3GPP TSG SA WG5 Meeting 138-e S5-214468

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

**Source: Nokia, Nokia Shanghai Bell, TELEFONICA S.A.**

**Title: management data isolation**

**Document for: Approval**

**Agenda Item: 6.5.3**

# 1 Decision/action requested

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

# 2 References

 [1] 3GPP TR 28.811: "Management and orchestration; Network Slice Management Enhancement"

 [2] GSMA NG.116: "Generic Network Slice Template"

# 3 Rationale

GSMA defined attribute in General Slice Template (GST) to isolate resource of network slices in different levels (refer to GSMA NG.116). E.g., there’s physical or logical isolation, the physical isolation includes processor, memory and network isolation, and logical isolation includes virtual resource, network function or service/tenant isolation, etc.

As data is critical asset of a network slice customer (NSC) for its business and operation, in GSMA GST, the data of one NSC is always required to isolate from other NSCs even for the least strict isolation level - service/tenant isolation.

This pCR is to introduce a new use case on management data isolation for network slice customers, and proposed potential requirements and solutions.

# 4 Detailed proposal

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

## 5.x Use case – management data isolation for different network slice customers

### 5.x.1 Description

There are different types of data in 5G network, including management data, signaling data and application data. Management data include business related data, e.g., charging information, SLA, tenant profile, subscriber data, etc., and operation related data, e.g. CM, PM, FM data, log, trace, MDT, QoE, policy, analytics report, software, etc.

**The data can be in different stages:**

* at rest, data that is housed on computer data storage (e.g. hard disk, CD, mobile, etc.) in any digital form (e.g. file, databases, data warehouses, etc.). e.g. management data stored in central or distributed database , etc.. The data at rest could be "stolen" by illegal entities who can gain physical or digitally access to the device or data storage media. Isolating storage, access control and data encryption are always employed to protect data at rest,
* in transit, data that is moving between nodes over public or private network. e.g. management data exchanged between customer tool and NSMF, between digital portal and NSMF/NSSMF/NFMF, between MnF and MnF/NF, etc.. The data in transit could be leaked or tampered by any probe or tap over wire, or any network nodes in the flow, when it leaves the confines of protected enclaves, especially when it flows over public network. Security protocols, e.g. TLS, IPSec, etc., are always applied to isolate and protect data in transit.
* in use: active data that is manipulated by an application or process, and is residing typically in computer random-access memory (RAM), CPU caches, or CPU registers . e.g. management data used in MDA, etc.. Unlike data at rest or in transit, the data in use is always decrypted to be used by process in most of operation systems today, therefore it can be stolen through e.g. memory dump, side channel attack, etc. The data in use could be protect by isolating applications in different VM or container with trusted host operation system and hardware.

As data is critical asset of a network slice customer (NSC) for its business and operation, in GSMA GST, the data of one NSC is always required to isolate from other NSCs even for the least strict isolation level - service/tenant isolation.

### 5.x.2 Issue and gaps

Management data isolation is needed in all stages of the data during its lifecycle to satisfy SLS of network slice customer (NSC, or tenant), security policies of network slice provider (NSP) and regional/industry regulations. Different NCSs may have different requirements on data isolation and protection and a single NSC may also have different data isolation and protection requirements for different types or stages of data. E.g. A NSC from public safety may require dedicated MnF to collect and transmit its management data via IPSec based VPN, while a NSC as media content provider may accept shared MnF but separated MnS and transport to collect and transmit its PM/FM data. Another example, for a NSC of vehicle industry, it may require to separate DB and protect anonymization for its MDT data, while just separate table for FM/PM data with availability and integrity protection.

The existing 3GPP management system capabilities cannot support management data isolation for NSCs/tenants described above. Clause 5.3 of this study report described a used case to isolate resources, especially managed resource (e.g. NFs, virtual resource, transport, etc.), of network slice. The potential requirements in clause 6.2 and possible solution in clause 7.1 proposed isolation group and isolation profile to solve slice isolation issue. However, there’s no concrete isolation polices define in isolation profile to isolate and protect data, especially management data, for each NSC/tenant/slice group.

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

|  |
| --- |
| **Start of 2nd Change** |

## 6.x Potential requirements for Network Slicing Management to support management data isolation for different NSCs

* The 3GPP management system should have the capability to support management data isolation for different network slice customers or different network slice groups.
* The 3GPP management system should have the capability to support management data isolation in network slice management, network slice subnet management and network function management layers.
* The 3GPP management system should have the capability to support management data isolation when data in collection, in transmission, in rest and in use.
* The 3GPP management system should have the capability to support different isolation and protection requirements for different types of management data.
* The 3GPP management system should have the capability to support provisioning of management data isolation policies.

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

|  |
| --- |
| **Start of 3rd Change** |

## 7.x Possible solutions for management data isolation for different NSCs

It is proposed to enhance the 5G NRM to support management data isolation for different NSCs/Tenants/Slice Groups. The management data isolation policies are defined in following table. It could be part of isolation profile, in this case the groupId is same to id of isolation group the isolation profile associates to. It could be part of service/slice profile, in this case, groupId is not needed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute Name | Support Qualifier | isReadable  | isWritable | isInvariant | isNotifyable |
| groupId | O | T | F | T | T |
| dataTypeList | M | T | T | F | T |
| dataClass | M | T | T | F | T |
| dataStage | O | T | T | F | T |
| analyticType | O | T | T | F | T |
| isolationRule | M | T | T | F | T |
| protectionReq | M | T | T | F | T |

Table 7.x-1: data isolation policy

* groupId is used to identify a group of slices.

Note: the group can be organized for a specific tenant, specific service type, specific region, etc..

* dataTypeList is used to categorize the data to different types,

Note: dataType could be, e.g. CM, PM, FM, MDT, QoE, trace data, etc..

* dataClass is used to define the classification of the management data in the dataTypeList.

 Note: dataClass could be, e.g. secret, confidential, business sensitive, normal, etc.

* dataStage is used to define the stage/phase of the data,

Note: dataStage could be, e.g. data in use, in transit, at rest, etc.

* analyticType is used to define the usage of the analytics function which takes the management data as input and output.

Note: e.g. the analytics function could be used by operator for business promotion, performance optimization or trouble shooting, etc. or by tenant for trouble shooting, etc. It's optional

* isolationRule is defined to isolate the data of a tenant/group for specific data types, and optionally in specific data stages.

Note: the isolationRule could be described as that dedicated DB allocated to the data. The data is MDT and QoE data (data types) in the rest (data stage) of tenant-1/slice group-1 (tenant/group),

* protectionReq is used to decide the security control to protect the isolated data of a tenant/group for specific data types, and optionally in specific data stages.

Note: protectionReq could be e.g. integration protect, confidentiality protect, privacy protect, etc. The technologies used for the protection is implementation dependent.

With the extended NRM, specific management function/service and corresponding transport, storage/DB/table and analytics function may be allocated to an NSC/tenant/group, isolated and protected according to data isolation policies of the tenant/slice group. See figure 7.x-1 for isolation of management data at rest, in transit and in use.



Figure 7.x-1 isolation of management data of different NSCs/tenants/groups

An example procedure for management data isolation:

@startuml

skinparam shadowing false

skinparam monochrome true

hide footbox

autonumber "0."

actor admin

participant Consumer

participant NSMF

participant NSSMF

participant "management function\n(monitoring function)" as MMnF

participant "other function" as OFunc

admin -> NSMF: create and configure isolation group and profile,\n associate the profile with the group

NSMF -> NSSMF: create and configure isolation group and profile,\n associate the profile with the group

NSSMF -> MMnF: create and configure MnF or MnS\nto collect and transmit data

MMnF -> OFunc: subscribe to data notification

OFunc --> MMnF: receive and proceed data

MMnF --> Consumer: send data to consumer

@enduml



Figure 7.x-2 example workflow for management data isolation

1. Through management portal or other tool, operator administrator creates an isolation group for a network slice customer, associates an isolation profile to the group, and defines management data isolation policies for the group for an NSC/tenant.

2. A network slice producer, e.g. NSMF, may call management service provided by network slice subnet producer, e.g. NSSMF, to create corresponding network slice subnet group, translate the isolation profile and policies accordingly if needed, and attach the corresponding isolation profile to the network slice subnet group.

3. An administrator or MnS producer, e.g. NSMF or NSSMF, may trigger to create dedicated monitoring MnSs, even MnS producer, for the network slice (subnet) group to collect monitoring data, e.g. PM, FM data, according to management data isolation policies in the isolation profile associated to the group.

4. The common or dedicated monitoring MnS producer may subscribe to PM, FM or other data notification which belong to the network slices of the group.

5. After the monitoring MnS producer received monitoring data, it allocates storage/database for the data if needed, associates the storage/database to the network slice (subnet) group, isolate and protect the storage according to management data isolation policy defined in the isolation profile for the group.

6. The monitoring MnS producer may send the collected management data to authorized MnS consumer (which could be another MnS producer or acting on behalf of a tenant ) through common or dedicated MnSs (and corresponding transport network), protect the MnSs and transports based on management data isolation policies in the isolation profile associated to the group.

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