3GPP TSG SA WG5 Meeting 135-e TDoc S5-211329

electronic meeting, online, 25 January - 3 February 2021

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

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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update use cases and requirements to replace Communication Service | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S5 | | | | | | | | | |
| ***Source to TSG:*** | Ericsson, Deutsche Telekom | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eCOSLA | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***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:*** | | The use cases and requirements use the phrases “ communication service” and “communication service assurance.” The solution does not include a communication service there the text should be updated to correct this misalignment. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Replace or remove communication service in use case and requirements where applicable.  Replace CS Assurance (CSA) tag with network slice Assurance (NSA) tag.  Remove FUN-03 not applicable any longer.  Replace expectation with requirements in FUN-04.  Remove duplicated requirement FUN-05.  Correct requirement CON-13.  Clarify “actions” in FUN-02 by replace with “log actions”. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The use case and requirements are not aligned with the solutions in stage 2 and 3 potentially leading to non compliant solutions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1.1, 5.1.2, 5.1.3, 5.1.4  6.1.1, 6.1.2, 6.1.3, 6.1.4  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's revision history:*** | |  | | | | | | | | |

|  |
| --- |
| **Start change** |

# 5 Business level use cases and requirements

## 5.1 Use cases

### 5.1.1 Communication service assurance

The CSP wants to meet the CSC expectations on automation as well as internal goals on CAPEX and OPEX efficiency.

The CSP has access to capabilities, procedures and tools that can address both CAPEX and OPEX in the provisioning and management of network slice(s) to their customers (CSC). The CSC expects the CSP to offer a variety of services including business critical communication services that allow the CSC (e.g. Enterprise) to run their applications in a predictable manner [2]. Hence automation of the on-boarding of the CSC application, which will use network slice(s) provided by the CSP, on a 5GS, is a requirement to meet the following needs:

- reduce the complexity for a CSC application to be on-boarded on a 5GS;

- improve the network performance over time, based on predicting service behaviour;

- reduce the cost ownership through automation.

During the operation of the network slice the CSP provides assurance of service quality requirements and CSP meets the CSC expectations on automation as well as internal goals on CAPEX and OPEX efficiency.

**REQ-NSA\_CSA-FUN-01** The CSP shall be able to provide a statement of network slice requirements to a 5GS and receive capability information about these from the 5GS.

**REQ-NSA\_CSA-FUN-02** The 5GS shall have the capabilities to monitor, and report to CSP the fulfilment of committed network slice requirements and log actions taken to adjust for deviations.

**REQ-NSA\_CSA-FUN-04** The 5GS shall have the capability to provide in-operation assurance of service quality requirements.

.

### 5.1.2 Communication service assurance for shared resources

A CSP network where at least one eMBB service is operating, providing services to end-users. A CSC requests from the CSP Order Care a new eMBB service (or any other service) for business-critical application(s), submitting an initial proposed SLA. The management system assists CSP Order Care with analysis of the proposed SLA and, when SLA is committed, works together with NF's to ensure SLA goals and optimal use of resources for previous as well as the new service(s).

In this scenario, it is assumed that the SLA's for the two services will allow for them to share resources, for example RAN and TN resources.

The management systems CS-Assurance service receives the request from Order Care and using a MDAS CS preparation assistance service, explores and evaluates service realisation and impact on other services, if any.

Once the Order Care has committed to an SLA with a CSC, the management system activates the service.

As the service operates, a management service for service assurance, continuously monitors the SLA fulfilment using MDAS, PM assurance services [3] including and core network NwDAF QoE analytics service, if available.

Based on goals for SLA fulfilment, or other KPIs, the CSA service may initiate an action when SLA goals are not met, be that over- or under fulfilment. The CSA service may use an MDAS to assist in selecting proper action and how to best execute the action.

The CSA service triggers the action by using provisioning service [4] towards RAN, transport and core network and monitors the effect of the change.

REQ-CSIA\_CON-01: The 3GPP management system shall have the capability providing a management service for assisting in assessing (evaluating) a proposed SLA for a requested service.

REQ-CSIA\_CON-02: The 3GPP management system shall have the capability providing a management service for assisting in asserting an agreed SLA for a requested service.

REQ-CSIA\_CON-03: The 3GPP management system shall have the capability to process 5GS data and provide analytics services to its consumers.

### 5.1.3 Use case for obtaining resource requirements for a service

Once a request for a service is received, in the service provisioning phase, the 3GPP management system needs to identify the resources required for this service in order to do service assurance. For example, during the feasibility study, in order to assure the performance, the 3GPP management system should be able to determine the resource availability for that service. This could be done by requesting the MDAS provider about the resource requirements and checking the available resources.

MDAS provider may already have resource requirement for a given service requirement, obtained by the historical analysis using offline or online monitoring of resource usage of similar services. In that case, the 3GPP management system can determine the feasibility and if feasible provision the services using those resources to go to the operational phase.

If the resource requirement cannot be determined (e.g. not sufficient prior data), the 3GPP management system may assign certain amount of initial resources and limit the number of users admitted by configuring the appropriate CN functions. The resource usage information and the services using those resources in a given time period with their performance (e.g. delay) is monitored by the 3GPP management system for different number of UEs to learn the resource requirement for different service requirements. This data could be used to determine resource requirements for future service requests during the provisioning phase or to adjust resources to reflect the changing service demands for the already admitted services.

It may be a continuous learning process in the run-time phase, since service degradation could happen due to various reasons and resources may need to be adjusted to address such situations.

**REQ-NSA\_RR-CON-01** The 3GPP management system shall be able to determine the resource requirement for a given service requirement.

**REQ-NSA\_RR-CON-02** The 3GPP management system shall be able to allocate certain amount of resources for a service and configure the 5GC functions to limit the number of users of a given service.

### 5.1.4 Use case for interaction with core network for service assurance

The goal is to enable the 3GPP management system to take early action to prevent service degradation.

The 3GPP management system configures the control plane functions (e.g. NWDAF) so as to report potential service degradation according to the SLS. Service load can be determined by considering both NF(s) load in 5GC and resource utilization in access network. If the service degradation occurs or predicted when the resources are scaled down, resources could be scaled up to solve the issue. Therefore, it is necessary for the 3GPP management system to configure the 5GC functions such that in the event that a potential service degradation or overloading is predicted, that is sent to the 3GPP management system. This can be done by properly configuring the overloading conditions (e.g. triggering parameters) in the 5GC functions of a selected service. The 3GPP management system could configure the 5GC functions to trigger when the service load is increased or predicted to be increased beyond a certain threshold level. The 3GPP management system could then do resource scaling or use MDAS to find a proper solution.

Similarly, when the resources are underutilized the 3GPP management system could do scaling down or deactivation of resources.

**REQ-NSA\_RR-CON-01** The 3GPP management system shall be able to configure the 5GC functions to make them report of a potential service load increase beyond a certain threshold so that the 3GPP management system can do scaling up of resources in time without impacting the SLA.

**REQ-NSA\_RR-CON-02** The 3GPP management system shall be able to determine the service load thresholds that need to be used by the 5GC functions to report, so that a potential resource overprovisioning situation can be ascertained.

**REQ-NSA\_RR-CON-03** The 3GPP management system shall be able to perform scaling down of resources when a resource overprovisioning is detected, and the overprovisioning is not needed.

# 6 Specification level use cases and requirements

## 6.1 Use cases

### 6.1.1 Service quality assurance and optimization of services on a network slice

The goal of the use case is to enable 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 services provided via certain NSI(s) or to IoT devices in certain area.

It is assumed that the relevant NFs are deployed and active in NG-RAN and 5GC. The group of NG-RAN and 5GC nodes, 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 above 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 services on a network slice.

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 a network slice service SLS are made, those changes may result as input to the 3GPP management system.

If the network performance does not recover or improve, the management system may adjust the modifications, for example roll back to previous configuration. In any case it continues collecting the network data and monitoring of the performance indicators.

### 6.1.2 NWDAF assisted SLS Assurance

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

3GPP management system can be leveraged to enable autonomous SLS assurance for a deployed 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 services, the corresponding QoE data for the target service needs to be ascertained. Once the QoE data for a 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 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 Assurance

The goal of this use case is to describe 5G Core management to assure compliance to SLSs (Service Level Specifications) for a 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 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 resource 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 SLS assurance control

The goal of this use case is to enable the MnS consumer to control the 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 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 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.

## 6.2 Requirements

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

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

**REQ-NSA-CON-03** The 3GPP management system shall have the capability to analyse the performance information related to the network slice serving certain group of UEs.

**REQ-NSA-CON-04** The 3GPP management system shall have the capability to modify the configuration parameters related to the network slice serving certain group of UEs.

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

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

**REQ-NSA-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-NSA-CON-09** The 3GPP management system shall have the capability to take corrective actions against the root cause identified.

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

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

**REQ-NSA-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-NSA-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-NSA-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-NSA-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-NSA-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.

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

|  |
| --- |
| **End change** |