes the service request message (or a hash of it) as one of the payload values.

Editor's Note: If not the hash but the whole message or headers is included, impact on throughput needs to be considered and is ffs.

Editor's note: It is ffs how the SCP can perform necessary message modifications, if the (hash of the) whole service request is included in CCA.

- The protected header list (HL) includes custom headers that shall be integrity protected and thus not be modifiable undetected by SCP.

If present, the NF Service Producer or the NRF can verify whether these data included in the CCA are matching the service request as sent by the NF Service Consumer. I.e. the NF Service Producer verifies that the data included in the payload is matching the service request received together with the CCA. The receiver also verifies that the headers in the protected header list are not modified.

Since CCA is digitally signed by the NF Service Consumer, thus the recipient can verify that the service request received from SCP is the original one as provided by the NF Service Consumer. The additional SRV payload provides authenticity of the service request.

NOTE: This solution assumes that an SCP does not need to modify service request details for providing its service of delegated discovery and access token request to NRF or transferring a service request to the NF Service Producer. If there are headers that need to be modified by SCP/Proxy, then those headers cannot be considered as payload of SRV. The NF Service Consumer provides in this case a separate list of headers (HL) to explicitly state what is covered under SRV. The destination endpoint (NRF or NF) can take them in consideration while verifying the received data.

In detail:

- NF Service Consumer creates a service request and creates a keyed hash value about those parts of the service request, that are not to be modifiable by the SCP, and generates CCA including a 'service request verification' (SRV) payload with the keyed hash value. If necessary, a protected HL is included.

Editor's Note: CT4 feedback is needed on which headers are not subject to modification, mediation, or alteration by the SCP and can be delivered as is to the other far end of the indirect communication.

Editor's Note: It is ffs if a keyed hash is necessary and if yes how the key is obtained or derived.

- NRF, after verifying the authenticity of NF Service Consumer by checking the CCA, it checks SRV, i.e. it verifies the authenticity of the service request by creating a hash of the service request and comparing it with the received SRV value. It also verifies that the headers in the protected HL are not modified.

- NF Service Producer, after receiving an access token and CCA/SRV from the SCP, it verifies the NF Service Consumer by checking the CCA, it checks whether the NF instance id for which the access token was provided, matches the identity in CCA and it verifies the authenticity of the service request by creating a hash of the service request and comparing it with the received SRV value. It also verifies that the headers in the protected HL are not modified.

### 6.4.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

## 6.5 Solution #5: End-to-end integrity protection of HTTP body and method

### 6.5.1 Introduction

This solution addresses the key issue #5 (End-to-end integrity protection of HTTP messages).

The core steps of this solution are:

- Use Client credentials assertions (CCAs) based authentication as specified in TS 33.501 [2] Clause 13.3.8 for NF-NRF or/and NF-NF communication.

- Enhance the Client credentials assertions (CCAs) to include a hash of the HTTP body and HTTP method to protect the message itself.

- The receiving node (NRF or NF producer) computes the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertions (CCAs).

Editor's Note: Backwards compatibility with Rel-16 NF producers supporting only existing CCA is ffs.

Editor's Note: This solution has dependency on CT4 feedback on what SCP exactly needs to modify.

### 6.5.2 Solution details



Figure 6.5.2-1 CCA based Authentication with HTTP hash enhancement

1. NF service consumer sends a service request including a signed Client credentials assertion (CCA) token to authenticate against NF service producer or NRF as described in TS 33.501 [2] Clause 13.3.8. But for this solution it is also proposed to add an optional field in CCA to protect the part of the message itself. The added field is a hash of HTTP body and HTTP method.

2. NF service producer or NRF validates the CCA as described in 3GPP 33.501 Clause 13.3.8.3. But since one optional field is supposed to be added to the CCA, the receiving end point (NF service producer or NRF) also needs to compute the hash of the HTTP body and HTTP method and validates that it is identical to the hash received in the Client credentials assertion.

The details of the hash are proposed to be specified as following:

For computation of the hash of the HTTP body and HTTP method for inclusion into the Client credential assertion, the input S to the KDF specified in Annex B of 3GPP TS 33.220 [4] is computed as follows:

- P0 = HTTP body;

- L0 = length of the HTTP body;

- P1 = HTTP method;

- L1 = length of HTTP method.

The input key KEY is equal to null. Note that the FC value will be allocated in the normative phase.

### 6.5.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

## 6.6 Solution #6: Verification of Service Response from a NF Service Producer at the expected NF Set

### 6.6.1 Introduction

This solution addresses key issue #1. In order to verify the message from NF Service Producer in indirect communication, it is proposed to append CCA of NFp. And NF Servcie Consumer may accept the certificate if it is verified well and NF Service Producer instances belongs to the expected NF Producer instance(s).

### 6.6.2 Solution details

When a NF Service Consumer discover a NF Servcie Producer for a service, NRF provides information of target NF set and candidate target NF instance IDs belonging to the target NF set.

The NF set information in the discovery response from NRF to NF consumer needs to be end to end integrity protected, by e.g. TLS or solution to Key Issue #5, so that the SCP cannot modify the NF set information in the discovery response.

Among the candidates NF instances list, the NF Service Consumer may select an NF instance for a Service Request. And the NF Service Consumer keep the list of candidate NF instances and NF set for verification of expected Service Response.

After acquiring an access token from the NRF, a NF Service Consumer may send a Service Request to the SCP. The service request includes the access token and CCA of the NF Service Consumer.

The service request includes the 3gpp-Sbi-Routing-Binding header and/or 3gpp-Sbi-Discovery header in order to specify target NF Service Producer and/or target NF Set, so that the SCP is instructed to perform the NFp reselection within the scope of NF Set.

An SCP forward a Service Request to the NF Service Producer. If needed, the SCP may reselect another NF Service Producer belonging to the same NF set.

Editor's Note: It is FFS how the solution may work with delegated discovery.

After receiving a Service Request, the NF Service Producer may verify the Service Request and may respond with a Service Response with CCA of the NF Service Producer. CCA of NF Service Producer includes NF instance ID of NF Service Producer and NF instance ID of NF Service Consumer.

When receiving a Service Response, the NF Service Consumer may verify whether the NF instances ID of NF Service Producer which sends the Service Response is in the list of candidate NF instances for the Service Request.

### 6.6.3 Evaluation

TBD

## 6.7 Solution #7: Access token request for NF Set

Editor’s Note: It is ffs whether using the same access token for different OAuth 2.0 clients follows the OAuth 2.0 RFC and best practices.

Editor's Note: How does the NRF/NFp verify the correctness of NFc set ID is ffs.

### 6.7.1 Introduction

This solution addresses KI#6.

SBA introduces the concepts of NF Set and NF Service Set. 5G SBA architecture design allows for the concept of stateless NFs. To avoid that a NF from a NF Set needs to request a new access token, when targeting a service of an existing resource requested before by another NF of the NF Set, it is proposed that any NF in a NF Set can request an access token for the NF Set. Thus, any NF Service Consumer targetting a service of an existing resource it can use the access token provided to a NF Set of NF Service Consumers.

### 6.7.2 Solution details

The NF Service Consumer belonging to a NF Set includes its NF Set ID in the Access Token Request message to NRF.

When the Access Token Request is processed by the NRF and a NF Set ID is included, the NRF knows that the NF Service Consumer requests an access token to be usuable by all NF Service Consumer instances within the NF Set. If NRF authorization of the NF Service Consumer is successful, NRF includes as claim the NF Set ID of the expected NF Service Consumer instances to allow the access token generated for usage by all NF Service Consumers in the NF Set. NRF sends the access token back to the requester.



Figure 1 – Access Token Request procedure (TS 33.501 Figure 13.4.1.1.1-1) enhanced with NF Set ID in the Access Token Request message

When a service is requested, the requester (NF Service Consumer or SCP) includes the NF Set ID of the NF Service Consumer in the Service API Request, in addition to the access token obtained from the NRF.

The NF Service Producer checks whether the Consumer NF Set Id in the Service Request matches with the NF Set ID claim in the Access token. If yes, it proceeds with serving the request, otherwise it rejects the request.

### 6.7.3 Evaluation

TBD

## 6.Y Solution #Y: <distinct solution name>

### 6.Y.1 Introduction

Editor's Note: Motivate how the potential security requirements of one or several key issues are addressed by this solution proposal.

### 6.Y.2 Solution details

TBD

### 6.Y.3 Evaluation

Editor's Note: Provide an analysis of the risks of threats mitigated by this solution. Provide a statement on complexity/impact/backward compatibility if one would follow this solution.

# 7 Conclusions

Editor's Note: The purpose of this TR is to make conscious decisions whether 5G SBA security needs to be enhanced to address specific threats and to which price (complexity versus security gain) this is possible. The clause will provide conclusive statements per key issue, i.e. whether and how to move forward with normative work and, if yes, which solutions are endorsed.

## 7.X <distinct KI name>

TBD

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-01 | SA3#102-e | S3-210420 |  |  |  | Skeleton of TR eSBA SEC | 0.0.0 |
| 2021-01 | SA3#102-e | S3-210679 |  |  |  | |  |  | | --- | --- | | S3-210562 | Introduction | | S3-210422 | Scope | | S3-210564 | Authentication of NRF and NFp in indirect communication | | S3-210565 | SCP deployment models | | S3-210653 | KI on Verification of UE in subscription and notification in the delegated “Subscribe-Notify” scenarios | | S3-210566 | KI on Dynamic authorization between SCPs or NF and SCP | | S3-210567 | End-to-End Critical HTTP headers and body parts integrity protection | | 0.1.0 |
| 2021-03 | SA3#102bis-e | S3-211344 |  |  |  | |  |  | | --- | --- | | S3-211224 | Rapporteurs update to 33.875 | | S3-211217 | Service response verification in indirect communication | | S3-211218 | More details on SCP deployment models | | S3-211046 | New Solution to KI#4: Using existing procedures for authorization of SCP to act on behalf of an NF Consumer | | S3-211220 | NF-SCP authorization | | S3-211221 | KI details added to End-to-end integrity protection of HTTP messages | | S3-211205 | New Solution to KI#5: End-to-end integrity protection of HTTP body and method | | S3-211223 | Service request authenticity verification in indirect communication | | S3-211225 | Mapping of solutions to key issues | | Rapporteur additional work done | Updating references, heading numbers and mapping tables in line with TR implementation, updating adding missing ed notes in TBD/empty clauses | | 0.2.0 |
| 2021-05 | SA3#103-e | S3-212297 |  |  |  | |  |  | | --- | --- | | S3-212292 | New solution for key issue#1: Authentication of NF service producer in indirect communication | | S3-212298 | Sol1 deployment scenarios | | S3-212299 | ENs on Sol1 Service response verification in model C | | S3-212300 | EN resolution on sol 2 - NFc authorizing SCP to act on its behalf | | S3-212301 | Evaluation on sol 2 - NFc authorizing SCP to act on its behalf | | S3-211973 | KI on Access token usage by all NFs of an NF Set | | S3-212394 | Solution on Access token request for NF Set | | S3-212303 | Trust model | | S3-212372 | Evaluation of Solution #3 "Using existing procedures for authorization of SCP to act on behalf of an NF Consumer" | | 0.3.0 |