Operation Profile for VOMS Attribute Authority Service – review

Date : 2010-10-15
Reviewer: vincent.ribaillier@idris.fr
URL of the reviewed document : https://grid.ie/eugridpma/wiki/AA_Profile
Status of this review: DRAFT, only intended as a starting point for the DEISA and PRACE security forum discussions.

About the document

→ IGTF draft managed by the EUGridPMA working group

→ Defines **minimum requirements and recommendations** for the **operation** of a **Attribute Authority** (**AA**) service operated by an **Attribute Authority Service Provider (AASP)** issuing **Attribute Assertions**. Attribute Assertions are used for authorisation decisions in Grid services.

Objective of this review

→ Identify if the DEISA User Administration System (DUAS) is compliant to the profile.

→ Identify the modifications that would be required either in the DUAS or in the profile to make the DUAS compliant.

→ See, if it would be useful for DEISA to have a service compliant to this profile.

Detailed analysis

Section	**Operation profile definition or requirements**	**DUAS status, comments**
Section 2 Definitions		Currently, only two lines of generic definitions.
Section 3 General Architecture	To achieve sustainability, an AASP should operate AA services as a long term commitment	OK, it is also the case for the DUAS. Statement not really related to architecture.
Section 4 Attributes	An attribute is a string, a named property which may be associated with an entity	OK, also the case in the DUAS.
	An attribute assertion is a statement that a subject is a holder of a specific attribute	OK.
	For VOMS, an attribute is a group, role or generalised attribute	OK. For DEISA, an attribute is - a role (e.g. accounting roles) - a profile (notion very similar to a role, e.g.: standard user, portal users, staffs...) - a group membership (e.g. A UNIX group membership, a project Membership) - generalised attributes (e.g.: deisaHomeOrgId = local identification of

		user at his home site) Attributes are also settable on group of users (e.g.: Execution Site of a project)
	Relying party requirements on lifetime of attributes, schema (to be detailed)	Lifetime is not static. Implicit rules: (E.g. All attribute of a project are valid until the end of project is reached).
	An attribute assertion must link the attribute to one and only one explicitly named entity	OK
	The lifetime of the assertion should take into account the dynamic nature. Not more than 24 hours	No maximum life time. An attribute is valid until it is present in LDAP. However, the actual policy is to regenerate all the authorisation assertions on a daily basis, based on the LDAP content.
	Dynamic updating of attribute schema by the VO is required... why ?	
4.1 VO membership administration	Must follow the VO Membership Management Policy	
	The AA service provider must provide an attribute administration service for use by the VO.	TBD
4.2 Attribute assertion lifetime	Maximal lifetime of the assertion should be 24 hours	Already discussed in section 4.
5. Operation Requirements	AA systems delivering AA need to be on dedicated machines	OK (at least in the beginning of DEISA)
	AA system in secure environment where access is controlled an limited to specific trained personal	OK
	List of AA signing key requirements	No notion of signing. Secured connection (TLS-SASL), mutual authentication at client/server level ONLY.
5.1 Network configuration	Highly protected and suitably monitor	OK
5.2 AASP documentation	Persistent contact details Aspect of operational environment relevant to evaluation of the security Statement of compliance with this profile	TBD
5.3 AA certificate and attribute format	AASP must provide registration information, DN, … to the AA repository.	

	AA issuer certificate profile format of the AC specified in RFC 3281	
5.4 Revocation	No revocation but RFC 3281 has provision for a CRL - PKC certification path verification - revocation of the AA certificate => kill all assertions signed by AA.	No signing notion currently.
5.5 AA key changeover	No identified problem.	
6. Site Security	Passphrase of private key kept offline	No signing notion currently. Content perhaps more appropriate for section 5.
7. Publication and Repository responsibilities		No signing notion currently
8. Audits	AA must record and archive all requests for attributes at least 180 d	OK. Done at least by some sites, probably all.
9. Privacy and confidentiality	Accredited AAs must define a privacy and a data release policy compliant with relevant legislation	
10. Compromise and disaster recovery	Procedure required	TBD
11. Relying Party obligations	Validate AA certificate and the Acs. More ?	
12. Accreditation process		
13. AASP naming		

Steps required for the DUAS to be compliant to this profile

If the document is made generic (no reference to VOMS, in particular in the title), the main problem for the DUAS to be a candidate for accreditation is the **notion of signed assertions** delivered for a **limited period of time** (max 24 H). So, because of this notion, the AASP operation profile model does not exactly match the DUAS model.

However, if the document includes an option to deliver unsigned assertions (or to accept that a private network of directory servers with mutual node to node authentication is equivalent to the concept of delivering signed assertions) as well as an option to have non limited in time assertions (or to accept that a daily regenerated assertion is equivalent to a maximal 24H lifetime assertion), then the work to achieve the accreditation would not be very important for DEISA (mainly organisational and documentation effort).

The other alternative for the DUAS to be compliant would be for DEISA to implement an additional layer on the top of LDAP that would precisely deliver signed assertions. The Shibboleth evaluation that have been performed in WP4 could be a good starting point. Shibboleth has been mainly evaluated as a mean to deliver Short Live Credentials (delivering of short lived X509 certificates) but not has a mean to deliver generic attribute assertions with a VOMS use case in mind.

Would it be useful for DEISA to have a service compliant to this profile ?

→ The current services deployed in DEISA do not make use of signed assertions. Such a service would however be an advantage to ease the integration of future services based on signed assertions.

→ The level of trust within partners is already very high in DUAS. The introduction of a accredited AASP would not improve significantly the trust level. However, it could improve the level of trust between users and DEISA. DEISA could state in its AUP that authorisations are managed with an accredited AASP.

→ Being compliant to this profile would be also interesting from an interoperability point of view (interoperability with EGI for e.g.).