**3GPP TSG-CT WG4 Meeting #115eC4-231xyz**

**E-Meeting, 17th– 21st April 2023 (revision of C4-231307)**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **29.500** | **CR** | **0382** | **rev** | **1** | **Current version:** | **18.1.0** |  |
|  |
| *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:***  | Correction of ABNF rules |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | CT4 |
|  |  |
| ***Work item code:*** | SBIProtoc18 |  | ***Date:*** | 2023-04-05 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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 canbe 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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | The SBI-specific HTTP headers defined in this TS contain a syntax definition based on the ABNF language.There are many errors in these definitions, such as:- Rules must not start with a digit (this affects ALL headers, since the main rule of each header is always prefixed by "3gpp-"- Rules are case insensitive (this affects some header, containing rules named as, e.g., "sNssai" and "snssai" or "acceptEncoding" and "acceptencoding")- Rules must not contain "underscore" character- Some rules are left undefined- Numerous syntax errors (e.g. missing, or misplacement of double quotes, etc..)These errors should be corrected, in order to allow the usage of tools to:1) ensure that the ABNF definition itself is correct2) facilitate the use of generic ABNF parsing software for the validation and processing of headers by 5GC NF implementationsOther aspects to correct (while they are not necssarily errors):- ABNF should be formatted in PL style and include all rules of a same header in a same "code block", rather than scattered along a whole clause- Rules should have unique names, since this prevents clashing with existing rules from RFCs (which are extensively re-used by this TS), and also allows to parse all the ABNF "code" of all headers in a single validation pass- The description of the headers frequently confuses what is a header *parameter*, with what is an ABNF production *rule*- Some headers have unclear definitions and their syntax should be re-discussed (e.g. headers defined as a comma-separated lists where each list item is, in turn, a set of semicolon-separated name-value pairs, while it seems that the intended syntax was simply to have a set of semicolon-separated name-value pairs). |
|  |  |
| ***Summary of change:*** | Correct all syntax errors in the SBI-specific headers defined in the TS. |
|  |  |
| ***Consequences if not approved:*** | A wrong syntax definition leads to wrong implementation of the header content by 5GC NFs, which difficults interoperability. |
|  |  |
| ***Clauses affected:*** | 5.2.3.2.2, 5.2.3.2.3, 5.2.3.2.4, 5.2.3.2.5, 5.2.3.2.6, 5.2.3.2.8, 5.2.3.2.9, 5.2.3.2.10, 5.2.3.2.11, 5.2.3.2.12, 5.2.3.2.13, 5.2.3.2.14, 5.2.3.2.15, 5.2.3.2.16, 5.2.3.2.17, 5.2.3.2.19, 5.2.3.2.20, 5.2.3.2.21, 5.2.3.3.2, 5.2.3.3.3, 5.2.3.3.4, 5.2.3.3.5, 5.2.3.3.7, 5.2.3.3.8, 5.2.3.3.10, 5.2.3.3.11, 5.2.3.3.12, 5.2.3.3.13 |
|  |  |
|  | **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:*** |  |

\*\*\* First Change \*\*\*

##### 5.2.3.2.2 3gpp-Sbi-Message-Priority

The header contains the HTTP/2 message priority value from 0 to 31, as defined in clause 6.8.4.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Message-Priority-Header = "3gpp-Sbi-Message-Priority:" OWS ( DIGIT / %x31-32 DIGIT / "3" %x30-31 )

A message with 3gpp-Sbi-Message-Priority "0" has the highest priority.

EXAMPLE: 3gpp-Sbi-Message-Priority: 10

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.3 3gpp-Sbi-Callback

The header contains the type of notification. The value for the notification type is a string used identifying a particular type of callback (e.g. a notification, typically the name of the notify service operation).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Callback-Header = "3gpp-Sbi-Callback:" OWS cbtype \*1( ";" OWS "apiversion=" majorversion )

cbtype = 1\*cbchar

cbchar = "-" / "\_" / DIGIT / ALPHA

majorversion = \*DIGIT

EXAMPLE 1: 3gpp-Sbi-Callback: Nnrf\_NFManagement\_NFStatusNotify

EXAMPLE 2: 3gpp-Sbi-Callback: Nudm\_SDM\_Notification; apiversion=2

The list of valid values for the cbtype is specified in Annex B.

The apiversion parameter should be present if the major version is higher than 1.

NOTE: The apiversion parameter can be used by the SEPP to identify the protection and modification policies applicable to the API version of a notification or callback request, or by the SCP to select a notification endpoint of a NF Service Consumer that supports the API version when forwarding a notification request issued for a default notification subscription.

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.4 3gpp-Sbi-Target-apiRoot

The header contains the apiRoot of the target URI (see clause 4.4 of 3GPP TS 29.501 [5]) in a request sent to an SCP when using Indirect Communication. This header contains the apiRoot of the selected or changed target URI in a response sent to an HTTP client, when SCP selected or reselected a new HTTP server to route the request and no Location HTTP header is included in the HTTP response. It may also be used in a request sent to a SEPP and in a request between SEPPs (see clause 6.1.4.3.2).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Target-apiRoot-Header = "3gpp-Sbi-Target-apiRoot" ":" OWS sbi-scheme "://" sbi-authority [ prefix ]

sbi-scheme = "http" / "https"

sbi-authority = host [ ":" port ]

port = \*DIGIT

prefix = path-absolute ; path-absolute production rule from IETF RFC 3986, clause 3.3

EXAMPLE: 3gpp-Sbi-Target-apiRoot: https://example.com/a/b/c

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.5 3gpp-Sbi-Routing-Binding

This header contains a Routing Binding Indication used to direct a service request to an HTTP server which has the targeted NF service resource context (see clause 6.12).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Routing-Binding-Header = "3gpp-Sbi-Routing-Binding:" OWS "bl=" blvalue 1\*( ";" OWS parameter )

blvalue = "nf-instance" / "nf-set" / "nfservice-instance" / "nfservice-set"

parameter = parametername "=" token

parametername = "nfinst" / "nfset" / "nfservinst" / "nfserviceset" / "servname" / "backupamfinst" / "backupnf"

The following parameters are defined:

- bl (binding level): the value of this parameter (blvalue) indicates a preferred binding to a binding entity, i.e. either to an NF Instance, an NF set, an NF Service Instance or an NF Service Set. If the binding level is set to an NF Service Instance (nfservice-instance), then either NF Service Set ID or NF Instance ID shall also be present to unambiguously identify the NF Service Instance.

- nfinst (NF instance): indicates an NF Instance ID, as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]. This parameter shall be present if the binding level is set to "nf-instance", or if the binding level is set to "nfservice-instance" and the nfserviceset parameter is not included.

- nfset (NF set): indicates an NF Set ID, as defined in clause 28.12 in 3GPP TS 23.003 [15]. This parameter shall be present if the binding level is set to "nf-set". It may be present otherwise (see clause 6.12.1).

- nfservinst (NF service instance): indicates an NF Service Instance ID. This parameter shall be present if the binding level is set to "nfservice-instance".

- nfserviceset (NF service set): indicates an NF Service Set ID as defined in clause 28.13 in 3GPP TS 23.003 [15]. This parameter shall be present if the binding level is set to "nfservice-set". It shall also be present if the binding level is set to "nfservice-instance" and the NF service instance indicated by the nfservinst parameter is part of an NF service set (see clause 6.12.1).

- servname (service name): indicates the name of a service, as defined in 3GPP TS 29.510 [8], or a custom service that handles a notification or a callback request. It may be present in a Routing Binding Indication in a notification or a callback request.

- backupamfinst (backup NF Instance): indicates the NF Instance ID (as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]) of the backup NF, i.e. the backup AMF as specified in 3GPP TS 23.501 [3]. The backupamfinst may be present only when the binding level is nf-instance or nfservice-instance or nfservice-set. When backupamfinst is present, no binding entity corresponding to NF set shall be present. When the binding level is nf-set, backupamfinst shall not be present.

- for the definition and encoding of the backupnf see clause 5.2.3.2.6.

See clause 3.2.6 of IETF RFC 7230 [12] for the "token" type definition. A token's value is a string, which contains a binding entity ID or a service name.

EXAMPLE 1: Binding to SMF set 1 of MCC 345 and MNC 012:

3gpp-Sbi-Routing-Binding: bl=nf-set; nfset=set1.smfset.5gc.mnc012.mcc345

EXAMPLE 2: Binding to an SMF instance within SMF set of Example 1:

3gpp-Sbi-Routing-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfset=set1.smfset.5gc.mnc012.mcc345

EXAMPLE 3: Binding to a SMF Service Set "xyz" within an SMF instance within SMF set of Example 1:

3gpp-Sbi-Routing-Binding: bl=nfservice-set; nfserviceset=setxyz.snnsmf-pdusession.nfi54804518-4191-46b3-955c-ac631f953ed8.5gc.mnc012.mcc345; nfset=set1.smfset.5gc.mnc012.mcc345

EXAMPLE 4: Binding to AMF set 1 within AMF region 48 (hexadecimal):
3gpp-Sbi-Routing-Binding: bl=nf-set; nfset=set1-region48.amfset.5gc.mnc012.mcc345

EXAMPLE 5: Binding for a subscription (i.e. notification requests) to AMF set 1 within AMF region 48 (hexadecimal) and Namf\_Communication service:
3gpp-Sbi-Routing-Binding: bl=nf-set; nfset= set1-region48.amfset.5gc.mnc012.mcc345; servname=namf-comm

EXAMPLE 6: Binding to the AMF Instance in addition with backup AMF, where the nfinst carries the Identity of the AMF to which the resource is bound and whose backup AMF is indicated in backupamfinst:
3gpp-Sbi-Routing-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed7; backupamfinst=54804518-4191-46b3-955c-ac631f953ed8

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.6 3gpp-Sbi-Binding

This header contains a comma-delimited list of Binding Indications from an HTTP server for storage and subsequent use by an HTTP client (see clause 6.12).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Binding-Header = "3gpp-Sbi-Binding:" 1#( OWS "bl=" blvalue 1\*( ";" OWS parameter ) [ ";" OWS recoverytime ] [ ";" OWS notif-receiver ] [ ";" OWS "group=" groupvalue ] [ 1\*( ";" OWS groupparameter ) ] [ ";" OWS "no-redundancy=" no-red-value ] )

blvalue = "nf-instance" / "nf-set" / "nfservice-instance" / "nfservice-set"

parameter = parametername "=" token

parametername = "nfinst" / "nfset" / "nfservinst" / "nfserviceset" / "servname" / "scope" / "backupamfinst" / "backupnf"

recoverytime = "recoverytime=" OWS DQUOTE date-time DQUOTE

notif-receiver = "nr=" URI ; URI production rule from IETF RFC 3986, Appendix A

groupvalue = "true" / "false"

groupparameter = groupparametername "=" token

groupparametername = "oldgroupid" / "groupid" / "uribase" / "oldnfinst / "oldservset" / "oldservinst" / "guami"

no-red-value = "true"

The following parameters are defined:

- scope: indicates the applicability of a Binding Indication in a service request other than a notification request, or in a notification or callback response. This may take one of the following values:

- "other-service": the binding information applies to other service(s) that the NF Service Consumer may later on provide as an NF Service Producer (see clause 6.12.3);

- "subscription-events": the binding information applies to subscription change event notifications (see clause 6.12.4);

- "callback": the binding information applies to notification or callback requests (see clauses 6.12.4 and 6.12.5).

The absence of this parameter in a Binding Indication in a service request other than a notification request, or in a notification or callback response, shall be interpreted as "callback".

Two scope parameters may be present in a Binding Indication if the binding information applies to notification/callback requests and to other services.

- servname (service name): indicates the name of a service, as defined in 3GPP TS 29.510 [8], or a custom service, i.e.:

- the name of the service that handles a notification or a callback request, when present in a Binding Indication for a subscription or a callback, i.e. with a scope parameter absent or set to "callback"; or

- the name of the other service(s) for which the binding applies, when present in a Binding Indication in a service request for the other services the NF Service Consumer can provide later on as an NF Service Producer, i.e. with the scope parameter set to "other-service". More than one servname parameter may be present to represent multiple such services. The absence of this parameter in a Binding Indication with the scope parameter set to "other-service" shall be interpreted as binding information that applies to all the services that the NF Service Consumer may provide later as an NF Service Producer.

- recoverytime: indicates the recovery timestamp of the entity corresponding to the highest resiliency level supported for the resource, that is, the higher level binding entity indicated in the Binding Indication. See Table 6.3.1.0-1 of 3GPP TS 23.501 [3] and clause 6.1 of 3GPP TS 23.527 [38]. The date-time type is specified in IETF RFC 5322 [37] and clause 7.1.1.1 of IETF RFC 7231 [11].

- nr: indicates the URI of the notification endpoint when this binding information is applicable; it applies to callback requests (see clause 6.12.4); if the notification URI does not contain a correlationID in the path (i.e. it is a common notification URI for multiple subscriptions), the correlationID shall be added as a fragment component of the URI (i.e. following the "#" character) at the end of the URI.

- for the definition and encoding of the blvalue, nfinst, backupamfinst, nfset, nfservinst and nfserviceset see clause 5.2.3.2.5.

- backupnf: indicates the backup NF service instance identifier and/or the backup NF identifier as defined in clause 5.2.2.2.2 or in 3GPP TS 29.510 [8], which shall be used when preferred binding entity is not reachable if supported.

- group: it is a boolean indicating if the binding indication is for a group of resource/session contexts.

- groupid (group id): indicates the group identifier allocated by the NF (service) instance, one ore more resource/session contexts are sharing the same groupid. The groupid is optional and it may be allocated when the resource/session context is created and then be updated afterwards. The groupid is global unique and it may be encoded using the same mechnaism for the NfInstanceId as specificed in 3GPP TS 29.571 [13].

- oldgroupid (old group id): indicates the group identifier allocated by the NF (service) instance previously and to be replaced by the groupid, hence it shall only be present when to update a Binding Indication for multiple contexts. When the if the oldgroupid is present, the groupid shall also be present to indicate the new groupid allocated.

- uribase: identify the apiroot and path segments part in the resource URI or notification/callback URI which is common to multiple contexts. This parameter may only be present when to update a Binding Indication for multiple contexts and when the "group" is set to "true". When included, it indicates that all resources or notification contexts with this uribase will use the updated Binding Indication subsequently. More than one uribase may be present.

- oldnfinst: indicates the NF Instance ID of the NF instance where the group of resource/session contexts are currently served (i.e. the Binding Indication allocated previously for the group of resource/session contexts includes the information of the NF instance), as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]. When included, it indicates that all the resource/session contexts served by this NF instance will use the updated Binding Indication subsequently.

- oldservset: indicates the NF Service Set ID of the NF Service Set where the group of resource/session contexts are currently served (i.e. the Binding Indication allocated previously for the group of resource/session contexts includes the information of the NF Service Set), as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]. When included, it indicates that all the resource/session contexts served by this NF Service Set will use the updated Binding Indication subsequently.

- oldservinst: indicates the NF Service Instance ID of the NF service instance where the group of resource/session contexts are currently served (i.e. the Binding Indication allocated previously for the group of resource/session contexts includes the information of the NF service instance), as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]. When included, it indicates that all the resource/session contexts served by this NF service instance will use the updated Binding Indication subsequently.

- guami (GUAMI): indicates the GUAMI of the AMF currently serving UE contexts, as defined in clause 5.3.4.1 of 3GPP TS 29.571 [13]. When included, it indicates that all the UE contexts associated with the GUMAI will use the updated Binding Indication subsequently.

- no-redundancy: it is a boolean set to true indicating that the resource is exclusively bound to the NF service instance identified in the binding indication. It may be present in a binding with any scope, i.e. "other-service", "subscription-events" or "callback", or with no scope parameter. When this parameter is present, the blvalue shall be set to "nfservice-instance", the nfservinst parameter shall be present and either the nfservset parameter or the nfinst parameter shall be present. The nfservset or nfinst parameter included in the binding indication shall only be used to identify the NF service instance and shall not be considered as a binding entity for reselection. The no-redundancy parameter shall only be signaled if the receiver of this information is known to support this parameter (see clause 6.12.1). Subsequently, when sending further requests targeting a resource with no-redundancy, the HTTP client shall not include any routing binding indication in the request message (to prevent the SCP from performing any reselection).

EXAMPLES 1 to 5: Same as EXAMPLES 1 to 5 defined in clause 5.2.3.2.5, with the header name "3gpp-Sbi-Binding" instead of "3gpp-Sbi-Routing-Binding".

EXAMPLE 6: Subscription request from one NF on behalf of another NF, with 2 binding indications:

3gpp-Sbi-Binding: bl= nf-set; nfset=set1.udmset.5gc.mnc012.mcc345; servname=nudm-ee;scope=subscription-events
3gpp-Sbi-Binding: bl= nf-set; nfset=set1.nefset.5gc.mnc012.mcc345; servname=nnef-event-exposure

EXAMPLE 7: Service request with 2 binding indications, for callback requests and for other services the NF Service Consumer may provide later as an NF Service Producer:

3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfset=set1.smfset.5gc.mnc012.mcc345; servname=nsmf-pdusession
3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfset=set1.smfset.5gc.mnc012.mcc345; scope=other-service; servname=nsmf-event-exposure

EXAMPLE 8: Service request with one binding indication applying to notification/callback requests and to any other services the NF Service Consumer may provide later as an NF Service Producer:

3gpp-Sbi-Binding: bl=nf-set; nfset=set1-region48.amfset.5gc.mnc012.mcc345; scope=callback; scope=other-service

EXAMPLE 9: Service request with one binding indication applying to notification/callback requests together with a recovery time stamp associated with the NF Set indicated in the binding indication and with the binding level set to "nfset":
3gpp-Sbi-Binding: bl=nfset; nfset=set1-region48.amfset.5gc.mnc012.mcc345; scope=callback; recoverytime= "Tue, 04 Feb 2020 08:49:37 GMT"

EXAMPLE 10: Service response with one binding indication applying to the session context with a recovery time stamp associated with the NF Set indicated in "nfset" in the binding indication and with the binding level set to "nfinstance":

3gpp-Sbi-Binding: bl= nfinstance; nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfset=set1.smfset.5gc.mnc012.mcc345; recoverytime= "Tue, 04 Feb 2020 08:49:37 GMT"

EXAMPLE 11: Service response with one binding indication applying to the session context with a recovery time stamp associated with the NF Instance included the binding indication and with the binding level set to nfserviceinstance:

3gpp-Sbi-Binding: bl=nfserviceinstance; nfservinst=xyz; nfinst=54804518-4191-46b3-955c-ac631f953ed8; recoverytime= "Tue, 04 Feb 2020 08:49:37 GMT"

EXAMPLE 12: Service response with one binding indication applying to the resource context pertaining to a group identified by "54804518-4191-46b3-955c-ac631f953ed1" together with a backup nf:

3gpp-Sbi-Binding: bl= nfinstance; nfinst=54804518-4191-46b3-955c-ac631f953ed0; nfset=set1.smfset.5gc.mnc012.mcc345; groupid=54804518-4191-46b3-955c-ac631f953ed1; backupnf=54804519-4191-46b3-955c-ac631f953ed2

EXAMPLE 13: A notification request message with one binding indication applying to the resource contexts with the oldgroup identifier "54804518-4191-46b3-955c-ac631f953ed1", where the preferred binding entity is changed to "nfinst=54804519-4191-46b3-955c-ac631f953ed0" together with a new group identifier "54804519-4191-46b3-955c-ac631f953ed3" allocated.

3gpp-Sbi-Binding: bl= nfinstance; nfinst=54804519-4191-46b3-955c-ac631f953ed0; nfset=set1.smfset.5gc.mnc012.mcc345; group=true; oldgroupid=54804518-4191-46b3-955c-ac631f953ed1; groupid=54804519-4191-46b3-955c-ac631f953ed3

EXAMPLE 14: A notification request message with one binding indication applying to the resource contexts identified by an uribase, where the preferred binding entity is changed to "nfinst=54804519-4191-46b3-955c-ac631f953ed0":

3gpp-Sbi-Binding: bl= nfinstance; nfinst=54804519-4191-46b3-955c-ac631f953ed0; nfset=set1.smfset.5gc.mnc012.mcc345; group=true; uribase= http%3A%2F%2F10.10.10.10%2Fstringxyz

EXAMPLE 15: A notification request message with one binding indication applying to the resource contexts served by the NF instance identified by "64804518-4191-46b3-955c-ac631f953ed8" where the preferred binding entity is changed to "nfinst=74804519-4191-46b3-955c-ac631f953ed0".

3gpp-Sbi-Binding: bl= nfinstance; nfinst=74804519-4191-46b3-955c-ac631f953ed0; nfset=set1.smfset.5gc.mnc012.mcc345; group=true; oldnfinst=64804518-4191-46b3-955c-ac631f953ed8

EXAMPLE 16: Service request message with an updated binding indication applying to the UE contexts for GUAMI" <mnc(012)><mcc(345)><AmfId("abcd12")> where the backupamfinst is changed.

3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed7; backupamfinst=54804520-4191-46b3-955c-ac631f953ed8; scope=other-service; group=true; guami={"plmnId":{"mnc":"012","mcc":"345"},"amfId":"abcd12"}

EXAMPLE 17: Service response with a binding indication applying to the resource context which is exclusively bound to a specific NF service instance.

 3gpp-Sbi-Binding: bl=nfserviceinstance; nfservinst=xyz; nfinst=54804518-4191-46b3-955c-ac631f953ed8; no-redundancy= true

NOTE: Examples 6 and 7 are formatted as two distinct headers (which improves the readability), but they can also be formatted as a single header with two Binding Indication values separated by a comma.

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.8 3gpp-Sbi-Producer-Id

This header contains the NF Service Producer Instance ID (see clause 6.10.3.4).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Producer-Id-Header = "3gpp-Sbi-Producer-Id:" OWS "nfinst=" nfinst [ OWS ";" "nfservinst=" nfservinst ] [ OWS ";" "nfset=" nfset ] [ OWS ";" "nfserviceset=" nfserviceset ]

lowerhexdig = DIGIT / "a" / "b" / "c" / "d" / "e" / "f"

nfinst = 1\*( lowerhexdig / "-" )

nfservinst = token

nfset = token

nfserviceset = token

The following parameters are defined:

- nfinst (NF instance): indicates a NF Instance ID, as defined in 3GPP TS 29.510 [8];

- nfservinst (NF service instance): indicates a NF Service Instance ID, as defined in 3GPP TS 29.510 [8];

- nfset (NF set): indicates an NF Set ID, as defined in clause 28.12 in 3GPP TS 23.003 [15];

- nfserviceset (NF service set): indicates an NF Service Set ID as defined in clause 28.13 in 3GPP TS 23.003 [15].

EXAMPLE 1: 3gpp-Sbi-Producer-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8

EXAMPLE 2: 3gpp-Sbi-Producer-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfservinst=xyz

EXAMPLE 3: 3gpp-Sbi-Producer-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfservinst=xyz; nfset=set1.smfset.5gc.mnc012.mcc345

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.9 3gpp-Sbi-Oci

The header contains a comma-delimited list of Overload Control Information (OCI). See clause 6.4.3.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Oci-Header = "3gpp-Sbi-Oci:" 1#( RWS timestamp ";" RWS validityPeriod ";" RWS olcMetric ";" RWS olcScope )

timestamp = "Timestamp:" RWS DQUOTE date-time DQUOTE

validityPeriod = "Period-of-Validity:" RWS 1\*DIGIT "s"

olcMetric = "Overload-Reduction-Metric:" RWS ( DIGIT / %x31-39 DIGIT / "100" ) "%"

olcScope = nfProducerScope / nfConsumerScope / scpScope / seppScope

nfProducerScope = ( ( "NF-Instance:" RWS nfinst )

 / ( "NF-Set:" RWS nfset )

 / ( "NF-Service-Instance:" RWS nfservinst [ ";" RWS "NF-Inst:" RWS nfinst ] )

 / ( "NF-Service-Set:" RWS nfserviceset )

 ) [ ";" RWS sNssaiList ";" RWS dnnList ]

nfConsumerScope = ( "NF-Instance:" RWS nfinst [ ";" RWS "Service-Name:" RWS servname ] )

 / ( "NF-Set:" RWS nfset [ ";" RWS "Service-Name:" RWS servname ] )

 / ( "NF-Service-Instance:" RWS nfservinst [ ";" RWS "NF-Inst:" RWS nfinst ] )

 / ( "NF-Service-Set:" RWS nfserviceset )

 / ( "Callback-Uri:" RWS URI \*( RWS "&" RWS URI ) )

scpScope = "SCP-FQDN:" RWS fqdn

seppScope = "SEPP-FQDN:" RWS fqdn

dnnList = "DNN:" RWS 1\*tchar \*( RWS "&" RWS 1\*tchar )

sNssaiList = "S-NSSAI:" RWS snssai \*( RWS "&" RWS snssai )

snssai = 1\*tchar

"Timestamp" (Mandatory parameter): The date-time type is specified in IETF RFC 5322 [37] and clause 7.1.1.1 of IETF RFC 7231 [11]. It indicates the timestamp at which the overload control information was generated.

"Period-of-Validity" (Mandatory parameter): Period of validity is a timer that is measured in seconds. Once the timer expires, the OCI becomes invalid.

"Overload-Reduction-Metric" (Mandatory parameter): Overload-Reduction-Metric up to 3 digits long decimal string and the value range shall be from 0 to 100.

The Overload Control Scope is a mandatory header component, and it shall contain one of the parameters: "NF-Instance", "NF-Set", "NF-Service-Instance" or "NF-Service-Set" (for NF consumers or NF producers), "Callback-URI" (for NF consumers), "SCP-FQDN" (for SCP), or "SEPP-FQDN" (for SEPP).

See clause 6.4.3.4.5. The nfinst, nfset, nfservinst, nfserviceset and servname parameters are defined in clause 5.2.3.2.8. fqdn shall encode an FQDN. URI is defined in clause 3 of IETF RFC 3986 [14].

When signaling overload control information of an NF service instance, the "NF-Inst" parameter shall be present to identify the NF service instance unambiguously. If the "NF-Inst" parameter is absent, the receiving NF should assume the last known NF instance ID of NF service producer or consumer, if available.

NOTE 1: Implementations complying with earlier versions of the specification can signal overload control information of an NF service instance without including the NF-Inst parameter.

"DNN" (Optional parameter): Used for S-NSSAI/DNN based overload control by SMF, see clause 6.4.3.4.5.2.2, that refers to one or more specific DNN(s). DNN format is defined in 3GPP TS 23.003 [15].

"S-NSSAI" (Optional parameter): Used for S-NSSAI/DNN based overload control by SMF, see clause 6.4.3.4.5.2.2, that refers to one or more specific S-NSSAI(s).

S-NSSAI format is defined in clause 5.4.4.2 of 3GPP TS 29.571 [13]. It shall be encoded as the object format (i.e. not converted to the string pattern defined in clause 5.4.4.2 of 3GPP TS 29.571 [13]).

EXAMPLE 1: Overload Control Information for an NF Instance:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 75s; Overload-Reduction-Metric: 50%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8

EXAMPLE 2: Overload Control Information for an NF Service Set:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 120s; Overload-Reduction-Metric: 50%; NF-Service-Set: setxyz.snnsmf-pdusession.nfi54804518-4191-46b3-955c-ac631f953ed8.5gc.mnc012.mcc345

EXAMPLE 3: Overload Control Information for an SMF instance related to a particular DNN of an S-NSSAI:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 600s; Overload-Reduction-Metric: 50%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: internet.mnc012.mcc345.gprs

NOTE 2: The S-NSSAI parameter corresponds to the JSON encoding: {"sst": 1, "sd": "A08923"} (see clause 5.2.3.1)

EXAMPLE 4: Overload Control Information for an SMF instance related to a particular DNN shared by two S-NSSAIs:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 240s; Overload-Reduction-Metric: 50%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D & %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08924%22%7D; DNN: internet.mnc012.mcc345.gprs

NOTE 3: The S- NSSAI parameter corresponds to the JSON encoding: {"sst": 1, "sd": "A08923"} & {"sst": 1, "sd": "A08924"} (see clause 5.2.3.1)

EXAMPLE 5: Overload Control Information sent by a NF service consumer with a scope set to a Callback-Uri:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 120s; Overload-Reduction-Metric: 25%; Callback-Uri: https://pcf12.operator.com/serviceY

EXAMPLE 6: Overload Control Information sent by a NF service consumer with a scope set to a specific NF Instance and service:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 120s; Overload-Reduction-Metric: 25%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; Service-Name: nsmf-pdusession

EXAMPLE 7: Overload Control Information sent by an SCP:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 120s; Overload-Reduction-Metric: 25%; SCP-FQDN: scp1.example.com

EXAMPLE 8: Example with two OCI values, one for an SMF Instance and another one for a specific DNN of an S-NSSAI for the same SMF Instance:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 75s; Overload-Reduction-Metric: 50%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8
3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 600s; Overload-Reduction-Metric: 40%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: internet.mnc012.mcc345.gprs

NOTE 4: The S-NSSAI parameter corresponds to the JSON encoding: {"sst": 1, "sd": "A08923"} (see clause 5.2.3.1)

EXAMPLE 9: Overload Control Information sent by an SEPP:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 120s; Overload-Reduction-Metric: 25%; SEPP-FQDN: sepp1.example.com

NOTE 5: Example 8 is formatted as two distinct headers (which improves the readability), but it can also be formatted as a single header with two OCI values separated by a comma.

EXAMPLE 10: Overload Control Information for an NF Service Instance:

3gpp-Sbi-Oci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Period-of-Validity: 75s; Overload-Reduction-Metric: 50%; NF-Service-Instance: xyz; NF-Inst: 54804518-4191-46b3-955c-ac631f953ed8

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.10 3gpp-Sbi-Lci

The header contains a comma-delimited list (see IETF RFC 7230 [12]) of Load Control Information (LCI). See clause 6.3.3.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Lci-Header = "3gpp-Sbi-Lci:" 1#( RWS timestamp ";" RWS lcMetric ";" RWS lcScope )

timestamp = "Timestamp:" RWS DQUOTE date-time DQUOTE

lcMetric = "Load-Metric:" RWS (DIGIT / %x31-39 DIGIT / "100") "%"

lcScope = lcNfProducerScope / scpScope / seppScope

lcNfProducerScope = ( ( "NF-Instance:" RWS nfinst )

 / ( "NF-Set:" RWS nfset)

 / ( "NF-Service-Instance:" RWS nfservinst [";" RWS "NF-Inst:" RWS nfinst] )

 / ( "NF-Service-Set:" RWS nfserviceset) )

 [ ";" RWS sNssaiList ";" RWS dnnList ";" RWS relativeCapacity ]

dnnList = "DNN:" RWS 1\*tchar \*( RWS "&" RWS 1\*tchar )

sNssaiList = "S-NSSAI:" RWS snssai \*( RWS "&" RWS snssai )

snssai = 1\*tchar

relativeCapacity = "Relative-Capacity:" RWS ( 1\*2DIGIT / "100" ) "%"

"Timestamp" (Mandatory parameter): The date-time type is specified in IETF RFC 5322 [37] and clause 7.1.1.1 of IETF RFC 7231 [11]. It indicates the timestamp associated with the load control information.

"Load-Metric" (Mandatory parameter): Load-Metric is up to 3 digits long decimal string and the value range shall be from 0 to 100.

The Load Control Scope is a mandatory header component, and it shall contain one of the parameters: "NF-Instance", "NF-Set", "NF-Service-Instance" or "NF-Service-Set" (for NF producers), "SCP-FQDN" (for SCP), or "SEPP-FQDN" (for SEPP); in its ABNF definition, the rules "scpScope" and "seppScope" are defined in clause 5.2.3.2.9.

See clause 6.3.3.4.4. The nfinst, nfset, nfservinst and nfserviceset parameters are defined in clause 5.2.3.2.5. fqdn shall encode an FQDN.

When signaling load control information of an NF service instance, the NF-Inst parameter shall be present to identify the NF service instance unambiguously. If the NF-Inst parameter is absent, the receiving NF should assume the last known NF instance ID of the NF service producer, if available.

NOTE 1: Implementations complying with earlier versions of the specification can signal load control information of an NF service instance without including the NF-Inst parameter.

"DNN" (Optional parameter): Used for S-NSSAI/DNN based load control by SMF, see clause 6.3.3.4.4.2.2, that refers to one or more specific DNN(s). DNN format is defined in 3GPP TS 23.003 [15].

"S-NSSAI" (Optional parameter): Used for S-NSSAI/DNN based load control by SMF, see clause 6.3.3.4.4.2.2, that refers to one or more specific S-NSSAI(s).

S-NSSAI format is defined in clause 5.4.4.2 of 3GPP TS 29.571 [13]. It shall be encoded as the object format (i.e. not converted to the string pattern defined in clause 5.4.4.2 of 3GPP TS 29.571 [13]).

"Relative-Capacity" (Optional parameter): Used for S-NSSAI/DNN based load control by SMF, see clause 6.3.3.4.5. Up to 3 digits long decimal string with value range from 0 to 100. The value applies to all combinations of S-NSSAIs and DNNs indicated in the LCI.

EXAMPLE 1: Load Control Information for an NF Instance:

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8

EXAMPLE 2: Load Control Information for an NF Service Set:

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; NF-Service-Set : setxyz.snnsmf-pdusession.nfi54804518-4191-46b3-955c-ac631f953ed8.5gc.mnc012.mcc345

EXAMPLE 3: Load Control Information for an SMF instance related to a particular DNN of an S-NSSAI (SST=1, SD="A08923"):

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: internet.mnc012.mcc345.gprs; Relative-Capacity: 20%

EXAMPLE 4: Load Control Information for an SMF instance related to a particular S-NSSAI (SST=1, SD="A08923"):

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; NF-Instance: 54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: internet.mnc012.mcc345.gprs; Relative-Capacity: 20%

NOTE 2: The S-Nssai parameter corresponds to the JSON encoding: {"sst": 1, "sd": "A08923"} (see clause 5.2.3.1)

EXAMPLE 5: Load Control Information for SCP:

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; SCP-FQDN: scp1.example.com

EXAMPLE 6: Example with two LCI values, for different DNNs of a same S-NSSAI (SST=1, SD="A08923"):

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 40%; NF-Instance=54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: internet.mnc012.mcc345.gprs; Relative-Capacity: 30%
3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 70%; NF-Instance=54804518-4191-46b3-955c-ac631f953ed8; S-NSSAI: %7B%22sst%22%3A 1%2C %22sd%22%3A %22A08923%22%7D; DNN: ciot.mnc012.mcc345.gprs; Relative-Capacity: 20%

NOTE: The S-Nssai parameter corresponds to the JSON encoding: {"sst": 1, "sd": "A08923"} (see clause 5.2.3.1)

EXAMPLE 7: Load Control Information for SEPP:

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Apr 2021 08:36:42 GMT"; Load-Metric: 25%; SEPP-FQDN: sepp1.example.com

NOTE 3: Example 6 is formatted as two distinct headers (which improves the readability), but it can also be formatted as a single header with two LCI values separated by a comma.

EXAMPLE 8: Load Control Information for an NF Service Instance:

3gpp-Sbi-Lci: Timestamp: "Tue, 04 Feb 2020 08:49:37 GMT"; Load-Metric: 25%; NF-Service-Instance: xyz; NF-Inst: 54804518-4191-46b3-955c-ac631f953ed8

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.11 3gpp-Sbi-Client-Credentials

The header contains client credentials assertion (see clause 13.3.8.1 of 3GPP TS 33.501 [17]).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Client-Credentials-Header = "3gpp-Sbi-Client-Credentials:" OWS jwt

jwt = 1\*b64urlchar "." 1\*b64urlchar "." 1\*b64urlchar

b64urlchar = ALPHA / DIGIT / "-" / "\_"

The client credentials assertion shall be a JSON Web Token (JWT) as specified in IETF RFC 7519 [41], digitally signed using JWS as specified in IETF RFC 7515 [24] and in clause 13.3.8.1 of 3GPP TS 33.501 [15]. It shall include:

- the claims defined in Table 5.2.3.2.11-1 encoded as a JSON object; and

- one of the following JOSE headers:

- the X.509 URL (x5u) header (see clause 4.1.5 of IETF RFC 7515 [26]) referring to a resource for the X.509 public key certificate or certificate chain used for signing the client authentication assertion, or

- the X.509 Certificate Chain (x5c) header (see clause 4.1.5 of IETF RFC 7515 [26]) including the X.509 public key certificate or certificate chain used for signing the client authentication assertion.

The digitally signed client credentials assertion shall be converted to the JWS Compact Serialization encoding as a string as specified in clause 7.1 of IETF RFC 7515 [24].

Table 5.2.3.2.11 -1: Definition of type ClientCredentialsAssertion

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description |
| sub | NfInstanceId | M | 1 | This IE shall contain the NF instance ID of the NF service consumer, corresponding to the standard "Subject" claim described in IETF RFC 7519 [41], clause 4.1.2. |
| iat | integer | M | 1 | This IE shall indicate the time at which the JWT was issued, corresponding to the standard "Issued At" claim described in IETF RFC 7519 [41], clause 4.1.6. This claim may be used to determine the age of the JWT. |
| exp | integer | M | 1 | This IE shall contain the expiration time after which the client credentials assertion is considered to be expired, corresponding to the standard "Expiration Time" claim described in IETF RFC 7519 [41], clause 4.1.4.  |
| aud | array(NFType) | M | 1..N | This IE shall contain the NF type of the NF service producer and/or "NRF", for which the claim is applicable, corresponding to the standard "Audience" claim described in IETF RFC 7519 [41], clause 4.1.3.  |

The JSON object containing the client credentials assertion shall comply with the following OpenAPI definition:

 ClientCredentialsAssertion:

 description: The data structure for the client credentials assertion

 type: object

 required:

 - sub

 - iat

 - exp

 - aud

 properties:

 sub:

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

 iat:

 type: integer

 exp:

 type: integer

 aud:

 type: array

 items:

 $ref: 'TS29510\_Nnrf\_NFManagement.yaml#/components/schemas/NFType'

 minItems: 1

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.12 3gpp-Sbi-Nrf-Uri

The header contains a list of NRF API URIs. See clauses 6.10.3.2 and 6.10.5.1.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Nrf-Uri-Header = "3gpp-Sbi-Nrf-Uri:" nrfUriParam \*( OWS ";" nrfUriParam )

nrfUriParam = nrfUriParamName ":" RWS ( nrfUriParamValue1 / nrfUriParamValue2 )

nrfUriParamName = "nnrf-disc" / "nnrf-nfm" / "nnrf-oauth2" / "oauth2-requested-services" / token

nrfUriParamValue1 = DQUOTE URI DQUOTE

nrfUriParamValue2 = ( nrfServiceName \*( "&" RWS nrfServiceName) )

nrfServiceName = "nnrf-disc" / "nnrf-nfm"

NOTE: token is defined for future extensibility.

- for the nnrf-disc, nnrf-nfm and nnrf-oauth2 parameters:

URI shall comply with the URI definition in IETF RFC 3986 [14].

- for the oauth2-requested-services parameter:

nrfServiceName shall encode an NRF API name, e.g. "nnrf-disc" or "nnrf-nfm".

When present, the oauth2-requested-services parameter shall indicate the list of NRF services for which OAuth2 based authorization is required for accessing the respective NRF services.

If OAuth2 based authorization is required for accessing the respective NRF services, the nnrf-oauth2 parameter shall be present and shall be used to request access token for NRF services.

The absence of the oauth2-requested-services parameter means that no indication is provided about the potential usage of Oauth2 for authorization.

EXAMPLE 1: Header with NRF NF Discovery, NF Management and Access Token API URIs, without indication on whether OAuth2-based authorization is required to access the NRF services:

3gpp-Sbi-Nrf-Uri: nnrf-disc: "https://nrf1.operator.com/nnrf-disc/v1"; nnrf-nfm: "https://nrf1.operator.com/nnrf-nfm/v1"; nnrf-oauth2: "https://nrf1.operator.com/oauth2"

EXAMPLE 2: Header with NRF NF Discovery, NF Management and Access Token API URIs, indication on whether OAuth2-based authorization is required to access the NRF services:

3gpp-Sbi-Nrf-Uri: nnrf-disc: "https://nrf1.operator.com/nnrf-disc/v1"; nnrf-nfm: "https://nrf1.operator.com/nnrf-nfm/v1"; nnrf-oauth2: "https://nrf1.operator.com/oauth2"; oauth2-requested-services: nnrf-disc & nnrf-nfm

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.13 3gpp-Sbi-Target-Nf-Id

This header contains the target NF (Service) Instance ID in an HTTP 307/308 response (see clause 6.10.9).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Target-Nf-Id-Header = "3gpp-Sbi-Target-Nf-Id:" OWS "nfinst=" nfinst [ ";" OWS "nfservinst=" nfservinst ]

The following parameters are defined:

- nfinst (NF instance): indicates a NF Instance ID, as defined in 3GPP TS 29.510 [8]; the ABNF is defined in clause 5.2.3.2.8.

- nfservinst (NF service instance): indicates a NF Service Instance ID, as defined in 3GPP TS 29.510 [8]; the ABNF is defined in clause 5.2.3.2.8.

EXAMPLE: 3gpp-Sbi-Target-Nf-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfservinst=xyz

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.14 3gpp-Sbi-Max-Forward-Hops

The header contains the value of maximum number of allowed hops with specified node type to relay the request message to the target NF.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Max-Forward-Hops-Header = "3gpp-Sbi-Max-Forward-Hops:" OWS (DIGIT / %x31-39 DIGIT) ";" OWS "nodetype=" nodetypevalue

nodetypevalue = "scp"

EXAMPLE: Allowed up to 5 SCP hops to relay the request:

3gpp-Sbi- Max-Forward-Hops: 5; nodetype=scp.

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.15 3gpp-Sbi-Originating-Network-Id

The header contains the PLMN Identity (MCC-MNC) of the source PLMN or the SNPN ID (MCC-MNC-NID) of the source SNPN of the received HTTP messages.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

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

upperOrLowerHexDig = HEXDIG / "a" / "b" / "c" / "d" / "e" / "f"

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

srctype = "SCP" / "SEPP"

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

The srcinfo shall only be present when SCP or SEPP was unable to uniquely determine the value, i.e. PLMN ID, and has decided to insert the header with the value derived by configuration as described in Table 5.2.3.2.1-1.

The srcfqdn shall indicate FQDN of SCP or SEPP that inserted the header when srcinfo is present.

EXAMPLE 1: For a source PLMN:

 3gpp-Sbi-Originating-Network-Id: 123-45

EXAMPLE 2: For a source PLMN and the header included by SEPP under the condition when the value of the header is derived based on the configuration and inserted by the SEPP:

 3gpp-Sbi-Originating-Network-Id: 123-45; src: SEPP-sepp001.sepp.5gc.mnc045.mcc123.3gppnetwork.org

EXAMPLE 3: For a source SNPN:

 3gpp-Sbi-Originating-Network-Id: 123-45-000007ed9d5

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.16 3gpp-Sbi-Access-Scope

The header indicates the access scope of the service request for NF service access authorization, as defined in clauses 6.7.3 and 6.10.11.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Access-Scope-Header = "3gpp-Sbi-Access-Scope:" OWS scope-token \*(SP scope-token)

scope-token = 1\*NQCHAR

Scope-token shall consist of a list of space-delimited, case-sensitive strings, containing the NF service name of the NF service producer corresponding to the service request and, if defined for the specific resource/operation in the corresponding API, the additional resource/operation-level scope.

NQCHAR is defined in Appendix A of IETF RFC 6749 [22].

NOTE 1: This corresponds to the "scope" syntax defined for OAuth in clauses 3.3 and A.4 of IETF RFC 6749 [22] and also to the syntax of the "scope" parameter in AccessTokenReq in 3GPP TS 29.510 [8]. This enables the SCP to set the scope parameter in the Nnrf\_Get Access Token Request to the value of the 3gpp-Sbi-Access-Scope header received in an incoming service request, or to a list of scopes that is the intersection of the scopes indicated in the 3gpp-Sbi-Access-Scope header and the scopes expected by the NF Service producer (as registered in its NF profile).

NOTE 2: For indirect communication with delegated discovery (see clause 6.10.11.2), for a specific resource / operation for which the API defines a resource/operation-level scope, the NF service consumer does not and need not know whether the NF service producer is configured to require the resource/operation level scope or not. The setting of the 3gpp-Sbi-Access-Scope header is the same regardless of whether the NF service producer is configured to require the resource/operation level scope or not.

EXAMPLE: 3gpp-Sbi-Access-Scope: nhss-ims-uecm nhss-ims-uecm:authorize:invoke

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.17 3gpp-Sbi-Access-Token

The header contains an Access Token in a service response, for possible re-use in subsequent service requests, as defined in clause 6.10.11.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Access-Token = "3gpp-Sbi-Access-Token:" OWS credentials

See Appendix C of IETF RFC 7235 [21] for the definition of "credentials".

NOTE: The 3gpp-Sbi-Access-Token header is encoded as the Authorization header.

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.19 3gpp-Sbi-Target-Nf-Group-Id

This header contains the NF Group ID (e.g. UDM, HSS, AUSF, UDR, CHF, PCF Group ID) of the NF service producer.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Target-Nf-Group-Id-Header = "3gpp-Sbi-Target-Nf-Group-Id:" OWS "nfgid=" nfGroupIdValue

nfGroupIdValue = DQUOTE token DQUOTE

The following parameter is defined:

- nfgid (NF Group ID): indicates a NF Group ID, as defined in 3GPP TS 29.571 [13].

EXAMPLE: 3gpp-Sbi-Target-Nf-Group-Id: nfgid="udm-group-15"

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.20 3gpp-Sbi-Nrf-Uri-Callback

The header contains the NRF API URI(s) of the NF discovery service and/or NF management service. See clauses 6.5.3.2.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Nrf-Uri-Callback-Header = "3gpp-Sbi-Nrf-Uri-Callback:" nrfUriCallbackParam \*( OWS ";" nrfUriCallbackParam )

nrfUriCallbackParam = nrfUriCallbackParamName ":" RWS nrfUriCallbackParamValue

nrfUriCallbackParamName = "nnrf-disc" / "nnrf-nfm" / token ; token is defined for future extensibility

nrfUriCallbackParamValue = DQUOTE URI DQUOTE

URI shall comply with the URI definition in IETF RFC 3986 [14].

EXAMPLE 1: Header with NRF NF Discovery Service:

 3gpp-Sbi-Nrf-Uri-Callback: nnrf-disc: "https://nrf1.operator.com/nnrf-disc/v1"

EXAMPLE 2: Header with NRF NF Discovery and NF Management Services:

 3gpp-Sbi-Nrf-Uri-Callback: nnrf-disc: "https://nrf1.operator.com/nnrf-disc/v1"; nnrf-nfm: "https://nrf1.operator.com/nnrf-nfm/v1"

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.2.21 3gpp-Sbi-NF-Peer-Info

This header contains the IDs of the NF (service) instance as HTTP client and the NF (service) instance as HTTP server.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-NF-Peer-Info-Header = "3gpp-Sbi-NF-Peer-Info" ":" OWS peerinfo \*( ";" OWS peerinfo )

peerinfo = peertype "=" token

peertype = "srcinst" / "srcservinst" / "srcscp" / "srcsepp" / "dstinst" / "dstservinst" / "dstscp" / "dstsepp"

The following peertype are defined:

- srcinst (Source NF instance): indicates the Source NF Instance ID, as defined in 3GPP TS 29.510 [8];

- srcservinst (Source NF service instance): indicates the Source NF Service Instance ID, as defined in 3GPP TS 29.510 [8]; if this parameter is present, srcinst shall also be present;

- srcscp (Source SCP): indicates the FQDN of the Source SCP, the format is "SCP-<SCP FQDN>"; this parameter shall only be included by an SCP, i.e. when the HTTP request or response message is originated or relayed by an SCP;

- srcsepp (Source SEPP): indicates the FQDN of the Source SEPP, the format is "SEPP-<SEPP FQDN>"; this parameter shall only be included by a SEPP, i.e. when the HTTP request or response message is originated or relayed by a SEPP;

- dstinst (Destination NF instance): indicates the Destination NF Instance ID, as defined in 3GPP TS 29.510 [8];

- dstservinst (Destination NF service instance): indicates the Destination NF Service Instance ID, as defined in 3GPP TS 29.510 [8]; if this parameter is present, dstinst shall also be present;

- dstscp (Destination SCP): indicates the FQDN of the Destination SCP, the format is "SCP-<SCP FQDN>"; this parameter shall contain the next-hop SCP of the HTTP request or response message to be included by an SCP or SEPP or by clients/servers sending requests/responses to an SCP;

- dstsepp (Destination SEPP): indicates the FQDN of the Destination SEPP, the format is "SEPP-<SEPP FQDN>"; this parameter shall be included by an SCP or by clients/servers sending requests/responses to a SEPP; it may also be included by a SEPP, based on operator's policy.

The header shall contain the source peer information, and should contain the destination peer information if available.

EXAMPLE: 3gpp-Sbi-NF-Peer-Info: srcinst=54804518-4191-46b3-955c-ac631f953ed8; dstinst=54804518-4191-4453-569c-ac631f74765cd

\*\*\* Next Change \*\*\*

##### 5.2.3.3.2 3gpp-Sbi-Sender-Timestamp

The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Sender-Timestamp-Header = "3gpp-Sbi-Sender-Timestamp:" OWS day-name "," SP date1 SP time-of-day "." milliseconds SP "GMT"

milliseconds = 3DIGIT

day-name, date1, time-of-day shall comply with the definition in clause 7.1.1.1 of IETF RFC 7231 [11].

When a 3gpp-Sbi-Sender-Timestamp header field is generated, the sender should generate its field value as the best available approximation of the date and time of message generation.

NOTE: This is the same format as the Date header of clause 7.1.1.2 of IETF RFC 7231 [11], but with the time expressed with a millisecond granularity.

EXAMPLE: 3gpp-Sbi-Sender-Timestamp: Sun, 04 Aug 2019 08:49:37.845 GMT

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.3 3gpp-Sbi-Max-Rsp-Time

The header indicates the duration, expressed in milliseconds since the request was originated, during which the HTTP client waits for a response. See clause 6.11.2.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Max-Rsp-Time-Header = "3gpp-Sbi-Max-Rsp-Time:" OWS 1\*5DIGIT

EXAMPLE: 3gpp-Sbi-Max-Rsp-Time: 10000

\*\*\* Next Change \*\*\*

##### 5.2.3.3.4 3gpp-Sbi-Correlation-Info

The header contains correlation information e.g. UE identifier related to the HTTP request or response.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Correlation-Info-Header = "3gpp-Sbi-Correlation-Info:" OWS correlationinfo \*( ";" OWS correlationinfo )

correlationinfo = ctype "-" cvalue

ctype = "imsi" / "impi" / "suci" / "nai" / "gci" / "gli" / "impu" / "msisdn" / "extid" / "imei" / "imeisv" / "mac" / "eui" / token

cvalue = 1\*( tchar / "@" )

NOTE 1: Only one of each ctype can be included in the 3gpp-Sbi-Correlation-Info header; the possibility to include more than one of the same ctype is kept for future extensibility.

NOTE 2: token is defined for future extensibility. See clause 3.2.6 of IETF RFC 7230 [12] for the "token" type definition.

The token of ctype shall not use the dash ("-") character.

The format of cvalue shall comply with the data type description provided in Table 5.2.3.3.4‑1.

Table 5.2.3.3.4-1: cvalue format

|  |  |
| --- | --- |
| ctype | Description |
| imsi | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for IMSI and starting after the string "imsi-" |
| impi | imsUeId format defined in Table 6.1.3.2.2‑1 of TS 29.562 [45] for IMPI and starting after the string "impi-" |
| suci | SupiOrSuci format defined in Table 5.3.2‑1 of TS 29.571 [13] for SUCI and starting after the string "suci-" |
| nai | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for NAI and starting after the string "nai-" |
| gci | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for GCI and starting after the string "gci-" |
| gli | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for GLI and starting after the string "gli-" |
| impu | imsUeId format defined in Table 6.1.3.2.2‑1 of TS 29.562 [45] for IMPU and starting after the string "impu-". Depending on whether the IMPU contains a SIP URI or a TEL URI, the corresponding pattern from the definition of imsUeId in Table 6.1.3.2.2‑1 of TS 29.562 [45] shall be used. |
| msisdn | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for MSISDN and starting after the string "msisdn-" |
| extid | VarUeId format defined in Table 5.2.2‑1 of TS 29.571 [13] for External Identifier and starting after the string "extid-" |
| imei | Pei format defined in Table 5.3.2‑1 of TS 29.571 [13] for IMEI and starting after the string "imei-" |
| imeisv | Pei format defined in Table 5.3.2‑1 of TS 29.571 [13] for IMEISV and starting after the string "imeisv-" |
| mac | Pei format defined in Table 5.3.2‑1 of TS 29.571 [13] for MAC address and starting after the string "mac-" |
| eui | Pei format defined in Table 5.3.2‑1 of TS 29.571 [13] for IEEE Extended Unique Identifier (EUI-64) and starting after the string "eui-" |

EXAMPLE 1: When UE identifier used is SUPI and SUPI type is an IMSI:

3gpp-Sbi-Correlation-Info: imsi-345012123123123

EXAMPLE 2: When UE identifier used is PEI and PEI type is an IMEISV:

3gpp-Sbi-Correlation-Info: imeisv-3550121231231230

EXAMPLE 3: When UE identifier used is PEI and PEI type is a MAC address:

3gpp-Sbi-Correlation-Info: mac-00-00-5E-00-53-00

EXAMPLE 4: When UE identifier used is GPSI and GPSI type is an MSISDN:

3gpp-Sbi-Correlation-Info: msisdn-1234567890

EXAMPLE 5: When UE identifier used is GPSI and GPSI type is an External Identifier:

3gpp-Sbi-Correlation-Info: extid-123456789@domain.com

EXAMPLE 6: When UE identifiers used are SUPI and GPSI where SUPI type is an IMSI and GPSI type is an MSISDN:

3gpp-Sbi-Correlation-Info: imsi-345012123123123; msisdn-1234567890

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.5 3gpp-Sbi-Alternate-Chf-Id

The header indicates a primary or a secondary CHF Instance ID. See clause 6.10.3.5.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Alternate-Chf-Id-Header = "3gpp-Sbi-Alternate-Chf-Id:" OWS "nfinst=" nfinst ";" OWS ( "primary" / "secondary" )

Parameter "nfinst" shall indicate an NF Instance ID, as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]; the ABNF is defined in clause 5.2.3.2.8.

EXAMPLE 1: Service response from a primary CHF instance signalling a secondary CHF instance Id:

3gpp-Sbi-Alternate-Chf-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8; secondary

EXAMPLE 2: Service response from a secondary CHF instance signalling a primary CHF instance Id:

3gpp-Sbi-Alternate-Chf-Id: nfinst=54804518-4191-46b3-955c-ac631f953ed8; primary

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.7 3gpp-Sbi-Consumer-Info

This header contains a comma-delimited list of NF service consumer information from an HTTP client (as NF service consumer).

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Consumer-Info-Header = "3gpp-Sbi-Consumer-Info:" 1#( OWS supportedService ";" OWS supportedVersions [ ";" OWS supportedFeatures ] [ ";" OWS acceptEncoding ] [ ";" OWS callback-uri-prefix ]) [ ";" OWS intraPlmnCallbackRoot ";" OWS interPlmnCallbackRoot ]

supportedService = "service=" servicename

servicename = 1\*( "-" / %x61-7A )

supportedVersions = "apiversion=" "(" OWS [ apimajorversion \*( RWS apimajorversion ) OWS ] ")"

apimajorversion = %x31-39 [ \*DIGIT ]

supportedFeatures = "supportedfeatures=" features

features = \*HEXDIG

acceptEncoding = "acceptencoding=" %x22 encodingList %x22

encodingList = #( codings [ weight ] )

intraPlmnCallbackRoot = "intraPlmnCallbackRoot=" OWS sbi-scheme "://" sbi-authority [ prefix ]

interPlmnCallbackRoot = "interPlmnCallbackRoot=" OWS sbi-scheme "://" sbi-authority [ prefix ]

sbi-scheme = "http" / "https"

sbi-authority = host [ ":" port ]

port = \*DIGIT

prefix = path-absolute ; path-absolute production rule from IETF RFC 3986, clause 3.3

callback-uri-prefix = "callback-uri-prefix=" OWS prefix

"service" (Mandatory parameter): Supported Service parameter indicates the name of a service, as defined in 3GPP TS 29.510 [8], which is supported by the sender as NF service consumer.

"apiversion" (Mandatory parameter): Supported Versions parameter indicates the major version(s) of the service API that are supported by the sender as NF service consumer.

"supportedfeatures" (Optional parameter): Supported Features parameter carries a string containing a bitmask in hexadecimal representation, as specified for SupportedFeatures data type in 3GPP TS 29.571 [13], to indicate the feature(s) of the service API that are supported by the sender as NF service consumer.

"acceptencoding" (Optional parameter): Accept Encoding carries a string indicating the accepted content encodings supported by the sender as NF service consumer, when receiving notifications defined by the service. In the ABNF definition, "codings" and "weight" are defined in IETF RFC 7231 [40] clause 5.3.4

"intraPlmnCallbackRoot", "interPlmnCallbackRoot" (Optional parameters): intra plmn callback root and inter plmn callback root supported by the sender as NF service consumer.

"callback-uri-prefix" (Optional parameter): The NF service consumer may include this parameter when providing a Callback URI when the authority part of the Callback URI is shared by several NF service consumer instances. When present, the "callback-uri-prefix" shall be a path-absolute as specified IETF RFC 3986 [14] (i.e. the first path segment(s) after the authority) which is part of the Callback URI provided by a NF service consumer in the corresponding service request message sent to a NF service producer. The authority and "callback-uri-prefix" in the Callback URI shall uniquely identify a consumer service instance. See clause 6.12.1 for the usage of this parameter.

EXAMPLE 1: The NF consumer supports Namf\_EventExposure OpenAPI "v1" without any optional feature:

 3gpp-Sbi-Consumer-Info: service=namf-evts; apiversion=(1)

EXAMPLE 2: The NF consumer supports Nsmf\_EventExposure OpenAPI "v1" and "v2" with optional feature number 1 and accepted encoding "gzip":

 3gpp-Sbi-Consumer-Info: service=nsmf-event-exposure; apiversion=(1 2); supportedfeatures=01; acceptencoding="gzip; q=1.0, \*;q=0.5"

EXAMPLE 3: The NF consumer supports both Namf\_EventExposure OpenAPI "v1" and Nsmf\_EventExposure OpenAPI "v2":

 3gpp-Sbi-Consumer-Info: service=namf-evts; apiversion=(1), service=nsmf-event-exposure; apiversion=(2)

EXAMPLE 4: An AMF service instance supports Nsmf\_PDUSession OpenAPI "v1", provides the callback URI <https://amf45.operator.com/servinst123/pdusession>, whereby the authority is shared by more than one AMF service instance, while the prefix "/servinst123" uniquely identifies a specific AMF service instance:

3gpp-Sbi-Consumer-Info: service=nsmf-pdusession; apiversion=(1); callback-uri-prefix=%2Fservinst123

EXAMPLE 5: The NF consumer supports Namf\_EventExposure OpenAPI "v1" and sends intra PLMN callback root "<https://operator.com>" and inter PLMN callback root "https://5gc.mnc012.mcc345.3gppnetwork.org" in the header:

 3gpp-Sbi-Consumer-Info: service=namf-evts; apiversion=(1); intraPlmnCallbackRoot= https%3A%2F%2Foperator.com; interPlmnCallbackRoot= https%3A%2F%2F5gc.mnc012.mcc345.3gppnetwork.org

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.8 3gpp-Sbi-Response-Info

The header contains a comma-delimited list of additional information related to an HTTP response. It may be included e.g. in a 4xx or 5xx response sent:

- by an SCP to indicate whether it attempted to retransmit the request to alternative HTTP server instances; or

- by an alternative HTTP server instance to indicate whether the corresponding resource or context has been transferred to the alternative HTTP server instance, or by an HTTP server instance to indicate that the failed request shall not be retried.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Response-Info-Header = "3gpp-Sbi-Response-Info:" 1#(OWS resp-info-param [ \*( ";" OWS resp-info-param ) ] )

resp-info-param = resp-info-param-name "=" RWS resp-info-param-value

resp-info-param-name = "request-retransmitted" / "nfinst" / "nfset" / "nfservinst" / "nfserviceset" / "context-transferred" / "no-retry" / token

resp-info-param-value = token

The following parameters are defined:

- "request-retransmitted": this parameter indicates, in an error response, whether the SCP attempted to (re)transmit the request to alternative HTTP server instances. When present, it shall be set to "true" if so, and to "false" otherwise. See clause 6.10.8.1.

- "nfinst", "nfset", "nfservinst", "nfserviceset": one or more of these parameters may be present in an error response, when the request-retransmitted is set to "true". When present, it shall indicate the NF Instances, NF Sets, NF Service Instances or NF Service Sets that were attempted to serve the request. See clause 6.10.8.1. The value of the nfinst, nfset, nfservinst and nfserviceset parameters shall be encoded as defined for the corresponding parameters in clause 5.2.3.2.5.

- "context-transferred": this parameter indicates, in an error response, whether the corresponding resource or context has been transferred to the HTTP server instance sending the response. When present, it shall be set to "true" if the request has been transferred, i.e. the subsequent requests towards the resource or context shall be sent to the HTTP server instance sending the response, and to "false" otherwise.

- "no-retry": this parameter indicates, in an error response, whether the failed request can be retried at other alternative HTTP server instance or not. When present, it shall be set to "true" if the failed request shall not be retried at other alternative NF instances, and to "false" otherwise.

NOTE: Additional parameters can be defined in future versions of the specification.

EXAMPLE 1: 3gpp-Sbi-Response-Info: request-retransmitted=true

EXAMPLE 2: 3gpp-Sbi-Response-Info: request-retransmitted=true; nfinst=54804518-4191-46b3-955c-ac631f953ed8; nfinst=54804518-4191-46b3-955c-ac631f953456; nfinst=54804518-4191-46b3-955c-ac631f953780

EXAMPLE 3: 3gpp-Sbi-Response-Info: context-transferred=false; no-retry=true

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.10 3gpp-Sbi-Selection-Info

The header contains a comma-delimited list of additional (re)selection information for an HTTP request message. It may be included by a NF service consumer or a NF service producer in a HTTP request message for indirect communication. If the header is received by the SCP and the SCP supports the header, the SCP shall:

- avoid forwarding the request message to the target NF as indicated in the 3gpp-Sbi-Target-apiRoot (if present in the request) or the request URI (otherwise) if reselection is set "true", i.e., the SCP shall perform a reselection; and

- use the selection-criteria included in this header together with 3gpp-Sbi-Routing-Binding or 3gpp-Sbi-Discovery-\* headers whichever available, when the SCP performs the (re)selection of the target NF.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Selection-Info-Header = "3gpp-Sbi-Selection-Info:" 1#( [ OWS "reselection=" reselectionvalue ] [ 1\*( ";" OWS selection-criteria ) ] )

reselectionvalue = "true" / "false"

selection-criteria = selection-action "=" token

selection-action = "not-select-nfservinst" / "not-select-nfserviceset" / "not-select-nfinst" / "not-select-nfset"

- reselection: it is a boolean and set to "false" by default. When it is set to "true", it indicates that the SCP shall perform a reselection, i.e., the SCP shall not forward the request message towards the target as indicated in the target uri or in the 3gpp-Sbi-Target-ApiRoot. When this parameter occurs multiple times in the comma-delimited list, all parameters shall have the same value.

- not-select-nfservinst (the NF service instance(s) that shall not be selected): indicates an NF Service Instance ID. This parameter shall be present if the sender of the request message knows that the target NF or other potential target NF service instance that shall not be selected, e.g., when the target NF service instance is overloaded, or some NF service instances are out of service. (see also clause 6.4.3.4.5.2.1) When this parameter is present, one of not-select-nfserviceset or not-select-nfinst shall be present to enable the SCP to identify the nfservinst.

- not-select-nfserviceset (the NF service instance pertaining to a NF service set in a NF instance that shall not be selected): indicates an NF Service Set ID as defined in clause 28.13 in 3GPP TS 23.003 [15]. This parameter shall be present if the sender of the request message knows that all NF service instances in the NF service set shall not be selected, e.g., when target NF service instance has indicated its overload and the overload scope is NF service set level, in this case, not-select-nfservinst shall not be present. (see also clause 6.4.3.4.5.2.1)

- not-select-nfinst (the NF instance(s) that shall not be selected): indicates an NF Instance ID, as defined in clause 5.2.2.2.2 in 3GPP TS 29.510 [8]. This parameter shall be present if the sender of the request message knows the target NF instance or other potential target NF instance that shall not be selected, e.g., when the target NF instance is overloaded, or other NF instance(s) is out of service, in this case, not-select-nfservinst shall not be present. (see also clause 6.4.3.4.5.2.1)

- not-select-nfset (the NF set that shall not be selected): indicates an NF Set ID, as defined in clause 28.12 in 3GPP TS 23.003 [15]. This parameter may be present, e.g., during an initial resource creation with Delegated Discovery (Indirect Communication Mode D), the NF service consumer knows certain NF set shall not be selected.

EXAMPLE 1: The SCP may or may not perform reselection, but when doing reselection, it shall not select NF instance as identified by 87654321-4191-46b3-955c-ac631f953ed8.

 3gpp-Sbi-Selection-Info: not-select-nfinst=87654321-4191-46b3-955c-ac631f953ed8

EXAMPLE 2: The SCP may or may not perform reselection, but when doing reselection, it shall not select NF service set in the NF instance (as identified in nfi87654321-4191-46b3-955c-ac631f953ed8).

 3gpp-Sbi-Selection-Info: not-select-nfserviceset=setxyz.snnsmf-pdusession.nfi87654321-4191-46b3-955c-ac631f953ed8.5gc.mnc012.mcc345;

EXAMPLE 3: The SCP shall perform reselection; and when doing reselection, it shall not select NF instance as identified by 87654321-4191-46b3-955c-ac631f953ed8.

 3gpp-Sbi-Selection-Info: reselection=true; not-select-nfinst=87654321-4191-46b3-955c-ac631f953ed8

EXAMPLE 4: The SCP shall perform reselection; and when doing reselection, the SCP shall not select NF service instance xyz1 and xyz2 in the NF instance identified by 87654321-4191-46b3-955c-ac631f953ed8, and NF service instance abc1 and abc2 in the NF instance identified by 12345678-4191-46b3-955c-ac631f953ed8.

 3gpp-Sbi-Selection-Info: reselection=true; not-select-nfservinst=xyz1; not-select-nfservinst=xyz2; not-select-nfinst=87654321-4191-46b3-955c-ac631f953ed8, reselection=true; not-select-nfservinst=abc1; not-select-nfservinst=abc2; not-select-nfinst=12345678-4191-46b3-955c-ac631f953ed8

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.11 3gpp-Sbi-Interplmn-Purpose

The header contains the intended purpose for inter-PLMN signaling. See clauses 6.14.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Interplmn-Purpose-Header = "3gpp-Sbi-Interplmn-Purpose:" OWS N32Purpose ":" OWS additional-info

N32Purpose = "ROAMING"

 / "INTER\_PLMN\_MOBILITY"

 / "SMS\_INTERCONNECT"

 / "ROAMING\_TEST"

 / "INTER\_PLMN\_MOBILITY\_TEST"

 / "SMS\_INTERCONNECT\_TEST"

 / "SNPN\_INTERCONNECT"

 / "SNPN\_INTERCONNECT\_TEST"

 / "DISASTER\_ROAMING"

 / "DISASTER\_ROAMING\_TEST"

 / token

additional-info = token

- N32Purpose: The parameter for N32Purpose indicates the intended purpose of inter-PLMN signaling, and values specified in 3GPP TS 29.573 [27] clause 6.1.5.3.9 are used.

EXAMPLE: 3gpp-Sbi-Interplmn-Purpose: ROAMING: usecaseA

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.12 3gpp-Sbi-Request-Info

The header contains a comma-delimited list of additional information related to a HTTP request which may be included by a NF or a SCP, to indicate e.g.:

- whether the HTTP request message is involving a reselection of an alternative NF;

- whether the HTTP request message is a retransmission of the message, i.e. the request message has been sent but being rejected with a temporary failure or timeout;

When the header is included by a NF acting as a HTTP client, an idempotency-key may be included for a non-idempotent request to enable the receiver to detect possible duplicated request messages as specified in clause 5.2.8.

The receiving NF may use the header, e.g. to determine whether to accept the request.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Request-Info-Header = "3gpp-Sbi-Request-Info:" 1#(OWS req-param [ \*( ";" OWS req-add-param ) ] )

req-param = req-param-name "=" RWS req-param-value

req-add-param = req-add-param-name "=" RWS req-param-value

req-param-name = "retrans" / "redirect" / "reason" / "idempotency-key" / token

req-add-param-name = "receivedrejectioncause" / token

req-param-value = token

The following parameters are defined:

- "reason": indicates the reason for which the NF resends or redirects the HTTP request message. This may take one of the following values:

- "unreachable": indicates that the HTTP request is redirected to an alternative NF due to the request URI (e.g. the resource URI or Notification/callback URI) is not reachable;

- "overloaded": indicates that the HTTP request is redirected to an alternative NF as result of overload control enforcement, by doing redirection towards an alternative NF (see clause 6.4.3.5.1);

- "3xx-redirect": indicates that the HTTP request is redirected to an alternative NF as result of receiving a 3xx status code.

- "temporary-rejection-cause": indicates the HTTP request is retransmitted towards the same or alternative NF due to a temporary rejection.

- "receivedrejectioncause": indicates a temporary rejection application cause received from the NF or SCP (for last attempt) as defined in clause 5.2.7.2, when the "retrans" parameter is set to "true" and the reason is set to "temporary-rejection-cause". The cause data type is specified in clause 5.2.4.1 of 3GPP TS 29.571 [13].

- "retrans": it is a boolean and shall be set to "true" to indicate that the request message has been retransmitted e.g. when the request didn't get any response or get a temporary failure cause, otherwise the "retrans" shall not be present.

- "redirect": it is a boolean and shall be set to "true" to indicate that the request message has been redirected to an alternative NF.

- "idempotency-key": it is a string and may be encoded using Universally Unique Identifier (UUID), as described in IETF RFC 4122 [47], to uniquely identify a request message (to be received) in the target NF. See clause 5.2.8.

EXAMPLE 1: For a request retransmitted to an alternative NF due to the rejection by the original target NF with a temporary rejection cause:

3gpp-Sbi-Request-Info: retrans=true; redirect=true; reason=temporary-rejection-cause; receivedrejectioncause=INSUFFICIENT\_RESOURCES

EXAMPLE 2: For a request sent towards an alternative NF due to the original target NF not reachable:

3gpp-Sbi-Request-Info: redirect=true; reason=unreachable

EXAMPLE 3: For a non-idempotent request:

 3gpp-Sbi-Request-Info: idempotency-key=54804518-4191-46b3-955c-ac631f953ed8

#####

\*\*\* Next Change \*\*\*

##### 5.2.3.3.13 3gpp-Sbi-Retry-Info

The header may be included in a HTTP request message for indirect communication to indicate that the request shall only be sent once and shall not be retried.

The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

Sbi-Retry-Info-Header = "3gpp-Sbi-Retry-Info:" OWS retriesindication

retriesindication = "no-retries"

The following value is defined:

- "no-retries" indicates that the request shall only be sent once and shall not be retried to the same nor alternative endpoints of the same target NF service instance nor towards another target NF service instance once the request has been forwarded once.

EXAMPLE 1: NF service consumer instructing the SCP to not perform any retries:

 3gpp-Sbi-Retry-Info: no-retries

EXAMPLE 2: NF service consumer instructing the SCP to perform an NF reselection, not reselecting the NF instance identified by 87654321-4191-46b3-955c-ac631f953ed8, and to not perform any retries then if no successful response is received from the reselected NF instance.

 3gpp-Sbi-Selection-Info: reselection=true; not-select-nfinst=87654321-4191-46b3-955c-ac631f953ed8
 3gpp-Sbi-Retry-Info: no-retries

\*\*\* End of Changes \*\*\*