AUTHORIZATION SERVICES

(AITIA & SINETIQ proposal)

It was agreed on RoadMap meeting at 24.05.2024, that the Authorization Core System's service interfaces have to use the Arrowhead terminology, so an authorization policy consists of provider, consumer, service, service operation and event type.

As it was written in SysD, Authorization should allow to specify the following kinds of rules:

- A provider's service/service operation/event with a specific type is accessible to anyone within the local cloud.
- A provider's service/service operation/event with a specific type is accessible to anyone within the local cloud, except a list of consumers (blacklist).
- A provider's service/service operation/event with a specific type is accessible to anyone within the local cloud whose names appear on a given list (whitelist). A peer-to-peer rule can be specified if this list only contains one consumer.
- A provider's service/service operation/event with a specific type is accessible to anyone within the local cloud who meet specified meta data requirements.
- A provider's service/service operation is accessible to anyone from a given neighbor cloud list (inter-cloud whitelist).

authorization service

The service is offered only for application systems and should contain three operations:

- validate

  A provider can validate one consumer's service operation consumption request at a time. It has to identify itself and specify the consumer's name, the service and the service-operation. The validate operation returns whether the consumer is allowed to consume the requested operation or not. No rule mapped to the actual consumers means no permission, otherwise all the related rules have to be passed.

- grant

  A provider can specify one authorization rule at a time (regarding its services, service operations or event types) and the grant operation returns a unique identifier for the rule created. Implementation should use "personal groups" for a provider.

- revoke

  A provider can revoke an authorization rule by specifying its unique id. A provider can only revoke the rules it has created. Rules created via management service cannot be revoked by an application system.

- get

  A provider can fetch the related rules what was created by itself (without the mgmt rules) in order to have the unique ids.

authorization-management service

The service is offered only for core and administrative support systems and should contain XX operations:

- query

  Returns a list of authorization rules with pagination support. The list can be filtered by provides, consumers, services, service operations and event types.

- validate-service

  Accepts a consumer, service/service operation request and a list of providers and returns a filtered providers list, based on the available authorization rules. Rules created via this management service are always have priority over the rules created by the providers itself. No rule mapped to the actual consumers means no permission, otherwise all the related rules have to be passed per provider.

- validate-event

  Accepts a publisher, event type and a list of subscribers and returns a filtered subscribers list, based on the available authorization rules. Rules created via this management service are always have priority over the rules created by the providers itself. No rule mapped to the actual subscriber means no permission, otherwise all the related rules have to be passed.

- grant

  A list of authorization rules can be specified at once (bulk operation).

- revoke

  A list of authorization rules can be revoked at once by specifying their unique ids. (bulk operation).