|  |
| --- |
| 3GPP TS 33.537 V0.3.0 (2022-11) |
| Technical Specificationt |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security Assurance Specification (SCAS) for the Authentication and Key Management for Applications (AKMA) Anchor Function (AAnF); (Release 18) |
|   |
|  | 3GPP-logo_web |
|  |
| 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.© 2022, 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 6

4 AAnF-specific security requirements and related test cases 7

4.1 Introduction 7

4.2 AAnF-specific adaptations of security functional requirements and related test cases 7

4.2.1 Introduction 7

4.2.2 Security functional requirements on the AAnF deriving from 3GPP specifications and related test cases 7

4.2.2.0 General 7

4.2.2.1 AKMA key storage and update 7

4.2.3 Technical Baseline 8

4.2.3.1 Introduction 8

4.2.3.2 Protecting data and information 8

4.2.3.2.1 Protecting data and information – general 8

4.2.3.2.2 Protecting data and information – unauthorized viewing 8

4.2.3.2.3 Protecting data and information in storage 8

4.2.3.2.4 Protecting data and information in transfer 8

4.2.3.2.4.1 Confidentiality, integrity and replay protections over SBA interface 8

4.2.3.2.4.2 Confidentiality, integrity and replay protections over SBA interface 9

4.2.3.2.5 Logging access to personal data 10

4.2.3.3 Protecting availability and integrity 10

4.2.3.4 Authentication and authorization 10

4.2.3.5 Protecting sessions 10

4.2.3.6 Logging 10

4.2.4 Operating systems 10

4.2.5 Web servers 10

4.2.6 Network devices 10

4.3 AAnF-specific adaptations of hardening requirements and related test cases. 10

4.3.1 Introduction 10

4.3.2 Technical Baseline 10

4.3.3 Operating Systems 10

4.3.4 Web Servers 10

4.3.5 Network Devices 10

4.3.6 Network Functions in service-based architecture 10

4.4 AAnF-specific adaptations of basic vulnerability testing requirements and related test cases 10

# Foreword

This Technical Specification 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

# 1 Scope

The present document contains requirements and test cases that are specific to the AAnF network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the AAnF network product class.

# 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 33.117: "Catalogue of general security assurance requirements"

[3] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[4] 3GPP TR 33.535: " Authentication and key management for applications based on 3GPP credential in 5G （AKMA）".

# 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].

## 3.2 Symbols

Void.

## 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].

AAnF Authentication and Key Management for Applications (AKMA) Anchor Function

# 4 AAnF-specific security requirements and related test cases

## 4.1 Introduction

AAnF specific security requirements include both AAnF-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to AAnF as described in TR 33.926 [3].

## 4.2 AAnF-specific adaptations of security functional requirements and related test cases

### 4.2.1 Introduction

The present clause contains AAnF-specific security functional adaptations of requirements and related test cases.

### 4.2.2 Security functional requirements on the AAnF deriving from 3GPP specifications and related test cases

#### 4.2.2.0 General

The general approach in TS 33.117 [2] clause 4.2.2.1 and all the requirements and test cases in TS 33.117 [2] clause 4.2.2.2 related to SBA/SBI aspects apply to the AAnF network product class.

#### 4.2.2.1 AKMA key storage and update

*Requirement Name*: AKMA key storage update

*Requirement Reference:* TS 33.535 [4], clause 6.1

*Requirement Description*: “The AAnF shall store the latest information sent by the AUSF. After receiving the new generated A-KID and KAKMA, the AAnF deletes the old A-KID and KAKMA and stores the new generated A-KID and KAKMA.” as specified in TS 33.535[4], clause 6.1.

*Threat References*: TR 33.926 [6], clause X.2.2.Y, AKMA key storage and update

*Test Case*:

**Test Name:** TC\_AKMA\_Key\_Storage\_Update

**Purpose:**

Verify that the AAnF stores only the latest AKMA context received by the AUSF.

**Pre-Conditions:**

- Test environment with AUSF and AF. The AUSF and the AF may be simulated.

- AAnF network product is connected in emulated/real network environment.

**Execution Steps**

Test A:

1. Primary authentication is simulated for a specific UE, leading to the simulated AUSF pushing SUPI, A-KID1, KAKMA1 to the AAnF.
2. The AF requests a KAF from the AAnF by proving A-KID1 and AF\_ID.
3. Another primary authentication is simulated for the same UE, leading to the simulated AUSF pushing SUPI, A-KID2, KAKMA2 to the AAnF.
4. The AF requests a KAF by providing A-KID1 to the AAnF.
5. The AF requests a KAF by providing A-KID2 to the AAnF.

**Expected Results:**

The AF received an error message indicating the AKMA context related to A-KID 1 is not found after step 4). After step 5), the AF received a KAF which is different from the KAF that received after step 2).

**Expected format of evidence:**

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

### 4.2.3 Technical Baseline

#### 4.2.3.1 Introduction

The present clause provides baseline technical requirements.

#### 4.2.3.2 Protecting data and information

##### 4.2.3.2.1 Protecting data and information – general

There are no AAnF-specific additions to clause 4.2.3.2.1 of TS 33.117 [2].

##### 4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no AAnF -specific additions to clause 4.2.3.2.2 of TS 33.117 [2].

##### 4.2.3.2.3 Protecting data and information in storage

There are no AAnF -specific additions to clause 4.2.3.2.3 of TS 33.117 [2].

##### 4.2.3.2.4 Protecting data and information in transfer

##### 4.2.3.2.4.1 Confidentiality, integrity and replay protections over SBA interface

*Requirement Name*: Confidentiality, integrity and replay protections over SBA interface

*Requirement Reference:* TS 33.535 [4], clause 4.4.0

*Requirement Description*: "The SBA interface between the AAnF and the AUSF shall be confidentiality, integrity and replay protected." as specified in TS 33.535 [4], clause 4.4.0

*Threat References*: TR 33.926 [3], clause Annex X.2.2.1, Control plane data protection with AUSF

*Test Case:*

**Test Name:** TC\_PROTECT\_SBA\_AAnF\_AUSF

**Purpose:**

Verify that the transported data between AAnF and AUSF are confidentiality, integrity and replay protected over SBA interface.

**Pre-Conditions:**

* AAnF and AUSF network products are connected in simulated/real network environment.
* Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.
* Tester shall have access to the SBA interface between AAnF and AUSF.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

**Expected Results:**

The user data transported between AAnF and AUSF is confidentiality, integrity and replay protected.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture or pcap traces.

##### 4.2.3.2.4.2 Confidentiality, integrity and replay protections over SBA interface

*Requirement Name*: Confidentiality, integrity and replay protections over SBA interface

*Requirement Reference*: TS 33.535 [4], clause 4.4.0

*Requirement Description*: "The SBA interface between AAnF and AF/NEF shall be confidentiality, integrity and replay protected." as specified in TS 33.535 [4], clause 4.4.0

*Threat References*: TR 33.926 [3], clause Annex X.2.2.2, Control plane data protection with AF/NEF

*Test Case*:

**Test Name**: TC\_PROTECT\_AAnF\_AF\_NEF

**Purpose**:

Verify that the transported data between AAnF and AF/NEF are confidentiality, integrity and replay protected over SBA interface.

**Pre-Conditions**:

- AAnF and AF/NEF network products are connected in simulated/real network environment.

- Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

- Tester shall have access to the SBA interface between AAnF and AF/NEF.

**Execution Steps**:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

**Expected Results**:

The user data transported between AAnF and AF/NEF is confidentiality, integrity and replay protected.

**Expected format of evidence**:

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture or pcap traces.

##### 4.2.3.2.5 Logging access to personal data

#### 4.2.3.3 Protecting availability and integrity

#### 4.2.3.4 Authentication and authorization

#### 4.2.3.5 Protecting sessions

#### 4.2.3.6 Logging

### 4.2.4 Operating systems

There are no AAnF-specific additions to clause 4.2.4 of TS 33.117 [2].

### 4.2.5 Web servers

There are no AAnF-specific additions to clause 4.2.5 of TS 33.117 [2].

### 4.2.6 Network devices

There are no AAnF-specific additions to clause 4.2.6 of TS 33.117 [2].

## 4.3 AAnF-specific adaptations of hardening requirements and related test cases.

### 4.3.1 Introduction

The present clause contains AAnF-specific adaptations of hardening requirements and related test cases.

### 4.3.2 Technical Baseline

There are no AAnF-specific additions to clause 4.3.2 of TS 33.117 [2].

### 4.3.3 Operating Systems

There are no AAnF-specific additions to clause 4.3.3 of TS 33.117 [2].

### 4.3.4 Web Servers

There are no AAnF-specific additions to clause 4.3.4 of TS 33.117 [2].

### 4.3.5 Network Devices

There are no AAnF-specific additions to clause 4.3.5 of TS 33.117 [2].

### 4.3.6 Network Functions in service-based architecture

There are no AAnF-specific additions to clause 4.3.6 of TS 33.117 [2].

## 4.4 AAnF-specific adaptations of basic vulnerability testing requirements and related test cases

There are no AAnF-specific additions to clause 4.4 of TS 33.117 [2].Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e | S3-221168 |  |  |  | TS skeleton | 0.0.0 |
| 2022-06 | SA3#107-e | S3-221168 |  |  |  | S3-220809, S3-221156, S3-221159 | 0.1.0 |
| 2022-08 | SA3#108-e | S3-222276 |  |  |  | S3-221752, S3-222134, S3-222135, S3-222138. S3-222139. S3-222140. S3-222141 | 0.2.0 |
| 2022-11 | SA3#109-e | S3-224098 |  |  |  | S3-223457 | 0.3.0 |