Moa technical profiles

Moa technical requirements are defined in the FedTLS schema as well as the below technical profile

Change log

Date	Author	Change
2023-02-22	Rasmus Larsson	Migrating profile from skolfederation.se to wiki Translating profile to English Adding Strengthened tags profile
2024-02-01	Johan Sandin	Added claim tags for clients Added tag 'gnapv1'
2024-03-20	Johan Sandin	Updated tag descriptions
2024-10-22	Rasmus Larsson	Added requirement for unique X509 Subject values for new issuer certificates to prevent TLS conflicts.

.

Moa Technical Profile

- when uploading metadata to the Moa production environment the member **MUST NOT** upload anything other than production metadata. Test environment metadata **MUST NOT** occur in the production environment,
- the member's metadata **MUST** be in accordance with actual version of Federated TLS Authentication (see respective environment under Moa environments for more information),
- for every `client's` claim `tags` there **MUST** exist one value in accordance with Strengthened Tags Profile.
- for every `server's` claim `tags` there **MUST** exist at least one value in accordance with Strengthened Tags Profile.
- for every `entity's` claim `organization` there **MUST** exist a value for the member organization's legal name,
- for every `entity's` claim `organization_id` there **MUST** exist a value for the member organization's organization number in format LLYYMMDDXXXX where LL stands for the country code in accordance with ISO 3166-1 alpha 2
- an issuer certificate can be included in multiple entities. However, If a new entity adds an issuer certificate that is not already present in the federation metadata, the X509 Subject of that issuer certificate MUST be unique to prevent potential conflicts with TLS implementations that may encounter issues when handling certificates with identical subjects.

Strengthened Tags Profile

Strengthened tags are tags used in metadata which are vetted and used by a community for a specific purpose or context. A strengthened tag may be restricted to be used by certain parties, and the definition of the tags usage (such as API definition and information model) is handled within each tag community.

Tag name	Description	Learn more
`egilv1`	Defines endpoints that support user provisioning in accordance with the EGIL profile	https://sambruk.github.io/EgilDoc/implementationsprofil.html
`bolv1`	Defines endpoints that support ordering and delivery of digital learning resources.	
`userlistv1`	Defines endpoints that support delegating the selection of users to provision to a service provider.	
`gnapv1`	Entities using GNAP (Grant Negotiation and Authorization Protocol). Among other services, the tag represents the authentication API of The Swedish National Agency for Education, verifying clients to enable them to acquire an authorization JWT.	Contact Skolverket's Technical Support (Swedish) for information about how to use GNAP: https://www.skolverket.se/om-oss/kontakta-oss

Metadata signature

The aggregated metadata is signed with JWS and published with JWS JSON Serialization. The metadata signatures are created with the algorithm ECDSA using P-256 and SHA-256 ("ES256"), according to the definition in RFC7518.

Metadata and validation examples

For metadata and validation examples, go to Moa metadata example