**3GPP TSG-SA3 Meeting #102Bis-e *draft\_S3-211156-r2***

**e-meeting, 1 - 5 March 2021** Revision of S3-20xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title: Rapporteur updates to 33875-101**

**Document for: Approval, Information, Discussion**

**Agenda Item: 2.20**

|  |
| --- |
| 3GPP TR 33.875 V0.1.0 (2021-01) |
| 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".

[X] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".

# 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 [X] 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.

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.

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

TBD

###  5.2.3 Potential security requirements

TBD

## 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.

### 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.

## 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.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 |