Certification and Trust between Assessment Stakeholders in ePortfolios: Literature Search

Robert Blowers
Electronics and Computer Science, University of Southampton
rwb104@ecs.soton.ac.uk

1. Introduction

This Literature Search focuses on topics related to the authentication of certified assessment objects within ePortfolios, starting with a review of the research into the development of interoperable ePortfolio frameworks. This highlights current gaps within the current research for services related to certified assessment, also known as e-certification. Existing security techniques, such as Digital Signatures and Public Key Infrastructure are then explored to understand how they could be used within an ePortfolio framework to authenticate and build trust between the certified assessment stakeholders.

2. Current ePortfolio Research

Background knowledge of what ePortfolios are and domain terminology was found in [1] and [2]. An ePortfolio is best summarized as "*a purposeful selection of evidence by the learner at a point in time, with an audience in mind*" and facilitates lifelong learning by providing this evidence at transition points in a learner's career (i.e. FE to HE) [1].

As highlighted by an Association for Learning Technology conference, "*ePortfolio technologies and practices are very new*". "*National agencies [drive] innovation in the UK*", such as the Joint Information Systems Committee (JISC), funding projects that develop frameworks utilizing interoperability specifications such as ePortfolio or Learner Information Profile (LIP) from IMS [3, 4]. Two such projects are the RIPPLL [5] and the ePortfolio Reference Model [6].

These projects defined use cases and services of how ePortfolios can be utilized during transitions. For example a learner could "*draw material from her ePortfolio to assert how she meets a course requirement*" when applying for HE via UCAS [6]. These assertions are then linked so some "*authenticated evidence*" within the ePortfolio [6]. Three generic stakeholders can be defined in this use case, the ePortfolio Owner, the Assessor who generates an authenticated artifact, and the Reviewer who verifies the artifact [7]. Unfortunately the means by which an assessor can certify an artifact are not discussed within these projects.

3. XML Security Technologies

One solution to "*maintain the credibility of learning artifacts*" is given by [7]. As most ePortfolio describe metadata in XML [7] suggests using a signed hash of the XML data in order to show that the artifact hasn't changed once it had been exported from the ePortfolio system.

Background information to digests and signatures was found in [8] and for details of XML and XML security technologies [9] and [10] were consulted. Greater detail into XML Digital Signatures was found in [11], as it described how the signatures could be inserted into XML documents in a variety of methods, from including the signature within the XML structure to the signature enveloping the entire XML document.

This can then be extended, as shown in [12], to apply to certain elements of the XML document, which paves the way for Contact Extraction Signatures. They ease privacy concerns by "*enabling selective disclosure of verifiable content*". The paper discusses a concrete example of how they could be utilized during interactions between "*a university, a student and a prospective employer"* when submitting an academic transcript, almost identical to the e-certification use cases discussed above [12].

Another paper that has parallels with the problem being addressed is [13], where secure XML document containers are formed for e-Government for "*secure contracting"* [13]. Within these document containers contract information is stored which must be "*protected against unauthorized manipulation*", exactly like the certified assertions in ePortfolio [13]. A signature block is defined "*to authenticate the responsible parties*" whenever changes are made to the container [13].

A development of this could be to store an assertion token with the ePortfolio XML document to say that it has been certified by an assessment body. SAML (Security Assertion Markup Language) by the OASIS committee "*defines a framework for exchanging security information"* in this manner [14]. An overview of SAML can be found within the specification, but is also given within [15]. SAML introduces two roles; an Asserting Party (AP), "*who can generate signed assertions*" and a Relying Party (RP) "*who wants to verify the validity of the assertion"* [15]. In the e-Certification use case the AP would be the certifying authority and the RP would be the reviewer of the ePortfolio. As SAML is extensible framework it could be extended to create a profile for use within e-Certification.

4. Forming Stakeholder Trust

As the SAML specification highlights the previous XML security technologies rely on "*a pre-existing trust relationship which typically relies on a Public Key Infrastructure (PKI)"* in order to trust any of the signatures used [14]. A good background to public key encryption and PKI is given within [8] explaining how PKI is used to certify public keys. This is very important to e-Certification as without a model of trust between the stakeholders it would be impossible to generate certified artifacts.

Typically a PKI infrastructure is constructed using a hierarchical model with a root Certificate Authority; however [16] also discusses other possible models, such as a bridge model that would allow for interoperability between different infrastructure models. This is taken further by [17] who also considers "*anarchy"* models such as PGP (Pretty Good Privacy) were there are no Certificate Authorities but instead one forms a chain of trust from a small community of friends.

The complexities of PKI can be reduced if a Federated Identity system is used which "*relaxes the dependence on PKI for user authentication*" shown in [18]. A federated system brings a group of trusting organizations together and "*enable sharing of user identity amongst themselves*" [18]. Such a system is already being deployed within the UK educational sector, Shibboleth, and has been used to provide a Single Sign On solution for ePortfolio projects [5]. Systems like Shibboleth place confidence in the robustness of member organizations authentication methods [19]. Shibboleth is based on the SAML framework discussed earlier, but uses the signed assertions to confirm a users' identity [18].

5. Summary

This literature search reviews the current research into ePortfolios and has highlighted a gap in the literature relating to e-Certification. Technologies that could be utilized to address the e-Certification use case are put forward, such as XML digital signatures and the SAML framework. PKI and Federated Identity are suggested as possible methods of engineering trust between the stakeholders, which is essential in order to attach value to the signatures used to certify ePortfolio artifacts.

References

[1] E. Hartnell-Young, C. Harrision, C. Crook, R. Pemberton, G. Joyes, T. Fisher, and L. Davies, "The impact of e-portfolios on learning", BECTA, Coventry 2007.

[2] S. Grant, "Clear e-portfolio definitions: a prerequisite for effective interoperability." in *ePortfolio Conference* Cambridge, 2005.

[3] G. Roberts, W. Aalderink, J. Cook, M. Feijen, and J. Harvey, "Reflective Learning, future thinking: digital repositories, e-portfolios, informal learning and ubiquitous computing", in *ALT/SURF/ILTA Spring Conference* Dublin, 2005.

[4] IMS Global, "IMS ePortfolio Best Practice and Implementation Guide", visited on 28 Nov 2007 at http://www.imsglobal.org/ep/epv1p0/imsep_bestv1p0.html

[5] E. Hartnell-Young, A. Smallwood, S. Kingston, and P. Harley, "Joining up the episodes of lifelong learning: A regional transition project", *British Journal of Educational Technology,* vol. 37, 2006.

[6] P. Rees Jones, "Specifying an ePortfolio: a Personal View", CETIS / JISC, Nottingham 2006.

[7] N. Carroll and R. Calvo, "Certified Assessment Artifacts for ePortfolios", in *International Conference on Information Technology and Applications* Sydney: IEEE, 2006.

[11] L. Sun and L. Yan, "XML Undeniable Signatures", in *International Conference on Intelligent Agents, Web Technologies and Internet Commerce* Vienna: IEEE, 2005.

[12] L. Bull, P. Stankski, and D. McG. Squire, "Content Extraction Signatures using XML Digital Signatures and Custom Transforms On-Demand", in *The Twelfth International World Wide Web Conference* Budapest, 2003.

[13] M. Greunz, B. Schopp, and J. Haes, "Integrating e-government infrastructures through secure XML document containers", in *34th Hawaii International Conference on System Sciences* Hawaii: IEEE, 2001.

[14] H. Lockhart, T. Wisniewski, S. Cantor, and P. Mishra, "Security Assertion Markup Language (SAML) V2.0 Technical Overview", OASIS 2006.

[15] S. Saclike, "Next Steps for Security Assertion Markup Language (SAML)", in *ACM Workshop on Secure Web Services*, Fairfax, Virginia, 2007.

[16] Z. Guo, T. Okuyama, and M. Finley, "A New Trust Model for PKI Interoperability", in *International Conference on Networking and Services* Papeete: IEEE, 2005.

[17] R. Perlman, "An overview of PKI trust models", *IEEE Network,* vol. 13, 1999.

[18] A. Bhargav-Spantzel, A. Squicciarini, and E. Bertino, "Establishing and protecting digital identity in federation systems", *Journal of Computer Security,* vol. 14, 2006.

[19] JISC, "Shibboleth: Connecting People To Resources", visited on 29 Nov 2007 at http://www.jisc.ac.uk/media/documents/publications/shibbolethbpv2.pdf

Bibliography

[8] A. Tanenbaum, *Computer Networks*. London: Pearson Education, 2003.

[9] C. F. Goldfarb and P. Prescod, *The XML handbook*, 2nd ed. Upper Saddle River, N.J.: Prentice Hall, 2000.

[10] E. Simon, P. Madsen, and C. Adams, "An Introduction to XML Digital Signatures", visited on 26 Nov 2007 at http://www.xml.com/pub/a/2001/08/08/xmldsig.html