

TC TrustCenter Nr. 13/08, Dezember 2008

## **Stellungnahme der TC TrustCenter GmbH zu dem Angriff gegen das MD5 Hash-Verfahren**

### **Hamburg, 31. Dezember 2008**

Wie in dem Artikel „MD5 considered harmful today - Creating a rogue CA certificate“ nachzulesen, ist es einem Forscherteam gelungen, durch eine MD5-Kollision ein gefälschtes Herausgeberzertifikat zu erzeugen, das von allen gängigen Browsern als vertrauenswürdig eingestuft wird. Bei MD5 handelt es sich um eine der möglichen Hash-Funktionen, die zur Integritätsprüfung von Daten benutzt werden und u.a. beim Signieren von Zertifikaten Anwendung finden.

Bereits 2007 wurde die Möglichkeit zur Konstruktion von Kollisionen erkannt und erste theoretische Angriffsszenarien auf MD5 wurden publiziert.

TC TrustCenter hat zu diesem Zeitpunkt sofort reagiert und bereits 2007 die Ausstellung von Zertifikaten auf Basis von MD5 Hash-Funktionen für seine Kunden eingestellt. Alle seitdem für Kunden ausgestellten Zertifikate nutzen andere Hash-Verfahren, wie z.B. SHA-1. Die TC TrustCenter GmbH wurde in dem oben genannten Artikel nur erwähnt, weil sie selbst für einige eigene Server MD5-basierte SSL Zertifikate verwendet.

Die Schwäche des MD5 Verfahrens allein reicht jedoch zur Erstellung eines gefälschten Herausgeberzertifikates nicht aus. Der jetzt veröffentlichte Angriff auf das SSL Zertifikatssystem wurde praktisch erst möglich, weil neben der MD5 Schwäche noch weitere Gegebenheiten ausgenutzt wurden, u.a.:

- Die Zertifizierungsstelle bietet einen online-Antragsweg, der es Endkunden ermöglicht, MD5-RSA signierte Zertifikate ohne weitere Prüfung zu erlangen. Dies ist bei TC TrustCenter nicht möglich.
- Die Seriennummer des Zertifikats ist vorhersagbar. Dies ist bei TC TrustCenter Zertifikaten nicht möglich, da eine von der Bundesnetzagentur empfohlene Methode zur Seriennummerngenerierung eingesetzt wird, die eine Vorhersagbarkeit nicht zulässt.

Aufgrund der von TC TrustCenter genutzten und vom dargestellten Angriffsszenario abweichenden Methoden bei der Zertifikatserstellung besteht keinerlei Sicherheitsrisiko, dass die von TC TrustCenter auf Basis des MD5 Verfahrens ausgestellten Zertifikate durch einen derartigen Angriff kompromittiert werden konnten.

Weitere Fragen zum Thema MD5 werden ebenfalls in der TC TrustCenter FAQ behandelt.

### Über TC TrustCenter

Seit mehr als zehn Jahren ist TC TrustCenter mit seinen Lösungen für Authentifizierung, Verifizierung und Verschlüsselung vertrauenswürdiger Partner der Finanzbranche und der Industrie. Als Trustcenter bildet das Unternehmen mit seinen Managed-Services weltweit die Grundlage für Vertrauen ins Internet und ins elektronische B2B-Geschäft. Sowohl in Europa als auch in den USA verfügt TC TrustCenter über ein breites Spektrum an Projekt- und

Branchenerfahrung im Public Key Infrastructure (PKI)-Umfeld und kann auf namhafte Referenzen internationaler Kunden verweisen.

Das Portfolio des Unternehmens reicht von Lösungen zum Schutz vor Phishing und zur Sicherung von Online-Transaktionen über Lösungen für die elektronische Rechnungssignatur bis hin zu umfassenden PKI-Lösungen und Managed Security-Services. Die weltweit ersten On Demand-PKI-Lösungen von TC TrustCenter zeichnen sich durch Kosteneffizienz, höchste Sicherheit und schnellstmögliche Implementierung aus.

Die TC TrustCenter GmbH ist eine gemäß Deutschem Signaturgesetz, Europäischem Signaturgesetz, Identrust, SAFE, TÜVIT und SISAC akkreditierte Zertifizierungsinstanz. Weitere Informationen sind unter [www.trustcenter.de](http://www.trustcenter.de) erhältlich.

Pressekontakt 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](mailto:stephanie.willemsen@trustcenter.de)

Web: [www.trustcenter.de](http://www.trustcenter.de)