|  |
| --- |
| 3GPP TR 33.894 V0.3.0 (2022-10) |
| Technical Specification|Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on applicability of the Zero Trust Security principles in mobile networks(Release 18) |
|   |
|  |  |
|  |
| 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 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Architectural and security assumptions 8

5 Evaluation of the current security mechanisms 8

5.Y Tenet #1: Resources 8

5.Y.1 Description 8

5.Y.2 Relevant security mechanisms 8

5.Y.3 Evaluation 8

5.Y Tenet #2: All communication is secured regardless of network location 8

5.Y.1 Description 8

5.Y.2 Relevant security mechanisms 9

5.Y.3 Evaluation 9

5.Y Tenet #3: Access granularity 9

5.Y.1 Description 9

5.Y.2 Relevant security mechanisms 9

5.Y.3 Evaluation 9

5.Y Tenet #5: Security posture 10

5.Y.1 Description 10

5.Y.2 Relevant security mechanisms 10

5.Y.3 Evaluation 10

5.Y Tenet #6: Access security 10

5.Y.1 Description 10

5.Y.2 Relevant security mechanisms 11

5.Y.3 Evaluation 11

5.Y Tenet #7: Data collection to improve security posture 11

5.Y.1 Description 11

5.Y.2 Relevant security mechanisms 11

5.Y.3 Evaluation 12

5.Y Tenet #Y: <Tenet Name> 12

5.Y.1 Description 12

5.Y.2 Relevant security mechanisms 12

5.Y.3 Evaluation 12

5.Z Tenet Evaluation summary 12

6 Key issues 13

6.X Key Issue #1: Need for continuous security monitoring 13

6.X.1 Key issue details 13

6.X.2 Security threats 13

6.X.3 Potential security requirements 13

6.X Key Issue #X: <Key Issue Name> 13

6.X.1 Key issue details 13

6.X.2 Security threats 13

6.X.3 Potential security requirements 13

7 Solutions 14

7.Y Solution #Y: <Solution Name> 14

7.Y.1 Introduction 14

7.Y.2 Solution details 14

7.Y.3 Evaluation 14

8 Conclusions 14

Annex A (informative): Change history 15

# 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

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The present document studies some Zero Trust Security principles that can be applied to the 5G System core network. The document will further analyse potential threats, study necessary security enhancements, and document various decisions related to solutions as to be adopted or not adopted after evaluating the associated risks and the complexity. The document specifically covers the following aspects.

* Analyse the 3GPP 5GS security scenarios related to the 5G core network that may benefit from a Zero Trust principle and identify the associated threats.
* Analyse the suitable Zero Trust security mechanisms (i.e., for enabling trust evaluation and ensuring trust) to address the threats identified where potential security risk exists.
* Provide recommendations for support of additional Zero Trust principles in 5GS security architecture with suitable future normative work directions, where such recommendations may include 3GPP 5G security requirements, technical enhancements, and procedural enhancements.

# 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] NIST Special Publication 800-207 Zero Trust Architecture.

[3] 3GPP TR 33.738: "Study on security aspects of enablers for network automation for the 5G system Phase 3".

# 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].

**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> <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> <Expansion>

# 4 Architectural and security assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Evaluation of the current security mechanisms

Editor's Note: This clause contains an evaluation of the current security mechanisms with respect to the zero trust security tenets described in [2].

## 5.Y Tenet #1: Resources

### 5.Y.1 Description

According to Tenet 1 in [2], it is expected that a zero trust architecture adheres to the principle that "all data sources and computing resources are considered resources".

Identifying resources, and hence what needs protection in an enterprise would be one of the most important steps in a zero trust plan. In this regard, Tenet 1 provides a definition for what is to be considered as a resource. In the context of the 5G Core any NF and their services are resources.

### 5.Y.2 Relevant security mechanisms

This tenet provides a definition for what needs protection in an enterprise network and serves rather as deployment guidance than a technical requirement. Therefore, this clause is not applicable for this tenet.

### 5.Y.3 Evaluation

Any Network Functions and their services in the 5G Core are to be considered as a resource in the context of a zero trust deployment plan.

Besides that, no additional security requirement related to 5G Core are needed for Tenet 1.

## 5.Y Tenet #2: All communication is secured regardless of network location

### 5.Y.1 Description

According to the NIST tenet 2 in [2], ‘*Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other nonenterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.*’.

The relevant principle for 5GS core network is that, all communications should be done in the most secure manner available, such as with confidentiality, integrity, and source authentication (as applicable). That implies there is default trust inside a secure domain. As a result, except supporting secure communications, other aspects mentioned in the tenet-2 is not applicable to the telecommunications network.

### 5.Y.2 Relevant security mechanisms

All the security mechanisms specified in TS 33.501 [b] pertaining to SBA communication such as in clause 13.1 as well as non-service based interfaces involving an entity in the 5G Core network such as clause 9, 12, etc.

### 5.Y.3 Evaluation

In general, the tenet is about communication security. From this perspective, the 5G Core security standards provide two means to protect communication in and with the 5G Core. On the network layer, there is the NDS/IP framework, relying on IPsec, specified in TS 33.210 [a]. On the transport layer there is TLS for which the profile is also captured in TS 33.210 [a]. Both security protocols provide integrity, confidentiality and replay protection. NDS/IP is applicable to all interfaces involving the 5G Core since they are all IP based. TLS is on the other hand applicable to all service-based ones since they are HTTP based. IPsec has the advantage of providing topology hiding but TLS whenever applicable can alleviate the dependency on perimeter security should the IPsec tunnel be terminated at the perimeter. With TLS the operator can further push the protection end points deeper within the perimeter.

Based on this analysis, no further actions are needed with respect to this tenet since the 5G Core standards provide the necessary means to secure the communication with and within the 5G Core and also independently of the location of the end points.

Except supporting secure communications, other aspects mentioned in the tenet-2 is not applicable to the telecommunications network.

## 5.Y Tenet #3: Access granularity

### 5.Y.1 Description

According to tenet 3 of [2], a zero trust architecture has to adhere to the principle that "Access to individual enterprise resources is granted on a per-session basis". This tenet is about access authorization to resources.

### 5.Y.2 Relevant security mechanisms

All the security mechanisms specified in TS 33.501 [a] related to SBA security.

### 5.Y.3 Evaluation

Authorization is one of the most important mechanism for protecting enterprise resources. From this aspect, 5GC indeed provides the necessary authorization and authentication mechanisms for NF to be deployed in the operator network.

In the 5GC, one can assimilate the notion of session from [2] to the TLS session, considering that TLS is used for the SBI interface protection as defined in TS 33.501 [a]. In fact, NF consumers and producers are first required to mutually authenticate during the TLS session establishment via certificates. Then the NF consumer may be required to present an OAuth2.0 authorization token to the producer in the service request within the TLS tunnel. These two mechanisms provide the necessary tools for an operator to control authorization at almost a service invocation level. In facts, via the claims in the OAuth tokens, an operator can restrict access to single instances, to particular services, to particular type of producers, to indicate the restrictions for different resoures in 5GC NFs, etc. In addition, via the optional "additional scope", the operator can further restrict the allowed resources and the allowed actions. This means that besides the per-TLS session authorization, 5GC core network provides much concrete granularity on the authorization based on the OAuth 2.0 mechanism.

However, the usage of such security mechanisms is left to the discretion of the operator and will depend on the deployment context. Nevertheless, based on the current standards, the operator of a 5G Core has the means to impose very granular and tight restrictions for access to resources. Therefore, no further actions from standard perspective are identified for this tenet.

## 5.Y Tenet #5: Security posture

### 5.Y.1 Description

According to tenet 5 in [2], "The enterprise monitors and measures the integrity and security posture of all owned and associated assets".

Editor's Note: description is FFS

### 5.Y.2 Relevant security mechanisms

The mechanisms specified in TS 23.288 [a] pertaining to data collection from NFs, e.g. clause 6.2.2 and analytics, e.g. clause 6.7.

### 5.Y.3 Evaluation

In general, the tenet touches upon two aspects. The first one is related to operation security. In this regard, it is expected that the proper security practices and guidelines are followed during deployment and operations in order to detect and mitigate vulnerabilities. This includes as described in [2] regular updates, security patches, and mitigation plans should there be a breach, etc. The enforcement of such practices depends heavily on the implementation and deployment context, e.g. infrastructure, enterprise network, etc. Therefore, it does not warrant the development of standard solutions. Nevertheless, it is worth mentioning that the 3GPP security standards in general are continuously evolving. In fact, vulnerabilities in the security mechanisms revealed either by individual 3GPP members or through one of the established CVD programs are always discussed and remediated whenever deemed necessary.

Editor's Note: Evaluation of the second aspect related to monitoring and measuring, required to evaluate the security posture of assets, is FFS.

## 5.Y Tenet #6: Access security

### 5.Y.1 Description

According to tenet 6 of [2], a zero trust architecture has to adhere to the principle that "All resource authentication and authorization are dynamic and strictly enforced before access is allowed". In the 5G Core context, this tenet also relates to how the access by service consumers to the services of producers is secured.

Editor's Note: How to map the aspects below on user access to the 5GC is FFS

Further in general the actual tenet 6 description in [2] states, *“This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.”*.[2]

The relevant principle for the 5GS core network is that, for access to network resources such as network services and data, the access control/management should consider the threat assessment and continuous trust (re-) evaluation results inaddition to the identity, and credentials-based authentication. Further based on policy defined and enforced (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) continual monitoring with possible re-authentication and re-authorization can be considered.

### 5.Y.2 Relevant security mechanisms

The current security mechanisms

All the security mechanisms specified in TS 33.501 [a] related to SBA security, in particular clauses 13.3 and 13.4 on authentication and authorization.

### 5.Y.3 Evaluation

According to the current security mechanisms, NF consumers and producers may be first required to mutually authenticate during the TLS session establishment via certificates. Then the NF consumer may be required to present an OAuth2.0 authorization token to the producer in the service request within the TLS tunnel. These two mechanisms provide the necessary tools for an operator to control access to the service producer resources dynamically at almost a service invocation level.

The choice of the security mechanisms including the static authorization is left to the discretion of the operator and will depend on the deployment context. Nevertheless, based on the current standards, the operator of a 5G Core has the means to enforce a dynamic access authorization in the sense of this tenet by the specified OAuth2.0 mechanism.

Editor's Note: further evaluation is FFS

## 5.Y Tenet #7: Data collection to improve security posture

### 5.Y.1 Description

According to tenet 7 titled, ‘The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture’ in [2] describes that, *“An enterprise should collect data about asset security posture,* *network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects (see Section 3.3.1).”*.

Security posture data collected from the network should be used for periodic review and improvement of an applied Zero Trust Architecture’s policies. These improvements include the creation of new policies and enforcement of existing policies.

### 5.Y.2 Relevant security mechanisms

There are currently no standard procedures for data collection to improve overall core network security posture.

### 5.Y.3 Evaluation

Tenet 7 is an overall directive to network operators to:

- facilitate data collection related to security posture, control plane network traffic (i.e., message exchanges between NFs) and access requests,

- processing of data (based on operator specific implementation), and

- use any insight gained to improve policy creation and enforcement (based on operator policies) in the 5GC.

Editor's Note: The rest of the evaluation is FFS.

## 5.Y Tenet #Y: <Tenet Name>

Editor's Note: This is the template for zero trust tenet analysis and for the evaluation of the relevant security mechanisms if any. This template is to be removed before the TR is sent for approval.

### 5.Y.1 Description

Editor's Note: This clause gives a short description of the tenet, any necessary details to put into the 5G System context and its relevance.

### 5.Y.2 Relevant security mechanisms

Editor's Note: This clause lists the relevant specified security mechanisms if any.

### 5.Y.3 Evaluation

Editor's Note: This clause gives an analysis and a stand point on the sufficiency of the relevant security mechanisms and identifies any potential gaps that would require a more thorough study.

## 5.Z Tenet Evaluation summary

Based on the evaluation discussed in Clause 5.Z related to the zero trust tenets and the current security mechanisms, an overview of the tenets whose applicability needs additional work in 5GS is presented in the following Table 5.Z-1.

Table 5.Z-1: Overall Tenet Evaluation Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Tenet No.** | **Short description** | **Supported/Not Supported** (by the current security mechanism related to the core network) | **Additional work needed (or) not** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
| 6 |  |  |  |
| 7 |  |  |  |

# 6 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 6.X Key Issue #1: Need for continuous security monitoring

### 6.X.1 Key issue details

The 5G system includes heterogeneous and varied network functions (NF) deployments, where the current security mechanisms determine service access among NFs by authentication (i.e., identifier and credentials based) and authorization. If any NF runs into errors (e.g., due to configuration issues) or behaves maliciously (e.g., due to insider threats/privilege misuse or cyber-attacks), then such NF behaviour information or related threat assessments will not be considered in the current security mechanisms (e.g., for any service access). Some of the zero trust tenets [2] (i.e, tenets 5,7) provides motivation that resource access (i.e., access control to network services) can be evaluated while also taking into account the dynamic policy(ies) that are defined and enforced related to security monitoring (i.e., threat assessments) and continuous trust evaluation, for example., according to [2] evaluation factor(s) may include observable state of the requestor, characteristics, behavioural attributes (e.g., subject analytics, measured deviations from the observed usage patterns), environmental attributes (location, time, reported attacks), security posture etc.

To achieve zero trust, the operator network (as in tenet 7) must gather as much data as possible about the state of the network function/application function, such as security posture, access request(s), communication, etc., process that data, and use any insights gained to improve policy creation and enforcement (e.g., to improve security posture).

No specification in 5GS guides continuous security monitoring and trust evaluation while considering the historical statistics, malicious behaviours, security posture, and risk factors. As a result, the solutions addressing this key issue can identify various NF/AF relevant factors for data collection to enable security monitoring and continual trust evaluation. Furthermore, findings of the security monitoring and continuous trust evaluation results (i.e., insights) may be used in the core network to propose and implement necessary security controls depending on the Operator's policies. The solution(s), where relevant, can consider the work being carried out in TR 33.738 [3] (e.g., anomalous NF behaviour detection, cyber-attack detection etc.,) to enable continuous security monitoring and trust evaluation accordingly.

Editor’s Note: Key Issue details is FFS.

### 6.X.2 Security threats

Editor’s Note: The threat is FFS.

### 6.X.3 Potential security requirements

Editor’s Note: The security requirement is FFS.

## 6.X Key Issue #X: <Key Issue Name>

### 6.X.1 Key issue details

### 6.X.2 Security threats

### 6.X.3 Potential security requirements

# 7 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 7.Y Solution #Y: <Solution Name>

### 7.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 7.Y.2 Solution details

### 7.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 8 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107e Adhoc | S3-221691 |  |  |  | Approved Skeleton (S3-221520) and Scope (S3-221588).  | 0.1.0 |
| 2022-08 | SA3#108-e | S3-222423 |  |  |  | Addition of tenet evaluation clause ([S3-222057](https://apc01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.3gpp.org%2Fftp%2FTSG_SA%2FWG3_Security%2FTSGS3_108e%2FDocs%2FS3-222057.zip&data=05%7C01%7Csmary%40LENOVO.COM%7C193a24bb76134356318008da875dc98f%7C5c7d0b28bdf8410caa934df372b16203%7C0%7C0%7C637971134133650941%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=s9e6chkMyfSi5BW0IzzgVIp2XBjp6WS6x3ncX4MIWS8%3D&reserved=0)). | 0.2.0 |
| 2022-10 | SA3#108adhoc-e | S3-223121 |  |  |  | Incorporated changes from S3-223075, S3-222992, S3-223076, S3-223077, S3-223078, S3-223079, S3-222994, S3-222999. | 0.3.0 |