Questions on 5G exposure:

1. Does SA5 have (a small number of) concrete use cases?
2. Exposure of WHAT?
   1. Products / Services / Resources (cf. TMF SID – GB 922)?



* 1. Are we going to expose:
     1. Management Services (with their Components Type A/B/C)?
     2. Or NRM fragments (‘XXX as a Service’ approach)?
  2. Whatever approach, shall we expose:
     1. network slice only?
     2. other NRM fragments?
  3. Should all attributes of an MOI be exposed similarly to all consumers?
  4. Should all contained objects of an MOI be exposed similarly to all consumers? (Root MOI only vs. root MOI + subtree down to nth level vs. ?)
  5. Should underlying virtualization resources be exposed as well?
  6. Regarding exposure of network slice:
     1. as a Managed Resource, via 3GPP management system?
     2. or as a Service (NSaaS), via BSS?
  7. Does SA5 have a clear separation of scope wrt. NEF (cf. TS 23.501)?

1. By WHOM? To WHOM?
   1. By CSP? NOP?
   2. To tenants? CSC? We often hear about 3rd-parties but, from a CSP point of view, the CSP is Party No. 1, CSC is Party No. 2, so who is the 3rd-party?
   3. Do we address B2B only? B2B2X as well? Is exposure transitive? Is abstraction needed? If yes, has intent-based management a role to play here?
   4. Any particularities in case of Non-Public Networks (S-NPN, PNI-NPN)?
2. Read / Write exposure (access)
   1. Read access: consumer has rights to a) read (cRud) exposed ‘entities’ and b) receive notifications?
   2. Write access: read access + rights to perform CrUD operations on ‘entities’? What happens in case of exposure of shared ‘entities’ (e.g. ‘Delete’ a MOI which represents a shared managed entity)? Any safeguard?
   3. The Support Qualifier for MnS operations and notifications has been removed from TS 28.532. Does that mean that any authorized consumers may consume all operations and notifications of the MnS, with no distinction?
3. Governance?
   1. Does SA5 agree that exposure is ruled by the contract between one provider and one customer?
   2. Does SA5 agree that any interactions related to exposed entities shall obey this contract?
   3. Any charging aspects? Example: in case of ‘pay-per-act’ model, should any request from a 3rd-party to e.g. access an exposed entity trigger a request from the 3GPP management system to the Charging System to check if the 3rd-party’s credit is not negative (cf. credit control, event-based charging, session-based charging)?
   4. What should be the role of EGMF (see TS 28.533)? It needs to be further specified.
4. Which Rel-17 WI(s) / SI(s) address the above questions?
   1. Any gap(s)?
   2. Any overlap(s)?

List of Rel-17 Work Items / Study Items which relate to 5G exposure:

|  |  |
| --- | --- |
| **WI / SI** | **Objectives** |
| FS\_NSCE  (Rapp. : Alibaba) | - Identify use cases and requirements regarding exposure of management capabilities and management services to externals, e.g. verticals and service providers.  - Conduct an analysis to determine gaps in existing specifications and studies (such as FS\_MNSAC) based on the identified requirements (see bullet point one).  - Propose mechanisms needed for specifying and handling rules for exposure of management capabilities and management services to external MnS consumer, if not covered by existing specification and studies such as FS\_MNSAC.  - Derive recommendations for a normative work.  NOTE1: The charging aspects of the management of network slice management capability is out of the scope of this SID.  NOTE2: The enforcement of the mechanism that used to express the set of rules for network slice management capability exposure can be studied in FS\_MNSAC. |
| FS\_MNSAC  (Rapp. : Nokia) | study use cases and various access scenarios on management services, and propose management capabilities and solutions to:   * support access control policy (including authentication and authorization policy) enforcement, e.g. enforce management service consumer authentication, authorization before exposing management services and processing service requests for the consumer, etc. * support identity management of management service, management service producer and consumer, e.g., create, delete, update identity of management service or management service consumer/producer. * support access control policy (including authentication and authorization policy) management, e.g. create, delete, update, etc., procedures. * support permission management, e.g. create, delete, update, etc., procedures. * Align the solution with management plane security requirements and solutions of SA3 when applicable. |
| FS\_NSMEN  (Rapp. : Huawei) | * Investigate and propose the potential network slice information model and management service enhancements to support cross-operator network slice management use case (e.g. for V2X, etc.) * Investigate and propose the potential new management capabilities to support end to end network slicing (e.g. identified by end to end network slicing ETSI ZSM work item, GSMA 5GJA work package 1, etc.) * Investigate and propose the potential new management capabilities to support security management of network slice (e.g. security isolation management, UP protection policy management, etc. )   Note: The study should clarify the meaning of the terms “cross-operator network slice management” and “end to end network slicing”. |
| eMEMTANE  (Rapp.: Huawei) | to specify possible enhancements for 5G network and network slice management and orchestration as following:  - Potential use case, conceptual description and requirements for management service (e.g., provisioning service) in multiple tenant environment.  - Potential solutions (e.g. NRM IOC) to support the new use case and requirements in release 17. |