



The Government Gateway: the clients that work and why others do not..... yet

The Government Gateway has been designed to follow standards and allow people to use the computer system and browser of their choice. There is nothing proprietary in the design but given the need for people to be confident that they can trust their electronic communications with Government there are some stringent security requirements.

The process

To register with the Government Gateway and enrol for specific services requires the https protocol with 128-bit (or better) encryption. This guarantees the confidentiality of the process and enables the client to verify that they are communicating with the Government Gateway. But, it provides no authentication of the client to the Gateway.

Clients can authenticate to the Gateway in either of two ways:

- Using a password of the users choosing. (A user-id will then be sent in the post to an address already registered with Government).
- Presenting a digital certificate.

The second method is preferred (and required for some transactions) but is dependent on the client having commercially available PKI software already installed and the user obtaining an X.509 certificate. Currently, we only have arrangements with ChamberSign and Equifax. The Entrust and Equifax software equates to tScheme level 2.

The commercial package will typically generate the private/public key pair locally on the users PC and export the public key to the chosen certificate provider for incorporation in the users certificate. However, possession of a digital certificate does not authenticate you. You need to establish rights to a service and subsequently sign something to demonstrate that you are still in possession of the correct private key.

Technique employed

The technique currently used by the Gateway to authenticate the client is to request that an XML object be signed. The mechanism is as follows:

- The Gateway delivers an XML object to the client together with a signed Java applet and some JavaScript. The Java applet adds some envelope information to the XML object and then uses the API provided

by the PKI commercial package supplier to get the object signed. The applet then posts the object back to the gateway.

Constraints

The first difficulty is that although standards are followed in that Java applets are signed with X.509 certificates, the mechanism used to package and sign the applets is proprietary. For example, Microsoft use a cab file and sign it using MS Authenticode whereas Netscape use a jar file and sign it with NS Object signing technology. Consequently, separately packaged applets have to be created for each browser and each package has to be signed with a separate certificate (from Entrust).

The second difficulty is the availability of packages to manage certificates on platforms other than Microsoft Windows. Such packages also need to support APIs that can be called by Java applets.

So, where does this leave us?

Broadly, the consequences of the above is that:

- IE 4.01 and above works under Windows (95, NT4 or above) with ChamberSign certificates
- IE5.01 and above works under Windows (95, NT4 or above) with Equifax certificates (new 1 May 2001).
- Netscape 4.08 and above (but excluding Netscape 6) works under Windows (95, NT4 or above) with ChamberSign certificates. Netscape 6 is not supported yet.

Full details of browsers and operating systems that have been validated are given towards the end of this document.

The issue is not about being vendor neutral; rather it is a problem with the way standards are implemented by vendors and a lack of offerings to manage digital certificates.

Other browsers (running under Windows, Unix or Linux) can provide the required SSL connectivity but the ability to manage certificates on open source platforms needs investigating. The Office of the e-Envoy will be funding some activity by the open source community to address this issue.

The security model described above met the design objectives but if alternatives are proposed, they will be considered.

Currently, browsers that have not been validated are denied access to the Government Gateway home page; this will be relaxed shortly so that news about the Gateway, including information about newly supported browsers, can be viewed.

Browsers and Operating Systems that have been tested to date

As of 9 May 2001 the Government Gateway supports the following browser and platform combinations:

Hardware

- PC or Macintosh
- A working Internet connection

Software - PC Users

- Microsoft Windows (Windows 95 and above or Windows NT 4 and above)
- Internet browser. Either Microsoft Internet Explorer (v4.01 or later) or Netscape Navigator (v4.08 or later). Please note that if you have installed Netscape 6, you will be able to browse the Government Gateway site, but will only be able to register for services that require a User ID and Password (such as the PAYE End-of-Year Returns service). ChamberSign and Equifax certificates are not currently supported on version 6 of the Netscape browser.
- Your browser must have JavaScript and Cookies enabled, and be capable of supporting 128bit SSL.

Software - Apple Macintosh Users

- Mac OS version 7.5 or later
- Internet browser. Either Microsoft Internet Explorer (v5.0 or later) or Netscape Navigator (v4.08 or later). Please note that although you can access the Government Gateway web site with these browsers, ChamberSign and Equifax digital certificates are not supported on the Macintosh. Macintosh users can currently only register for Government services that require a User ID and Password, not services that require a digital certificate (such as the Electronic VAT Return or MAFF IACS Area Aid Application).
- Your browser must have JavaScript and Cookies enabled, and be capable of supporting 128bit SSL

Other operating systems and browsers will be tested as soon as possible; the most popular ones have been done first.

Some Statistics on Browser/OS Usage

Looking at a week of ukonline.gov.uk statistics shows a clear breakdown of operating systems and browser types/versions.

Figures are shown as a % of total hits (objects retrieved), of which there were 2.5 million in this period.

Browser and Version	%
lycos	0.001794
AltaVista	0.007401
Netscape Navigator 2	0.008747
Internet Explorer 2	0.03282
Internet Explorer 6	0.038726
Opera	0.114011
Netscape Navigator 6	0.223611
Others	0.291868
Internet Explorer 3	0.297401
MSPProxy	1.34092
Netscape Navigator 3	1.569839
Internet Explorer 4	7.750512
Netscape Navigator 4	11.51168
Not Specified ¹	12.63482
Internet Explorer 5	64.17584

Operating System	%
OS/2	0.003811
BSD	0.008743
SunOS	0.029518
Windows 3.1	0.096774
Linux	0.383509
Macintosh	1.437635
Windows 95	13.67136
Not Specified ²	21.73767
Windows NT ³	23.23808
Windows 98	39.3929

The most popular browsers are Internet Explorer 5 and Netscape 4. The most popular OS's are Win 98 and Win NT, closely followed by Win 95.

Linux falls well below Macintosh (which is supported).

¹ The information could not be collected; a proxy server probably removed it.

² As previous footnote.

³ Including Windows 2000

