|  |  |
| --- | --- |
| 3GPP TS 29.309 V18.2.0 (2024-06) | |
| Technical Specification | |
| 3rd Generation Partnership Project;  Technical Specification Group Core Network and Terminals;  5G System;  Bootstrapping Server Function (GBA BSF) Services;  Stage 3  (Release 18) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal 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.  © 2024, 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 and abbreviations 8

3.1 Definitions 8

3.2 Abbreviations 8

4 Overview 8

5 Services offered by the GBA BSF 9

5.1 Introduction 9

5.2 Nbsp\_GBA Service 9

5.2.1 Service Description 9

5.2.2 Service Operations 9

5.2.2.1 Introduction 9

5.2.2.2 BootstrapInfo 10

5.2.2.2.1 General 10

5.2.2.2.2 Boostrapping Info Retrieval 10

5.2.2.3 PushInfo 10

5.2.2.3.1 General 10

5.2.2.3.2 Push Info Retrieval 10

6 API Definitions 11

6.1 Nbsp\_GBA Service API 11

6.1.1 Introduction 11

6.1.2 Usage of HTTP 12

6.1.2.1 General 12

6.1.2.2 HTTP standard headers 12

6.1.2.2.1 General 12

6.1.2.2.2 Content type 12

6.1.2.3 HTTP custom headers 12

6.1.3 Resources 12

6.1.3.1 Overview 12

6.1.4 Custom Operations without associated resources 13

6.1.4.1 Overview 13

6.1.4.2 Operation: Bootstrapping Info Retrieval 13

6.1.4.2.1 Description 13

6.1.4.2.2 Operation Definition 13

6.1.4.3 Operation: Push Info Retrieval 14

6.1.4.3.1 Description 14

6.1.4.3.2 Operation Definition 14

6.1.5 Notifications 15

6.1.6 Data Model 15

6.1.6.1 General 15

6.1.6.2 Structured data types 16

6.1.6.2.1 Introduction 16

6.1.6.2.2 Type: BootstrappingInfoRequest 17

6.1.6.2.3 Type: BootstrappingInfoResponse 17

6.1.6.2.4 Type: PushInfoRequest 17

6.1.6.2.5 Type: PushInfoResponse 18

6.1.6.2.6 Type: NafId 18

6.1.6.2.7 Type: UssListItem 18

6.1.6.2.8 Type: Uss 18

6.1.6.2.9 Type: UeIdsItem 19

6.1.6.2.10 Type: FlagsItem 19

6.1.6.3 Simple data types and enumerations 19

6.1.6.3.1 Introduction 19

6.1.6.3.2 Simple data types 19

6.1.6.3.3 Enumeration: KeyChoice 20

6.1.6.3.4 Enumeration: UiccOrMe 20

6.1.6.3.5 Enumeration: SecFeature 21

6.1.6.3.6 Enumeration: GbaType 21

6.1.6.3.7 Enumeration: UeIdType 21

6.1.7 Error Handling 21

6.1.7.1 General 21

6.1.7.2 Protocol Errors 21

6.1.7.3 Application Errors 21

6.1.8 Feature negotiation 22

6.1.9 Security 22

Annex A (normative): OpenAPI specification 23

A.1 General 23

A.2 Nbsp\_GBA API 23

Annex B (informative): Change history 30

# 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 Nbsp Service Based Interface. It provides stage 3 protocol definitions and message flows, and specifies the API for each service offered by the GBA BSF.

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

The stage 2 architecture and procedures of SBA-enabled GBA is specified in 3GPP TS 33.220 [14] and 3GPP TS 33.223 [15].

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].

# 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] OpenAPI: "OpenAPI Specification Version 3.0.0", <https://spec.openapis.org/oas/v3.0.0>.

[7] 3GPP TR 21.900: "Technical Specification Group working methods".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[10] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[11] IETF RFC 9113: "HTTP/2".

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

[13] IETF RFC 9457: "Problem Details for HTTP APIs".

[14] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[15] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[16] 3GPP TS 33.224: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer".

[17] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[18] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

# 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].

**Bootstrapping Server Function:** BSF is hosted in a network element under the control of an MNO. BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure. The shared secret can be used between NAFs and UEs, for example, for authentication purposes. In the context of the present specification, the BSF is an SBA-capable BSF.

**GBA Function:** A function on the ME executing the bootstrapping procedure with BSF (i.e. supporting the Ub reference point) and providing Ua applications with security association to run bootstrapping usage procedure. GBA function is called by a Ua application when a Ua application wants to use bootstrapped security association.

**Network Application Function:** NAF is hosted in a network element. GBA may be used between NAFs and UEs for authentication purposes, and for securing the communication path between the UE and the NAF. In the context of the present specification, the NAF is an SBA-capable NAF.

**GBA User Security Settings:** GUSS contains the BSF specific information element and the set of all application-specific USSs.

**Ua Application:** An application on the ME intended to run bootstrapping usage procedure with a NAF.

## 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].

BSF Bootstrapping Server Function

GBA Generic Bootstrapping Architecture

GUSS GBA User Security Settings

HSS Home Subscriber System

NAF Network Application Function

SBA Service-Based Architecture

USS User Security Setting

# 4 Overview

Nbsp is a Service-based interface exhibited by GBA BSF (Generic Bootstrapping Architecture; Bootstrapping Server Function) which is a Network Function that supports the following functionality:

- Allows the NAF and the Push-NAF to fetch the key material agreed during a previous protocol run between the UE and the GBA BSF. It is also used to fetch application-specific user security settings from the GBA BSF, if requested by the NAF.

The reference points N66 and N67 (see Fig 4-1 below) show the interaction between the GBA BSF and the NAF and Push-NAF Network Functions.



Figure 4-1: Reference Model – Nbsp

In the context of the present specification, the GBA BSF is an SBA-capable BSF, and the NAF and Push-NAF are also SBA-capable Network Functions (see 3GPP TS 33.220 [14] and 3GPP TS 33.223 [15]).

# 5 Services offered by the GBA BSF

## 5.1 Introduction

The GBA BSF offers the following services via the Nbsp interface:

- Nbsp\_GBA Service

Table 5.1-1 summarizes the corresponding APIs defined for this specification.

Table 5.1-1: API Descriptions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Service Name | Clause | Description | OpenAPI Specification File | apiName | **Annex** |
| Nbsp\_GBA | 5.2 | Nbsp GBA Service | TS29309\_Nbsp\_GBA.yaml | nbsp-gba | A.2 |

## 5.2 Nbsp\_GBA Service

### 5.2.1 Service Description

This service is exposed by the GBA BSF for the purpose of providing GBA bootstrap information to an SBI-capable NAF, and GBA push information (GPI) to an SBI-capable Push-NAF, for the derivation of the application key material (e.g. Ks\_(ext/int)\_NAF). It also supports to fetch application-specific user security settings (USS) from the GBA BSF.

### 5.2.2 Service Operations

#### 5.2.2.1 Introduction

For the Nbsp\_GBA service the following service operations are defined:

- BootstrapInfo

- PushInfo

#### 5.2.2.2 BootstrapInfo

##### 5.2.2.2.1 General

This service operation is used between the SBI-capable NAF and the GBA BSF to request the key material agreed during bootstrapping from the UE to the GBA BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

##### 5.2.2.2.2 Boostrapping Info Retrieval

Figure 5.2.2.2.2-1 shows a scenario where the NF Service Consumer (e.g. the SBI-capable NAF) sends a request to the GBA BSF to receive the bootstrapping info and optionally the user security settings.



Figure 5.2.2.2.2-1: Requesting Bootstrapping Info

1. The NF Service Consumer sends a POST request (custom method "bootstrapping-info-retrieval") to the GBA BSF. The request includes the B-TID, the NAF-Id and optionally a flag to indicate that the NAF is GBA\_U aware, and a list of GAA Service Identifiers (GSID).

2a. On success the GBA BSF responds with "200 OK" and including in the message body the key material (Ks\_NAF in case of GBA\_ME and Ks\_ext\_NAF in case of GBA\_U), the key material lifetime and the bootstrapping creation time. Optionally, it may include additional key material (i.e. Ks\_int\_NAF), application-specific user security settings and the UE private identity.

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the POST response body.

In the case of redirection, the GBA BSF shall return 3xx status code, which shall contain a Location header with an URI pointing to the endpoint of another GBA BSF (service) instance.

#### 5.2.2.3 PushInfo

##### 5.2.2.3.1 General

This service operation is used between the SBI-capable Push-NAF and the GBA BSF to request the GBA Push Information (GPI) in order to bootstrap the UE with GBA key material. It is also used to fetch application-specific user security settings from the BSF, if requested by the Push-NAF.

##### 5.2.2.3.2 Push Info Retrieval

Figure 5.2.2.3.2-1 shows a scenario where the NF Service Consumer (e.g. the SBI-capable Push-NAF) sends a request to the GBA BSF to receive the bootstrapping info and optionally the user security settings.



Figure 5.2.2.3.2-1: Requesting Push Info

1. The NF Service Consumer sends a POST request (custom method "push-info-retrieval") to the GBA BSF. The request includes the User Identity (Private or Public Identity), User Identity type, UICC application identifier, Push-NAF-Id, Push-NAF SA identifier, Indicator for use of GBA\_ME or GBA\_U, Requested Push-NAF key lifetime, Private User Identity indicator, list of GAA Service Identifiers (GSID), AUTS and RAND.

2a. On success the GBA BSF responds with "200 OK" and including in the message body the GPI data, key material (Ks\_NAF in case of GBA\_ME and Ks\_ext\_NAF in case of GBA\_U), key material lifetime, application-specific user security settings. Optionally, it may include additional key material (i.e. Ks\_int\_NAF), application-specific user security settings and the UE private identity.

On failure, the appropriate HTTP status code indicating the error shall be returned and appropriate additional error information should be returned in the POST response body.

In the case of redirection, the GBA BSF shall return 3xx status code, which shall contain a Location header with an URI pointing to the endpoint of another GBA BSF (service) instance.

# 6 API Definitions

## 6.1 Nbsp\_GBA Service API

### 6.1.1 Introduction

The Nbsp\_GBA service shall use the Nbsp\_GBA API.

The API URI of the Nbsp\_GBA API shall be:

**{apiRoot}/<apiName>/<apiVersion>**

The request URIs used in HTTP requests from the NF service consumer towards the NF service producer shall have the Resource URI structure defined in clause 4.4.1 of 3GPP TS 29.501 [5], i.e.:

**{apiRoot}/<apiName>/<apiVersion>/<apiSpecificResourceUriPart>**

with the following components:

- The {apiRoot} shall be set as described in 3GPP TS 29.501 [5].

- The <apiName>shall be "nbsp-gba".

- The <apiVersion> shall be "v1".

- The <apiSpecificResourceUriPart> shall be set as described in clause 6.1.3.

### 6.1.2 Usage of HTTP

#### 6.1.2.1 General

HTTP/2, IETF RFC 9113 [11], shall be used as specified in clause 5 of 3GPP TS 29.500 [4].

HTTP/2 shall be transported as specified in clause 5.3 of 3GPP TS 29.500 [4].

The OpenAPI [6] specification of HTTP messages and content bodies for the Nbsp\_GBA API is contained in Annex A.

#### 6.1.2.2 HTTP standard headers

##### 6.1.2.2.1 General

See clause 5.2.2 of 3GPP TS 29.500 [4] for the usage of HTTP standard headers.

##### 6.1.2.2.2 Content type

JSON, IETF RFC 8259 [12], shall be used as content type of the HTTP bodies specified in the present specification as specified in clause 5.4 of 3GPP TS 29.500 [4]. The use of the JSON format shall be signalled by the content type "application/json".

"Problem Details" JSON object shall be used to indicate additional details of the error in a HTTP response body and shall be signalled by the content type "application/problem+json", as defined in IETF RFC 9457 [13].

#### 6.1.2.3 HTTP custom headers

The mandatory HTTP custom header fields specified in clause 5.2.3.2 of 3GPP TS 29.500 [4] shall be supported, and the optional HTTP custom header fields specified in clause 5.2.3.3 of 3GPP TS 29.500 [4] may be supported.

### 6.1.3 Resources

In this release of this specification, no resources are defined for the Nbsp\_GBA service.

#### 6.1.3.1 Overview

The structure of the Resource URIs of the Nbsp\_GBA service is shown in figure 6.1.3.1-1.



Figure 6.1.3.1-1: Resource URI structure of the Nbsp\_GBA API

### 6.1.4 Custom Operations without associated resources

#### 6.1.4.1 Overview

Table 6.1.4.1-1: Custom operations without associated resources

|  |  |  |  |
| --- | --- | --- | --- |
| Operation Name | Custom operation URI | Mapped HTTP method | Description |
| Bootstrapping Info Retrieval | /bootstrapping-info-retrieval | POST |  |
| Push Info Retrieval | /push-info-retrieval | POST |  |

#### 6.1.4.2 Operation: Bootstrapping Info Retrieval

##### 6.1.4.2.1 Description

##### 6.1.4.2.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 6.1.4.2.2-1 and 6.1.4.2.2-2.

Table 6.1.4.2.2-1: Data structures supported by the POST Request Body

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| BootstrappingInfoRequest | M | 1 | Request body of the Bootstrapping Info Request |

Table 6.1.4.2.2-2: Data structures supported by the POST Response Body

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| BootstrappingInfoResponse | M | 1 | 200 OK | A response body containing the BootstrappingInfoResponse shall be returned. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection.  (NOTE 2) |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection.  (NOTE 2) |
| ProblemDetails | O | 0..1 | 403 Forbidden | The NAF is not authorized to request Bootstrapping Information from the GBA BSF. |
| NOTE 1: The mandatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.  NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. | | | | |

Table 6.1.4.2.2-3: Headers supported by the 307 Response Code

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | An alternative URI of the resource located on an alternative service instance within the same GBA BSF (service) set. For the case when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4]. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance ID towards which the request is redirected. |

Table 6.1.4.2.2-4: Headers supported by the 308 Response Code

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | An alternative URI of the resource located on an alternative service instance within the same GBA BSF (service) set. For the case when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4]. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance ID towards which the request is redirected. |

#### 6.1.4.3 Operation: Push Info Retrieval

##### 6.1.4.3.1 Description

##### 6.1.4.3.2 Operation Definition

This operation shall support the response data structures and response codes specified in tables 6.1.4.3.2-1 and 6.1.4.3.2-2.

Table 6.1.4.3.2-1: Data structures supported by the POST Request Body

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| PushInfoRequest | M | 1 | Request body of the Push Info Request |

Table 6.1.4.3.2-2: Data structures supported by the POST Response Body

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Response  codes | Description |
| PushInfoResponse | M | 1 | 200 OK | A response body containing the PushInfoResponse shall be returned. |
| RedirectResponse | O | 0..1 | 307 Temporary Redirect | Temporary redirection.  (NOTE 2) |
| RedirectResponse | O | 0..1 | 308 Permanent Redirect | Permanent redirection.  (NOTE 2) |
| ProblemDetails | O | 0..1 | 403 Forbidden | The Push-NAF is not authorized to request GBA Push Information (GPI) from the GBA BSF. |
| NOTE 1: The mandatory HTTP error status code for the POST method listed in Table 5.2.7.1-1 of 3GPP TS 29.500 [4] also apply.  NOTE 2: RedirectResponse may be inserted by an SCP, see clause 6.10.9.1 of 3GPP TS 29.500 [4]. | | | | |

Table 6.1.4.3.2-3: Headers supported by the 307 Response Code

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | An alternative URI of the resource located on an alternative service instance within the same GBA BSF (service) set. For the case when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4]. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance ID towards which the request is redirected. |

Table 6.1.4.3.2-4: Headers supported by the 308 Response Code

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| Location | string | M | 1 | An alternative URI of the resource located on an alternative service instance within the same GBA BSF (service) set. For the case when a request is redirected to the same target resource via a different SCP, see clause 6.10.9.1 in 3GPP TS 29.500 [4]. |
| 3gpp-Sbi-Target-Nf-Id | string | O | 0..1 | Identifier of the target NF (service) instance ID towards which the request is redirected. |

### 6.1.5 Notifications

In this release of this specification, no notifications are defined for the Nbsp\_GBA service.

### 6.1.6 Data Model

#### 6.1.6.1 General

This clause specifies the application data model supported by the API.

Table 6.1.6.1-1 specifies the data types defined for the Nbsp\_GBA service-based interface protocol.

Table 6.1.6.1-1: Nbsp\_GBA specific Data Types

|  |  |  |
| --- | --- | --- |
| Data type | Clause defined | Description |
| BootstrappingInfoRequest | 6.1.6.2.2 | Request body of the HTTP POST operation for resource "/bootstrapping-info-request". |
| BootstrappingInfoResponse | 6.1.6.2.3 | Response body of the HTTP POST operation for resource "/bootstrapping-info-request". |
| PushInfoRequest | 6.1.6.2.4 | Request body of the HTTP POST operation for resource "/push-info-request". |
| PushInfoResponse | 6.1.6.2.5 | Response body of the HTTP POST operation for resource "/push-info-request". |
| NafId | 6.1.6.2.6 | NAF ID, containing the NAF FQDN and the Ua Security Protocol Identifier. |
| UssListItem | 6.1.6.2.7 | Data item in a User Security Settings array list. |
| Uss | 6.1.6.2.8 | User Security Settings for a given GAA Service. |
| UeIdsItem | 6.1.6.2.9 | Data item in a UE ID array list. |
| FlagsItem | 6.1.6.2.10 | Data item in a Flags array list. |
| GsId | 6.1.6.3.2 | GAA Service Identifier. |
| GsType | 6.1.6.3.2 | GAA Service Type. |
| BtId | 6.1.6.3.2 | Bootstrapping Transaction Identifier. |
| MeKeyMaterial | 6.1.6.3.2 | ME Key Material (hex-encoded string). |
| UiccKeyMaterial | 6.1.6.3.2 | UICC key material (hex-encoded string). |
| UeId | 6.1.6.3.2 | Public Identity of the UE. |
| Impi | 6.1.6.3.2 | IMS Private Identity of the UE |
| Flag | 6.1.6.3.2 | GAA authorization flags, as defined in 3GPP TS 29.109 [17], Annex C. |
| GbaPushInfo | 6.1.6.3.2 | GBA Push Info (hex-encoded string). |
| NafGroup | 6.1.6.3.2 | NAF Group (string). |
| PtId | 6.1.6.3.2 | P-TID. |
| UiccAppLabel | 6.1.6.3.2 | UICC Application Label (string). |
| Auts | 6.1.6.3.2 | AUTS in UMTS AKA. |
| Rand | 6.1.6.3.2 | RAND in UMTS AKA. |
| KeyChoice | 6.1.6.3.3 | Type of key (ME-based or UICC-based) that the NAF shall use. |
| UiccOrMe | 6.1.6.3.4 | Indicates whether GBA\_ME or GBA\_U is to be used for GBA push. |
| SecFeature | 6.1.6.3.5 | Security features supported by the BSF or the NAF. |
| GbaType | 6.1.6.3.6 | Authentication type used by the UE for GBA. |
| UeIdType | 6.1.6.3.7 | Type of UE Identity (public or private). |

Table 6.1.6.1-2 specifies data types re-used by the Nbsp\_GBA service-based interface protocol from other specifications, including a reference to their respective specifications and when needed, a short description of their use within the Nbsp\_GBA service-based interface.

Table 6.1.6.1-2: Nbsp\_GBA re-used Data Types

|  |  |  |
| --- | --- | --- |
| Data type | Reference | Comments |
| Uint32 | 3GPP TS 29.571 [18] | Unsigned 32-bit integer. |
| DateTime | 3GPP TS 29.571 [18] | String with a "date-time" format, as defined by OpenAPI [6]. |
| ProblemDetails | 3GPP TS 29.571 [18] | Response body of error response messages. |
| RedirectResponse | 3GPP TS 29.571 [18] | Response body of a redirect response message. |
| Fqdn | 3GPP TS 29.571 [18] | Fully Qualified Domain Name |

#### 6.1.6.2 Structured data types

##### 6.1.6.2.1 Introduction

This clause defines the structures to be used in resource representations.

##### 6.1.6.2.2 Type: BootstrappingInfoRequest

Table 6.1.6.2.2-1: Definition of type BootstrappingInfoRequest

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| btId | BtId | M | 1 | Bootstrapping Transaction Identifier |
| nafId | NafId | M | 1 | NAF Identifier |
| gbaUAware | boolean | O | 0..1 | GBA-U Awareness Indicator.  true: The sending node is GBA\_U aware  false (default) or absent: The sending node is not GBA\_U aware. |
| gsIds | array(GsId) | O | 1..N | GBA Service Identifiers |

##### 6.1.6.2.3 Type: BootstrappingInfoResponse

Table 6.1.6.2.3-1: Definition of type BootstrappingInfoResponse

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| meKeyMaterial | MeKeyMaterial | M | 1 | ME key material (Ks\_NAF or Ks\_Ext\_NAF) |
| uiccKeyMaterial | UiccKeyMaterial | O | 0..1 | UICC key material (Ks\_Int\_NAF) |
| keyExpiryTime | DateTime | O | 0..1 | Key expiry time |
| bootstrappingInfoCreationTime | DateTime | O | 0..1 | Bootstrapping Info Creation Time |
| ussList | array(UssListItem) | O | 1..N | GBA User Security Settings per GBA Service Identifier |
| gbaType | GbaType | O | 0..1 | Authentication type that was used by the UE during the bootstrapping procedure. |
| impi | Impi | O | 0..1 | UE Private Identity |

##### 6.1.6.2.4 Type: PushInfoRequest

Table 6.1.6.2.4-1: Definition of type PushInfoRequest

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| ueId | UeId | M | 1 | User Identity. |
| ueIdType | UeIdType | M | 1 | Type of UE identity (public or private). |
| uiccAppLabel | UiccAppLabel | M | 1 | UICC Application Label. |
| nafId | NafId | M | 1 | NAF Identifier. |
| ptId | PtId | M | 1 | P-TID (NAF SA Identifier). |
| uiccOrMe | UiccOrMe | M | 1 | Indicates whether GBA\_ME or GBA\_U is to be used for GBA push. |
| requestedLifeTime | DateTime | M | 1 | Requested key lifetime for the NAF keys. |
| privateIdRequest | boolean | O | 0..1 | Indicates to the BSF whether the UE private identity shall be returned to the NAF in the response message.  true: the private identity is requested by the NAF, and it shall be returned by the BSF.  false (default) or absent: the private identity is not requested by the NAF. |
| gbaUAware | boolean | O | 0..1 | GBA-U Awareness Indicator.  true: The sending node is GBA\_U aware  false (default) or absent: The sending node is not GBA\_U aware. |
| gsIds | array(GsId) | O | 1..N | GBA Service Identifiers. |
| auts | Auts | O | 0..1 | AUTS in UMTS AKA. |
| rand | Rand | O | 0..1 | RAND in UMTS AKA. |
| securityFeaturesRequest | array(SecFeature) | O | 1..N | Security Features supported by the NAF. |

##### 6.1.6.2.5 Type: PushInfoResponse

Table 6.1.6.2.5-1: Definition of type PushInfoResponse

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| meKeyMaterial | MeKeyMaterial | M | 1 | ME key material (Ks\_NAF or Ks\_Ext\_NAF). |
| gbaPushInfo | GbaPushInfo | M | 1 | GBA Push Info |
| uiccKeyMaterial | UiccKeyMaterial | O | 0..1 | UICC key material (Ks\_Int\_NAF). |
| keyExpiryTime | DateTime | O | 0..1 | Key expiry time. |
| bootstrappingInfoCreationTime | DateTime | O | 0..1 | Bootstrapping Info Creation Time. |
| ussList | array(UssListItem) | O | 1..N | GBA User Security Settings per GBA Service Identifier |
| gbaType | GbaType | O | 0..1 | GBA Type. |
| impi | Impi | O | 0..1 | UE Private Identity. |
| securityFeaturesResponse | array(SecFeature) | O | 0..N | If the BSF does not support the usage of securityFeatures or the NAF did not include any securityFeaturesRequest attribute in the PushInfoRequest message, this IE shall be absent.  If securityFeatures element is not defined in the GUSS of the UE, or there is no common securityFeature between NAF and BSF, the BSF shall include an empty array in the securityFeaturesResponse attribute. |

##### 6.1.6.2.6 Type: NafId

Table 6.1.6.2.6-1: Definition of type NafId

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| nafFqdn | Fqdn | M | 1 | FQDN of the NAF. |
| uaSecProtId | string | M | 1 | Ua Security Protocol Identifier.  It shall contain 5 octets, as described in 3GPP TS 33.220 [14], encoded as a sequence of 10 hexadecimal characters.  pattern: "^[A-Fa-f0-9]{10}$" |

##### 6.1.6.2.7 Type: UssListItem

Table 6.1.6.2.7-1: Definition of type UssListItem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| uss | Uss | M | 1 | User Security Settings. |

##### 6.1.6.2.8 Type: Uss

Table 6.1.6.2.8-1: Definition of type Uss

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| gsId | GsId | M | 1 | GAA Service ID. |
| gsType | GsType | M | 1 | GAA Service Type. |
| ueIds | array(UeIdsItem) | M | 1..N | List of UE Identities |
| nafGroup | NafGroup | O | 0..1 | NAF Group. |
| flags | array(FlagsItem) | O | 1..N | List of security flags supported for the current GAA service. |
| keyChoice | KeyChoice | O | 0..1 | Type of key that the NAF shall use. |

##### 6.1.6.2.9 Type: UeIdsItem

Table 6.1.6.2.9-1: Definition of type UeIdsItem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| ueId | UeId | M | 1 | Identity of the UE |

##### 6.1.6.2.10 Type: FlagsItem

Table 6.1.6.2.10-1: Definition of type FlagsItem

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| flag | Flag | M | 1 | Security flag supported for the corresponding GAA Service. |

#### 6.1.6.3 Simple data types and enumerations

##### 6.1.6.3.1 Introduction

This clause defines simple data types and enumerations that can be referenced from data structures defined in the previous clauses.

##### 6.1.6.3.2 Simple data types

The simple data types defined in table 6.1.6.3.2-1 shall be supported.

Table 6.1.6.3.2-1: Simple data types

|  |  |  |
| --- | --- | --- |
| Type Name | Type Definition | Description |
| GsId | Uint32 | GAA Service Identifier.  For 3GPP standardized values, see 3GPP TS 29.109 [17], Annex B. |
| GsType | Uint32 | GAA Service Type.  For 3GPP standardized values, see 3GPP TS 29.109 [17], Annex B. |
| BtId | string | Bootstrapping Transaction Identifier. It shall take the form of a NAI, where the realm part identifies the FQDN of the BSF. See 3GPP TS 33.220 [14]. |
| MeKeyMaterial | string | ME key material, containing a 256-bit key, encoded as a sequence of 64 hexadecimal characters.  pattern: "^[A-Fa-f0-9]{64}$" |
| UiccKeyMaterial | string | UICC key material, containing a 256-bit key, encoded as a sequence of 64 hexadecimal characters.  pattern: "^[A-Fa-f0-9]{64}$" |
| UeId | string | Identity of the UE. |
| Impi | string | IMS Private Identity of the UE. |
| Flag | Uint32 | GAA authorization flags, associated to the specific GAA Service Type, as defined in 3GPP TS 29.109 [17], Annex C. |
| GbaPushInfo | string | GBA Push Info binary data, as defined in 3GPP TS 33.223 [15], clause 5.3.5, encoded as a sequence of hexadecimal characters.  pattern: "^([A-Fa-f0-9]{2})+$" |
| NafGroup | string | NAF Group. |
| PtId | string | P-TID. |
| UiccAppLabel | string | UICC Application Label. |
| Auts | string | AUTS in UMTS AKA, containing a 112-bit value, encoded as a sequence of 28 hexadecimal characters.  pattern: "^[A-Fa-f0-9]{28}$" |
| Rand | string | RAND in UMTS AKA, containing a 128-bit value, encoded as a sequence of 32 hexadecimal characters.  pattern: "^[A-Fa-f0-9]{32}$" |

##### 6.1.6.3.3 Enumeration: KeyChoice

The enumeration KeyChoice represents the type of key that the NAF shall use. It shall comply with the provisions defined in table 6.1.6.3.3-1.

Table 6.1.6.3.3-1: Enumeration KeyChoice

|  |  |
| --- | --- |
| Enumeration value | Description |
| "ME\_BASED\_KEY" | Ks\_ NAF or Ks\_ext\_NAF shall be used by the NAF. |
| "UICC\_BASED\_KEY" | Ks\_int\_NAF shall be used by the NAF. |
| "ME\_UICC\_BASED\_KEYS" | Ks\_ext\_NAF or Ks\_int\_NAF can be used by the NAF. |

##### 6.1.6.3.4 Enumeration: UiccOrMe

The enumeration UiccOrMe represents whether GBA\_ME or GBA\_U is to be used for GBA push. It shall comply with the provisions defined in table 6.1.6.3.4-1.

Table 6.1.6.3.4-1: Enumeration UiccOrMe

|  |  |
| --- | --- |
| Enumeration value | Description |
| "GBA\_ME" | GBA\_ME shall be used. |
| "GBA\_U" | GBA\_U shall be used. |

##### 6.1.6.3.5 Enumeration: SecFeature

The enumeration SecFeature represents security features supported by the BSF or the NAF. It shall comply with the provisions defined in table 6.1.6.3.5-1.

Table 6.1.6.3.5-1: Enumeration SecFeature

|  |  |
| --- | --- |
| Enumeration value | Description |
| "GPL\_U" | The UICC supports Generic Push Layer, as specified in 3GPP TS 33.224 [16]. |

##### 6.1.6.3.6 Enumeration: GbaType

The enumeration GbaType represents the authentication type that was used during bootstrapping procedure. It shall comply with the provisions defined in table 6.1.6.3.6-1.

Table 6.1.6.3.6-1: Enumeration GbaType

|  |  |
| --- | --- |
| Enumeration value | Description |
| "3G\_GBA" | The 3G GBA has been performed as defined in 3GPP TS 33.220 [14]. |
| "2G\_GBA" | The 2G GBA has been performed as defined in 3GPP TS 33.220 [14], Annex I. |
| "GBA\_DIGEST" | The GBA Digest has been performed as defined in 3GPP TS 33.220 [14], Annex M. |

##### 6.1.6.3.7 Enumeration: UeIdType

The enumeration UeIdType represents the type of the identity of the user. It shall comply with the provisions defined in table 6.1.6.3.7-1.

Table 6.1.6.3.7-1: Enumeration UeIdType

|  |  |
| --- | --- |
| Enumeration value | Description |
| "PUBLIC" | Public user identity. |
| "PRIVATE" | Private user identity. |

### 6.1.7 Error Handling

#### 6.1.7.1 General

For the Nbsp\_GBA API, HTTP error responses shall be supported as specified in clause 4.8 of 3GPP TS 29.501 [5]. Protocol errors and application errors specified in table 5.2.7.2-1 of 3GPP TS 29.500 [4] shall be supported for an HTTP method if the corresponding HTTP status codes are specified as mandatory for that HTTP method in table 5.2.7.1-1 of 3GPP TS 29.500 [4].

In addition, the requirements in the following clauses are applicable for the Nbsp\_GBA API.

#### 6.1.7.2 Protocol Errors

No specific procedures for the Nbsp\_GBA service are specified.

#### 6.1.7.3 Application Errors

The application errors defined for the Nbsp\_GBA service are listed in Table 6.1.7.3-1.

Table 6.1.7.3-1: Application errors

|  |  |  |
| --- | --- | --- |
| Application Error | HTTP status code | Description |
|  |  |  |

### 6.1.8 Feature negotiation

The optional features in table 6.1.8-1 are defined for the Nbsp\_GBA API. They shall be negotiated using the extensibility mechanism defined in clause 6.6 of 3GPP TS 29.500 [4].

Table 6.1.8-1: Supported Features

|  |  |  |
| --- | --- | --- |
| Feature number | Feature Name | Description |
|  |  |  |

### 6.1.9 Security

As indicated in 3GPP TS 33.501 [8] and 3GPP TS 29.500 [4], the access to the Nbsp\_GBA API may be authorized by means of the OAuth2 protocol (see IETF RFC 6749 [9]), based on local configuration, using the "Client Credentials" authorization grant, where the NRF (see 3GPP TS 29.510 [10]) plays the role of the authorization server.

If OAuth2 is used, an NF Service Consumer, prior to consuming services offered by the Nbsp\_GBA API, shall obtain a "token" from the authorization server, by invoking the Access Token Request service, as described in 3GPP TS 29.510 [10], clause 5.4.2.2.

NOTE: When multiple NRFs are deployed in a network, the NRF used as authorization server is the same NRF that the NF Service Consumer used for discovering the Nbsp\_GBA service.

The Nbsp\_GBA API defines the following scopes for OAuth2 authorization:

Table 6.1.9-1: Oauth2 scopes defined in Nbsp\_GBA API

|  |  |
| --- | --- |
| Scope | Description |
| "nbsp-gba" | Access to the Nbsp\_GBA API |
| "nbsp-gba:bootstrapping-info-retrieval:invoke" | Access to invoke the Bootstrapping Info Retrieval custom operation |
| "nbsp-gba:push-info-retrieval:invoke" | Access to invoke the Push Info Retrieval custom operation |

Annex A (normative):  
OpenAPI specification

# A.1 General

This Annex specifies the formal definition of the API(s) defined in the present specification. It consists of OpenAPI 3.0.0 specifications in YAML format.

This Annex takes precedence when being discrepant to other parts of the specification with respect to the encoding of information elements and methods within the API(s).

NOTE 1: The semantics and procedures, as well as conditions, e.g. for the applicability and allowed combinations of attributes or values, not expressed in the OpenAPI definitions but defined in other parts of the specification also apply.

Informative copies of the OpenAPI specification files contained in this 3GPP Technical Specification are available on a Git-based repository that uses the GitLab software version control system (see 3GPP TS 29.501 [5] clause 5.3.1 and 3GPP TR 21.900 [7] clause 5B).

# A.2 Nbsp\_GBA API

openapi: 3.0.0

info:

version: '1.1.0'

title: 'GBA BSF Nbsp\_GBA Service'

description: |

GBA BSF Nbsp\_GBA Service.

© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

externalDocs:

description: >

3GPP TS 29.309 V18.2.0; 5G System; Bootstrapping Server Function (GBA BSF) Services; Stage 3

url: 'https://www.3gpp.org/ftp/Specs/archive/29\_series/29.309/'

servers:

- url: '{apiRoot}/nbsp-gba/v1'

variables:

apiRoot:

default: https://example.com

description: apiRoot as defined in clause 4.4 of 3GPP TS 29.501

security:

- {}

- oAuth2ClientCredentials:

- nbsp-gba

paths:

/bootstrapping-info-retrieval:

post:

summary: Retrieve Bootstrapping Info from GBA BSF from NAF

operationId: BootstrappingInfoRetrieval

tags:

- Bootstrapping Info Retrieval (Custom Operation)

security:

- {}

- oAuth2ClientCredentials:

- nbsp-gba

- oAuth2ClientCredentials:

- nbsp-gba

- nbsp-gba:bootstrapping-info-retrieval:invoke

requestBody:

content:

application/json:

schema:

$ref: '#/components/schemas/BootstrappingInfoRequest'

required: true

responses:

'200':

description: Expected response to a valid request

content:

application/json:

schema:

$ref: '#/components/schemas/BootstrappingInfoResponse'

'307':

$ref: 'TS29571\_CommonData.yaml#/components/responses/307'

'308':

$ref: 'TS29571\_CommonData.yaml#/components/responses/308'

'400':

$ref: 'TS29571\_CommonData.yaml#/components/responses/400'

'401':

$ref: 'TS29571\_CommonData.yaml#/components/responses/401'

'403':

$ref: 'TS29571\_CommonData.yaml#/components/responses/403'

'404':

$ref: 'TS29571\_CommonData.yaml#/components/responses/404'

'411':

$ref: 'TS29571\_CommonData.yaml#/components/responses/411'

'413':

$ref: 'TS29571\_CommonData.yaml#/components/responses/413'

'415':

$ref: 'TS29571\_CommonData.yaml#/components/responses/415'

'429':

$ref: 'TS29571\_CommonData.yaml#/components/responses/429'

'500':

$ref: 'TS29571\_CommonData.yaml#/components/responses/500'

'501':

$ref: 'TS29571\_CommonData.yaml#/components/responses/501'

'503':

$ref: 'TS29571\_CommonData.yaml#/components/responses/503'

default:

$ref: 'TS29571\_CommonData.yaml#/components/responses/default'

/push-info-retrieval:

post:

summary: Retrieve Push Info from GBA BSF from Push-NAF

operationId: PushInfoRetrieval

tags:

- Push Info Retrieval (Custom Operation)

security:

- {}

- oAuth2ClientCredentials:

- nbsp-gba

- oAuth2ClientCredentials:

- nbsp-gba

- nbsp-gba:push-info-retrieval:invoke

requestBody:

content:

application/json:

schema:

$ref: '#/components/schemas/PushInfoRequest'

required: true

responses:

'200':

description: Expected response to a valid request

content:

application/json:

schema:

$ref: '#/components/schemas/PushInfoResponse'

'307':

$ref: 'TS29571\_CommonData.yaml#/components/responses/307'

'308':

$ref: 'TS29571\_CommonData.yaml#/components/responses/308'

'400':

$ref: 'TS29571\_CommonData.yaml#/components/responses/400'

'401':

$ref: 'TS29571\_CommonData.yaml#/components/responses/401'

'403':

$ref: 'TS29571\_CommonData.yaml#/components/responses/403'

'404':

$ref: 'TS29571\_CommonData.yaml#/components/responses/404'

'411':

$ref: 'TS29571\_CommonData.yaml#/components/responses/411'

'413':

$ref: 'TS29571\_CommonData.yaml#/components/responses/413'

'415':

$ref: 'TS29571\_CommonData.yaml#/components/responses/415'

'429':

$ref: 'TS29571\_CommonData.yaml#/components/responses/429'

'500':

$ref: 'TS29571\_CommonData.yaml#/components/responses/500'

'501':

$ref: 'TS29571\_CommonData.yaml#/components/responses/501'

'503':

$ref: 'TS29571\_CommonData.yaml#/components/responses/503'

default:

$ref: 'TS29571\_CommonData.yaml#/components/responses/default'

components:

securitySchemes:

oAuth2ClientCredentials:

type: oauth2

flows:

clientCredentials:

tokenUrl: '{nrfApiRoot}/oauth2/token'

scopes:

nbsp-gba: Access to the Nbsp\_GBA API

nbsp-gba:bootstrapping-info-retrieval:invoke: >-

Access to invoke the Bootstrapping Info Retrieval custom operation

nbsp-gba:push-info-retrieval:invoke: >-

Access to invoke the Push Info Retrieval custom operation

schemas:

#

# STRUCTURED TYPES

#

BootstrappingInfoRequest:

description: >

Request body of the HTTP POST operation for resource /bootstrapping-info-request

type: object

required:

- btId

- nafId

properties:

btId:

$ref: '#/components/schemas/BtId'

nafId:

$ref: '#/components/schemas/NafId'

gbaUAware:

type: boolean

default: false

gsIds:

type: array

items:

$ref: '#/components/schemas/GsId'

minItems: 1

BootstrappingInfoResponse:

description: >

Response body of the HTTP POST operation for resource /bootstrapping-info-request

type: object

required:

- meKeyMaterial

properties:

meKeyMaterial:

$ref: '#/components/schemas/MeKeyMaterial'

uiccKeyMaterial:

$ref: '#/components/schemas/UiccKeyMaterial'

keyExpiryTime:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/DateTime'

bootstrappingInfoCreationTime:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/DateTime'

ussList:

type: array

items:

$ref: '#/components/schemas/UssListItem'

minItems: 1

gbaType:

$ref: '#/components/schemas/GbaType'

impi:

$ref: '#/components/schemas/Impi'

PushInfoRequest:

description: Request body of the HTTP POST operation for resource /push-info-request

type: object

required:

- ueId

- ueIdType

- uiccAppLabel

- nafId

- ptId

- uiccOrMe

- requestedLifeTime

properties:

ueId:

$ref: '#/components/schemas/UeId'

ueIdType:

$ref: '#/components/schemas/UeIdType'

uiccAppLabel:

$ref: '#/components/schemas/UiccAppLabel'

nafId:

$ref: '#/components/schemas/NafId'

ptId:

$ref: '#/components/schemas/PtId'

uiccOrMe:

$ref: '#/components/schemas/UiccOrMe'

requestedLifeTime:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/DateTime'

privateIdRequest:

type: boolean

default: false

gbaUAware:

type: boolean

default: false

gsIds:

type: array

items:

$ref: '#/components/schemas/GsId'

minItems: 1

auts:

$ref: '#/components/schemas/Auts'

rand:

$ref: '#/components/schemas/Rand'

securityFeaturesRequest:

type: array

items:

$ref: '#/components/schemas/SecFeature'

minItems: 1

PushInfoResponse:

description: Response body of the HTTP POST operation for resource /push-info-request

type: object

required:

- meKeyMaterial

- gbaPushInfo

properties:

meKeyMaterial:

$ref: '#/components/schemas/MeKeyMaterial'

gbaPushInfo:

$ref: '#/components/schemas/GbaPushInfo'

uiccKeyMaterial:

$ref: '#/components/schemas/UiccKeyMaterial'

keyExpiryTime:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/DateTime'

bootstrappingInfoCreationTime:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/DateTime'

ussList:

type: array

items:

$ref: '#/components/schemas/UssListItem'

minItems: 1

gbaType:

$ref: '#/components/schemas/GbaType'

impi:

$ref: '#/components/schemas/Impi'

securityFeaturesResponse:

type: array

items:

$ref: '#/components/schemas/SecFeature'

NafId:

description: NAF ID, containing the NAF FQDN and the Ua Security Protocol Identifier

type: object

required:

- nafFqdn

- uaSecProtId

properties:

nafFqdn:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Fqdn'

uaSecProtId:

type: string

pattern: '^[A-Fa-f0-9]{10}$'

UssListItem:

description: Data item in a User Security Settings array list

type: object

required:

- uss

properties:

uss:

$ref: '#/components/schemas/Uss'

Uss:

description: User Security Settings for a given GAA Service

type: object

required:

- gsId

- gsType

- ueIds

properties:

gsId:

$ref: '#/components/schemas/GsId'

gsType:

$ref: '#/components/schemas/GsType'

ueIds:

type: array

items:

$ref: '#/components/schemas/UeIdsItem'

minItems: 1

nafGroup:

$ref: '#/components/schemas/NafGroup'

flags:

type: array

items:

$ref: '#/components/schemas/FlagsItem'

minItems: 1

keyChoice:

$ref: '#/components/schemas/KeyChoice'

UeIdsItem:

description: Data item in a UE ID array list

type: object

required:

- ueId

properties:

ueId:

$ref: '#/components/schemas/UeId'

FlagsItem:

description: Data item in a Flags array list

type: object

required:

- flag

properties:

flag:

$ref: '#/components/schemas/Flag'

#

# SIMPLE TYPES

#

GsId:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uint32'

GsType:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uint32'

BtId:

description: Bootstrapping Transaction Identifier

type: string

MeKeyMaterial:

description: ME Key Material (hex-encoded string)

type: string

pattern: '^[A-Fa-f0-9]{64}$'

UiccKeyMaterial:

description: UICC key material (hex-encoded string)

type: string

pattern: '^[A-Fa-f0-9]{64}$'

UeId:

description: Public Identity of the UE

type: string

Impi:

description: IMS Private Identity of the UE

type: string

Flag:

$ref: 'TS29571\_CommonData.yaml#/components/schemas/Uint32'

GbaPushInfo:

description: GBA Push Info (hex-encoded string)

type: string

pattern: '^([A-Fa-f0-9]{2})+$'

NafGroup:

description: Character string representing a NAF Group

type: string

PtId:

description: Character string representing a P-TID

type: string

UiccAppLabel:

description: Character string representing an UICC Application Label

type: string

Auts:

description: AUTS value in UMTS AKA

type: string

pattern: '^[A-Fa-f0-9]{28}$'

Rand:

description: RAND in UMTS AKA

type: string

pattern: '^[A-Fa-f0-9]{32}$'

#

# ENUMS

#

KeyChoice:

description: Type of key (ME-based or UICC-based) that the NAF shall use

anyOf:

- type: string

enum:

- ME\_BASED\_KEY

- UICC\_BASED\_KEY

- ME\_UICC\_BASED\_KEYS

- type: string

UiccOrMe:

description: Indicates whether GBA\_ME or GBA\_U is to be used for GBA push

anyOf:

- type: string

enum:

- GBA\_ME

- GBA\_U

- type: string

SecFeature:

description: Security features supported by the BSF or the NAF

anyOf:

- type: string

enum:

- GPL\_U

- type: string

GbaType:

description: Authentication type used by the UE for GBA

anyOf:

- type: string

enum:

- 3G\_GBA

- 2G\_GBA

- GBA\_DIGEST

- type: string

UeIdType:

description: Type of UE Identity (public or private)

anyOf:

- type: string

enum:

- PUBLIC

- PRIVATE

- type: string

Annex B (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-02 | CT4#102 | C4-211396 |  |  |  | TS template agreed | 0.0.0 |
| 2021-04 | CT4#103 | C4-212594 |  |  |  | Incorporation of agreed pCRs from CT4#103: C4-212527, C4-212528, C4-212529 | 0.1.0 |
| 2021-05 | CT4#104 | C4-213524 |  |  |  | Incorporation of agreed pCRs from CT4#104: C4-213293, C4-213316 | 0.2.0 |
| 2021-09 | CT4#105 | C4-214751 |  |  |  | Incorporation of agreed pCRs from CT4#105: C4-214340, C4-214341 | 0.3.0 |
| 2021-10 | CT4#106 | C4-215515 |  |  |  | Incorporation of agreed pCRs from CT4#106: C4-215330 | 0.4.0 |
| 2021-12 | CT#94 | CP-213154 |  |  |  | V1.0.0. presented for information | 1.0.0 |
| 2022-03 | CT4#108 | C4-221637 |  |  |  | Incorporation of agreed pCRs from CT4#108: C4-221174, C4-221355 | 1.1.0 |
| 2022-03 | CT#95 | CP-220101 |  |  |  | TS presented for information | 2.0.0 |
| 2022-03 | CT#95 |  |  |  |  | TS approved | 17.0.0 |
| 2022-06 | CT#96 | CP-221032 | 0001 | - | F | Fqdn Data Type Definition | 17.1.0 |
| 2022-06 | CT#96 | CP-221051 | 0002 | - | F | 29.309 Rel-17 API version and External doc update | 17.1.0 |
| 2023-09 | CT#101 | CP-232033 | 0005 | - | B | OAuth2 scopes in the Nbsp\_GBA API | 18.0.0 |
| 2023-09 | CT#101 | CP-232060 | 0006 | - | F | 29.309 Rel-18 API version and External doc update | 18.0.0 |
| 2023-12 | CT#102 | CP-233028 | 0007 | 1 | F | Default values of privateIdRequest and gbaUAware | 18.1.0 |
| 2023-12 | CT#102 | CP-233027 | 0008 | - | F | Location header description | 18.1.0 |
| 2023-12 | CT#102 | CP-233028 | 0009 | 1 | B | HTTP RFCs obsoleted by IETF RFC 9110, 9111 and 9113 | 18.1.0 |
| 2023-12 | CT#102 | CP-233029 | 0010 | 2 | F | ProblemDetails RFC 7807 obsoleted by 9457 | 18.1.0 |
| 2023-12 | CT#102 | CP-233030 | 0011 | - | F | Editorial and Style Corrections | 18.1.0 |
| 2023-12 | CT#102 | CP-233060 | 0012 | - | F | 29.309 Rel-18 API version and External doc update | 18.1.0 |
| 2024-06 | CT#104 | CP-241052 | 0013 | - | F | 29.309 Rel18 API version and External doc update | 18.2.0 |