3GPP TSG SA WG5 Meeting 138-e S5-214462

**electronic meeting, online, 23 -31 August 2021** revision for S5-21xxxx

**Source: Nokia, Nokia Shanghai Bell, Samsung**

**Title: possible solution to support access control on management service**

**Document for: Approval**

**Agenda Item: 6.5.5**

# 1 Decision/action requested

***The group is asked to discuss and approve the proposal..***

# 2 References

 [1] 3GPP TR 28.817: "Management and orchestration; Study on access control for management service"

# 3 Rationale

The use cases, issues and potential requirements for access control on management services were discussed and agreed in the study. This pCR is to propose possible solutions to support access control related capabilities in service based management architecture.

# 4 Detailed proposal

|  |
| --- |
| **Start of 1st Change** |

## 7.x possible solution to support access control on management service

## 7.x.1 enhance Service Based Management Architecture (SBMA) to support authentication capability (update clause 4 of 28.533)

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 credential management capabilities. Credential management of MnS consumers includes creating, reading, updating and deleting credentials.

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. Authentication service producer issues an assertion to the MnS consumer after successfully authenticated the MnS consumer.

Note: 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 https if stage 3 solution set is OpenAPI, 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 validates the assertion issued by trusted authentication service producer to authenticate a MnS consumer.

Note: Certificate issued by trusted CA is used by MnS consumer to authenticate a MnS producer. E.g. a MnS consumer access the MnS through https if stage 3 solution set is OpenAPI, then the MnS consumer could authenticate the producer through validating the signature signed with certificate of the producer issued by the trusted CA.

Authentication Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) to support access control between MnS consumer and producer inside the same domain, and/or in a centralized manner (e.g. at a PLMN level) especially to support access control between MnS consumer and producer from different domains. The Centralized Authentication Service producer can be named as Cross Domain Authentication Service producer.



Figure 7.x.1-1 Authentication capability on service based architecture

Note: ANS stands for authentication service

## 7.x.2 enhance Service Based Management Architecture (SBMA) to support authorization administrative/decision capabilities (update clause 4 of 28.533)

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

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

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

Authorization service producer provides capabilities to validate the token presented by a MnS consumer to a MnS producer.

Note: 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.

Authorization Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) to support access control between MnS consumer and producer inside the same domain, and/or in a centralized manner (e.g. at a PLMN level) especially to support access control between MnS consumer and producer from different domains. The Centralized Authorization Service producer can be named as Cross Domain Authorization Service producer.



Figure 7.x.2-1 Authorization capability on service based architecture

Note: ARS stands for authorization service

## 7.x.3 enhance Service Based Management Architecture (SBMA) to support audit capabilities (update clause 4 of 28.533)

Audit service producer provides capabilities to collect security logs from authentication service producer, authorization service producer and MnS producer. Similar to fault supervision management service, audit service producer could retrieve or receive security log from other components.

Audit service producer provides capabilities to track the access behaviors of a MnS consumer based on security logs collected.

The security log includes information, e.g. when and what MnS consumer did try to log on to the authentication service producer, when and what MnS consumer did try to get permissions from the authorization service producer, when and what MnS consumer did try to access MnSs, what's the result of aforementioned requests, success or fail? If it's fail, what's the reason, etc.

Audit Service producer can be deployed at different levels, for example, at a domain level (e.g. in RAN, CN, domain) to support log collection and audit for a specific domain, and/or in a centralized manner (e.g. at a PLMN level) to support log collection and audit for all domains of a PLMN.



Figure 7.x.3-1 Audit capability on service based architecture

Note: ADS stands for audit service

## 7.x.4 enhance Request-response communication paradigm to support authentication and authorization (update clause 5 of 28.533)



Figure 7.x.4-1 Request-response communication paradigm with access control

Precondition:

1. The MnS consumer and producer are configured in authentication and authorization service producer. The MnS consumer is always assigned for specific role in specific group.

2. The permissions for specific role or group are configured in authorization service producer.

Procedures:

1. MnS consumer logs on to authentication service producer for authentication.

2. Authentication service producer returns authentication assertion to the MnS consumer once successfully authenticate the MnS consumer.

3. With the authentication assertion, the MnS consumer asks permissions from authorization service producer.

4. Authorization service producer validates the assertion, check the role/group of the MnS consumer and assigns related permissions to the MnS consumer. Authorization service producer constructs access token based on granted permissions and sends back the token to the MnS consumer.

The token can be described as below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Attributes** | **Support** | **Cardinality** | **Description** |
|  | token ID | M | 1 | The identification of the token |
|  | Validity | M | 1 | The time based validity of the token, beyond which the token will be considered in-valid. |
|  |  | authorizedMnS | M | 1…\* | List of management services and its capabilities the consumer is authorized to access. |
|  |  |  | MnS Type, Label, Version | O | 0…1 | Type of MnS (PROVISIONING, FAULT\_SUPERVISION, PERFORMANCE\_ASSURANCE), Label: human readable description, Version: version of the MnS |
|  |  |  | allowedComponentA | M | 1…\* | The list of operation of the MnS, consumer is authorized to access. This will be the {MnSRoot} in case of OpenAPI implementations |
|  |  |  | allowedComponentB | M | 1…\* | The list of IOC the consumer can access.  |
|  |  |  |  | uri | M | 1 | The URI of the NRM fragment (IOC) |
|  |  |  |  | allowedAttr | M | 1…N | The list of attributes permission present in the IOC |
|  |  |  |  |  | attName | M | 1 | Attribute name present in the IOC |
|  |  |  |  |  | attPermission | M | 1 | The type of permission (Readonly, Writeable) |
|  |  |  | allowedComponentC | O | 0…1 | The list of performance measurement and the KPI, the consumer is authorized to collect. |
|  |  |  |  | allowedMeasurement  | M | 1..\* | List of authorized measurements |
|  |  |  |  |  | managedEntity | M | 1 | Managed entity producing the measurement |
|  |  |  |  |  | perfMeasurement | M | 1 | Measurement the consumer is authorized to collect. |
|  |  |  |  | allowedKPI  | M | 1..\* | List of authorized KPI |
|  |  |  |  | allowedAlarmInfo | O | 1…\* | List of alarm info the consumer is authorized to receive |
|  |  |  |  |  | managedEntityAlarmInfo | M | 1 | Alarm info |
|  |  |  | allowedNotifications | M | 1…\* | The url of the notification which consumer is authorized to subscribe for. |

Notes: The table above is an example, the concrete structure will be decided in normative phase.

5. The MnS consumer checks the access token, construct a service request based on permissions in the token, and sends service request, including access token, to MnS producer.

6. MnS producer validates the access token, perform the request and return result to the MnS consumer.

## 7.x.5 enhance NRM and operations to support authentication, authorization and audit capability

Note: what's the exact change in stage 2 and stage 3 will be decided in normative phase.

|  |
| --- |
| **End of Change** |