

TC TrustCenter Nr. 13/08, December 2008

TC TrustCenter Response to SSL Vulnerability Paper

Hamburg, 31st December 2008

According to the research, “MD5 is considered harmful today – Creating a rogue CA certificate” a research team succeeded in generating a rogue CA certificate trusted by all popular browsers. The attack takes advantage of a weakness in the MD5 hash function. MD5 is one of a series of hash functions that are used to check the integrity of data. Such hash functions are used for signing certificates.

In 2007 the risk of generating MD5 collisions was already recognized and theoretical MD5 attacks were published.

TC TrustCenter at this time reacted immediately and stopped issuing MD5-RSA based certificates to its customers in 2007. All certificates issued to its customers since that time use other hash procedures, such as SHA-1. TC TrustCenter was mentioned in the paper only because it uses MD5 based certificates for some of its SSL servers.

The vulnerability of MD5 alone is not sufficient to generate a rogue CA certificate. The recently published attack on the SSL certificate systems can now be realized, not only because of the MD5 weakness, but also because of other criteria including:

- The CA processes online requests for MD5 based certificates in an automated way. This does not apply to TC TrustCenter: TC TrustCenter ceased using an online certificate request channel for MD5-RSA server certificates sometime ago.
- It is possible to predict a serial number with reasonable probability of success. This does not apply to TC TrustCenter: Following the recommendations of the German Signature Act, TC TrustCenter uses a unique method to construct serial numbers which are not predictable.

Due to the methods TC TrustCenter uses for certificate generation, the described attack does not apply to any certificates issued by TC TrustCenter on base of MD5. So, the described attack does not mean any risk to TC TrustCenter’s customers.

Further questions regarding MD5 are discussed in the TC TrustCenter FAQ.

About TC TrustCenter

For more than 10 years TC TrustCenter has been the partner for the financial sector and the industry with its solutions for authentication, verification and encryption. As one of the first Trustcenters we provide world wide trust to the internet and electronic B2B Business with our Managed Services. In Europe as well as in the US we do have a broad range of project and industry experience regarding PKI and considerable references of international customers.

Our portfolio ranges from solutions for Phishing Protection, Security of Online Transactions, and Electronic Invoicing to broad PKI solutions and Managed Security Services. Our On Demand PKI Solutions are cost-efficient, highly secure and fast to implement

TC TrustCenter is accredited according to the German Signature Act, European Signature Act, Identrust, SAFE, TÜVIT and SISAC.

Press contact TC TrustCenter:

Stephanie Willemsen

Sonninstrasse 24-28

D-20097 Hamburg

Tel.: +49 40 808026-0

Fax: +49 40 808026-126

E-Mail: stephanie.willemsen@trustcenter.de

Web: www.trustcenter.de