**3GPP TSG-SA3 Meeting #105-e *S3-214450 rev of S3-214251***

e-meeting, 8 - 19 November 2021

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Living document for GBA\_5G: draftCR to TS 33.223: SBA support for Zpn | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SBI capable BSF, HSS, Push-NAF do not exist in 5G. Therefore the Generic Boostrapping Architecture (GBA) Push cannot operate in 5G core networks.  For supporting GBA Push in the Service Based Archtiecture, the legacy interfaces Zpn and Zh need to be specified for a SBI capable BSF and an SBI capable HSS respectively. An interface for the UDM is also needed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The CR includes the following changes  - Service Based Architecture for GBA Push  - Reference point architecture for GBA Push  - Specification of a service based interface for an SBI capable Push-NAF towards an SBI capable BSF corresponding to the Zpn interface in legacy GBA  - Relevant selection and discovery clauses for an SBI capable BSF, SBI capable HSS and UDM.  - Roaming considerations | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No support for GBA Push in 5G | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, Annex X (new), X.1 (new), X.1.1 (new), X.1.2 (new), X.1.3 (new), X.1.4 (new), X.2 (new), X.2.1 (new), X.2.1(new), X.2.1.2 (new), X.2.1.2.1 (new), X.2.1.2.2 (new), X.2.2 (new), X.2.2.1 (new), X.2.2.2 (new), X.2.2.3 (new), X.2.3 (new), X.2.4 (new), X.2.4.1 (new), X.2.4.2 (new), X.3 (new), X.3.1 (new), X.3.2 (new), X.3.3 (new), X.3.4 (new). | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

**\*\*\*\*** 1st CHANGE **\*\*\*\***

# 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 TS 33.220: "Generic Authentication Architecture (GAA); Generic bootstrapping architecture".

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] 3GPP TS 33.210: "3G Security; Network Domain Security; IP network layer security".

[4] Void

[5] Void.

[6] 3GPP TS 33.102: "3G Security; Security architecture".

[7] FIPS PUB 180-2 (2002): "Secure Hash Standard".

[8] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".

[9] ISO/IEC 10118-3:2004: "Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[10] NIST Special Publication 800-38A: "Recommendation for Block Cipher Modes of Operation"

[11] FIPS PUB 197: "Advanced Encryption Standard"

[12] Void

[13] 3GPP TS 33.222 "Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[14] 3GPP TS 29.109 "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[15] 3GPP TS 33.224 "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer".

[15] 3GPP TS 31.101 "UICC-terminal interface; Physical and logical characteristics".

[16] IETF RFC 4330: "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI".

[XY] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[XZ] 3GPP TS 23.501: " System architecture for the 5G System (5GS)"

**\*\*\*\*** 2nd CHANGE **\*\*\*\***

# Annex X (normative): Support of SBA in GBA Push

## X.1 General

### X.1.1 Overview

This Annex X describes support for SBA for GBA Push.

### X.1.2 Architectural Support

Figure X.1.1-1 shows the non-roaming architecture to support SBA interactions in GBA. An SBI capable BSF, HSS and Push-NAF shall implement the SBA interfaces specified in this Annex. An SBI capable NF can invoke SBA services provided by SBI capable NFs and may expose services itself. For this Annex an SBI capable BSF uses and provides SBA services, an SBI capable HSS provides SBA services, a UDM provides SBA service, while an SBI capable Push-NAF only uses SBA services. The BSF, HSS, UDM and Push-NAF reside in the home network.

If there is no HSS or if the HSS does not support the N65 and Zh reference points within the GBA architecture, then the BSF shall be configured to use the N68 reference point with the UDM. If the N65 or Zh reference point is available in the HSS, then it shall be used between the BSF and the HSS.



Figure X.1.2-1: System Architecture to support SBA in GBA

Figure X.1.2-2 shows the architecture using the reference point representation. It should be observed that this annex address only the specification of the N65 (between the BSF and HSS), N68 (between the BSF and UDM) and N67 (between the Push-NAF and BSF) reference point interfaces as SBA interfaces. The specification of Upa and Ub is not impacted by the introduction of the SBA interfaces between the Push-NAF, BSF and HSS or UDM. Therefore, the BSF and Push-NAF are exposed to the UE as in the legacy GBA case.



Figure X.1.2-2: System Architecture to support SBA in reference point representation

With respect to roaming, the roaming requirements in clause 4.4.3 and the Zn-Proxy architecture in clause 4.1 are applicable for the case of SBA GBA Push.

In addition, the following requirements shall be followed in roaming scenarios:

- The SBI capable Push-NAF shall support the legacy Zpn interface towards the Zn-Proxy.

- An SBI capable BSF shall support the legacy Zpn' interface.

### X.1.3 Reference point to support SBA in GBA Push

The following reference points are realized by service-based interfaces in GBA:

**N65:** Reference point between an SBI capable BSF and an SBI capable HSS. The SBA interface of the N65 reference point is specified in TS 33.220 [1].

**N67**: Reference point between an SBI capable BSF and an SBI capable Push-NAF, i.e. a Push-NAF that supports an SBI interface towards the an SBI capable BSF.

**N68**: Reference point between an SBI capable BSF and a UDM.

### X.1.4 Service based interface to support SBA in GBA Push

The following service-based interfaces are defined or reused:

**Nhss**: Service-based interface exhibited by an SBI capable HSS.

**Nbsp**: Service-based interface exhibited by an SBI capable BSF.

**Nudm**: Service-based interface exhibited by a UDM.

These SBI services provide equivalent functionality to the Diameter Zh and Zpn reference points. The specification of the Nhss interface is in TS 33.220 [1].

To support co-existence of GBA nodes supporting SBA services and GBA nodes not supporting SBA services SBI capable GBA nodes may support both SBI and non-SBI interfaces.

## X.2 GAA/GBA Push SBA Services

### X.2.1 BSF Services

#### X.2.1.1 General

The following table shows the services exposed by an SBI capable BSF.

Table X.2.1.1-1: GBA Services provided by an SBI capable BSF

|  |  |  |  |
| --- | --- | --- | --- |
| Service | Service Operations | Operation Semantics | Example Consumer(s) |
| Nbsp\_Gba | PushInfo | Request/Response | Push-NAF |

#### X.2.1.2 Nbsp\_Gba service

##### X.2.1.2.1 General

This clause describes the SBA interfaces exposed by the BSF for the purpose of providing the GBA Push Information (GPI) information to the Push-NAF.The GBA Push Information (GPI) data type used in the Nbsp\_Gba service is defined in clause 5.2.1.

##### X.2.1.2.2 Nbsp\_Gba\_PushInfo service operation

**Service operation name:** Nbsp\_Gba\_PushInfo

**Description:** This service operation is used between the Push-NAF and the 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.

**Inputs, Required:**, 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 Global Service Identifiers (for USS information), AUTS, RAND.

**Inputs, Optional:** None.

**Outputs, Required:**. GPI data, key material, Push-NAF key lifetime, Application-specific USS. The key material consists of Ks\_NAF in case of GBA\_ME and Ks\_ext\_NAF in case of GBA\_U. The key lifetime is the lifetime associated to the key material.

**Outputs, Optional:** Key material, Private Identity.

NOTE X: Depending on the value of the indicator use of GBA\_ME or GBA\_U more key material (i.e. Ks\_int\_NAF) may be returned as output.

NOTE Y: The Push-NAF in clause X.1.2 can be a Push-NAF either internal to the PLMN or provided by the 3rd party.

NOTE Z: When the Push-NAF belongs to a third party the User Private Identity will be exposed to the Push-NAF if the BSF is configured to return the Private Identity to the Push-NAF.

### X.2.2 HSS Services

#### X.2.2.1 General

An SBI capable HSS supports providing the authentication vectors and the subscription profile, i.e. GUSS, to an SBI capable BSF via service-based interfaces.

#### X.2.2.2 Nhss\_GbaSubscriberDataManagement (GbaSDM) service

See TS 33.220 [1].

#### X.2.2.3 Nhss\_GbaUEAuthentication service

See TS 33.220 [1].

### X.2.3 UDM Services

See TS 33.220 [1] for N68 support in Nudm service.

### X.2.4 Mapping of Zpn operations and terminology to SBI services

#### X.2.4.1 General

This clause gives mappings from Zpn operations to SBI services and service operations.

#### X.2.4.2 Mapping of Zpn messages to BSF SBI services

The following table defines the mapping between Zpn messages and BSF SBI services and service operations:

Table X.2.4.2-1: Zpn messages to BSF SBI services and service operations mapping

|  |  |  |  |
| --- | --- | --- | --- |
| Zpn message | Source | Destination | BSF SBI service operation name |
| Zpn interface: Push-NAF requests the GBA Push Information (GPI) from the BSF | Push-NAF | BSF | Nbsp\_Gba\_PushInfo |

## X.3 SBI Capable NF Discovery and Selection

### X.3.1 General

During the GBA Push procedures SBI capable network functions such as the BSF and Push-NAF need to discover and select other SBI capable network functions such as the HSS or the UDM and the BSF respectively.

If there is no HSS or if the HSS does not support the N65 and Zh reference points within the GBA architecture, then the BSF shall be configured to discover and use SBA services of a UDM.

### X.3.2 SBI Capable BSF Discovery and Selection

An SBI capable Push-NAF performs discovery and selection of an SBI capable BSF. The SBI capable Push-NAF shall utilize the NRF to discover an SBI capable BSF unless the information about SBI capable BSF instance(s) is available by other means, e.g. locally configured on the SBI capable Push-NAF. The BSF selection function in SBI capable Push-NAF entities selects an SBI capable BSF instance based on the available SBI capable BSF instances (obtained from the NRF or locally configured).

The BSF selection in an SBI capable Push-NAF shall consider the BSF server name.

NOTE: The Push-NAF derives the BSF server name as defined in Annex B.

Unless the information about the interface type to be used towards the BSF is locally configured on the SBI capable Push-NAF, an SBI capable Push-NAF can also use the NRF to decide the type of interface (SBI vs diameter) to be used towards BSF. For this purpose, an SBI capable Push-NAF can send a Nnrf\_NFDiscovery\_Request to NRF as defined in TS 23.502 [XY] to discover SBI capable BSF instances within a given PLMN. The SBI capable Push-NAF may store all returned SBI capable BSF instances and their NF profiles for subsequent use. If no SBI capable BSF instance is available in the PLMN, then the NRF replies to the SBI capable Push-NAF with no information. In this case, the SBI capable Push-NAF may then attempt to communicate with the BSF using non-SBA legacy GBA and legacy GBA Push protocols.

An SBI capable Push-NAF in a PLMN can serve both as an HPLMN Push-NAF for non-roaming UEs or a VPLMN Push-NAF for roaming UEs.

Unless the information about the network function (BSF or Zn-Proxy) to be used is locally configured on the SBI capable Push-NAF, the SBI capable Push-NAF shall use the BSF server name to determine if the requested BSF is in the same PLMN or a different one. If the requested BSF is in a different PLMN the SBI capable Push-NAF shall use the legacy Zpn interface towards the Zn-Proxy. Otherwise the SBI capable Push-NAF uses the procedures specified earlier in this clause.

### X.3.3 SBI Capable HSS Discovery and Selection

See TS 33.220 [1].

### X.3.4 UDM Discovery and Selection

See TS 23.501 [XZ] clause 6.3.8.

**\*\*\*\*** END OF CHANGES **\*\*\*\***