ETSI TS 129 573 V15.6.0 (2022-10)

5G;
5G System;
Public Land Mobile Network (PLMN) Interconnection;
Stage 3
(3GPP TS 29.573 version 15.6.0 Release 15)

Reference
RTS/TSGC-0429573vf60

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

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 specifies the stage 3 protocol and data model for the PLMN interconnection Interface. It provides stage 3 protocol definitions and message flows, and specifies the APIs for the procedures on the PLMN interconnection interface (i.e N32).

The 5G System stage 2 architecture and procedures are specified in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

The Technical Realization of the Service Based Architecture and the Principles and Guidelines for Services Definition are specified in 3GPP TS 29.500 [4] and 3GPP TS 29.501 [5].

The stage 2 level N32 procedures are specified in 3GPP TS 33.501 [6].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[5] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[7] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[8] IETF RFC 8259: "The JavaScript Object Notation (JSON) Data Interchange Format".

[9] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[10] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[11] IETF RFC 793: "Transmission Control Protocol".

[12] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

[13] IETF RFC 7518: "JSON Web Algorithms (JWA)".

[14] IETF RFC 7516: "JSON Web Encryption (JWE)".

[15] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[16] IETF RFC 7515: "JSON Web Signature (JWS)".

[17] IETF RFC 6901: "JavaScript Object Notation (JSON) Pointer".

[18] 3GPP TS 29.510: "Network Function Repository Services; Stage 3".

[19] 3GPP TS 23.003: "Numbering, addressing and identification".

[20] 3GPP TR 21.900: "Technical Specification Group working methods".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

c-SEPP: The SEPP that is present on the NF service consumer side is called the c-SEPP.

p-SEPP: The SEPP that is present on the NF service producer side is called the p-SEPP.

NOTE: For the purpose of N32-c procedures, the two interacting SEPPs are called "initiating" SEPP and "responding" SEPP. The c-SEPP and p-SEPP terminology is not used in this specification though it is used in 3GPP TS 33.501 [6].

c-IPX: The IPX on the NF service consumer side.

p-IPX: The IPX of the NF service producer side.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

IPX	IP Exchange Service
JOSE	Javascript Object Signing and Encryption
JWE	JSON Web Encryption
JWS	JSON Web Signature
PRINS	PRotocol for N32 INterconnect Security
SEPP	Security and Edge Protection Proxy
TLS	Transport Layer Security

4 General Description

4.1 Introduction

This clause provides a general description of the interconnect interfaces used between the PLMNs for transporting the service based interface message exchanges.

4.2 N32 Interface

4.2.1 General

The N32 interface is used between the SEPPs of a VPLMN and a HPLMN in roaming scenarios. The SEPP that is on the NF service consumer side is called the c-SEPP and the SEPP that is on the NF service producer is called the p-SEPP. The N32 interface can be logically considered as 2 separate interfaces as given below.

- N32-c, a control plane interface between the SEPPs for performing initial handshake and negotiating the parameters to be applied for the actual N32 message forwarding.

- N32-f, a forwarding interface between the SEPPs which is used for forwarding the communication between the NF service consumer and the NF service producer after applying application level security protection.

4.2.2 N32-c Interface

The following figure shows the scope of the N32-c interface.

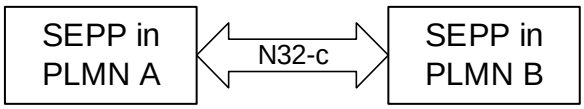

Figure 4.2.2-1: N32-c Interface

The N32-c interface provides the following functionalities:

- Initial handshake procedure between the SEPP in PLMN A (called the initiating SEPP) and the SEPP in PLMN B (called the responding SEPP), that involves capability negotiation and parameter exchange as specified in 3GPP TS 33.501 [6].

4.2.3 N32-f Interface

The following figure shows the scope of the N32-f interface.

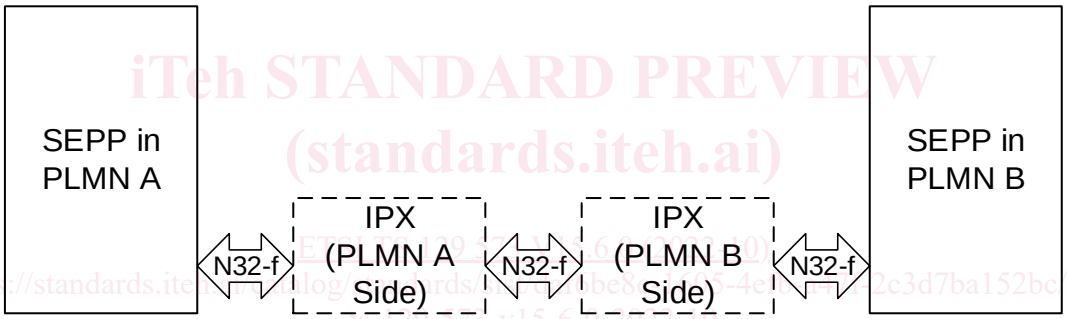

Figure 4.2.3-1: N32-f Interface

The N32-f interface shall be used to forward the HTTP/2 messages of the NF service producers and the NF service consumers in different PLMN, through the SEPPs of the respective PLMN. The application layer security protection functionality of the N32-f is used only if the PRotocol for N32 INterconnect Security (PRINS) is negotiated between the SEPPs using N32-c.

The N32-f interface provides the following application layer security protection functionalities:

- Message protection of the information exchanged between the NF service consumer and the NF service producer across PLMNs by applying application layer security mechanisms as specified in 3GPP TS 33.501 [6].

- Forwarding of the application layer protected message from a SEPP in one PLMN to a SEPP in another PLMN. Such forwarding may involve IPX providers on path.

- If IPX providers are on the path from SEPP in PLMN A to SEPP in PLMN B, the forwarding on the N32-f interface may involve the insertion of content modification instructions which the receiving SEPP applies after verifying the integrity of such modification instructions.

If TLS is the negotiated security policy between the SEPP, 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.

4.3 Protocol Stack

4.3.1 General

The protocol stack for the N32 interface is shown below in Figure 4.2.1-1

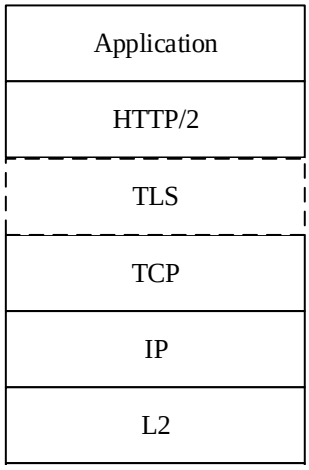

Figure 4.3.1-1: N32 Protocol Stack

The N32 interfaces (N32-c and N32-f) use HTTP/2 protocol (see clause 4.2.2) with JSON (see clause 4.2.4) as the application layer serialization protocol. For the security protection at the transport layer, the SEPPs shall support TLS as specified in 3GPP TS 33.501 [6].

For the N32-f interface, the application layer (i.e the JSON payload) encapsulates the complete HTTP/2 message between the NF service consumer and the NF service producer, by transforming the HTTP/2 headers and the body into specific JSON attributes as specified in clause 6.2.

4.3.2 HTTP/2 Protocol

4.3.2.1 General

HTTP/2 as described in IETF RFC 7540 [7] shall be used for N32 interface.

4.3.2.2 HTTP standard headers

The HTTP request standard headers and the HTTP response standard headers that shall be supported on the N32 interface are defined in Table 4.2.2.2-1 and in Table 4.2.2.2-2 respectively.

Table 4.3.2.2-1: Mandatory to support HTTP request standard headers

Name	Reference	Description
Accept	IETF RFC 7231 [9]	This header is used to specify response media types that are acceptable.
Accept-Encoding	IETF RFC 7231 [9]	This header may be used to indicate what response content-encodings (e.g gzip) are acceptable in the response.
Content-Length	IETF RFC 7230 [10]	This header is used to provide the anticipated size, as a decimal number of octets, for a potential payload body.
Content-Type	IETF RFC 7231 [9]	This header is used to indicate the media type of the associated representation.

Table 4.3.2.2-2: Mandatory to support HTTP response standard headers

Name	Reference	Description
Content-Length	IETF RFC 7230 [10]	This header may be used to provide the anticipated size, as a decimal number of octets, for a potential payload body.
Content-Type	IETF RFC 7231 [9]	This header shall be used to indicate the media type of the associated representation.
Content-Encoding	IETF RFC 7231 [9]	This header may be used in some responses to indicate to the HTTP/2 client the content encodings (e.g gzip) applied to the response body beyond those inherent in the media type.

4.3.2.3 HTTP custom headers

The HTTP custom headers specified in clause 5.2.3 of 3GPP TS 29.500 [4] shall be supported on the N32 interface.

4.3.2.4 HTTP/2 connection management

Each SEPP initiates HTTP/2 connections towards its peer SEPP for the following purposes

- N32-c interface
- N32-f interface

The scope of the HTTP/2 connection used for the N32-c interface is short-lived. Once the initial handshake is completed the connection is torn down as specified in 3GPP TS 33.501 [6]. The HTTP/2 connection used for N32-c is end to end between the SEPPs and does not involve an IPX to intercept the HTTP/2 connection, though an IPX may be involved for IP level routing.

The scope of the HTTP/2 connection used for the N32-f interface is long-lived. The N32-f HTTP/2 connection at a SEPP can be:

- Case A: Towards a SEPP of another PLMN without involving any IPX intermediaries or involving IPX intermediaries where IPX does not require modification or observation of the information; or
- Case B: Towards a SEPP of another PLMN via IPX where IPX requires modification or observation of the information. In this case, the HTTP/2 connection from a SEPP terminates at the next hop IPX with the IPX acting as a HTTP proxy.

For the N32-f interface the HTTP/2 connection management requirements specified in clause 5.2.6 of 3GPP TS 29.500 [4] shall be applicable. The URI scheme used for the N32-f JOSE protected message forwarding API shall be "http". If confidentiality protection of all IEs for the N32-f JOSE protected message forwarding procedure is required, then:

- For case A, the security between the SEPPs shall be ensured by means of IPSec or TLS VPN;
- For case B, hop-by-hop security between the SEPP and the IPXs should be established on N32-f. This hop-by-hop security shall be established using an IPSec or TLS VPN.

4.3.3 Transport Protocol

The Transmission Control Protocol as described in IETF RFC 793 [11] shall be used as transport protocol as required by HTTP/2 (see IETF RFC 7540 [7]). When there is no IPX between the SEPPs or IPX(s) are offering only IP routing service without modification or observation of the content, TLS shall be used for security protection (see clause 13.1 of 3GPP TS 33.501 [6]). When there is IPX between the SEPPs and IPX requires modification or observation of the content, TLS or NDS/IP should be used for security protection as specified in clause 13.1 of 3GPP TS 33.501 [6].

NOTE: When using TCP as the transport protocol, an HTTP/2 connection is mapped to a TCP connection.

4.3.4 Serialization Protocol

The JavaScript Object Notation (JSON) format as described in IETF RFC 8259 [8] shall be used as the serialization protocol.

5 N32 Procedures

5.1 Introduction

The procedures on the N32 interface are split into two categories:

- Procedures that happen end to end between the SEPPs on the N32-c interface;
- Procedures that are used for the forwarding of messages on the service based interface between the NF service consumer and the NF service producer via the SEPP across the N32-f interface.

5.2 N32 Handshake Procedures (N32-c)

5.2.1 General

The N32 handshake procedure is used between the SEPPs in two PLMNs to mutually authenticate each other and negotiate the security mechanism to use over N32-f along with associated security configuration parameters.

A HTTP/2 connection shall be established between the initiating SEPP and the responding SEPP end to end over TLS. The following N32 handshake procedures are specified in the clauses below.

- Security Capability Negotiation Procedure
- Parameter Exchange Procedure
- N32-f Context Termination Procedure
- N32-f Error Reporting Procedure

5.2.2 Security Capability Negotiation Procedure

The initiating SEPP shall initiate a Security Capability Negotiation procedure towards the responding SEPP to agree on a security mechanism to use for protecting NF service related signalling over N32-f. An end to end TLS connection shall be setup between the SEPPs before the initiation of this procedure. The procedure is described in Figure 5.2.2-1 below.

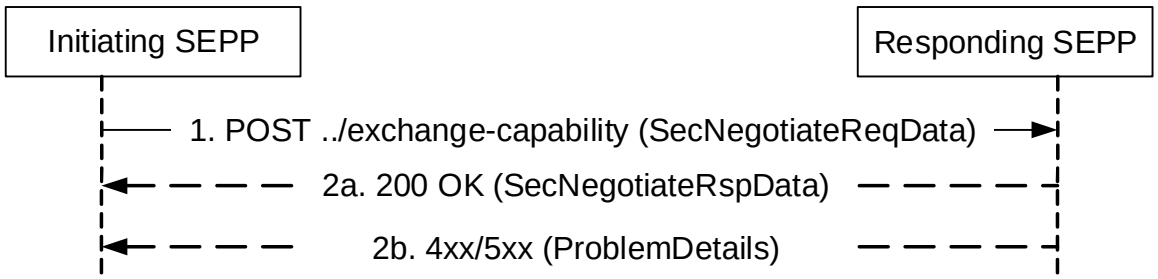

Figure 5.2.2-1: Security Capability Negotiation Procedure

1. The initiating SEPP issues a HTTP POST request towards the responding SEPP with the request body containing the "SecurityNegotiateReqData" IE carrying the following information

- Supported security capabilities (i.e PRINS and/or TLS)

2a. On successful processing of the request, the responding SEPP shall respond to the initiating SEPP with a "200 OK" status code and a POST response body that contains the following information

- Selected security capability (i.e PRINS or TLS)

The responding SEPP compares the initiating SEPP's supported security capabilities to its own supported security capabilities and selects, based on its local policy, a security mechanism, which is supported by both the SEPPs. If the selected security capability indicates any other capability other than PRINS, then the HTTP/2 connection initiated between the two SEPPs for the N32 handshake procedures shall be terminated. The negotiated security capability shall be applicable on both the directions. If the selected security capability is PRINS, then the two SEPPs may decide to create (if not available) / maintain HTTP/2 connection(s) where each SEPP acts as a client towards the other (which acts as a server). This may be used for later signalling of N32-f error reporting procedure (see clause 5.2.5) and N32-f context termination procedure (see clause 5.2.4).

2b. On failure, the responding SEPP shall respond to the initiating SEPP with an appropriate 4xx/5xx status code as specified in clause 6.1.4.2.

5.2.3 Parameter Exchange Procedure

5.2.3.1 General

The parameter exchange procedure shall be executed if the security capability negotiation procedure selected the security capability as PRINS. The parameter exchange procedure is performed to:

- Agree on a cipher suite to use for protecting NF service related signalling over N32-f; and
- Optionally, exchange the protection policies to use for protecting NF service related signalling over N32.

5.2.3.2 Parameter Exchange Procedure for Cipher Suite Negotiation

The parameter exchange procedure for cipher suite negotiation shall be performed after the security capability negotiation procedure if the selected security policy is PRINS.

The procedure is described in Figure 5.2.3.2-1 below.

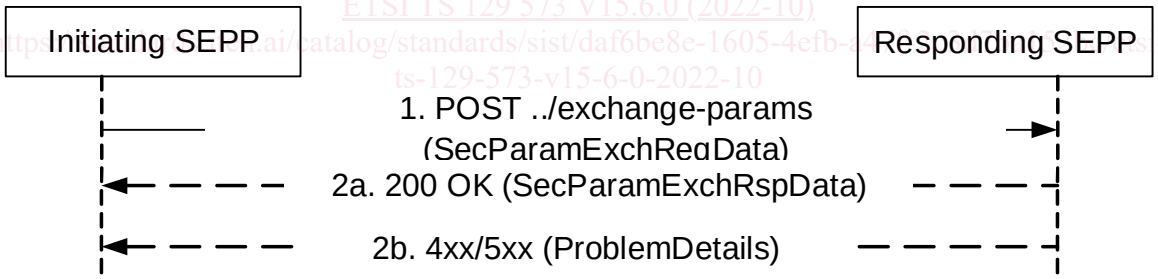

Figure 5.2.3.2-1: Parameter Exchange Procedure for Cipher Suite Negotiation

1. The initiating SEPP issues a HTTP POST request towards the responding SEPP with the request body containing the "SecParamExchReqData" IE carrying the following information

   - Supported cipher suites;

   The supported cipher suites shall be an ordered list with the cipher suites mandated by 3GPP TS 33.501 [6] appearing at the top of the list.

   The initiating SEPP also provides a N32-f context identifier for the responding SEPP to use towards the initiating SEPP for subsequent JOSE Protected Message Forwarding procedures over N32-f (see clause 5.3.3) when the responding SEPP acts as the forwarding SEPP.

2a. On successful processing of the request, the responding SEPP shall respond to the initiating SEPP with a "200 OK" status code and a POST response body that contains the following information

   - Selected cipher suite

   The responding SEPP compares the initiating SEPP's supported cipher suites to its own supported cipher suites and selects, based on its local policy, a cipher suite, which is supported by both the SEPPs. The responding