UK Access Management Federation for Education and Research

Federation Technical Specifications

Ian A. Young

6 October 2006

DRAFT Version 0.7
ND/ATG/AAI/DOC/016

1 Introduction

This document specifies the detailed technical architecture of the UK Access Management Federation for Education and Research.

Where appropriate, this document also describes the rationale behind the particular choices made. Paragraphs describing rationale are formatted in this way.

A companion document, the *Technical Recommendations for Participants* ([UKTRP]), provides specific technical recommendations for members of the federation based on these specifications.

1.1 Keeping Up To Date

Due to the rapidly changing nature of the software and standards associated with identity technologies, it will be necessary to update this document frequently to reflect new developments. The latest version of this document can always be found on the federation web site (see [UKFTS]); federation members should review the latest version of this document periodically and in any case whenever a new deployment is contemplated.

New editions of this and other federation technical documents, as well as other announcements thought to be relevant to federation members, are reported on the federation mailing list. The technical and administrative contacts listed for all entities registered with the federation are made members of the mailing list automatically; other addresses can be added to the list by request.

1.2 Document Status

This document is an early review copy for the purposes of the consultation exercise and will evolve to include material on federation metadata generation and signature, as well as definitions of the federation's definitions for particular metadata elements.

2 Trust Fabric

The underlying trust fabric for the federation is based on PKI technology, which enables mutual authentication between IdP and SP servers and user browsers. This is based on use of the SSL/TLS protocol and XML digital signatures using keys contained in X.509 certificates, conventionally obtained from independent Certification Authorities (CAs).

An alternative approach, supported in Shibboleth 1.3 onwards, is to dispense with CAs altogether and simply to bind keys asserted by members directly to Shibboleth entities by including these public keys in the federation metadata. In effect, the Federation Provider assumes the role of CA.

This approach may in time become accepted as a method conferring a degree of assurance similar to that given by conventional certification. For the foreseeable future, however, the federation requires members to obtain X.509 certificates from one of a specified group of conventional CAs. The current list of acceptable certificate products is described in [UKTRP]; the process by which new CAs and CA products are validated and accepted into the federation's trust fabric is described in [UKPROC].

At a technical level, switching from a PKI trust fabric to a 'direct key' mode would require all federation members to be capable of operating on the basis of keys embedded directly in the metadata. This mode of operation is supported by Shibboleth 1.3 and later, and by Guanxi, but not by earlier versions of Shibboleth or by current versions of AthensIM. At present, therefore, the federation membership appears too heterogeneous to allow for a purely direct key regime.

The second issue with a pure direct key trust fabric is that the federation operator can no longer rely on the verified procedures of the CA to take some of the load of identity proofing for entities. This increases the federation operator's costs. Against this must be balanced the costs of verifying the CA's own procedures and tracking technical changes in the CA's certificate product offerings over time. This trade-off changes as the size of the federation increases: at larger scales, it is more cost-effective to 'outsource' institutional identity proofing by qualifying commercial CAs than it is for the federation operator to perform the same work.

As an alternative to requiring that either the CA-based or the direct key scheme is used exclusively, it may be possible to reach a compromise between the two pure schemes by implementing one of a range of hybrid models, in which both direct keys and CAs play their part. Such a hybrid trust fabric can combine the performance and other benefits of the direct key approach with the external identity proofing advantages of PKI using commercial CAs, and could be operated without interruption during a transition phase from one scheme to the other. Additional work is still required, however, to determine whether a hybrid approach would be appropriate for the federation.

A move towards a hybrid trust fabric is likely to be required in any case in order to support some features of SAML 2.0, such as signing and encryption of SAML messages.

The use of commercial CAs is not a perfect solution. Their registration procedures are not fully transparent and are subject to change without notice. Further, each new certificate product proposed for use in the federation has to be tested for the rigour of its enrolment procedure and for its technical compatibility with Shibboleth, both of which are time-consuming tasks.

In the Server Certificate Service (SCS) under development within TERENA, the national academic operator in each country acts as Registration Authority (RA), and communicates certification requests to a single commercial CA. (In the UK, the RA is UKERNA.) This offers several advantages over the use of commercial CAs:

- the CA is acting according to service requirements set by the academic community;
- the cost to institutions is lower, and billing is simpler;
- the RAs already have a trust relationship with the client institutions.

3 References

[ShibProt] S. Cantor et al. *Shibboleth Architecture: Protocols and Profiles.* Internet2-MACE, September 2005. Document ID internet2-mace-shibboleth-archprotocols. See http://shibboleth.internet2.edu/shibboleth-documents.html

[UKFTS] *UK Access Management Federation for Education and Research: Federation Technical Specifications.* Document ID ND/ATG/AAI/DOC/016; this document. See http://www.ukfederation.org.uk/

[UKPROC] *UK Access Management Federation for Education and Research: Procedures.* Document ID ND/ATG/AAI/DOC/019. See http://www.ukfederation.org.uk/

[UKTRP] *UK Access Management Federation for Education and Research: Technical Recommendations for Participants.* Document ID ND/ATG/AAI/DOC/015. See http://www.ukfederation.org.uk/ ND/ATG/AAI/DOC/015