Using server certificates factsheet

PB/INFO/069

Most users know vaguely that web addresses beginning **http://** and **https://** are different. An **https://** web site ('secure HTTP') provides users with some protection against some types of Internet threat (though both server and client computers have to do more work):

- communications between the browser and server are encrypted and cannot be read in transit by a third party
- there is some assurance of server identity: that the web site to which the user is passing information is the one they intended to visit.

So, for instance, sensitive information such as credit card numbers or passwords is relatively safe as it crosses the network, and it is possible to know with reasonable confidence the destination to which it has been sent. Note, however that although identity checks can detect simple web site impersonation they cannot prevent the use of similar-looking, but different, domain names: for instance, **www.example.com** [1] (using the letter 'l') and **www.examp1e.com** [2] (using the digit '1') could both have valid certificates.

Both encryption and identity checking require the owner of the server to obtain and install a digital certificate. For some types of certificate, the user may also need to perform manual checks or adjust their browser. This factsheet discusses the different types of **server certificate** and what each means for server and browser owners. Note that, although they use the same technology, the service certificates that are the subject of this factsheet are obtained and used differently from the identity certificates that are sometimes used to provide proof of identity of an individual.

Certificates, Keys and Signatures

A digital certificate contains a public encryption/signature key, an identity (for a server certificate, a DNS domain name), and the digital signature of a person or organisation who has checked the ownership of the key and the identity it claims. Any certificate can therefore be used to enable encryption; certificates differ in who signs the key and what checks they perform before signing it. It is left to the browser user to decide whether the checks give sufficient confidence that the identity and the key belong to the actual owner (different applications require different levels of confidence).

There are effectively three alternatives:

- The server owner may sign their own certificate. Such **self-signed** certificates give no independent verification of the identity of the server but this may not matter if all users are able to identify the server by other means (e.g. on an internal server only accessible from within a department's network). Indeed a self-signed certificate may be the best option where it is important for users or their computers to be able to identify a specific

server, rather than one of a number of servers with certificates issued by the same authority.

- The organisation that owns the server, or a parent or related organisation, may sign **organisational** certificates for servers within its area of interest. Since the organisation is vouching for the identity of each server and may affect its reputation by doing so, it should perform some checks (for example that the server is 'official' and that the person running it is an authorised member of the organisation) before it issues a certificate. For a server whose readers are mostly members of the organisation, this may be sufficient proof of identity. If an organisation issues certificates for publicly-visible servers then it should publish a description of its checks so that external users can make an informed decision on how much confidence they give.

- Some, usually **commercial**, organisations issue certificates as part of their business; these organisations also arrange that their certificates will be recognised automatically by all common browsers (see below). Most will sell a certificate to anyone subject to their identity checking processes, which may be different for each organisation; some offer different levels of certificate based on the checks done. Most require written proof of the ownership of the Internet domain and the customer's authority to acquire a certificate on the owner's behalf; there may be requirements for technical and organisational measures to prevent misuse of the certificate. Extended Validation (EV) certificates (see Guidelines for EV certificates [3]) require additional checks of the legal and physical existence of the customer organisation and its representatives. Commercial certificate providers should publish details of these checks.

What is the Effect on the Browser?

When a browser visits an **https://** web site, the use of encryption is indicated by an icon, often a padlock. Depending on the type of certificate used and the browser configuration, a pop-up alert box may also offer details of the server's certificate, but the information is hard to interpret and users will need training to recognise the pop-up as a source of useful information rather than an annoyance.

- Self-signed certificates will almost always produce an alert showing the identity asserted (but not proved) by the server owner. The user is likely to be offered the option to recognise this certificate in future (effectively silencing the alert).
- Organisation-signed certificates are also likely to result in an alert that names the organisation. An organisation with an existing relationship with most of the users of the site (as will be common for internal university and college servers) can instruct them to configure their browsers (or can do it for them in a tailored browser image) to silently recognise certificates signed by their own organisation.
- Commercial certificates will usually be recognised silently by browsers, with no pop-up or alert. EV certificates will often cause a colour change in the browser status bar, and provide a link to the registered details of the owning organisation.

Choosing and Obtaining a Certificate

The choice of self-signed, organisation or commercial certificate therefore depends on the user community and on whether encryption, identification, or both is most important. In outline:

- for servers with a relatively small number of users who are known in advance, a self- or organisationsigned certificate may give users confidence that they are indeed accessing

a particular server

- for servers used by a large or unknown population, a commercial certificate recognised by unmodified client software is likely to cause fewest problems.

Whichever type of certificate is chosen, the steps to obtain it are the same:

1. Create a Certificate Signing Request (CSR) – a file containing details of the server which is used to create the certificate. Any server software that can support hTTPS connections should be able to generate a CSR.
2. Obtain a signed certificate. A self-signed certificate can be created on the server; for an organisational or commercially signed certificate, the cSR and the required documentation will need to be sent to the organisation for signing.
3. Install the certificate. The signed certificate (another file) needs to be installed on the server. Different servers have their own ways of doing this.

Jisc has arrangements with commercial certificate providers on behalf of Jisc customers: see https://www.jisc.ac.uk/certificate-service [4].

Certificates for Other Services

Digital certificates are most commonly used on web servers to support HTTPS. They can also be used with many other types of server including remote authentication (e.g. **EAP-TTLS**) and mailbox access (**IMAPS** and **POPS**). Similar considerations apply when choosing the appropriate type of certificate for these services.

Links
[1] http://www.example.com
[2] http://www.examp1e.com
[3] http://cabforum.org/EV_certificate_Guidelines_V11.pdf
[4] https://www.jisc.ac.uk/certificate-service