Press release

Safety of private keys of CAcert-Certificates

Currently US press[1] spreads information that government organizations demand private keys from service providers for decrypting secret communications.

When creating certificates with CAcert, private keys never leave the system of the user, and therefore are not transmitted to CAcert. Hence, private keys cannot be disclosed by CAcert and thus certificates from CAcert provide a means to safeguard a secure communication.

[1] http://news.cnet.com/8301-13578_3-57595202-38/feds-put-heat-on-web-firms-for-master-encryption-keys/

69 words 572 characters

1 Press release material

1.1 CAcert

The aim of CAcert is to offer free digital certificates that meet the X.509 standard. These digital certificates can be used to sign and encrypt documents as well as to establish secure data communication links.
The CAcert project has 250,000 registered users. CAcert Inc. is an incorporated non-profit association with approx. 100 members and is registered with New South Wales (NSW), Australia. - It was incorporated by 24 July 2003, with the full association name CAcert Incorporated under the Incorporation No INC9880170. We have a DUNS number 75-605-6102. [2] CAcert is financed by donations.

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

More information about CAcert:
https://wiki.cacert.org/FAQ/AboutUs
https://en.wikipedia.org/wiki/CAcert

2 Contact CAcert

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