

3GPP TS 33.226 v19.0.0 (2025-10)

Technical Specification

**3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security assurance for IP Multimedia Subsystem (IMS)
(Release 19)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and Reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://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.

© 2025, 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 members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® 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.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations.....	8
4 IMS-specific security requirements and related test cases.....	8
4.1 Introduction.....	8
4.2 IMS-specific adaptations of security functional requirements and related test cases.....	8
4.2.1 Introduction.....	8
4.2.2 Security functional requirements on the IMS product classes deriving from 3GPP specifications and related test cases.....	8
4.2.2.1 Introduction.....	8
4.2.2.2 Security functional requirements on the S-CSCF deriving from 3GPP specifications and related test cases.....	8
4.2.2.2.1 No de-registration during the authentication.....	8
4.2.2.2.2 Unprotected register message.....	9
4.2.2.2.3 Synchronization failure handling.....	10
4.2.2.3 Security functional requirements on the P-CSCF deriving from 3GPP specifications and related test cases.....	11
4.2.2.3.1 High-priority algorithm selection.....	11
4.2.2.3.2 Bidding down on security association set-up.....	12
4.2.2.3.3 Protection of IMS signalling in transfer.....	14
4.2.2.3.4 Bidding down on security association set-up in case the P-CSCF policy requiring confidentiality.....	15
4.2.2.3.5 Different SPIs.....	16
4.2.2.4 Security functional requirements on the I-CSCF deriving from 3GPP specifications and related test cases.....	17
4.2.2.4.1 Encryption in network hiding.....	17
4.2.2.5 Security functional requirements on the IBCF deriving from 3GPP specifications and related test cases.....	18
4.2.2.5.1 Encryption in network hiding.....	18
4.2.2.5.2 Replacement in network hiding.....	20
4.2.2.6 Security functional requirements on the AS deriving from 3GPP specifications and related test cases.....	21
4.2.2.6.1 User authorization.....	21
4.2.2.6.2 ID privacy.....	22
4.2.2.7 Security functional requirements on the MRFP deriving from 3GPP specifications and related test cases.....	23
4.2.2.8 Security functional requirements on the IMS MGW deriving from 3GPP specifications and related test cases.....	23
4.2.2.9 Security functional requirements on the MGCF deriving from 3GPP specifications and related test cases.....	23
4.2.2.10 Security functional requirements on the IMS-AGW deriving from 3GPP specifications and related test cases.....	23
4.2.2.11 Security functional requirements on the TrGW deriving from 3GPP specifications and related test cases.....	23
4.2.3 Technical Baseline.....	23
4.2.3.1 Introduction.....	23
4.2.3.2 Protecting data and information.....	23
4.2.3.2.1 Protecting data and information – general.....	23
4.2.3.2.2 Protecting data and information – unauthorized viewing.....	24
4.2.3.2.3 Protecting data and information in storage.....	24
4.2.3.2.4 Protecting data and information in transfer.....	24

4.2.3.2.5	Logging access to personal data.....	24
4.2.3.3	Protecting availability and integrity.....	24
4.2.3.4	Authentication and authorization.....	24
4.2.3.5	Protecting sessions.....	24
4.2.3.6	Logging.....	24
4.2.4	Operating Systems.....	24
4.2.5	Web Servers.....	24
4.2.6	Network Devices.....	24
4.3	IMS-specific adaptations of hardening requirements and related test cases.....	24
4.3.1	Introduction.....	24
4.3.2	Technical baseline.....	24
4.3.3	Operating systems.....	25
4.3.4	Web servers.....	25
4.3.5	Network devices.....	25
4.4	IMS-specific adaptations of basic vulnerability testing requirements and related test cases.....	25
Annex A (informative):	Change history.....	26

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.

1 Scope

The present document contains objectives, requirements and test cases that are specific to the IMS network product classes. 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 IMS network product classes.

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 TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".
 - [3] 3GPP TR 33.203: "3G security; Access security for IP-based services".
 - [4] 3GPP TR 33.328: "IP Multimedia Subsystem (IMS) media plane security".
 - [5] 3GPP TS 33.117: "Catalogue of general security assurance requirements".
 - [6] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)".
-

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

4 IMS-specific security requirements and related test cases

4.1 Introduction

IMS specific security requirements include both requirements derived from IMS-specific security functional requirements in relevant specifications as well as security requirements introduced in the present document derived from the threats specific to IMS network product classes as described in TR 33.926 [1].

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

4.2.1 Introduction

The present clause describes the security functional requirements and the corresponding test cases for IMS network product classes. The proposed security requirements are classified in two groups:

- Security functional requirements derived from TS 33.203 [2] and TS 33.328 [3], and detailed in clause 4.2.2.
- General security functional requirements which include requirements not already addressed in TS 33.203 [2] and TS 33.328 [3] but whose support is also important to ensure that IMS network products conforms to a common security baseline detailed in clause 4.2.3.

4.2.2 Security functional requirements on the IMS product classes deriving from 3GPP specifications and related test cases

4.2.2.1 Introduction

The security functional requirements and the related test cases specific for IMS products are described in this clause.

4.2.2.2 Security functional requirements on the S-CSCF deriving from 3GPP specifications and related test cases

4.2.2.2.1 No de-registration during the authentication

Requirement Name: No de-registration during the authentication

Requirement Reference: TS 33.203 [3], clause 6.1.1

Requirement Description:

"It should be noted that the UE initiated re-registration opens up a potential denial-of-service attack. That is, an attacker could try to register an already registered IMPU and respond with an incorrect authentication response in order to make the HN de-register the IMPU. For this reason a subscriber, when registered, shall not be de-registered if it fails an authentication."

as specified in TS 33.203 [3], clause 6.1.1.

Threat References: O.3.2 Threats related to de-registration during the authentication

Test case:

Test Name: TC_NO_DE-REGISTRATION_AUTH_FAIL

Purpose:

Verify the S-CSCF shall not de-register the registered UE when it fails an authentication during re-registration.

Procedure and execution steps:

Pre-Conditions:

- S-CSCF under test is connected in simulated/real network environment including P-CSCF and HSS.
- The UE supporting IMS AKA has already been registered into the IMS network.
- The tester shall have access to the Mw interface between the P-CSCF and S-CSCF.
- The tester shall have access to the Cx interface between the HSS and S-CSCF.

Execution Steps

- 1) During a new IMS AKA procedure, the UE initiates the re-registration scenario, the tester sends a SM7 register message including the IMPI, and an incorrect authentication response.
- 2) The S-CSCF under test retrieves the active XRES for that user and uses this to check the received authentication response

Expected Results:

The S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed.

The S-CSCF does not initiate de-registration procedure within the Registration expiration interval defined in TS 24.229 [6], i.e. send either Cx-Put (Public User Identity, Private User Identity, clear S-CSCF name) or Cx-Put (Public User Identity, Private User Identity, keep S-CSCF name) to the HSS. Or, the IMPU status in the HSS is registered within the Registration expiration interval defined in TS 24.229 [6].

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text.

Save the logs and the communication flow in a .pcap file.

4.2.2.2 Unprotected register message

Requirement Name: Unprotected register message

Requirement Reference: TS 33.203 [3], clause 7.4.0

Requirement Description:

"If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol."

as specified in TS 33.203 [3], clause 7.4.0.

Threat References: O.3.3.1 Unprotected register message

Test case:

Test Name: TC_UNPROTECTED_REGISTER_MESSAGE

Purpose:

Verify whether the S-CSCF authenticates the user by means of the AKA protocol, if the UE sends unprotected REGISTER messages, regardless whether the UE is already registered or not.

Procedure and execution steps:

Pre-Conditions:

- S-CSCF network product are connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF under test.
- The UE and the P-CSCF are simulated.
- The UE supports a list of ordered integrity and encryption algorithms.
- The tester has access to the Gm interface between the UE and P-CSCF.
- The tester has access to the Mw interface between the P-CSCF and S-CSCF.
- The UE has an already active pair of security associations.

Execution Steps

This test is performed in the Authenticated re-registration procedure, the UE has an already active pair of security associations.

- 1) The UE sends unprotected REGISTER messages (SM1) to the P-CSCF.
- 2) The P-CSCF sends unprotected REGISTER messages (SM2) to the S-CSCF under test.
- 3) The S-CSCF under test receives the SM2 from the P-CSCF.
- 4) The tester examines whether the S-CSCF under test sends SM4: Auth_Challenge to the P-CSCF to authenticate the user by means of the AKA protocol.

Expected Results:

The S-CSCF under test authenticates the user by means of the AKA protocol after.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.2.3 Synchronization failure handling

Requirement Name: Synchronization failure handling

Requirement Reference: TS 33.203 [3], clause 6.1.3

Requirement Description: "The HSS checks the AUTS as in clause 6.3.5 of TS 33.102 [1]. After potentially updating the SQN, the HSS sends new AVs to the S-CSCF in CM4.

CM4:

Cx-AV-Req-Resp(IMPI, n,RAND₁||AUTN₁||XRES₁||CK₁||IK₁,...,RAND_n||AUTN_n||XRES_n||CK_n||IK_n)

When the S-CSCF receives the new batch of authentication vectors from the HSS it deletes the old ones for that user in the S-CSCF.

The rest of the messages i.e. SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1."

as specified in TS 33.203[2], clause 6.1.3.

Threat References: O.3.3.2 No resynchronization

Test Case:

Test Name: TC_SYNC_FAIL_S-CSCF

Purpose:

Verify that in synchronization failure scenario, a new authentication will be triggered by the S-CSCF.

Pre-Conditions:

- Test environment with UE, P-CSCF and HSS. The UE, P-CSCF and HSS may be simulated.
- S-CSCF network product is connected in emulated/real network environment.

Execution Steps

- 1) The UE sends an SM7 to the S-CSCF under test with REGISTER(Failure = Synchronization Failure, AUTS, IMPI).
- 2) The S-CSCF under test sends a CM3 message to the HSS with Cx-AV-Req(IMPI, RAND, AUTS, m).
- 3) The HSS sends a CM4 message to the S-CSCF under test with Cx-AV-Req-Resp(IMPI, n, RAND_i||AUTN_i||XRES₁||CK₁||IK₁, ..., RAND_n||AUTN_n||XRES_n||CK_n||IK_n).

Expected Results:

After receiving CM4 from the HSS, the S-CSCF initiates a new authentication towards the UE, and sends the RAND_i and AUTN_i to the UE, where RAND_i and AUTN_i belong to one of the authentication vectors received in CM4 message.

Expected format of evidence:

Save the logs and the communication flow in a .pcap file.

4.2.2.3 Security functional requirements on the P-CSCF deriving from 3GPP specifications and related test cases

4.2.2.3.1 High-priority algorithm selection

Requirement Name: High-priority algorithm selection

Requirement Reference: TS 33.203 [3], clause 7.2

Requirement Description:

"In order to determine the integrity and encryption algorithm the P-CSCF proceeds as follows: the P-CSCF has a list of integrity and encryption algorithms it supports, ordered by priority. The P-CSCF selects the first algorithm combination on its own list which is also supported by the UE. If the UE did not include any confidentiality algorithm in SM1 then the P-CSCF shall either select the NULL encryption algorithm or abort the procedure, according to its policy on confidentiality."

as specified in TS 33.203 [3], clause 7.2.

Threat References: O.2.2.1 High-priority algorithm selection

Test case:

Test Name: TC_HIGH_PRIORITY_ALGORITHM_SELECTION

Purpose:

Verify the P-CSCF selects the highest priority algorithm combination on its own list which is also supported by the UE.

Procedure and execution steps:

Pre-Conditions:

- P-CSCF under test is connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF under test by the tester.
- The UE supporting IMS AKA may be simulated.
- The UE supports a list of integrity and encryption algorithms.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps

This test is performed in the registration procedure, the UE sends a Register message towards the S-CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

- 1) The UE sends SM1 with integrity and encryption algorithms list to the P-CSCF under test.
- 2) The P-CSCF under test receives the SM1 with integrity and encryption algorithms list. The P-CSCF under test selects algorithms.
- 3) The tester examines the selected algorithm combination in the SM6 sent from the P-CSCF under test to the UE via the Gm interface.

Expected Results:

The selected algorithms are the first algorithm combination on its own list which is also supported by the UE.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file

4.2.2.3.2 Bidding down on security association set-up

Requirement Name: Bidding down on security association set-up

Requirement Reference: TS 33.203 [3], clause 7.2

Requirement Description:

"After receiving SM7 from the UE, the P-CSCF shall check whether the integrity and encryption algorithms list, *SPI_P* and *Port_P* received in SM7 is identical with the corresponding parameters sent in SM6. It further checks whether *SPI_U* and *Port_U* received in SM7 are identical with those received in SM1. If these checks are not successful the registration procedure is aborted. The P-CSCF shall include in SM8 information to the S-CSCF that the received message from the UE was integrity protected as indicated in clause 6.1.5. The P-CSCF shall add this information to all subsequent REGISTER messages received from the UE that have successfully passed the integrity check in the P-CSCF."

as specified in TS 33.203 [3], clause 7.2.

Threat References: O.2.2.2 Bidding down on security association set-up

Test case:

Test Name: TC_BIDDING_DOWN_ON_SECURITY_ASSOCIATION_SET_UP

Purpose:

Verify the P-CSCF checks whether the integrity and encryption algorithms list, *SPI_P* and *Port_P* received in SM7 is identical with the corresponding parameters sent in SM6.

Verify the P-CSCF checks whether *SPI_U* and *Port_U* received in SM7 are identical with those received in SM1.

Verify whether the P-CSCF abort the registration procedure, if the above checks are not successful.

Procedure and execution steps:

Pre-Conditions:

- The P-CSCF under test is connected in simulated/real network environment.
- The list of ordered integrity and encryption algorithms are configured on the P-CSCF under test.
- The UE and the S-CSCF are simulated.
- The UE supports a list of ordered integrity and encryption algorithms. The list contains at least one encryption algorithm other than NULL algorithm.
- The tester has access to the Gm interface between the UE and P-CSCF.
- The tester has access to the Mw interface between the P-CSCF and S-CSCF.

Execution Steps

This test is performed in the registration procedure, the UE sends a Register message towards the S-CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

Test cases 1-4 are performed as follows:

- 1) The UE sends SM1 with the Security Parameter Index values (*SPI_U*) and the protected ports selected by the UE (*Port_U*) to the P-CSCF under test.
- 2) The P-CSCF under test receives the SM1 with the Security Parameter Index values (*SPI_U*) and the protected ports selected by the UE (*Port_U*). The P-CSCF under test store the *SPI_U* and the *Port_U* received in the SM1.
- 3) The P-CSCF under test contains the *SPI_P*, the ports assigned by the P CSCF (*Port_P*) and a list of integrity and encryption algorithms supported by the P-CSCF under test. The P-CSCF under test sends SM6 to the UE.
- 4) The UE receives the SM6 from the P-CSCF under test.

Test case 1:

The UE contains the incorrect *SPI_U* and *Port_U*, which are different from *SPI_U and Port_U* sent in SM1, and *SPI_P* and *Port_P* received in SM6, and a list of integrity and encryption algorithms received in SM6 supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 2:

The UE contains the incorrect *SPI_U* and *Port_U*, which are different from *SPI_U and Port_U* sent in SM1, and incorrect *SPI_P* and *Port_P*, which are different from *SPI_U and Port_U* received in SM6, and a list of integrity and encryption algorithms received in SM6 supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 3:

The UE contains the *SPI_U* and *Port_U* sent in SM1, and incorrect *SPI_P* and *Port_P*, which are different from *SPI_U and Port_U* received in SM6, and a list of integrity and encryption algorithms supported by the P-CSCF under test in the SM7. The UE sends SM7 to the P-CSCF under test.

Test case 4:

The UE contains the *SPI_U* and *Port_U* sent in SM1, and *SPI_P* and *Port_P* received in SM6, and a list of integrity and encryption algorithms in the SM7 which are different from those sent by the P-CSCF under test in the SM6. The UE sends SM7 to the P-CSCF under test.

Expected Results:

For test 2-5, the P-CSCF under test aborts the registration procedure, and sends a suitable 4xx response message to the UE.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.3.3 Protection of IMS signalling in transfer

Requirement Name: Protection of IMS signalling transported between UE and P-CSCF

Requirement Reference: TS 33.203 [3], clause 7.1

Requirement Description:

"For protecting IMS signalling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication and confidentiality, in accordance with the provisions in clauses 5.1.3, 5.1.4, 6.2, and 6.3.

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure are:

- **Encryption algorithm**

Both the UE and the P-CSCF shall adhere to the profiling given in clause 5.3.3 of 33.210 [5] with the addition that only algorithms that can be signalled according to Annex H needs to be supported.

- **Integrity algorithm**

Both the UE and the P-CSCF shall adhere to the profiling given in clause 5.3.4 of 33.210 [5] with the addition that only algorithms that can be signalled according to Annex H needs to be supported."

as specified in TS 33.203 [3], clause 7.1.

Threat References: O.2.3 Threats related to IMS signalling transport

Test case:

Test Name: TC_PROTECT_IMS_SIGNALLING_TRANSFER

Purpose:

Verify the IMS signalling protection mechanisms implemented in P-CSCF adherer to profiling given in clause 5.3.4 of TS 33.210 [5] with the addition that only algorithms that can be signalled according to Annex H of TS 33.203 [3] needs to be supported.

Procedure and execution steps:

Pre-Conditions:

- P-CSCF network products are connected in simulated/real network environment.
- The UE supporting IMS AKA may be simulated.
- Tester shall have the knowledge of the security profiles for the IPsec ESP protection.
- Tester shall have the keys derived from the IMS AKA to negotiate the SA parameters required for IPsec ESP.

Execution Steps

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [3].

Expected Results:

- The P-CSCF under test and the UE established TLS if the TLS profiles used by the UE are compliant with the profile requirements in TS 33.203[3] Annex H.

- The P-CSCF under test and the UE failed to establish TLS if the TLS profiles used by the UE are forbidden in TS 33.203 [3] Annex H.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.3.4 Bidding down on security association set-up in case the P-CSCF policy requiring confidentiality

Requirement Name: Bidding down on security association set-up

Requirement Reference: TS 33.203 [3], clause 7.2

Requirement Description:

"NOTE 4: It should be noted that, if the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network. This would apply in particular to UEs, which support only a Release 5-version of this specification or only GIBA according to Annex T of this specification."

as specified in TS 33.203 [3], clause 7.2.

Threat References: O.2.2.2 Bidding down on security association set-up

Test case:

Test Name: TC_BIDDING_DOWN_ON_SECURITY_ASSOCIATION_SET_UP

Purpose:

Verify that the P-CSCF policy requires confidentiality, then all UEs with no encryption support would be denied access to the IMS network.

NOTE1: The test case below is optional, which only applies to the P- policy requires confidentiality.

Procedure and execution steps:

Pre-Conditions:

- The P-CSCF policy requires confidentiality.
- The UE and the S-CSCF are simulated.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps

This test is performed in the registration procedure, the UE sends a Register message towards the S-CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

Test case 1:

- 1) The UE includes only UE integrity algorithms list in SM1 to the P-CSCF under test.
- 2) The P-CSCF under test receives SM1 and sends SM2 to the S-CSCF.

Test case 2:

- 1) The UE includes UE integrity and encryption algorithms list in SM1 to the P-CSCF under test, where the encryption algorithms are NULL.
- 2) The P-CSCF under test receives SM1.

Expected Results:

For test case, the P-CSCF sends a suitable error message to the UE.

NOTE 2: The suitable error message could be used to identify that the procedure is aborted.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text.

Save the logs and the communication flow in a .pcap file.

4.2.2.3.5 Different SPIs

Requirement Name: Different SPIs

Requirement Reference: TS 33.203 [3], clause 7.1

Requirement Description:

"The SPI is allocated locally for inbound SAs. The triple uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. clause 7.2. In an authenticated registration, the UE and the P-CSCF each select two SPIs, not yet associated with existing inbound SAs, for the new inbound security associations at the UE's client and server ports and the P-CSCF's client and server ports respectively."

NOTE 3: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs."

as specified in TS 33.203 [3], clause 7.1.

Threat References: O.2.4 Threats related to SPI allocation

Test case:

Test Name: TC_DIFFERENT_SPIS

Purpose:

Verify the P-CSCF selects SPIs that are different than the SPIs sent by the UE.

Procedure and execution steps:

Pre-Conditions:

- P-CSCF under test is connected in simulated/real network environment.
- The UE supporting IMS AKA may be simulated.
- The tester has access to the Gm interface between the UE and P-CSCF.

Execution Steps

This test is performed in the registration procedure, the UE sends a Register message towards the S-CSCF through the P-CSCF to register the location of the UE and to set-up the security mode.

- 1) The UE sends SM1 with *spi_uc* (the SPI of the inbound SA at UE's the protected client port) and *spi_us* (the SPI of the inbound SA at the UE's protected server port) to the P-CSCF under test.
- 2) The P-CSCF under test receives the SM1 with *spi_uc* and *spi_us*. The P-CSCF under test selects *spi_pc* (the SPI of the inbound SA at the P-CSCF's protected client port) and *spi_ps* (the SPI of the inbound SA at the P-CSCF's protected server port).
- 3) The tester examines the *spi_pc* and *spi_ps* in the SM6 sent from the P-CSCF under test to the UE via the Gm interface.

Expected Results:

The *spi_pc* and *spi_ps* are different than *spi_uc* and *spi_us*.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.4 Security functional requirements on the I-CSCF deriving from 3GPP specifications and related test cases

4.2.2.4.1 Encryption in network hiding

Requirement Name: Encryption in network hiding

Requirement Reference: TS 33.203 [3], clause 6.4

Requirement Description:

"The Hiding Mechanism is optional for implementation. All I-CSCFs/IBCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF/IBCF shall encrypt the hiding information elements when the I-CSCF/IBCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF/IBCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF/IBCF shall decrypt those information elements that were encrypted by I-CSCF/IBCF in this hiding network domain."

as specified in TS 33.203 [3], clause 6.4.

Threat References: O.4.2.1 encryption in network hiding

Test case:

Test Name: TC_ENCRYPTION_IN_NETWORK HIDING

Purpose:

Verify the I-CSCF encrypts the hiding information elements when the I-CSCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the I-CSCF decrypts those information elements that were encrypted by the I-CSCF in this hiding network domain when the I-CSCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Procedure and execution steps:

Pre-Conditions:

- I-CSCF network products are connected in simulated/real network environment.
- The network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The same encryption and decryption key Kv is configured on the I-CSCFs under test by the tester.
- The encryption algorithm is configured on the I-CSCF under test by the tester.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and I-CSCF.
- The tester has access to the interface between the element outside the hiding network's domain and I-CSCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the encryption of the hiding information elements in the I-CSCF are implemented.

Test case 1: The I-CSCF forwards SIP messages to the outside of the hiding network's domain

- 1) The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the I-CSCF under test.
- 2) The I-CSCF under test forwards the SIP message to the network element outside the hiding network's domain.
- 3) The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The I-CSCF forwards SIP messages to the hiding network's domain

- 1) The network element outside the hiding network's domain sends a SIP message which contains information elements that were encrypted by the I-CSCF in this hiding network domain to the I-CSCF under test.
- 2) The I-CSCF under test forwards the SIP message to the network element in the hiding network's domain.
- 3) The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the I-CSCF under test encrypts the hiding information elements when the I-CSCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the I-CSCF under test decrypts those information elements that were encrypted by the I-CSCF in this hiding network domain when the I-CSCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.5 Security functional requirements on the IBCF deriving from 3GPP specifications and related test cases

4.2.2.5.1 Encryption in network hiding

Requirement Name: Encryption in network hiding

Requirement Reference: TS 33.203 [3], clause 6.4

Requirement Description:

"The Hiding Mechanism is optional for implementation. All I-CSCFs/IBCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF/IBCF shall encrypt the hiding information elements when the I-CSCF/IBCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF/IBCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF/IBCF shall decrypt those information elements that were encrypted by I-CSCF/IBCF in this hiding network domain."

as specified in TS 33.203 [3], clause 6.4.

Threat References: O.5.2.1 encryption in network hiding

Test case:

Test Name: TC_ENCRYPTION_IN_NETWORK HIDING

Purpose:

Verify the IBCF encrypts the hiding information elements when the IBCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the IBCF decrypts those information elements that were encrypted by the IBCF in this hiding network domain when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Procedure and execution steps:**Pre-Conditions:**

- IBCF network products are connected in simulated/real network environment.
- The encryption of the hiding information as the network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The same encryption and decryption key Kv is configured on the IBCFs under test by the tester.
- The encryption algorithm is configured on the IBCF under test by the tester.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and IBCF.
- The tester has access to the interface between the element outside the hiding network's domain and IBCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the encryption of the hiding information elements in the IBCF are implemented.

Test case 1: The IBCF forwards SIP messages to the outside of the hiding network's domain

- 1) The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the IBCF under test.
- 2) The IBCF under test forwards the SIP message to the network element outside the hiding network's domain.
- 3) The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The IBCF forwards SIP messages to the hiding network's domain

- 1) The network element outside the hiding network's domain sends a SIP message which contains information elements that were encrypted by the IBCF in this hiding network domain to the IBCF under test.
- 2) The IBCF under test forwards the SIP message to the network element in the hiding network's domain.
- 3) The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the IBCF under test encrypts the hiding information elements when the IBCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the IBCF under test decrypts those information elements that were encrypted by the IBCF in this hiding network domain when the IBCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.5.2 Replacement in network hiding

Requirement Name: Replacement in network hiding

Requirement Reference: TS 24.229 [6], clause 5.10.4.1

Requirement Description:

"The IBCF shall apply network topology hiding to all header fields which reveal topology information, such as Via, Route, Record-Route, Service-Route, and Path."

as specified in TS 24.229 [6], clause 5.10.4.1.

Threat References: O.5.2.2 replacement in network hiding

Test case:

Test Name: TC_REPLACEMENT IN NETWORK HIDING

Purpose:

Verify the IBCF replaces the hiding information elements to constant values when the IBCF forwards SIP Request or Response messages to the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Verify the IBCF replaces the constant values that were replaced by the IBCF in this hiding network domain to the hiding information elements when the IBCF receives a SIP Request or Response message from the outside of the hiding network's domain, in cases of the network hiding mechanism is used and the operator policy states that the topology shall be hidden.

Procedure and execution steps:

Pre-Conditions:

- IBCF network products are connected in simulated/real network environment.
- The replacement of the hiding information as network hiding mechanism is configured to be used and the operator policy is configured that the topology shall be hidden.
- The network element in the hiding network's domain may be simulated.
- The network element outside the hiding network's domain may be simulated.
- The tester has access to the interface between the element in the hiding network's domain and IBCF.
- The tester has access to the interface between the element outside the hiding network's domain and IBCF.

Execution Steps:

NOTE: This test is performed in case the network hiding mechanism and the replacement of the hiding information elements in the IBCF are implemented.

Test case 1: The IBCF forwards SIP messages to the outside of the hiding network's domain

- 1) The network element in the hiding network's domain sends a SIP message which contains hiding information elements (e.g. addresses of SIP proxies) to the IBCF under test.
- 2) The IBCF under test forwards the SIP message to the network element outside the hiding network's domain.
- 3) The tester examines the SIP message forwarded to the network element outside the hiding network's domain.

Test case 2: The IBCF forwards SIP messages to the hiding network's domain

- 1) The network element outside the hiding network's domain sends a SIP message which contains information elements that were encrypted by the IBCF in this hiding network domain to the IBCF under test.
- 2) The IBCF under test forwards the SIP message to the network element in the hiding network's domain.

- 3) The tester examines the SIP message forwarded to the network element in the hiding network's domain.

Expected Results:

For Test case 1, the IBCF under test replaces the hiding information elements to constant values when the IBCF under test forwards the SIP message to the network element outside the hiding network's domain.

For Test case 2, the IBCF under test replaces the constant values that were replaced by the IBCF in this hiding network domain to the hiding information elements when the IBCF under test forwards the SIP message to the network element in the hiding network's domain.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

4.2.2.6 Security functional requirements on the AS deriving from 3GPP specifications and related test cases

4.2.2.6.1 User authorization

Requirement Name: User authorization

Requirement Reference: TS 24.229 [6], clause 5.7.1.5

Requirement Description:

"If the user is considered anonymous, the AS shall check whether the authorization policy defined for this request allows anonymous requests. If anonymous requests are allowed, then the AS can proceed with the requested functionality, otherwise, the AS shall not proceed with the requested functionality.

...

If the request is not authorized, the AS shall either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted. "

Threat References: O.6.2.1 No user authorization

Test case:

Test Name: TC_USER_AUTHORIZATION

Purpose:

Verify that the AS would reject the anonymous request if anonymous request is not allowed.

Procedure and execution steps:

Pre-Conditions:

- The authorization policy of the AS does not allow anonymous request.
- The UE is simulated.
- The tester has access to the interface between the UE and AS.

Execution Steps

The UE sends the anonymous request message towards the AS, in which the P-Asserted-Identity is set to "Anonymous".

Expected Results:

For test case, the AS either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text.

Save the logs and the communication flow in a .pcap file.

4.2.2.6.2 ID privacy

Requirement Name: ID privacy

Requirement Reference: TS 24.229 [6], clause 5.7.3

Requirement Description:

"5.7.3 Application Server (AS) acting as originating UA

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set a display-name of the From header field to "Anonymous" as specified in RFC 3261 [26] and set an addr-spec of the From header field to Anonymous User Identity as specified in TS 23.003 [3]. "

Threat References: O.6.2.1 No ID privacy

Test case:

Test Name: TC_USER_AUTHORIZATION

Purpose:

Verify that the AS acting as originating UA should send the anonymous identity if privacy is required.

Procedure and execution steps:

Pre-Conditions:

- The privacy of the P-Asserted-Identity is required in AS.
- The UE is simulated.

Execution Steps

The AS under test sends the initial request for a dialog or request for a standalone transaction.

Expected Results:

The display-name of the From header field of the initial request is set to "Anonymous".

The addr-spec of the From header field of the initial request is set to Anonymous User Identity.

Expected format of evidence:

Provide evidence of the check of the product documentation in plain text.

Save the logs and the communication flow in a .pcap file.

4.2.2.7 Security functional requirements on the MRFP deriving from 3GPP specifications and related test cases

There are no MRFP-specific test cases according to the security functional requirements on the MRFP deriving from TS 33.203 [3] and TS 24.229 [6] and security requirements derived from the threats specific to MRFP as described in TR 33.926 [2].

4.2.2.8 Security functional requirements on the IMS MGW deriving from 3GPP specifications and related test cases

There are no IMS MGW -specific test cases according to the security functional requirements on the IMS MGW deriving from TS 33.203 [3] and TS 24.229 [6] and security requirements derived from the threats specific to IMS MGW as described in TR 33.926 [2].

4.2.2.9 Security functional requirements on the MGCF deriving from 3GPP specifications and related test cases

There are no MGCF -specific test cases according to the security functional requirements on the MGCF deriving from TS 33.203 [3] and TS 24.229 [6] and security requirements derived from the threats specific to MGCF as described in TR 33.926 [2].

4.2.2.10 Security functional requirements on the IMS-AGW deriving from 3GPP specifications and related test cases

There are no IMS-AGW -specific test cases according to the security functional requirements on the IMS-AGW deriving from TS 33.203 [3] and TS 24.229 [6] and security requirements derived from the threats specific to IMS-AGW as described in TR 33.926 [2].

4.2.2.11 Security functional requirements on the TrGW deriving from 3GPP specifications and related test cases

There are no TrGW -specific test cases according to the security functional requirements on the TrGW deriving from TS 33.203 [3] and TS 24.229 [6] and security requirements derived from the threats specific to TrGW as described in TR 33.926 [2].

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 IMS-specific additions to clause 4.2.3.2.1 of TS 33.117 [5].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no IMS-specific additions to clause 4.2.3.2.2 of TS 33.117 [5].

4.2.3.2.3 Protecting data and information in storage

There are no IMS-specific additions to clause 4.2.3.2.3 of TS 33.117 [5].

4.2.3.2.4 Protecting data and information in transfer

There are no IMS-specific additions to clause 4.2.3.2.4 of TS 33.117 [5].

4.2.3.2.5 Logging access to personal data

There are no IMS-specific additions to clause 4.2.3.2.5 of TS 33.117 [5].

4.2.3.3 Protecting availability and integrity

There are no IMS-specific additions to clause 4.2.3.3 of TS 33.117 [5].

4.2.3.4 Authentication and authorization

There are no IMS-specific additions to clause 4.2.3.4 of TS 33.117 [5].

4.2.3.5 Protecting sessions

There are no IMS-specific additions to clause 4.2.3.5 of TS 33.117 [5].

4.2.3.6 Logging

There are no IMS-specific additions to clause 4.2.3.6 of TS 33.117 [5].

4.2.4 Operating Systems

There are no IMS-specific additions to clause 4.2.4 of TS 33.117 [5].

4.2.5 Web Servers

There are no IMS-specific additions to clause 4.2.5 of TS 33.117 [5].

4.2.6 Network Devices

There are no IMS-specific additions to clause 4.2.6 of TS 33.117 [5].

4.3 IMS-specific adaptations of hardening requirements and related test cases

4.3.1 Introduction

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

4.3.2 Technical baseline

There are no IMS-specific additions to clause 4.3.2 of TS 33.117 [5].

4.3.3 Operating systems

There are no IMS-specific additions to clause 4.3.3 of TS 33.117 [5].

4.3.4 Web servers

There are no IMS-specific additions to clause 4.3.4 of TS 33.117 [5].

4.3.5 Network devices

There are no IMS-specific additions to clause 4.3.5 of TS 33.117 [5].

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

There are no IMS-specific additions to clause 4.4 of TS 33.117 [5].

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-06	SA#92e	SP-210431				Presented for information and approval	1.0.0
2021-06	SA#92e					EditHelp review and upgrade to change control version	17.0.0
2021-12	SA#94e	SP-211372	0001	-	F	Add the threat references in the TS 33.226	17.1.0
2024-03	-	-	-	-	-	Update to Rel-18 version (MCC)	18.0.0
2025-10	-	-	-	-	-	Update to Rel-19 version (MCC)	19.0.0