3GPP TSG SA WG2 #166 S2-2412762

18 - 22 November 2024, Orlando, USA (revision of 12493 was S2-2411775 was S2-2411077)

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **5629** | **rev** | **7** | **Current version:** | **19.1.0** |  |
|  |
| *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:***  | Energy related information for NF selection and discovery |
|  |  |
| ***Source to WG:*** | Samsung, [Rakuten Mobile, Vivo], NEC, [ZTE], ETRI, [Nokia, Huawei, HiSilicon], Motorola Mobile Com Technology, Lenovo, [InterDigital], SK Telecom, China Mobile, Toyota, Deutsche Telekom |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | EnergySys |  | ***Date:*** | 2024-11-08 |
|  |  |  |  |  |
| ***Category:*** | ***B*** |  | ***Release:*** | *Rel-19* |
|  | *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:*** | Based on KI#3 conclusion in TR 23.700-66, NF discovery and (re-)selection should support the use of energy related information as one of criteria for NF selection. |
|  |  |
| ***Summary of change:*** | * Energy related information to be included to the NF profile is introduced.
* Energy related information awared NF discovery and selection principles and related procedure descriptions are introduced.
 |
|  |  |
| ***Consequences if not approved:*** | The NF selection/re-selection related functionalities considering energy saving and energy efficiency cannot be supported. |
|  |  |
| ***Clauses affected:*** | 5.X.Y (new), 5.X.Z (new), 6.2.6.2, 6.3.1 |
|  |  |
|  | **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 (all text is new)\* \* \* \*

### 5.X.Y Energy related information in NF profile

NRF maintains energy related information as part of NF profile for the registered NF instance. The energy related information includes the following information as defined in Table 5.X.2-1.

Table 5.X.2-1: Energy related information in NF profile

|  |  |  |
| --- | --- | --- |
| Information | Description | Category |
| NF Energy Saving State Information  | This parameter indicates the energySavingstate will be applied to the NF and optionally the associated timing information (e.g. the NF will be in energySaving state at a timestamp and/or for a time period).  | Optional |
| Energy Priority Information | This parameter indicates the priority relative to other NFs of the same type by considering the energy characteristics of the NF and the energy saving state of the NF (NOTE 1).  | Optional |
| NOTE 1:The Energy Priority Information is operator-specific. Based on operator policy and configuration, the determination of Energy Priority Information may consider various energy characteristics of the NF, for example by weighting of different energy characteristics. The energy characteristics may include one or list of: energy consumption, energy efficiency, renewable energy and/or carbon emission factors, etc.  |

Editor’s Note: whether the NF energy saving state information and/or priority information can be combined into one parameter and whether additional parameters are needed for NF profile is FFS.

Editor’s Note: whether an existing parameter defined by SA5 can be used instead of NF Energy Saving State Information is FFS.

\* \* \* \* Second change \* \* \* \*

6.2.6.2 NF profile

NF profile of NF instance maintained in an NRF includes the following information:

- NF instance ID.

- NF type.

- PLMN ID in the case of PLMN, PLMN ID + NID in the case of SNPN.

- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID.

- FQDN or IP address of NF.

- NF capacity information.

- NF priority information.

NOTE 1: This parameter is used for AMF selection, if applicable, as specified in clause 6.3.5. See clause 6.1.6.2.2 of TS 29.510 [58] for its detailed use.

- NF Set ID.

- NF Service Set ID of the NF service instance.

- NF Specific Service authorization information.

- if applicable, Names of supported services.

- Endpoint Address(es) of instance(s) of each supported service.

- Identification of stored data/information.

NOTE 2: This is only applicable for a UDR profile. See applicable input parameters for Nnrf\_NFManagement\_NFRegister service operation in clause 5.2.7.2.2 of TS 23.502 [3]. This information applicability to other NF profiles is implementation specific.

- Other service parameter, e.g. DNN or DNN list, notification endpoint for each type of notification that the NF service is interested in receiving.

- Location information for the NF instance.

NOTE 3: This information is operator specific. Examples of such information can be geographical location, data centre.

- TAI(s).

- NF load information.

- Energy related information, see clause 5.X.Y.

- Routing Indicator, Home Network Public Key identifier, for UDM and AUSF.

- For UDM, AUSF and NSSAAF in the case of access to an SNPN using credentials owned by a Credentials Holder with AAA Server, identification of Credentials Holder (i.e. the realm of the Network Specific Identifier based SUPI).

- For UDM and AUSF, and if UDM/AUSF is used for access to an SNPN using credentials owned by a Credentials Holder, identification of Credentials Holder (i.e. the realm if Network Specific Identifier based SUPI is used or the MCC and MNC if IMSI based SUPI is used); see clause 5.30.2.1.

- For AUSF and NSSAAF in the case of SNPN Onboarding using a DCS with AAA server, identification of DCS (i.e. the realm of the Network Specific Identifier based SUPI).

- For UDM and AUSF, and if UDM/AUSF is used as DCS in the case of SNPN Onboarding, identification of DCS (i.e. the realm if Network Specific Identifier based SUPI, or the MCC and MNC if IMSI based SUPI).

- One or more GUAMI(s), in the case of AMF.

- For the UPF, see clause 5.2.7.2.2 of TS 23.502 [3].

- UDM Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of internal group identifiers, range(s) of external group identifiers for UDM.

- UDR Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of external group identifiers for UDR.

- AUSF Group ID, range(s) of SUPIs for AUSF.

- PCF Group ID, range(s) of SUPIs for PCF.

- HSS Group ID, set(s) of IMPIs, set(s) of IMPU, set(s) of IMSIs, set(s) of PSIs, set(s) of MSISDN for HSS.

- For NWDAF, the following information are supported:

- Analytics ID(s) (possibly per service).

- NWDAF Serving Area information (i.e. list of TAIs for which the NWDAF can provide services and/or data).

- Supported Analytics Delay per Analytics ID (if available).

- NF types of the NF data sources, NF Set IDs of the NF data sources, if available.

- Analytics aggregation capability (if available).

- Analytics metadata provisioning capability (if available).

- ML model Filter information parameters include S-NSSAI(s) and Area(s) of Interest for the trained ML model(s) per Analytics ID(s).

- ML Model Interoperability indicator (if available) per Analytics ID(s).

- FL capability information per analytics ID including FL capability type (i.e. FL server and/or FL client, if available).

- Time interval supporting FL (if available).

- Accuracy checking capability for ML model accuracy monitoring or Analytics Accuracy Monitoring (if available).

- Roaming exchange capability (if available).

NOTE 4: The NWDAF's Serving Area information is common to all its supported Analytics IDs.

NOTE 5: The Analytics IDs supported by the NWDAF may be associated with a Supported Analytics Delay i.e. the Analytics report can be generated with a time (including data collection delay and inference delay) in less than or equal to the Supported Analytics Delay.

NOTE 6: The determination of Supported Analytics Delay, and how the NWDAF avoid updating its Supported Analytics Delay in NRF frequently is NWDAF implementation specific.

- Event ID(s) supported by AFs, in the case of NEF.

- Event Exposure service supported event ID(s) by UPF.

- Application Identifier(s) supported by AFs, in the case of NEF.

- Range(s) of External Identifiers, or range(s) of External Group Identifiers, or the domain names served by the NEF, in the case of NEF.

NOTE 7: This is applicable when NEF exposes AF information for analytics purpose as detailed in TS 23.288 [86].

NOTE 8: It is expected service authorization information is usually provided by OA&M system, and it can also be included in the NF profile in the case that e.g. an NF instance has an exceptional service authorization information.

NOTE 9: The NRF may store a mapping between UDM Group ID and SUPI(s), UDR Group ID and SUPI(s), AUSF Group ID and SUPI(s) and PCF Group ID and SUPI(s), to enable discovery of UDM, UDR, AUSF and PCF using SUPI, SUPI ranges as specified in clause 6.3 or interact with UDR to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID based on UE identity, e.g. SUPI (see clause 6.3.1 for details).

- IP domain list as described in clause 6.1.6.2.21 of TS 29.510 [58], Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes, Range(s) of SUPIs or Range(s) of GPSIs or a BSF Group ID, in the case of BSF.

- SCP Domain the NF belongs to.

- DCCF Serving Area information, NF types of the data sources, NF Set IDs of the data sources, if available, in the case of DCCF.

- Supported DNAI list, in the case of SMF.

- For SNPN, capability to support SNPN Onboarding in the case of AMF and capability to support User Plane Remote Provisioning in the case of SMF.

- IP address range, DNAI for UPF.

- Supported DNS security protocols, in the case of EASDF.

- Additional V2X related NF profile parameters are defined in TS 23.287 [121].

- Additional ProSe related NF profile parameters are defined in TS 23.304 [128].

- Additional MBS related NF profile parameters are defined in TS 23.247 [129].

- Additional UAS related NF profile parameters are defined in TS 23.256 [136].

- Additional Ranging based services and Sidelink Positioning related NF profile parameters are defined in TS 23.586 [180].

- For additional information in PCF profile, see clause 5.2.7.2.2 of TS 23.502 [3].

\* \* \* \* Third change \* \* \* \*

6.3.1 General

The NF discovery and NF service discovery enable Core Network entities (NFs or Service Communication Proxy (SCP)) to discover a set of NF instance(s) and NF service instance(s) for a specific NF service or an NF type. NF service discovery is enabled via the NF discovery procedure, as specified in clauses 4.17.4, 4.17.5, 4.17.9 and 4.17.10 of TS 23.502 [3].

Unless the expected NF and NF service information is locally configured on the requester NF, e.g. when the expected NF service or NF is in the same PLMN as the requester NF, the NF and NF service discovery is implemented via the Network Repository Function (NRF). NRF is the logical function that is used to support the functionality of NF and NF service discovery and status notification as specified in clause 6.2.6.

NOTE 1: NRF can be colocated together with SCP e.g. for communication option D, depicted in Annex E.

In order for the requested NF type or NF service to be discovered via the NRF, the NF instance need to be registered in the NRF. This is done by sending a Nnrf\_NFManagement\_NFRegister containing the NF profile. The NF profile contains information related to the NF instance, such as NF instance ID, supported NF service instances (see clause 6.2.6 for more details regarding the NF profile). The registration may take place e.g. when the producer NF instance and its NF service instance(s) become operative for the first time. The NF service registration procedure is specified in clause 4.17.1 of TS 23.502 [3].

In order for the requester NF or SCP to obtain information about the NF and/or NF service(s) registered or configured in a PLMN/slice, based on local configuration the requester NF or SCP may initiate a discovery procedure with the NRF by providing the type of the NF and optionally a list of the specific service(s) it is attempting to discover. The requester NF or SCP may also provide other service parameters e.g. slicing related information. For the detailed service parameter(s) used for specific NF and NF service discovery refer to clause 5.2.7.3.2 of TS 23.502 [3]. The requester NF may also provide NF Set related information to enable reselection of NF instances within the NF set. The requester NF may also provide the required supported features of the NF.

For some Network Functions which have access to the subscription data (e.g. HSS, UDM) the NRF may need to resolve the NF Group ID corresponding to a subscriber identifier. If the NRF has no stored configuration mapping identity sets/ranges to NF Group ID locally, the NRF may retrieve the NF Group ID corresponding to a specific subscriber identifier from the UDR using the Nudr\_GroupIDmap\_Query service operation.

In the case of Indirect Communication, a NF Service Consumer employs an SCP which routes the request to the intended target of the request.

If the requester NF is configured to delegate discovery, the requester NF may omit the discovery procedure with the NRF and instead delegate the discovery to the SCP; the SCP will then act on behalf of the requester NF. In this case, the requester NF adds any necessary discovery and selection parameters to the request in order for the SCP to be able to do discovery and associated selection. The SCP may interact with the NRF to perform discovery and obtain discovery result and it may interact with the NRF or UDR to obtain NF Group ID corresponding to subscriber identifier.

NOTE 2: For delegated discovery of the HSS or the UDM, the SCP can rely on the NRF to discover the group of HSS/UDM instance(s) serving the provided user identity, or in some deployments the SCP can first query the UDR for the HSS/UDM Group ID for the provided user identity. It is expected that the stage 3 defines a single encoding for the user identity provided by the service consumer that can be used for both variants of delegated discovery to avoid that the service consumer needs to be aware of the SCP behaviour.

The NRF provides a list of NF instances and NF service instances relevant for the discovery criteria. The NRF may provide the IP address or the FQDN of NF instance(s) and/or the Endpoint Address(es) of relevant NF service instance(s) to the NF Consumer or SCP. The NRF may also provide NF Set ID and/or NF Service Set ID to the NF Consumer or SCP. The response contains a validity period during which the discovery result is considered valid and can be cached. The result of the NF and NF service discovery procedure is applicable to any subscriber that fulfils the same discovery criteria. The entity that does the discovery may cache the NF profile(s) received from the NF/NF service discovery procedure. During the validity period, the cached NF profile(s) may be used for NF selection for any subscriber matching the discovery criteria.

NOTE 3: Refer to TS 29.510 [58] for details on using the validity period.

In the case of Direct Communication, the requester NF uses the discovery result to select NF instance and a NF service instance that is able to provide a requested NF Service (e.g. a service instance of the PCF that can provide Policy Authorization).

In the case of Indirect Communication without Delegated Discovery, the requester NF uses the discovery result to select a NF instance while the associated NF service instance selection may be done by the requester NF and/or an SCP on behalf of the requester NF.

In both the cases above, the requester NF may use the information from a valid cached discovery result for subsequent selections (i.e. the requester NF does not need to trigger a new NF discovery procedure to perform the selection).

In the case of Indirect Communication with Delegated Discovery, the SCP will discover and select a suitable NF instance and NF service instance based on discovery and selection parameters provided by the requester NF and optional interaction with the NRF. The NRF to be used may be provided by the NF consumer as part of the discovery parameters, e.g. as a result of a NSSF query. The SCP may use the information from a valid cached discovery result for subsequent selections (i.e. the SCP does not need to trigger a new NF discovery procedure to perform the selection).

NOTE 4: In a given PLMN, Direct Communication, Indirect Communication, or both may apply.

The requester NF or SCP may subscribe to receive notifications from the NRF of a newly updated NF profile of an NF (e.g. NF service instances taken in or out of service), or newly registered de-registered NF instances. The NF/NF service status subscribe/notify procedure is defined in clauses 4.17.7 and 4.17.8 of TS 23.502 [3].

For NF and NF service discovery across PLMNs, the NRF in the local PLMN interacts with the NRF in the remote PLMN to retrieve the NF profile(s) of the NF instance(s) in the remote PLMN that matches the discovery criteria. If the NRF in the local PLMN indicated support, for the local PLMN, of indirect communication with delegated discovery with NF (re)selection at target PLMN (Model D in Annex E with SCP in target PLMN doing NF (re)selection) and/or of indirect communication without delegated discovery with NF (re)selection at target PLMN (Model C in Annex E with SCP in target PLMN doing NF (re)selection), based on operator's policy and the capabilities of the local PLMN, the NRF in the remote PLMN may also return an indication that indirect communication with delegated discovery with NF (re)selection at target PLMN is requested or that indirect communication without delegated discovery with NF (re)selection at target PLMN is requested and, for delegated discovery in target PLMN, omit NF profiles. The NRF in the local PLMN reaches the NRF in the remote PLMN by forming a remote PLMN specific query using the PLMN ID provided by the requester NF. The remote PLMN NRF may further interact with a target PLMN NRF as specified in clause 6.2.6.1. Based on operator's policy and configuration, the NRF in the local PLMN may also determine without interaction with the NRF in the remote PLMN that indirect communication with delegated discovery with NF (re)selection at target PLMN is requested for communication for that remote PLMN. The NF/NF service discovery procedure across PLMNs is specified in clauses 4.17.5, 4.17.10 and 4.17.10a of TS 23.502 [3].

NOTE 5: See TS 29.510 [58] for details on using the target PLMN ID specific query to reach the NRF in the remote PLMN.

NOTE 6: The NRF in the local PLMN can interact with NRFs in target PLMNs already before receiving related discovery requests to inquire the support of indirect communication by those target PLMNs, cache the received information, and use it for subsequent discovery requests.

For topology hiding, see clause 6.2.17.

For NF and NF service discovery and selection based on the Energy related information, see clause 5.X.Y.

\* \* \* \* End of changes \* \* \* \*