CAcert Assurance Programme

Identity Verification Form (CAP) form

CAcert Inc. - P.O. Box 4107 - Denistone East NSW 2112 - Australia - http://www.cacert.org

CAcert Root Certificate ***class 1***: 135C EC36 F49C B8E9 3B1A B270 CD80 8846 76CE 8F33 ***class 3***: DB4C 4269 073F E9C2 A37D 890A 5C1B 18C4 184E 2A2D

The CAcert Assurance Programme (CAP) aims to verify the identities of Internet users through face to face witnessing of government-issued photo identity documents. The Applicant asks the Assurer to verify to the CAcert Community that the Assurer has met and verified the Applicant's identity against original documents. Assurer may leave a copy of the details with the Applicant, and may complete and sign her final form after the meeting. If there are any doubts or concerns about the Applicant's identity, do not allocate points. You are encouraged to perform a mutual Assurance.

For more information about the CAcert Assurance Programme, including detailed guides for CAcert Assurers, please visit: http://www.cacert.org

A CAcert Arbitrator can require the Assurer to deliver the completed form in the event of a dispute. After 7 years this form should be securely disposed of to prevent identity misuse, e.g. shred or burn the form. The Assurer does not retain copies of ID at all.

For the CAcert Organisation Assurance Programme there is a separate special COAP form.

Location (and event name) of the face-to-face meeting:

Applicant's Identity Information		points allocated
Exact full name on the ID	*type of ID shown*	max 35
Email address	*Date of Birth (yyyy-mm-dd)*	

Applicant's Statement

Make sure you have read and agreed with the CAcert Community Agreement (CCA)

☑ I hereby confirm that the information stating my Identity Information is both true and correct and request the CAcert Assurer (see below) to witness my identity in the CAcert Assurance Programme.

☑ I agree to the CAcert Community Agreement (CCA).

Date (yyyy-mm-dd) *Applicant's signature*

Assurer's Statement

Assurer's Name *Date of Birth (yyyy-mm-dd)*

Assurerś email address (optional)

☑ I, the Assurer, hereby confirm that I have verified the Applicant's Identity Information, I will witness the Applicant's identity in the CAcert Assurance Programme, and allocate Assurance Points.

☑ I am a CAcert Community Member, have passed the Assurance Challenge, and have been assured with at least 100 Assurance Points.

Date (yyyy-mm-dd) *Assurerś signature*

a Certificate Authority service for free certificates

"To create a community based, non-profit Certificate Authority."

CAcert is a Community which runs a Certificate Authority. Issued Individual and Organisation certificates are free of charge. CAcert is a non-profit and Open Source community based effort.

What are digital certificates about?

Digital certificates are used as an identity and security measurements in internet land. Digital certificates are standardized X.509 certificates.

Nearly all communication tools such as browsers and email clients and web servers support them. With these certificates, your software can encrypt documents for secure communication, to identify your counter party, and mark documents as securely coming from you.

Users such as banks may use them to send statements or transactions reports to you securely. Some tax departments can accept documents so prepared, and e.g. lawyers gain more security and privacy as well.

Browser users know "https" in URL address, and the little padlock icon. Technical people recognize TLS, SSL, and S/MIME as common protocols based on these certificates.

The certificate consists of two parts: a *private* encryption key part (kept on a safe place) and a public (key) part. The latter needs some mark from a certificate authority (CA) so that you really can say: "*yes this certificate is not a fake one it is really from me*".

E.g. so if a document is signed and/or is encrypted by the sender part of the certificate and/or you as receiver are able to decrypt it. And you know for sure it came from this sender with the help of this shown signing certificate.

If someone starts sending information encrypted with the identified certificate key one is sure that only the owner of the certificate can read that information. If both parties are using their certificate keys, one is sure that only those two are able to encypher the information. One is sure that the message came from that particular person.

Certificates are used for data identification (who is talking to me), for securing information and/or hiding (crypting) the information for third parties.

What is a Certificate Authority about?

A Certificate Authority (CA) issues certificates (your public key signed) when it has conducted some basic checks. Generally, the CA needs to know who you are and be sure that you personally are requesting this certificate to be signed by the CA.

CAcert uses a wide network of human Assurers who identify you (Web-of-Trust), check your name(s) and email address for on the certificate and make sure you agree to the CAcert Community Agreement (CCA).

Once these information has been sufficiently checked by CAcert, you

can issue CAcert certificates showing your checked name, issue domain certificates, do code signing, etc.

Why is CAcert so unique?

CAcert signs certificates free of charge, because we leverage our user base to do the certificate information function. This is called W*eb-of-Trust.*

Each user, once assured to a sufficient level (the 100 Assurance Points level), and has passed the Assurer Challenge will then help to assure other, newer users.

You can issue as many CAcert client and server certificates as you need: identification, email, system access, VPNs, secure web servers, host identification, etc. You can issue certificates with one of your own individual full names (the Certificate Assurances Programme) or with your organisation name (the Certificate Organisation Assurance Programme).

Why CAcert?

Commercial CAs may have their place for large corporations, but many people wish to use their free software to the fullest without being charged for each and every certification.

When users only want to secure personal emails or run local family photo websites, or small developers want to develop secure code for plugging into major applications like Firefox, CAcert is there with all the certificates they need: free of charge! CAcert certificates are provided unlimited in amounts, encryption strength, etc.

How is CAcert doing it?

Based on OpenSSL, PHP, MySQL, etc. CAcert has built not only a Certificate Authority which can verify your e-mail address or domain, but has built in a mechanism to expand the trust model beyond what some commercial CA's can provide, to prove your identity.

More than 150.000 (status of 2009) persons have joined the CAcert Community. More than 300.000 certificates were issued. More than 100.000 domains are using CAcert certificates to secure their web services. More than 5.000 free CAcert certificates are issued every month. 2.000 new persons are joining each month.

The CAcert Assurers are active all around the world to help you to get your free certificate.

How to sign up

Before signing up with CAcert read the Community Agreement (usage license, privacy measurements, arbitration, liability, security measurements, policies) from www.CAcert.org web site.
If you agree, click on 'Join'. In the first step of the registration process, you will be asked some questions. You are obliged to fill in the correct identification information. Read also the CAcert Privacy Statement.

To help you to re-identify you (e.g. password recovery) CAcert ask you to provide five questions/answers. For these questions, you can give arbitrary or bogus answers, as long as you are sure you can remember them!

Once you have completed the registration process, you will receive an "Email Ping" to your account email address. Follow the directions in that email to complete enrollment, and to enable your account with CAcert. Once enrolled, you can have CAcert issue you your first (temporary) certificate. However, instead of your name, "CAcert User Cert" will appear as 'Common Name' on the certificate. To have one of your full name

included in the certificate, you need to join the Assurance Program. A full name of an ID is included on the issued certificates as soon as you have reached the 50 Assurance Point level.

From then you can start requesting certificates for all email addresses you have registered.

How to get you assured? Individuals

For every assurance complete the CAcert Individual Assurance form (available from the CAcert web site), bring along at least one national ID with a photo (e.g. your passport, your ID card, your driver license).

Locate and make an appointment with a CAcert Assurer. The easiest way is on an event as conference, workshop, IT exhibition, etc.

The “in a hurry” way is to locate CAcert Assurers near you (see the web site) and make an appointment.

In this way you can collect *Assurance Points*. With two IDs you will collect at most 35 trust points from one Assurer. So you need minimal two Assurances for 50 Assurance Points.

With at least 100 Assurance Points and passing the Assurer Challenge (visit https://cats.cacert.org) you can immediately start to assure other people yourself.
If you made your assurance *before* you had “joined” CAcert, please create the CAcert account as soon as possible and immediately inform your Assurer that you did so.

Back at home
Start installing your free CAcert certificate into your browser, e-mail reader, code signing, time stamping of documents, etc. and start using the certificates for e-mail, for your server software, etc. And... upload the CAcert Root Certificate (see www.CAcert.org web page) into your browser and system.
And even better: start to widen the CAcert web of trust and use of certificates and start helping other CAcert users and support the CAcert Community force.

PGP key signing
You will also be able to exchange PGP public keys. E.g. CAcert Assurers once they have assured you, will also sign your PGP key. Be prepared and bring along your PGP fingerprint.

Organisations

If you are an organisation, you can have your organisation name on certificates as well. Your need to proof the legal status and identity of signing authorities of your organisation e.g. via the trade office register. The CAcert Organisation Assurance Programme will serve you for this.

After the organisation assurance you can issue free certificates via your system administrator (a CAcert Assurer), and issue server domain certificates.

You need more info?

All instructions for CAcert certificates are available from the web site www.CAcert.org. Do not hesitate to ask your questions, e.g. via the support email list cacert-support@lists.cacert.org.

Visit also http://wiki.cacert.org/wiki/ wiki pages. The wiki will explain in detail the “how to's”, e.g. deal with certificates, create them, have them signed, to install them, to maintain them, to recover passwords, to locate Assurers nearby you, to join the Community and to help to improve the services and support others.

Thanks for using CAcert!

Thanks for your support

 V2.1 Apr 2009/teus