Open Authentication Systems For The Web

Abstract

The rapid growth in Internet services has led to a demand for scaleable authentication systems to restrict access to licensed services (such as bibliographical services, databases, etc.) to authorised users. An increasing number of proprietary applications which provide authentication services are available. However such applications may only provide an interim solution, until authentication services based on open protocols are available. This article reviews developments to such open authentication protocols.

Background

The World Wide Web became popular during the mid 1990s as a means of accessing freely-available information on the Internet. As the Web grew in popularity and sophistication it began to be used to provide information within closed communities such as members of an organisation (the term *Intranet* was coined to describe this type of usage) and restricted access to resources within closed communities (sometimes the term term *Extranet* is used in this context).

Initially access was restricted using the web server's authentication system based on usernames and passwords. However, as anyone who has had difficulties in remembering their PIN number for ATMs, burglar alarms, mobile phones, etc. will know, this is not a scaleable solution as there is a limit to the number of username and password combinations people will be prepared to memorise.

Solutions such as restricting access based on the computer's IP number also have limitations. The use of IP numbers as a means of authentication is likely to become more difficult in the light of developments such as increased use of proxy servers and dynamic IP allocation and the dangers of "*IP spoofing*".

A third way of managing access to resources is through the use of third-party proprietary applications. A wide range of products, such as **iland's** *Password Protection Web Software* [1], and **Banyan's** *SiteMinder* [2] and *Intranet Protect* [3] are available. Many of these products have been developed for the Intranet. A more ambitious attempt has been made in **Athens** [4]. Athens has been developed by NISS as a means of providing a unified authentication system to nationally provided data sets using a system based on the Sybase database software.

However the use of proprietary applications to provide authentication services have a number of limitations:

- They are often restricted to authenticating *users* and cannot be used for authentication of the *service* or *software*.
- Being based on a proprietary application, rather than open protocols, they can lock the user into the application vendor, with the inherent dangers of changes in licensing arrangements, company takeovers, etc.
- They may fail to provide richer functionality provided by products developed in a wider marketplace.

This paper reviews the use of open systems based on *digital signatures*, *certificates* and *certification authorities* for providing a range of authentication services.

Authentication Examples

Let us begin by describing a variety of examples in which some form of authentication is required within the UK Higher Education Community.

1. **Authentication of the sender of an email message**: for example an email message is sent apparently from a lecturer saying that lectures have been cancelled.
2. **Authentication of mobile code**: for example a distributed teaching and learning application has been developed using ActiveX (or Java). The code needs to be authenticated to prevent the display of unnecessary dialogue boxes warning of the dangers of running software from untrusted sources.
3. **Authenticated access to Intranet resources**: for example restricting access to resources to members of staff, who may be using browsers in a variety of locations, such as the office, at home, at a conference at a cyber café, etc.
4. **Authenticated access to Extranet resources**: for example restricting access to confidential minutes to members of a national group.
5. **Authenticated access to mailing list archives**: for example restricting access to Mailbase list archives to the list members using both Web access to the Web archives and email access using email protocols such as IMAP.
6. **Authenticated access to licensed resources**: for example restricting access to licensed datasets.

As can be seen from the last three examples, *authentication* is closely related to *authorisation*. In addition authentication is closely related to *encryption*.

What Is A Digital Signature?

A **digital signature** is a encrypted digest of an electronic document - if the cryptographic and digest functions are properly designed, and one is sure of the veracity of a public key, then one can be sure that the document can only have been originated by the owner of the matching private key. As with a letter written on paper, a signature verifies to a recipient that the contents must have originated with the sender - and if that signature has been widely used by the owner, it is very hard for that sender to deny the signature (at least without casting all the other documents signed into doubt).

For a letter or email designed to be read by a specific human, a signature is all that is required - the meaning of the document is generally clear. However, where a document should be processed by a third party - which in the case of an electronic document may be a computer program - with the intention that the third will may grant the recipient some service, we use a specific kind of signed document: a certificate.

A **certificate** is an authenticated document which uses a standard layout understood by all interested parties, and which will usually make some statement about the identity of the holder, and what services are available; usually this is a device for permitting information about a contract of some sort (though the certificate need not be - and usually is not - the actual contract document itself).

Think about a motor insurance certificate - it is separate from the policy, and its purpose is to demonstrate to a police officer or the post office clerk who issues the tax discs that one possesses appropriate insurance. Generally any form that we submit (the word "form" implies the standardised document structure) with a signature or other authenticator is a certificate.

Digital Signature Protocols

It may be useful to compare electronic documents (and concepts such as signatures and certificates) with their paper counterparts that we use in everyday life. Unfortunately computer bits and bytes are much easier to forge than pen strokes, seals and the various other authenticators which have evolved over the past few centuries, along with the laws and regulations which give them legal force. The description of signatures above glosses over an important point - once you are sure that the document has been satisfactorily signed how can you be sure that the key used genuinely belongs to the sender. It is very easy to duplicate a signature with all the human readable details apparently identical. How can a human check that the key - a very long random number - is the correct very long random number?

As long as communications only occurs electronically using an untrusted network such as the Internet - one can't, so "out of band" contact is required. This usually means that the key (or a more manageable form of key "fingerprint") is distributed by a more trustworthy means. In practice, this frequently means on a piece of paper which can't itself be easily forged. My PGP key fingerprint is printed on the back of my business card. Whenever I give out my email address, I also give out evidence which the other party can use to check if PGP signed email which they receive in future really is from me (or at least that bloke they met some time ago). In the case of a Web service, one can publish the key in the mass media. A number of organisations use the classified ads section of national newspapers for their public key fingerprints.

But what if I want to exchange email and perform secure Web transactions with people I have never met? All practical digital signature protocols permit the idea of a trusted third party (or **certificate authority**) - whom one trusts to provide evidence (in the form of a specific kind of digital certificate) that a key really does belong to the genuine holder. This, however, does introduce a couple of other problems: first it's a bit too powerful - if one extends a signature chain to more than two links, the usefulness degrades quickly (the play "Six Degrees of Separation" is based on the widely quoted statement that every person in the world is no more than six steps of acquaintanceship away from every other). Second - even when there is only one third party certificate the key, one must be very sure about exactly what is being certified. As a member of University staff, I'd be happy to sign a student's PGP key on production of their university ID card. This does not mean that I would regard that student as particularly trustworthy, and I'm certainly not making any such recommendation. This has been neatly summed up by a US commentator: "I trust Mom, and Mom trusts the President, but this does not mean that I trust the President".

The X.509 standard is used for certificates in the SSL (Secure Sockets Layer) protocol now supported by most Web clients and servers. It supports certificate authorities - this is how the browser's padlock icon knows whether to be open or closed. The keys of various well-known CAs are distributed along with the browser itself, and as long as an SSL secured Web server has a server certificate signed by one of these CAs, the browser happily displays a secure icon and - assuming that one's Web browser installation comes from a reputable source, one has verified the identity of the certificate, and the organisation so authenticated appears reputable, sending one's credit card number is probably more secure than dictating it down a phone line or letting a waiter disappear into the kitchen with it.

However just because SSL and X.509 certificates allow us to perform Internet shopping with some degree of security does not mean that they are limited only to services which have certificates signed by well known CAs. A closed user group can issue its own certificate and be its own certificate authority if appropriate. Browsers

will support this - though they will not by default trust certificates which are not signed by a well known CA, they can be given the details of the local CA and told to trust server certificate it signs. Banks issue their own bank cards and will usually honour bank cards from other banks (though usually offering less facilities to customers holding other banks cards than to their own). Similarly, airlines issue their own tickets which they will accept - but they are in a standard form that partner airlines will also accept and that all travel agents can issue.

Banks and airlines don't appear to require a common authentication agency - and as there's no point in trying to feed an airline ticket into a cash machine, this is not too much of a problem. Similarly if a group of service providers - such as libraries - wish to honour the passes of each other's readers (though maybe not to the extent that they would their own), then that's their business. The type of trust is highly dependent on the business model.

Further information on digital signatures, certificates and certifying authorities is given in RSA's FAQ about today's cryptography [5].

Support For Digital Signatures

We have given the background to digital signatures and outlined digital signature protocols. We will now review support for digital signatures provided by software companies.

Browser Support

Both Netscape and Microsoft provide support for digital signatures in their browsers. Figure 1 shows the interface used for viewing the digital signatures for the end user, certificate authorities and publishers.

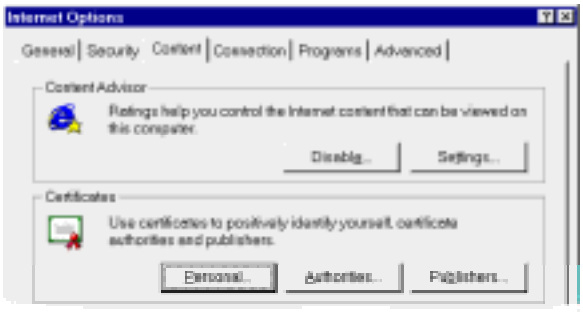

Figure 1 - Internet Explorer Provides Support For Digital Signatures

The interface illustrated in Figure 1 can be used to:

- Import and view a personal certificate.
- Choose the certification authorities you trust.
- Choose the "publishers" you trust. Information, such as software, from these trusted publishers can be accessed without notification. Otherwise a dialogue box will typically be displayed.

Figure 2 illustrates how a browser processes a digital signature it receives from a Web server. In Figure 2 Netscape Communicator version 4 is used to access the Cranfield University Web site [6] on a port running SSL.

Figure 2 - Accessing a Web Site Which Provides A Certificate

When this site is accessed the browser will normally display a series of dialogue boxes which provide information about the site, as illustrated in Figure 3.

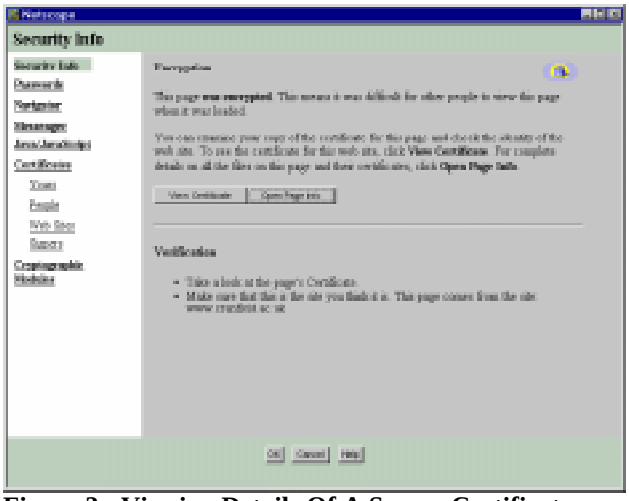

Figure 3 - Viewing Details Of A Server Certificate

This information can also be viewed by clicking on the padlock in the bottom left-hand corner of the browser window, or by choosing the appropriate menu option.

Email Support

In addition to support by the current generation of mainstream Web browsers, an increasing number of email clients provide support for digital signatures, such as Microsoft's Outlook Express. Figure 3 illustrates how Outlook Express displays a message which contains a digital signature.

Figure 4 - Outlook Express Recognises Digital Signatures

Server Support

Server support for digital signatures is provided by server software such as Apache and Microsoft's IIS.

SSL (Secure Sockets Layer) [7] has been developed by Netscape for managing the security of message transmissions in a network. Netscape has offered SSL as a proposed standard protocol to the World Wide Web Consortium and the Internet Engineering Task Force as a standard security approach for Web browsers and servers.

Apache uses the mod-SSL server module which is built using SSLeay (a free implementation of SSL) to provide support for digital signatures. As described in the SSLeay FAQ "*SSLeay is a free implementation of Netscape's Secure Socket Layer - the software encryption protocol behind the Netscape Secure Server and the Netscape Navigator Browser*" [8]. **Apache-SSL** is secure Web server software, based on Apache and SSLeay [9]. Digital certificates are available for Apache-SSL from a number of companies including Thawte Consulting, CertiSign Certificadora Digital Ltda, IKS GmbH, Uptime Commerce Ltd, BelSign NV/SA, Verisign, TC TrustCenter (Germany) and NLsign BV.

Microsoft provide support for certificates with their **Certificate Server.** As described in the *Certificate Server White Paper* [10] the software can be used to implement an Extranet for use, for example, by current and former employees of an organisation. It is possible to set up Certificate Authorities and to distribute CA root certificates to end users. Certificate Server provides a group of administration tools for configuring, monitoring and controlling the operations of the server.

Certification Companies

Commercial companies such as **Verisign** [11], BT's **TrustWise** [12] and **Thawte** [13] have been set up from which a variety of signatures can be obtained. Although the licensing arrangements are liable to change, currently personal certificates can be obtained free of charge and server certificates can be obtained for a small fee.

Figure 5 - Verisign Home Page

An additional example of how authentication software based on open standards is becoming increasingly pervasive can be seen from the review of PKI (Public Key Infrastructure) software in *Secure Computing* [14]. Software included in the review included **Blueprint** by PC Security Ltd [15], **Entrust/PKI** by Entrust Technologies Ltd [16], **Notary** by Entegrity Solutions [17] and **UniCERT** by Baltimore [18].

Political Developments

The growth in electronic commerce is being accompanied by a range of political initiatives. The European Commission has published a policy paper entitled *Towards a European Framework for Digital Signatures And Encryption* [19]. This paper aims to ensure that EU countries establish a common framework for digital signatures, cryptographic services and products in order to enable users in all economic sectors to benefit from the opportunities of the global information society. An example of the commitment to Digital Signatures within the European Commission can be seen from the *Call for a Certification Service Provider for electronic signatures for the Community Research Programmes open procedure* [20].

In the UK the Department of Trade and Industry published a briefing paper in July 1998 which included brief details on UK policy for *Encryption and Digital Signature* [21]. The Briefing Paper described that work is now underway to prepare the Secure Electronic Communications (SEC) Bill. In October 1998 Barbara Roche MP announced the UK government's statement on electronic commerce [22]. The paper on *Net Benefit: The*

Electronic Commerce Agenda For The UK informed us that:

The UK Government proposes to introduce legislation to license (on a voluntary basis) organisations providing cryptography keys. This legislation will set standards for certification and guarantee legal recognition to electronic transactions facilitated by electronic signatures.

As well as European and UK initiatives, there have also recently been a number of international meetings at government level which have addressed policy issues. The OECD (Organisation for Economic Cooperation and Development) held a ministerial meeting in Ottawa in October 1998. The meeting addressed the theme of dismantling barriers to global electronic commerce. Topics covered at the meeting included data protection and privacy, taxation and authentication. Background reports prepared for the Ottawa Ministerial Conference included *Inventory of Controls on Cryptography Technologies* [23] and *Inventory of Approaches to Authentication and Certification in a Global Networked Society* [24].

The Conference produced a number of outcomes, as described in the *Ottawa Conference Report* [25]. The Conference Action plan [26] stated that "*The OECD will facilitate the exchange of information and experiences in the areas of authentication and certification in the context of global electronic commerce*".

Futures

This paper has given an overview of digital signature technologies and reviewed developments of support for digital signatures in client software (such as Web browsers and email programs) and in Web servers. The paper has described how certification authorities are needed in order to provide a trust mechanism. But how is deployment of digital signatures to be achieved?

We are already seeing commercial developments, such as free email from companies such as HotMail [27] and free Internet access from Freeserve [28], which are beginning to have an impact on services provided by Universities.

In the light of stories in the press speculating on the Government providing digital signatures for all British citizens, and interest in authentication being shown by the Post Office, BT and a number of banks. Will authentication within UK Universities be provided by a commercial vendor, or should we set up our own infrastructure? As Ton Verschuren describes in a paper on *Smart Access: Strong Authentication on the Web* presented at the ISOC Conference 1998 [29] "*SURFnet* [the Dutch equivalent of UKERNA] *could, in its role as National Research Network, authenticate its customers (students and staff) on behalf of information providers belonging to its constituency.*" SURFNet is currently running a project is to develop such an authentication service.

In the US the University of California Common Authentication Project (UCCAP) [30] proposes a certificate-based solution to authentication. The project has an ambitious aim of including everyone associated with the University of California.

Within the UK HE community these questions are being addressed by JTAP (JISC Technology Application Programme). The JISC Circular 14/98 [31] announced that it wished:

"*to fund studies to identify appropriate protocols and to test deployment [of Digital Signatures]. We are seeking to fund an overview report at a cost of £5k and a technology deployment pilot ...*"

and, under the heading of *Certificate Based Infrastructure Services*:

"*.. require more work of a technical overview and pilot nature. Current developments need to be set in a broader context. We are seeking to fund an overview and technology watch project at a cost of £25,000, followed by one or two deployment pilots ...*"

We await the results of these reports and pilot studies with eager anticipation.

References

1. *Password Protection Web Software*, iland <URL: http://www.iland.com/secure/>
2. *SiteMinder*, Banyan <URL: http://www.banyan.com/products/siteminder/>
3. *Intranet Protect*, Banyan <URL: http://www.banyan.com/products/intranet.protect.html >
4. *Athens*, Home page <URL: http://www.athens.ac.uk/>
5. *RSA Laboratories' Frequently Asked Questions About Today's Cryptography*, RSA <URL: http://www.rsa.com/rsalabs/faq/html/questions.html>
6. *Cranfield University*, University Entry Point <URL: https://www.cranfield.ac.uk/>
7. *SSL*, whatis.com, <URL: http://www.whatis.com/ssl.htm>
8. *SSLeay and SSLapps FAQ*, Web FAQ <URL: http://www.psy.uq.oz.au/~ftp/Crypto/>
9. *Apache-SSL*, Organisational Entry Point <URL: http://www.apache-ssl.org/>
10. *Certificate Server White Paper*, Microsoft <URL: http://www.microsoft.com/workshop/security/client/certsvr.asp>

11. *Verisign*, Organisational Entry Point <URL: http://www.verisign.com/>
12. *Trustwise*, Organisational Entry Point <URL: http://www.trustwise.com/>
13. *Thawte*, Organisational Entry Point <URL: http://www.thawte.com/>
14. *Secure Computing*, March 1999, West Cost Publishing <URL: http://www.westcoast.com/>
15. *Blueprint*, PCSL <URL: http://www.pcsl-europe.com/>
16. *Entrust/PKI*, Entrust Technologies Ltd <URL: http://www.entrust.com/>
17. *Notary*, Entegrity Solutions <URL: http://www.entegrety.com/>
18. *UniCERT*, Baltimore <URL: http://www.baltimore.com/>
19. *Towards A European Framework for Digital Signatures And Encryption*, European Commission, Directorate-General XIII, <URL: http://www.ispo.cec.be/eif/policy/97503toc.html>
20. *Call for a Certification Service Provider for electronic signatures for the Community Research Programmes open procedure*, European Commission, <URL: http://www.cordis.lu/fifth/src/call-cer.htm>
21. *Encryption and Digital Signatures*, DTI, <URL: http://www.dti.gov.uk/eurobrief/3encrypt.htm>
22. *NetBenefit: The Electronic Commerce Agenda for the UK*, DTI, <URL: http://www.dti.gov.uk/cii/ecom.htm>
23. *Inventory of Controls on Cryptography Technologies*, OECD Background Paper, <URL: http://www.oecd.org/dsti/sti/it/ec/prod/reg_4e.pdf>
24. *Inventory of Approaches to Authentication and Certification in a Global Networked Society*, OECD Background Paper, <URL: http://www.oecd.org/dsti/sti/it/ec/prod/reg_3e.pdf>
25. *OECD Conference Report*, OECD Conference, October 1998 <URL: http://www.oecd.org/dsti/sti/it/news/ottrepor.htm>
26. *OECD Action Plan for Electronic Commerce*, OECD Conference, October 1998 <URL: http://www.oecd.org/dsti/sti/it/ec/prod/sgec_9e.pdf>
27. *HotMail*, Web site <URL: http://www.hotmail.com/>
28. *Freeserve*, Web site <URL: http://www.freeserve.com/>
29. *Smart Access: Strong Authentication on the Web*, ISOC Conference 1998 <URL: http://www.isoc.org/inet98/proceedings/1a/1a_2.htm>
30. *UCCAP Working Details*, University of California, <URL: http://www.ucop.edu/irc/auth/work.html >
31. *JISC Circular 14/98*, JTAP, October 1998 <URL: http://www.jtap.ac.uk/bid/c14_98.html>

Contact Details

Brian Kelly
UK Web Focus
UKOLN
University of Bath
Bath BA2 3LY
Email: B.Kelly@ukoln.ac.uk
Tel: 01225 323943

Peter Lister
Computer Centre
Cranfield University
Beds
MK43 0AL
Email: P.Lister@cranfield.ac.uk
Tel: 01234 754200 ext. 2828