Title: (ilab_blk.eps)
Creator: Adobe Illustrator(R)
8.0
Preview: This EPS picture
was not saved with a

How do I use Certificates on the WWW?

If you have used the web, you have probably already used certificates: secure web servers will send their certificate to your browser to prove who they are. Whenever you use an `https://` link, http-over-SSL will be invoked and certificate authentication takes place.

SSL (Secure Sockets Layer) is the protocol used by web browsers and servers to negotiate an encrypted connection. SSL was developed by Netscape for use with their web servers and web browsers. TLS (Transport Layer Security) is the IETF-standardized version of the protocol. There are very few differences between SSL version 3 (which is supported by all current versions of web browsers) and TLS, and some products support both. For simplicity, we'll refer to the family of both protocols (SSLv3 and TLS) as "SSL."

In SSL, certificates are used to authenticate the server to the client, and, optionally, to authenticate the client to the server. Before authentication begins, negotiation is used to establish what type of encryption and hashing will be used to protect the traffic on the connection. When the server is offered an acceptable encryption/protection algorithm it will send its certificate to the client. The client generates a random number to be used as a session encryption key, encrypts this session key using the server's public key found in the certificate, and sends it to the server. The server uses its private key to decrypt the session key, and now both sides of the connection have a shared session key that can be used for fast encryption.[1]

The most common authentication used today on the web with SSL is one-way authentication - a server sends its certificate to your browser to prove its identity. The server does not require authentication of you. However, SSL can be used with mutual authentication. In that case, your browser sends your personal certificate to the server to authenticate who you are. You don't have to type in a username and password, because your certificate does all that for you. Properly implemented, certificate-based authentication is both much more convenient for users, gives greater knowledge of who is on the other end than other types of authentication, and offers greater security. However, it does require users to have certificates---PKI---and web browsers to request those certificates.

The iLabs PKI demonstration area has several web servers:

`https://n1.pki.ilabs.interop.net/`	doesn't require browser certs
`https://L1.pki.ilabs.interop.net/sslinfo.php`	asks for browser certs
`https://w4.pki.ilabs.interop.net/`	requires browser certs
`https://n1.pki.ilabs.interop.net:8100/`	requires server admin certs (and will not communicate otherwise)

[1] The key exchange described in this paragraph is for the RSA protocol. DH/DSS is supported in SSLv3 and required in TLS. When using DH/DSS the key exchange is quite different. DH/DSS is virtually never used.

The demonstrations of PKI usage with web servers concentrate on built-in capabilities of web servers to accept and handle certificates. Some web servers, such as Microsoft's IIS, integrate the acceptance of certificates more tightly into existing user authentication databases. For example, when you authenticate with a certificate in Microsoft IIS, you can be mapped to an existing Windows user, and thus all file ACL (access control list) entries which refer to real users will apply to you.

For a cross-platform/multi-server example of user-based certificate authentication, see the SafeWord demonstration highlighted in a different white paper in the PKI iLabs.

No user authentication

Browse to `https://n1.ilabs.pki.interop.net.` If you are using Netscape, in the bottom left corner of the menu bar, you will see a padlock symbol. If the padlock is locked, then SSL is being used for the network connection. This means that at a minimum, the web server authenticated to your browser using a certificate, and the traffic over the network is encrypted.

Microsoft's Internet Explorer web browser does not have a consistent icon indicating a secure SSL connection. In any case, though, if the URL starts with `https://`, then you have asked for an SSL connection. Because you could have been redirected to another site, it is important that you check the status in your browser to see whether the page was encrypted or not. In Netscape, click on the Security icon in the icon bar at the top. This will let you examine the server certificate and the type of encryption used.

Optional user authentication

As part of SSL, a server may request or require you to authenticate. To see how this happens in our demonstration, go to one of the client systems and start up a new copy of the www browser to clear out any authentication information leftover. Browse to `https://L1.ilabs.pki.interop.net/sslinfo.php` (that's letter-el number-one.pki...). You will be prompted to identify yourself to the server by selecting a certificate which has been (previously) loaded into your browser, to send as proof of your identity. If you have configured your browser Security to require passwords, you will also be prompted with a password which is used to unlock (decrypt) the private key before you can authenticate yourself with the certificate. If you choose **Cancel** in the dialog box, you are refusing to send your certificate to the server. It may then decide to allow access without the certificate. It may refuse you entirely, or perhaps you will be not be allowed to browse some areas of the site. Try both options with `L1` - refuse to send the client certificate. Then you must exit Netscape to reset your choice for this page, and try again, this time sending the client certificate.

Required user authentication

Browse to `https://w4.pki.ilabs.interop.net` and send the user certificate. Now, exit the browser and try it again, and this time cancel out of sending the browser certificate. This web server is configured to only accept connections if the client authenticates to the server. You'll see an error dialog box from your browser because the connection to the web server could not be established.