**3GPP TSG-SA5 Meeting #142-e *S5-222524***

**, 4th – 12th April 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **28.535** | **CR** | **draftCR** | **rev** | **-** | **Current version:** | **17.4.0** |  |
|  | | | | | | | | |
| *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 | **X** | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clean-up use cases and requirements | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, Deutsche Telekom | | | | | | | | | |
| ***Source to TSG:*** | S5 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCOSLA | | | | |  | ***Date:*** | | | 2022-02-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **C** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Some use cases and requriements do not have a corresponding solution in TS 28.536 and that should be clarified in TS 28.535. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1) Add Editor’s note under 6.1.6 to state use case is not supported  2) Add NOTE under 6.1.7 to state use case is not supported  3) Add Editor’s note under **REQ-CSA-CON-16** to state use case is not supported  4) Add NOTE under **REQ-CSA-CON-17** to state use case is not supported | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The TS 28.535 (stage 1) and TS 28.536 (stage 2/3) are not aligned which may cause confusion and potentially incompatible implementations | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.6, 6.1.7, 6.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 is input to draftCR S5-215622 | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| **1st Change** |

# 6 Specification level use cases and requirements

## 6.1 Use cases

### 6.1.1 Communication service quality assurance and optimization

The goal of the use case is to enable communication service quality assurance and optimization for the set of services provided by the network to certain group (category) of UEs. For example, the set can include the communication services provided via certain NSI(s) or to IoT devices in certain area.

The group of NG-RAN and 5GC nodes (deployed and active), which are essential for the set of E2E services, provide provisioning and PM management services. It is also assumed that the providers of the related NSI / NSSI provisioning and PM management services are deployed and active.

The management system is consuming the afore mentioned management services either directly or through proxy nodes that re-expose the management services; the management system is aware of the performance requirements imposed on the set of communication services.

The management system is collecting the service experience information and monitoring the key performance indicators, KPIs, related to the targeted services. Analytics hosted by the MDAF may be utilized for processing of the network data to derive and analyse the KPIs. If the service quality assurance and optimization function detects performance degradation the 3GPP management system may continuously modify the configuration parameters in the corresponding NG-RAN and 5GC nodes and NSI(s)/NSSI(s), to satisfy the SLA requirement. In case that changes of communication service SLS are needed, those changes may result as input to the 3GPP management system.

If the network performance does not recover or improve, the management system may further adjust the network configuration, or roll back to the previous configuration. At all times the management system continues to collect the network data and to monitor the performance indicators.

### 6.1.2 NWDAF assisted communication service SLS Assurance

The goal of this use case is to assure the SLSs (Service Level Specifications) for a particular communication service is crucial for the 5G network management. The negotiated SLS for a particular communication service should be assured in an autonomous way.

3GPP management system can be leveraged to enable autonomous SLS assurance for a deployed communication service. 3GPP management system can collect QoE data, related to network slice and applications, from NWDAF. Since the data collected will relate to network slice and a single NSI may be serving multiple communication services, the corresponding QoE data for the target communication service needs to be ascertained. Once the QoE data for a communication service is known, the SLS breach can also be ascertained. If the SLS is breached, the root cause analysis is performed to find the cause for SLS breach. Depending on the location of cause (at RAN or at, 5GC), remedial actions will be initiated to mitigate the SLS breach and network optimization is done so that the negotiated SLS can be assured.

The QoE analytical data from NWDAF is per Application for an NSI. It is crucial to derive which communication service is associated to the QoE data from the data received from NWDAF in order to ascertain the SLS breach.

### 6.1.3 5G Core assisted SLS communication service Assurance

The goal of this use case is to describe 5G Core management to assure compliance to SLSs (Service Level Specifications) for a communication service in 3GPP management system.

3GPP management system receives the SLS requirements that required by CSP or NOP. 3GPP management system is capable to translate e2e SLS goal and set the 5GC goal(s) of SLS related to 5GC and activate a closed control loop for service assurance goal(s). To fulfill the SLS requirements, 3GPP management system is capable to configure the management resource and 5GC network functions (e.g. AMF, SMF, NWDAF) to monitor measurements and fault alarms that are relevant to the SLS. Since, for example, a network slice for eMBB can provide multiple communications services, one or multiple closed control loops for service assurance goals are set, and the network resource and performance measurements which are relevant to the SLS.

During the process of service assurance of 5GC, the 5GC domain MDAS provider can be used to provide analysis of 5GC related network resource, virtual resources and performance assurance related to SLS in 5GC. The 5GC domain analysis report may be provided to 3GPP management system as part of the analysis result(s) of 5GC SLS.

Together with the report from NWDAF, performance measurements and fault alarms related to 5GC NFs are also available for analysis of any potential service degradation.

### 6.1.4 Communication service SLS assurance control

The goal of this use case is to enable the MnS consumer to control the communication service SLS assurance closed control loop(s) (e.g. specify the SLS to be assured, enable/disable the SLS assurance, specify the assurance time for certain SLS) and obtain the SLS fulfilment information provided by MnS producer. It is assumed that the MnS producer maintains SLS assurance closed control loops for multiple SLSs. The detailed SLSs for network slice assurance are captured in ServiceProfile (e.g. latency, Throughput) associated to network slice and the detailed SLS for network slice subnet assurance are captured in SliceProfile (e.g. latency, Throughput) associated to network slice subnet.

When an MnS producer receives an SLS assurance closed control loops(s) creation request with SLS assurance requirements for certain managed Entity (i.e. network slice, network slice subnet) from an MnS consumer, the SLS assurance requirements may include information of which SLS should be assured (e.g. latency should be assured), the SLS assurance granularity (e.g. per UE, per Network Slice, per S-NSSAI), SLS assurance condition (e.g. SLS assurance duration time, SLS assurance fulfilment requirements (e.g. the ratio of the SLS assurance time during the whole service usage time) ), the MnS producer create SLS closed control loop managed object instance contained by the specified managed Entity (i.e. NetworkSlice, NetworkSliceSubnet) and configures the received SLS assurance requirements in the created SLS closed control loop managed object instances. The MnS producer performs the network and/or service management to satisfy the SLS assurance requirements by adjusting the network (e.g. adjust the network topology, configure RRM policy) to satisfy the required SLS assurance requirements.

During the SLS assurance closed control loop operation phase, the MnS consumer may request MnS producer to enable/disable the corresponding SLS assurance or update the SLS assurance requirements if needed, then MnS producer update corresponding the SLS assurance closed control loop managed object instance to ensure the MnS producer perform the SLS assurance closed control loop based on the new request.

During the SLS assurance closed control loop operation phase, the MnS producer may report the SLS assurance closed control loop progress information and fulfilment information (e.g. SLS assurance requirements is satisfied or not) to the MnS consumer.

### 6.1.5 Network prediction assisted SLS communication service Assurance

The goal of this use case is to identify the management of network prediction assisted SLS communication service assurance. The SLS related to a particular communication service can be assured by considering the predicted network resource usage and performance (e.g. latency, throughtput) for the managed entity (e.g. network slice, network slice subnet) associated with the SLS closed control loop managed object instance within a certain time frame.

The 3GPP management system will have the most comprehensive network operating data, such as network resource utilization, network performance parameters in different periods, which would include different collection granularities (e.g. per UE, per S-NSSAI) and have corresponding performance parameters respectively in NG-RAN or 5GC. By introducing MDAS and NWDAF into both the management system and core network, it is possible that the network operating data can be the input of the closeloop to fulfil SLS requirements from CSP or NOP. The MDAS could predict the network resource usage and performance for the whole network as well as different domain, for example, the MDAS could predict the resource utilization and throughtput for the NSSI in the NG-RAN within a certain time period.

In a certain period of time, the current network condition is good enough to satisfy the SLS requirements. By introducing the prediction results from the analysis of MDAF and NWDAF, the historical data shows that the network will experience a traffic burst in certain area and certain time which can cause network resource shortage and performance degradation. This predictional results can directly trigger the MDAF to analyse the root cause for performance degradation and analyse the solution which is used for making the network desicion such as reconfiguration and resource reallocation before the predicted traffic burst time. And the resource reallocation could be conducted between the multiple NSIs or NSSIs, for example, there are different network slices in the network for SLS communication service assurance, the resources between network slices could be adjusted dynamically based on the MDAF analysis results. Similarly, in office area, the network will not active during holiday but will have network surges on working day, the network prediction can also trigger resource release and network function reconfiguration. This can not only save network operating costs on holiday but also achieve the goal of network service assurance on working day.

### 6.1.6 Limiting the actions of an assurance closed loop

The goal of this use case is to provide the consumer of an assurance closed loop the ability to limit actions the assurance closed loop can execute. This renders the assurance closed loop taking action (configuration of MoI attributes) that are within the limits of the scope as defined by the consumer.

Assurance closed loops have a defined assurance goal related to a communication service SLS may execute various actions in the deployed operator network. There may be cases in which two or more assurance closed loops can execute the same or related set of actions on a managed entity. For example, assurance closed loops ACL1 and ACL2 for coverage optimization running in neighbouring RAN domains may take independent decision on the radio signal strength and azimuth to optimize the coverage. These assurance closed loops therefore may have the capability to cause a conflict with both simultaneously changing the azimuth to address a coverage-hole thereby causing an unnecessary coverage-overlap instead.

An authorized coordinating entity (authorized common consumer of the two ACL), should be able to configure the closed loops in a way that such occurrences are minimized. To coordinate the execution of multiple such assurance closed loops in the system the common authorized consumer of the assurance closed loop limits the set of actions of the assurance closed loops to avoid possible conflicts between the two or more assurance closed loops. In the example above: The authorized consumer of an assurance closed loops may limit the coverage optimization configurations signal strength and azimuth configurations to be done only by ACL1.

The 3GPP management system shall therefore provide the ability to limit action capabilities (possible configurations of an MoI attributes) that an assurance closed loop can take, this can be for example via operational policy configurations.

The MnS consumer obtains the allowed action capabilities (configurations that assurance closed loops could execute on an managed entitiy) from the MnS producer. The MnS consumer may then internally compare the action capabilities allowed that can be taken by a set of assurance closed loops to determine if possible conflicts exist. If conflicts are found, and the MnS consumer determines a possible resolution by limiting the action capabilities of a set of assurance closed loops, then it requests the MnS producer to limit the set of action capabilities, for example: by configuring new operational policies.

NOTE: This use case is not supported

### 6.1.7 Trigger based Assurance Closed Control Loop (ACCL) state change

The goal of this use case is to provide the consumer of an assurance closed loop the ability to set conditions (example threshold crossings) in the 3GPP management system that when met, trigger changes in ACCL state (enable or diable an ACCL). This implies that an ACCL may be activated or deactivated if the set condition in the 3GPP network is met (example: the threshold is crossed).

Assurance closed loops may be required to run at different times and network conditions in the 3GPP network. For example, an ACCL related to handover optimization may only execute when the handover failure crosses a certain threshold. Similarly, an ACCL managing energy efficiency may be disabled when the network is overloaded beyond a certain threshold. These conditions (network overload, handover failure threshold crossing) can therefore be associated with a change in state (enable/disable) of an ACCL to further support autonomy of the 3GPP management domain.

An authorized entity (authorized consumer of the ACCL), for example, another closed loop or operator, should be able to configure the condition and its association with an ACCL state transition (enable/disable) in the 3GPP management domain.

The 3GPP management system shall therefore provide the ability to configure conditions and associate them with the state transition of an ACCL. The 3GPP management system then configure appropriate listeners to monitor the configured threshold crossing and once triggered execute a state transition (enable/disable) of the associated ACCL.

The MnS consumer obtains the possible conditions as well as the possible ACCL state transitions they can be associated with. The MnS consumer may then configure condition in the 3GPP network. When the threshold crossing notification is received the MnS producer it executes the associated state transition (enable/disable) of the ACCL.

NOTE: This use case is not supported

|  |
| --- |
| **2nd Change** |

## 6.2 Requirements

**REQ-CSA-CON-01** The 3GPP management system shall have the capability to take actions for a set of communication services serving certain group of UEs based on the target SLS.

**REQ-CSA-CON-02** The 3GPP management system shall have the capability to collect service experience information.

**REQ-CSA-CON-03** The 3GPP management system shall have the capability to analyse the performance information related to the set of communication services serving certain group of UEs.

**REQ-CSA-CON-04** The 3GPP management system shall have the capability to modify the configuration parameters related to the set of communication services serving certain group of UEs.

**REQ-CSA-CON-05** The 3GPP management system shall have the capability to collect NSI related data from one or more 5GC NF(s).

NOTE 1: An example for NSI related data may be QoE data.

**REQ-CSA-CON-06** The 3GPP management system shall have the capability to derive which communication service is associated to the QoE data from the collected NSI related QoE data.

NOTE 1a: A communication service in the 3GPP management system is identified by an S-NSSAI (the Slice/ServiceType, SST in the S-NSSAI identifies a communication service which can be detailed using the SliceDifferentiattor, SD), see TS 23.003 [10].

**REQ-CSA-CON-07** The 3GPP management system shall have the capability to ascertain SLS breach.

**REQ-CSA-CON-08** The 3GPP management system shall have the capability to perform the root cause analysis (e.g., identifying the underlying reason) for an SLS breach.

**REQ-CSA-CON-09** The 3GPP management system shall have the capability to take corrective actions to ensure the target goal.

**REQ-CSA-CON-10** The 3GPP management system shall have the capability to translate network slice requirements to cross domain network slicesubnet SLS goal and single domain network slicesubnet SLS goal.

**REQ-CSA-CON-11** The 3GPP management system shall have the capability to collect single domain SLS analysis as input to cross domain SLS analysis.

**REQ-CSA-CON-12** The 3GPP management system shall have the capability to allow its authorized consumer to control the SLS assurance (e.g. specify the SLS to be assured, enable/disable, specify the assurance time and update the SLS assurance requirements).

**REQ-CSA-CON-13** The 3GPP management system shall have the capability to allow its authorized consumer to obtain the SLS assurance fulfilment status information.

NOTE 2: The management system refers to the producer of management service for SLS assurance.

**REQ-CSA-CON-14** The 3GPP management system shall have the capability to do network prediction (e.g. network resource usage and network performance) by analysing the network operation information in special scenarios.

**REQ-CSA-CON-15** The 3GPP management system shall have the capability to take actions such as network configuration and perform network resource reallocation according to the network prediction results.

**REQ-CSA-CON-16** The 3GPP management system shall have the capability to allow its authorized consumer to limit the set of action capabilities executable by an assurance closed loop.

NOTE: This requirement is not supported.

**REQ-CSA-CON-17** The 3GPP management system shall allow an authorized consumer to set a condition to enable/disable an ACCL.

NOTE: This requirement is not supported.

**REQ-LCM-CON-01** The 3GPP management system shall have the capability of lifecycle management of a closed control loop.

|  |
| --- |
| **End of Changes** |