CAcert assurer training

Rights, obligations, tasks

CAcert assurer training

Important notes

- This tutorial is part of CAcert's education campaign. Any usage beside this is only allowed with the permission of CAcert.
- If you have any improvement suggestions, remarks or questions, please contact us:
  - *Jens Paul*
    CAcert Education Officer
    edo@cacert.org
  - *CAcert Support Team*
    support@cacert.org
- Version:
  Version 1.0.0 [status: final version], dated 18 Apr 2007

CAcert assurer training

Agenda

1. Who is CAcert, what are digital certificates?
2. Requirements for becoming an assurer
3. Assurance process
4. Starting a local CAcert office
5. Support

1 - CAcert & digital certificates

Overview about CAcert, electronic signatures and digital certificates

CAcert assurer training

Definitions

Electronic signature

The electronic signature (sometimes referred as digital signature) is a generic term used for different forms of signatures.

In many countries there are signature laws. They usually define an electronic signature not as a writing attached to a document but instead as a digital seal containing a hash value of the signed data.

Digital certificate

Part of a digital certificate is a cryptographic key and some information about the owner of that key. This can be a person, company or institution (for example the certificate is used for signing emails, encrypting data or user authentication) or a machine (for example a web server using SSL).

In most cases, the digital certificate is the origin for creating an electronic signature.

CAcert assurer training

Elements of a digital certificate

Herausgegeben für

Allgemeiner Name (CN)	Jens Paul
Organisation (O)	<kein Teil des Zertifikats>
Organisationseinheit (OU)	<kein Teil des Zertifikats>
Seriennummer	02:A3:BA

Herausgegeben von

Allgemeiner Name (CN)	CA Cert Signing Authority
Organisation (O)	Root CA
Organisationseinheit (OU)	http://www.cacert.org

Validität

Herausgegeben am	05.09.2006
Läuft ab am	05.09.2007

Fingerabdrücke

SHA1-Fingerprint	CA:BB:B8:8D:F1:B1:9C:6E:B5:BC:E2:0C:B6:64:BF:89:AB:38:7C:59
MD5-Fingerprint	55:55:63:67:F2:27:73:5C:FB:E9:C4:17:B4:39:94:D4

- Information about the owner of the certificate
- Information about the certificate authority
- Electronic fingerprints for the validation of the certificate and the owner of the certificate.
- Issuing date and expiration date of the certificate

Public key

```
30 82 01 0a 02 82 01 01 00 b2 d8 fb 99 f5 07 a9
6e ee 2d 8a 97 c0 de 60 40 bb 64 a7 ec 04 b6 01
be 3c 5c 8e 41 8c d1 6f c6 bb 72 81 b7 15 52 dc
a2 fe 96 64 04 79 6c 88 01 94 21 74 63 55 cc c4
d8 07 46 60 45 93 65 d1 ce a6 b2 39 8a 9b b8 7d
49 7d 81 54 bb 20 07 95 b9 a1 86 37 d1 31 28 2b
0b 7a c1 c0 07 3b 96 6b 48 ab 25 0d 74 77 33 03
22 ae 6f fd 09 6b 6a 68 dd 4f 2b 5c 9d 7a 7f a9
17 50 fe 4c 3b 6f a5 fd b4 26 d8 16 b8 32 b3 ad
89 7b 27 14 d0 01 98 48 57 41 0d 9d fc 91 50 1c
83 ce 5c 95 ff 53 ff 13 40 bd 2c 6a e9 41 56 6a
c9 46 b2 51 87 94 55 39 1b 62 48 cb bb 10 a2 a8
0a 09 20 67 7c 7d 73 a6 79 72 6c 58 51 5c 5f 54
09 63 df a6 7e f3 0c a0 e0 07 ba 48 bf 3b 2f 4b
84 1d 7b fb 67 35 0d b0 51 77 fa 26 e6 5a 6f d8
f8 c6 ca dc 74 70 92 e1 66 52 88 8e c5 30 06 09
bb 33 d1 2c 4f 45 f1 61 27 02 03 01 00 01 11
```

Private key

...

- A public key which allows your communication partner to decrypt hash values of your signed mails and which allows him to encrypt mails he is sending to you.
- A private key which allows you the decryption of messages sent to you and which is needed to create the hash value in the signature of your outgoing mails.

CAcert assurer training

What are requirements for a digital certificate / for CA's in common?

Requirements (common, not limited to CAcert)

- For personal certificates, a CA should issue certificates with *sender@sender.com* and real name *Joe Average* in the certificate.
- The CA's should strive to be broadly recognized by the society and / or the government as trustworthy.
- The issuing organization should implement a process for ID checking (for example a personal meeting with ID check) to make sure that the identity of the applicant is without any doubt.
- The recipient of a message signed with a CA issued certificate should be able to control the trustworthiness of the certificate. This checking process has to be easy or even better it should be fully automated.

CAcert assurer training

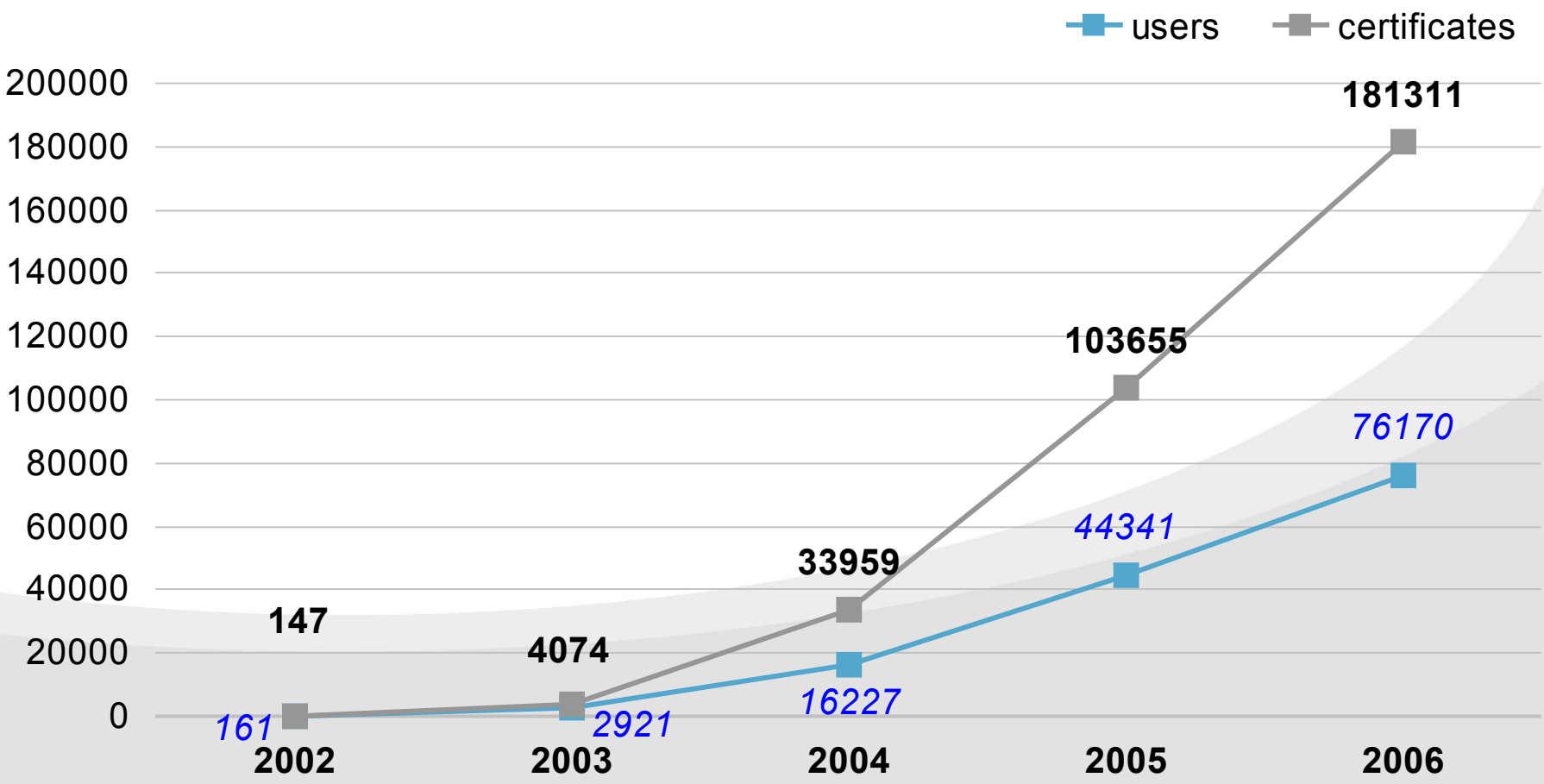
CAcert – the community's certificate authority

History of the Organization

- CAcert Inc. is a non profit organization located in Australia.
- CAcert provides free email-, server- and code-signing certificates.
- The project http://www.cacert.org/ was started in 2002; the organization CAcert Inc. was founded in 2003.
- The idea behind CAcert is, that we shouldn't be charged high amounts of money for security based on certificates which shouldn't cost the earth. We will never be able to reach the goal of secure environments and secure communication as long as only a fraction of all Internet users and companies can afford a digital certificate.
- The approach of commercial CA"s is to centralize both identity control and certificate issuing in one place. This approach is costly and combined with their goal to make profit leads to expensive certificates. CAcert splits the costly part of the assurance (ID check) from the management of the X.509 certificates and is therefore able to run on a small budget.
- The major goal of CAcert is to provide a life long user account with the ability to use as many certificates as you like without paying anything for it.

CAcert assurer training

Development of CAcert over the past years



CAcert assurer training

Certificate Usage

Definition

- CAcert serves as issuer of certificates for individuals, businesses, governments, charities, associations, churches, schools, non-governmental organizations or other groups. CAcert certificates are intended for low-cost community applications especially where volunteers can become Assurers and help CAcert to help the community.
- Types of Certificate and their appropriate and corresponding applications are defined in CAcert's CPS and CP:
  - http://www2.futureware.at/svn/sourcerer/CAcert/policy.htm
- Additional information is found within the CPS about prohibited applications.
- Specialist uses may be agreed by contract or within a specific environment, as described in the CPS.
- Note also the unreliability caveats in and risks, liabilities and obligations

CAcert assurer training

Types of certificates (according to CAcert CPS and CP)

Type		*Appropriate certificate uses*	
General	Protocol	Description	Comments
Server	TLS	Webserver encryption	Enables encryption
	Embedded	Embedded server authentication	Mailservers, IM-servers
Client	S/MIME	email encryption	*digital signatures* employed in S/MIME are not legal / human signatures, but instead enable the encryption mode of S/MIME
	TLS	Client authentication	The nodes must be secure
	TLS	Web based signature applications	The certificate authenticates only. See CPS.
	Advanced Signing	For document signature uses	only within a wider application such as mandated by regulations, as agreed by contract. See CPS.
Code		Code signing	Signatures on packages are indicative of Identity
PGP	OpenPGP	Key signing	Signatures on User Keys are indicative of Identity.

2 – Requirements for becoming an assurer

What are the requirements for becoming an assurer; what rights and obligations do I have?

CAcert assurer training

What are the requirements for becoming an assurer?

Requirements

Anyone interested in becoming an assurer, should meet these requirements:

- You can become an assurer even if you are still underage. But in that case you will be limited to grant a maximum of 10 points during an assurance process.
- You have to reach 100 assurance points before you can become an assurer (which means that a minimum of three assurers checked your identity).
- You need to take part in the assurer training and you have to successfully pass the assurer testing. You will then be certified to be a CAcert Assurer.
- Once an Assurer, you will need to keep up to date on policy updates.

CAcert assurer training

What rights do I have as an assurer?

Rights

As an CAcert assurer, you have several rights:

- You can issue every natural person (even underage persons) assurance points, up to the maximum you are currently allowed to (which means between 10 and 35), in order to help them getting assured. The process of an assurance is described in chapter 3 *assurance process* in detail.
- You are allowed to refuse issuing points to someone if you have any doubts about the identity of that person.
- You can always contact the CAcert headquarters if you encounter any problems during an assurance.
- You are allowed to use the title of *CAcert Assurer* and any logos associated to that title.

CAcert assurer training

What obligations do I have as an assurer?

Obligations

In addition there are also some obligations for CAcert assurers:

- You have to accept and act according to the current rules for accomplishing an assurance.
- You should ensure that your level of education in this field is up to date. Keep abreast for future training updates!
- You should thoroughly accomplish every assurance and refuse an assurance whenever you are unsure about someone's identity.
- You must keep the CAP forms of all assurances for seven years. If a form is requested by the headquarters (for example if there is a legal dispute), you must provide it to them.
- You should review the person's understanding of their rights and obligations within CAcert. You as Assurer will be on the front line of educating our registered members as to how CAcert works.

CAcert assurer training

Can I be made liable for my assurances?

Overview

There still is a vivid discussion about when and with what extent assurers can be made liable for there assurances. On the following pages you will find some examples which are kind of a consensus about that topic within the community.

We cannot answer the question “can I be made liable” for the different local law situations before there have been any court decisions which we hope to avoid at all.

In conclusion, we feel that if an assurer thoroughly accomplishes every assurance without any deliberate or roughly negligent behavior, there should not be any legal issues at all.

But the most important point is that at CAcert we aim to make the first court our court, and we aim to make this a complete and final court where we can. That’s why we have a dispute resolution policy. We will discuss this later …

CAcert assurer training

Can I be made liable for my assurances?

Scenario 1

The assurer did a good job. The documents were valid and the person is the correct one.

The assurer is not in danger because s/he did a good job.

Scenario 2

There were minor flaws. For example, the documents were recently expired, but the person is the correct one.

The assurer is confident that there hasn't been any damage and no one will complain. CAcert Assurers will be liable towards other CAcert registered users within our internal jurisdiction of Dispute Resolution.

CAcert assurer training

Can I be made liable for my assurances?

Scenario 3

The assurer really tried to do a good job but was presented forged documents of good quality.

CAcert as an association, and on behalf of all registered users, disclaims all liability to Non-related-persons (NRP's). That means, although you may become liable in a court of law, our position is that you disclaim all liability to the extent possible, and you can draw on the resources of CAcert to help in this mission.

Scenario 4

The assurer did a bad job. For example s/he assured someone without checking the documents or the documents presented were obviously forged.

This is a case of gross negligence which usually makes you liable for damage which resulted from this action. Probably CAcert will take action of its own against that person to prevent them from corrupting the database any further.

CAcert assurer training

Can I be made liable for my assurances?

Scenario 5

The assurer knowingly made a false assurance either because of a joke (“Ah, he just wanted to pull a joke on someone”) or with criminal intensions.

No one can prevent liability for deliberate actions. You are always liable for any criminal behavior, which automatically belongs to the normal courts of the land. But, we aim to make the first court our court, and we aim to make this a complete and final court where we can.

CAcert assurer training

How can we solve disputes?

Dispute resolution policy (interim)

There is an (interim) dispute resolution policy and rules for CAcert. Disputes arising out of operations by CAcert and interactions between users may be addressed through this policy. You'll find it at:

http://www2.futureware.at/svn/sourcerer/CAcert/dispute_resolution.html

Basically anyone can file a dispute if needed (they become *Claimants*) and send it to the normal support channel of CAcert, then a *Case Manager* takes control of the filing and selects an *Arbitrator* to deal with that dispute. After a quick phase of conducting some preliminaries, the *Arbitrator* moves on towards *Jurisdiction*. He establishes the facts (collecting evidence, getting support or informations), apply the rules of the CPS and the governing law and makes a considered *Ruling*.

For a more detailed view, please check the policy.

3 – Assurance process

What is the process of assuring people? What is the point pattern? What are typical mistakes?

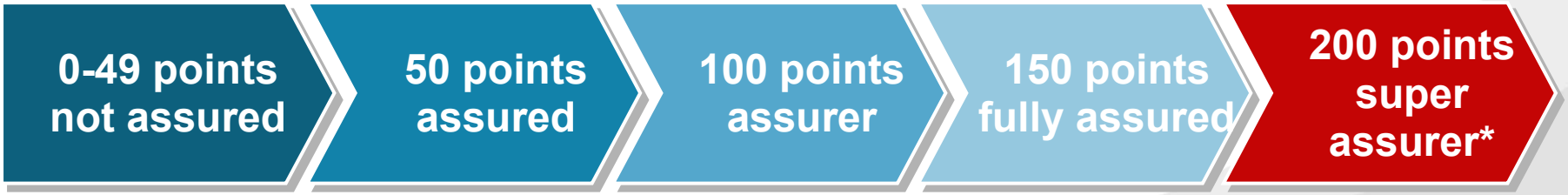
CAcert assurer training

What is our point system?

- Name is not included in any certificate.
- You can get client and server certificates (valid for 6 months).

- Maximum number of points you can get by assurances from CAcert Assurers.
- You can apply for a code-signing certificate.
- You can attend an assurer training.

- Used for mass assurances on big events or in *new* areas.
- Temporary status.
- Two board members must agree to that status.



- Full name is included in the certificate.
- Server certificate is valid for 24 months.
- PGP/GPG key can be signed by CAcert.

- Maximum number of points you can reach via TTP or by assuring other people.
- As an assurer, you can now issue the maximum of 35 points.

*not available in all countries anymore (for example: Germany)

CAcert assurer training

How many points can I issue?

As soon as you've reached 100 points and passed the assurer training, you are allowed to accomplish you own assurances. With every assurance made you get an additional 2 points, up to a maximum of 150 points.

Depending on your points total you can issue the following number of points:

from 100 points: 10 points max
from 110 points: 15 points max
from 120 points: 20 points max
from 130 points: 25 points max
from 140 points: 30 points max
from 150 points: 35 points max

Exception: underage assurers can issue a maximum of 10 points.

CAcert assurer training

Short representation of an assurance

Preparation

- Print forms
- Take some ballpoint pens with you!
- Agree to a personal meeting or take part in an event.

Assurance

- The applicant should fill out 2 forms (or more if needed) if he has not printed them pre-filled.
- Check all data in the form.
- Check the applicants ID(s).

Transferring points

- Go to http://www.cacert.org/ and log in. Go to the topic *CAcert Web of Trust* and then *assure someone*.
- Insert applicant's e-mail and complete the form.
- Logout and close your browser window.

After the meeting

- If you assured someone without a CAcert account: check if he / she already created one and transfer the points you issued.
- Keep the forms for 7 years.
- If there have been any doubts, please contact headquarters.

CAcert assurer training

Detailed description of the assurance process:

-1- Preparation

- If the applicant forgot to print his pre-filled forms or if you are assuring people new to CAcert (for example during a big event) you should always have some neutral forms ready. Direct document link: http://www.cacert.org/cap.php
- Especially during events the applicants often do not have a ballpoint pen with them, so you should bring some (better: a lot) of them with you. Maybe there is a friendly company in the booth across to help you out …
- Please read the rules for the assurance process again!

CAcert assurer training

Detailed description of the assurance process:

-2- Assurance

- The applicant should fill out 2 forms (or more if needed) if he has no pre-filled ones with him.
- The assurer has to check the following:
  - Is the form completely filled out (people like to forget the date or their signature)?
  - Is the name, birth date and signature on the form identical to those on the presented ID card (please read the following page for more information)?
  - Is the e-mail address clearly legible? You need to type it into the system later, so if there is any doubt write it again in uppercase letters.
- Write down which kind of ID you checked, but do not write down any numbers!
- Issue assurance points (there are some pages within this presentation which help you decide if you should issue the maximum number of points or not).
- Insert your name and date and sign the form. Keep it!

CAcert assurer training

Detailed description of the assurance process:

-2- Assurance

ID-checking

- You have to check at least one ID (passport, drivers license), but it is recommended to check two.
- Student ID, bank cards, membership cards, … can be used to strengthen an identity check, but they cannot substitute an official ID.
- Please check:
  - *Picture* (Expect old pictures especially if their is no expiration date of the ID (i.e.: German driver license). If you are not sure about the picture, ask for another ID!
  - *Signature* (If there is a big difference between the signature on the ID and the one on the form, ask the applicant to sign somewhere in the same way as he signed the ID.

CAcert assurer training

Detailed description of the assurance process:

-2- Assurance

- Please check:
  - *Security characteristics*
    - Is the picture and the ID officially stamped (if necessary in your country)?
    - Hologram
    - Printing Style
    - Stamp marks (was the picture substituted?)
    - If there is a machine-readable part? Is the information there identical to the written ones above?
  - *Date of birth*
    - Is it plausible?
    - Please remember that there is a difference between the way you write a date for example in some parts of the world (2007-01-20) and in Germany (20.01.2007).
    - There is no minimum age for an assurance, but 1 year olds usually can't walk, and 200 year olds … well …

CAcert assurer training

Detailed description of the assurance process:

-2- Assurance

- Please check:
  - *Expiration date*
    - There might be no expiration date for the driver's license in some countries, but there is always one on the passport.
    - Expired documents can be used to strengthen the identity check, but they are worth less than a valid ID.
    - Please inform the applicant that the document has expired.
    - Is the difference between expiration date and issuing date logical (for example 10 years)?
  - *Other things*
    - Please watch out for people who are born in 2007 or signed the form in 1970...
  - *Ask Questions*
    - Date of birth, place of birth
    - Eye color (yeeees, you are allowed to look in their eyes …)
    - Artist name or nickname if part of the ID in your country.

CAcert assurer training

Detailed description of the assurance process:

-2- Assurance

Issuing points

Issue points on your own estimate. But consider:

- Do I know the identity of that person?
- Could the ID's shown prove that identity 100%?
- Have all documents been valid or have some expired?
- Do I have any doubts about the picture or the signatures?
- If there are any doubts, issue less points. If there are no doubts, issue the maximum points you can.
- If you have extreme doubts:
  - Let the applicant fill out the form.
  - Check the ID and **only** in this case, write down the numbers.
  - Keep the form and send it immediately to CAcert headquarters for further investigation!
  - Tell them what happened in detail!

CAcert assurer training

Detailed description of the assurance process:

-3- Transferring points

- You can directly transfer the points or at the end of the business day, after the event,… but within reason.
- Use a secure environment free of viruses, worms, … If you are not sure about that use a live CD (i.e. Knoppix).
- Start a new browser session. Go to http://cacert.org and use *password login*.
- Type your e-mail and password.
- Go to the topic *CAcert Web of Trust* and then *assure someone*.
- Insert the applicant's e-mail and complete the form. You only need to insert the date if the meeting took place on another date.
- When you are finished, log out and close your browser session for security purposes.

CAcert assurer training

Detailed description of the assurance process:

-4-
After the meeting

- If you assured someone without a CAcert account: check if he / she already created one and transfer the points you issued. Maybe you have to come back a couple of times during the next few days after the event.
- Mark the forms as *completed* after you transferred the points.
- Please remember to keep the forms for seven years. You are personally responsible for that!
- If you have any doubts, please contact headquarters. It that case, you will need to mail / fax the form.

CAcert assurer training

In which cases should you issue the maximum number of points?

Overview

In general, the rule is that you should only assure people with an identity check free of any doubts. In reality there are often minor flaws (old picture, expired documents, …) which can make you uncertain about the assurance.

Although there is no official ID checking policy (yet?), the following ideas can help you decide if you should issue the maximum number of points or not.

This is just one idea. Feel free to think about your own personal proceeding.

CAcert assurer training

In which cases should you issue the maximum number of points?

(A) Identity check

- **Positive**
  - Every ID (passport, drivers license, …) if name and date of birth matches those on the form.
- **Negative**
  - If the picture cannot be matched with the applicant (old picture, major change of the appearance, …).
  - If the signature on the ID does not match exactly with that on the form.
  - If the ID has expired or the security characteristics are damaged.
  - If there are any doubts about the date of birth, for example, the applicant seems to be much younger / older than you could expect by the date of birth.

CAcert assurer training

In which cases should you issue the maximum number of points?

(B) Strengthen the ID

- **Positive**
  - Every student ID, bank card presented, which is valid and matching the name and signature on the form.
  - If at least one of those cards has a matching picture.
  - If the applicant can show several membership cards.

CAcert assurer training

In which cases should you issue the maximum number of points?

(C) Fraud suspicion

- **Negative**
  - If the applicant behaves erratically, tells you to hurry because he has no time, …
  - If the applicant tried to push back a document (passport, drivers license, credit card, …) which could not pass your check. It is possible that this document is not genuine or is stolen.

CAcert assurer training

In which cases should you issue the maximum number of points?

(D) Special situations

- **Positive**
  - If it is your initiative to get someone to a CAcert booth during an event. You cannot expect that the applicant was prepared for that.
  - If the assurer convincingly assures that he could not expect the need of multiple IDs, for example because he did not know anything about CAcert before the event, …
  - If you meet the applicant at his workplace and minimum of two colleagues present can confirm his identity.
  - If the applicant is a child and one of his parents can show a valid ID containing the same name.
  - If the assurer is a long time friend of the applicant (remember: this is only a positive aspect and not a substitution for the checking process!).

4 – Starting a local CAcert office

If you are interested in starting a local CAcert office, which requirements should be met?

CAcert assurer training

CAcert office – what is the idea behind it?

Objective

Sometimes it can be pedantically and time consuming for an applicant to contact two different assurers, agree to a meeting date and drive to that meeting. Many potential applicants are not willing to make that effort *just* to get a certificate.

Therefore it is our objective to give those applicants some more service. A CAcert office is a place with regulated opening times where you can meet a minimum of two assurers, which means you can get assured with just one visit.

It doesn't matter if the office is placed at an existing organization or it is a temporary place (i.e. at the local university or even a pub). More important is the fact that the opening times are regulated.

CAcert assurer training

CAcert office – what are the requirements to start?

Requirements

- During opening hours there should always be a minimum of two assurers on staff.
- The Assurers on staff should have some experience in assuring people. To get some experience it is a good idea to assure your family, friends or colleagues or to attend a larger CAcert event.
- You should publicize your opening hours and location on http://www.cacert.org/. All changes should be reported to headquarters in a timely manner.

CAcert assurer training

CAcert office – Which data should you provide?

Data	Example
▪ Opening hours ▪ Address ▪ Phone number, mobile ▪ e-mail ▪ Travel advice	**CAcert Office Pirmasens** c/o Paul-Datenverarbeitung GmbH Carl-Schurz-Straße 21-23 66953 Pirmasens GERMANY Tel. +49 (6331) 5192-0 e-mail: cacert@canyonsport.de Opening hours: Mo-Do 9:00-12:00, 13:30-16:00 Assurer: Jens Paul, Eckhard Köhler, Marc Henkel, Michelle Stahl, Uwe Lieberknecht Travel advice: The office is located in the commercial area „Husterhöhe“, opposite the university. You can find a driving sketch at http://www.paul-dv.de/anfahrt

CAcert assurer training

CAcert office – Can you charge for the assurance?

Prices

- CAcert certificates are always free of charge. After a successful assurance the applicant can get them on line.
- If assurer and applicant have not agreed to a charge before the meeting, than the assurance process must be free of charge. But it is possible that the Assurer asks for a small fee before the meeting (to cover his time, travel costs, …).
- We encourage you not to charge anything, but if you feel that it is necessary to cover your time, travel expenses or something else, you are allowed to charge something.
- There is no limit, maximum charge or anything like that because for example the ‘time value’ is specific to every single place on earth. But please, stay within reasonable borders …

CAcert assurer training

CAcert office – Can you charge for the assurance?

Prices

- If you are assuring students, regular customers (if you are running a business) it is a good idea to lower your prices.
- If you are assuring at a big event you should work free of charge if possible.
- Please do not charge for a VIP assurance! A VIP assurance is for persons which are important to CAcert. If there is an upcoming VIP assurance you will be informed by CAcert in advance who is coming. Please help to make that person feel comfortable and make the assurance as easy as possible. But still, be extremely careful with the assurance process. Bad VIP assurances could be fatal for CAcert!

5 – Support

How can you get support? Who are the people you may contact?

CAcert assurer training

I need help! Where can I get support?

Support

- Use the support form at http://www.cacert.org/ (direct link to the form: http://www.cacert.org/index.php?id=11).
- Join our mailing lists: http://lists.cacert.org/cgi-bin/mailman/listinfo
- Read the wiki, then read it again: http://wiki.cacert.org/
- Contact us using IRC:
  - irc://irc.CAcert.org/CAcert (english)
  - ircs://irc.cacert.org:7000/CAcert (english secure)
  - irc://irc.cacert.org/cacert.ger (german)
  - ircs://irc.cacert.org:7000/cacert.ger (german, secure)
  - irc://irc.cacert.org/cacert.fr (french)
  - ircs://irc.cacert.org:7000/cacert.fr (french secure)

CAcert assurer training

I need help! Where can I get support?

Support

- Write to CAcert:
  CAcert Inc. Headquarters
  P.O. Box 81
  2216 Banksia/NSW
  AU - Australia
- And don't forget: Use all available training possibilities offered and attend upcoming update sessions!

Any questions?

Just ask. We are here to answer them!