Memorandum of Understanding
“Audit for CAcert” Project

The parties:

Stichting NLnet, domiciled in Amsterdam, The Netherlands, referred to as "NLnet" in this document, represented by Mr. Hans Onvlee, chairman, and Mr. Jos Alsters, secretary/treasurer,

and

CAcert Inc. association domiciled in NSW Australia, referred to as CAcert in this document, represented by Greg Rose, president,

given that:

- CAcert is conducting an independent audit of the organisation and its procedures in order to enable inclusion of the CAcert root certificate into the main stream browsers;
- NLnet wishes to contribute to the audit of the CAcert organisation,
- CAcert is committed to organise an independent audit by attracting external parties for that,

agree to the following:

1. CAcert has written a proposal for the funding of the Audit for CAcert, version 2, 2007-12-22, is attached to this document as Annex1.

2. The Audit for CAcert Project consists of executing all activities as described in the project plan, which is provided in Appendix 1. In the project plan, these activities are divided into 3 Milestones.

3. The completion of each of the 3 Milestones will be subjected by review and agreement from Stichting Oophaga Foundation, the Netherlands. For each of the three milestones Oophaga sends a Milestone Report to NLnet. Such Milestone Report will serve as a ground for corresponding Milestone payment.

4. CAcert shall report its progress on a bi-monthly basis to NLnet and shall maintain a public status page for the Project. Overall project management shall be directed by Greg Rose, Project Manager and shall be run under the oversight of the CAcert Board of Directors.

5. NLnet commits to contributing an amount of Euro 36.000 to CAcert for funding of the Project. The funding will be paid in the following phases:
   - Euro 9.000 when the Project is started;
   - Euro 9.000 after completion of the Milestone 1;
   - Euro 9.000 after completion of the Milestone 2;
   - Euro 9.000 after completion of the Milestone 3.

   All payments will be made by wire transfer into an account to be designated by CAcert under review of Stichting Oophaga Foundation.

6. At an appropriate time, NLnet and CAcert will issue a joint public statement announcing this project and NLnet's financial support.

7. CAcert is understood to be responsible for coordinating the project and allocating funds - in line with the terms of the proposal and budget.

8. Funding to any particular group or person will be on the understanding that they coordinate their activities in agreement with CAcert, in the spirit of cooperation, and in an effort to achieve the successful release of the results of the Project.

9. Annex 1 (project plan Audit for CAcert Project, version 2, dated 2007-12-22) forms an integral part of this Memorandum of Understanding. If and where statements in the Annex 1 are in contradiction with the statements in the main memorandum text, the statements in the main memorandum text will prevail.

Amsterdam, December 26, 2007,

Hans Onvlee	Jos Alsters	Greg Rose,
Stichting NLnet	Stichting NLnet	CAcert

Annex 1.

Proposal for the funding of the Audit for CAcert Inc. V2

NSW, Australia, 22 December 2007.

I. Executive Summary

This plan proposes that the audit for CAcert, an open and free certificate authority, be funded for a period of 18 months, in 3 tranches of 6 months each.

The plan was prepared and proposed by the Advisory of CAcert (Teus Hagen, Ian Grigg, Jens Paul). The board reviewed and approved the plan at the September, 2007 meeting (m20070919.5). The plan was revised in December 2007 to include changes to milestones, work completed, and to agree with MoU.

II. Introduction

CAcert is an open and free certificate authority that operates across the world as a community. It is open because anyone can join, and it is free of cost for all of its certificates. It works because we are a community devoted to securing the Internet access of our users.

CAcert community

The headline task of the CAcert community is to assure people according to their identity documents. Once this identity is established, certificates can be created which claim the identity of the user.

As users gain more points from more assurance, they themselves are encouraged to become Assurers, thus creating a self-perpetuating force of Assurers. The combination of free certificates, an ability to gain points, and help assure others has resulted in a strongly growing community, one that uniquely addresses a cross-section of computing world, wherever people feel they need certificates.

CAcert and the Commercial Market for Certificates

CAcert reaches a particular segment of the market for certificates: those individuals, communities, non-profits, small and large companies, that find that the price of certificates puts them out of the market. Certificates are generally available from commercial CAs from $20 and upwards, but even this low value is impractical for users in poor countries or small and non-commercial organisations that require many certificates.

CAcert provides this service of free certificates by enrolling the users themselves to do the work. In that sense, it is not totally free, as users are encouraged to become Assurers and to contribute time and effort rather than money. Many of CAcert's users are very happy with this offering and are keen to contribute.

CAcert does not compete with commercial suppliers, rather it expands the market for certificates into areas they do not look at. For example, CAcert does not offer support services with guaranteed reaction times. Instead we offer free community-based support without such guarantees.

Browser Popups

CAcert is not however free of industry standards, norms and conventions. Although our community is successful, it has effectively stalled due to one major cause: the lack of being recognised in the browser "root lists". Without being in the "root lists," our users and the general public are plagued by annoying popups that warn about scary security situations.

Lack of browser representation is the number one request for the users, and the number one reason why people join, but never utilise the services and never fully join the community. Therefore CAcert has a goal to get into the browsers.

III. The Audit of the CA

Root Lists

Major browsers (Mozilla, IE) require an independent audit to be conducted. Therefore, CAcert must have an audit in order to get into the browsers.

Strategy. Microsoft has around 66% of the market for browsers [1]. Microsoft's policy on CAs is closed and likely inflexible and expensive.

Mozilla Foundation in contrast works to their Mozilla CA Certificate Policy [2]), a transparent policy that was developed in an open community process (including help from CAcert's Founder and the current Auditor). Mozilla's processes are also more responsive to community pressure. As the market share for Mozilla's Firefox continues to grow (25% around the world, higher in Europe [3]), this is sufficient to generate "marketing pressure," and sufficient to encourage CAcert's community to migrate. Acceptance in Mozilla's root list will then likely assist in negotiations with Microsoft.

Hence the strategy is *Mozilla first, Microsoft second.*

Mozilla First. Negotiations with Mozilla were conducted under their then-emerging policy. The criteria selected and negotiated with Mozilla is that written by David Ross (known as "DRC" [4]). The criteria are divided into 3 groups or phases, being A (documentation), B (public access), and C (operational review). This criteria is agreed with Mozilla as a suitable base for the CAcert audit, and is awaiting internal examination for general approval for other CAs.

Progress

Engagement. CAcert engaged Ian Grigg to conduct the Audit in January of 2006 (CV at [5]). The initial target of securing entry into Mozilla Foundation's root list, and therefore Firefox, Thunderbird and other applications managed by Mozilla was agreed. The adminstrative agreement was to cover expenses.

The audit proceeded rapidly to identify missing documentation for the CA to prepare. These tasks primarily reflect criteria in phases A and B of the DRC, and predict a dramatic increase in the overall quality of the service provision, over time.

Most of the policies have been written in at least DRAFT form, and are close to approval. Much work has been done to place the structures on a more formal footing. See Appendix A.1 for a full listing of work done to date within the audit project.

Issues

Management and Consulting The progress of the audit highlighted over 2006 an important lack in the ability of the CA to manage its large and growing user base, and the systems that were needed to satisfy the wider security and browser communities. The Auditor was called upon to assist in addressing this gap in management. See Appendix A.4. Indeed, most of the Auditor's time, until recently, was spent in explanation and discussion of the improvements needed. This need for *consulting* carries on to the current day, and is an important factor in future planning.

The double-life of Auditors as Consultants is more or less routine in audit practice, the major difference being that professional audit firms sell "related consulting" for fairly hefty fees. There is then the potential of a serious *conflict of interest* in both the charging of fees and the advice provided (is the audit promoting fee-based consulting?), and this has to be managed carefully.

Audit Freezing. Unfortunately, around mid-2006, the Auditor determined that CAcert's management was inadequate to the task of running a CA. This inadequacy is a normal and routine response to an organisation growing too fast and stretching past the abilities of the original Founder. The Auditor's opinion was established by repeated failures of the board and management to deal with requests to approve or comment on new documentation. Specific restrictions were put on discussions with partners, testing of Assurers, Organisation Assurance and operations phase of

Audit.

Management Change. This crisis was resolved with the resignation of the entire committee (board) of CAcert. A Special General Meeting of the Association elected a new board, end May 2007. The Board recovered control of essential assets (bank accounts, domains, etc) and then moved to restart serious work on audit and other priorities.

Work completed second half 2007.The board met in Europe during September to seriously kick-start the process. An Executive Summary and Minutes of the September meeting is published on the wiki [TopMinutes-20070917]. The board approved the critical policies to unblock the progress of the audit (Policy on Policy, Cacert Community Agreement, Non-Related Parties—Disclaimer and Licence, Dispute Resolution Policy, Principles). With the nature and inclusion of the community now defined, Audit restriction on discussions with partners was lifted (Oophaga and NLnet were closely monitored exceptions to that restriction). Organisation Assurance was reviewed, rewritten, approved and restarted. The CAcert Assurer Test System (CATS) was written and deployed as of December 2007, and rollout to Assurers is imminent as the *Assurer Challenge*. Negotiations were advanced on outsourcing the production of the Security Manual.

Status

The audit remains approximately half completed. The majority of documentation is written. That which remains is to finish, approve and distribute the documentation, push through the indicated operational changes, and to conduct the compliance and operational audit phase (DRC part C). See Appendix A.2 for fuller details.

Audit Restrictions. In addition to the audit being a block to entry in browser root lists, the operational phase of the audit itself remains blocked by three elements:

- critical systems need to be moved fully to Netherlands Ede facility of BIT,
- dual control mechanisms have to be put in place, and
- Security Manual needs to be written and approved.

Removal of these barriers will speed up the audit process and result in dramatic growth in the size and depth of community.

Audit Options and their Funding implications

The Auditor, Ian Grigg, has indicated that the "direct-expenses-only" agreement covering the 24 months of 2006-2008 is unlikely to be sustained. In the short term, CAcert has examined funding scenarios for audit continuation. This section summarises the known options.

0. The Null Option. CAcert could simply abandon the audit process. As the current primary goal of the community is to get into the browsers, and this result will cause dramatic expansion of the power and utility of the community, the Null Option has been widely rejected.

1. Funding the Continuation of the Current Audit. A budget for funding the current audit and necessary work is presented at Appendix B. This budget sets €36.000 over one year, and a follow-on phase of €20.000.

2. Funding an Audit by Audit Firms. It is estimated that the cost of an Audit by a formal audit firm would cost around €200.000 to €250.000, directly billed by an audit firm. Such an audit would likely be conducted to the WebTrust criteria, which has the advantage of being more acceptable to Microsoft. This however takes no account of costs in time and effort to the CA.

3. *pro bono* Audit. CAcert has talked to many auditors about the possibilities of a *pro bono* ("for free") audit. It is customary for Audit firms to do *pro bono* work for worthy causes, and larger audit firms have departments for this purpose. However, no firm or individual has agreed. It is speculated that after the first audits are completed, and the CA is "in the browsers" then it may be worth the while of the big firms to then attach their names to the success. Until then, CAcert faces a chicken-and-egg problem in needing to prove itself, by completing a first audit, and getting into the browsers first. Alternatively, it could be that doing a free audit for a CA would raise conflicts with the other clients of audit firms, as the CA business is competitive.

Source Code, Reports and Documentation

The board of CAcert Inc. has approved a policy that source code and documentation be under free and open licence.

IV. Conclusion

Proposal

It is proposed that funding be raised for continuing the current audit, Option 1 above. This is estimated in Appendix B as €36.000 over a period of 12 months. It is predicted that a maximum of €20.000 will be required for a further 6 months in order to wrap-up and fully benefit from a completed audit. It is proposed that this funding be raised from NLnet, a foundation oriented to similar goals as CAcert in the Netherlands.

Benefits

A completed audit enables CAcert to petition Mozilla for addition to their browsers and other software. This if approved will result in a dramatic increase in the utility of the certificates to all users in the community and the public at large. Further, the flow-through benefits of the changes imposed by the audit will increase the professionalism and utility of the CA, which is of special benefit to companies.

As the approach of CAcert's audit work-through has been fundamentally open and honest, the result is also likely to challenge the entire CA industry to lift its game. Although difficult to predict, these changes could change the way CAs and certificates work, and thus the way security is delivered by Internet software to users.

Risks

- The Audit process is strictly independent of CAcert and the desires of the community. In essence, the Auditor works to the interests of the browsers, the relying parties and other users, and does not work for the CA.
- Therefore, the Audit can simply fail at any time. This will be signalled to the world.
- Funding for the Audit should be provided or overseen by an agency other than CAcert itself, in order to preserve the independence of the Auditor.
- Fundamentally, the work required to be presented for the Audit is done by the CA, and as CAcert is a community, individuals within the community must do that work, voluntarily. Most of these individuals are not paid and cannot be instructed, therefore, there is no guarantee that their work will be done.
- Because of all the above, it is neither useful nor appropriate for the Auditor or CAcert to make any reliable or strong prediction of completion date.
- Even when a formal Audit opinion is delivered, there will be substantial follow-on work of monitoring, user-presentation, and additional tasks. If these are undone, the investment could lose value.

Governance

In order to address and protect against conflicts of interest, the following recommendations are made:

- The Auditor be engaged to report to the community of CAcert registered users, to Mozilla Foundation, and/or to NLnet, rather than to CAcert Inc. (This separation of parties is familiar in the systems audit world, although novel for CA audits.)
- Stichting Oophaga Foundation (Netherlands) be charged as independent reviewer, with oversight and review of the programme and funding.
- Any changes to payments are subject to approval by independent reviewer. CAcert Inc or Auditor may appeal to Oophaga to change any terms and conditions.
- Auditor be retained on fixed monthly retainer, rather than hourly-based rates as is more

normal in the audit industry, or results-based rates common in other projects.

- The salient details of financing will need to be published under the terms of Mozilla CA Certificate Policy, pt10.

Timeline

Remembering the above risks and governance recommendations, if systems are moved and dual control is implemented, and the individuals manage to prepare and complete the work, the audit may complete early 2009. The following timeline is presented as strictly illustrative.

Dates	**Activities**	**Reports**
Jan 2008	complete Assurance Policy and Statement start of Assurer testing start of Security Manual	community report
Mar 2008	stop assurances by untested Assurers review of CPS completion of third party licence	community report
May 2008	First draft of Security Manual Completion of Documentation (DRC-A,B)	**Milestone 1**: Major Review (a) on Documentation Phase, May 2008;
Aug 2008	Approval of Security Manual Business side of Compliance Evaluation	community report
Nov 2008	Systems side of Compliance Evaluation	**Milestone 2**: Major Review (b) on Compliance, Nov 2008.
Dec 2008	Write-up of major shortfalls negotiations for next Audit start negotiations with Browsers	
Jan 2009	Audit completion presentation to Browsers	**Milestone 3**: Major Review (c) on Audit Completion, Jan 2009. Formal Opinion
Feb-Jul 2009	monitoring, compliance, presentation to users	**Follow-up**: Major Review Jul 2009

Milestones. There are 3 points at which a Major Review can be made to the interested parties (NLnet, Oophaga, CC to CAcert) at approximately 6 month intervals: (a) After the completion of all documentation needs, (b) after completion of the Compliance Evaluation, and (c) after Audit completion. Each report will detail work completed. Each phase will begin with a plan for the next phase, this present document may stand as the first plan. Community reports every 2-3 months will be brief (1 page) posts on the CAcert resources (wiki, lists), listing work achieved, and critical work outstanding.

Appendix A -- Documents and Processes

to the Proposal for the funding of the Audit for CAcert

A.1 Work Done to Date

The following are completed steps in the audit process, or side-results.

- CPS ("certification practice statement") was rewritten to cope with audit requirements [*work-in-progress* CPS]. This is a complex 27 page document that specifies reliance, operating parameters and rules for the CA. Requires review and alignment.
- A new regime and strategy was created to offer the users and the public a fair and sustainable deal. This is embodied in the following documents, written for the audit process:
  - Non-Related Persons -- Disclaimer and Licence [*POLICY* NRP-DaL] for the wider public, modelled on an open source licence.
  - CAcert Community Agreement [*DRAFT* CCA]. This is the user agreement for the registered users. Users are those who are "inside" the community and are therefore subject to CAcert's own forum of dispute resolution (ADR, or Arbitration).
  - To accompany the above CCA, a document has been created to collect and define the *Principles of the Community* [Principles]. This is a developing, consensual document, but it has a serious mission: it provides a foundation of conventions and culture which can be drawn on in event of disputes. This means that the CCA does not need to nail tricky issues precisely.
  - Third Party Vendors Licence has been started, is a work-in-progress.

  This contractual, customary and community arrangement dances the line between the current CA practice of selling trust but disclaiming all liability, and offering a service of value and honesty to all.
- Privacy policy was amended by (old) Board mid-2006 [Privacy Policy].
- Dispute Resolution was introduced as a fundamental tool to insert humans into every "exceptional" decision. Policy [*POLICY* DRP] and Case manager's guide written.
- Assurance.
  - Organisational Assurance Policy [*POLICY* OA Policy] was rewritten entirely.
  - Assurance of the identity of the users was put onto a more professional footing with the creation of an education department, a training programme, and an automated testing system [Education Campus]. This creates a "Quality" approach to Assurance, in that claims made can be backed up with processes.
  - Assurance Policy is work-in-progress.
- Serious questions were raised about a future phase of systems auditing, which had a material effect in later negotiations with NLnet. These led to the creation of the NL data center, and Stichting Oophaga as a custom-created partner in NL to support CAcert.
- Events (conferences) have been moved from ad hoc to organised activities where the leaders are responsible for the activities of the Assurers, including on-the-job training and supervision.
- Board meeting held Europe, September 2007.
  - Most above documents were approved at the meeting.
  - Policy on Policy -- transfered the basic mechanism for control for policy to an open policy group (IETF fashion) leaving only a veto right with the Board.
  - Residual oversight by Auditor was handed over to new Board.
  - Creation of management sub-committee to supervise processes and replace informal role of Advisory.

A.2 CA outstanding Work List

Responsibility of CAcert. Auditor consults in a supporting role.

- Systems And Security
  - migrate critical systems to Oophaga's NL datacenter (*Systems Administration*).

    - dual control / 4 eyes needs over critical systems (*Systems Administration*).
    - Security Manual (*Security*). This large document needs to be written and is only in early "headline" form.
    - CPS needs to be reviewed and aligned with all other policies (*Security*).
- Configuration-Control Specification (*Documentation*). Although simple, the specification of the controlled documents needs to be updated and approved. Policy on Policy (above) define documentary parts of this, but software and hardware sections remain to be defined.
- Ongoing Risks/Liabilities/Obligations work (*Assurance*):
    - Finalise the CAcert Community Agreement (CCA) to POLICY status.
    - Assurance Policy has to be reviewed by policy group and taken to DRAFT. This includes finalising the Assurance Statement which is the foundation stone on which the certificate's claim of identity rests.
    - Code-signing Assurance Policy has to be started.
    - Work on and take to DRAFT a licence for 3rd party vendors, for example Mozilla.
- Promulgation of this regime through the community (education, documentation, events, ADR) (*Internal Marketing?*)
- Organisation Assurance work has substantial community implications (*Assurance*):
    - Write detailed 'country' policies for Organisation Assurance and take to DRAFT.
    - New Organisation Assurers need to be trained, tested and appointed.
- Complete review of the Privacy Policy due to changed systems circumstances (*Privacy*).
- Bed in Dispute Resolution process. Show as workable and fair (*Dispute Resolution*).

(*Responsible team/officer*) shown above in parentheses. Board is expected to review and adjust, so ultimate responsibility falls to board (President, Greg Rose) via Management Sub-Committee.

A.3 Auditor Responsibilities

Processes in the hands of the Auditor. CAcert provides support.

- Systems Security Review (Audit). As the operational systems come out of their build-up (shift to NL data center), there is a review required under DRC-C. Will require on-site visits.
- Review of Assurance "exceptions".
    - Super-assurance, being specially designated assurers with increased powers.
    - TTP -- trusted third parties.
    - Minors (those under 18 years of age).
    - Code-signing.
    - Organisation Assurance.

  These have been deferred until basic web-of-trust (Individual) assurance is stabilised.
- Documentation and policies review.
- Review for conformance with policies (DRC-C):
    - websites and public comments (e.g., is a disclaimer to public obvious and prolific?).
    - Assurers' knowledge (e.g., do they know and present a correct and fair picture?).
    - operations practices.
- Preparation of Audit Opinion.
- Preparation of future recommendations.
- Consulting in explaining results.

A.4 Related Consulting

In addition to direct audit responsibilities, there have been substantial callings for non-audit related consulting activities. The following are some of the areas where contributions have been made.

- Human resources: methods of selection processes and supervision of officers.
- Succession: assisted a transition from old management to new.
- Education: future training needs of the community.
- Governance of the community: foundations, financing, responsibilities, conflicts of interest.
- Secretarial: Documenting and Review of all decisions over three years. Minutes.
- Partnerships: Negotiation and oversight, preserving interests of users and community.

These roles are formalised within the ambit of the Advisory, a small group of senior managers that provides optional advice and facilitation to the community and to the board. As a member of the Advisory, the Auditor can then more clearly signal which hat is being worn at any given time, and continue to maintain an independent posture.

A.5 Follow-up Phase

When/if Audit is complete, there is a lot of benefit in conducting a follow-up phase. This is anticipated being around 6 months and involving internal and external communication work. The following is illustrative of the activities that could be undertaken.

- Negotiations with third party software vendors (Mozilla, Microsoft).
- Preparation for next audit (general expectation is that next audit starts immediately).
- Wider paper on the Audit of an open source certificate authority, for publication at major Internet conference.
- Wider paper on the legal framework that is constructed.
- Presentation of audit work to local chapters within the community. This would predict Europe due to current user base, but also would see UK and the Americas.
- Roll out of Education by means of Assurer Educator training.
- Press articles in major Internet publications.

Appendix B -- Budget for Continuing Audit

Constructed in 3 phases, with follow-up phase for ...

Item	Description	Amount
Phase 1	**Policies Review**	9.000
Phase 2	**Operational Review**	9.000
Phase 3	**Audit Completion**	9.000
Total	3 phases	**36.000**
Follow-up Phase	Monitoring, Promulgation, Explanation	**20.000**

Follow-up Phase. Once the Audit is formally passed, there will remain a significant need for attention: monitoring for compliance, promulgation of existing work, any remaining tasks to complete, new work as directed, and importantly, explaining the big changes to the internal user community and the external world. This will involve more travel than the earlier phases.

Without doing this work, it is likely that the good work of the audit will stop, or indeed reverse. For this reason, to preserve and reinforce the audit, it is estimated that a further €20.000 should be invested as needed in a follow-on phase (after formal completion). This estimate of 20K is a maximum and is suggested as an investment to warrant that the first year's work will be a success.

Break Down of Costs. Each phase is anticipated to break down into three components of €3.000 each: (a) Basic retainer of all Auditor services; (b) Direct audit costs for travel, equipment, etc; and (c) policy authoring by Senior Assurers and operational support by systems personnel.