



AAF Shibboleth Operational Requirements and Recommendations

Final Draft following Sector Consultation

28th August 2008

Introduction

| | | |
|----------|--|-----------|
| 1 | Common (IdP and SP) Requirements and Recommendations | 6 |
| 1.1 | Technical Infrastructure | 6 |
| 1.1.1 | Federation Software | 6 |
| 1.1.2 | PKI Certificates | 6 |
| 1.1.2.1 | Server Certificate for Server-to-Server Interactions (i.e. back-channel) | 6 |
| 1.1.2.2 | Server Certificate for Browser-based interactions | 6 |
| 1.1.2.3 | Certificate Management | 7 |
| 1.1.3 | Time Synchronisation | 7 |
| 1.1.4 | Entity NameSpaces | 7 |
| 1.1.5 | Customised Federation Metadata | 7 |
| 1.1.5.1 | Downloading Federation Metadata | 7 |
| 1.1.5.2 | Maintaining AAF Shibboleth Federation Member Details for Federation Metadata | 7 |
| 1.1.6 | Domain Names | 8 |
| 1.2 | Usage of Attributes | 8 |
| 1.3 | Support and Liaison | 8 |
| 1.3.1 | Liaison Person for AAF Shibboleth Federation Members | 8 |
| 1.3.2 | Restrictions on End-User Support | 8 |
| 1.3.3 | Transaction Logging to Assist Federation Operator | 9 |
| 1.3.4 | AAF Shibboleth Federation Member Security Alerts | 9 |
| 1.3.5 | Support Staff Training | 9 |
| 2 | Identity Provider Requirements and Recommendations | 10 |
| 2.1 | Identity Management of End-users | 10 |
| 2.1.1 | Floor of Trust (Base Level of Assurance) | 10 |
| 2.1.2 | Higher Level of Assurance ("level 3") | 11 |
| 2.2 | Attribute Management | 11 |
| 2.2.1 | Release of Personal Information | 11 |
| 2.2.2 | Attribute Mapping | 12 |
| 2.2.3 | Core Attributes | 12 |
| 2.2.3.1 | eduPersonTargetedID (EPTID) | 13 |
| 2.2.3.2 | auEduPersonSharedToken (AEPST) | 13 |
| 2.2.3.3 | eduPersonAffiliation and eduPersonScopedAffiliation | 14 |
| 2.2.3.4 | eduPersonEntitlement | 14 |
| 2.2.3.5 | mail | 15 |
| 2.2.3.6 | displayName | 15 |
| 2.2.4 | Non-Core Attributes | 15 |
| 2.2.4.1 | eduPersonPrincipalName (EPPN) | 15 |
| 2.2.4.2 | auEduPersonAuthenticationLoA (and SAML AuthenticationMethod) | 16 |
| 2.2.4.3 | auEduPersonIdentityLoA | 17 |
| 2.3 | Attribute Release | 18 |
| 2.3.1 | Minimum Disclosure | 18 |
| 2.3.2 | IdP Administrator Configuration of ARPs | 18 |
| 2.3.3 | End-user Management of Attributes & Personal Information | 18 |
| 2.4 | IdP Management | 19 |
| 2.4.1 | IdP Information Web Pages | 19 |
| 2.4.2 | IdP Infrastructure | 19 |
| 2.4.3 | IdP End-User Support | 19 |
| 2.4.4 | IdP End-User Logging & Traceability | 19 |
| 2.5 | Federation Shared Services | 20 |
| 2.5.1 | Federation White Pages Service | 20 |
| 2.5.2 | Federation AuEduPersonSharedToken (FAST) Service | 20 |
| 2.5.3 | Federation Entitlement Service | 20 |

| | | |
|----------|--|-----------|
| 2.5.4 | Virtual Home Organisation..... | 20 |
| 3 | Service Provider Requirements and Recommendations | 21 |
| 3.1 | Service Descriptions and Service Offerings..... | 21 |
| 3.2 | Privacy and Personal Information | 23 |
| 3.2.1 | Handling of Personal Information..... | 23 |
| 3.2.2 | Personalisation and Anonymity | 23 |
| 3.2.3 | Commercial SP requests for personal information attributes | 23 |
| 3.2.4 | Continuity of Access | 23 |
| 3.3 | SP Management | 24 |
| 3.3.1 | SP authentication attribute processing | 24 |
| 3.3.2 | SP Information webpage..... | 24 |
| 3.3.3 | Error Pages..... | 24 |
| 3.3.4 | End-User Direct Contact | 24 |
| 3.3.5 | SP Logging and Troubleshooting | 25 |
| 3.3.6 | Where Are You From (WAYF) | 25 |
| 3.3.7 | SP Terms and Conditions and Storage of End-user Information..... | 25 |
| 3.3.8 | SPs that act as Gateways to other Services..... | 26 |

Background to this Document - Final Draft following Sector Consultation

This document describes Final Draft Requirements and Recommendations for the operation of the AAF Shibboleth Federation, based on lessons learned from the MAMS Testbed Federation and from other Federations around the world.

This version is a final draft prepared for consideration by the AAF Steering Committee on 5th September, based on comments received during the whole of sector consultation in June -July 2008, as well as previous rounds of consultation.

Implementers are encouraged to contact the MAMS team to clarify any issues or discuss questions about the content of the document.

Any outstanding issues not addressed in this document should be emailed to James Dalziel by 4th of September for discussion during the AAF Steering Committee review of this document on the 5th.

This document is available at: <http://federation.org.au/requirementsfinaldraft.pdf>

Reference Materials for this Document

This document makes reference to a number of systems under development by the MAMS project (Federation Manager, ShARPE, Autograph, People Picker and IAMSuite). While full details of these systems will be available later in 2008, an annotated set of screenshots has been created to assist with understanding of how the Requirements and Recommendations of this document relate to the features of these systems. These screenshots are available from: <http://federation.org.au/screenshots.pps>

Other reference materials to assist with understanding this document include:

Attribute Recommendations for AAF Participants:

http://www.aaf.edu.au/docs/Attributes_for_use_with_AAF_v01.4.0.pdf

Shibboleth 1.x Website

<https://spaces.internet2.edu/display/SHIB/WebHome>

MAMS Testbed Federation

<http://www.federation.org.au/>

Introduction

The AAF Shibboleth Federation will have three levels of documentation.

The top level is the AAF “Rules of Membership”, which describes the general legal obligations of all AAF Members and non-member Participant Organisations. The AAF Rules of Membership is expected to cover general issues across both Shibboleth and PKI technologies in a single document. This document will be available for review in the coming months following a legal review of AAF issues and decisions on AAF governance.

The second level is a set of documents that describe the specific technical and administrative Requirements (ie, mandatory) and Recommendations (ie, encouraged but not mandatory) of the AAF Shibboleth part of the Federation. Two documents are expected at this level for the AAF Shibboleth part of Federation – the *Attribute Recommendations for AAF Participants*¹(currently a working draft accepted by the AAF Steering Committee) and the final version of this document – the AAF Shibboleth Operational Requirements and Recommendations. The current version of this document is part of a consultation process to gain feedback on the operation of the AAF Shibboleth part of the Federation. Once finalised, this document will be referenced by the AAF Rules of Membership.

The third level is a wide range of advice and guidelines documents to assist with implementation details of the AAF Shibboleth part of the Federation. These will be provided over time as required to assist AAF Members (both Identity Providers – IdPs and Service Providers – SP).

Key Terms

The following terms are central to understanding this document:

Australian Access Federation (AAF): The legal entity that oversees the Australian higher education and research Federation for Shibboleth and PKI technologies, and enters into agreements with AAF Members.

AAF Shibboleth Federation: The Shibboleth (or equivalent technology) part of the Australian Access Federation.

AAF Shibboleth Federation Operator: The Operator of the AAF Shibboleth Federation, sub -contracted by the AAF.

AAF Shibboleth Federation Member: An organisation (IdP, SP or both) that has agreed to the Shibboleth Requirements of the AAF Rules of Membership.

AAF Shibboleth Federation Operator website: The website used by AAF Shibboleth Federation Members to manage their membership of the AAF Shibboleth Federation.

End-user: An individual (eg, staff, student) from an AAF Shibboleth Federation Member who uses the Federation.

Service Description: A structured description of a Service Provider, including one or more Service Offerings. Service Description information is conveyed to relevant IdPs in the Federation Metadata.

Service Offering: A description of the attribute requirements for (potential) IdP access to a service offered by a SP.

AAF Shibboleth Federation Themes

The Requirements and Recommendations in this document arise from lessons learned from the MAMS Testbed Federation and other Shibboleth federations around the world. These lessons can be summarised under a number of key themes that inform the content of this document:

(1) Unified Fabric for Authorisation

At the heart of a successful Shibboleth Federation is the need to create an end -to-end “fabric” for authorisation. Identity Providers and Service Providers benefit from agreement on end -user attributes and mechanisms for describing and exchanging attribute requirements (eg, Service Descriptions). A unified authorisation fabric avoids fragmentation of the Federation into smaller clusters of IdPs and SPs (which lack interoperability between clusters). The goal of this theme is a truly national federation that still provides mechanisms for many different trust relationships to exist within a common framework.

¹ <http://www.aaf.edu.au/documentation>

(2) Service Descriptions

A key innovation for the AAF Shibboleth Federation, based on the success of the MAMS Testbed Federation, is the requirement that all Service Providers complete a Service Description that outlines their service and its attribute requirements (and if relevant, the IdPs specified for this service). The Service Description information, combined with the MAMS “Federation Manager” system and the IdP “ShARPE” system, provides a mechanism for easy sharing of service information across the Federation, and can allow for automatic enablement of new services by IdPs if desired. The use of Service Descriptions avoids cumbersome bilateral liaison and agreements between each IdP and new SPs, and hence enhances efficiency of the Federation as a whole.

(3) Customised Federation Metadata

One of the challenges of growing federations is that Members need to manage a large set of federation metadata even when much of this metadata may not be relevant to their organisation (eg, SPs that are not accessed by a particular IdP). The AAF Shibboleth Federation will customise the metadata for each organisation based only on those entries which are relevant to the organisation, hence reducing the administrative burden on Members and avoiding information overload for End-users.

(4) End-user management of release of Personal Information

End-users should have control over the release of their Personal Information in a Shibboleth Federation. One way to achieve this is a system which intervenes in a Shibboleth transaction to let a user know what Personal Information (if any) is about to be released about them to a new SP, and permits the end-user to approve (or deny) this release of information. The “Autograph” system has been developed for the AAF Shibboleth Federation to support this requirement.

(5) Prepared software packages or freedom to build own systems

The AAF Shibboleth Federation Operator can provide free validated software packages (Shibboleth IdP, Shibboleth SP, ShARPE, Autograph, etc) to support the Requirements and Recommendations of this document – this is to minimise the technical obligations on IdPs and SPs. However, the requirements have been written so as to permit those institutions that wish to build their own systems to do so, as long as they interoperate with the requirements of the AAF Shibboleth Federation.

(6) Two Levels of Assurance (LoA)

The AAF Shibboleth Federation will be the first major federation to provide more than one trust level across the Federation. The base level (“Floor of Trust”) should be sufficient for standard “name and password” style contexts, but for situations where a higher level of assurance is needed by a Service (eg, access to Grid computing), a second, higher level of assurance can be implemented. Further information about LoAs is provided in Section 2, especially 2.2.4.2 and 2.2.4.3.

(7) Core Attributes implementation detail

This document provides detailed implementation information on the use of core attributes for the Federation’s “authorisation fabric”. This includes careful identification of (mandatory) Requirements as opposed to (encouraged but not mandatory) Recommendations, and systems to assist with implementation (eg ShARPE and Autograph).

(8) Federation Shared Services

The AAF Shibboleth Federation Operator will provide a number of shared services to enhance the operation of the Federation such as a Federated White Pages Service, an optional service for generating and managing auEduPersonSharedToken, etc. These shared services reduce or eliminate the effort otherwise required of AAF Shibboleth Federation Members, and hence provide a more efficient approach to shared infrastructure.

(9) Assistance with liaison, support and logging

The Requirements and Recommendations are designed to assist IdPs and SPs in conducting effective support and liaison between AAF Shibboleth Federation Members and, where appropriate, for end users. This will be further supported by expert assistance to IdPs and SPs by the AAF Shibboleth Federation Operator.

Taken together, these themes lay the foundation for a secure, efficient and scalable Federation, based on the lessons learned from the MAMS Testbed Federation and other Federations around the world.

1 Common (IdP and SP) Requirements and Recommendations

1.1 Technical Infrastructure

1.1.1 Federation Software

AAF Req01. AAF Shibboleth Federation members must conform to technical standards and behaviours equivalent to Shibboleth version 1.3.3.

The AAF Shibboleth Federation is based on Shibboleth 1.3.3. Shibboleth 1.3.3 technical specification documents are available from Internet2 (see <https://spaces.internet2.edu/display/SHIB/WebHome>).

While AAF Shibboleth Federation Members are not required to use Shibboleth 1.3.3 software, any alternative software (eg, Shibboleth 2; ESOE, etc) must fully interoperate with Shibboleth 1.3.3 and the Requirements of the AAF Shibboleth Federation (ie, the requirements in this document). The AAF Shibboleth Federation Operator can provide advice to assist with conformance of IdPs and SP installations for Members not using Shibboleth 1.3.3 software.

In the future, the AAF Shibboleth Federation may be based on new standards or new versions of Shibboleth. Changes to new standards or versions of Shibboleth would require community consultation and approval by the AAF Steering Committee. This requirements document would be revised in the case of a future change.

AAF Rec01. It is recommended that AAF Shibboleth Federation members install only validated software packages made available from the AAF Shibboleth Federation Operator and retain standard configurations where appropriate.

The AAF Shibboleth Federation Operator will provide validated versions of Shibboleth IdP and SP, as well as related systems such as ShARPE and Autograph, and Shibboleth-enabled applications which may be used in delivering a service. Validated software versions have been tested and have standard configuration files. AAF Shibboleth cannot provide detailed technical support for software other than those validated packages.

1.1.2 PKI Certificates

1.1.2.1 Server Certificate for Server-to-Server Interactions (i.e. back-channel)

AAF Req02. AAF Shibboleth Federation members must use an AAF approved certificate for secure server-to-server (i.e. back-channel) SAML transactions.

The AAF Shibboleth Federation uses PKI certificates for secure communication between AAF Shibboleth IdPs and SPs. Certificates must be signed by an AAF approved CA.

1.1.2.2 Server Certificate for Browser-based interactions

AAF Req03. AAF Shibboleth Federation Members are required to use widely adopted browser-trusted AAF approved PKI certificates.

In order to minimise user disruption due to browser certificate warning messages (which may diminish the overall trust of end-users in the AAF Shibboleth Federation), all AAF Shibboleth Federation Members must use a front-end certificate issued by a widely adopted (installed in over 90% of Federation users current browsers) web browser trusted CA (eg, Verisign).

1.1.2.3 Certificate Management

AAF Req04. AAF Shibboleth Federation Members must manage their certificates according to PKI industry standard practices.

AAF Shibboleth Federation Members are responsible for certificate management (maintaining validity, revocation in case of suspected compromise, etc) according to industry standard practices. Further information is available from AusCERT.

1.1.3 Time Synchronisation

AAF Rec02. AAF Shibboleth Federation members should use accurate time synchronisation.

Shibboleth uses time-stamping for security. A common cause of Shibboleth problems is lack of time synchronization for Shibboleth servers.

1.1.4 Entity NameSpaces

AAF Req05. AAF Shibboleth Federation Members must use the EntityID assigned to them by the AAF Shibboleth Federation Operator.

IdPs and SPs are known by their "providerId" or "entityID", which is typically a URN of a specific format designated by the AAF Shibboleth Federation Operator of the format urn:mace:federation.org.au:aaf:X eg, urn:mace:federation.org.au:aaf:idp.mq.edu.au. This information is provided as part of the entity registration process.

1.1.5 Customised Federation Metadata

AAF Req06. Each AAF Shibboleth Federation Member must use their customised Federation Metadata issued to them by the AAF Shibboleth Federation Operator.

The AAF Shibboleth Federation will provide customised metadata to each member based on the information that is applicable to them about trusted entities within the Federation.

AAF Shibboleth Federation members should not change the content of their file downloaded from the AAF Shibboleth Federation Operator. They may, however, choose to add a local metadata file in order to support access to services that exist outside the AAF.

A generic AAF Shibboleth Federation metadata file (ie, all IdPs and SPs, but excluding any "private" SPs) will also be available when required (eg, interoperation with other country federations).

1.1.5.1 Downloading Federation Metadata

AAF Rec03. AAF Shibboleth Federation members should download their federation metadata on an hourly basis.

AAF Rec04. AAF Shibboleth Federation members should perform cryptographic integrity checking of their downloaded Federation Metadata using the AAF Shibboleth Federation Operator server certificate.

Federation Metadata should be regularly updated by each AAF Shibboleth Federation Member, sourced from their designated location by the Shibboleth Federation Operator. The AAF Shibboleth Federation Operator will provide tools and advice on conducting this process.

1.1.5.2 Maintaining AAF Shibboleth Federation Member Details for Federation Metadata

AAF Req07. AAF Shibboleth Federation Members must ensure the accuracy of their member details used in Federation Metadata.

AAF Shibboleth Federation Members must enter and update (when relevant) their metadata via the AAF Shibboleth Federation Operator website.

1.1.6 Domain Names

AAF Rec05. IdP and SP domain-names should be sub-domains of the organisation's primary domain.

Use of a sub-domain of the organisation's primary domain can assist with security (eg, phishing).

1.2 Usage of Attributes

AAF Req08. AAF Shibboleth Federation Members are required to use the definitions (syntax, semantics, constraints) of AAF attributes specified by Attribute Recommendations for AAF Participants and this document

IdPs are not required to implement AAF attributes in their directory – the requirement is only that when they conduct a Shibboleth transaction, that the attributes in that transaction conform to the Attribute specification and this document. There are various mechanisms available (eg, mappings in ShARPE) to construct AAF Attributes from other relevant and authoritative information held by the organization (eg, in the directory).

The AAF should be notified of any uncertainty in implementation arising from apparent discrepancies between this document and the Attribute Recommendations for AAF Participants so that appropriate revisions can be investigated.

1.3 Support and Liaison

1.3.1 Liaison Person for AAF Shibboleth Federation Members

AAF Req09. AAF Shibboleth Federation Members must provide a liaison person(s) for all administrative and technical interaction with the AAF Shibboleth Federation Operator and other AAF Shibboleth Federation Members.

AAF Rec06. AAF Shibboleth Federation Members should provide both an email and telephone contact(s), and should monitor the contact(s) during business hours.

The AAF Shibboleth Federation Operator requires a liaison person(s) for each AAF Shibboleth Federation Member to allow for notifications and interaction regarding any AAF Shibboleth Federation matters, and to support communication among AAF Shibboleth Federation Members. Members provide details of the designated liaison person(s) via the Membership section of the AAF Shibboleth Federation Operator website. This information is included in AAF Shibboleth Federation Metadata. Processes for joining the AAF, including initial verification of organisations and designated liaison person(s) will be addressed in the upcoming information on Rules of Membership.

The AAF Shibboleth Federation Operator will provide support during business hours to the designated AAF Shibboleth Federation Member's liaison person(s). For security reasons, the AAF Shibboleth Federation Operator will only provide support to designated liaison person(s). Members provide details of the designated liaison person(s) via the Membership section of the AAF Shibboleth Federation Operator website.

1.3.2 Restrictions on End-User Support

AAF Req10. Unless specified otherwise, the AAF Shibboleth Federation Operator and AAF Shibboleth Federation Service Providers do not provide end-user support.

Service Providers may choose to offer end-user support and may advertise this in their service information page, but the default assumption is that Service Providers would only provide support to administrative contacts from the AAF Shibboleth Federation Operator and Identity Providers. AAF Shibboleth Federation Operator support is only available to the designated liaison person(s) of AAF Shibboleth Federation Members (not end-users).

Identity Provider obligations for end-user support are described below under IdP Specific Requirements and Recommendations.

1.3.3 Transaction Logging to Assist Federation Operator

AAF Rec07. AAF Shibboleth Federation Members should provide a mechanism whereby relevant log information can be made available to the AAF Shibboleth Federation Operator for support requests.

In order to promote effective and efficient support, AAF Shibboleth Federation members should be able to make relevant logs available to the AAF Shibboleth Federation Operator for support requests. The AAF Shibboleth Federation Operator can provide advice and systems to provide such access. Validated Shibboleth (IdP and SP) software packages will be configured to capture relevant logs. Where appropriate, logs can also be shared between IdPs and SPs to resolve support issues.

1.3.4 AAF Shibboleth Federation Member Security Alerts

AAF Rec08. AAF Shibboleth Federation Members should receive and acknowledge security alerts via email within one business day. Where requested, Members should provide information to the AAF Shibboleth Federation Operator on their planned response within five business days.

The AAF Shibboleth Federation Operator may need to provide security alerts to AAF Shibboleth Federation Members. For example, in the case of a security alert and patch being released by the AAF Shibboleth Federation Operator, or planned downtime of an AAF Shibboleth Federation Operator service (eg, Federation White Pages Service).

The AAF Shibboleth Federation Operator may need to take urgent action to resolve security problems related to vulnerabilities identified in Federation software, and if such an issue impacts other members, members are requested to inform the AAF Shibboleth of their plan to address the vulnerability. The AAF Shibboleth Federation Operator can provide advice and assistance to Members in the case of security vulnerability.

AAF Rec09. Any security issues identified by AAF Shibboleth Federation Members with their components of the Federation (e.g. software that is not part of the validated software provided by the AAF Shibboleth Federation Operator) should be reported to the AAF Shibboleth Federation Operator once identified, and where there could be a security impact on other Members, the planned response should be notified within five business days.

If AAF Shibboleth Federation Members use software that presents a security risk to the AAF Shibboleth Federation Operator or other Members, they are responsible for informing the AAF Shibboleth Federation operator of the risk and taking action to resolve the risk.

1.3.5 Support Staff Training

AAF Rec10. AAF Shibboleth Federation Members should ensure that their designated support staff have undergone training by the AAF Shibboleth Federation Operator on the AAF Shibboleth Federation.

The AAF Shibboleth Federation relies on a level of AAF Shibboleth Federation expertise by administrative and technical staff at Member sites. The AAF Shibboleth Federation Operator will provide AAF Shibboleth Federation support training courses periodically.

2 Identity Provider Requirements and Recommendations

2.1 Identity Management of End-users

2.1.1 Floor of Trust (Base Level of Assurance)

AAF Req11. IdP Identity Management must meet the minimum requirements of the AAF Shibboleth Federation "Floor of Trust" – which includes institutional assertion of end-user identities and attributes (including maintenance of currency of user accounts and attributes); IdP authentication using passwords with a minimum of six characters (with at least one letter and one number); and promptly disabling accounts if a breach is detected or if an end-user is no longer a member of the IdP.

AAF Shibboleth Federation IdPs will need to meet a minimum level of Identity Management (called “Floor of Trust”) which provides SPs with a base level of confidence in the accuracy of information delivered by IdPs (authentication information, user attributes).

The “Floor of Trust” will be the base level of assurance applicable to standard use of the Shibboleth federation. For identity proofing, it requires institutional assertion of identity and attributes for end-users (not self-assertion by end-users), but does not require face to face verification of end-user identities (eg, Human Resources or Student Information System records of an end-user based on correspondence may be sufficient). For authentication method, an account with a password is used, and the password must contain at least six characters including at least one letter and one number.

IdPs should also proactively manage the currency and security of user accounts, and promptly disable an account if a breach is detected or if an end-user is no longer a member of the IdP. Currency of attributes is also a requirement (eg, changing the eduPersonAffiliation value if a student moves to a staff role).

A successful password-based authentication at an IdP within the AAF Shibboleth Federation is itself the requirement to meet Floor of Trust, so no other information is required as evidence. In practice, this means that no value for auEduPersonIdentityLoA (see 2.2.4.3 below) or auEduPersonAuthenticationLoA (see 2.2.4.2 below) needs to be provided by IdPs or processed by SPs – values for these attributes are only required for levels above the Floor of Trust.

Additional Identity Management procedures required for the Floor of Trust may be developed following further consultation.

In addition to the specific requirements here, the Floor of Trust is also based on the legal agreement “Rules of Membership” which deals with general obligations of all AAF member organizations.

While most IdPs will maintain a single account for each end-user, there may be cases where multiple accounts exist inside an IdP for certain users (eg, individuals who have both staff and student roles). In these cases, the key requirement on IdPs is that regardless of the account used by the end-user, the attributes asserted about the end-user to AAF SPs are true. It should be noted that where an end-user uses multiple accounts from an IdP to access the same SP, the SP will normally be unable to provide access to a single SP user account. IdPs that allow multiple accounts must provide support to end-users in the event of confusion about access to SP accounts. SPs that wish to provide access to a single SP user account for end-users with multiple accounts may use AEPST as a basis for end-user resolution.

NB: It is possible that there are some desirable Floor of Trust requirements that are not ready to be implemented by a sufficient number of IdPs at the start of the AAF, but which should be requirements in the future. In this case, the AAF Shibboleth Federation may identify “sunrise” requirements which will come into effect as requirements at a future date (eg, two years after AAF launch), but which are not requirements initially.

2.1.2 Higher Level of Assurance (“level 3”)

AAF Req12. AAF Shibboleth Federation IdPs are not required to implement a higher level of assurance (ie, a level above “Floor of Trust”), but any that do implement the “level 3” assurance must meet the specified requirements for any relevant end-users – which includes “100 point” identity proofing and strong IdP authentication such as PKI or equivalent.

Initially, two levels of assurance of identity management will be supported in the AAF Shibboleth Federation – the “floor of trust” (required) and a higher level of assurance (optional) called “level 3” (as defined by the combined requirements of level 3 for both auEduPersonIdentityLoA and auEduPersonAuthenticationLoA). Additional levels may be added in the future if needed. Please refer to 2.2.4.2 below for details of LoA levels.

For the higher level of assurance (“level 3”), identity proofing must be equivalent to the “100 point test”, including face to face verification of identities as specified in auEduPersonIdentityLoA level 3. For authentication method, a minimum strong authentication technology such as PKI or equivalent will be required as specified in auEduPersonAuthenticationLoA. Please refer to 2.2.4.3 below for details of LoA levels.

IdPs are not required to implement the higher level of assurance (“level 3”), but in this case, end-users will be unable to access SPs that require this higher level of assurance. IdPs may choose to only implement the higher level of assurance for a subset of end-users (ie, those who require it for particular SPs, such as for the Grid).

2.2 Attribute Management

2.2.1 Release of Personal Information

AAF Req13. AAF Shibboleth Federation IdPs must ensure that end-users provide informed consent to the release of their personal information to SPs.

AAF Rec11. When an end-user first visits a SP that requires personal information for access, the IdP should alert the user to this requirement, and allow the end-user to approve or disapprove the release of their personal information prior to access to the SP.

End-users should provide informed consent to the release of their personal information to SPs. Personal information includes the core attributes: displayName, mail, and auEduPersonSharedToken; as well as other non-core attributes which might reveal, either singly or in conjunction with other attributes, the identity of the user.

In the AAF Shibboleth Federation, this can be achieved with the Autograph tool, which, prior to access to an SP, displays a page which indicates the SP’s request for personal information, and allows the end-user to approve or disapprove release of this information (in the case of disapproval, then SP access would normally be denied).

While the use of Autograph is not a requirement of the AAF Shibboleth Federation, IdPs that do not use Autograph should implement an approach that achieves the requirement for informed consent (this could be a system with similar behaviour to Autograph, or alternatively a paper-based process in which end-users give prior approval to the release of personal information to any IdP approved SPs). Another approach is a single online “terms of use” agreement that end-users accept once for

all use of the Federation (in which case, personal information will be automatically released to all relevant SPs once the federation “terms of use” are accepted – Autograph provides this feature as an alternative to “per SP” approval).

The AAF Shibboleth Federation Operator recommends use of the Autograph tool to inform users the first time they release personal information to an SP, but not on every occasion after first access. However, end-users should be able to review the personal information being sent to any SP, and may choose to disapprove this at any time (Autograph provides support for these features).

There may be certain cases where the relevant technology may not be suitable for web browser display inside the authentication flow (such as command line Grid access), and hence an Autograph-style approach to personal information management would be inappropriate. These cases may choose to use one-off paper or digital “terms of use” style agreements with end-users to avoid technology conflicts.

IdPs are not expected to notify end-users of the release of attributes which do not reveal the identity of the user, such as EPTID, eduPersonAffiliation, eduPersonEntitlement, etc.

2.2.2 Attribute Mapping

AAF Rec12. AAF Shibboleth Federation IdPs should either manage AAF-required attributes in their directory or alternatively construct AAF attributes using mappings to non-AAF attributes (so long as the resulting attribute meets AAF attribute requirements).

For some IdPs, it will be easiest to manage AAF-required attributes in their core directory. However, this is not a requirement of the AAF Shibboleth Federation – attributes can be created via mappings (or other methods) so long as the attributes which are provided from IdPs to SPs meet the syntax, semantics and constraint requirements outlined in the AAF Attribute specification and this document.

The AAF Shibboleth Federation Operator provided “ShARPE” tool provides facilities for attribute mapping, combination, etc.

2.2.3 Core Attributes

AAF Req14. AAF Shibboleth Federation IdPs must be able to deliver the core attributes defined in Attribute Recommendations for AAF Participants (ie, eduPersonTargetedID, eduPersonAffiliation, eduPersonScopedAffiliation, auEduPersonSharedToken, eduPersonEntitlement, mail, displayName) for any IdP staff end-user who needs to use the AAF Shibboleth Federation.

This requirement ensures that AAF Shibboleth Federation SPs have a minimum set of attributes on which they can rely for access and authorisation transactions involving relevant staff from AAF Shibboleth Federation IdPs. Note that these attributes are only required for staff that need to use the AAF Shibboleth Federation, not necessarily all IdP staff.

AAF Rec13. Core attributes should be available for all potential end-users within an AAF Shibboleth Federation IdP.

While it is not a requirement for core attributes to be available for all end-users of an IdP (eg, students, alumni, etc), it is recommended that these attributes be available to enhance the breadth of potential access to SPs.

In addition, there may be cases where some, but not all, of the core attributes can be made available for non-staff end-users at IdPs (eg, students may not have auEduPersonSharedToken).

2.2.3.1 eduPersonTargetedID (EPTID)

AAF Req15. AAF Shibboleth Federation IdPs must not re-use EPTID values across different end-users, and for each end-user, IdPs must use a different eduPersonTargetedID value for each different SP.

EPTID is an important privacy preserving, anonymous access mechanism. For the AAF Shibboleth Federation, a different value for each end-user will be delivered to each SP, as delivering the same value to a group of SPs introduces considerable complexity (e.g. group management) and runs the risk of diluting the strong privacy protection associated with this attribute. Identification across multiple SPs can be achieved by using auEduPersonSharedToken. EPTID values used for one end-user must not be re-assigned to another end-user.

The AAF Shibboleth Federation Operator can provide advice and systems for generating and managing EPTID (eg, ShARPE).

AAF Rec14. AAF Shibboleth Federation IdPs should assist SPs with EPTID roll-over/account re-association to enable end-users moving to another IdP.

In some cases, SPs alone are unable to handle account re-association without the assistance of both the previous and current IdP, and hence IdPs are expected to assist with this process.

2.2.3.2 auEduPersonSharedToken (AEPST)

AAF Req16. For any end-user who requires an auEduPersonSharedToken, AAF Shibboleth Federation IdPs must either (1) generate and use an AEPST value conforming to the specified syntax and constraints; or (2) use the AAF Shibboleth Federation AEPST Service. auEduPersonSharedToken values must not be re-used across different end-users.

There is a recognised need to provide an identifier which is used across multiple service providers (non-targeted) and which is persistent over time (in particular, it is portable so the same value is used when the user changes IdPs).

auEduPersonSharedToken (AEPST) can act as a long-lived personal identifier, and is not privacy preserving (like EPTID), so its use should take these factors into account.

IdPs have two choices for implementing AEPST, either (1) generate and maintain AEPST locally or (2) use the AAF Shibboleth Federation AEPST Service. In the first case, the IdP must generate (using the specified AEPST algorithm) and store locally the AEPSTs of relevant end-users. In the second case, the IdP implements a secure connection from the IdP to the AEPST generation and management Service provided by the AAF Shibboleth Federation Operator, which provides creation, management and on-demand delivery of AEPSTs on behalf of relevant end-users for the IdP (no local storage of AEPST by IdPs is required for the second option). Further implementation details of both approaches will be available from the AAF Shibboleth Federation Operator and <http://www.aaf.edu.au/documentation> .

AAF Rec15. AAF Shibboleth Federation IdPs should support AEPST portability for end-users moving from one IDP to another IdP.

IdPs should provide a mechanism for portability of AEPST, both for end-users that move from the IdP to a new IdP, and for new staff arriving at the IdP with an existing AEPST from a prior IdP. For IdPs that are unable to support portability, additional liaison with SPs to re-establish end-user access to relevant SP accounts may be required.

2.2.3.3 eduPersonAffiliation and eduPersonScopedAffiliation

AAF Req17. AAF Shibboleth Federation IdPs must be able to assert the value of “staff” for all IdP-designated staff end-users that need to use the AAF Shibboleth Federation.

AAF Rec16. Affiliations values should be available for all potential end-users within an AAF Shibboleth Federation IdP, based on IdP designation of individuals to relevant values.

While “staff” is a required value for eduPersonAffiliation, IdPs that do not have affiliation values available for some or all other categories of end-users can leave this attribute blank (or use the value “member” where appropriate).

As the meaning of the terms “staff”, “student”, etc, is not defined in Attribute Recommendations for AAF Participants, IdPs designate the individuals appropriate to these values based on internal mechanisms. As a result, temporary, visiting, contract and other staff may be asserted as “staff” within the AAF Shibboleth Federation, and SPs that rely on the “staff” affiliation value do so within this acknowledged constraint. Similar issues may also arise for the recommended (not but required) values of student, alumni, etc, and SPs that rely on any of these values do so within the same constraint of internal designation by IdPs of individuals to these categories.

Values for eduPersonScopedAffiliation can be dynamically generated from eduPersonAffiliation, so it is not necessary for both attributes to be implemented. The AAF Shibboleth Operator can provide assistance with dynamic generation of eduPersonScopedAffiliation from eduPersonAffiliation.

2.2.3.4 eduPersonEntitlement

AAF Req18. AAF Shibboleth Federation IdPs must implement the eduPersonEntitlement attribute, but there is no mandatory requirement for any particular value to be created or released.

AAF Rec17. AAF Shibboleth Federation IdPs should filter the values released for eduPersonEntitlement to the minimum value(s) required for each specific SP.

While eduPersonEntitlement is a required field, this does not mean that for any given SP entitlement value, the IdP is required to store or release it – this is a matter for each IdP to decide and manage. SPs cannot “force” an IdP to create an entitlement.

SPs are required to specify any eduPersonEntitlements they expect in their Service Description, which are provided to all relevant IdPs. An explanation of the entitlement is contained with the Service Description to allow IdPs to know how to assign the entitlement to relevant IdP end-users. If no explanation is available (such as where the basis of the entitlement is restricted information), the IdP should contact the SP for further details.

Filtering avoids the problem of releasing all possible end-user entitlement values to every SP that requires the entitlement attribute (when typically only one of these entitlement values is relevant to each SP). The AAF Shibboleth Federation Operator can provide tools to IdPs to assist with filtering (ShARPE and Autograph).

Entitlement is a somewhat unusual attribute in that it is managed by IdPs, but its content is usually a collection of various SP-defined entitlement values that are assigned by the IdP based on the entitlement definition provided by the SP. In the AAF Shibboleth Federation, entitlement is most useful for cases where an IdP has existing directory information (often separate from the attributes required for AAF) that can be used to automatically construct an entitlement (eg, all staff in a particular department). It can also be used by IdPs to assign entitlements to named individuals provided to the IdP by the SP, but this style of authorisation can more easily be solved by the SP using the Federation White Pages Service to select individuals to be given access on the “SP side” rather than requiring the IdP to add an entitlement value on behalf of the SP.

Put another way, other core AAF attributes (eg, affiliation) are most useful for SP authorisation when thousands of potential users are involved; entitlement is most useful when there are hundreds of potential users and IdP information exists to make the assignment of the entitlement value easy; and the Federation White Pages Service is most useful when tens (to perhaps a few hundred) of potential users are involved (SPs select the relevant individuals “by hand”, and don’t need IdP assistance).

Third-party entitlements (such as those asserted by authoritative organisations – eg, the entitlement “Psychologist” as asserted by the Australian Psychological Society) will be explored in the future, based on a Federation-level entitlement service. This approach can also provide a mechanism for clusters of SPs to share entitlements, including SP identifier-style entitlements.

2.2.3.5 mail

AAF Req19. Where the “mail” attribute is implemented for relevant end-users (ie, for relevant staff it is required, for other end-users it is recommended), AAF Shibboleth Federation IdPs must provide only a single value for this attribute that represents (or is forwarded to) an active email account.

AAF Rec18. AAF Shibboleth Federation IdPs should implement “mail” values that are persistent over the life of the end-user’s association with the IdP.

Certain SPs (those accessed non-anonymously) may provide a mechanism for contacting a user by email (eg, for account information confirmation purposes), or may use email as an account identifier. The email address provided by IdPs should either represent an active email account (active from the perspective of the IdP – ie, the IdP is not expected to assess ongoing use of the account by the end-user) or be forwarded to an active email account.

IdPs should, where possible, implement mail values that are persistent over the life of the end-user’s association with the IdP, ie, not changing the mail value for users over time (as some SPs use email as an account identifier). However, this is not a requirement, as it is recognised that this recommendation is not practical in certain contexts.

2.2.3.6 displayName

AAF Req20. AAF Shibboleth Federation IdPs must ensure the suitability and accuracy of displayName.

In order to provide a user-friendly name string, and also as a non-unique but identifying string for certain services using AEPST such as logs in Grid services, a display name is to be specified or generated for all users. This value can be generated from existing institutionally-asserted name entries (such as “cn” – common name).

If the IdP permits (some) users to provide a self-asserted value for displayName (eg, where their preferred name of address is different from the official institutional name entry), the IdP needs to ensure the suitability and accuracy of this value as it is used in the Federation (if an IdP becomes aware of an inappropriate value, it should be changed to an appropriate value). Display names should be collected in a context that makes it clear that the supplied displayName will be used for professional identification.

2.2.4 Non-Core Attributes

2.2.4.1 eduPersonPrincipalName (EPPN)

AAF Rec19. IdPs should exercise caution when releasing EPPN as it may contain account authentication information.

While eduPersonPrincipalName can be useful to local institution (ie, non-federated) authentication and account provisioning, as well as a useful attribute as a basis for algorithmic generation of identifiers (such as EPTID or AEPST), IdPs should exercise caution when using it within the Federation due to its potential inclusion of transparent local account information.

2.2.4.2 auEduPersonAuthenticationLoA (and SAML AuthenticationMethod)

AAF Req21. **If an AAF Shibboleth Federation IdP releases a value of “3” from auEduPersonAuthenticationLoA, the end-user authentication act must meet, at a minimum, the requirements of “level 3” for this attribute (see notes below). This value must be conveyed using the SAML AuthenticationMethod attribute (not auEduPersonAuthenticationLoA), and IdPs must ensure the security of the SAML AuthenticationMethod attribute.**

AAF Rec20. **In addition to the requirement for “3” from auEduPersonAuthenticationLoA, AAF Shibboleth Federation IdPs may also assert values of “2” and “4” using the SAML AuthenticationMethod attribute in accordance with the requirements for these values (see notes below).**

The AAF Shibboleth Federation does not require the processing of SAML AuthenticationMethod for standard use of the Federation. A successful password-based authentication at an IdP within the AAF Shibboleth Federation is itself the requirement to meet Floor of Trust, so no other information is required as evidence.

If an IdP supports a higher level of assurance for (some) end-users, it is required to support the requirements of the value of “3” from auEduPersonAuthenticationLoA. This requirement supports “2.1.2 Higher Level of Assurance”. For an end-user who meets this requirement, a value of “3” is conveyed to the SP using SAML AuthenticationMethod (NB: auEduPersonAuthenticationLoA is not used as an attribute in this context – it just provides vocabulary definitions for AAF Shibboleth Federation values used within SAML AuthenticationMethod).

IdPs must ensure the security of SAML AuthenticationMethod (eg, prevent end-user spoofing of values). The AAF Shibboleth Federation Operator will provide software to help protect the security of SAML AuthenticationMethod as part of the validated IdP software package. Guidelines and assistance will be provided for IdPs not using the validated IdP package to assist with secure configuration.

auEduPersonAuthenticationLoA allows for additional levels of granularity in strength of authentication above the “Floor of Trust” level which may be useful in certain contexts – however, any SP application that wishes to rely on these additional levels will need to be configured to process these other values of auEduPersonAuthenticationLoA as conveyed within the SAML Authentication attribute. In addition, the “1” value of auEduPersonAuthentication should not be used, as it represents a level different from the Floor of Trust.

For IdPs that do not implement the auEduPersonAuthenticationLoA and auEduPersonIdentityLoA attributes, the AAF Shibboleth Operator can provide software for PKI-based end-user authentication that, following successful authentication, will dynamically provide a value of “3” for SAML AuthenticationMethod and auEduPersonIdentityLoA – subject to the issuance of the relevant certificate used for authentication also meeting the requirements of level 3 for auEduPersonIdentityLoA (see 2.2.4.3 below).

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.

2.2.4.3 auEduPersonIdentityLoA

AAF Req22. If an AAF Shibboleth Federation IdP releases a value of “3” for auEduPersonIdentityLoA, the end-user identity proofing must meet, at a minimum, the requirements of “level 3” for this attribute (see notes below).

AAF Rec21. In addition to the requirement for “3” for auEduPersonIdentityLoA, AAF Shibboleth Federation IdPs may also assert values of “2” and “4” in accordance with the requirements for this attribute (see notes below).

auEduPersonIdentityLoA is not needed for the standard level of assurance in the Federation (ie, Floor of Trust), as inclusion of an end-user into the IdP is itself the requirement for meeting the Floor of Trust, and so no other information is required as evidence.

As with auEduPersonAuthenticationLoA, if an IdP supports a higher level of identity assurance for (some) end-users, it is required to support, at a minimum, an official Federation value of “3” for auEduPersonIdentityLoA. This requirement supports “2.1.2 Higher Level of Assurance”.

This attribute allows for additional levels of granularity in strength of authentication above the “Floor of Trust” level which may be useful in certain contexts – however, any SP application that wishes to rely on these additional levels will need to be configured to process these other values of auEduPersonIdentityLoA attribute. In addition, the “1” value of this attribute should not be used, as it represents a level below the Floor of Trust.

IdPs that do not implement auEduPersonIdentityLoA, but use the dynamic generation approach described under auEduPersonAuthenticationLoA, should ensure that AAF authentication certificates (or other stronger authentication methods) are only provided to end-users who also meet, at a minimum, the requirements of level 3 for auEduPersonIdentityLoA.

A proposed measure is defined in auEduPersonIdentityLoA and has values representing four levels - an AAF specific Floor of Trust 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.

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 subject's identity is based on a continuous relationship with the Identity Provider organization for a period of greater than three years.

2.3 Attribute Release

2.3.1 Minimum Disclosure

AAF Rec22. AAF Shibboleth Federation IdPs should adopt a policy of "minimum disclosure" when releasing attributes to SPs. Only attributes specifically required by SPs should be released to them.

IdPs should avoid attribute release policies that release more information than is required for access to relevant SPs (eg, "release all available attributes").

2.3.2 IdP Administrator Configuration of ARPs

AAF Rec23. AAF Shibboleth Federation IdPs should make use of the AAF Shibboleth Federation Operator-provided ShARPE tool, or an equivalent system, for configuring ARPs, including automatic enablement of SPs that meet an IdP's pre-defined requirements.

ShARPE is available to all IdPs to assist with the management of ARPs. If this tool is not used, a similar web-based management approach is recommended, rather than hand editing of ARP XML files.

The AAF Shibboleth Federation Operator will provide notification to IdPs of new SP Service Descriptions. IdPs using ShARPE can choose to automatically enable appropriate ARPs for these new SPs, or enable these subject to review of the SP by the IdP administrator. This approach greatly reduces the administrative overhead of enabling new SPs for IdPs.

2.3.3 End-user Management of Attributes & Personal Information

AAF Rec24. AAF Shibboleth Federation IdPs should provide a mechanism for informing users of the release of personal information on first visit to a SP, and subsequently when the set of personal information released is changed, or new personal information is required. AAF Shibboleth Federation IdPs should encourage use of the AAF Shibboleth Federation Operator-provided Autograph tool, or an equivalent system, for end-users to manage their attributes and privacy.

Use of Autograph (or an equivalent tool) should be encouraged not only as a means of privacy control, but as a means of end-users obtaining information on use of Attributes by SPs. Autograph can be used in two ways: (1) Stand-alone use of Autograph to review the attributes expected by an SP for a given Service Offering and (2) Where Autograph displays a page prior to SP access showing any personal information attributes that are to be released, and confirms acceptance of this release (or deny). Confirmation can be "once for all future access" (default) or "confirm for each access"

However, this approach to privacy management is a recommendation, not a requirement. IdPs may choose not to use the processes described, but instead use a single "terms of use" style agreement with end-users about their use of the AAF (which would include agreement to the release of their personal information to any relevant SP). This single "terms of use" can be implemented online (Autograph provides a feature for this approach) or via a paper-based process. Regardless of the method of implementation, the key requirement in this area is specified under 2.2.1

2.4 IdP Management

2.4.1 IdP Information Web Pages

AAF Rec25. AAF Shibboleth Federation IdPs should provide information to end-users which describes the IdP's involvement in the AAF Shibboleth Federation, including a list of services that are relevant to end-users.

The AAF Shibboleth Federation is intended to be an "information rich" federation, providing comprehensive information on IdPs and SPs to AAF Shibboleth Federation end-users. IdPs should, at a minimum, provide end-users with basic information about their involvement in the AAF Shibboleth Federation, including a list of potentially relevant services and any comments on these services.

The AAF Shibboleth Operator will provide customised metadata for each IdP, based on filtering of only the Service Offerings of SPs that are potentially relevant to the IdP.

IdPs can use the Autograph tool provided by the AAF Shibboleth Federation Operator to present this information to users, including filtering of services according to end-user interest and display of SP requirement such as attributes.

2.4.2 IdP Infrastructure

AAF Rec26. AAF Shibboleth Federation IdPs should implement a high-availability IdP.

IdP end-users rely on the Shibboleth IdP software (or equivalent other systems) to access Federation Services, hence it is recommended that IdPs adopt a high-availability server configuration. The AAF Shibboleth Federation Operator can provide advice and example implementations to assist with configuring the Shibboleth IdP for high availability.

2.4.3 IdP End-User Support

AAF Req23. AAF Shibboleth Federation IdPs must provide a first-level support capability for their end-users to help resolve problems in using the Federation.

AAF Rec27. IdPs should endeavour to resolve end-user support requests locally before forwarding requests to SPs or the AAF Shibboleth Federation Operator.

IdPs should use the AAF Shibboleth -provided Autograph tool, or an equivalent approach, for end-user trouble-shooting to determine the effective ARP for particular Service Providers, and comparison of this with the required attributes specified in the relevant Service Offering.

2.4.4 IdP End-User Logging & Traceability

AAF Req24. AAF Shibboleth Federation IdPs must maintain authentication and transaction logs which enable traceability of end-users.

AAF Rec28. AAF Shibboleth Federation IdPs should maintain logs of the session-based "user-handle" value issued to the SP and the relevant end-user eduPersonTargetedID, to enable traceability to an identity at the IdP.

IdPs need logs of end-user authentication and transactions for cases where an end-user's behaviour needs to be traced, such as unexpected failures to access relevant services, or in cases of misuse. Logs should be maintained for a minimum of six months.

2.5 Federation Shared Services

2.5.1 Federation White Pages Service

AAF Req25. AAF Shibboleth Federation IdPs must provide support for the Federation White Pages Service for searching for relevant staff end-users (at a minimum, showing displayName and email).

AAF Req26. Any AAF Shibboleth Federation SP that invites users to access a service via email must sign the invitation email using an AAF approved PKI certificate.

The Federated White Pages Service is key to enabling Federation-wide designation of individual end-users for SP access (via identification using their email address). It is also convenient as a web-based white-pages service. Where possible, IdPs should provide additional information about users which can help to distinguish between people of the same name (eg, Department, Title, etc this information may not match an existing AAF Attribute).

NB: The Service is not public - it is protected for use only by AAF Shibboleth Federation end-users (therefore email harvesting is not considered to be a risk).

2.5.2 Federation AuEduPersonSharedToken (FAST) Service

AAF Rec29. AAF Shibboleth Federation IdPs should implement a secure connection to the Federation AuEduPersonSharedToken (FAST) Service when the IdP uses FAST to manage AuEduPersonSharedToken.

As described in the comments for auEduPersonSharedToken, IdPs that choose to rely on management of this attribute at Federation level need to implement a secure connection to the Federation AuEduPersonSharedToken (FAST) Service.

2.5.3 Federation Entitlement Service

AAF Rec30. AAF Shibboleth Federation IdPs should implement a secure connection to the Federation Entitlement Service for entitlements managed by the Federation Entitlement Service.

In the future, some entitlements may be managed at Federation level (eg, third party entitlements, SP cluster entitlements). To access these entitlements, IdPs need to implement a secure connection to the Federation Entitlements Service (in a similar way to the Federation AuEduPersonSharedToken).

2.5.4 Virtual Home Organisation

AAF Rec31. The AAF Shibboleth Federation Operator will provide a Virtual Home Organisation (VHO) service for end-users who require access to the AAF, but who lack an AAF-enabled IdP at their home organisation. The currency and accuracy of information held in the VHO will be managed in accordance with AAF VHO policies.

Some end-users may not have access to an AAF-enabled IdP, in which case the VHO service can provide an alternative AAF login mechanism. Policies for the ensuring the currency and accuracy of end-user records in the VHO will be provided by the AAF (to be developed in Q3 2008).

3 Service Provider Requirements and Recommendations

3.1 Service Descriptions and Service Offerings

AAF Req27. Each AAF Shibboleth Federation SP must provide a Service Description which describes the Service Offering(s) and the attributes (and if relevant, attribute values) required for access.

Service Descriptions are a key feature of the AAF Shibboleth Federation to efficiently provide SP information and attribute release requirements to AAF Shibboleth Federation IdPs. The AAF Shibboleth Federation Operator website provides tools for creating Service Descriptions as part of the process for SPs to join the Federation.

While a given Service Offering may not be offered to all IdPs by an SP, the Service Description is still included in the Federation Metadata.

AAF Req28. AAF Shibboleth Federation SPs must specify in the Service Description which IdPs are potentially able to access the Service Offering(s).

This requirement allows for filtering out of Service Offerings which are not relevant to a given IdP. It also allows an SP to have different agreements with individual IdPs (via designation of a Service Offering which is available only to a single IdP).

While many SPs will be viewable by any IdP (ie, if at least one Service Offering is available to them), it is possible to have “private” SPs which are only viewable by designated IdPs. This is achieved via customized federation metadata. One possible use of “private” SPs is for intra-institutional Single Sign-On that is facilitated by the Federation infrastructure, but no other AAF Shibboleth Federation Member can view or access the internal SPs of the organisation.

NB: Offering a service from an SP to an IdP (via a Service Description) is not the same as the SP providing automatic access to an IdP end-user. SPs will often have additional requirements (apart from IdP attribute release requirements) prior to enabling service access for IdP end-users, eg, IdP and/or end-user agreement to SP Terms and Conditions; payment of a subscription fee (if relevant); designation of named individuals who are permitted to access the service, etc. SPs always have control over the conditions for access to their Services. The designation of potential IdPs, and the attributes required from them, can be a necessary but not sufficient condition for end-user access.

AAF Rec32. Service Offerings should request only attributes defined in Attribute Recommendations for AAF Participants.

Attribute Recommendations for AAF Participants defines the syntax, semantics and constraints for the AAF Shibboleth Federation. To ensure broad understanding of the interactions between IdPs and SPs, Service Offerings should avoid using any other attributes outside the Attribute Recommendations for AAF Participants document.

AAF Rec33. Service Offerings should request only the minimum attributes required to enable effective use by end-users.

As part of the general AAF principle of minimum disclosure, AAF Shibboleth Federation SPs should only request the attributes (and values) they require for effective use by end-users (rather than, say, “all available attributes” requests).

AAF Rec34. Service Descriptions should provide a text description of attributes (and if relevant, the values of attributes required) to gain access.

Providing information on the attributes required (and where relevant, attribute values – such as “staff” for eduPersonAffiliation) may assist IdP administrators to resolve SP access issues for end-users. This text description can contain information meant for IdP administrators that may not be appropriate to list on the general “SP Information Web Page” (see below).

AAF Rec35. If a Service Offering includes any optional attributes, these should be distinguished from the required attributes.

In general, Service Offerings only consist of required attributes (and if relevant, required values for these attributes) – that is, the attributes which are necessary for access to the service. If any of the required attributes are not provided, access to the service would be denied.

In special cases, a Service Offering may wish to specify an optional attribute (eg, displayName) that is not required for service access, but which may enhance the end-user’s experience of the service (eg, by welcoming the end-user by name). In these cases, optional attributes can be specified, but they are not required for service access – IdPs or end-users could block the release of these optional attributes without affecting access to the relevant Service Offering.

It should be noted that in some cases, a service may have two different Service Offerings (eg, one anonymous and one identified by name) which provide different features for users according to the different attributes required. In this case, the SP should provide two distinct Service Offerings with two different attribute requirements (not use an optional attribute).

AAF Rec36. In cases where the attributes (or attribute values) provided by an IdP for an end-user may enable access to more than one Service Offering, the AAF Shibboleth Federation SP is responsible for determining the appropriate Service Offering to provide to an end-user.

There may be cases where an end-user has more than one Service Offering enabled for them for a given SP, and hence the IdP may provide a set of attributes (or multiple attribute values) for the end-user to the SP for all applicable Service Offerings. For example, a PhD student who is also a tutor may have both the “student” and “staff” values for eduPersonAffiliation, and this value may be relevant to enabling different Service Offerings. It is the responsibility of the SP (not the IdP) to determine the appropriate Service Offering to provide to the end-user (either automatically, or by manually allowing the end-user to choose if appropriate).

AAF Rec37. Service Offerings that contain required eduPersonEntitlement values should specify the value using the format urn:mace:federation.org.au:aaf:[EntitlementIssuingOrg-ID (usually the SP)]:[entitlementvalue] , and provide either a description of how an IdP should assign this entitlement, or contact details for IdP-SP discussion of assignment.

Entitlement values need to be unique within the federation, hence the format of the value (eg, urn:mace:federation.org.au:aaf:onlinelib.mq.edu.au:operator). SPs should provide a text description in the Service Offering that explains to IdPs how to assign the entitlement, or in cases of restricted information for creating the entitlement (such as a list of named individuals), the SP should provide contact details for the IdP to discuss entitlement assignment. A SP which has an existing (unique) entitlement value of a format other than that described above (eg, a global SP that operates in multiple federations) may specify and use their existing value.

AAF Rec38. Service Offerings that require eduPersonEntitlement values should use an opaque value if privacy concerns may exist around the release of this value to SPs other than the intended target.

SPs should note that while filtering of entitlements is recommended, it is not a requirement, and hence an entitlement value assigned to an individual may be viewed by any SP that requires the entitlement attribute. For this reason, entitlement values should be opaque (eg, a string of numbers) rather than transparent (eg, “authorized pornography researcher”) in cases where privacy

concerns may exist about the release of the specific SP entitlement value to all SPs that use the entitlement attribute.

3.2 Privacy and Personal Information

3.2.1 Handling of Personal Information

AAF Req29. AAF Shibboleth Federation SPs must handle end-user personal information in a way that minimises the risk of unauthorised disclosure. SPs must not use end-user attribute information for purposes other than delivery of the service to relevant end-users (and any other SP obligations under the AAF).

SPs should take all reasonable steps to minimise the risks of unauthorised disclosure of end-user personal information. This includes limiting the amount of personal information requested in Service Descriptions to that which is necessary; limiting the timeframes for caching personal information during transactions; avoiding storage of personal information when ongoing records of user behaviour are not required for the relevant Service Offering(s); and secure management of any stored records of user behaviour where storage is required by the nature of the relevant Service Offerings(s). SPs should use the attribute information that they receive about end-users from IdPs only for provision of relevant services – this information may not be used for other purposes (except those purposes required under the obligations of participation in the AAF, such as resolution of support issues). SPs also must not release personal information to third parties external to the AAF (such as selling or sharing end-user data with other organisations, etc).

3.2.2 Personalisation and Anonymity

AAF Rec39. If personalisation or user tracking is required for an anonymous Service Offering, SPs should use the opaque identifier eduPersonTargetedID (EPTID).

SPs that support anonymous (ie, pseudonymous) access are still able to provide personalisation for users (eg, keeping records of past search requests) by using EPTID as the identifier for the user.

In addition, SPs which support anonymous access, but which may occasionally need to block access for an individual user (eg, due to misuse) can use EPTID as a basis for blocking an individual without needing to block access for all users.

3.2.3 Commercial SP requests for personal information attributes

AAF Req30. Any commercial SP Service Descriptions that request personal information attributes (eg, mail, name, AEPST) will be reviewed against AAF policies on SP use of end-user personal information, and Service Descriptions that do not meet AAF policies will not be provided to IdPs.

The AAF Shibboleth Federation Operator will review relevant Commercial SP Service Offerings that require end-user personal information (eg, mail, name, auEduPersonSharedToken) to ensure there is a demonstrated need for end-user personal information. Advice on alternative attribute requirements will be provided to Commercial SPs in cases where personal information is not required, such as anonymous access to journal articles from a Commercial publisher (eg, in the case of Commercial SPs which do not need a long-lived personal identifier for access, but rather could use attributes such as EPTID). AAF review is not required for SPs from universities, NCRIS areas, ARCS or ANDS services or other non-commercial SPs.

3.2.4 Continuity of Access

AAF Rec40. AAF Shibboleth Federation SPs should be able to map an existing user account to a new AAF Shibboleth Federation identifier (eg, EPTID, AEPST) when necessary.

AAF Rec41. AAF Shibboleth Federation SPs that need email as an account identifier should also record EPTID in the event that an end-user's email address changes over time.

End-user identifiers (such as EPTID and AEPST) may change in certain circumstances (eg, revocation of a past identifier, change of institution by end-user), so SPs should maintain mechanism for remapping an existing user account (associated with a prior identifier) to a new identifier.

While email is not recommended as a definitive end-user identifier (due to the potential for change over time), some SPs need to use email as an account identifier due to internal application requirements (this is only applicable to SPs that are non-anonymous). In these cases, the SP should also record EPTID to allow for re-association of accounts with a user when an email address changes.

3.3 SP Management

3.3.1 SP authentication attribute processing

AAF Rec42. SPs that require a higher level of assurance (eg, “level 3”) than the “Floor of Trust” should process the values of the `auEduPersonIdentityLoA` and `SAML AuthenticationMethod` attributes.

The AAF Shibboleth Federation requires IdPs to ensure that any standard end-user authentication (ie, password based) meets the requirements of the “Floor of Trust”, and hence the act of successful authentication itself is proof of meeting this level, and hence no value is required for `SAML AuthenticationMethod`. For a higher level of assurance (eg, “Level 3”), the SP needs to process the `auEduPersonIdentityLoA` and `SAML AuthenticationMethod` attributes.

3.3.2 SP Information webpage

AAF Req31. An AAF Shibboleth Federation SP must provide a URL for information about its service.

AAF Rec43. The information URL for an AAF Shibboleth Federation SP should contain information about the SP, the Service Offering(s), attribute and attribute value requirements for access, other requirements for access (Terms and Conditions, subscription, named individuals only, etc), how attributes are used (eg, for account creation), and whether attributes are cached/retained after access (and if so, provide details of why they are retained, for how long, etc).

AAF Shibboleth Federation SPs should provide information to end-users about the SP and Service Offerings, and this should include details of how their attributes are used by the SP. This information helps end-users to understand the SPs in the Federation, and the requirements for access.

There may be cases where it is not appropriate to provide certain information to end-users (eg, values for some required attributes). However, if this information could be provided to IdP administrators, it can be included in the text description that accompanies a Service Description (see above).

3.3.3 Error Pages

AAF Rec44. AAF Shibboleth Federation SPs should provide informative error pages in order that end-users can understand why they have encountered an error (and take effective action if appropriate).

Federated access to services has the potential to confuse users and leave them in the dark regarding their inability to access a service. It is important in terms of minimising support burden to provide informative error messages in order that the user can understand the error situation and take action if appropriate.

3.3.4 End-User Direct Contact

AAF Rec45. If AAF Shibboleth Federation SPs intend to make contact with end-users outside the context of their use of the relevant SP, users should provide prior approval for this contact.

If SPs wish to make direct contact with end-users for reasons that are outside the context of their use of the SP (eg, promotion of new services or other matters not related to access to the current SP), they should first gain permission for direct contact from the end-user via an indirect mechanism (eg, by providing users with information about the proposed contact when they are using the relevant SP application, and gaining end-user approval for direct contact). This recommendation is needed to avoid the potential for SPs to “Spam” users with unwanted contact or information.

Prior end-user approval is not required in the case of a signed email invitation arising from use of the Federation White Pages Service.

3.3.5 SP Logging and Troubleshooting

AAF Rec46. AAF Shibboleth Federation SPs should capture logs of basic information about end-user access, and should assist the AAF Shibboleth Federation Operator with troubleshooting where relevant.

Logs can assist with identifying and resolving problems with end-user access, although these logs should be managed according to AAF requirements for handling personal information.

The validated SP software available from the AAF Shibboleth Federation Operator will come pre-configured to assist with capturing basic log information. SPs should work together with the AAF Shibboleth Federation Operator to resolve access problems where possible.

3.3.6 Where Are You From (WAYF)

AAF Rec47. AAF Shibboleth Federation SPs should provide a custom WAYF if the Service is applicable to only a small number of IdPs; otherwise SPs should redirect to the Federation WAYF.

The Federation WAYF provides a listing of all Identity Providers so that an end-user can select their home IdP for authentication. For SPs that are applicable to only a small number of IdPs, a Custom WAYF that only shows a list of the relevant IdPs for access to the SP is recommended. Where appropriate, a Custom WAYF may provide a link to the Federation WAYF.

3.3.7 SP Terms and Conditions and Storage of End-user Information

AAF Rec48. AAF Shibboleth Federation SPs should provide an information screen prior to access to a Service Offering that describes any Terms and Conditions applicable to the Service Offering, as well as any storage of end-user information by the SP (including the reasons for storage and limits on the use of end-user information). End-users should have the opportunity to accept or reject the requirements described on the information screen prior to first access.

Many SPs will have requirements related to end-user access – these SP Terms and Conditions may cover appropriate use of the service, legal rights related to access and use of the service (including use of information within the service, such as datasets), and other information that should be notified to an end-user prior to first access, such as any storage of end-user attributes (or related information such as user actions within the service) by the SP (including reasons for storage, eg, account management), and relevant limits on the potential use of this information (eg, only for the designated purposes of this SP alone). After reviewing the information screen, end-users should have the ability to accept or reject these Terms and Conditions (rejection would normally mean inability to access the service).

If there are different Terms and Conditions relevant to different Service Offerings provided by a SP, then end-users should be presented with information for any relevant Service Offerings they can access.

SP Terms and Conditions should be presented on first access. Subsequent use of the service is covered by the initial acceptance of the requirements. Depending on the nature of the requirements,

SPs may need to present this information each time the service is accessed, rather than only on the first time it is accessed. If the information is only presented on the first time, a link for this information should be provided (if end-users wish to review it at a later date).

In cases where the login process for a SP would become too complex for users arising from the recommendation above, an alternative mechanism for providing this information should be considered (eg, link to this information from relevant SP screens, email message, etc).

3.3.8 SPs that act as Gateways to other Services

AAF Rec49. If an AAF Shibboleth Federation SPs acts as a gateway to other Services (which are not registered as AAF SPs), end-users should be made aware of the nature of these other Services, including information about the storage and use of end-user information by these Services.

In certain cases, an SP may not represent a single service, but rather act as a gateway to a range of services that exist outside the AAF Shibboleth Federation (eg, Grid services behind a Shibboleth-enabled Grid Gateway; Virtual Organisation management systems such as IAMSuite accessed via an AAF SP, etc). End-users should be made aware of the existence and purposes of these other Services, and in particular, their storage and use of end-user information. This is to allow end-users to determine whether to accept or reject the “passing through” of their information from the SP gateway to the Services “behind” the gateway. This information can be presented when an end-user first accesses a SP acting as a gateway; or if this would become too complex for users, an alternative mechanism for providing this information should be considered (eg, link to this information from relevant SP screens, email message, general “terms of use” agreement (either paper or digital) that describes the context of use of this SP, etc). Services behind SP Gateways are still required to abide by the requirements of this document in relation to management of Privacy and Personal Information.

SPs that act as Gateways to other Services must still provide a Services Description (see 3.1) and either (i) a single Service Offering that represents the superset of attributes required for all the Services behind the gateway; or (ii) provide individual Service Offerings for each Service behind the gateway.