|  |
| --- |
| 3GPP TR 33.894 V0.8.0 (2023-08) |
| 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 16Intpp.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

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 8

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

5 Evaluation of the current security mechanisms 8

5.1 Tenet Evaluation Details 8

5.1.1 Tenet #1: Resources 8

5.1.1.1 Description 8

5.1.1.2 Relevant security mechanisms 8

5.1.1.3 Evaluation 8

5.1.2 Tenet #2: All communication is secured regardless of network location 9

5.1.2.1 Description 9

5.1.2.2 Relevant security mechanisms 9

5.1.2.3 Evaluation 9

5.1.3 Tenet #3: Access granularity 9

5.1.3.1 Description 9

5.1.3.2 Relevant security mechanisms 9

5.1.3.3 Evaluation 9

5.1.4 Tenet #4: Resource access 10

5.1.4.1 Description 10

5.1.4.2 Relevant security mechanisms 10

5.1.4.3 Evaluation 10

5.1.4 Tenet #5: Maintain the integrity and security posture of all owned and associated assets 10

5.1.4.1 Description 10

5.1.4.2 Relevant security mechanisms 11

5.1.4.3 Evaluation 11

5.1.5 Tenet #6: Access security 12

5.1.5.1 Description 12

5.1.5.2 Relevant security mechanisms 12

5.1.5.3 Evaluation 12

5.1.6 Tenet #7: Data collection to improve security posture 12

5.1.6.1 Description 12

5.1.6.2 Relevant security mechanisms 12

5.1.6.3 Evaluation 13

5.2 Security Mechanism Evaluation summary 13

6 Key issues 15

6.1 Key Issue #1: Need for continuous security monitoring 15

6.1.1 Key issue details 15

6.1.2 Security threats 16

6.1.3 Potential security requirements 16

7 Solutions 16

7.1 Solution #1: Data Collection to enable security monitoring for the Core Network 16

7.1.1 Introduction 16

7.1.2 Solution details 16

7.1.3 Evaluation 17

8 Conclusions 18

Key Issue #1 Conclusion 18

Annex A (informative): Change history 19

# 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.

# 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".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[6] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[7] 3GPP TS 29.520: "5G System; Network Data Analytics Services; Stage 3".

[8] NIST Special Publication 800-92 Guide to Computer Security Log Management.

[9] 3GPP TS 23.502 : "Procedures for the 5G System (5GS)".

# 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 TS 33.501 [4] apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and TS 33.501 [4] 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].

# 5 Evaluation of the current security mechanisms

## 5.1 Tenet Evaluation Details

### 5.1.1 Tenet #1: Resources

#### 5.1.1.1 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.

#### 5.1.1.2 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.

#### 5.1.1.3 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.

### 5.1.2 Tenet #2: All communication is secured regardless of network location

#### 5.1.2.1 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.

#### 5.1.2.2 Relevant security mechanisms

All the security mechanisms specified in TS 33.501 [4] 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.

#### 5.1.2.3 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 [5]. On the transport layer there is TLS for which the profile is also captured in TS 33.210 [5]. 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.

### 5.1.3 Tenet #3: Access granularity

#### 5.1.3.1 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.

#### 5.1.3.2 Relevant security mechanisms

All the security mechanisms specified in TS 33.501 [4] related to SBA security.

#### 5.1.3.3 Evaluation

Authorization is one of the most important mechanisms 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 [4]. 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 resources 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.

### 5.1.4 Tenet #4: Resource access

#### 5.1.4.1 Description

According to tenet 4 of [2], a zero trust architecture has to adhere to the principle that "Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes… Environmental attributes may include such factors as requestor network location, time, reported active attacks, etc.".

The tenet in [2] describes the access to resources by clients which is related to a user or service, but the user (being part of UE) is not in the scope of this study. Nevertheless, without fully assimilating NFs to users, one can evaluate this tenet from the perspective of NFs being clients when acting as service consumers in the 5G Core.

#### 5.1.4.2 Relevant security mechanisms

The dynamic authorization mechanism based on OAuth2.0 specified in clause 13.4 of TS 33.501 [4].

#### 5.1.4.3 Evaluation

Before accessing services, an NF consumer may be required to obtain and present an OAuth2.0 token as specified in TS 33.501 [4]. But the existing Oauth based access control decisions do not consider the factors e.g., related to behavioural aspects/reported attack. The specified requirements include detailed provisions for the usage of the claims. In particular, the scope claims, the optional "additional scope", the NF set ID, and slice information provide the necessary flexibility to the operators to authorize access at the desired granularity level. For example, the claims can be changed to restrict the access to single instances, to particular services, to particular type of producers, or even to restrict the allowed actions depending on the operator’s policy. Observe that such restrictions or expansions of the scopes do not have to be static and can be changed dynamically even at every service invocation.

Document [2] goes to a great extent into describing the use of "behavioral attributes" as input to the access authorization process. On this particular aspect, the current security standards do not take into account this so far and do not provide any mechanisms for the definition and the collection of such attributes for NFs. Nevertheless, should there be any useful information collected from NFs for access authorization purposes, the same information would be also equally relevant in a security monitoring context. This is covered under the evaluation of Tenet 5 in clause 5.4.

### 5.1.4 Tenet #5: Maintain the integrity and security posture of all owned and associated assets

#### 5.1.4.1 Description

According to tenet 5 in [2], "The enterprise monitors and measures the integrity and security posture of all owned and associated assets".Further description in [2] shows that this tenet majorly covers operational security and evaluation of the asset’s security posture during evaluation of resource request. The tenet focuses on the posture of all resources and devices. In the context of this study, resources and devices can be assimilated to 5G System consisting of RAN, Core and UEs, whereas the RAN and UE being out of scope. In general, for 5G System entities the tenet recommends processes in place in order to ensure that the security best practices and guidelines are followed as well as a robust security monitoring and reporting solution in place.

All the associated assets connected to the network infrastructure are continuously monitored to ensure that they remain configured in a state that is known to be legitimate and secure. Therefore, the security challenge "Trust Nothing and Verify Everything" is considered.

In the 5G core network, this principle refers to the data that can be collected from the NFs that can be used to perform threat assessment as part of continuous security monitoring and trust evaluation.

#### 5.1.4.2 Relevant security mechanisms

The mechanisms specified in TS 23.288 [6] pertaining to data collection from NFs, e.g., clause 6.2.2 and analytics, e.g., clause 6.3 to 6.7.

There is currently no explicit standardized security monitoring within NWDAF or in other NF.

The NWDAF defined in 3GPP TS 29.520 [7] is used to preform network analytics on data collected from user equipment, network functions, and operations, administration, and maintenance (OAM) systems, etc.

Monitoring of the integrity and security posture of the 5G Core, that also take into account other factors of the infrastructure, already exists today in operators' network infrastructure. These monitoring systems are out of scope of the 3GPP specifications.

#### 5.1.4.3 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.

The second aspect is related to monitoring. In this regard, TS 23.288 [6] provides a framework for data collection services that can further enhance whatever security monitoring solution an operator has. For NF monitoring, the framework of [6] includes analytics for performance monitoring in clause 6.6 and load monitoring in clause 6.5. Such data could be used for example to evaluate the state of the NF and whether it is behaving normally. However, the framework in [6] relies on the NWDAF, a 5G Core NF, to leverage such services. From a higher-level perspective taking into account the enterprise as a whole with the 5G Core being one part of it, such relevant information exposed by the 5G Core NFs (if any) directly or indirectly via the NWDAF is very likely to be used by an entity outside the 5G Core itself. This could be the operator security monitoring solution or whatever current proprietary solutions being used to achieve the same goals. Overall, this does not warrant standardizing a 5G Core-specific security monitoring procedure.

NWDAF supports data collection and network monitoring for general aspects related to NF load, performance etc. However, the NWDAF is a Network Function in the 5G Service-Based Architecture itself. According to NIST SP 800-92 [8], sections 2.3.2 and 5.1.3, as well as similar guidance on security logs like, it is important to separate and isolate security logs, So, a security monitoring function can be outside the SBA and the security monitoring function itself would be mostly proprietary.

It is worth noticing that on the one hand, such information could include data like network traffic or logs that is not accessible at the SBA layer. This type of data is not specific to the 5G system itself and highly dependent on the deployment, e.g., platforms and technologies used. Therefore, for data collection and sharing, care must be taken in order to follow the security best practices such as the guidelines of NIST SP 800-92 [8] on security logs.

Therefore, based on this analysis, it is worth investigating whether there is any additional information that could be exposed by the 5G Core NFs for monitoring purposes. In the event of that this study determines that strengthening of the external to 3GPP security monitoring is needed, with not yet specified data collection, this information needs to be well defined and explicitly specified to allow for interoperability and secure operation of installed base.

 Besides this no further actions are required.

### 5.1.5 Tenet #6: Access security

#### 5.1.5.1 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". The remaining description of the tenet in [2] relates more to user access to resources and related aspects such as credential management, activity monitoring, etc. Clause 2.2 provides "A Zero Trust View of a Network" in [2], which states that every asset must have its security posture evaluated via a PEP before a request is granted to an enterprise-owned resource (similar to tenet 6 above for assets as well as subjects). In the 5G Core context, and without fully assimilating NFs to users, this tenet can be evaluated from the perspective of NFs consumers. More precisely, how the access by service consumers to the services of producers is secured.

#### 5.1.5.2 Relevant security mechanisms

All the security mechanisms specified in TS 33.501 [4] related to SBA security, in particular clauses 13.3 and 13.4 on authentication and authorization.

#### 5.1.5.3 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.

The currently standardized access control related security mechanisms support authentication and authorization for network service access based on identity and credentials. However, they do not consider security monitoring related information (e.g., threat assessments, security posture etc.,) or any other aspect that is highly dependent on the deployment. Lack of considering security monitoring information for access decisions will allow the NFs with malicious behaviours to remain unidentifiable and continue to access the services from NF service producers which may lead to lateral movement of the attacks. From a standardization perspective, at the 3GPP SBA layer one can investigate whether there is any additional information that could be exposed for security monitoring purposes and how such information is used for access control decisions e.g., authorization. This is covered in the evaluation of Tenet 5 in clause 5.4.

### 5.1.6 Tenet #7: Data collection to improve security posture

#### 5.1.6.1 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], *“An enterprise are expected to 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. In relation to this, section 3.3.1 of [2] gives more details on how 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 can be used for dynamically improving zero trust related security policies. These improvements could include the creation of new policies and enforcement of such policies.

#### 5.1.6.2 Relevant security mechanisms

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

#### 5.1.6.3 Evaluation

Tenet 7 is an overall directive for operator network 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.

The tenet reuses principles and mechanisms that are covered in detail in other tenets such as tenet 5 and 6. This tenet provides some additional clarifications on what kind of data can be collected (i.e., related to tenet 5). Consequently, any provisions for such tenets would constitute the building blocks for tenet 7. The data collection related to abnormal behaviour from NFs and related security analysis outcome considerations can help to apply more fine-grained security policies in 5GC.

## 5.2 Security Mechanism Evaluation summary

Based on the evaluation of the current security mechanisms with respect to the zero trust security tenets in the context of the 5GC discussed in Clause 5.1, a summary is presented in the following Table 5.2-1. Table 5.2-1 contains excerpts from the evaluation details in Clause 5.1. For detail content refer to Clause 5.1.

Table 5.2-1: Overall Tenet Evaluation Summary

|  |  |  |  |
| --- | --- | --- | --- |
| **Tenet No.** | **Short description** | **Relevant security mechanism(s)** | **Evaluation** |
| 1 | Tenet 1 provides a definition for what is to be considered a resource. In the context of the 5G Core, any NF and their services are considered resources. | This is not applicable for Tenet 1 as it is a definition for a resource. | No additional study is needed |
| 2 | Tenet 2 describes how trust is not implicit and cannot be granted automatically based on location, therefore in a ZTA all communications for the 5G Core network should be done in the most secure manner possible. | The 5G Core security standards provide two means to protect communications in and with the 5G Core. On the network layer, there is the NDS/IP framework, relying on IPsec, specified in TS 33.210 [2]. On the transport layer there is TLS for which the profile is also in TS 33.210 [2]. | No additional study is needed. |
| 3 | Tenet 3 is the principle that resources are granted on a per-session basis thus authorization and authentication mechanisms are to be used to gain access to resources. | In the 5G Core context, a session can be equated to a TLS session that uses certificates to provide mutual authentication. In addition, the 5G Core network provides granularity on a per session basis via the OAuth 2.0 mechanism. | No additional study is needed. |
| 4 | Tenet 4 is the principle that access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioural and environmental attributes. In the context of the 5GC, one can evaluate this tenet from the perspective of NFs being clients when acting as service consumers. | The dynamic authorization mechanism based on OAuth2.0 specified in clause 13.4 of TS 33.501 [4]. But the existing access control decisions do not consider the factors e.g., related to behavioural aspects/reported attack. | Should there be any useful information collected from NFs for access authorization purposes, the same information would be also equally relevant in a security monitoring context. The current security standards do not take into account the use of "behavioral attributes" as input to the access authorization process so far and do not provide any mechanisms for the definition and the collection of such attributes for NFs. |
| 5 | Tenet 5 states that the enterprise monitors and measures the integrity and security posture of all owned associated assets as it pertains to operational security and evaluation of the asset’s security posture during evaluation of resource request. In the 5G Core network, data can be collected from NFs and used to perform threat assessment as part of continuous security monitoring and trust evaluation. | The mechanisms specified in TS 23.288 [6] pertaining to data collection from NFs, e.g., clause 6.2.2 and analytics, e.g., clause 6.3 to 6.7.There is currently no explicit standardized security monitoring within NWDAF or in other NF.Operational security is proprietary, and it is expected proper security practices and guidelines are followed during deployment and operations to monitor and measure security posture.  | Development of standard solutions for operational security are not needed.It is worth investigating whether there is any additional information that could be exposed by the 5G Core NFs for monitoring purposes.In the event that this study determines that strengthening of the external to 3GPP security monitoring is needed, with not yet specified data collection, this information needs to be well defined and explicitly specified to allow 5G Core NFs to expose additional information for monitoring. |
| 6 | Tenet 6 states resource authentication and resource authorization are dynamic and strictly enforced before access is allowed. In the 5G Core context, this can be evaluated from the perspective of NF consumer and therefore every request and the resource must have its security posture evaluated before access is granted (e.g., in the form of a PEP/PDP). | In the 5G Core context, a TLS session can be used to provide mutual authentication and OAuth2.0 token can be used to provide authorization.The currently standardized access control related security mechanisms support authentication and authorization for network service access based on identity and credentials. However, they do not consider security monitoring related information (e.g., threat assessments, security posture etc.,) or any other aspect that is highly dependent on the deployment.  | Can investigate whether there is any additional information that could be exposed for security monitoring purposes and how such information is used for access control decisions e.g., authorization.  |
| 7 | Tenet 7 provides a directive to the network operators to facilitate security-related data collection, data processing, and to provide insights to improve the security posture within the 5G Core network. | There are currently no standard procedures for data collection to improve overall 5G core network security posture. | The tenet reuses principles and mechanisms that are covered in detail in other tenets such as tenet 5 and 6. This tenet provides some additional clarifications on what kind of data can be collected (i.e., related to tenet 5). Consequently, any provisions for such tenets would constitute the building blocks for tenet 7. The data collection related to abnormal behaviour from NFs and related security analysis outcome considerations can help to apply more fine-grained security policies in 5GC. |

# 6 Key issues

## 6.1 Key Issue #1: Need for continuous security monitoring

### 6.1.1 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.

The solutions addressing this key issue can aim to identify relevant factors for data collection that could potentially enhance security monitoring and mitigate against insider attacks. 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.,).

NOTE: Considering [2], Zero trust security models assume that an attacker may be present in the environment.

### 6.1.2 Security threats

If any NF that has been deployed in the core network, becomes compromised or starts to behave maliciously, and remain undetected then the NF could be misused in attacks leading to a service failure, data loss/theft, etc.

### 6.1.3 Potential security requirements

The 5GS is required to support mechanisms to collect necessary data to enable security monitoring.

NOTE 1: The actual set of data that can be collected to realize any threat assessments will be addressed during the solution phase.

NOTE 2: The algorithms or logic for trust monitoring and evaluation are outside the scope of 3GPP.

NOTE 3: The handling of potentially compromised NFs (e.g., based on detection) with required security aspects (e.g., applying necessary security patches/fixes) is Operator's implementation choice.

NOTE 4: The key issue and related work considers SBA in the Core network and so, the solutions details should consider the same as the scope of the solution.

# 7 Solutions

## 7.1 Solution #1: Data Collection to enable security monitoring for the Core Network

### 7.1.1 Introduction

The solution addresses KI#1.

The solution describes how various data can be collected and exposed to an external function (i.e., operator’s security evaluation and monitoring entity which is outside the 3GPP domain e.g., a SIEM). The data that need to be collected related to NFs for security monitoring can include information on any violations to the normal behaviour (i.e., 3GPP specified service-based message exchanges in TS 23.502 [9] Clause 5.2) observed in a NF (i.e., an evaluation target). The collected data such as malicious behaviours/activity need to go through security evaluation to enable the overall security monitoring process.

### 7.1.2 Solution details

The malicious behaviour related data can be identified related to various events such as predefined service operation violations (e.g., malformed messages), unintended configuration change(s), message requests exceeding configured limits, and current resource utilization information (if exceeds resource utilization limits) which can be collected as inference data in the form of security logs or reports from the evaluation targets indirectly via the OAM. For malicious behaviour related new data, the solution involves indirect data collection from the evaluation target(s) via the OAM to limit the impact (e.g., over the existing event exposure services) by reusing and leveraging OAM data collection procedure specified in TS 23.288 [6]. The data collection and exposure to enable security evaluation for monitoring is shown in Figure 7.1.2-1:



Figure 7.1.2-1: Procedure to enable Security Monitoring during normal active phase of the NF

1. The NWDAF based on operator local policy can collect the data and provide to the external operator function to enable (i.e., assist) security evaluation and monitoring.

2a-b. The NWDAF can collect data related to NF load and resource utilization by reusing existing data collection procedures specified in TS 23.288 [6] clause 6.5.2 related to NF load (i.e., collection from NRF) and NF resource usage (i.e., collection from OAM).

2c. The NWDAF can use management service from OAM to additionally collect inference data related to various malicious behaviours specific to event identifiers for one or more evaluation target NF(s). For OAM based data collection, the NWDAF can reuse TS 23.288 clause 6.2.3.2 to collect input data specific to the evaluation target NF(s) identification information and target event identifier(s). The OAM collects the inference data (e.g., as a form of security logs/reports) from the target evaluation NFs based on the events indicated and provides the collected inference data to the NWDAF.

NOTE 1: How the OAM collects the inference data and what type of additional security related data (e.g. security logs or events) is collected is for further study.

3. The NWDAF acts as proxy and can provide the collected data to an external operator managed function (i.e., to enable security evaluation and monitoring) via the NEF.

NOTE 2: The external operator function/entity, algorithm(s) or intelligence used for the evaluation, security analysis is upto the operator’s implementation.

NOTE 3: The interface used between NWDAF to NEF and NEF to AF i.e., the external operator function is upto the normative work (e.g., it can be similar to the interface between NEF and external AF (or) can be same as N6). For NEF service exposure to AF, existing NEF services (e.g., TS 23.502 [9] Clause 5.2.6.2.2) can be reused as much as possible with the necessary adaptations.

### 7.1.3 Evaluation

The solution has not been evaluated.

# 8 Conclusions

## Key Issue #1 Conclusion

Solution#1 illustrates how existing services can be used to collect the necessary data listed in the solution for security monitoring purposes in line with the principles of zero trust (Tenet 5). However, no consensus could be reached on the 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 S3-223134, S3-222992, S3-223135, S3-223077, S3-223078, S3-223079, S3-222994, S3-222999. | 0.3.0 |
| 2022-11 | SA3#109 | S3-224162 |  |  |  | Incorporated changes from S3-223864, S3-224031, S3-224126 | 0.4.0 |
| 2023-02 | SA3#110 | S3-231528 |  |  |  | Update of Key Issue#1 (S3-231527) | 0.5.0 |
| 2023-04 | SA3#110 adhoc-e | S3-232228 |  |  |  | Incorporated changes from S3-232018, S3-232102, S3-232103 | 0.6.0 |
| 2023-05 | SA3#111 | S3-233448 |  |  |  | Incorporated Changes from S3-233320 | 0.7.0 |
| 2023-08 | SA3#112 | S3-234318 |  |  |  | Incorporated changes from S3-234200, S3-234201, S3-234202, S3-234203, S3-234204, S3-234224, S3-234205 | 0.8.0 |