Inter-SEPP connection testing Guidelines

Version 1.0

27 Jan 2025

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document provides testing guidelines for connecting various types of SEPPs and proxies, operated by operators or service providers in the operator domain or in the IPX service domain.

These tests validate parts of the N32 interface as defined in 3GPP TS 29.573 [3], as well as the N32s and N32p interfaces as defined in GSMA NG.113 [1])

Editor note:

- The current version of this document does not cover PRINS/ALS and HTTP proxies.

Annex A contains a detailled description of the different tests.

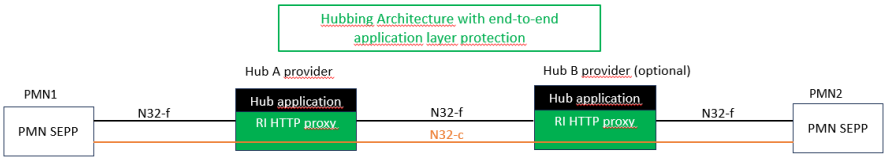
1.2 Scope

This document provides guidelines to test 5G SA signalling between various types of SEPPs used in roaming.

The following interfaces should be tested:

1. N32 for bilateral (using TLS security mechanism) – called N32(TLS)

2. N32 for hubbing (using PRINS security mechanism) – called N32(PRINS)



3. N32s (using TLS security mechanism)

4. N32p (using TLS security mechanism)

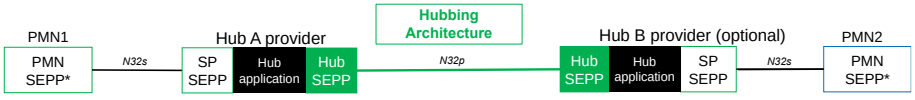


Figure 1: Roaming framework as defined in NG.113 [1]

The scope of this testbook is to test the N32 (N32-c/N32-f) interface as well as the N32p and N32s interfaces between two SEPP for the following contexts:

- Testing N32 connection setup before 5G SA roaming opening (N32) as defined in NG.143
- Testing N32 connection when upgrading SEPP software or changing SEPP supplier

NOTE: SEPP hereby refers to various types of SEPPs defined by GSMA in addition to the PMN SEPP defined in 3GPP 5G specifications. MNO 5G SA signalling simulator will be used to emulate MNO.

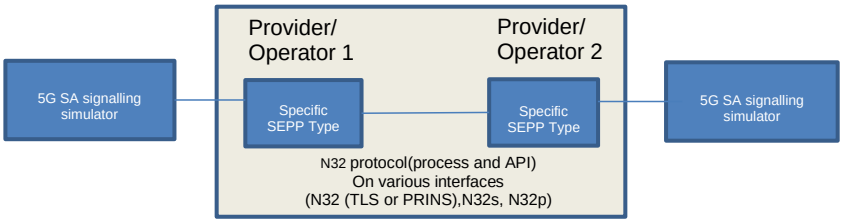


Figure 2: Scope of testing in this document

1.3 Definition of Terms

Term	Description
i-SEPP	Initiating SEPP identified uniquely by i-SEPP FQDN
i-	Prefix used to indicate that the parameter is related to i-SEPP domain
r-SEPP	Responding SEPP identified uniquely by r-SEPP FQDN
r-	Prefix used to indicate that the parameter is related to r-SEPP domain

1.4 Document Cross-References

Ref	Document Number	Title
1	GSMA PRD NG.113	5GS Roaming guidelines
2	GSMA PRD FS.34	Key Management for 4G and 5G inter-PMN Security
3	3GPP TS 29.573	5G System; Public Land Mobile Network (PLMN); Interconnection; Stage 3
4	3GPP TS 23.501	System architecture for the 5G System (5GS); Stage 2
5	3GPP TS 23.502	Procedures for the 5G System (5GS); Stage 2
6	3GPP TS 33.501	Security architecture and procedures for 5G system
7	3GPP TS 29.500	Technical Realization of Service Based Architecture; Stage 3
8	GSMA PRD IR.67	DNS Guidelines for Service Providers and GRX and IPX Providers
9	GSMA PRD NG.143	5G SA Roaming Testing
10	IETF RFC 5256	The Transport Layer Security (TLS) Protocol v1.2

11	IETF RFC 8446	The Transport Layer Security (TLS) Protocol v1.3
12	3GPP TS 33.517	5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class

2 SEPP Provider configuration

2.1 SEPP interface configuration

This section contains the interface configuration of different SEPPs, defined in the section 1.2.
The SEPP interface configuration is provided for different interfaces (N32, N32s, N32p) ; only SEPP FQDN are changed depending on the interface.

The tests described in Annex A use the N32 protocol message format. Since N32-c/-f identical to the format used on N32s and N32p, a single N32 test description can be valid for the interfaces N32s and N32p in addition to N32. However, some tests do not apply to all interfaces; for these tests, this is indicated.

N32 interface configuration (N32(TLS) or N32(PRINS))

Parameter	PROVIDER1	PROVIDER2
Well-known FQDN	sepp.5gc.mnc1.mcc1. 3gppnetwork.org	sepp.5gc.mnc2.mcc2. 3gppnetwork.org
SEPP FQDN	PMN SEPP: Sepp1.sepp.5gc.mnc1.mcc1. 3gppnetwork.org or Hosted/Group SEPP: Sepp1.sepp.5gc.mnc1.mcc1. <PROVIDER1>.ipxpnetwork.org	PMN SEPP: Sepp1.sepp.5gc.mnc2.mcc2. 3gppnetwork.org or Hosted/Group SEPP: Sepp1.sepp.5gc.mnc2.mcc2. <PROVIDER2>.ipxpnetwork.org
SEPP IP address	IP1	IP2
PlmnId used for MNO	MCC1 - MNC1 MCC1a – MNC1a (for multiple plmnId)	MCC2 - MNC2 MCC2a – MNC2a (for multiple plmnId)

N32s interface configuration

Parameter	PROVIDER1	PROVIDER2
Well-known FQDN	sepp.5gc.mnc1.mcc1. 3gppnetwork.org	sepp.5gc.mnc2.mcc2. 3gppnetwork.org
SEPP FQDN (option1)	PMN SEPP: Sepp1.sepp.5gc.mnc1.mcc1. 3gppnetwork.org	SP SEPP: Sepp2.sepp.5gc.mnc2.mcc2. <PROVIDER1>.ipxpnetwork.org
SEPP FQDN (option 2)	SP SEPP: Sepp1.sepp.5gc.mnc1.mcc1. <PROVIDER1>.ipxpnetwork.org	PMN SEPP: Sepp2.sepp.5gc.mnc2.mcc2. 3gppnetwork.org
SEPP IP address	IP1	IP2
PlmnId used for MNO	MCC1 - MNC1 MCC1a – MNC1a (for multiple plmnId)	MCC2 - MNC2 MCC2a – MNC2a (for multiple plmnId)

N32p interface configuration

Parameter	PROVIDER1	PROVIDER2
Well-known FQDN	sepp.5gc.<Hub-ID1>.ipxnetwork.org	sepp.5gc.<Hub-ID2>.ipxnetwork.org
SEPP FQDN	Sepp1.sepp.5gc.<Hub-ID1>.ipxnetwork.org	Sepp1.sepp.5gc.<Hub-ID2>.ipxnetwork.org
SEPP IP address	IP1	IP2

PlmnId used for MNO	MCC1-MNC1 MCC1a – MNC1a (for multiple plmnId)	MCC2-MNC2 MCC2a – MNC2a (for multiple plmnId)

2.2 SEPP 3GPP release and features

This testbook assumes that R16 is the basic 3GPP release to be supported by the PMN SEPP and covers tests for releases from R16 onwards.
This testbook is valid for different configurations, supporting the PMN SEPP in different 3GPP releases and features and supporting GSMA additionally defined SEPP types in NG.113 [1].

Editor's Note: RI HTTP proxy tests to be added in next version.

Typical examples of N32 protocol (N32 procedures and API) are listed hereafter

- N32-c termination
- Usage of 3gpp-Sbi-Originating-Network-Id (R17)
- Error cause on N32-c or N32-f ()

Some test cases are not applicable if the SEPP does not support the functionality, feature or header. For example, Tests 4.6.1 is not applicable if the SEPP does not support the custom header 3ggp-Sbi-Originating-Network-Id.

Apart from these optional features, some technical assumptions are applied in this document:

- Usage of TLS or PRINS as security mecanism
- Usage of custom HTTP header 3gpp-Sbi-Target-apiRoot (R16) (not telescopic FQDN)
- Usage of 3gpp-Sbi-Originating-Network-Id (if available)

2.3 Certificates

2.3.1 Root Certificate

This section shows examples of certain fields in the root certificates exchanged by IPX providers to enable TLS authentication.

More details can be found in annex B.1.

Root certificate (PMN-SEPP)	**Issuer:** CN = CA. mnc1.mcc1.3gppnetwork.org **Subject:** CN=CA. <PLMN-Id>.3gppnetwork.org

Root c ertificate (Hosted -SEPP)	**Issuer:** CN = CA. .<HS-Id>.ipxnetwork.org **Subject:** CN=CA.<HS-Id>.ipxnetwork.org

Root certificate (Hub -SEPP)	**Issuer:** CN = CA. .<Hub-Id>.ipxnetwork.org, **Subject:** CN=CA.<Hub-Id>.ipxnetwork.org

2.3.2 Leaf Certificate

This section contains certain fields of the leaf certificates exchanged between two SEPP types to enable TLS authentication.
More details can be found in annex B.2.

Leaf certificate (PMN-SEPP)	**Issuer:** CN=CA.mnc1.mcc1.3gppnetwork.org **Subject:** CN=sepp1.sepp.5gc.mnc1.mcc1.3gppnetwork.org **Subject Alternative Name:** sepp1.sepp.5gc.mnc1.mcc1.3gppnetwork.org, sepp1.sepp.5gc.mnc1a.mcc1a.3gppnetwork.org,

Note: This leaf certificate is used on N32 and N32s interfaces

Leaf certificate (Hosted-SEPP)	**Issuer:** CN=CA.HS1.ipxnetwork.org **Subject:** CN=sepp1.sepp.5gc.mnc1.mcc1.HS1.ipxnetwork.org **Subject Alternative Name:** sepp1.sepp.5gc.mnc1.mcc1.HS1.ipxnetwork.org, sepp1.sepp.5gc.mnc1a.mcc1a.HS1.ipxnetwork.org,

Note: This leaf certificate is used on N32 and N32s interfaces

Leaf certificate (Hub SEPP)	**Issuer:** CN=CA.Hub1.ipxnetwork.org **Subject:** CN=sepp1.sepp.5gc.Hub1.ipxnetwork.org **Subject Alternative Name:** sepp1.sepp.5gc.Hub1.ipxnetwork.org,

Note: This leaf certificate is used on N32p and N32s interfaces

3 Process

1. Exchange testing document with SEPP configuration
2. Exchange root TLS certificates
3. Configure SEPP type with remote SEPP type and associated certificates, including trust anchors/trust stores.
4. Configure the 5G SA signalling simulators.

4 Test lists

The test descriptions use the N32 protocol message format. Since N32-c/f is identical to the format used on N32s and N32p, a single N32 test description can be valid for the interfaces N32s and N32p in addition to N32. However, some tests do not apply to all interfaces; for these tests, this is indicated.

4.1 SEPP discovery via DNS

This section describes the discovery procedure for the i-SEPP discovering the r-SEPP, with the following technical assumptions:

- Usage of Well-known FQDN + DNS
- Usage of SEPP FQDN + DNS

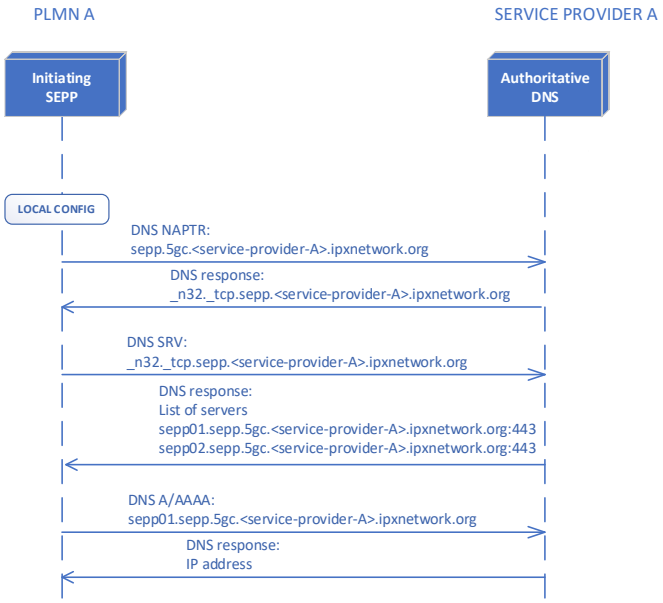


Figure 3: SEPP discovery via DNS (See NG.113 [1])

Test list
- SEPP discovery via DNS (See A.1)

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.2 Basic N32 connection

This section describes the basic N32 connection, with the following technical assumptions:
- PLMN is composed of a unique PLMNId

The purpose of this test is to verify that the capability negotiation procedure works as intended.

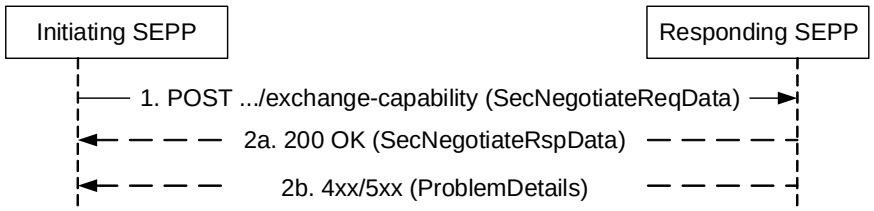


Figure 4 [3] Figure 5.2.2-1: Security Capability Negotiation Procedure

Test list
- Create N32 connection ((TLS or PRINS) (See A.2.1)
- Exchange N32 messages (See A.2.2)
- Stop N32 connection (See A.2.3)

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- I-SEPP / r-SEPP actors

Commented [aj1]: UNCLEAR

Either the text is for TLS to be established or for a message exchanged over N32-c

If it is alread a POST, it is an HTTP message over N32-c, while basic TLS N32 connection suggests it is about the setup of TLS

Commented [MB2R1]: It is about N32 CONNECTION. 3GPP TS 29.573 [3], 5.2 (N32 using supportedSecCapability=TLS)

Commented [MB3]: Defined beginning of the doc

Commented [MB4]: Defined beginning of the doc

4.3 Multi PLMNId N32 connection

This section describes the same tests as previous section, but the PLMN is composed of several PLMNId.

Configuration example with two PLMN IDs:

Parameter	IPX1	IPX2
SEPP FQDN	Sepp1.sepp.5gc.mnc1.mcc1. 3gppnetwork.org	Sepp2.sepp.5gc.mnc2.mcc2. 3gppnetwork.org
PlmnId used for MNO	MCC1 - MNC1 MCC1a – MNC1a (for multiple plmnId)	MCC2 - MNC2 MCC2a – MNC2a (for multiple plmnId)

Test list
- Create N32 connection (TLS or PRINS) (See A.3.1)
- Exchange N32 messages (See A.3.2) with all the different PLMNId
- Stop N32 connection (See A.3.3)

Test variants
- N32 (TLS or PRINS) / N32s (not applicable to N32p due to the fact that PLMNid are not defined for N32p negotiation)
- I-SEPP / r-SEPP actors

4.4 Certificate error

This section describes tests containing certificate errors.
Same configuration as 4.1 except of certificate configuration containing some errors.

Multiple cause could be simulated see Alert message enum in annex D:

4.4.1 Wrong r-SEPP root/leaf certificate at i-SEPP

This section describes tests containing certificate errors at the initiating SEPP.

Test list
- r-SEPP root certificate error at i-SEPP side (See A.4.1)
- r-SEPP leaf certificate error at i-SEPP side (See A.4.2)

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.4.2 Wrong i-SEPP root/leaf certificate at r-SEPP

This section describes tests containing certificate errors at the receiving SEPP.

Test list
- i-SEPP root certificate error at r-SEPP side (See A.4.3)
- i-SEPP leaf certificate error at r-SEPP side (See A.4.4)

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.5 N32-c error cases

Several parameters are tested: N32-c connection is rejected if one of the following N32-c parameter is wrongly configured:

- plmnIdList
- supportedSecCapability
- 3gpp-Sbi-Target-apiRoot-Supported
- Sender

4.5.1 N32-c error with wrong PLMNid

N32-c connection is rejected if PLMNid is not matching the agreed one.

Test list
- N32-c error with wrong PLMNid (See A.5.1) and check that N32-c is rejected when PLMNid is not matching the agreed one

Test variants
- N32 (TLS or PRINS) / N32s
- i-SEPP / r-SEPP actors

4.5.2 N32-c error with wrong supportedSecCapability

N32-c connection is rejected if supportedSecCapability is not matching the agreed one.

Test list
- N32-c error with wrong supportedSecCapability (See A.5.2) and check that N32-c is rejected when supportedSecCapability is not matching the agreed one

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.5.3 N32-c error with wrong 3gpp-Sbi-Target-apiRoot-Supported

N32-c connection is rejected if 3gpp-Sbi-Target-apiRoot-Supported is not matching the agreed one.

Test list
- N32-c error with wrong 3gpp-Sbi-Target-apiRoot-Supported (See A.5.3) and check that N32-c is rejected when 3gpp-Sbi-Target-apiRoot-Supported is not matching the agreed one

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.5.4 N32-c error with wrong Sender

N32-c connection is rejected if Sender is not matching the agreed one.

Test list
- N32-c error with wrong sender (See A.5.4) and check that N32-c is rejected when sender is not matching the agreed one

Test variants
- N32 (TLS or PRINS) / N32s / N32p
- i-SEPP / r-SEPP actors

4.6 N32-f policing

As defined in 3GPP TS 23.501 [4], section 5.9.3.2, the SEPP shall implement anti-spoofing mechanisms that enable cross-layer validation of source and destination address and identifiers (e.g. FQDNs or PLMN IDs).. An example for such an anti-spoofing mechanism is the following: If there is a mismatch between different layers of the message or the destination address does not belong to the SEPP's own PLMN, the message is discarded.

Generally, two options could be used to block the message:
- silently discard (log the event or do not log the event)
- reject with error

4.6.1 N32-f policing with wrong 3gpp-Sbi-Originating-Network-Id

3gpp-Sbi-Originating-Network-Id HTTP custom header is defined in 3GPP TS 29.500 (R17) [7]. This header shall be inserted by an NF service consumer or an NF service producer originating an HTTP request message towards a different PLMN.

The SEPP shall implement anti-spoofing mechanisms on 3gpp-Sbi-Originating-Network-Id. If there is a mismatch, the message is blocked (discarded or rejected).

Test list
- N32-f policing with wrong 3gpp-Sbi-Originating-Network-Id (R17) (See A.6.1)

Test variants
- N32 / N32s / N32p
- I-SEPP / r-SEPP actors

4.6.2 N32-f policing with wrong 3GPP-sbi-target-apiroot

This 3GPP-sbi-target-apiroot header is used between SEPPs to indicate the apiRoot of the target URI towards HTTP server in another PLMN, when TLS security with the 3gpp-Sbi-Target-apiRoot header is used between the SEPPs.

The SEPP shall implement anti-spoofing mechanisms on 3gpp-Sbi-target-apiroot. If there is a mismatch, the message is blocked (discarded or rejected).

Test list
- N32-f policing with wrong 3GPP-sbi-target-apiroot (See A.6.2)

Test variants
- N32 / N32s / N32p
- I-SEPP / r-SEPP actors

4.6.3 N32-f policing with wrong authority

The SEPP shall implement anti-spoofing mechanisms on authority. If there is a mismatch, the message is blocked (discarded or rejected).

Test list
To verify that N32-c establishment is rejected by i-SEPP/r-SEPP for this reasons:

- N32-f policing with wrong authority (See A.6.3)

Test variants

- N32 / N32s / N32p
- I-SEPP / r-SEPP actors

4.7 N32-f parameters

Some N32-f parameters require specific management.

4.7.1 N32-f addition of 3gpp-Sbi-Originating-Network-Id

3gpp-Sbi-Originating-Network-Id HTTP custom header is defined in 3GPP TS 29.500 (R17) [7]. This header shall be inserted by an NF service consumer or an NF service producer originating an HTTP request message towards a different PLMN.

If the sending SEPP or the receiving SEPP cannot uniquely determine the PLMN-ID, it is a configuration/deployment aspect to determine which PLMN-ID value should be included in the header by these entities or if the message should be dropped.

It shall indicate the PLMN-ID of the source PLMN of the HTTP request message (i.e., the PLMN ID of the NF Service Consumer or NF Service Producer).

Test list

- Check that i-SEPP will generate 3gpp-Sbi-Originating-Network-Id on each N32-f message where 3gpp-Sbi-Originating-Network-Id is not present (See A.7.1)

Test variants

- N32 / N32s / N32p
- I-SEPP / r-SEPP actors

4.8 SEPP restart

In case of restart with loss of data, the i-SEPP will set-up automatically all connections to the remote peers/partners (r-SEPP) according to the roaming configuration of the i-SEPP.

Annex A Test descriptions

The tests described in this annex use the N32 protocol message format. Since N32-c/f is identical to the format used on N32s and N32p, a single N32 test description can be valid for the interfaces N32s and N32p in addition to N32. However, some tests do not apply to all interfaces; for these tests, this is indicated.

A.1 SEPP discovery via DNS

Description

The i-SEPP shall initiate a r-SEPP discovery based on:

- Well-knowm FQDN + DNS
- SEPP FQDN + DNS

Applicability

3GPP Release 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications

GSMA PRD IR.67 [8] - DNS Guidelines for Service Providers and GRX and IPX Providers section 4.19
GSMA NG.113 [1], including Detailed Design of TLS hop-by-hop

Reason for test

To verify that i-SEPP can discover the r-SEPP dynamically (Well-known FQDN + DNS, SEPP FQDN + DNS)

Initial configuration

It is assumed that a DNS client within the SEPP takes care of the DNS queries either directly or through a local DNS cache. The DNS client does not make any decisions on next steps but returns the result of each query up to the SEPP application layer. The SEPP application layer decides on the next DNS query to be sent. (Also see section 4.19 of IR.67).

Expected behaviour

Test is successful if the i-SEPP has discovered the correct r-SEPP IP address.

Message flow

Step	Direction	i-SEPP	Message	r-DNS	Comments
PROCEDURE DNS Well-known fqdn **(OPTIONAL)**					
1	-->	**DNS NAPTR Req:** *fqdn = <r-well-known FQDN>*			
2	<--	**DNS NAPTR Resp:** *SRV = _n32._tcp.*<r-sepp domain>			
Procedure DNS with SEPP fqdn **(OPTIONAL)**					
1	-->	**DNS SRV Req:** *SRV = _n32._tcp.* <r-sepp domain>			
2	<--	**List of SEPP servers with priority/weight** <r-SEPP FQDN>			Or one SEPP
3	-->	**DNS A/AAAA Req:** *URI = _n32._tcp.* <r-SEPP FQDN>			
4	<--	**DNS A/AAAA Resp:** *@IP of r-SEPP*			

A.2 Basic N32 connection

A.2.1 Create N32 connection between SEPPs

Description

The initiating SEPP shall initiate a Security Capability Negotiation procedure towards the receiving SEPP. An N32-c end-to-end TLS connection shall be setup between the SEPPs before the initiation of this procedure. This procedure may also be used to tear down the N32-f TLS connection if the remote SEPP indicated support of the feature NFTLST (N32-f TLS connection termination) during the setup of the N32-c connection.

Applicability
3GPP Release 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Note: N32-f TLS part of the test is not part of the test if not set up immediately or PRINS is negotiated in N32-c. This is because “N32-f TLS” term is used in this test for addressing N32s-f and N32p-f or N32-f in case TLS is negotiated in N32-c.

Related core specifications
SEPP to support the 3gpp-Sbi-Target-apiRoot header as specified in 3GPP Release 16 TS 29.500
3GPP TS 29.573 [3], 5.2 (N32) and Annex C.2.2.5
GSMA NG.113 [1], including Detailed Design of TLS hop-by-hop

Reason for test
To verify that i-SEPP can successfully establish N32 between i-SEPP and r-SEPP based on TLS connection.

Initial configuration
i-SEPP is configured with r-SEPP root certificate.
r-SEPP is configured with i-SEPP root certificate.
The IP address of the r-SEPP is configured statically or discovered dynamically by DNS as described in SEPP discovery test (See A.1)

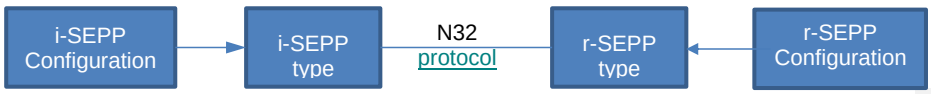


Figure 5: Test context – Create N32 connection

Expected behaviour
Test is successful if

- A TLS connection for N32-c has been established
- a N32-c between i-SEPP and r-SEPP is established and TLS for N32-f negotiated
- a TLS connection for N32-f has been established between i-SEPP and r-SEPP

Test procedure

-	Test procedure	Expected behaviour
1	Configure the r-SEPP using i-SEPP configuration Configure the i-SEPP using r-SEPP configuration	r-SEPP is active in i-SEPP i-SEPP is active in r-SEPP

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANDSHAKE (for N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify ChangeCipherSpec Finished	
4	<--	ChangeCipherSpecFinished	
PROCEDURE N32-c HANDSHAKE (HTTP/2 capability exchange)			
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: i-PLMNid • sender: i-SEPP • supportedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	Check PLMN-ID list at r-SEPP Note: No PLMNId are exchanged for N32p
2	<--	200 OK (SecNegotiateRspData) • plmnIdList: r-PLMNid • sender: r-SEPP • selectedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	Check PLMN-ID list at i-SEPP
PROCEDURE TLS HANDSHAKE (for N32-f) – OPTIONAL (could be setup later)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify ChangeCipherSpec Finished	
4	<--	ChangeCipherSpecFinished	Check that TLS connection is successful for N32-f

A.2.2 Exchange NF signalling messages via N32-f

Description
The i-SEPP shall exchange 5G SA Signalling messages on N32-f connection with r-SEPP. If TLS is the negotiated security policy between the SEPP on N32-c, then the N32-f shall involve only the forwarding of the HTTP/2 messages of the NF service producers and the NF service consumers without any reformatting at the SEPPs and/or the IPXs.

Applicability
3GPP Release 16 or later
N32, N32s, N32p (see Figure 1)

Related core specifications
SEPP to support the 3gpp-Sbi-Target-apiRoot header as specified in 3GPP Release 16 TS 29.500
3GPP TS 29.573 [3], 5.2 (N32) and Annex C.2.2.5
GSMA NG.113 [1], including Detailed Design of TLS hop-by-hop

Reason for test
To verify that i-SEPP can successfully forward N32-f messages between i-SEPP and r-SEPP.

Initial configuration
i-SEPP is configured with r-SEPP root certificate.
r-SEPP is configured with i-SEPP root certificate.
N32 connection is configured and working successfully (test A.2.1)

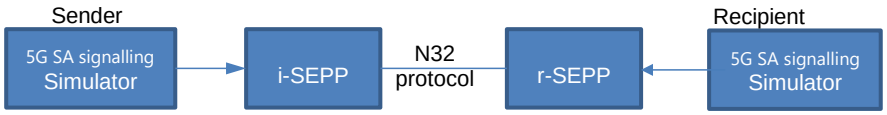


Figure 6: Test context – Exchange N32 messages

Expected behaviour
Test is successful if the i-SEPP has forwarded one N32-f message between i-SEPP and r-SEPP and received a message acknowledgement.

Test procedure

-	Test procedure	Expected behaviour
1	5G SA signalling simulator (sender) will generate a N32 message (example NRF discovery request) to the i-SEPP	i-SEPP will forward the message to r-SEPP r-SEPP will forward the message to 5G SA signalling simulator (recipient)
2	5G SA signalling simulator (recipient) will generate a N32 answer (example NRF discovery response) to the r-SEPP	r-SEPP will forward the message to i-SEPP i-SEPP will forward the message to 5G SA signalling simulator (sender)

Message flow

Step	Direction	i-SEPP	Message	r-SEPP	Comments
PROCEDURE N32-f					
1	-->		HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = i-PLMNid • 3GPP-sbi-target-apiroot= r-NRF • authority = r-SEPP		Check that N32-f message is correctly received at r-SEPP
2	<--		HTTP/2 Nnrf_NF Discovery Response status: 200 OK		Check that N32-f message acknowlegment is correctly received at i-SEPP

A.2.3 Stop N32 connection

Description
The i-SEPP shall delete an existing N32 connection with r-SEPP.
This procedure is used to tear down the N32-f TLS connection if the remote SEPP indicated support of the feature NFTLST (N32-f TLS connection termination) during the setup of the N32-c connection.

Applicability
3GPP Release 17
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
SEPP to support the 3gpp-Sbi-Target-apiRoot header as specified in 3GPP Release 16 TS 29.500 [3]
3GPP TS 29.573 [3], 5.2 (N32) and Annex C.2.2.5
GSMA NG.113 [1], including Detailed Design of hop-by-hop TLS

Reason for test
To verify that i-SEPP can successfully delete N32 connection between i-SEPP and r-SEPP.
To verify that when the request is for tearing down the existing N32-f TLS connection, the "SecNegotiateRspData" IE shall contain “Supported security capability” set to "NONE" and, subsequently, both SEPP shall terminate the N32-c and N32-f TLS connection.

Initial configuration
i-SEPP is configured with r-SEPP root certificate.
r-SEPP is configured with i-SEPP root certificate.
N32 connection is configured and N32-c and N32 working successfully (test A.2.1 and A.2.2)

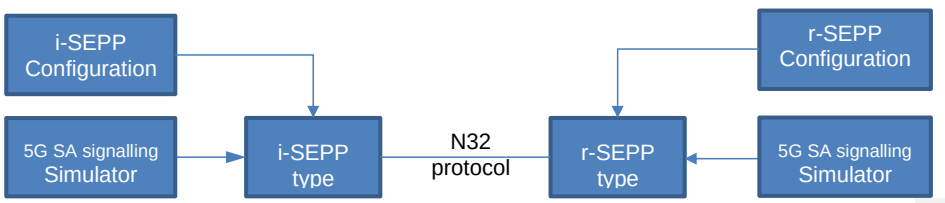


Figure 7: Test context – Stop N32 connection

Expected behaviour
Test is successful if the i-SEPP has deleted N32 connection between i-SEPP and r-SEPP.

Test procedure

-	Test procedure	Expected behaviour
1	Stop the remote r-SEPP using i-SEPP configuration	r-SEPP is no more active in i-SEPP i-SEPP is no more active in r-SEPP
2	Try to exchange N32 messages by sending signalling from the 5G SA signalling simulator	No possible to exchange N32 message, because the N32 interface is stopped

Message flow

Step	Direction	i-SEPP	Message	r-SEPP	Comments
PROCEDURE N32-c					
1	-->		POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList : i-PLMNid • sender: i-SEPP • supportedSecCapability: NONE • 3gpp-Sbi-Target-apiRoot-Supported: True		To tear down the N32-f TLS connection, this IE shall set SecurityCapability as "NONE".
2	<--		200 OK (SecNegotiateRspData) • plmnIdList: r-PLMNid • sender: r-SEPP • selectedSecCapability: NONE • 3gpp-Sbi-Target-apiRoot-Supported: True		Check that N32 connection is closed on r-SEPP and i-SEPP

A.3 Multi PLMNid N32 connection

A.3.1 Create N32 connection – multi-PLMNid

Description
Same tests as A.2.1, but the i-PLMN and r-PLMN are composed of several PLMNId.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s (see Figure 1)

Note: N32-f TLS part of the test is not part of the test if not set up immediately or PRINS is negotiated in N32-c. This is because “N32-f TLS” term is used in this test for addressing N32s-f and N32p-f or N32-f in case TLS is negotiated in N32-c.

Related core specifications
See A.2.1

Reason for test
To verify that i-SEPP can successfully establish a N32 between i-SEPP and r-SEPP based on TLS connection with multi-PLMNId

Initial configuration
Reuse of A.2.1

Expected behaviour
Test is successful if the i-SEPP has established

- a N32-c between i-SEPP and r-SEPP and has TLS negotiated for N32-f
- a TLS connection was successfully setup for N32-f

Test procedure

-	Test procedure	Expected behaviour
1	Configure the r-SEPP using i-SEPP configuration	r-SEPP is active in i-SEPP i-SEPP is active in r-SEPP

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANSHAKE (for N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	Check the SAN of the certificate to verify the PLMN-ID list at r-SEPP is equal to (i-PLMNidList) hosted by the i-SEPP
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify ChangeCipherSpec Finished	Check the SAN of the certificate to verify the PLMN-ID list at r-SEPP is equal to (r-PLMNid) at i-SEPP
4	<--	ChangeCipherSpecFinished	
PROCEDURE N32-c Handshake			
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: i-PLMNidList • sender: i-SEPP • supportedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	Check PLMN-ID list at r-SEPP is matching the i-PLMNidList
2	<--	200 OK (SecNegotiateRspData) • plmnIdList: r-PLMNidList • sender: r-SEPP • selectedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	Check PLMN-ID list at i-SEPP is matching the r-PLMNidList
PROCEDURE TLS HANSHAKE (for N32-f) – OPTIONAL (could be setup later)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify ChangeCipherSpec Finished	
4	<--	ChangeCipherSpecFinished	Check that TLS connection is successful for N32-f

A.3.2 Exchange NF signalling messages via N32-f – multi-PLMNId

Description
Same tests as A.2.2, but the i-PLMN and r-PLMN are composed of several PLMNId.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
Similar to A.2.2

Reason for test
To verify that i-SEPP can successfully forward N32-f messages between i-SEPP and r-SEPP for all PLMNid(s) on i-SEPP and r-SEPP

Initial configuration
Similar to A.2.2

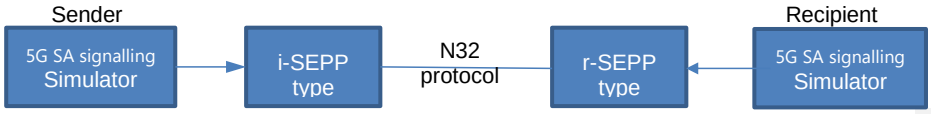


Figure 8: Test context – Exchange N32 messages

Expected behaviour
Test is successful if the i-SEPP has forwarded one N32-f message between i-SEPP and r-SEPP (one per PLMN) and received a message acknowledgement (one per PLMN).

Test procedure

-	Test procedure	Expected behaviour
1	5G SA signalling simulator (sender) will generate a N32 message (example NRF discovery request) to the i-SEPP	i-SEPP will forward the message to r-SEPP r-SEPP will forward the message to 5G SA signalling simulator (recipient)
2	5G SA signalling simulator (recipient) will generate a N32 answer (example NRF discovery response) to the r-SEPP	r-SEPP will forward the message to i-SEPP i-SEPP will forward the message to 5G SA signalling simulator (sender)

Message flow

Step	Direction	i-SEPP	Message	r-SEPP	Comments
PROCEDURE N32-c					
1	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = i-PLMNid • 3gpp-sbi-target-apiroot= r-NRF • authority = r-SEPP			1rst PLMNId
2	<--	HTTP/2 Nnrf_NF Discovery Response status: 200 OK			
3	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = i-PLMNid1 • 3gpp-sbi-target-apiroot= r-NRF • authority = r-SEPP			2nd PLMNId
4	<--	HTTP/2 Nnrf_NF Discovery Response status: 200 OK			

A.3.3 Stop N32 connection (TLS) - multi-PLMNid

Same tests as A.2.3, but the i-PLMN and r-PLMN are composed of several PLMNId.
Apply on N32 (TLS or PRINS), N32s (see Figure 1)

A.4 Certificate error

A.4.1 r-SEPP root certificate error at i-SEPP

Description
This section describes tests containing r-SEPP root certificate errors at the initiating SEPP (See A.2.1).

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP 33.501 [6]
3GPP 33.517 [12]: clause 4.2.5

Reason for test
To verify that N32-c establishment is rejected by i-SEPP for r-SEPP root certificate error.

Initial configuration
Reuse of A.2.1 and change the pre-configuration
Delete the r-SEPP root certificate on i-SEPP and verify that TLS connection is rejected.

Test procedure
See A.2.1

Expected behaviour
Test is successful if the N32-c establishment is rejected by i-SEPP with the appropriate error cause (“unknow_ca”).

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANSHAKE (N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateVerify	WRONG r-SEPP root certificate
3	-->	Alert message {cause=” unknow_ca”}	Verify the TLS handshake failed with alert message

A.4.2 r-SEPP leaf certificate error at i-SEPP

Description
This section describes tests containing r-SEPP leaf certificate errors at the initiating SEPP (See A.2.1).

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP 33.501 [6]

Reason for test
To verify that N32-c establishment is rejected by i-SEPP for r-SEPP leaf certificate error.

Initial configuration
Reuse of A.2.1 and change the pre-configuration
Change on r-SEPP the MCC-MNC of CN and SAN of the r-SEPP leaf certificate (with a wrong MCC-MNC – 000-00)

Test procedure
See A.2.1

Expected behaviour
Test is successful if the N32-c establishment is rejected by i-SEPP with the appropriate error cause (“bad_certificate”).

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANSHAKE (N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateVerify	WRONG r-SEPP leaf certificate
3	-->	Alert message {cause=” bad_certificate”}	Verify the TLS handshake failed with alert message

A.4.3 i-SEPP root certificate error at r-SEPP

Description
This section describes tests containing i-SEPP root certificate errors at the receiving SEPP (See A.2.1).

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP 33.501 [6]
3GPP 33.517 [12]: clause 4.2.5

Reason for test
To verify that N32-c establishment is rejected by r-SEPP for i-SEPP root certificate error.

Initial configuration
Reuse of A.2.1 and change the pre-configuration
Delete the i-SEPP root certificate on r-SEPP and verify that TLS handshake is rejected.

Test procedure
See A.2.1

Expected behaviour
Test is successful if the N32-c establishment is rejected by i-SEPP with the appropriate error cause (“unknow_ca”).

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANSHAKE (N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify	WRONG i-SEPP root certificate
4	<--	Alert message {cause=”unknown_ca”}	Verify the TLS handshake failed with alert message

A.4.4 i-SEPP Leaf certificate error at r-SEPP

Description
This section describes tests containing i-SEPP leaf certificate errors at the receiving SEPP (See A.2.1).

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP 33.501 [6]

Reason for test
To verify that N32-c establishment is rejected by i-SEPP for r-SEPP leaf certificate error.

Initial configuration
Reuse of A.2.1 and change the pre-configuration
Change on i-SEPP the MCC-MNC of CN and SAN of the i-SEPP leaf certificate (with a wrong MCC-MNC – 000-00).

Test procedure
See A.2.1

Expected behaviour
Test is successful if the N32-c establishment is rejected by r-SEPP with the appropriate error cause (“bad_certificate”).

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE TLS HANSHAKE (N32-c)			
1	-->	i-SEPP Hello	
2	<--	r-SEPP Hello Certificate (r-SEPP) CertificateRequest ServerKeyExchange r-SEPP_HelloDone	
3	-->	Certificate (i-SEPP) i-SEPP_KeyExchange CertificateVerify	WRONG i-SEPP leaf certificate
4	<--	Alert message {cause=”bad_certificate”}	Verify the TLS handshake failed with alert message.

A.5 N32-c error cases

A.5.1 N32-c error with wrong PLMNid

Description
N32-c connection is rejected if PLMNid is not matching the agreed one.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.573 [3] R17, Section 5.2.2 (Security Capability Negotiation Procedure)
3GPP TS 29.573 [3] R17, Section 6.1.4.2.2 REQUESTED_PURPOSE_NOT_ALLOWED
3GPP TS 29.500 [7] R16, Section 5.2.7 MANDATORY_QUERY_PARAM_INCORRECT

Reason for test
To verify that N32-c establishment is rejected by r-SEPP if PLMNid proposed by i-SEPP is different of PLMNidList configured in the r-SEPP

Initial configuration
Similar to A.2.1
Change the PLMNidList of i-SEPP to a wrong PLMNid (not i-SEPP).

Test procedure
See A.2.1

Expected behaviour
Test is successful if N32-c establishment is rejected by r-SEPP.

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE N32-c			
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: WRONG-PLMNid • sender: i-SEPP • supportedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	WRONG PLMNid could use MCC=000, MNC=00
2a (If R16)	<--	400 NOK (SecNegotiateRspData) • {(MANDATORY_QUERY_PARAM_INCORRECT }	check that the SecNegociateReqData is rejected
2b (If R17+)	<--	403 NOK (SecNegotiateRspData) • {REQUESTED_PURPOSE_NOT_ALLOWED }	check that the SecNegociateReqData is rejected

A.5.2 N32-c error with incompatible supportedSecCapability

Description
N32-c connection is rejected none of the offered supportedSecCapability is matching the agreed one.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.500 [3] R16, Section 5.2.7 MANDATORY_QUERY_PARAM_INCORRECT
3GPP TS 29.573 [7] R17, Section 5.2.2 (Security Capability Negotiation Procedure)
3GPP TS 29.573 [7] R17, Section 6.1.4.2.2 [REQUESTED_PURPOSE_NOT_ALLOWED]

Reason for test
To verify that N32-c establishment is rejected by r-SEPP if supportedSecCapability proposed by i-SEPP does not include the agreed one.

Initial configuration
See A.2.1
r-SEPP is configured to support only a particular method (TLS or PRINS) for the PLMN IDs of i-SEPP
Change the supportedSecCapability of i-SEPP to not include the selected method above.

Test procedure
See A.2.1

Expected behaviour
Test is successful if negotiation fails

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
		PROCEDURE N32-c	
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: i-PLMNid • sender: i-SEPP • supportedSecCapability: wrong value • 3gpp-Sbi-Target-apiRoot-Supported: True	wrong supportedSecCapability value
2a (If R16)	<--	400 NOK (SecNegotiateRspData) • ProblemDetail ((MANDATORY_QUERY_PARAM_INCORRECT)	check that the SecNegociateReqData is rejected
2b (If R17+)	<--	403 NOK (SecNegotiateRspData) • ProblemDetail (REQUESTED_PURPOSE_NOT_ALLOWED)	check that the SecNegociateReqData is rejected

A.5.3 N32-c error with wrong 3gpp-Sbi-Target-apiRoot-Supported

Description
N32-c connection is rejected if 3gpp-Sbi-Target-apiRoot-Supported is not matching the agreed one.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.500 [3] R16, Section 5.2.7 MANDATORY_QUERY_PARAM_INCORRECT
3GPP TS 29.573 [7] R17, Section 5.2.2 (Security Capability Negotiation Procedure)
3GPP TS 29.573 [7] R17, Section 6.1.4.2.2 [REQUESTED_PURPOSE_NOT_ALLOWED]

Reason for test
To verify that N32-c establishment is rejected by r-SEPP if 3gpp-Sbi-Target-apiRoot-Supported proposed by i-SEPP is different of True

Initial configuration
Similar to A.2.1 and change the 3gpp-Sbi-Target-apiRoot-Supported [3] = False

Test procedure
See A.2.1

Expected behaviour
Test is successful if negotiation fails.

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE N32-c			
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: i-PLMNid • sender: i-SEPP • supportedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: False	WRONG 3gpp-Sbi-Target-apiRoot-Supported: False
2a (If R16)	<--	400 NOK (SecNegotiateRspData) ProblemDetail ((MANDATORY_QUERY_PARAM_INCORRECT)	check that the SecNegociateReqData is rejected
2b (If R17+)	<--	403 NOK (SecNegotiateRspData) ProblemDetail (REQUESTED_PURPOSE_NOT_ALLOWED)	check that the SecNegociateReqData is rejected

A.5.4 N32-c error with wrong Sender

Description
N32-c connection is rejected if Sender is not matching the agreed one.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.500 [3] R16, Section 5.2.7 MANDATORY_QUERY_PARAM_INCORRECT
3GPP TS 29.573 [7] R17, Section 5.2.2 (Security Capability Negotiation Procedure)
3GPP TS 29.573 [7] R17, Section 6.1.4.2.2 [REQUESTED_PURPOSE_NOT_ALLOWED]

Reason for test
To verify that N32-c establishment is rejected by r-SEPP if Sender proposed by i-SEPP is different of i-SEPP

Initial configuration
Similar to A.2.1
Change the Sender of i-SEPP to a wrong Sender (not i-Sender).

Test procedure
See A.2.1

Expected behaviour
Test is successful if negotiation fails

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
		PROCEDURE N32-c	
1	-->	POST ../exchange-capability (SecNegotiateReqData) path: /n32c-handshake/v1/exchange-capability/ authority: r-SEPP • plmnIdList: i-PLMNid • sender: WRONG-SEPP • supportedSecCapability: TLS or PRINS • 3gpp-Sbi-Target-apiRoot-Supported: True	WRONG PLMNid could use MCC=000, MNC=00
2a (If R16)	<--	400 NOK (SecNegotiateRspData) ProblemDetail (MANDATORY_QUERY_PARAM_INCORRECT)	check that the SecNegociateReqData
2b (If R17+)	<--	403 NOK (SecNegotiateRspData) ProblemDetail (REQUESTED_PURPOSE_NOT_ALLOWED)	check that the SecNegociateReqData

A.6 N32-f policing

A.6.1 N32-f policing with wrong 3gpp-Sbi-Originating-Network-Id (R17)

Description

The SEPP shall implement anti-spoofing mechanisms on 3gpp-Sbi-Originating-Network-Id. If there is a mismatch, the message is blocked (discarded or rejected).

Applicability
3GPP Rel. 17 or later
N32, N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.573 [7] R18, section 5.3.3 Table 5.3.3-1

Reason for test
Verify that r-SEPP will discard the receiving N32-f message with wrong 3gpp-Sbi-Originating-Network-Id (not defined for this N32 connection).

Initial configuration
N32 connection is configured and working successfully (test A.1.1)

Test procedure
See A.2.2

Expected behaviour
Test is successful if r-SEPP discards or rejects the receiving N32-f message.

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE N32-f			
1	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = WRONG-PLMNid • 3gpp-sbi-target-apiroot= r-NRF • authority = r-SEPP	WRONG PLMNid could use MCC=000, MNC=00
2a	<--	Optional in case of rejection HTTP/2 Nnrf_NF Discovery Response status: 403 NOK (“CONTEXT_NOT_FOUND”)	Verify that N32-f message is rejected at r-SEPP
2b	<--		Verify that N32-f message is discarded (No Nnrf_NF_Discovery response)

A.6.2 N32-f policing with wrong 3GPP-sbi-target-apiroot

Description

The SEPP shall implement anti-spoofing mechanisms on 3gpp-Sbi-target-apiroot. If there is a mismatch, the message is blocked (discarded or rejected).

Applicability
3GPP Rel. 16 or later
N32, N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.573 [7] R18, section 5.3.3 Table 5.3.3-1

Reason for test
Verify that r-SEPP will discard the receiving N32-f message with wrong 3GPP-sbi-target-apiroot (not defined for this N32 connection).

Initial configuration
N32 connection is configured and working successfully (test A.2.1)

Test procedure
See A.2.2

Expected behaviour
Test is successful if r-SEPP discards or rejects the receiving N32-f message.

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
		PROCEDURE N32-f	
1	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = r-PLMNid • 3gpp-sbi-target-apiroot= WRONG-NRF • authority = r-SEPP	WRONG id could use MCC=000, MNC=00
2a	<--	Optional in case of rejection HTTP/2 Nnrf_NF Discovery Response status: 403 NOK (CONTEXT_NOT_FOUND)	Verify that N32-f message is rejected at r-SEPP
2b	<--		Verify that N32-f message is discarded (No Nnrf_NF_Discovery response)

A.6.3 N32-f policing with wrong authority

Description

The SEPP shall implement anti-spoofing mechanisms on authority. If there is a mismatch, the message is blocked (discarded or rejected).

Applicability
3GPP Rel. 16 or later
N32, N32s, N32p (see Figure 1)

Related core specifications
See A.2.1
3GPP TS 29.573 [7] R18, section 5.3.3 Table 5.3.3-1

Reason for test
Verify that r-SEPP will discard the receiving N32-f message with wrong authority (not defined for this N32 connection).

Initial configuration
N32 connection is configured and working successfully (test A.2.1)

Test procedure
See A.2.2

Expected behaviour
Test is successful if r-SEPP discards or rejects the receiving N32-f message.

Message flow

Step	Direction	i-SEPP Message r-SEPP	Comments
PROCEDURE N32-f			
1	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = r-PLMNid • 3gpp-sbi-target-apiroot= r-NRF • authority = WRONG-SEPP	WRONG id could use MCC=000, MNC=00
2a	<--	Optional in case of rejection HTTP/2 Nnrf_NF Discovery Response status: 403 NOK (CONTEXT_NOT_FOUND)	Verify that N32-f message is (rejected at r-SEPP
2b	<--		Verify that N32-f message is discarded (No Nnrf_NF_Discovery response)

A.7 N32-f parameters

A.7.1 N32-f addition of 3gpp-Sbi-Originating-Network-Id

Description
Check that i-SEPP will generate 3gpp-Sbi-Originating-Network-Id on each N32-f message where 3gpp-Sbi-Originating-Network-Id is not present.

Applicability
3GPP Rel. 17 or later
N32, N32s, N32p (see Figure 1)

Related core specifications
3GPP TS 29.500 [3], section 5.2.3.2.1 (R17) [7]

Reason for test
Receive N32-f message without 3gpp-Sbi-Originating-Network-Id
Check that i-SEPP will generate 3gpp-Sbi-Originating-Network-Id on each N32-f message where 3gpp-Sbi-Originating-Network-Id is not present.

Initial configuration
N32 connection is configured and working successfully (test A.2.1)
MNO (i-NRF or i-NF or MNO SEPP) sends N32-f message without 3gpp-Sbi-Originating-Network-Id

Test procedure
See A.2.2

Expected behaviour
Test is successful if i-SEPP generates 3gpp-Sbi-Originating-Network-Id on N32-f message where 3gpp-Sbi-Originating-Network-Id is not present.

Message flow

Step	Direction	MNO	Message	i-SEPP	Comments
PROCEDURE N32-f					
1.a	-->		HTTP/2 Nnrf_NF Discovery Request • 3gpp-sbi-target-apiroot= r-NRF • authority = i-SEPP		No presence of 3gpp-Sbi-Originating-Network-Id
2.a	<--		HTTP/2 Nnrf_NF Discovery Response status: 200 OK		

Step	Direction	i-SEPP Message r-SEPP	Comments
		PROCEDURE N32-f	
1.b	-->	HTTP/2 Nnrf_NF Discovery Request • 3gpp-Sbi-Originating-Network-Id = i-MCC.i-MNC, srctype = “SEPP”, srcfqdn =sepp1.sepp.5gc.i-mnc.i-mcc.3gppnetwork.org • 3gpp-sbi-target-apiroot= r-NRF • authority = r-SEPP	Verify that 3gpp-Sbi-Originating-Network-Id is added by i-SEPP
2.b	<--	HTTP/2 Nnrf_NF Discovery Response status: 200 OK	

A.8 SEPP restart

Description
In case of restart with loss of data, the i-SEPP will set-up automatically all connections to the remote peers/partners (r-SEPP) according to the roaming configuration of the i-SEPP.

Applicability
3GPP Rel. 16 or later
N32 (TLS or PRINS), N32s, N32p (see Figure 1)

Related core specifications
See A.2.1

Reason for test
Check that, in case of restart, the i-SEPP will set-up automatically all connections to the remote peers/partners (r-SEPP) according to the roaming configuration of the i-SEPP.

Initial configuration
i-SEPP is configured with r-SEPP root certificate.
r-SEPP is configured with i-SEPP root certificate.

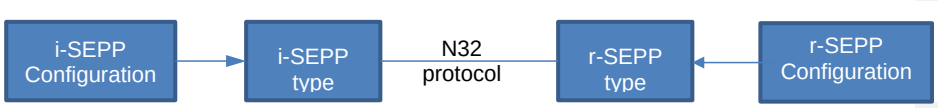


Figure 9: Test context – Create N32 connection

Expected behaviour
Test is successful if the i-SEPP has re-established

- a N32-c between i-SEPP and r-SEPP with TLS selected for N32-f
- a TLS connection for N32-f

Test procedure
See A.2.1

Annex B Certificate: typical examples

B.1 Root Certificate

Root Certificate (Model 1-PLMN SEPP)

Version: 3 (0x2)

Signature Algorithm: ecdsa-with-SHA256

Issuer:

CN = CA. mnc1.mcc1.3gppnetwork.org, O = PLMNid1, ST = France,

C = FR, L=Paris/ emailAddress=pki@PLMNId1.com

Validity:

Not Before: Jan 6 07:25:54 2023 GMT+1

Not After : Jan 5 07:25:54 2024 GMT+1

Subject:

CN= CA. mnc1.mcc1.3gppnetwork.org, O = PLMNid1, ST = France, C=FR, L=Paris/emailAddress=pki@PLMNId1.com

Public Key Algortighm: id-ecPublicKey

Public-key: (521 bit)

Pub: XX:YY:ZZ:MM:NN:SS:…

X509v3 extensions: X509v3 Basic Constraints: critical

X509v3 Key Usage: critical Key Encipherment, Certificate Sign

CA: TRUE

Signature Algorithm: ecdsa-with-SHA256

ZZ:XX:YY:LL:MM:PP:…02

Root Certificate (Model 2-Hosted SEPP)

Version: 3 (0x2)

Signature Algorithm: ecdsa-with-SHA256

Issuer:

CN = CA. .<HS-Id>.ipx.network.org, O = .<HS-Id>.carrier, ST = France,

C = FR, L=Paris/ emailAddress=pki@HS1carrier.com

Validity:

Not Before: Jan 6 07:25:54 2023 GMT+1

Not After : Jan 5 07:25:54 2024 GMT+1

Subject:

CN=CA.<HS-Id>.ipx.network.org, O=.<HS-Id>.carrier, ST=France, C=FR, L=Paris/emailAddress=pki@<HS-Id>carrier.com

Public Key Algortighm: id-ecPublicKey

Public-key: (521 bit)

Pub: XX:YY:ZZ:MM:NN:SS:…

X509v3 extensions: X509v3 Basic Constraints: critical

X509v3 Key Usage: critical Key Encipherment, Certificate Sign

CA: TRUE

Signature Algorithm: ecdsa-with-SHA256

ZZ:XX:YY:LL:MM:PP:…02

Root Certificate (Model 3/4 - Hub SEPP/HTTP Proxy)

Version: 3 (0x2)

Signature Algorithm: ecdsa-with-SHA256

Issuer:

CN = CA. .<Hub-Id>.ipx.network.org, O = .<Hub-Id>.carrier, ST = France,

C = FR, L=Paris/ emailAddress=pki@<Hub-Id>carrier.com

Validity:

Not Before: Jan 6 07:25:54 2023 GMT+1

Not After : Jan 5 07:25:54 2024 GMT+1

Subject:

CN=CA.<Hub-Id>.ipx.network.org, O=.<Hub-Id>.carrier, ST=France, C=FR, L=Paris/emailAddress=pki@<Hub-Id>carrier.com

Public Key Algortighm: id-ecPublicKey

Public-key: (521 bit)

Pub: XX:YY:ZZ:MM:NN:SS:…

X509v3 extensions: X509v3 Basic Constraints: critical

X509v3 Key Usage: critical Key Encipherment, Certificate Sign

CA: TRUE

Signature Algorithm: ecdsa-with-SHA256

YY: XX:LL:MM:PP:…02

B.2 Leaf Certificate

Leaf certificate (PLMN-SEPP)	**Version:** 3 (0x2) **Signature Algorithm:** ecdsa-with-SHA256 **Issuer:** CN=CA. mnc1.mcc1.3gppnetwork.org, O=HS1carrier, ST=France, C=FR, L=Paris/emailAddress=pki@PLMNId1.com **Validity:** Not Before: Feb 6 07:25:54 2023 GMT+1 Not After : Feb 4 07:25:54 2024 GMT+1 **Subject:** CN=sepp1.sepp.5gc.mnc1.mcc1.3gppnetwork.org, O=PLMNId1, ST=France, C=FR, L=Paris/emailAddress=pki@PLMNId1.com **Public Key Algortighm: id-ecPublicKey** **Public-key: (521 bit)** **Pub:** XX:YY:ZZ:MM:NN:SS:… **X509v3 extensions:** **X509v3 Key Usage:** critical Digital Signature, Key Encipherment **X509v3 Extended key Usage:** critical TLS Web Client Authentication, TLS Web Server Authentication **X509v3 Subject Alternative Name:** sepp1.sepp.5gc.mnc1.mcc1.3gppnetwork.org, sepp1.sepp.5gc.mnc1a.mcc1a.3gppnetwork.org, **Signature Algorithm:** ecdsa-with-SHA256 DD:LL/MM:PP:02…

Leaf certificate (Hosted-SEPP)	**Version:** 3 (0x2) **Signature Algorithm:** ecdsa-with-SHA256 **Issuer:** CN=CA.HS1.ipxnetwork.org, O=HS1carrier, ST=France, C=FR, L=Paris/emailAddress=pki@HS1carrier.com **Validity:** Not Before: Feb 6 07:25:54 2023 GMT+1 Not After : Feb 4 07:25:54 2024 GMT+1 **Subject:** CN=sepp1.sepp.5gc.mnc1.mcc1.HS1.ipxnetwork.org, O=HS1carrier, ST=France, C=FR, L=Paris/emailAddress=pki@HS1carrier.com **Public Key Algortighm: id-ecPublicKey** **Public-key: (521 bit)** **Pub:** XX:YY:ZZ:MM:NN:SS:… **X509v3 extensions:** **X509v3 Key Usage:** critical Digital Signature, Key Encipherment **X509v3 Extended key Usage:** critical TLS Web Client Authentication, TLS Web Server Authentication **X509v3 Subject Alternative Name:** sepp1.sepp.5gc.mnc1.mcc1.HS1.ipxnetwork.org, sepp1.sepp.5gc.mnc1a.mcc1a.HS1.ipxnetwork.org, **Signature Algorithm:** ecdsa-with-SHA256 DD:LL/MM:PP:02…

Leaf certificate (Hub provider - SEPP)	**Version:** 3 (0x2) **Signature Algorithm:** ecdsa-with-SHA256 **Issuer:** CN=CA.Hub1.ipxnetwork.org, O=Hub1-provider, ST=France, C=FR, L=Paris/emailAddress=pki@Hub1-provider.com **Validity:** Not Before: Feb 6 07:25:54 2023 GMT+1 Not After : Feb 4 07:25:54 2024 GMT+1 **Subject:** CN=sepp1.sepp.5gc.Hub1.ipxnetwork.org, O=SH1carrier, ST=France, C=FR, L=Paris/emailAddress=pki@Hub1-provider.com **Public Key Algortighm: id-ecPublicKey** **Public-key: (521 bit)** **Pub:** XX:YY:ZZ:MM:NN:SS:… **X509v3 extensions:** **X509v3 Key Usage:** critical Digital Signature, Key Encipherment **X509v3 Extended key Usage:** critical TLS Web Client Authentication, TLS Web Server Authentication **X509v3 Subject Alternative Name:** sepp1.sepp.5gc.Hub1.ipxnetwork.org, **Signature Algorithm:** ecdsa-with-SHA256 DD:LL/MM:PP:02…

Annex C Test list

One test list template (excel file) for each interface (N32 (TLS or PRINS) /N32s/N32p) shall be described herafter:

Test case	i-SEPP	r-SEPP	Test results
A.1.1	PROVIDER1	PROVIDER2	OK/NOK
A.7.1	PROVIDER1	PROVIDER2	

Annex D Parameter definition

D.1 Sbi-Originating-Network-Id

Defined in 29.500 5.2.3.2.15

```
Sbi-Originating-Network-Id-Header = "3gpp-Sbi-Originating-Network-Id:" OWS 3DIGIT "-" 2*3DIGIT
[ "-" 11HEXDIGIT ] [ ";" OWS srcinfo ] OWS

srcinfo = "src" ":" RWS srctype "-" srcfqdn

srctype = "SCP" / "SEPP"

srcfqdn = 4*( ALPHA / DIGIT / "-" / "." )
```

D.2 TLS Alert enum

Defined in RFC 5246 [10] for TLS 1.2 and in RFC 8446 [11] for TLS 1.3

D.2.1 TLS 1.2 Alert enum

Alert enum {
    close_notify(0),
    unexpected_message(10),
    bad_record_mac(20),
    decryption_failed_RESERVED(21),
    record_overflow(22),
    decompression_failure(30),
    handshake_failure(40),
    no_certificate_RESERVED(41),
    bad_certificate(42),
    unsupported_certificate(43),
    certificate_revoked(44),
    certificate_expired(45),
    certificate_unknown(46),
    illegal_parameter(47),
    unknown_ca(48),
    access_denied(49),
    decode_error(50),
    decrypt_error(51),

```
    export_restriction_RESERVED(60),
    protocol_version(70),
    insufficient_security(71),
    internal_error(80),
    user_canceled(90),
    no_renegotiation(100),
    unsupported_extension(110),
    (255)
 } AlertDescription;
```

D.2.2 TLS 1.3 Alert enum

```
enum {
        close_notify(0),
        unexpected_message(10),
        bad_record_mac(20),
        record_overflow(22),
        handshake_failure(40),
        bad_certificate(42),
        unsupported_certificate(43),
        certificate_revoked(44),
        certificate_expired(45),
        certificate_unknown(46),
        illegal_parameter(47),
        unknown_ca(48),
        access_denied(49),
        decode_error(50),
        decrypt_error(51),
        protocol_version(70),
        insufficient_security(71),
        internal_error(80),
        inappropriate_fallback(86),
        user_canceled(90),
        missing_extension(109),
        unsupported_extension(110),
        unrecognized_name(112),
        bad_certificate_status_response(113),
        unknown_psk_identity(115),
        certificate_required(116),
        no_application_protocol(120),
        (255)
    } AlertDescription;
```

Annex E Document Management

E.1 Document History

Version	Date	Brief Description of Change	Editor / Company
0.0.9	23 Feb 2024	Initial version	Marc Balon / Tidiane Diallo (Orange)
1.0	27 Jan 2025	Include comments from Ericsson, Nokia, NTT and BSI	Marc Balon / Tidiane Diallo (Orange)

Other Information

Type	Description
Document Owner	GSMA NG (NRG)
Editor / Company	Marc Balon / Tidiane Diallo (Orange)

Feedback

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.