Assurance Policy for CAcert Community Members

Editor: Teus Hagen
Creation date: 2008-05-30
Last change by: Iang
Last change date: 2009-01-08
Status: POLICY p20090105.2

0. Preamble

0.1. Definition of Terms

Member
: A Member is an individual who has agreed to the CAcert Community Agreement (CCA) and has created successfully a CAcert login account on the CAcert web site.

Assurance
: Assurance is the process by which a Member of CAcert Community (Assurer) identifies an individual (Assuree).

Prospective Member
: An individual who participates in the process of Assurance, but has not yet created a CAcert login account.

Name
: A Name is the full name of an individual.

Secondary Distinguishing Feature
: An additional personal data item of the Member that assists discrimination from Members with similar full names. (Currently this is the Date of Birth (DoB).)

0.2. The CAcert Web of Trust

In face-to-face meetings, an Assurer allocates a number of Assurance Points to the Member being Assured. CAcert combines the Assurance Points into a global *Web-of-Trust* (or "WoT").

CAcert explicitly chooses to meet its various goals by construction of a Web-of-Trust of all Members.

0.3. Related Documentation

Documentation on Assurance is split between this Assurance Policy (AP) and the Assurance Handbook. The policy is controlled by Configuration Control Specification (CCS) under Policy on Policy (PoP) policy document regime. Because Assurance is an active area, much of the practice is handed over to the Assurance Handbook, which is not a controlled policy document, and can more easily respond to experience and circumstances. It is also more readable.

See also Organisation Assurance Policy (OAP) and CAcert Policy Statement (CPS).

1. Assurance Purpose

The purpose of Assurance is to add confidence in the Assurance Statement made by the CAcert Community of a Member.

With sufficient assurances, a Member may: (a) issue certificates with their assured Name included, (b) participate in assuring others, and (c) other related activities. The strength of these activities is based on the strength of the assurance.

1.1.The Assurance Statement

The Assurance Statement makes the following claims about a person:

1. The person is a bona fide Member. In other words, the person is a member of the CAcert Community as defined by the CAcert Community Agreement (CCA);

2. The Member has a (login) account with CAcert's on-line registration and service system;

3. The Member can be determined from any CAcert certificate issued by the Account;

4. The Member is bound into CAcert's Arbitration as defined by the CAcert Community Agreement;

5. Some personal details of the Member are known to CAcert: the individual Name(s), primary and other listed individual email address(es), secondary distinguishing feature (e.g. DoB).

The confidence level of the Assurance Statement is expressed by the Assurance Points.

1.2.Relying Party Statement

The primary goal of the Assurance Statement is for the express purpose of certificates to meet the needs of the *Relying Party Statement*, which latter is found in the Certification Practice Statement (CPS).

When a certificate is issued, some of the Assurance Statement may be incorporated, e.g. Name. Other parts may be implied, e.g. Membership, exact account and status. They all are part of the *Relying Party Statement*. In short, this means that other Members of the Community may rely on the information verified by Assurance and found in the certificate.

In particular, certificates are sometimes considered to provide reliable indications of e.g. the Member's Name and email address. The nature of Assurance, the number of Assurance Points, and other policies and processes should be understood as limitations on any reliance.

2. The Member

2.1. The Member's Name

At least one individual Name is recorded in the Member's CAcert login account. The general standard of a Name is:

- The Name should be recorded as written in a government-issued photo identity document (ID).

- The Name should be recorded as completely as possible. That is, including all middle names,

any titles and extensions, without abbreviations, and without transliteration of characters.

- The Name is recorded as a string of characters, encoded in unicode transformation format.

2.2. Multiple Names and variations

In order to handle the contradictions in the above general standard, a Member may record multiple Names or multiple variations of a Name in her CAcert online Account. Examples of variations include married names, variations of initials of first or middle names, abbreviations of a first name, different language or country variations, and transliterations of characters in a name.

2.3. Status and Capabilities

A Name which has reached the level of 50 Assurance Points is defined as an Assured Name. An Assured Name can be used in a certificate issued by CAcert. A Member with at least one Assured Name has reached the Assured Member status. Additional capabilities are described in Table 1.

Table 1: Assurance Capability

Minimum Assurance Points	*Capability*	*Status*	*Comment*
0	Request Assurance	Prospective Member	Individual taking part of an Assurance, who does not have created a CAcert login account (yet). The allocation of Assurance Points is awaiting login account creation.
0	Request unnamed certificates	Member	Although the Member's details are recorded in the account, they are not highly assured.
50	Request named certificates	Assured Member	Statements of Assurance: the Name is assured to 50 Assurance Points or more
100	Become an Assurer	Prospective Assurer	Assured to 100 Assurance Points (or more) on at least one Name, and passing the Assurer Challenge.

A Member may check the status of another Member, especially for an assurance process. Status may be implied from information in a certificate. The number of Assurance Points for each Member is not published.

The CAcert Policy Statement (CPS) and other policies may list other capabilities that rely on Assurance Points.

3. The Assurer

An Assurer is a Member with the following:

- Is assured to a minimum of 100 Assurance Points;

- Has passed the CAcert Assurer Challenge.

The Assurer Challenge is administered by the Education Team on behalf of the Assurance Officer.

3.1. The Obligations of the Assurer

The Assurer is obliged to:

- Follow this Assurance Policy;
- Follow any additional rules of detail laid out by the CAcert Assurance Officer;
- Be guided by the CAcert Assurance Handbook in their judgement;
- Make a good faith effort at identifying and verifying Members;
- Maintain the documentation on each Assurance;
- Deliver documentation to Arbitration, or as otherwise directed by the Arbitrator;
- Keep up-to-date with developments within the CAcert Community.

4. The Assurance

4.1. The Assurance Process

The Assurer conducts the process of Assurance with each Member.

The process consists of:

1. Voluntary agreement by both Assurer and Member or Prospective Member to conduct the Assurance;
2. Personal meeting of Assurer and Member or Prospective Member;
3. Recording of essential details on CAcert Assurance Programme form;
4. Examination of Identity documents by Assurer and verification of recorded details (the Name (s) and Secondary Distinguishing Feature, e.g., DoB);
5. Allocation of Assurance Points by Assurer;
6. Optional: supervision of reciprocal Assurance made by Assuree (Mutual Assurance);
7. Safekeeping of the CAcert Assurance Programme (CAP) forms by Assurer.

4.2. Mutual Assurance

Mutual Assurance follows the principle of reciprocity. This means that the Assurance may be two-way, and that each member participating in the Assurance procedure should be able to show evidence of their identity to the other.

In the event that an Assurer is assured by a Member who is not certified as an Assurer, the Assurer supervises the Assurance procedure and process, and is responsible for the results.

Reciprocity maintains a balance between the (new) member and the Assurer, and reduces any sense of power. It is also an important aid to the assurance training for future Assurers.

4.3. Assurance Points

The Assurance applies Assurance Points to each Member which measure the increase of confidence in the Statement (above). Assurance Points should not be interpreted for any other purpose. Note that, even though they are sometimes referred to as *Web-of-Trust* (Assurance) Points, or *Trust* Points, the meaning of the word 'Trust' is not well defined.

Assurance Points Allocation
An Assurer can allocate a number of Assurance Points to the Member according to the Assurer's experience (Experience Point system, see below). The allocation of the maximum means that the Assurer is 100% confident in the information presented:

- Detail on form, system, documents, person in accordance;
- Sufficient quality identity documents have been checked;
- Assurer's familiarity with identity documents;
- The Assurance Statement is confirmed.

Any lesser confidence should result in less Assurance Points for a Name. If the Assurer has no confidence in the information presented, then *zero* Assurance Points may be allocated by the Assurer. For example, this may happen if the identity documents are totally unfamiliar to the Assurer. The number of Assurance Points from *zero* to *maximum* is guided by the Assurance Handbook and the judgement of the Assurer. If there is negative confidence the Assurer should consider filing a dispute.

Multiple Names should be allocated Assurance Points independently within a single Assurance.

A Member who is not an Assurer may award an Assurer in a reciprocal process a maximum of 2 Assurance Points, according to her judgement. The Assurer should strive to have the Member allocate according to the Member's judgement, and stay on the cautious side; the Member new to the assurance process should allocate *zero* Assurance Points until she gains some confidence in what is happening.

In general, for a Member to reach 50 Assurance Points, the Member must have participated in at least two assurances, and at least one Name will have been assured to that level.

To reach 100 Assurance Points, at least one Name of the Assured Member must have been assured at least three times.

The maximum number of Assurance Points which can be allocated for an Assurance under this policy and under any act under any Subsidiary Policy (below) is 50 Assurance Points.

4.4. Experience Points

The maximum number of Assurance Points that may be awarded by an Assurer is determined by the

Experience Points of the Assurer.

Table 2: Maximum of Assurance Points

Assurer's Experience Points	*Allocatable Assurance Points*
0	10
10	15
20	20
30	25
40	30
>=50	35

An Assurer is given a maximum of 2 Experience Points for every completed Assurance. On reaching Assurer status, the Experience Points start at 0 (zero).

Less Experience Points (1) may be given for mass Assurance events, where each Assurance is quicker.

Additional Experience Points may be granted temporarily or permanently to an Assurer by CAcert Inc.'s Committee (board), on recommendation from the Assurance Officer.

Experience Points are not to be confused with Assurance Points.

4.5. CAcert Assurance Programme (CAP) form

The CAcert Assurance Programme (CAP) form requests the following details of each Member or Prospective Member:

- Name(s), as recorded in the on-line account;
- Primary email address, as recorded in the on-line account;
- Secondary Distinguishing Feature, as recorded in the on-line account (normally, date of birth);
- Statement of agreement with the CAcert Community Agreement;
- Permission to the Assurer to conduct the Assurance (required for privacy reasons);
- Date and signature of the Assuree.

The CAP form requests the following details of the Assurer:

- At least one Name as recorded in the on-line account of the Assurer;
- Assurance Points for each Name in the identity document(s);
- Statement of Assurance;

- Optional: If the Assurance is reciprocal, then the Assurer's email address and Secondary Distinguishing Feature are required as well;
- Date, location of Assurance and signature of Assurer.

The CAP forms are to be kept at least for 7 years by the Assurer.

5. The Assurance Officer

The Committee (board) of CAcert Inc. appoints an Assurance Officer with the following responsibilities:

- Reporting to the Committee and advising on all matters to do with Assurance;
- Training and testing of Assurers, in association with the Education Team;
- Updating this Assurance Policy, under the process established by Policy on Policy (PoP);
- Management of all Subsidiary Policies (see below) for Assurances, under Policy on Policy;
- Managing and creating rules of detail or procedure where inappropriate for policies;
- Incorporating rulings from Arbitration into policies, procedures or guidelines;
- Assisting the Arbitrator in any requests;
- Managing the Assurer Handbook;
- Maintaining a sufficient strength in the Assurance process (web-of-trust) to meet the agreed needs of the Community.

6. Subsidiary Policies

The Assurance Officer manages various exceptions and additional processes. Each must be covered by an approved Subsidiary Policy (refer to Policy on Policy => CAcert Official Document COD1). Subsidiary Policies specify any additional tests of knowledge required and variations to process and documentation, within the general standard stated here.

6.1. Standard

Each Subsidiary Policy must augment and improve the general standards in this Assurance Policy. It is the responsibility of each Subsidiary Policy to describe how it maintains and improves the specific and overall goals. It must describe exceptions and potential areas of risk.

6.2. High Risk Applications

In addition to the Assurance or Experience Points ratings set here and in other subsidiary policies, the Assurance Officer or policies can designate certain applications as high risk. If so, additional measures may be added to the Assurance process that specifically address the risks.

Additional measures may include:

- Additional information can be required in process of assurance:

    - unique numbers of identity documents,
    - photocopy of identity documents,
    - photo of User,
    - address of User.

    Additional Information is to be kept by Assurer, attached to CAcert Assurance Programme (CAP) form. Assurance Points allocation by this assurance is unchanged. User's CAcert login account should be annotated to record type of additional information;

- Arbitration:

    - Member to participate in Arbitration. This confirms their acceptance of the forum as well as trains in the process and import,
    - Member to file Arbitration to present case. This allows Arbitrator as final authority;
- Additional training;

- Member to be Assurer (at least 100 Assurance Points and passed Assurer Challenge);

- Member agrees to additional specific agreement(s);

- Additional checking/auditing of systems data by CAcert support administrators.

Applications that might attract additional measures include code-signing certificates and administration roles.

7. Privacy

CAcert is a "privacy" organisation, and takes the privacy of its Members seriously. The process maintains the security and privacy of both parties.

Information is collected primarily to make claims within the certificates requested by users and to contact the Members. It is used secondarily for training, testing, administration and other internal purposes.

The Member's information can be accessed under these circumstances:

- Under Arbitrator ruling, in a duly filed dispute (Dispute Resolution Policy => COD7);

- An Assurer in the process of an Assurance, as permitted on the CAcert Assurance Programme (CAP) form;

- CAcert support administration and CAcert systems administration when operating under the authority of Arbitrator or under CAcert policy.