Pressemitteilung

Sicherheit der privaten Schlüssel von CAcert-Zertifikaten

In den Medien[1] wurde jetzt bekannt, dass US-Regierungsbehörden zur Entschlüsselung der verschlüsselten Kommunikation möglicherweise die privaten Schlüssel von Dienstanbietern fordert.

Bei der Zertifikatserstellung mit CAcert-Zertifikaten verlassen die privaten Schlüssel niemals den Rechner des Anwenders und werden damit nicht etwa an CAcert übertragen. CAcert kann deshalb die privaten Schlüssel auch nicht weitergeben. Dadurch stellen Zertifikate von CAcert ein Verfahren dar, mit dem sichere Kommunikation gewährleistet werden kann.

[1] http://heise.de/-1924012

74 Wörter, 622 Zeichen

1 Material zur Pressemitteilung

1.1 CAcert

Ziel von CAcert ist es kostenfreie Digitale Zertifikate nach dem X.509 Standard anzubieten. Diese Digitalen Zertifikate können zum Unterschreiben und Verschlüsseln von Dokumenten als auch zum Aufbau von gesicherten Datenverbindungen genutzt werden.
CAcert hat zur Zeit 250.000 angemeldete Benutzer [1].
CAcert Inc. ein eingetragener Verein mit Sitz in New South Wales (NSW), Australia. CAcert Inc. hat ca. 100 Mitglieder und wurde am 24. Juli 2003 unter dem vollständigen Name "CAcert Incorporated" mit der Incorporation Nummer INC9880170 gegründet. Die DUNS Nummer ist 75-605-6102. [2]
CAcert finanziert sich aus Spenden.

[1] https://www.cacert.org/stats.php
[2] https://wiki.cacert.org/CAcertInc

Weitere Informationen über CAcert:
https://wiki.cacert.org/CAcertInShort-de

2 Ansprechpartner CAcert

Alexander Bahlo, Officer for Public Relations
pr@cacert.org