



N32 Handshake

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 subclauses below:

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

N32-c connection: A TLS based connection between a SEPP in one PLMN and a SEPP in another PLMN.



Note This is a long-lived connection that is used between the SEPPs for cipher suite and protection policy exchange, and error notifications.

N32-f connection: Logical connection that exists between a SEPP in one PLMN and a SEPP in another PLMN for exchange of protected HTTP messages.



Note When IPX providers are present in the path between the two SEPPs, an N32-f HTTP connection is setup on each hop towards the other SEPP.

- [OpenAPI, on page 2](#)
- [info, on page 2](#)
- [externalDocs, on page 2](#)
- [servers, on page 2](#)
- [paths, on page 2](#)
- [components, on page 6](#)

OpenAPI

OpenAPI Version: 3.0.0

info

Version: '1.0.0'

Title: 'N32 Handshake API'

Description: 'N32-c Handshake'

externalDocs

Description: 3GPP TS 29.573 V15.1.0; 5G System; Public Land Mobile Network (PLMN) Interconnection; Stage 3

URL: http://www.3gpp.org/ftp/Specs/archive/29_series/29.573/

servers

URL: '{apiRoot}/n32c-handshake/v1'

Variables:

API Root:

Default: <https://example.com>

Description: apiRoot as defined in subclause 4.4 of 3GPP TS 29.501.

paths

/exchange-capability

Method: Post

Summary: Security Capability Negotiation

Tags:

- Security Capability Negotiation

Operation ID: PostExchangeCapability

Request Body:

Description: Custom operation for security capability negotiation

Required/Optional: true

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/SecNegotiateReqData'

Responses:

'200' OK (Successful negotiation of security capabilities)

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/SecNegotiateRspData'

'400': Reference 'TS29571_CommonData.yaml#/components/responses/400'

'411': Reference 'TS29571_CommonData.yaml#/components/responses/411'

'413': Reference 'TS29571_CommonData.yaml#/components/responses/413'

'415': Reference 'TS29571_CommonData.yaml#/components/responses/415'

'429': Reference 'TS29571_CommonData.yaml#/components/responses/429'

'500': Reference 'TS29571_CommonData.yaml#/components/responses/500'

'503': Reference 'TS29571_CommonData.yaml#/components/responses/503'

default:

Description: Unexpected error

/exchange-params

Method: Post

Summary: Parameter Exchange

Tags:

- Parameter Exchange

Operation ID: PostExchangeParams

Request Body:

Description: Custom operation for parameter exchange

Required/Optional: true

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/SecParamExchReqData'

Responses:

'200' OK (Successful exchange of parameters)

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/SecParamExchRspData'

'400': Reference 'TS29571_CommonData.yaml#/components/responses/400'

'411': Reference 'TS29571_CommonData.yaml#/components/responses/411'

'413': Reference 'TS29571_CommonData.yaml#/components/responses/413'

'415': Reference 'TS29571_CommonData.yaml#/components/responses/415'

'429': Reference 'TS29571_CommonData.yaml#/components/responses/429'

'500': Reference 'TS29571_CommonData.yaml#/components/responses/500'

'503': Reference 'TS29571_CommonData.yaml#/components/responses/503'

default:

Description: Unexpected error

/n32f-terminate

Method: Post

Summary: N32-f Context Terminate

Tags:

- N32-f Context Terminate

Operation ID: PostN32fTerminate

Request Body:

Description: Custom operation for n32-f context termination

Required/Optional: true

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/N32fContextInfo'

Responses:

'200' OK (Successful exchange of parameters)

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/N32fContextInfo'

'400': Reference 'TS29571_CommonData.yaml#/components/responses/400'
'411': Reference 'TS29571_CommonData.yaml#/components/responses/411'
'413': Reference 'TS29571_CommonData.yaml#/components/responses/413'
'415': Reference 'TS29571_CommonData.yaml#/components/responses/415'
'429': Reference 'TS29571_CommonData.yaml#/components/responses/429'
'500': Reference 'TS29571_CommonData.yaml#/components/responses/500'
'503': Reference 'TS29571_CommonData.yaml#/components/responses/503'

default:

Description: Unexpected error

/n32f-error

Method: Post

Summary: N32-f Error Reporting Procedure

Tags:

- N32-f Error Report

Operation ID: PostN32fError

Request Body:

Description: Custom operation for n32-f error reporting procedure

Required/Optional: true

Content:

Application/JSON:

Schema:

Reference: '#/components/schemas/N32fErrorInfo'

Responses:

'204' successful error reporting

'400': Reference 'TS29571_CommonData.yaml#/components/responses/400'

'411': Reference 'TS29571_CommonData.yaml#/components/responses/411'

'413': Reference 'TS29571_CommonData.yaml#/components/responses/413'

'415': Reference 'TS29571_CommonData.yaml#/components/responses/415'

'429': Reference 'TS29571_CommonData.yaml#/components/responses/429'

'500': Reference 'TS29571_CommonData.yaml#/components/responses/500'

'503': Reference 'TS29571_CommonData.yaml#/components/responses/503'

default:

Description: Unexpected error

components

schemas

SecurityCapability

anyOf:

- type: string

enum:

- TLS

- ALS

- type: string

ApiSignature

oneOf:

- \$ref: 'TS29571_CommonData.yaml#/components/schemas/Uri'

- \$ref: '#/components/schemas/CallbackName'

HttpMethod

anyOf:

- type: string

enum:

- GET

- PUT

- POST

- DELETE

- PATCH

- HEAD

- OPTIONS

- CONNECT

- TRACE

- type: string

leType

anyOf:

- type: string

enum:

- UEID
- LOCATION
- KEY_MATERIAL
- AUTHENTICATION_MATERIAL
- AUTHORIZATION_TOKEN
- OTHER
- NONSENSITIVE
- type: string

leLocation**anyOf:**

- type: string

enum:

- URI_PARAM
- HEADER
- BODY
- MULTIPART_BINARY
- type: string

leInfo

Type: object

Required:

- ieLoc
- ieType

Properties:**ieLoc:**

Reference: '#/components/schemas/leLocation'

ieType:

Reference: '#/components/schemas/leType'

reqIe:

Type: string

rspIe:

Type: string

isModifiable:

Type: boolean

ApileMapping

Type: object

Required:

- apiSignature

- apiMethod

- IList

Properties:

apiSignature:

Reference: '#/components/schemas/ApiSignature'

apiMethod:

Reference: '#/components/schemas/HttpMethod'

IList:

Type: array

Items:

Reference: '#/components/schemas/IInfo'

minItems: 1

ProtectionPolicy

Type: object

Required:

- apiIleMappingList

Properties:

apiIleMappingList:

Type: array

Items:

Reference: '#/components/schemas/ApiIleMapping'

minItems: 1

dataTypeEncPolicy:

Type: array

Items:

Reference: '#/components/schemas/IeType'

minItems: 1

SecNegotiateReqData

Type: object

Required:

- sender
- supportedSecCapabilityList

Properties:

sender:

Reference: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Fqdn'

supportedSecCapabilityList:

Type: array

Items:

Reference: '#/components/schemas/SecurityCapability'

minItems: 1

SecNegotiateRspData

Type: object

Required:

- sender
- selectedSecCapability

Properties:

sender:

Reference: 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Fqdn'

selectedSecCapability:

Reference: '#/components/schemas/SecurityCapability'

SecParamExchReqData

Type: object

Required:

- n32fContextId

Properties:

n32fContextId:

Type: string

jweCipherSuiteList:

Type: array

Items:

Type: string
minItems: 1
jwsCipherSuiteList:
Type: array
Items:
Type: string
minItems: 1
protectionPolicyInfo:
Reference: '#/components/schemas/ProtectionPolicy'

SecParamExchRspData

Type: object
Required:
 - n32fContextId
Properties:
n32fContextId:
Type: string
selectedJweCipherSuite:
Type: string
selectedJwsCipherSuite:
Type: string
selProtectionPolicyInfo:
Reference: '#/components/schemas/ProtectionPolicy'

N32fContextInfo

Type: object
Required:
 - n32fContextId
Properties:
n32fContextId:
Type: string

CallbackName

Type: object
Required:
 - callbackType

Properties:**callbackType:**

Type: string

N32fErrorInfo

Type: object

Required:

- n32fMessageId

- n32fErrorType

Properties:**n32fMessageId:**

Type: string

n32fErrorType:**Reference:** '#/components/schemas/N32fErrorType'**failedModificationList:**

Type: array

Items:**Reference:** '#/components/schemas/FailedModificationInfo'**minItems:** 1**errorDetailsList:**

Type: array

Items:**Reference:** '#/components/schemas/N32fErrorDetail'**minItems:** 1**FailedModificationInfo**

Type: object

Required:

- ipxId

- n32fErrorType

Properties:**ipxId:****Reference:** 'TS29510_Nnrf_NFManagement.yaml#/components/schemas/Fqdn'**n32fErrorType:****Reference:** '#/components/schemas/N32fErrorType'

N32fErrorDetail

Type: object

Required:

- attribute
- msgReconstructFailReason

Properties:

attribute:

Type: string

msgReconstructFailReason:

Reference: '#/components/schemas/FailureReason'

N32fErrorType

anyOf:

- type: string

enum:

- INTEGRITY_CHECK_FAILED
- INTEGRITY_CHECK_ON_MODIFICATIONS_FAILED
- MODIFICATIONS_INSTRUCTIONS_FAILED
- DECIPHERING_FAILED
- MESSAGE_RECONSTRUCTION_FAILED
- type: string

FailureReason

anyOf:

- type: string

enum:

- INVALID_JSON_POINTER
- INVALID_INDEX_TO_ENCRYPTED_BLOCK
- INVALID_HTTP_HEADER
- type: string