Trust framework for participation of UK schools within the *UK Access Management Federation for Education and Research*

Frances Burton
23 February 2010
V1.1

Introduction

This paper sets out the trust framework for the adoption of Federated Access Management (FAM) in the UK Schools sector through participation in the UK Access Management Federation for Education and Research (UK federation).

The UK federation trust fabric is based on the ability of an end-user organisation to make true statements about their users. Each education institution and participating Service Provider (SP) is required to join the UK federation by signing up to its Rules of Membership[1].

To reinforce this trust fabric the UK federation makes use of a domain name, registered to the member, to form the basis of a scope used in the eduPersonScopedAffiliation attribute asserted for each user. This domain name is chosen because it is both unique and controlled by the registering party[2].

It is recognised, however, that it would be impractical for every Government funded school in the UK to join the UK federation and the need to find a suitable trust model in this sector was identified. As described in the following sections, the close legal links between Local Authorities (LAs), Regional Broadband Consortia (RBCs) and schools in their areas allow LAs and RBCs to make statements on behalf of those schools while preserving the required level of trust. This means that schools neither have to join the UK federation nor have to have a domain name they own asserted in any Identity Provider service (IdP).

Development of a synthetic scope

As each school is able to procure content and services for itself, a need was identified for SPs to recognise individual schools within an IdP. There has been some work to define a synthetic scope for use in the UK schools sector and further information can be found from the UK federation website. http://www.ukfederation.org.uk/library/uploads/Documents/proposal-for-synthetic-schools-scope.pdf

School to Local Authority link

The link between a Local Authority (LA) with a remit for education and the schools in their area is established via the Education Act 1996[3]. It was noted that, under the Act, the provision of education within the area was the responsibility of the Local Authority, thereby establishing a clear responsibility for schools. In addition it was also noted that under the Children's Act 2004[4] the LA has to appoint a Director of Children's Services who "...has

---

[1] UK Access Management Federation Rules of Membership:
http://www.ukfederation.org.uk/library/uploads/Documents/rules-of-membership.pdf

[2] UK Access Management Federation for Education and Research Technical Recommendations for Participants:
http://www.ukfederation.org.uk/library/uploads/Documents/technical-recommendations-for-participants.pdf

[3] Education Act 1996; http://www.opsi.gov.uk/ACTS/acts1996/ukpga_19960056_en_1

[4] Children Act 2004: http://www.opsi.gov.uk/acts/acts2004/ukpga_20040031_en_1

direct responsibility for local authority functions relating to the education and social care of children and young people."(DCSF 2009) [5]

Having established this link it was agreed that, in the context of the UK federation, local authorities would be regarded as End-user Organisations and able to make statements about the users within their remit.

Local Authority to Regional Broadband Consortium link
Regional Broadband Consortia are viewed as aggregators of local authorities and are made up of representatives from the LAs in a given geographical region. They have a very clear remit to act on behalf of these LAs in the provision of services to the region and receive funding from the Harnessing Technology Grant[6] directly from these LAs. Therefore, as agents of the LAs, the RBCs were considered able to make statements on behalf of the users within each of their member authority areas.

In order to preserve the trust fabric in this model, RBCs will only be allowed to hold information in their IdP for those users located within their member LAs.

Outsourcing arrangements
Those eligible to register an identity Provider (IdP) in the UK federation are able to outsource their provision to a third party provider[7], where upon, both the third party provider and the end user organisation are required to join the UK federation.

Given the relationship established between the LA and their RBC it was agreed that, for the purposes of participating in the UK federation, the RBC is viewed as the End User Organisation the LA would not have to join the UK federation and formally outsource its identity provision to the RBC.

If an LA would like to take advantage of identity provision from another RBC area, they will be required to join the UK federation in their own right and formally outsource their provision to the third party provider.

Devolved administrations
The devolved administrations of Scotland, Northern Ireland and Wales are treated as RBCs in this model. They are therefore able to utilise the synthetic scope to identify individual schools and provision has been made for some flexibility in the scope so that it may be adapted for each country's school identifier system.

LAs that opt out of RBC provision
If a Local Authority decides to opt-out of the RBC provision, or if there is no RBC to offer that provision, they will have to join the UK federation in their own right in order to participate.

Independent schools
Independent schools currently fall outside the eligibility framework for the UK federation but may be granted membership on a trial basis pending the release of a charging and eligibility

---

[5] DCSF Statutory Guidance, Roles and Responsibilities of the Lead Member for Children's Services and the Director of Children's Services: http://publications.everychildmatters.gov.uk/eOrderingDownload/Roles-and-Responsibilities.pdf

[6] Harnessing Technology funding 2009-10: Guidance for local authorities: http://publications.becta.org.uk/display.cfm?resID=39756

[7] Using an Outsourced Provider: http://www.ukfederation.org.uk/content/Documents/OutsourcedIdP

framework. If granted trial membership status they will be permitted either to implement their own IdP or to outsource provision to another member.