

# STAY SMART ONLINE ALERT SERVICE

## Factsheet 9

### What is a web site digital certificate and why is it important to check?

Web site digital certificates can help users decide when it is safe to transact online and when it is not.

This factsheet explains how to check if a digital certificate is present on a web site, how to check if the certificate is valid and if so, whether it should be trusted.

Users that have a better understanding of how SSL and digital certificates contribute to online security and trust will be better able to detect phishing sites and protect themselves from online fraud.

---

#### 1. What is a digital certificate?

A digital certificate is a mechanism for users to obtain assurance about the identity and authenticity of a web site. By inspecting the digital certificate on a web site users can help defend against identity theft and fraud. For example, a phishing site set up by criminals which masquerades as a legitimate web site (such as an online banking web site) can often be identified by an invalid digital certificate.

Digital certificates are implemented as part of a set of security mechanisms provided by SSL. Another key feature of SSL is that it encrypts all traffic passed between the user's computer and the remote web site to prevent the data being read in transit as it passes from a user's computer (the client) to the web site and vice versa.

Generally, any web site that requires you to provide a user name and password, financial details or personal identifying information should provide SSL.

Generally, whenever you connect to an SSL enabled web site, it will provide a digital certificate. Figure 1 (Mozilla Firefox web browser) and figure 2 (Microsoft Internet Explorer version 7 web browser) are examples of an SSL-enabled web site ([www.auscert.org.au](http://www.auscert.org.au)) with (circled):

- the correct form of an SSL web site address (using 'https://')
- a padlock image indicating that the connection is secure and has a valid certificate

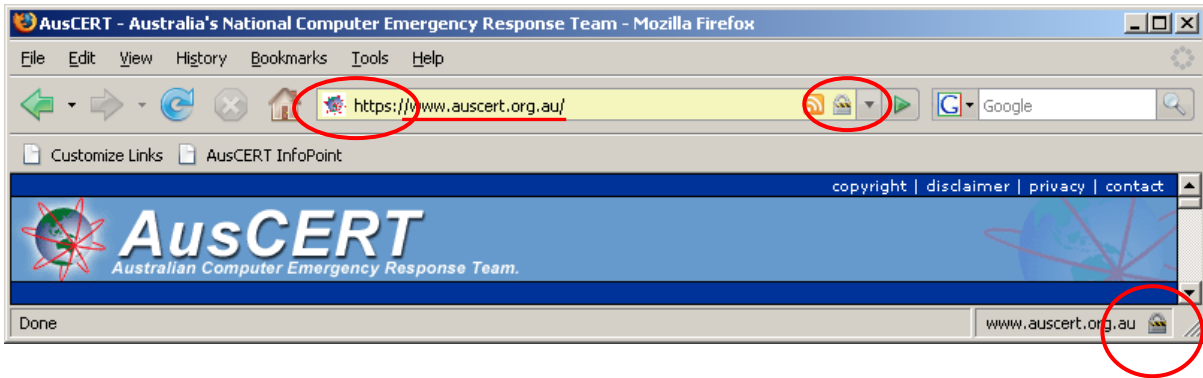


Figure 1, Mozilla Firefox, SSL session

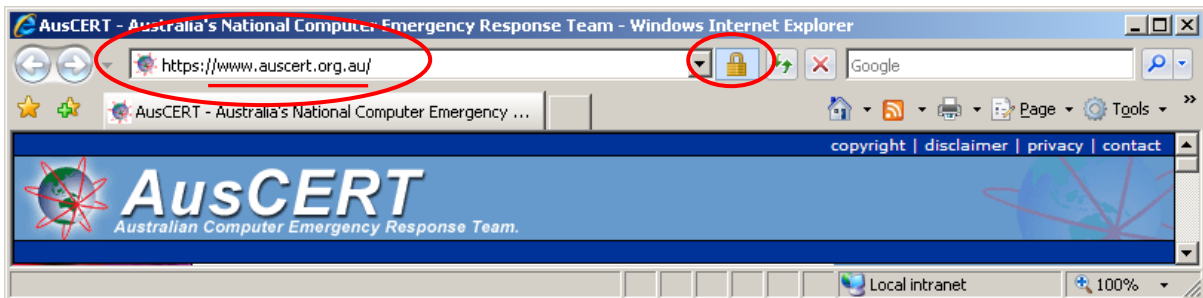


Figure 2, Microsoft Internet Explorer v7, SSL session

You should always inspect the digital certificate of a web site if you intend to submit financial or personal identifying information (PII) to it. To view more information about the digital certificate, click or double-click the padlock image.

Generally, phishing sites often do not attempt to include padlocks or digital certificates. Hence the absence of these on web sites that normally include such mechanisms is a sign that the site is probably fraudulent and should not be trusted.

Recommendation: As a general rule, do not provide login credentials or other personal information to any web site that does not correctly implement SSL digital certificates in the way described here.<sup>1</sup> If you cannot inspect the digital certificate of a web site to your satisfaction *you should not submit information to the site.*

<sup>1</sup> Caveat: some well known Australian organisations enable SSL on their web site but remove parts of the web interface that enable users to check and verify that the digital certificate is valid. This is poor practice as it allows attackers to more easily impersonate these web sites and provides the legitimate customers or users of these web sites no mechanism to verify whether they should trust the legitimate web site. Fortunately most organisations correctly implement SSL on their web site so it is still worthwhile to check for the presence and validity of web digital certificates.

## 2. Why should I inspect the digital certificate?

The web browser window has, in the past, been vulnerable to manipulation by criminals and the presence of a padlock image may not be enough to provide assurance of security. This means that once you have checked for the presence of the padlock, it is still wise to view and check the validity of the certificate itself.

Figures 3 and 4 display information about the digital certificate for AusCERT's web site. This window reports that a Certificate Authority (a trusted third party, called Thawte) has verified that the domain name `www.auscert.org.au` belongs to an organisation called AusCERT. If this window reports that the certificate cannot be verified or is untrustworthy *you should not submit information to the site*.

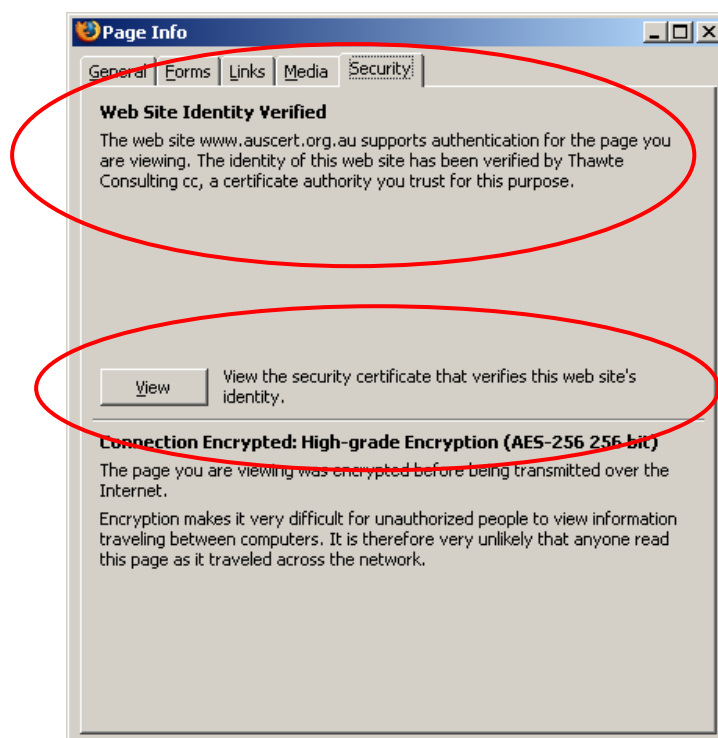


Figure 3, Mozilla Firefox, digital certificate information

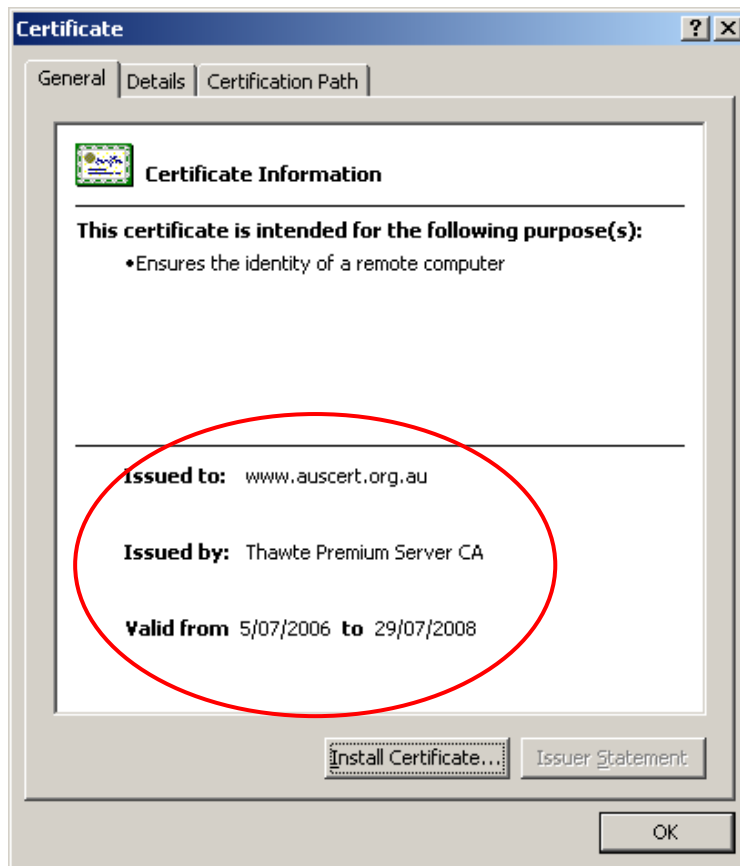


Figure 4, Internet Explorer, digital certificate information

### 3. Browser warnings

The main reasons that a web browser will warn users about problems with a digital certificate are when the certificate :

- is self-signed,
- has expired, or
- the domain name on the certificate does not match the domain name of the web site address.

Any of these warnings may indicate that the web site is not legitimate and has been created to fool users into disclosing sensitive or other personal information.

Figures 5 and 6 provide an example of a browser warning for an expired certificate.<sup>2</sup>

---

<sup>2</sup> In the case of this digital certificate, the web domain for www2.auscert.org.au is not in public use at the time of writing and the expired certificate been created for educational purposes only.

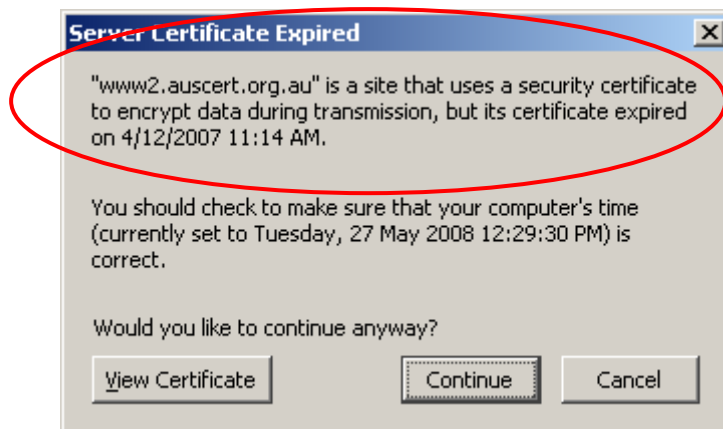


Figure 5, Browser warning for an invalid certificate

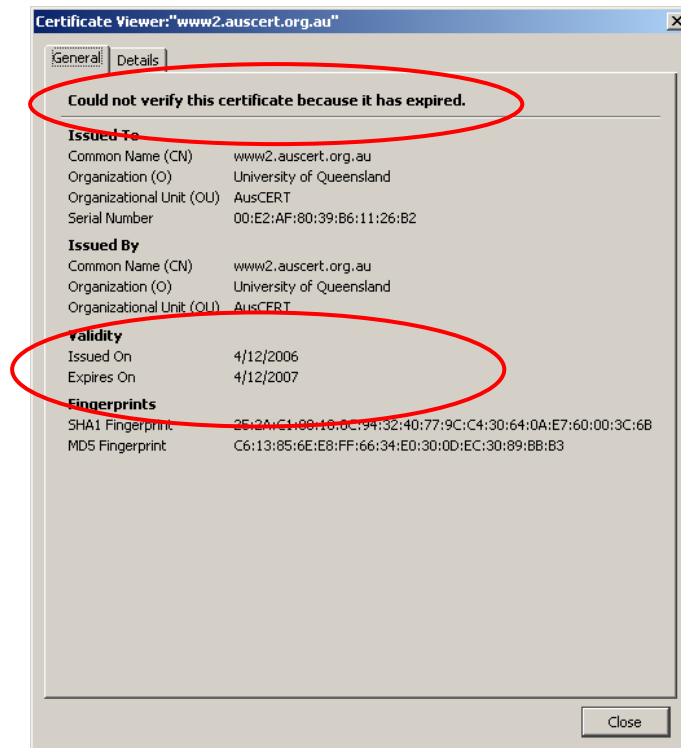


Figure 6, Example of a self-signed and expired digital certificate

Recommendation: In all cases, browser warnings need to be understood before determining whether the site should be trusted. If you do not know of a legitimate reason why the certificate cannot be verified *you should not submit information to the site.*

## 5. Check if a digital certificate exists and is valid

In summary, to check if a digital certificate exists and is valid, check that:

- https appears in the browser address bar; and
- a padlock exists adjacent to the address bar; and
- click on the padlock to see if the domain name listed on the digital certificate is exactly the same as the domain name in the address bar; and
- the certificate is not self-signed, ie not signed by the same entity that owns the web domain; and
- the certificate has not expired.

## 6. Common misconceptions about SSL and digital certificates

Having explained what a digital certificate is and why it is important to check, it is relevant to explain what SSL can and cannot do.

### Facts about SSL

- a) When a web site's identity is verified by a trusted third party, which is evident by examining the digital certificate, it provides an assurance that the web domain name belongs to the entity claimed. In other words, it provides an assurance about the identity and authenticity of the web site and hence helps users decide whether the web site can or should be trusted, particularly if the user needs to submit personal or other sensitive information to the web site.
- b) SSL encrypts the traffic in transit between your computer and the web site to protect the confidentiality of the data *in transit only*.
- c) If one of the computers that participates in an SSL session is compromised with certain types of malware (typically a user's computer that connects to the web site with a browser), attackers may still read and capture the data after it has been decrypted on the user's computers or before it is encrypted by the user's computer and sent to the web site.

### Myths about SSL

- a) **Myth** An SSL protected web site means it is a secure web site and less likely to be hacked.

An SSL protected web site provides no assurance about the security of the web site itself or how well those who manage the web site handle your personal information stored on its databases. An SSL protected web site is not necessarily more secure than a web site that does not use SSL. An SSL web site is no more or less able to be compromised or defaced than one that does not use SSL. SSL mainly provides protection for data in transit only.

- b) **Myth** Attackers cannot see, access or capture or modify any information obtained or submitted during an SSL protected session.

See paragraph c above for an explanation.