|  |
| --- |
| 3GPP TR 33.875 V0.2.0 (2021-03) |
| 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Trust model 7

5 Key issues 7

5.1 Key issue #1: Authentication of NRF and NF Service Producer in indirect communication 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key issue #2: SCP security domains 7

5.2.1 Key issue details 7

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.3 Key Issue #3: Service access authorization in the "Subscribe-Notify" scenarios 8

5.3.1 Key issue details 8

5.3.2 Security threats 9

5.3.3 Potential security requirements 9

5.4 Key issue #4: Authorization of SCP to act on behalf of an NF or another SCP 9

5.4.1 Key issue details 9

5.4.2 Security threats 9

5.4.3 Potential security requirements 9

5.5 Key issue #5: End-to-end integrity protection of HTTP messages 9

5.5.1 Key issue details 9

5.5.2 Security threats 9

5.5.3 Potential security requirements 10

5.X Key issue #X: <distinct KI name> 10

5.X.1 Key issue details 10

5.X.2 Security threats 10

5.X.3 Potential security requirements 10

6 Solutions 10

6.Y Solution #Y: <distinct solution name> 10

6.Y.1 Introduction 10

6.Y.2 Solution details 10

6.Y.3 Evaluation 10

7 Conclusions 10

7.X <distinct KI name> 11

Annex A (informative): Change history 12

# 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

Editor’s note: which entities operate which functions (or proxies, for that matter)

# 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.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 |  |  |  |
| #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 |  |  |  |
|  |  |  |  |  |  |  |  |  |

## 6.1 Solution #1: Service response verification in indirect communication without delegated discovery

### 6.1.1 Introduction

This solution is addressing KI#1.

A malicious SCP or a Man in the Middle (MitM) could forward the service request to a malicious or unauthorized NF Service Producer. 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.

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.

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

This solution allows the NF Service Consumer (NFc) to verify the genuineness of the NF Service Producer (NFp) or the NRF which is sending the response, when an SCP is used in indirect communication scenario and does not perform re-selection and the discovery of NFp is not delegated to the SCP (see 3GPP TS 33.501 [X] Annex R, model C).

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. NFc can now validate the identity of NFp, even though the response is sent via SCP. 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.

Editor's Note: It is ffs whether a match of the NFp ID between access token and CCA\_NPp provides validation of the identity of the NFp or authentication of the NFp

Thus, if the NFp includes its own CCA\_NFp in the service response, NFc can verify that the service response received from the specific NFp was requested in the original service request from this producer.

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. In case of failure, error messages can be triggered and reported to the operator.

Editor's Note: Flow chart with step by step description to be added.

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.

Editor's Note: It is ffs whether the CCA\_SCP is necessary if there is a direct TLS connection between SCP and NRF.

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.

Editor's Note: It is ffs whether the consumer can authorize the SCP if there is more than one SCP between the consumer and the producer.

### 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.

## 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

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.

## 6.4 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.X.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.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 |