Category: guidelines document
Status: AGREED
Document: EUGridPMA-AASP-Operations-20120509-v1-1.doc
Editor: davidg
Last updated: Thu, 10 May 2012

Guidelines for Attribute Authority Service Provider Operations

Abstract
This guideline describes the minimum requirements and recommendations for the operation of Attribute Authority Services.

Table of Contents

1 About this document

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 documented by the AASP such that relying parties can decide whether to accept the exception.

2 Definitions

AA

An Attribute Authority. This is the body responsible for managing the binding between subjects and attributes within a Community. The AA selects an AASP to host AA services.

AA service

The technical entity which maintains bindings and issues attribute assertions

AASP

An Attribute Authority Service Provider is an organization (or group within an organization) that runs Attribute Authority services for one or more Attribute Authorities on behalf of one or more defined Communities[1]

Attribute

An attribute is a named property associated with an entity.

Subject

A subject is an entity, whose identity can be authenticated, belonging to the scope of the AA.

Attribute Assertion

An attribute assertion is a statement, made by the Attribute Authority service, about the attributes of a subject[2].

3 Introduction

This document describes the minimum requirements and recommendations for the operation by an AASP of an AA service issuing Attribute Assertions. The Community and/or the AA selects one or more AASPs and informs Relying Parties regarding the metadata of these AASPs. Attribute information is securely maintained by the AASP. Attributes are securely delivered on request to authorized information requestors. These attributes are typically aggregated with identity assertions from an Identity Provider and are then used for authorisation decisions.

To achieve sustainability, an AASP should operate AA services as a long-term commitment. An AASP must be supported and endorsed by its host organisation.

These guidelines are intended to facilitate the assessment of Attribute Authority Service Providers rather than of an individual Attribute Authority or an AA service or a Community.

This document does not provide guidance on the management of attributes or the mechanisms by which attributes are entered into the AA service.

[1] for example a virtual organization, a project, etc

[2] attribute assertions may include time of issuance, may include time of expiration and may be signed.

4 Naming

Identifiers of the AASP and the AA must both be persistent and globally unique. The AA must use a defined naming scheme for subjects and attributes. Subject identifiers must be persistent and unique within an AA.

5 Attribute Management and Attribute Release

The AA is responsible for the semantics, lifecycle and release policy[3] of attributes stored or asserted by the AA service.

The AA must document how it addresses these issues. The AASP must collect and make these AA documents available to Relying Parties.

6 Attribute Assertions

Assertions provided by an AA service must be integrity protected. They must either be signed by the AA service or be transmitted over an integrity protected channel where the server has been authenticated..

The assertion must be traceable back to the AA.

The AA service must meet the confidentiality requirements of the Community and the AA release policy. This may mean that AA services require client authentication

Assertions that are bound to an authenticatable subject must only be issued to valid subjects.

These guidelines do not require a revocation mechanism for attribute assertions.

Assertions without a specified lifetime are only guaranteed to be valid at time of issue.

If the assertion contains a lifetime, this should be no more than 24 hours. The AA will be held responsible for an assertion during its entire lifetime.

Footnote to max lifetime: Renewal is no different from any initial assertion and must be based on information held by the AASP at the time of renewal. (see SLCS)

Assertions may be requested from the AASP by an information requestor authorised by the Community, AA or subject.

7 Relying Party Obligations

If a community uses AA services operated by multiple AASPs then Relying Parties must assess each of the AASPs individually.

Relying Parties must validate the integrity of attribute assertions and their binding to a valid subject at the time of reliance.

Relying Parties must rely on assertions with an explicit lifetime only for as long as they are valid.

[3] this must also address any requirements for confidentiality

Relying Parties must assess the risk of relying on assertions with no explicit lifetime and must not rely on them for longer than 24 hours after issuance[4].

Relying Party must validate all verifiable elements[5].

8 Operational Requirements

An AA service system that issues attribute assertions must be a dedicated machine, running no other services than those needed for the AA operations and/or other security-sensitive services.
An AA service may be run in a virtual environment that has the same security for all services running in this environment and external users must not have interactive access to this environment.

The AA service system must be located in a secure environment where access is controlled and limited to specific trained personnel.

8.1 For AA services issuing signed assertions

The key used to sign assertions should be dedicated to assertion signing functions.
This key must not be shared between AASPs. A single AASP may use the same signing key for multiple AA services.

This key must have a strength equivalent to or better than an 2048 bit RSA key.

AASPs are encouraged to consider using an HSM to store the signing keys. Otherwise, when using software-based private keys these must be suitably protected by the operating system.
In either case the keys must only be accessible by the service and trained personnel with procedural controls.

8.2 For AA services providing attribute lookup

The AA service must provide for connections to its protocol endpoint via integrity protected and mutually authenticated channels.

The keys used to authenticate and integrity protect the channel must have a strength equivalent to or better than an 2048 bit RSA key. The keys must be suitably protected by the operating system or an HSM, and must only be accessible by the service and trained personnel with procedural controls.

8.3 Network configuration

The network to which the AA service system is connected must be highly protected and suitably monitored.

9 Site security

The AASP should document the physical site security controls and maintain them in a state consistent with the security requirements of the hosted AAs.

[4] neither the AASP nor the AA are responsible for decisions based on information without a specified lifetime after the AA service has updated its own database.
[5] verifiable elements include such as the full certification path of the subject identity certificate, any CRLs, etc.

10 Publication and Repository responsibilities

The AASP must publish the following metadata for each AA it hosts, to the Community and related relying parties:

- persistent contact details for the AASP, including at least one email address and one postal contact address
- those aspects of their operational environment which are relevant to the evaluation of the security and trust by the AAs and Relying Parties
- the signing certificate, where relevant, or the set of certificates up to a self-signed root;
- a URL of the AA service for general information

The AASP should provide a means to validate the integrity of its roots of trust.

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

AAs must be informed if AASP procedures change.

11 Audits

Any binding between subjects and attributes should be verifiable and auditable for a defined time period.

The AASP must record and archive all of the following for all of its hosted AA services:

- all requests for attributes
- all issued attribute assertions
- all login/logout/reboot/key activitions of the issuing machine
- any configuration change to the AA service relevant to the access control of the attribute repository
- any change affecting the binding between subjects and attributes

The AASP must keep these records for at least 180 days after termination of the effects of the auditable event.

The AASP must provide assistance to operational security teams during a security incident.

The AASP must accept being audited following reasonable requests from an AA and/or a Community it serves to verify its compliance with these guidelines.

The AASP should perform operational audits of its staff at least once per year. A list of AASP staff should be maintained and verified at least once per year.

12 Privacy and confidentiality

AASPs must define an appropriate privacy and data release policy compliant with the relevant legislation and the requirements of the Community or AA.

13 Compromise and disaster recovery

The AASP must have an adequate compromise and disaster recovery procedure, and must be willing to discuss this with the hosted AAs or with an assessor. The AASP should be willing to disclose this to the Community or related Relying Parties.

14 Statement of compliance

Compliance with these guidelines may be claimed by the AASP itself or stated by a third party, such as an AA hosted by the AASP or a Community served by the AASP. The statement of compliance must identify who is making the claim or statement.

Relying parties should decide who they wish to trust to make statements of compliance.

A statement of compliance may refer to these guidelines but must not use the name of the IGTF to endorse or promote the AASP or hosted AAs without specific prior written permission from the IGTF.