Hoeveel kost CAcert

De certificaten zijn gratis.
Dank zij vele vrijwilligers van CAcert en de geautomatiseerde diensten van CAcert, is CAcert in staat om zeer kosten effectief te werken. Uw schenkingen om de bedrijfskosten van CAcert te helpen dekken worden zeer gewaardeerd.

Hoe kan ik CAcert steunen?

- Word lid van de CAcert gemeenschap en gebruik de certificaten van CAcert
- Neem de waarmerkers test en wordt CAcert waarmerker
- Steun CAcert op beurzen, congressen enz, draag de boodschap uit
- Help met de kern processen van CAcert, b.v. systeem administratie of ondersteuning

Zie: http://wiki.cacert.org/HelpingCAcert.

Waar kan ik meer informatie vinden?

Voor meer informatie bezoek de CAcert web site:
http://www.cacert.org of http://www.cacert.nl

Documentatie is beschikbaar op de CAcert wiki:
http://wiki.cacert.org

CAcert heeft IRC chat kanalen op irc.cacert.org waar u op de CAcert diensten kunt reageren, steun vragen, of om enkel te praten met Cacert gemeenschaps leden

Channels: #cacert (Engels)
#cacert.ger (Duits)
#cacert.fr (Frans)

Voor een beveiligde chat, gebruik SSL port 7000.

Hebben geen IRC programma? Gebruik de Webinterface
http://irc.cacert.org

Support email:
cacert-support@lists.cacert.org

Support informatie:
http://wiki.cacert.org/GettingSupport

http://www.cacert.org

Support

Email: cacert-support@lists.cacert.org
IRC channel: #cacert on server irc.cacert.org

Fingerprints

CAcert Root certificate

SHA1: 13:5C:EC:36:F4:9C:B8:E9:3B:1A:B2:70:CD:80:88:46:76:CE:8F:33
MD5: A6:1B:37:5E:39:0D:9C:36:54:EE:BD:20:31:46:1F:6B

CAcert Class 3 Root certificate

SHA1: AD:7C:3F:64:FC:44:39:FE:F4:E9:0B:E8:F4:7C:6C:FA:8A:AD:FD:CE
MD5: F7:25:12:82:4E:67:B5:D0:8D:92:B7:7C:0B:86:7A:42

Flyer-2s-3c-NI 2.05 rev. 01 (June 2011)

Digitale certificaten
voor Individuen
en Organisaties

cliënt certificaten
server certificaten
code signing

X.509 ◆ SSL/TLS ◆ S/MIME
PGP ◆ GnuPG ◆ OpenPGP

http://www.cacert.org

Digitale Certificaten

Wat is CAcert?

CAcert is een gemeenschaps gebaseerde organisatie, zonder winst oogmerk en is in Australië geregistreerd.

De doelstellingen van CAcert zijn:
- veiligheid in de IT arena te verbeteren
- gebruikers in hun veiligheids inspanningen te ondersteunen
- om hulpmiddelen en mechanismen voor de veiligheid in de IT te leveren

De aandachts gebieden omvatten:
- beveiligen van Webservers door HTTPS te gebruiken en versleutelen van elektronische post
- SSL/TLS server toepassingen en web communicatie
- VPN communicatie
- code signing (b.v. Java)
- het digitaal ondertekenen van documenten

CAcert poogt veiligheid vrij voor de IT wereld ter beschikking te stellen en de veiligheidsmiddelen voor iedereen betaalbaar te maken. CAcert is een open gemeenschap en gebruikt de filosofie van Open Source om haar doelstellingen te bereiken.

Waarom meedoen?

Beveiliging:
Bevorder veiligheid voor u zelf en andere Internet gebruikers.

Privacy:
De certificaten van CAcert helpen om uw privacy op Internet te handhaven.

Authentificatie:
Bewijs dat uw identiteit is gecontroleerd en dat u werkelijk bent wie u zegt u bent.

Gratis e-mail en server certificaten

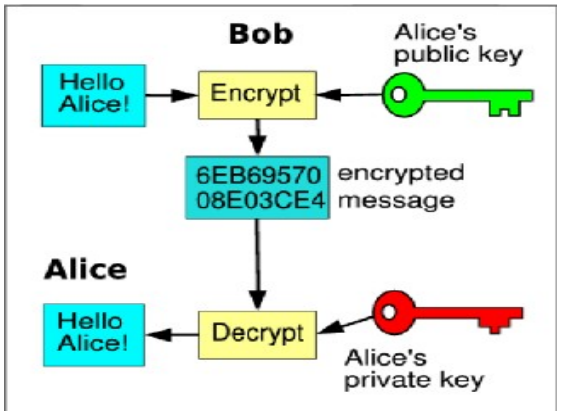
X.509 certificaten worden gebruikt om e-mail te ondertekenen met S/MIME en maken het mogelijk dat servers, zoals Web en mail servers, veilige verbindingen maken. Andere certificatie autoriteiten vragen gewoonlijk hoge prijzen voor hun diensten: het controleren van uw identiteit en of een website of het e-mailadres werkelijk van u is. CAcert biedt kosten loos dit aan.

Hoe werkt CAcert?

Om u bij CAcert aan te sluiten moet u aanmelden op http://www.cacert.org. U moet slechts uw volledige naam, geboorte datum en e-mailadres specificeren. U kunt een onbeperkte aantal e-mailadressen voor cliëntcertificaten en domeinnamen voor servercertificaten later toevoegen. Na aanmelding kunt u beginnen zelf certificaten aan te maken via de Webinterface. Om uw naam in het certificaat te krijgen moet uw identiteit gecontroleerd zijn. Neem contact op met waarmerkers (b.v., door te zoeken naarwaarmerkers op de website) of via ontmoeting beurzen en bijeenkomsten.

Gratis PGP key signing

Hebt u PGP/GnuPG/OpenPGP keys? Zodra u gewaarmerkt bent kan uw sleutels worden ondertekend met de PGP sleutel van CAcert.



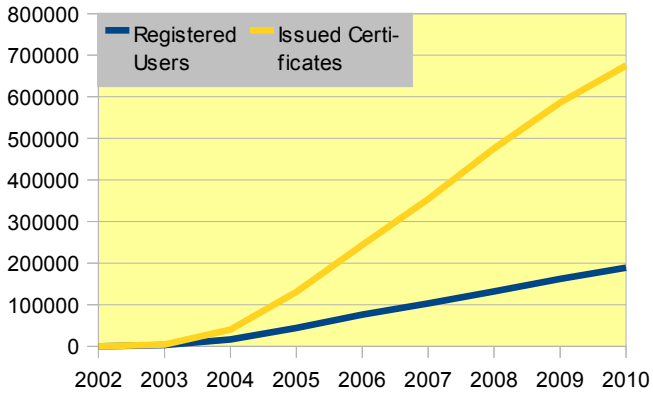
Hoe public key encryption werkt

Code signing

U kunt uw software digitaal ondertekenen gebruikend makend van CAcert certificaten om het te identificeren en authentiek te verklaren.

Organisatie waarmerking

Voor bedrijven en andere organisaties heeft CAcert een Organisatie Waarmerkings Programma. Zodra gewaarmerkt, kunnen de certificaten die de naam van de organisatie bevatten worden verstrekt en de werknemers van de organisatie kunnen hun eigen certificaten krijgen verstrekt door de organisatie zelf.



De groei van CAcert sinds stichting in 2002

Welke software ondersteunt CAcert certificaten?

U kunt CAcert cliëntcertificaten gebruiken in alle software geschikt voor X.509 certificaten (van S/MIME), zoals:

- Microsoft Outlook en Office
- Mozilla Thunderbird en Firefox
- OpenOffice.org

U kunt CAcert servercertificaten gebruiken in alle software geschikt voor op SSL-Gebaseerde certificaten, zoals:

- Apache web server
- Microsoft Internet Information Services
- Mailservers (b.v. Postfix, Sendmail, Courier)
- OpenSSL/OpenVPN