NERC Data Grid Security

Options for Shibboleth Integration

Version 0.2

P J Kershaw

Document Log

Version Number	Date	Comment
0.1	11/02/08	First Draft
0.2	25/02/08	Include summary and section for user ID requirement for data download

Contents

1. References 4

2. Summary 5

3. Introduction 6

3.1 Drivers for NDG Security Shibboleth Integration 6

4. Shibboleth Background 7

5. Implications of Shibboleth Integration 8

6. How to integrate? 9

6.1 User Identity and SAML Authentication Assertions 9

6.2 Shibboleth Enable NDG Login 9

6.3 SAML Attribute Assertions for NDG Role Based Access Control 9

6.4 NDG Role Mapping and Shibboleth 10

6.5 Shibboleth enable an NDG Attribute Authority 10

6.6 Session Manager and Gatekeeper Considerations 10

1. REFERENCES

1. NERC Data Grid Security Computational Viewpoint, P J Kershaw, version 0.1, 05/02/2008

2. Shibboleth Architecture Protocols and Profiles, Scott Cantor, 10/09/2005, http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf

3. Electronic Authentication Guideline Recommendations of the National Institute of Standards and Technology, William E. Burr, Donna F. Dodson, W. Timothy Polk, NIST Special Publication 800-63, version 1.0.2,, April 2006 http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

2. SUMMARY

- ➔ There is sufficient cross-over between Shibboleth and NDG Security architectures for NDG Security to adopt part or all of the Shibboleth architecture.
- ➔ Two alternative strategies can be envisaged for integration:
  - ➔ make NDG Security interoperable with Shibboleth sites. i.e. write a Shibboleth API for NDG Security.
  - ➔ adopt the Shibboleth architecture in it's entirety for NDG Security.
- ➔ Whatever is chosen a piecemeal step-by-step approach will enable a continuous assessment of the benefits along the way.
- ➔ There are key architectural issues to tackle:
  - ➔ Single Sign On: Shibboleth and NDG Security are closely aligned. NDG would benefit from the use of a widely adopted standard.
  - ➔ User anonymity: Shibboleth operates on the principle of opaque user handles to identify users but NDG partners have a legal requirement in some cases to know the identity of a user requesting a dataset. NDG Data Providers (aka Shiboleth SPs) could place a requirement on Shibboleth IdPs to release user IDs in authentication assertions
  - ➔ Granularity of user attributes: attributes are typically defined on a per project basis at NDG partner sites. UK Federation attributes do not give this level of granularity. However, Shibboleth does allow for SPs to define their specific user attributes
  - ➔ Role mapping and federated versus bilateral trust: Shibboleth has no concept of role mapping. Adapt for NDG by applying role mapping at the NDG Gatekeeper. An NDG Gatekeeper would apply the mapping through a back-end connection to its Attribute Authority or role mapping service. Another alternative would be for NDG to define its own federation.
  - ➔ Command line use case: Shibboleth is web based architecture not suited for NDG's to this use case. Ignore Shibboleth for the NDG Security command line use case and retain the existing mechanism based on PKI and proxy certificates.
- ➔ Membership of the Shibboleth UK Federation places legal requirements on participants

3.INTRODUCTION

This document considers how NDG Security could integrate with Shibboleth.

3.1 Drivers for NDG Security Shibboleth Integration

- ➔ wider access to NDG services for UK academia and internationally
- ➔ adoption of standards based, peer reviewed, well understood model
- ➔ potential for wider interoperability

4. SHIBBOLETH BACKGROUND

- ➔ Shibboleth is an architecture not a framework or software implementation. There implementations e.g. Internet2 and Guanxi but the Shibboleth specification exists independently of these.
- ➔ It is built on the OASIS SAML 1.1 Specification
- ➔ Shibboleth realises a more static structure for interfaces and services than envisaged by the model for the Grid.
- ➔ Shibboleth is oriented around a web based architecture.

5. IMPLICATIONS OF SHIBBOLETH INTEGRATION

- ➔ Federation wide versus bilateral trust
- ➔ User identity assurance levels
- ➔ Perceived coarse grained federation wide attributes
- ➔ Legal requirements are placed on an organisation for it to become a member of an official Shibboleth federation. e.g.
  - ➔ to become an IdP, the organisation must have technical, administrative and support contacts. These may be one and the same person.
  - ➔ IdPs must keep authentication logs for an agreed minimum period.
- ➔ Lack of support for command line / application based interface.
- ➔ PKI with static machine / organisation based certificates versus grid based dynamic user proxy certificates
- ➔ User anonymity user session handles versus user proxy certificates. A Shibboleth SP can log which *organisation* has made an access request but not the identity of the *individual*. However, it has a record of the user session handle for a given request. It can present this to an IdP and request the identity of that user.
- ➔ Legal Requirements for data release some datasets held by the BADC are distributed on the basis that the requester must provide their user identity. A user session handle is not sufficient. SAML Authentication assertions in the context of NDG must provide some from of user ID.

6. HOW TO INTEGRATE?

This could cover a spectrum of options from at one end support for authentication through Shibboleth IdP to full application for AuthN, AuthZ attribute management. Adopting a piecemeal approach would ease the integration effort and enable continual assessment of the benefits with the option to halt at any given stage.

6.1 User Identity and SAML Authentication Assertions

Shibboleth SAML Authentication assertions do not contain a user ID, only a user session handle. Some datasets held by NDG partners require a valid user ID to be provide in order for the data to be released. To interoperate with NDG then, authentication assertions would be required to contain some form of user ID in order for access to these datasets to be enabled.

Two options are:

1) require IdPs to provide user ID information. If an IdP doesn't release it then its users will not have access to the given data. One issue is take into account is that this data is not permitted to be passed on to any other organisation than the SP host.

2) associate user e-mail address with the ePTID (federation wide identity attribute). This is the solution JISCMAIL used. There are some data protection issues that you need permission from the user to "process" the data.

6.2 Shibboleth Enable NDG Login

NDG Data Provider WAYFs would include Shibboleth IdPs or alternatively link to the UK or other Shibboleth Federation WAYFs.

- ➔ What assurance level does NDG put on Shibboleth users?
- ➔ Following from this, what NDG attributes are assigned to Shibboleth users?
- ➔ MyProxy to enable dynamic generation of user certificate from Shibboleth Authentication assertion?
- ➔ The NDG Data provider Login Service interaction would need to be adapted. Data Provider would require a Shibboleth SP interface to a Shibboleth IdP

6.3 SAML Attribute Assertions for NDG Role Based Access Control

The UK Federation supports only a limited number of very generic attributes through the eduPersonEntitlement element. These are too coarse grained for NDG Data Providers who use are accustomed to per-project allocation of role names and in some case per project coupled with access right constraints (NOCS).

However, Shibboleth does allow individual IdPs and SPs to assign their own attributes. Attributes have global scope across a federation but they can be defined as a URI enabling the use of name spaces to avoid possible naming conflicts.

Attribute Release policies determine which attributes are transparent to the wider federation. This applies on a per user basis to the attributes a user is entitled to and per organisation i.e. the attributes an organisation is prepared to expose to the wider federation.

6.4 NDG Role Mapping and Shibboleth

Given that organisations within a Shibboleth federation can allocate their own attributes. Service Provider Gatekeepers could still apply role mapping to attribute assertions from users of another organisation.

6.5 Shibboleth enable an NDG Attribute Authority

- ➔ The Attribute Authority would need an additional interface to support SAML based attribute queries

- ➔ Significantly, a Shibboleth Attribute Authority receives an Attribute query containing the user's session handle whereas an NDG Attribute Authority receives a user ID in the form of a signed request. The Shibboleth AA requires a link to it's IdP so that it can match up the user session handle to the user's identity held in the IdPs authentication log. Likewise an NDG AA would require a link to login / Session Manager to enable a link between user identity and user session handle.

6.6 Session Manager and Gatekeeper Considerations

Shibboleth allows for a pull model where a Service Provider may request a user's attributes from their IdP Attribute Authority. NDG Security could adopt the same approach or retain its existing model of pulling attributes from a users CredentialWallet held by a Session Manager.