

TC Safety Information

SSL CERTIFICATES

Internet security is everyone's concern

One thing is certain: successful online business is primarily based on trust. With the Secure Sockets Layer – SSL for short – and a suitable certificate for your server, you provide your customers and business partners with what's important: security and trust.

But users must also do their part to navigate securely on the Internet. Over the last ten years the web has developed from the display of simple text pages to an extensive, interactive application. Many old browsers can no longer properly display these new contents. But what's worse, they have considerable security gaps. In addition to fraudulent websites, worms, viruses and trojans are other familiar risks for which protection is also available. For example, secure access to the Internet includes not only current antivirus software, but also a computer with a current operating system and browser. Regular updating of outdated systems is urgently necessary, as otherwise known security gaps endanger the integrity of data, systems and networks.

For example:

<http://www.itworld.com/security/98372/another-day-another-internet-explorer-security-hole/>

Another day, another Internet Explorer security hole. It seems like every other week there's a new Internet Explorer security hole.

<http://www.sophos.com/blogs/gc/g/2010/03/23/critical-firefox-security-hole-fixed-updated/>

Critical Firefox security hole fixed - have you updated? Mozilla has responded to concern about a critical security vulnerability in Firefox 3.6, by releasing version 3.6.2 of its popular browser ahead of schedule.

Security of root certificates

In addition, outdated operating system and browser versions do not support the checking of many SSL certificates and confuse users with corresponding error messages or give them a false sense of security. Generally, outdated browsers and/or operating systems do not have the current root certificates required for checking the authenticity of an SSL certificate. In contrast to modern systems, older systems do not have automatic update capabilities so that missing root certificates are no longer loaded at a later time. These root certificates can generally be manually loaded from the websites of the SSL suppliers at a later time (e.g. at TC TrustCenter under: http://www.trustcenter.de/en/infocenter/root_certificates.htm).

However, this procedure should only be used as an exception. For higher-level security reasons, an upgrade to current browser versions, e.g. MS IE 7 or Firefox 3.1x, is always preferable in these cases. What good is a tested SSL certificate for online banking if the PC is otherwise wide open for attacks?

This situation becomes even worse for users of older systems due to the fact that many certificate suppliers will soon renew their root certificates in order to meet more demanding security requirements for key lengths. As a result, as of the beginning of the year TC TrustCenter also uses root certificates with an extended key length.

The reason for this is the current estimates on the security of key lengths and cryptographic algorithms by recognized institutions like the National Institute of Standards and Technology (NIST), the European Telecommunications Standards Institute (ETSI) and the German Bundesamt für Sicherheit in der Informationstechnik (Federal Office of Security in Information Technology - BSI).

The use of so-called intermediate CA certificates (also called sub-CA certificates) is another mechanism for strengthening security of certificates. In the process, the server or client certificates are not directly signed by the root CA, but instead by an intermediate, separate CA certificate. TC TrustCenter has taken this new root generation into account during the conversion and has only issued server and client certificates below a sub-CA certificate since 11 December, 2009. As a side effect, this model reduces the size of the revocation lists (CRLs), which results in an accelerated validation process with CRL-based methods. Installation information for sub-CA certificates from TC TrustCenter is available here:

http://www.trustcenter.de/en/installation_instruction_for_intermediate_ca_certificate_ll.ht In accordance with this, the leading browser producers Microsoft and Mozilla have introduced stricter requirements for the preinstallation of root certificates in the certificate memories of their browsers. As a result, the conversion to extended key lengths and the use of sub-CA certificates will soon be carried out by many suppliers. As a result, outdated browser and/or operating systems now only have poor chances. In this case the only remedy is upgrading to current, secure browsers.

TC Safety Information

SSL CERTIFICATES

Secure browser software

Here are the browsers that ensure secure navigation on the Internet:

Microsoft Internet Explorer 7.0+

<http://www.update.microsoft.com/windowsupdate/>

Mozilla Firefox 3.0+

<http://www.mozilla.com/en-US/>

Google Chrome 4.0+

<http://www.google.de/chrome?platform=mac&hl=en/>

Opera 10+

<http://www.opera.com/download/>

Safari 3.0+

<http://www.apple.com/safari/>

Browser producers like Microsoft, Mozilla (Firefox) and Apple offer regular updates. If an automated update function is not used, it is advisable to visit the producer's update websites regularly in order to download and install the current updates. With the Internet Explorer the updates are controlled as part of the Windows Update function, which is highly recommendable anyway.

This kind of operating system service is not available for Firefox. Therefore, it has its own update function (Extras/Settings/Advanced/Update), which can and should be set so that the browser is automatically updated.

In company networks, updating of the software used is usually realized with automatic software distribution or the request for a manual update. In this case those responsible for IT in the company need to take the necessary security requirements into account in patch management.

The Secunia Personal Software Inspector (PSI) from Secunia is excellently suited for locating outdated software on Windows systems: http://secunia.com/vulnerability_scanning/personal

Key lengths for server and client certificates

However, stricter requirements will not only apply to root and CA certificates in the future:

For example, in the Guidelines for Extended Validation (EV) Certificates published in 2007, the CA/Browser Forum, a voluntary association of leading certification authorities (CAs) and Internet browser software suppliers, calls for certificates which are valid beyond 31 December, 2010 to have a key length of least 2,048 bits. Therefore, the key length of 2,048 bits is already mandatory today for Extended Validation (EV) Certificates (e.g. TC Extended Trust SSL).

The National Institute of Standards and Technology (NIST) generally recommends increasing key lengths to 2,048 bits by the end of 2010: http://csrc.nist.gov/publications/drafts/800-131/draft-800-131_transition-paper.pdf

The Windows® Root Certificate Program from Microsoft (<http://technet.microsoft.com/en-us/library/cc751157.aspx>) completely prohibits the registered certification authorities from issuing certificates with 1,024 bits below a public root as of 01/01/2011.

For security reasons, TC TrustCenter recommends already using a key length of 2,048 bits today.

Our recommendation for online suppliers: Enlighten your customers!

In their own interest, some suppliers of online services, which exchange confidential data with their customers (banks, shops with payment functions, etc.) inform their customers on security risks and protection possibilities directly on their website. In addition, the enlightenment is viewed by many customers as a sign of trustworthy customer services.