final, 05/11/08

CAcert Inc.
Annual General Meeting 2008
Association Board Report

Prologue

"trust comes with the speed of snail mail, and leaves with the speed of email"

CAcert services are based on a *Web of Trust* that is built from Assurance of the identity of individuals and organisations: "*are you who you say you are?*" In addition to human checks, CAcert verifies technical information about those legal entities: e.g. email address, and domain name: "*does this domain belong to that entity?*" We verify the information so that we can rely on it: this is building real trust.

The Assurance of the full name is done by an experienced Assurer, a special class of Community Members. In this respect CAcert differs dramatically from other Certificate Authorities, who generally use a (yearly) fee for the same basic notion: "*does this issued certificate really belongs to this person or organisation?"*

CAcert seeks trust, and wants to earn that trust fairly! Our standard and our commitment is to be fully transparent and fully open. We fully support, allow and promote individual freedom. We strive for technical openness (open source, standard tooling), state of the art and proven security and innovative governance. The message for the future of CAcert is clear: use our community and security advantages to build trust in our certificates. CAcert Inc. works to defend that trust because it is an association of members; you can't buy your way in.

This open, community-based and conceptually free approach to building and running a Certification Authority is not however without its costs: It is complex. It is slow, it is intensive, and it is hard to achieve real "*trust*".

Trust itself is a psychological phenomenon, usually and conventionally the easiest to be obtained via financial measurements and the lack of published events in the history.

Indeed, scientific research often indicates that many choices of the CAcert Community are counter productive! I have to hand a recent book, *The Trust Crisis* that seeks to explain the ingredients we need [1]:

1. More individual freedom creates less trust;
2. More transparency gives less trust (the sendmail Open Source problem);
3. The requirement for full control is counter-productive to trust (the long lists of requirements for a CA);
4. More security results in less trust (passwords, keys, ...);
5. The more checking, the less the trust (lock icon, exactness of name);
6. More choices gives less trust (Extended Validation);
7. More secularization provides less trust (the claiming culture).

The social psychologist Prof Hans Boutillier of Free University in Amsterdam, describes it in his scientific articles as follows: "*The network community on one side demands more trust, but on the other side has a big need for more supervision and control.*"

With its Web of Trust concept, built from Assurance, and with a high level of technical verification, CAcert has very strong and unique tools to support the *trust* in its issued certificates. The challenge is to defend this and get it accepted in a world which is

accustomed to other more commercially-driven proposals. Open Source finds full acceptance today, yet it started in the 1980s.. CAcert started in July 2003, from the initiative of founder Duane Groth. We face a major step and a major challenge: to get CAcert accepted as CA within the commercial world. The audit project to take us forward into the browsers has this year, 2008, been awarded a basic level of funding from Stichting NLnet, but it remains driven forward by a dozen of volunteers of a high level of expertise. CAcert is freely available for everyone and it strives to earn your trust; likewise we need your support. Help us to complete the process, any way you can.

Teus Hagen, President.

Some facts and figures about CAcert

The growth of CAcert Community and certificate usage has been very stable over the last 4 years: 8000 certificates issued per month, 2200 new Community Members per month, 2000 new Assurers per year. There are now 10.000 Assurer candidates world wide. The coverage of Assurers is getting there, so the need to assign Super Assurer status is fading away. The total of client certificates issued today is 165.000, there are 90.000 server certificates issued.

The CAcert web page is available now in 26 languages. Thanks to the volunteers on the Translingo system. The Translingo system is also used for translation of web pages by other (open source) web sites.

During 2007, the CAcert Assurer Challenge (CATS system) was developed, and went live in 2008 (thanks to Paul Datenverarbeitung Gmbh). 10% of Assurers have now passed the challenge and retain the title, being tested and confirmed as up to our standard. The remainder are now termed candidate Assurers for the moment, but will lose their Assurance capabilities soon.

CAcert certificates are widely used. Statistics indicate that CAcert's two Roots belong in the top 15 Cas, world-wide.

CAcert Organisation

CAcert went through a lot of reorganisation over the last two years. The organisation chart (http://svn.cacert.org/CAcert/organisation/CAcert-Organogram.jpg) gives an overview: board, management sub-committee, several technical offices, the business services offices, the policy offices and a few CAcert national organisations.

Board

Current board: Teus Hagen (president), Robert Cruikshank (treasurer), Evaldo Gardenali (secretary), and Guillaume Romagny (member). Greg Rose resigned from the board on 29th of February 2008, due to well-signalled changes in his work. Evaldo has had very limited of time for board activities since finishing University studies in the spring of 2008. In October 2008 he started a new job, with possibilities to take up his board activities again.

Sub-committees

1. The *Management Sub-Committee* (http://wiki.cacert.org/wiki/ManagementSubCommittee) started in September 2007 (task: “CEO-like duties”) with Jens Paul (he left due to work requirements in December 2007), Evaldo Gardenali (his work contribution dropped to zero in June 2008), Teus Hagen and auditor Ian Grigg (observer). The committee met

once per two weeks. Tasks, minutes of meetings, decisions of the sub-committee are made available in the mentioned wiki pages. Some of the topics tackled by this team: Organisation Assurance management and reorganisation for Germany, Holland, Austria, Sweden, USA, Australia and Ireland (all European countries are now in one sub-policy), Assurer testing and the CATS system, house style guide, audit plan and audit project start, re-hosting of servers to the Netherlands, CAcert associations (the Netherlands and Germany), marketing and PR, policy discussions and definitions (agreements, privacy matters e.g. EU DPA, code signing, TTP assurances, Assurer classes (junior, senior), and development of the new Assurance and Experience point system.

In May 2008 all work of the committee transferred to the board, as one voting member is too low for a quorum.

An overview of the management sub-committee decisions is published [2]. The decisions include those of operational character (CATS system, audit system), as well the proposal of the Memorandum of Understanding for the audit project (CAcert - NLnet) and auditor (CAcert - Ian Grigg).

2. Sub-Committee Root Key Generation Task Force

The Root Key Generation Task force is created by order of the board in October 2008 with the task to generate a new Root Key and two new sub-Root Keys, by the end of November 2008. Members are: Guillaume Rogmany, Teus Hagen and Ian Grigg (auditor as observer).

3. Board Election Sub-Committee

A request to take part in the election sub-committee in June 2008 had no success. The committee could not be installed. However Gary Lee Adams took efforts in October 2008 to get association members nominated and board members to be nominated.

CAcert Community "offices"

This year most attention has been on the "*technical offices.*" All task and work areas have been steered by Philipp Gühring, since taking over from Duane Groth in December 2006. In the second half of 2007, the public services (irc, blog, wiki, svn, bugs, email lists, revocation) were re-located to the Ede, the Netherlands, data center run by BIT, under contract with Stichting Oophaga Foundation in Holland. CATS and audit (webserver) were maintained by Evaldo up until September 2008, and are now also in the Netherlands data center.

Critical systems were hosted with Sonance/FunkFeuer in Vienna (from December 2007 to September 2008) and were then re-hosted to the Netherlands in October 2008 (May Plan CR-Day). A new team of volunteers located in the Netherlands has taken over the system administration work over from Philipp for these critical systems. Members active on system administration tasks are background-checked, and non-disclosure agreements are held by CAcert Inc.

As the new systems administration team does its "work-through," attention in the new year will shift to the software development team, with the same goal: rebuild the team to be able to cope with the business demands of a growing and active CA.

Many other CAcert Community Members fill out the other tasks. The group is large and varying, but we will mention some key players: Philipp Gühring, Evaldo Gardenali, Daniel Black, Guillaume Romagny, Philipp Dunkell, Michael Diederich, Bernhard Fröhlich, Michelle Stahl, Jens Paul, Sam Johnston, Robert Cruikshank, Mario Lipinski, Johan Vromans, Henrik Heigl, Greg Stark, Ian Grigg, Rasika Dayarathna, Teus Hagen,

Greg Rose, Wytze van der Raay, Mendel Mobach, Marcus Hermans, and the Oophaga team: Rudi van Drunen, Rudi Engelbertink, Robert Kochheim, and Hans Verbeek. Many others are active on policy development, arbitration, etc.

CAcert national organisations

In the Netherlands: *Stichting Oophaga Foundation* takes care of connectivity, physical security, hardware and maintenance of the servers for the CAcert (critical and non-critical) services.

In Germany: *secure-U e. V. association* does CAcert fund-raising, merchandising and assurance events in Germany. Secure-U has been not very active in the last 6 months. Secure-U is involved with the CAcert Assurance event on Systems October event in Germany.

Sonance Verein managed the Vienna connection from December 2007 to September 2008, but now stands down from active service.

CAcert Association membership and board

The CAcert association membership register holds 58 members. Up to November 2008 28 members have paid up their membership fee and have voting rights in this annual general meeting, upcoming 7th November 2008. Five members Thomas Wildhalm, Philipp Gühring, Sam Johnston, Mario Lipinski and Pete Stephenson joined the association by board resolution this year. One person resigned from his membership. Wren Hunt, a former long-serving member of CAcert's board, passed away in October 2008.

At the AGM in 2007 a resolution was passed that when an association member has not paid the yearly fee for 3 succeeding years, this member will resign from the association automatically. As the membership registration list is only fully updated from November 2007 (AGM), resignations of this type are not due this year. The secretary received 11 bounces on emails sent to association members.

Board and board election

As signalled well in advance, Greg Rose resigned on 29th of February as board member of CAcert Inc. Teus Hagen took over as President. The current board (Teus Hagen/president, Robert Cruikshank/treasurer and Public Officer, Evaldo Gardenali/secretary, and Guillaume Rogmany/board member) have stated that they intend to stand for re-election. As of this writing, also four association members have indicated an intention to stand for election to the board: Philipp Dunkel, Sam Johnston (acceptation of nomination not received before the deadline), Greg Stark, and Alejandro Mery Pellegrini. If for all persons involved nomination, seconder and acceptance have been received by the secretary there will be a real board election this year. Note that votes for election and other motions may be received by signed email.

Robert Cruikshank, board member, treasurer and Public Officer, is resident in NSW, Australia. The NSW, Australia Associations law requires that the PO is located in the state. Robert is nominated and he accepts his nomination for PO for CAcert Inc. He is expected to be elected to the post of PO unopposed.

Special General Meeting (4th of April 2008)

A Special General Meeting of the Association was held, 4th April 2008. In this meeting new rules of the Association were proposed and accepted: general meeting votes via signed email, and special rules to obtain and preserve the non-profit status of the

Association (application of assets and arrangements for assets when the association is dissolved).

Board decisions in 2007-2008

A full list of board decisions and minutes is available [3]. In brief, decisions covered these topics: provision of income via Google advertisements, eToken with CAcert logo (secure-U merchandising), GPL is default licensing model for CAcert (GPL V3 and FSF FDL for documents is still pending for decision), raise to 50 experience points for two Australian assurers for an assurer event, acceptance of secure-U and Oophaga under foundations policy, installation of Arbitration officers (9 arbiters), Organisation Assurance Officer (general and the Netherlands, Austria, and USA), updates on CAcert Organisation chart, more push on Organisation Assurances, approval of system administrators (Daniel Black, Wytze van de Raay and Mendel Mobach), and a CAcert work laptop for Evaldo and Robert.

Audit project plan
The general audit wiki (http://wiki.cacert.org/wiki/Audit) describes the audit work in general. At the TOP meeting in October 2007 in Permasens, Germany a funding proposal (http://svn.cacert.org/CAcert/CAcert_Inc/Funding/proposal_funding_top.html) was proposed to initiate work and funding for work to get CAcert Root Key into the browser main stream. Stichting NLnet was prepared to fund the funding proposal (http://svn.cacert.org/CAcert/CAcert_Inc/Funding/NLnet_Audit_Agreement_Scanned_signed.pdf) which describe auditing work, documentation work and community awareness work plan to achieve the audit goal. A Memorandum between the auditor and CAcert Inc. (http://svn.cacert.org/CAcert/CAcert_Inc/Funding/Iang_Audit_Agreement_20080303.pdf) was agreed and signed in March 2008. The audit work was formerly started.

The progress of work has been slow due to underestimated time constraints to reach acceptance and conclusions of various debates within a community context as well underestimation of the total of work involved. However several barriers were taken successfully as completion of the migration of servers to a secure location, instalment of a critical systems administration team, instalment of security measures in a formal way, initiation of new Root Key generation, acceptance to draft of various agreements (CAcert Community Agreement, Non Related Persons Agreement, CAcert Contributor License Agreement), and many policies (Policy on Policies, Dispute Resolution, Organisation Assurance Policy, Organisation Assurance sub-policies (Europe, Australia, USA) CAcert Policy Statement, Policy on Foundations) and initiation (Work in Progress and intermediate drafts) on policies such as Configuration Control Specification, Document Policy, Privacy Policy, X509 Implementation Policy and CAcert User License Agreement. A CAcert Security Manual is written with the help of Pat Wilson (under contract).

Ian reports once every two months on the progress made (http://wiki.cacert.org/wiki/AuditPresentations), as well in the CAcert blog news service (http://blog.cacert.org/).

Most of the audit policy work is done on the policy email list of CAcert Community. Acceptance and decisions are taken from the the Community. CAcert Inc. has veto right on these decisions.

The original plan in May 2007 was to have all CAcert servers moved to Holland in 2007. This process has been delayed for the CAcert critical servers (user database and signing server). The delay was caused by technical security problems, human

resources allocation and availability. This caused the cancel of an initial plan in January 2008. The May Plan (http://svn.cacert.org/CAcert/CAcert_Inc/hosting/MayPlanNLrehosting.pdf) resulted in the organisation of the completion of the rehosting on CR-Day (1-3 of October 2008). The critical systems administration has been taken over by a special team located in Holland. One barrier for the audit completion has been removed. The funding for the rehosting has been part of the audit project.

CAcert Communication Policy (directive) CCP

The CAcert Communication Policy (http://svn.cacert.org/CAcert/Policies/CAcertCommunicationPolicy.html) describes how CAcert communicates as required for achieving its mission. It handles subjects as press releases, announcements, internet email and chat (IRC). It has been accepted as directive in April 2008.

Privacy

When the user data base was moved from Sydney, Australia to Austria (and in October 2008 to the Netherlands), the user data came within the European Union jurisdiction and as such this falls under the the EU DPA (privacy) directive. This change initiated a discussion, and measures were planned to restructure the user data base to provide a much improved privacy handling of the user data. In the past, information collected by means of its Assurers (in those days, called Notaries) and Trusted Third Parties (centrally archived) included photocopies of formal identity documents, social security numbers, etc. This practice was influenced by attitudes and policies of other Certificate Authorities. In 2005 this was dropped as a requirement for Assurances, but archives were still maintained. In 2008, the requirement to keep the copy of ID from TTP assurances has been dropped as well, and a request has been made to destroy the copies of ID's in all CAcert and Assurer archives.

During 2008, CAcert policy group debated and approved that any full name on an approved form of ID can be assured (in effect, an individual can have more than one formal full name). Policy group decided that there is a continuing need to record the date of birth of an individual (taken from the ID) in order to discriminate between two similar names. Nick names cannot be assured. It is observed that CAcert is recording a very minimal set of personal information, being only that information which is needed for the CAcert certificate service operations, and far less information than most other comparable.

To meet the EU DPA directive CAcert (the association) has to make certain arrangements. However this is an exceedingly complex issue. CAcert Inc. is an Australian Association. The Community Members perform the system administration tasks remotely even from outside the EU (there is a non-disclosure agreement with those administrators), however the machinery is owned by Oophaga foundation, based in the EU. However there is more complexity: due to the Certificate Authority nature the access to data is very limited due to security requirements (Audit requirements, in common with the CA industry in general, are not aligned with the EU data protection directive: choose one requirement and it does not adhere to the other requirement). In other words, the Data Protection project may delay the audit process further, yet again. However CAcert and Oophaga are working to investigate a possible exception: associations and foundation may have an exception under the Dutch Data Protection Act under EU DPA. Also note that, CAcert has a very limited amount of personal information: primarily the full name(s), date of birth, email address(es) and maybe domain name(s), and some logging (assurance points, certificates issued, etc.). Therefore it represents a lower risk than most other organisations, especially those

with people involved in and recorded by anorganisation (e.g. copies of ID's, physical addresses, social security numbers, etc.).

Thanks

Throughout the last year, a lot of members worked very hard, and we saw a lot of good results for the Community. We are not there yet, as the Root Certificate is not yet in the mainstream browsers, but the board is confident that we will get there. It is the membership – of the Community and of the Association -- who got us this far, and will take us to the next challenge. 2009, Roots and browsers, Onwards!

*Board of CAcert Inc., 7*th *of November 2008*

References and Notes

[1] *The Trust Crisis,* published by Meulenhoff, ISBN 9789029083751, November 2008. Ed. Simon Knepper and Johan Kortenray, including many contributions of well-known (Dutch) authors.

[2] Management Sub-Committee decisions
http://wiki.cacert.org/wiki/ManagementSubCommitteeDecisions

[3] Board's decisions http://wiki.cacert.org/wiki/EmailBoardDecisionsUpdateFeb2008