What is CAcert?
CAcert was founded as a organisation to establish the first non-profit certification authority. Until CAcert, verified certificates were only created by commercial CAs who charged high prices. This was too expensive, so most people use the internet without encryption and verification. CAcert aims to bring the open source philosophy to the wold of IT security and to make security affordable and available for everyone. At Events CAcert will offer to verify your identify in order to allow you to create your own personal certificates for free.

What is it used for?
The certificates allow you to secure your webserver with HTTPS, to sign and encrypt your emails with S/MIME. You are no longer dependent to self-signed certificates. The certificates may be used for personal and business use.

Where can I get my certificate?
CAcert assurers verify your identify with two officially issued photo identities (passport, drivers license). Certificates can be created on our website on demand and will contain the data verified by CAcert.

Can I have more than one email address or domain?
Yes, of course – an unlimited number. You can register unlimited email addresses and domains. For every email address or domain you will receive a confirmation mail to the address itself or to an official email address of the domain (eg. postmaster@domain).

When does the account expire?
Your CAcert account does not expire. The certificates have to be renewed every two years. No new assurance is needed for renewal.

Where is the CAcert root certificate already integrated?
We are already in the standard cache of different Linux distributions. However, many browsers (Microsoft Internet Explorer, Mozilla Firefox) use their own certificate store.

When will you be in the browsers?
This is one of our main targets. We are looking to achieve this ASAP. A requirement for this is an audit (such as WebTrust, ONR 17700 or equivalent), which costs appr. 70,000 EUR and so is not easily affordable for a non-profit organisation. Your donation is welcome!

What happens until then?
Until then you have to add our root-certificate yourself to trust all (at the momenent over 100,000) certificates issued by CAcert.

Why should I trust CAcert?
We verify the identity of all our users with at least one official photo identity and every user is normally verified by more than one assurer.

Is my data secure?
We do not save any identity data from your identity like identity number and therefore are less vulnerable to identity theft such as in the United States. We hold your name, date of birth and email data and may release this under due process (such as court order).

How does the point system work?
CAcert uses a point system to determine how well your identity has been verified. You need 100 points to be able to use CAcert completely. On big events you can get 100 points at once and then you are allowed to assure others. You can find more details on our website

http://www.cacert.org.

Points	Status	personal client certificates	code-signing certificates	PGP/GPG signature	validity for server certificates	max. issuable points
0 to 49	unassured				6 month	
50 to 100	assured	yes	yes		24 month	
Assurer Challenge: CATS test						
100 to 149	Assurer	yes	yes	yes	24 month	10 to 30
150	fully assured	yes	yes	yes	24 month	35

Can points expire or decrease?
No. Points are valid for life time, as long they were collected according to the rules. So it is useful to get assured by as many people as possible to strengthen the web of trust.

Can I use the certificates for commercial applications?
Of course! Additionally CAcert offers to assure organisations so as to get the name of the organisation into the certificate. Please ask our local organisation consultant.

What does an assurer have to care for?
User accepts CCA. Follow the Assurance Policy.
http://wiki.cacert.org/AssuranceHandbook2 provides some basic information.

Where do I get support?
Email: support@cacert.org
Chat: irc.cacert.org #cacert (english) or #cacert.ger (german)
wiki: http://wiki.cacert.org

I forgot my password, what do I have to do?
There are four options:
  • You log in using the client certificate
  • You can answer the 5 questions you provided when you created the account.
  • You can create a new account and lose all your points. You can recover your email addresses and domains from your old account by using the dispute system.
  • You can pay 10,- EUR to CAcert to have an admin reset your password.

What is the fingerprint of the 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

How can I help?
http://wiki.cacert.org/HelpingCAcert

This document is signed by

	Signatory	EMAILADDRESS=ulrich@cacert.org, CN=Ulrich Schroeter
	Date/Time	Fri Feb 19 18:04:54 CET 2010
	Issuer-Certificate	EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority, OU=http://www.cacert.org, O=Root CA
	Serial-No.	434828
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)
Note	This signature can be verified, if you open the document with Adobe Reader!	