AA Profile

September 3, 2008

Discussion

This is a **draft** of a document describing the minimum requirements for the operation of Attribute Authorities. It is loosely based on V4.1 of the IGTF "Authentication Profile for Classic X.509 Public Key Certification Authorities with secured infrastructure" (dated 1 Dec 2006).

It is far from final and certainly not approved by the EU Grid PMA or IGTF!

Abstract: This is a draft document of the International Grid Trust Federation describing the minimum requirements for the operation of an Attribute Authority (AA) service. The AA service is run by or on behalf of a Grid Virtual Organisation (VO) and maintains attributes for registered VO users and/or VO services. Attribute assertions are securely delivered on request to members of the VO. They are presented by the user and/or service, together with an X.509 credential for authentication, for the purposes of Authorisation of access to a Grid resource.

This document is managed by the EUGridPMA Authorisation working group.

1 About this document

Do we repeat the abstract?

This is a draft document of the International Grid Trust Federation describing the minimum requirements for the operation of an Attribute Authority (AA) service. The AA service is run by or on behalf of a Grid Virtual Organisation (VO) and maintains attributes for registered VO users and/or VO services. Attribute assertions are securely delivered on request to members of the VO. They are presented by the user and/or service, together with an X.509 credential for authentication, for the purposes of Authorisation of access to a Grid resource.

In this document the key words 'must', 'must not', 'required', 'shall', 'shall not', 'recommended', 'may', and 'optional' are to be interpreted as described in RFC 2119. If a 'should' or 'should not' is not followed, the reasoning for this exception must be explained to the PMA to make an informed decision about accepting the exception, or the applicant must prove to the PMA that an equivalent or better solution is in place.

note: "PMA" here means the accrediting body.

2 General Architecture

There should be a single Attribute Authority (AA) managing the VO-related attributes. The AA service may be run by the VO or on behalf of the VO by an AA service provider. There should be one integrated master database in the AA service. This may be replicated for reasons of performance and/or fault tolerance.

To achieve sustainability, it is expected that each AA service will be operated as a long-term commitment ... *expand?*

The AA service should be operated in accordance with the requirements of the VO Membership Management Policy (ref) and provide the necessary technical implementation.

3 Attributes

An attribute is ... *expand this definition*

Explain Relying party requirements on lifetime of attributes, schema etc.

An attribute assertion must be linked to one and only one entity.

The lifetime of the assertion should take into account the dynamic nature. Not more than 24 hours. (MS)

Dynamic updating of the attribute schema by the VO is required ...*why?*

3.1 VO membership administration

Must follow the VO Membership Management Policy (ref).

The AA service provider must provide an attribute administration service for use by the VO.

3.2 Attribute assertion lifetime

Maximum lifetime is 24 hours... *expand*

There is no revocation mechanism.

3.3 Removal of an attribute authority accreditation

An accredited authority may be removed from the list of accredited authorities if it fails to comply with the provisions of this document, via the voting process described in the Charter of the PMA to which this authority is accredited.

4 Operational Requirements

The AA computer that issues attribute assertions needs to be a dedicated machine, running no other services than those needed for the AA operations and/or similar CA or AA instances. The AA computer must be located in a secure environment where access is controlled, limited to specific trained personnel.

The AA signing key must have a minimum length of 1024 bits and should be dedicated to atrribute signing functions. *And tied to the AA or the VO?*

Software-based private keys of the AA must be protected with a pass phrase of at least 15 elements and that is known only by designated personnel of the Authority. *Just on boot? not at all?*

AAs are encouraged to use an HSM which must adopt a similar or better level of security. *activation on boot?* Copies of the encrypted private key must be kept on off-line media in secure places where access is controlled.

4.1 HSM and network configuration

Do we require an HSM? No, not today.

The AA computer must(?) be connected to a highly protected/monitored network, connected to the internet. The secure environment must be documented and approved by the PMA, and that document or an approved audit thereof must be available to the PMA.

The on-line AA architecture should provide for a (preferably tamper-protected) log of issued assertions.

4.2 Certificate Policy and Practice Statement Identification

Every AA must have an Attribute Practice Statement (APS Document) and maybe assign it a globally unique object identifier (OID). *can we demand this?*

APS document should be structured as defined in RFC 3647 *or a new template?*

4.3 AA Certificate and attribute format

The accredited authority must publish a X.509 signing certificate as a root of trust.

Do we insert an extension to mark as AA certificate?
AA controls (see 7.4 RFC3281)?
What do we say about AC format?
FQAN...?

4.4 Revocation

There is no revocation.... *But RFC3281 has provision for a CRL.*

4.5 AA key changeover

Any problem with AA key change?

5 Site security

Do we need something here?

CA profile said...

The pass phrase of the encrypted private key must be kept also on an offline medium, separated from the encrypted keys and guarded in a safe place where only the authorized personnel of the Authority have access. Alternatively, another documented procedure that is equally secure may be used.

6 Publication and Repository responsibilities

Each authority must publish for the VO members, relying parties and for the benefit of distribution by the PMA and the federation

- the AA signing certificate or the set of AA certificates up to a self-signed root (?);
- a http or https URL of the PEM-formatted AA certificate;
- a http URL of the PEM or DER formatted CRL; *?? put information - "no CRL"?*
- a http or https URL of the web page of the AA for general information (*Admin interface?*);
- the APS document
- an official contact email address for inquiries and fault reporting
- a physical or postal contact address

The AA should provide a means to validate the integrity of its root of trust.

Furthermore, the AA shall provide their trust anchor to a trust anchor repository, specified by the accrediting PMA, via the method specified in the policy of the trust anchor repository. *CIC portal?*

The repository must be run at least on a best-effort basis, with an intended continuous availability.

The originating authority must grant to the PMA and the Federation - by virtue of its accreditation - the right of unlimited re-distribution of this information.

7 Audits

The AA must record and archive all requests for attributes, along with all the issued attributes and the login/logout/reboot (key activitions) of the issuing machine.

The AA must keep these records for at least 180 days. Assist in incident response.

Each AA must accept being audited by the accrediting body to verify its compliance with the rules and procedures specified in its APS document.

The AA should perform operational audits at least once per year. A list of AA personnel should be maintained and verified at least once per year.(?)

8 Privacy and confidentiality

Accredited AAs must define a privacy and data release policy compliant with the relevant legislation.

9 Compromise and disaster recovery

The AA must have an adequate compromise and disaster recovery procedure, and be willing to discuss this procedure in the PMA. The procedure need not be disclosed in the practice statements.

10 Relying Party obligations

Validate AA certificate and the ACs. More?