

## **Implementing Levels of Assurance in a Trust federation using PKI and Shibboleth**

### **Table of Contents**

Executive Summary .....	2
Background .....	4
Risk and Mitigation.....	4
Levels of Assurance .....	5
Types of Assertions.....	5
LoA Definitions .....	7
Risk Levels.....	7
Identity LoA.....	7
Authentication LoA .....	8
Appendix A – An option for configuring a Shibboleth Identity Provider for proposed AAF policy LoA requirements. ....	9
Authentication LoA .....	9
Identity LoA.....	9
Appendix B – LoA Attribute definitions .....	11
Identity LoA.....	11
Authentication LoA .....	12

## **Executive Summary**

A trust federation allows each organisation in the federation to accept identities managed at the other organisations in place of managing all accepted identities locally. The trust federation lowers costs, removes hurdles and provides an enabling infrastructure for collaboration and resource sharing.

The AAF is being established as a trust federation to underpin and enable the collaborative use of resources. In a federation like this, participants agree to trust information that is passed between them on the basis that each member has agreed to abide by a commonly accepted set of rules.

Within the federation there are broadly two types of participant; those managing and providing identities to the federation (Identity Providers) and those providing services (Service Providers). A single entity can participate in both ways or just one way. A Service Provider has to trust the information about an entity that is passed to them by the Identity Provider. When providing a Service within the federation, a Service Provider has to decide which identities it will provide services to and this determination will take account of information about the identity which may be provided by the Identity Provider. Some of the information to be passed may include information about “Levels of Assurance” (LOA) which is essentially an indication of the strength of the underlying processes for identity management and the method used for authentication.

More levels, within the LOA, mean finer granularity in the information that may be available to a service provider but they can also add to complexity. The AAF Project Group and Steering Committee have been considering the natural tension which exists between LOA simplicity, complexity and compatibility with emerging practice so as to find the best approach for the AAF. The project is specifically seeking feedback from CAUDIT IT Directors and their teams about this topic.

A number of federations are considering the use of LOA. The AAF is defining four levels of strength relating to identity management and four levels measuring the strength of authentication. Additionally, while it is essential to have consistent definitions used across the PKI and Shibboleth technologies, it not expected that all levels will be utilised by any particular Identity Provider. For example at the start of the AAF identities provided via the shibboleth technology would come in just two levels: the AAF floor of trust for identity and authentication, and a higher level of assurance (level 3 for identity and authentication). Nevertheless, some number of levels may be necessary to cope with the differing requirements of Service Providers and as the AAF develops; the needs of Service Providers will drive what is required.

The project team has identified an approach that appears to be a good compromise between the competing requirements of simplicity and the requirement for more granular data. Feedback on this approach from some CAUDIT members has indicated

# AAF LoA Consultative Whitepaper



that the definitions for LOA should be set from the beginning, but that the choice of which levels to implement and use in the federation may change over time.

It is suggested that the AAF will design the technical framework for the different Levels of Assurance so that there is a definition of how LOA will be implemented both now and in the future. At startup, however, effectively only two levels would be implemented from a business perspective (i.e., the floor of trust; and identity LOA 3 combined with either authentication LOA 3 or 4). Business implementation means that there are policies and processes in place for each level of assurance. The AAF would only support those levels which had been implemented in this business sense. Additional levels would then be implemented when required, using the technical framework already defined.

This appears to strike a balance between simplicity and granularity in allowing the AAF to have a clearly defined technical framework which can be implemented once, but allows simplicity of initial implementation which can be extended when needed. It is also suggested that the base level of assurance (the “floor of trust”) will be sufficiently strong to engender confidence in it by the majority Service Providers who join the AAF Shibboleth Trust Federation.

The rest of this paper provides more detail of what is being suggested as a starting point for discussion and feedback from CAUDIT members is specifically sought to allow the project team to effectively consider this approach. Please send your feedback to [aaf@aaf.edu.au](mailto:aaf@aaf.edu.au).

## **Background**

A trust federation allows each organization in the federation to accept identities credentialed and managed at the other organizations in place of managing all accepted identities locally. The trust federation lowers costs, removes hurdles and provides an enabling infrastructure for collaboration and resource sharing.

Identity management and authentication technologies are unlikely to be uniform within even a single organization, but across all the organizations in a federation there will be a wide spectrum of current practice. This can be a barrier to trust, because in the absence of LOA information each organization can only rely on an identity from another organization meeting the lowest standards for identity and credential management within the range of that spectrum.

Trust is sometimes defined as an expectation of consistent performance. When each organization in the federation agrees to abide by the federation policy, the requirements in those policies become the factors for which the federation members can hold “an expectation of consistent performance”. Thus the adherence to a known set of policies is the basis for trust within the federation and between the federation and other entities.

The federation agreement requires all federation members to follow the published federation policies when making assertions regarding identities that are to be relied upon by other federation participants or indeed in the case of PKI credentials (signed documents etc) other entities outside the federation.

### ***Risk and Mitigation***

Any provider of services takes on a risk when transacting on a network with another party. One risk relates to the possibility of providing services to the wrong entity. Increasing the service provider’s belief that the transaction is being made with the correct entity can mitigate this risk. This belief is based on three assurances.

1. An assurance in the process of identifying the entity and assigning them a digital identity for use online.
2. An assurance in the strength of the technology implementing the method by which that entity can later authenticate over the network as that identity.
3. An assurance that the entities carrying out the processes of identification, authentication and management of supporting systems/data are operating under a policy regime supporting the consistent evaluation of those assurances.

## ***Levels of Assurance***

This document describes a proposed federation policy, in which the processes of identification and authentication method are measured in a way consistent with accepted security practices and divided into levels. These are termed the Identity Levels of Assurance – Identity LoA and the Authentication Strength Levels of Assurance – Authentication LoA. There are three proposed policy clauses.

1. The federation policy should require that any statement used for, or to describe an authentication event include an authentication LoA value that describes the strength of that authentication event.

Note: As these statements already contain an authentication descriptor the effect of this policy is only to require a value defined and understood by the federation community.

2. The federation policy should state that any party, after receiving an authentication assertion, may request and expect to receive an Identity LoA associated with the identity previously authenticated.

Note: It is only expected that this LoA assertion will be provided on request.

3. A third policy should specify that all federation identity credentials (via Shibboleth and/or PKI certificates) should assert LoA values for which the identity provider is confident that all the operational processes to which the LoA applies are met in line with the federation guidelines for that LoA value. Note: The “floor of trust” specifies the minimum standards and processes for identification and authentication in the AAF. Identity Providers will have an obligation to ensure all identities it asserts meet the floor of trust (for authentication and identification). Provided an identity provider meets its obligations, a shibboleth IdP can simply be configured to issue the floor of trust LOA values by default.

These three policies combined with mutual trust between the parties to the federation agreement, meet the three assurance requirements set out in the previous section. The result is that any service provider can assess the assurance level of any user requesting service. Without LoAs, service providers with high assurance requirements may not use the federation as an authentication infrastructure. LoAs also allow identity providers the scope to implement different levels of identification and authentication practices they feel appropriate to their business or community needs. Importantly, it provides a framework within the federation to adopt and benefit from, stronger security practices where used or required.

## ***Types of Assertions***

Three types of assertions are covered by the federation policies, X.509 Certificates, SAML Authentication Assertions and SAML Attribute Assertions.

# AAF LoA

## Consultative Whitepaper



An X.509 Certificate is an assertion issued by a Certification Authority CA that a particular identity is in sole possession of a particular secret key. By demonstrating possession of the secret to a relying party, which trusts the issuing CA, the certified identity can be authenticated. X.509 Certificates issued under the federation policy always contain an Identity LoA and an Authentication LoA along with a CPS policy which includes a statement that all federation policies applicable to the LoAs were observed in the processes leading to the creation of the certificate.

A SAML Authentication assertion is a document created by an Identity Provider IdP for an audience of Service Providers SP. The assertion indicates that the subject has authenticated to the IdP as an identity known to that IdP. We propose that SAML Authentication assertions, issued under federation policy, always contain an authentication LoA for the authentication event between the subject and the IdP.

A SAML Attribute assertion is a document created by an Identity Provider IdP for an audience of Service Providers SP. The assertion indicates that the subject, referenced in a prior authentication assertion, has particular values for a set of attributes known by the IdP. We propose that if an SP requests an Identity, an IdP will include the Identity LoA attribute for the subject in the Attribute assertion. The one sensible possible exception to this behaviour would be for anonymous authentication.

## **LoA Definitions**

### ***Risk Levels***

Each party providing access to a service must evaluate their own risks with regard to the service being provided inappropriately. However two useful references which define risk levels are:

The Australian Government e-Authentication Framework (AGAF)  
<http://www.agimo.gov.au/infrastructure/authentication>

and

The U.S. Government - E-Authentication Guidance for Federal Agencies  
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

In both cases risks are measured and divided into four categories. Risk mitigation is accomplished by ensuring that identities are established and authenticated with an appropriate level of assurance. These guides, and others derived from them, classify the procedures for establishing identities into four levels appropriate for the corresponding risks and also the technology for authentication into four levels again appropriate for the corresponding risks.

### ***Identity LoA***

The federation policy could define a measure of identification establishment procedures that is compatible with the frameworks above and appropriate to the federation membership.

A proposed measure is defined in `auEduPersonIdentityLoA` and has values representing four levels an AAF specific floor of trust<sup>1</sup> and levels 2 through 4. Levels 2 through 4 should be closely aligned with the internationally accepted NIST 800-63 and the AGAF standards. Brief summaries of the floor of trust and level 3 definitions are given below.

The floor of trust Identity LOA includes an institutional assertion of end-user identity and attributes. The information cannot be self asserted by end-users, but it is not required that end users identities undergo face to face verification. The identity floor of trust includes obligations with respect to maintenance of currency of user accounts and attributes eg, changing the `eduPersonAffiliation` value if a student moves to become a staff member. Identity Providers should also pro-actively manage the currency and security of user accounts, and disable an account if a breach is detected or if an end-user leaves the organizations.

---

<sup>1</sup> **Floor of Trust** for both Identification and Authentication is included as defined by the MAMs team and may be revised after completion of community feedback processes.

# AAF LoA

## Consultative Whitepaper



Identity LoA Level 3 corresponds to an identity asserted by a federation Identity Provider for which a trusted Identity Registrar has carried out an in-person identity proofing meeting the 100 point test, or the subjects identity is based on a continuous relationship with the Identity Provider organization for a period of greater than three years.

### ***Authentication LoA***

The federation policy will define a measure of authentication method strength that is compatible with the frameworks above and appropriate to the federation membership.

An existing attribute for authentication LoA is already supported by Shibboleth using SAML AuthenticationMethod. The proposed auEduPersonAuthenticationLoA provides suggested authentication LoA values corresponding to the floor of trust and levels 2 to 4. The AAF policies will detail the technical definitions for all levels, with levels 2 through 4 based on the NIST 800-63 and the AGAF standards. A very brief non-technical guide to the authentication floor of trust and levels 2 to 4 is given below.

The authentication “floor of trust” includes authentication using passwords with a minimum of six characters (with at least one letter and one number). The authentication floor of trust includes obligations with respect to maintenance of currency of user accounts and disabling of accounts if a breach is detected.

Authentication LoA Level 2 includes best practice, managed password based systems.

Authentication LoA Level 3 includes two-factor systems using hard tokens or software based X.509 certificates in conjunction with pass-phrases or pins.

Authentication LoA Level 4 includes some hardware based X.509 certificate systems, such as crypto tokens.

## **Appendix A – An option for configuring a Shibboleth Identity Provider for proposed AAF policy LoA requirements.**

### ***Authentication LoA***

To configure an IdP to assert the AAF “floor of trust” authentication LoA, add the `defaultAuthMethod` attribute below to the `<IdPConfig>` element in the `idp.xml` file

```
defaultAuthMethod = "urn:oid:1.3.6.1.4.1.27856.1.2.3.1"
```

If the default authentication method employed by an IdP satisfies the AAF policy requirements for a higher Authentication LoA, that higher value may be used.

To configure an IdP to assert multiple AAF authentication LoAs, the IdP should either use multiple authentication modules or a single multi-strength module.

The following steps must be taken.

1. The `defaultAuthMethod` should be set to the lowest Authentication LoA value supported by the IdP.
2. The `idp.xml` should configure a http header able to override the `defaultAuthMethod`.
3. The `defaultAuthMethod` can be overridden by having the authentication module create an HTTP header `SAMLAuthenticationMethod` containing the appropriate Authentication LoA.
4. The IdP must be running Shibboleth 1.3.3 or later.
5. ALL authentication modules MUST ensure that any http header value received by the authentication modules from the user browser is always overwritten by the authentication module with the appropriate AAF authentication LoA value. This can be achieved with a simple Apache configuration or by using a Tomcat filter in deployments not using Apache to front their Tomcat server.

### ***Identity LoA***

To define a default Identity LoA of "urn:oid:1.3.6.1.4.1.27856.1.2.4.1", to indicate Level 1, but still allow the directory to override this with another value, the `resolver.xml` file should contain the following.

```
<!-- Resolver for auEduPersonIdentityLoA -->  
<ScriptletAttributeDefinition  
id="urn:oid:1.3.6.1.4.1.27856.1.2.4">  
  <DataConnectorDependency requires="directory"/>  
  <Scriptlet><![CDATA[  
    // Check for existing value in directory
```

# AAF LoA Consultative Whitepaper



australian access  
federation

```
Attributes attributes =
dependencies.getConnectorResolution("directory");
Attribute loa =
attributes.get("auEduPersonIdentityLoA");
String auEduPersonIdentityLoA;
if (loa == null)
    // no value in directory, so use default value

resolverAttribute.addValue("urn:oid:1.3.6.1.4.1.27856.1.2.
4.1");
else
    // use existing directory value
    resolverAttribute.addValue(loa.get(0));
]]>
</Scriptlet>
</ScriptletAttributeDefinition>
```

## Appendix B – LoA Attribute definitions

### Identity LoA

The auEduPersonIdentityLoA has values representing the AAF floor of trust and levels 2-4. The following table details the globally unique naming of the attribute and values for use in AAF PKI certificates and AAF Shibboleth SAML assertions.

	OID namespace
<b>Attribute Name or Policy</b>	1.3.6.1.4.1.27856.1.2.4
<b>AAF floor of trust</b>	1.3.6.1.4.1.27856.1.2.4.1
<b>Level 2</b>	1.3.6.1.4.1.27856.1.2.4.2
<b>Level 3</b>	1.3.6.1.4.1.27856.1.2.4.3
<b>Level 4</b>	1.3.6.1.4.1.27856.1.2.4.4

Note: OIDs correspond to ISO (1).Identified-organisation (3).DoD (6).Internet (1).Private (4).Enterprises (1).Australian Access Federation (27856).auEduPerson (1).Attribute (2).Identity LoA (4).Level Id (1-4)

Example LDAP schema attribute declaration:

```
attributetype (1.3.6.1.4.1.27856.1.2.4
  NAME 'auEduPersonIdentityLOA'
  DESC 'Level of assurance for the identity to identifier binding as specified in
        federation policy. Values listed correspond to four levels
        1.3.6.1.4.1.27856.1.2.4.1,
        1.3.6.1.4.1.27856.1.2.4.2,
        1.3.6.1.4.1.27856.1.2.4.3,
        1.3.6.1.4.1.27856.1.2.4.4'
  EQUALITY caseExactMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Example attribute use in SAML attribute statement:

```
<saml:AttributeStatement>
  <saml:Subject>
    <saml:NameIdentifier Format="urn:mace:shibboleth:1.0:nameIdentifier"
      NameQualifier="https://identity.provider.fqdn/shibboleth-idp">
      3f7b3dcf-1674-4ecd-92c8-1544f346baf8
    </saml:NameIdentifier>
  </saml:Subject>
  <saml:Attribute AttributeName="urn:oid:1.3.6.1.4.1.27856.1.2.4"
    AttributeNamespace="urn:mace:shibboleth:1.0:attributeNamespace:uri">
    <saml:AttributeValue>1.3.6.1.4.1.27856.1.2.4.1.3</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

# AAF LoA Consultative Whitepaper



australian access  
federation

## Authentication LoA

The auEduPersonAuthenticationLoA has values corresponding to the AAF floor of trust and levels 2-4. The following table details the globally unique naming of the auEduPersonAuthenticationLoA attribute and values for use in AAF PKI certificates and AAF Shibboleth SAML AuthenticationMethod assertions. Note: Not all values need be used by identity providers or technologies. Specifically, initially PKI will use authentication LOAs level 3 and 4; and shibboleth IdPs may typically use “floor of trust” and level 3 authentication LOAs.

	OID namespace
Attribute Name or Policy	1.3.6.1.4.1.27856.1.2.3
AAF floor of trust	1.3.6.1.4.1.27856.1.2.3.1
Level 2	1.3.6.1.4.1.27856.1.2.3.2
Level 3	1.3.6.1.4.1.27856.1.2.3.3
Level 4	1.3.6.1.4.1.27856.1.2.3.4

Note: OIDs correspond to ISO (1).Identified-organisation (3).DoD (6).Internet (1).Private (4).Enterprises (1).Australian Access Federation (27856).auEduPerson (1).Attribute (2).Authentication LoA (3).Level (1-4)

Example LDAP schema attribute declaration:

```
attributetype (1.3.6.1.4.1.27856.1.2.3
  NAME 'auEduPersonAuthenticationLOA'
  DESC 'Level of assurance for the authentication method as specified in
        federation policy. Values listed correspond to four levels
        1.3.6.1.4.1.27856.1.2.3.1,
        1.3.6.1.4.1.27856.1.2.3.2,
        1.3.6.1.4.1.27856.1.2.3.3,
        1.3.6.1.4.1.27856.1.2.3.4'
  EQUALITY caseExactMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Example attribute use in SAML authentication statement:

```
<AuthenticationStatement
  AuthenticationInstant="2007-03-26T10:51:49.900Z"
  AuthenticationMethod="urn:oid:1.3.6.1.4.1.27856.1.2.3.3">
<saml:Subject>
  <saml:NameIdentifier Format="urn:mace:shibboleth:1.0:nameIdentifier"
    NameQualifier="https://identity.provider.fqdn/shibboleth-idp">
    3f7b3dcf-1674-4ecd-92c8-1544f346baf8
  </saml:NameIdentifier>
</saml:Subject>
<SubjectLocality
  IPAddress="10.0.1.1">
</SubjectLocality>
</AuthenticationStatement>
```