**3GPP TSG-SA5 Meeting #139-e *S5-215220***

**e-meeting, 11 - 20 October 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **28.533** | **CR** | **0087** | **rev** | - | **Current version:** | **17.0.0** |  |
|  |
| *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:***  | enhance SBMA to support access control |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S5 |
|  |  |
| ***Work item code:*** | MSAC |  | ***Date:*** | 2021-09-29 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | According to conclusion of TR 28.817, the service based management architecture should be updated to support authentication and authorization capabilities for management service access control. |
|  |  |
| ***Summary of change:*** | As proposed in possible solution to support access control on management service in 7.1 of TR 28.817:Enhance Service Based Management Architecture (SBMA) to support authentication capability.Enhance Service Based Management Architecture (SBMA) to support authorization capability |
|  |  |
| ***Consequences if not approved:*** | No standardized way for access control on management service of 3GPP management system, that may cause interoperability issue once security feature is enabled. |
|  |  |
| ***Clauses affected:*** | 2, 4.x (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

|  |
| --- |
| **Start of 1st modification** |

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 32.101: "Telecommunication management; Principles and high level requirements".

[3] 3GPP TS 28.530: "Management and orchestration of networks and network slicing; Concepts, use cases and requirements".

[4] 3GPP TS 28.541: "Management and orchestration of 5G networks; Network Resource Model (NRM); Stage 2 and stage 3".

[5] 3GPP TS 28.552: "Management and orchestration of 5G networks; Performance measurements and assurance data".

[6] 3GPP TS 28.554: "Management and orchestration of 5G networks; 5G End to end Key Performance Indicators (KPI)".

[7] 3GPP TS 32.425: "Telecommunication management; Performance Management (PM); Performance measurements Evolved Universal Terrestrial Radio Access Network (E-UTRAN)".

[8] 3GPP TS 28.531: "Management and orchestration of 5G networks; Provisioning; Stage 1".

[9] 3GPP TS 28.532: "Management and orchestration; Management services".

[10] 3GPP TS 28.500: "Telecommunication management; Management concept, architecture and requirements for mobile networks that include virtualized network functions"

[11] 3GPP TS 28.510; "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Requirements".

[12] 3GPP TS 28.511; "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Procedures".

[13] 3GPP TS 28.512; "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 2".

[14] 3GPP TS 28.513: "Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 3".

[15] 3GPP TS 28.515; "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Requirements".

[16] 3GPP TS 28.516: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Procedures".

[17] 3GPP TS 28.517: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 2".

[18] 3GPP TS 28.518: "Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 3".

[19] 3GPP TS 28.520: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Requirements".

[20] 3GPP TS 28.521: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Procedures".

[21] 3GPP TS 28.522: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Stage 2".

[22] 3GPP TS 28.523: "Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Stage 3".

[23] 3GPP TS 28.525: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Requirements".

[24] 3GPP TS 28.526: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Procedures".

[25] 3GPP TS 28.527: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Stage 2".

[26] 3GPP TS 28.528: "Telecommunication management; Life Cycle Management (LCM) for mobile networks that include virtualized network functions; Stage 3".

[27] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV V1.3.1 (2018-01)".

[28] 3GPP TS 28.545: "Management and orchestration; Fault Supervision (FS)".

[29] ETSI GS ZSM 002: "Zero-touch Network and Service Management (ZSM); Reference Architecture V.1.1 (2019-08)".

[30] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[31] 3GPP TS 23.501: "System Architecture for the 5G system".

[32] 3GPP TS 28.622: "Telecommunication management; Generic Network Resource Model (NRM) Integration Reference Point (IRP); Information Service (IS)".

[x] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[y] IETF RFC 4253: "The Secure Shell (SSH) Transport Layer Protocol".

|  |
| --- |
| **End of modification** |

|  |
| --- |
| **Start of 2nd modification** |

## 4.x Access control capability

### 4.x.1 Authentication service

Authentication service producer provides identity management capabilities. Identity management of MnS consumers and producers includes creating, reading, updating and deleting identities.

Authentication service producer provides authentication policy management capabilities. Authentication policy management of MnS consumers and producers includes creating, reading, updating and deleting authentication policies.

Authentication service producer provides capabilities for authentication of MnS consumer. Optionally, authentication service producer issues an assertion to the MnS consumer after successfully authenticated the MnS consumer.

Note 1: Certificate issued by trusted CA is used by MnS consumer to authenticate the authentication service producer. E.g. a MnS consumer access the authentication servicer through Transport Layer Security (TLS) (see [x]), then the MnS consumer could authenticate the producer through validating the signature signed with certificate of the producer issued by the trusted CA.

MnS producer may validate the assertion issued by trusted authentication service producer to authenticate a MnS consumer. Alternatively, MnS producer may authenticate a MnS consumer based on local policy.

Note 2: Generally, certificate issued by trusted CA is used by MnS consumer to authenticate a MnS producer. E.g. a MnS consumer access the MnS through TLS (see [x]) or SSH in case explicit server authentication is adopted for SSH key exchange (see [y]), then the MnS consumer could authenticate the MnS producer through validating the signature signed with certificate of the producer issued by the trusted CA. Known shared secret may be used by MnS consumer to authenticate a MnS producer, e.g. MnS consumer access the MnS through SSH in case implicit server authentication is adopted for SSH key exchange (see [y]).

Authentication Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) and/or in a centralized manner (e.g. at a PLMN level). The Centralized Authentication Service producer can be named as Cross Domain Authentication Service producer.

Note 3: If the MnS consumer and the MnS producer to be accessed are inside the same domain, Authentication Service producer may be deployed at domain level to support authenticating the MnS consumer. If the MnS consumer and the MnS producer to be accessed are in the different domain, Authentication Service producer is deployed in a centralized manner to support authenticating the MnS consumer.



Figure 4.x.1: Authentication capability on service based architecture

### 4.x.2 Authorization service

Authorization service producer provides capabilities to manage access permissions on MnSs for a MnS consumer or a group of MnS consumers, including permissions to create, read, update and delete managed objects.

Authorization service producer provides capabilities to grant permissions to a MnS consumer. Optionally, authorization service producer sends a token to the MnS consumer based on permissions assigned to the MnS consumer in the specific context.

Note 1: A token may include a list of permissions with conditions and a digital signature signed by the authorization service producer.

Optionally, authorization service producer provides capabilities to validate the token presented by a MnS consumer to a MnS producer.

Note 2: Authorization enforcement is performed by the MnS producer based on permissions in the token included in the service request, or the MnS producer may check the permissions of a MnS consumer via authorization decision service provided by authorization service producer. or the MnS producer may check the permissions of a MnS consumer based on local policies.

Authorization Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) and/or in a centralized manner (e.g. at a PLMN level). The Centralized Authorization Service producer can be named as Cross Domain Authorization Service producer.

Note 3: Authorization Service producer may be deployed at domain level to support access control between MnS consumer and producer inside the same domain. Specifically, an domain Authorization Service producer may be deployed together with managemnet service producer. Authorization Service producer is deployed in a centralized manner to especially to support access control between MnS consumer and producer from different domains.



Figure 4.x.2 Authorization capability on service based architecture

|  |
| --- |
| **End of modification** |