**TSG SA Meeting #87-e SP-200063**

**e-meeting, 17-20 March 2020 (was S2-2001329)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **23.502** | **CR** | **2002** | **rev** | **3** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
|  | | | | | | | | |
| *For* [***HELP***](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:*** | Corrections on I-NEF call flow | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | SA2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_CIoT | | | | |  | ***Date:*** | | | 2020-03-17 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | *Rel-16* |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12) Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Original CR from Nokia, Nokia Shanghai Bell.  I-NEF service operation parameters are incorrect and clause 4.15.3.2.3a Step 3 is incomplete, as this step is notification from SMF to AMF, but the referred step 6e in 4.15.3.2.3 is SMF notification to NEF. Notification events detected by SMF do not require corresponding monitoring event in the AMF, as the SMF notifies the NEF (I-NEF) directly.  I-NEF subscription to AMF in step 2d is superfluous, as the AMF has already received the I-NEF routing address in the Ninef\_EventExposure\_Subscribe request.  Event notifications should be conditional, depending on the detection of the subscribed monitoring event by either SMF or AMF.  Public identifiers cannot be used between SMF/AMF and I-NEF.  The handling of redundant I-NEF configuration is not removed from the old SMF after SMF change.  Event filtering is not I-NEF task. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | I-NEF call flow and service operation parameters are corrected:  - AMF/SMF store the I-NEF event notification address from the Ninef\_EventNotification\_Subscribe Response.  - For a given monitoring event, either AMF or SMF configures the I-NEF, but not both (depending on which one of the two is monitoring that event)  - If I-NEF is needed, the AMF/SMF configures I-NEF with routing path to NEF and sends notifications to that I-NEF.  - In clause 4.15.3.2.3a step 2-3, the I-NEF need not subscribe to notifications from the AMF or SMF.  - Monitoring event notifications are conditional, subject to the notification event detection.  - Unnecessary Event Filter parameter is removed from the I-NEF configuration.  - user is identified by SUPI or Internal Group Identifier between SMF/AMF and I-NEF.  - the old SMF removes its I-NEF association after SMF change.  Various editorial mistakes are also corrected. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Lack of guidance from SA2 to CT3 to design the stage 3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.15.3.1, 4.15.3.2.3a, 4.26.5.3, 5.2.6A.2.2, 5.2.6A.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | |  | | |
| ***affected:*** | |  | **X** | Test specifications | | | |  | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | |  | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Changes in r2: Ninef\_EventExposure\_Notify is replaced by AMF and SMF notifications that are already supported by NEF in order to allow better re-use of service operations both in specification and implementation.  Revision into SA#87e  #1 Add NOTE that Ninef\_EventExposure serivce is not subscribing to receive I-NEF notifications but configuring a routing address for sending its own notifications by means of subscription on behalf of NEF (as captured in SA2 LS response [S2-2001575](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_136AH_Incheon/Docs/S2-2001575.zip) to CT3).  #2 Change step 5 (i.e. Nsmf\_EventExposure\_Notify) and step 7 (i.e. Namf\_EventExposure\_Notify) in Rev2 back to Ninef\_EventExposure\_Notify, reasoning:  I-NEF is not a provider of Namf\_EventExposure\_Notify (or Nsmf\_EventExposure\_Notify) service operation, therefore in our view, such modelling is not aligned with service based Subscribe/Notify principle.  In the case that Namf\_EventExposure\_Notify (or Nsmf\_EventExposure\_Notify) is updated, in our view, the I-NEF needs to recognize the update and decide what to be sent to the NEF, that is, the impact on I-NEF is inevitable.  Any optimization related to service operation reuse, it’s suggested to leave it to stage 3 as such discussion is within their remit.  #3 Remove changes to 5.2.6A.1 and 5.2.6A.2.4 which are not needed. | | | | | | | | |

*FIRST CHANGE*

#### 4.15.3.1 Monitoring Events

The Monitoring Events feature is intended for monitoring of specific events in 3GPP system and making such Monitoring Events information reported via the NEF. It is comprised of means that allow NFs in 5GS for configuring the specific events, the event detection, and the event reporting to the requested party.

To support the roaming agreement requirements for monitoring features in roaming scenarios between the HPLMN and the VPLMN, I-NEF may be deployed as defined in clause 6.2.5a of TS 23.501 [2]. If I-NEF is deployed, the AMF or SMF in the VPLMN provides the configuration for a given Monitoring Event to the I-NEF and sends subsequent Monitoring Event reports via the I-NEF. Based on the Monitoring Event routing configuration, the I-NEF forwards normalized Monitoring Event report towards the NEF.

The set of capabilities required for monitoring shall be accessible via NEF to NFs in 5GS. Monitoring Events via the UDM, the AMF, the SMF and the GMLC enables NEF to configure a given Monitoring Event at UDM, AMF, SMF or GMLC, and reporting of the event via UDM and/or AMF or GMLC. Depending on the specific Monitoring Event or information, it is the AMF, GMLC or the UDM that is aware of the Monitoring Event or information and reports it via the NEF.

The following table enumerates the monitoring events and their detection criteria:

Table 4.15.3.1-1: List of events for monitoring capability

|  |  |  |
| --- | --- | --- |
| Event | Detection criteria | Which NF detects the event |
| Loss of Connectivity | Network detects that the UE is no longer reachable for either signalling or user plane communication (see NOTE 4).  The AF may provide a Maximum Detection Time, which indicates the maximum period of time without any communication with the UE after which the AF is to be informed that the UE is considered to be unreachable. | AMF |
| UE reachability | Detected when the UE transitions to CM-CONNECTED state or when the UE will become reachable for paging, e.g., Periodic Registration Update timer. It indicates when the UE becomes reachable for sending either SMS or downlink data to the UE.  The AF may provide the following parameters:  1) Maximum Latency;  2) Maximum Response Time;  3) Suggested number of downlink packets. (see NOTE 5). | AMF |
| Location Reporting | This event is detected based on the Event Reporting Information Parameters that were received in the Monitoring Request (one-time reporting, maximum number of reports, maximum duration of reporting, periodicity, etc., as specified in clause 4.15.1).  It indicates either the Current Location or the Last Known Location of a UE.  When AMF is the detecting NF:  One-time and Continuous Location Reporting are supported for the Current Location. For Continuous Location Reporting the serving node(s) sends a notification every time it becomes aware of a location change, with the granularity depending on the accepted accuracy of location. (see NOTE 1) For Last Known Location only One-time Reporting is supported  When GMLC is the detecting NF:  Immediate and Deferred Location Reporting is supported. For Deferred Location Reporting the event types UE availability, Area, Periodic Location and Motion are supported. | AMF, GMLC |
| Change of SUPI-PEI association | This event is detected when the association between PEI and subscription (SUPI) changes (USIM change). | UDM |
| Roaming status | This event is detected when the UE's current roaming status (the serving PLMN and/or whether the UE is in its HPLMN) and notification when that status changes. (see NOTE 2). | UDM |
| Communication failure | This event is detected when RAN or NAS level failure is detected based on connection release and it identifies RAN/NAS release code. | AMF |
| Availability after Downlink Data Notification failure | This event is detected when the UE becomes reachable again after data delivery failure. | AMF |
| PDU Session Status | This event is detected when PDU session is established or released. (see NOTE 6) | SMF |
| Number of UEs present in a geographical area | This event is detected based on the Event Reporting Information Parameters that were received in the Monitoring Request (Level of aggregation, Sampling ratio, see clause 4.15.1).  It indicates the number of UEs that are in the geographic area described by the AF. The AF may ask for the UEs that the system knows by its normal operation to be within the area (Last Known Location) or the AF may request the system to also actively look for the UEs within the area (Current Location). | AMF |
| CN Type change | The event is detected when the UE moves between EPC and 5GC. It indicates the current CN type for a UE or a group of UEs when detecting that the UE switches between being served by a MME and an AMF or when accepting the event subscription. (see NOTE 3) | UDM |
| Downlink data delivery status | It indicates the downlink data delivery status in the core network. Events are reported at the first occurrence of packets being buffered, transmitted or discarded, including:  - Downlink data in extended buffering, including:  - First data packet buffered event  - Estimated buffering time, as per clause 4.2.3.3  - First downlink data transmitted event  - First downlink data discarded event | SMF |
| UE reachability for SMS delivery | This event is detected when an SMSF is registered for a UE. This enables the UE to receive an SMS.  HSS can subscribe to notifications about SMSF registration events in UDM for a given UE as defined in TS 23.632 [68]. | UDM: reachability for SMS |
| User State Information in 5GS | Provides user state information in 5GS. | AMF |
| NOTE 1: Location granularity for event request, or event report, or both could be at cell level (Cell ID) or TA level. The granularity can also be expressed by other formats such as geodetic uncertainty shapes (e.g. polygons, circles, etc.) or civic addresses (e.g. streets, districts, etc.) which can be mapped by NEF to AMF specific granularity levels.  NOTE 2: Roaming status means whether the UE is in HPLMN or VPLMN.  NOTE 3: CN type of CN Type change event is defined in clause 5.17.5.1 of TS 23.501 [2].  NOTE 4: In the case of UDM service operation information flow, the UDM should set the subscribed periodic registration timer to a smaller value than the value of Maximum Detection Time, since the value of the mobile reachable timer is larger than the value of the periodic registration timer.  NOTE 5: Maximum Latency, Maximum Response Time and Suggested number of downlink packets are defined in clause 4.15.6.3a.  NOTE 6: The NEF makes a mapping between the 5GS internal event "PDU Session Status" and the T8 API event "PDN Connectivity Status". | | |

*NEXT CHANGE*

##### 4.15.3.2.3a I-NEF service operations information flow

The procedure is used by the NF (AMF, SMF) in VPLMN to provision monitoring configurations and to explicitly cancel a previous monitoring configuration at I-NEF. Cancelling is done by sending Ninef\_EventExposure\_UnSubscribe request identifying the monitoring configuration to cancel. The notification steps 3 to 5 are not applicable in cancellation case.



Figure4.15.3.2.3a-1: Ninef\_EventExposure\_Subscribe, Unsubscribe and Notify operations

1. NEF or UDM subscribe or unsubscribe to the notification of monitoring events at SMF or AMF as refered to steps 1 to 2 in clause 4.15.3.2.1, steps 1 to 3 in clause 4.15.3.2.2, and steps 1 to 5 in clause 4.15.3.2.3.

2a-b. For SMF detected monitoring requests, if the SMF determines that the UE is in roaming and I-NEF is needed, it requests to provision Monitoring Event routing configuration on I-NEF in Ninef\_EventExposure\_Subscribe. The Monitoring Event routing configuration on I-NEF includes the notification endpoint information of the NEF that is expected to receive normalized Notification Reports. I-NEF includes a target address to receive notifications in Ninef\_EventExposure\_Subscribe Response. The SMF updates the monitoring configuration created in step 1 with the notification target address but keeps also the previously stored NEF address in case possible need to remove I-NEF arises later. The I-NEF Monitoring Event routing configuration is removed by sending Ninef\_EventExposure\_UnSubscribe Request.

NOTE1: During SMF change, new SMF does not receive the monitoring configuration from the old SMF.

3a-b. For AMF detected monitoring requests, if the AMF determines that the UE is in roaming and I-NEF is needed, it requests to provision Monitoring Event routing configuration on I-NEF in Ninef\_EventExposure\_Subscribe. The Monitoring Event routing configuration on I-NEF includes the notification endpoint information of the NEF that is expected to receive normalized Notification Reports. I-NEF includes a target address to receive notifications in Ninef\_EventExposure\_Subscribe Response. The AMF updates the monitoring configuration created in step 1 with the notification target address but keeps also the previously stored NEF address in case it needs to be restored after inter-AMF mobility that removes the need for I-NEF. The I-NEF Monitoring Event routing configuration is removed by sending Ninef\_EventExposure\_UnSubscribe Request.

NOTE2: During inter-AMF mobility, the new AMF receives the notification target address as part of the AMF context transfer which includes also the monitoring configuration.

4. [Conditional- depending on the Event] The SMF detects that the related event occurs and sends the event report in Nsmf\_EventExposure\_Notify to the I-NEF that was configured in step 2. Refer to step 6e in clause 4.15.3.2.3.

5. [Conditional - depending on the Event] The I-NEF performs normalization of reports and generation of charging/accounting information as defined in clause 6.2.5a of TS 23.501 [2]. The I-NEF then sends the Ninef\_EventExposure\_Notify message to the NEF that was configured in step 2.

6. [Conditional – depending on the Event] The AMF detects the related event occurs, it sends the event report by means of Namf\_EventExposure\_Notify message to the I-NEF that was configured in step 3.

7. [Conditional - depending on the Event] The I-NEF performs normalization of reports and generation of charging/accounting information as defined in clause 6.2.5a of TS 23.501 [2]. The I-NEF sends the event report by means of Ninef\_EventExposure\_Notify message to the NEF that was configured in step 3.

*NEXT CHANGES*

#### 4.26.5.3 SMF Context Transfer procedure, LBO or no Roaming, no I-SMF

In the case of dynamic IP address assignment (IPv4 address and/or IPv6 prefix), the procedure in figure 4.26.4.1.1-1 assumes that, if the UE IP address is received from Old SMF, the control of the IP address(es) assigned by Old SMF is moved to New SMF by O&M procedures. New SMF is in full control of the concerned IP address(es) when the transfer is complete.

NOTE 1: If UPF has the IP point of presence from the DNN, the same UPF is used.



Figure 4.26.4.1.1-1: Context transfer of a PDU session

1. SM context transfer is triggered, e.g. by OAM to Old SMF including SUPI, PDU session ID and New SMF ID or SMF set ID. The SMF selection by using SMF set ID not applicable when the IP range is managed by SMF.

2. [Conditional - depending on current subscription] Old SMF subscribes to events when UE status becomes CM-IDLE or CM-CONNECTED with RRC inactive state (Namf\_EventExposure\_Subscribe).

3. [Conditional - depending on the event] The AMF detects the monitored event occurs and sends the event report by means of Namf\_EventExposure\_Notify message, to Old SMF.

4. From Old SMF to AMF Nsmf\_PDUSession\_SMContextStatusNotify (SMF transfer indication, Old SMF ID, New SMF ID or SMF set ID from Step 1, PDU Session ID, SUPI, SM Context ID).

5. AMF, or SCP if delegated discovery is used, uses New SMF ID or SMF set ID to select New SMF and sends Nsmf\_PDUSession\_CreateSMContext request (PDU Session ID, Old SMF ID, SM Context ID in Old SMF, UE location info, Access Type, RAT Type, Operation Type, SMF transfer indication). The same PDU Session ID as received in step 4 is used. If the AMF receives the service request from the UE for the PDU session(s) affected by this procedure the AMF delays the transaction with the SMF until the step 13 completes. If the AMF receives the UE context transfer request from the other AMF due to the UE mobility, the AMF defers the response until the step 13 completes. Also, to void infinite waiting time, the AMF starts a locally configured guard timer upon sending the request to the SMF, and the AMF decides the procedure has failed at expiry of the guard timer.

NOTE 2: Either delay or failure of the SM Context transfer may incur timeout or failure in UE procedure(s).

6. From New SMF to Old SMF SMF Nsmf\_PDUSession\_ContextRequest request (SM Context type, SM Context ID, SMF transfer indication). If New SMF is not capable to transfer this SM Context (e.g. it is not responsible for the IP range), steps 9 to 12 are skipped.

7. Old SMF releases the N4 session with the UPF by sending a flag notifying the UPF about the expected re-establishment of the N4 session for the same PDU session. Based on this, if supported, the UPF should delay the release of the N4 session up to step 10.2 to allow for uninterrupted packet handling until the N4 session is re-established by New SMF.

8. From Old SMF to New SMF Nsmf\_PDUSession\_ContextRequest response (SM Context or endpoint where New SMF can retrieve SM Context). The SM Context includes the IP address(es) in case PDU session is of typ IPv4, IPv6 or IPv4v6, or the Ethernet MAC address(es) in case PDU session type Ethernet as well as the UPF to be selected by New SMF. Old SMF starts a timer to monitor the SMF context transferring process.

9. [Conditional] If dynamic PCC is used for the PDU Session, New SMF sets up a new policy association towards PCF.

10.1. UPF receives a N4 session establishment request for the same PDU session from step 7. The parameters from step 8 and, if applies, step 9 are used.

10.2. New SMF performs a full re-establishment of the N4 session, establishing a new N4 session. All information related to the N4 session of Old SMF that is not used by the N4 session of New SMF is removed from UPF if not already done.

11. New SMF registers to UDM. The information stored at the UDM includes SUPI, SMF identity and the associated DNN and PDU Session ID.

12. New SMF subscribes to subscription changes for the UE.

13. From New SMF to AMF: Nsmf\_PDUSession\_CreateSMContext response. If this response indicates a redirect (e.g. another SMF in the set), the procedure moves to step 5 with the indicated endpoint as target.

14. UDM notifies Old SMF that it is deregistered for the PDU Session by sending Nudm\_UECM\_DeregistrationNotification, optionally including New SMF ID

15. [Conditional] If 14 was not received and the timer from step 8 expires, Old SMF re-establishes the N4 session. The UPF may for the purpose use the information stored in step 7. In this case, the procedure ends here.

16. [Conditional] If Nudm\_UECM\_DeregistrationNotification in step 14 was received, Old SMF removes its policy association with PCF. Any changes to the QoS rules need to be sent to the UE when it becomes active.

17. Old SMF releases any internal resources corresponding to the indicated PDU session. Subscribers to SMContextStatusNotify for the transferred SM context are notified of the context transfer and optionally of the new location of the transferred SM context. If old SMF has set up I-NEF routing configurations, then it should delete those that are still valid by sending Ninef\_EventExposure\_Unsubscribe request.

*NEXT CHANGES*

##### 5.2.6A.2.2 Ninef\_EventExposure\_Subscribe operation

**Service operation name:** Ninef\_EventExposure\_Subscribe

**Description:** the consumer subscribes on behalf of a third party, such as NEF, to an event with monitoring configuration in I-NEF.

**Inputs (required):** NF ID, (Set of) Event ID(s) as specified in clause 4.15.3.1, Target of Event Reporting (SUPI or Internal Group Identifier), Event Reporting Information defined in Table 4.15.1-1, Notification Target Address (+ Notification Correlation ID), Subscription Correlation ID.

**Inputs (optional):** Expiry time, Chargeable Party Identifier.

**Outputs (required):** Expiry time (required if the subscription can be expired based on the operator's policy), cause.

**Outputs (optional):** notification target address to receive notifications to be forwarded to the NEF.

NOTE 1: Via I-NEF Event Exposure, the consumer (e.g. AMF or SMF) is not subscribing to receive I-NEF notifications but configuring a routing address for sending its own notifications by means of subscription on behalf of NEF.

*NEXT CHANGE*

##### 5.2.6A.2.3 Ninef\_EventExposure\_Unsubscribe service operation

**Service operation name:** Ninef\_EventExposure\_Unsubscribe

**Description:** the NF consumer deletes Monitoring Event routing configuration for an event if already defined in I-NEF.

**Inputs (required):** Subscription Correlation ID.

**Outputs (required):** Operation execution result indication.

*END OF CHANGES*