Branding
and
Style Guide

CAcert.org

Version 0.4 – October 2007

Introduction

CAcert today stands for Free Certificates and things around it. The focus of our visual identity is our logo, the unifying element of CAcert.org. We want our corporate logo to represent the value we deliver to users, association members, core team members, partners, community and the internet at large. This Branding and Style Guide is intended to help everyone participate in the CAcert community.

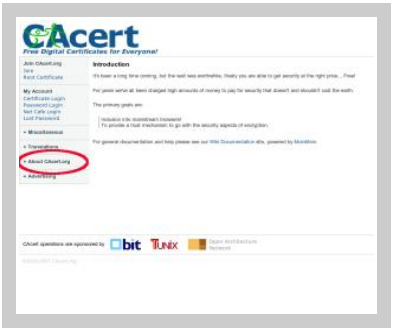
The CAcert style philosophy is based on the following principle: We have *one* corporate logo. This logo is used to identify *all* parts of the CAcert project.

This document describes how the CAcert logo should be used on all communication materials such as stationary, brochures and advertisements.

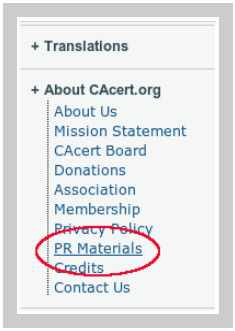
How to get CAcert Public Relations materials

CAcert PR materials can be downloaded from the CAcert web site, http://www.CAcert.org.

From the ‘About Cacert.org’ menu on the main page, choose ‘PR Materials’. You may need to click on ‘About Cacert.org’ to show the menu choices. On the PR Materials page you can find updated versions of this Branding and Style Guide, logos, example documents, and other materials.



CAcert main page



`About’ menu

Basic elements

The CAcert logo

The CAcert.org logo is the unifying visual identifier to be used across all our community and for official use. Using the logo consistently and correctly is vitally important in reaffirming our brand promise to both internal and external audiences.

The logo should be the same as presented in this Branding and Style Guide and in the CAcert website.

There are two versions of the basic logo: a colour version, and a monochrome version. The colour version should be used whenever possible, and must always be placed on a white background. The monochrome version must be used in situations where the colour version can not be reproduced correctly, e.g., on cheap printers and fax covers, and on coloured backgrounds. Both versions are equal in status, but should not mixed together in a single document.

Colour version	*Monochrome version*

The logo colours are:

Colour	CMYK-values	RGB-values	HTML-code	Remarks
'the blue'	88, 39, 0, 45	17, 86, 140	#11568C	Pantone© 647C
'the lime'	22, 0, 100, 0	199, 255, 0	#CFFF00	
'the green'	77, 0, 100, 0	0, 190, 0	#00BE00	

For professional printing, the CMYK or Pantone colours should be used. The RGB values and HTML codes are merely approximations and only suitable for cheap printing or screen use.

The logo should appear in the top right hand corner on all communication materials such as stationary, brochures and advertisements. Other locations are acceptable if required by the design of the materials. For example, on web pages it is usually better to place the logo flush left. To ensure its integrity and impact, always maintain a protective clear area around it.

The following are examples of unacceptable uses of the logo.

The logo may not be rotated.	*Wrong colour use.*

Unauthorised addition to the logo.	*Not distinguished from the background.*

CAcert.org is a community where anyone is permitted and encouraged to create materials for the benefit of the community. Permission is broadly given to registered users to use the CAcert logo to that end. However, such permission does not imply that you are a legal agent of CAcert.org in contract or similar terms, and you should not represent yourself as an agent. Use of the logo is subject to the normal dispute resolution rules of CAcert.

Note that use of the logo does not make a document 'official'. Every official document must be verified and approved by the CAcert Public Relations department.

The subtitle

Under the logo a subtitle may be placed to specify the use of the logo in specific situations, e.g., "Assurer", "Partner", or "Community". The subtitle should be placed centred under the logo unless it is very short, e.g., four letters or less. In that case it should be placed right aligned under the logo.

For *official* purposes, the subtitle should be written in an upright sans-serif type, using the blue colour, or black. As stated above, official purposes must be approved by the CAcert Public Relations department.

For *community* (unofficial) purposes, the subtitle should be written in an italic sans-serif type, using the green colour, or black.

Official logo	*Community used logo*

Text Usage

The only important rule is to write CAcert exactly the way it is shown here. Capital 'C', capital 'A', lower case 'cert'. Not 'cacert'. Not 'Cacert'. Not 'CACert'. Not 'CaCert' and so on. It's 'CAcert'.

If the CAcert *company* (the .Inc) is meant it must always be written as "CAcert.org". Do not leave out the ".org" in this situation.

If it fits in the design of the application, a sans-serif typeface like Vera Sans, Arial or Verdana should be used. CAcert encourages the use of open source typefaces like Vera and Liberation.

Style guide for documents

Stationery

By its very nature, stationery is the most personal and yet formal of all CAcert.org media. It is a key medium for communicating our position as a community based Certificate Authority.

Each time you mail a letter to a partner, hand a business card to a customer or send a memo to a colleague, you have an opportunity to impart the CAcert.org image. By using the elements of our corporate stationery system correctly and consistently, you help to reinforce the worldwide image of CAcert.org. No matter how innovative we are, we will never replace the personal touch of a hand-signed letter or a handwritten note of thanks.

Stationery is also our primary means of formal correspondence. Letters, for example, are often legally binding and memoranda are frequently used to document internal agreements.

CAcert will publish templates for stationery, brochures, logos, and guidelines on its web site. Together, your efforts and the guidelines will ensure that our stationery is always elegant, always consistent and always visually coherent.

Letterheads

Preferrably, letters should conform to ISO or local standards. The logo must be placed in the upper right corner of the first page. Subsequent pages may have the logo in the same location. Printed stationery should use the coloured version of the logo.

At the bottom of the first page, the official CAcert.org web adress must be included. If apporpriate, a local contact address of a CAcert representative may be added. [[also as the Root-Certificate Fingerprint implemented at the bottom of the pages. -- don't think this is useful]]. Subsequent pages may have the same bottom line.

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used.

For an example of a style conformant letter, see the appendix.

Business cards

Use the coloured version of the logo in the upper right corner.

The person name and function should be put under the logo, at the same *left* margin.

Bottom left, mirrored with regard to the logo, the contact information. This must include the official CAcert web side address.

For an example, see the appendix.

Reports and other information materials

Use the coloured version of the logo in the upper right corner of the pages. If mirrored pages are used, do not use the logo on the left pages.

On each page, add a footer with copyright notice, document name and page number.

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used.

At the end of the document, add an outstanding paragraph or section with full CAcert contact information and web site address.

This style guide may be considered to be an example document.

Memos

Use the logo in the upper right corner on the first page and, optionally, on subsequent pages.

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used.

Badges

Use the coloured version of the logo in the upper right corner. The “function” of the person should be under his/her name (e.g. “Assurer”). Following the contact information, the web address of the official CAcert web site must be included.

[[Also the CAcert.org root-cert fingerprint should be on the bottom. -- see earlier remark]]

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used.

For an example of a CAcert business card, see the appendix.

Presentations

Use the logo in the upper right or lower right corner. With a white (or nearly white) background, use the full-coloured logo, otherwise use the monochrome version of the logo.

At the bottom of each slide, the web address of the official CAcert web site must be included.

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used.

At the end of the presentation, add a slide with full CAcert contact information, web site, and root-cert fingerprint.

For some examples of presentation slides, see the appendix.

Brochures

Brochures differ very much, depending on subject and target. So only very general guidelines apply to brochures.

Most important:

Recruitment Advertisements, etc.

Use the logo in the upper right corner. Use the monochrome version of the logo unless you are sure that it will be reproduced correctly, e.g., in a glossy magazine.

If possible, a sans-serif typeface like Vera Sans, Arial or Verdana should be used. The CAcert ‘blue’ colour can be used for the text.

Signage

[[I don’t have the faintest idea what this section is supposed to mean]]

Signs are a vital part of the CAcert.org identity. They not only serve a practical purpose – identifying our sites and guiding users and visitors within them – they are also one of the most visible expressions of the CAcert.org brand. Great care has been taken to develop a

flexible system of signs which expresses the unique personality of CAcert.org in a unified, consistent way throughout the world.

It is recommend that all official use is signed by the person who write or build the document or other parts made for CAcert.Inc.

About CAcert

CAcert.org was founded in 2002 by Duane Groth. Its aim is to offer digital certificates for everyone, to stimulate confidence and safety consciousness in and around the Internet.

In 2003 CAcert became an Incorporated with seat in Australia and therefore is a registered non-profit organization.

For more information, visit the CAcert web site, http://www.cacert.org.

Updated versions of this document will be made available on the CAcert web site as described in the introduction.

The CAcert Root Certificate

All CAcert issued certificates are digitally signed by the CAcert Root Certificate. For certificate validation to work, the Root Certificate must be accessible to your software. Often this is the case, but sometimes it is necessary to manually install the CAcert Root Certificate. Instructions for this can be found on the CAcert web site.

The identitity of the Root Certificate can be verified with its *checksum*, also called *fingerprint*, *digest*, or *thumbprint*. Some software uses the so called MD5 algorithm to calculate this checksum, some software uses the SHA1 algorithm, some software uses both algorithms to calculate the checksum.

These are the checksums for the CAcert Root Certificate.

Algorithm	**Checksum as shown**
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

The checksums for the CAcert Root Certificate are included on many web sites and CAcert related documents. If you want to verify its identity, always consult several *independent* sources.

Appendix: Sample documents

Letterheads

CAcert
Squirrel Consultancy
Cadetlaan 6
7875 EB Exloo
☎ 0123-4567890
jvmmans@squirrel.nl

<First Name> <Last Name>
<Company>
<Street>
<City> <State> <ZIP/Postal Code>

Exloo, October 11, 2007

Subject: <Subject>

To Whom it May Concern

<Enter your text here>

Sincerely

Johan Vromans

Visit our web site at http://www.cacert.org

Business cards

Industry standard, 85 x 55 mm. White background, full colours.

Badges

Industry standard, 90 x 60 mm. White background, full colours.

Presentations

Introduction page

Typical content page

[[TODO: find out if the contrast of CAcert blue on grey is acceptable]]

Brochures

IN WELCHEN PROGRAMMEN KANN MAN CACERT ZERTIFIKATE EINBINDEN?

1. Client Zertifikate
In jedem Programm welches mit X.509 (S/Mime) Zertifikaten umgehen kann. Dazu gehören unter anderem

- Microsoft Outlook
- Adobe Acrobat
- OpenOffice

2. Server Zertifikate
Alle Serverprodukte, die mit SSL basierten Zertifikaten umgehen können.

Dazu gehören unter anderem

- Apache Webserver
- Microsoft Internet Information Server
- OpenSSL / OpenVPN

WAS MUSS ICH SONST NOCH WISSEN?

Alle Infos sind entweder unter www.cacert.org oder http://wiki.cacert.org zu finden.

Desweiteren gibt es einen IRC Chat

IRC Server: irc.cacert.org

Channel: #cacert (in English)
#cacert.ger (in deutsch)

Weitere Supportinfos:
http://wiki.cacert.org/wiki/GettingSupport

Für Spenden besuchen Sie bitte
http://www.cacert.org/index.php?id=13

CAcert.org
http://www.cacert.org
Support: irc.cacert.org #cacert oder #cacert.ger

For most software, the fingerprint is reported as:
A6:1B:37:5E:39:0D:9C:36:
54:EE:BD:20:31:46:1F:6B

Under MSIE the thumbprint is reported as:
135C EC36 F49C B8E9 3B1A
B270 CD80 8846 76CE 8F33

CAcert

- Client-Zertifikate
- Server-Zertifikate
- Web-Of-Trust
- Organisation-Assurance

SSL/TLS
S/MIME
OpenPGP
Code-Signing

CAcert
CAcert.org
http://www.cacert.org

CAcert
DIGITALE ZERTIFIKATE

WAS IST CACERT ?

CAcert.Inc ist ein Communitybasierter, eingetragenen Non-Profit Verein mit Sitz in Australien. Ziel ist der Betrieb eines kostenfrei arbeitenden Zertifizierungsdienste-Anbieters (CA) zur Ausstellung von elektronischen Zertifikaten nach dem X.509 Standard.
Die Anwendungsbereiche sind u.a. :

- Webserver mit HTTPS absichern
- Unterschreiben und Verschlüsseln von Emails
- SSL/TLS Serverprogramme
- Anmeldung bei Webseiten
- Anmeldung bei VPN´s
- digitales unterschreiben von selbst erstelltem Programmcode (z.B. Java)

CAcert.Inc will somit die OpenSource Philosophie auf die IT-Sicherheitswelt übertragen, und Sicherheit für jeden erschwinglich und verfügbar machen.

KOSTENLOSE E-MAIL UND SERVER ZERTIFIKATE

Wer seinen E-Mail-Verkehr und/oder (Web)Server mittels S/MIME digital signieren oder sicheren Zugriff auf seine Online-Präsenz über HTTPS anbieten möchte, braucht -- mitunter sehr teure -- X.509-Zertifikate. Er zahlt dafür, dass eine Firma diese sogenannte Trustcenter-Aufgaben wahrnimmt: Sie prüft, ob dem Kunden wirklich die Webseite oder die E-Mail-Adresse gehören (Identitätsüberprüfung). Dies kann je nach zu erwartendem Verwaltungsaufwand mehrere hundert Euro kosten.

WIE GEHT DAS MIT CACERT

Interessierte Personen müssen eigentlich im ersten Schritt nichts weiter tun als sich kostenfrei und ohne jede weitere Verpflichtung bei www.CAcert.org anzumelden. Anzugeben sind lediglich Ihre E-mail Adresse, Name und Geburtsdatum. In einem zweiten Schritt haben Sie z.B. bei Veranstaltungen oder auf Einzelanfrage die Möglichkeit sich beglaubigen zu lassen (Assurance) um Ihre Identität zu verifizieren. Danach können Sie Ihre eigenen Zertifikate über das gesicherte Webinterface ausstellen und weiterverwenden.

KOSTENLOSE PGP/GNUPG KEYSIGNING

Auch Ihren PGP/GnuPG Key können Sie innerhalb des CAcert Web-of-Trust beglaubigen lassen.

CODESIGNING

Wenn Sie Programmierer sind und Ihren Code als Ihren eigenen kennzeichnen und Ihn ebenso digital unterschreiben möchten ist dies auch möglich.

ORGANISATIONS ASSURANCES

Bei CAcert. Inc. können auch im Handelsregister eingetragene Gesellschaften, Kaufleute und Vereine ebenso wie Hochschulen, Städte, Gemeinden, Ämter und andere siegelführende Körperschaften und Gesellschaften des bürgerlichen Rechts von einem CAcert Organisations-Assurer abgenommen und beglaubigt werden.

WIESO SOLLTE MAN MITMACHEN?

Sicherheit:
Sie erhöhen Ihre eigene Sicherheit und den sichereren Umgang im täglichen Umfeld des Internets.

Authentisch: Andere können sich sicher sein, das Sie auch wirklich Sie selbst sind.

WIE KANN MAN MITMACHEN ?

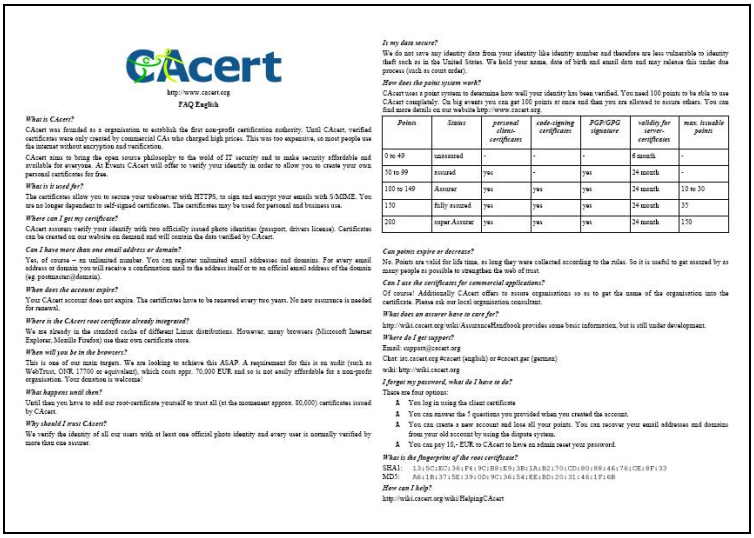
Sie können sich zum einen natürlich einen CAcert.org Account anlegen und aktiv Zertifikate zur Sicherstellung Ihrer Identität verwenden. Sie es im E-mail Verkehr, in Dokumenten oder auf Servern.

Desweiteren können Sie CAcert natürlich auch selbst aktiv als Assurer unterstützen und andere Leute assuren (Identitäten beglaubigen).

WAS KOSTET MICH NUN DAS GANZE?.

Dadurch, das der technische und organisatorische Teil getrennt ist und der organisatorische Teil von Freiwilligen und Interessierten übernommen wird, ist der administrative Aufwand sehr gering und somit werden hier keinerlei Kosten für Sie anfallen. Die Zertifikate kosten also rein garnichts.

CAcert Assurer



CAcert
http://www.cacert.org
FAQ English

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 world of IT security and to make security affordable and available for everyone. At Events CAcert will offer to verify your identity 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 dependant to self-signed certificates. The certificates may be used for personal and business use.

Where can I get my certificate?
CAcert assurers verify your identity 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 momement approx. 80.000) 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 99	assured	yes	-	yes	24 month	-
100 to 149	Assurer	yes	yes	yes	24 month	10 to 30
150	fully assured	yes	yes	yes	24 month	35
200	super Assurer	yes	yes	yes	24 month	150

Can points expire or decrease?
No. Points are valid for life time, so 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?
http://wiki.cacert.org/wiki/AssurancHandbook provides some basic information, but is still under development.

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:

- Yes 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/wiki/HelpingCAcert