Proposal for a solution for the shortage of costs and time finances of the CAcert Audit Project.

Board CAcert Inc.

author: teus hagen

June 2009

Need to discuss mentioned figures and time estimates with Ian before things are sent to NLnet!

Abstract

The MoU (Nov 2007) between NLnet and CAcert describes the work and funding for the “audit for CAcert” project. The audit work (compliance, policy definitions and documentations, technical arrangements definition and operational aspects) is defined by the MoU (March 2008) between CAcert and Ian Grigg. The milestones as defined in these MoU's have exceeded considerable the planned delivery dates, as well costs in 2009 for meetings, events, travel are exceeding the budgets more as could be anticipated upon in 2007. This creates a problem for the finances of the remainder one third of work.

Executive summary

Half way on delayed end of work for Phase B in the “Audit of CAcert” project available finances run out unforeseen. Financial liquidity position of CAcert Inc. is by far insufficient to carry extra need for cost coverage. A funding renewal request/proposal with finer detail on costs and planning is offered to NLnet for more funding on this project work. The increase of costs are due to community acceptance delay and extra work, to changes in requirements and to better insight in needed technical arrangements, policies and documents and reorganisation of the CAcert organisation structure.

The extra funding required is limited to the main audit work area of Phase A and B (from original 18.000 Euro and 6 months of work to 25.000 Euro and 21 months of work; Phase A and B ending now at the end of 2009) where document drafting and acceptance process within the CAcert community, and first check of compliance for assurance, system administration and required software developments make the work and financial planning very complex and risky. So far Phase C plan of work does not need to be changed.

New funding needs to be found as soon as possible in order not to stall the audit process and avoid desinvestments.

Care should be taken for funding web account software development as current software is outdated and not supporting newly accepted policies.

Proposal of solution

Update “Audit for CAcert” project definition with new info and costs factors. Ask NLnet to fund this. Estimation of increase funding need for Phase B is: +4.000 audit work and +3.000 for travel/meeting/misc costs. Phase B to end end of 2009. Details of planning for Phase B work by Ian Grigg as soon as possible.

Investigate project planning, programming resources and funding for web account software (update and renewal).

Preliminaries and history

2006 Auditor Ian Grigg entered CAcert community to assist with the management of the fast growing user base and arrangements needed to satisfy the requirements of the browser communities. Mid 2006 this was halted till May 2007 with a new board installed with CAcert Inc. And serious work within CAcert community started to get CAcert as CA in compliance with the requirements of Mozilla for CA list inclusion (DRC part a,B,C).

By November 2007 the statements was: audit is approximately half completed and majority of documentation is written.

“Audit for CAcert” Project

In November 2007 a funding arrangements (MoU Audit Project CAcert-NLnet) was made between CAcert Inc. and Stichting NLnet (dutch foundation stimulating network technology via project funding). This project (Audit Plan) describes completion of work with 3 milestones elapsing each over 6 months. The total budgets for the milestone planning sets 36.000 Euro. A followup phase is expected to be needed for ca 20.000 Euro.

In March 2008 an MoU between Ian Grigg and CAcert Inc. was signed to work on the Audit Plan funded by the NLnet-CAcert MoU arrangement (36.000 Euro: 9.000 Euro at start and 9.000 Euro for completing each milestone of the Audit Plan). Each 9.000 Euro retainer is divided in three equal 3.000 Euro budgets: audit services by auditor, travel/equipment/misc costs, assistance costs (policy authoring, operational support).

For each phase planning and planned expenditure has to be provided to CAcert. At approximately every two month period a report will be provided to fulfill NLnet report requirement.

Any changes to terms, conditions and/or payments are subjected approval of Oophaga.

See the two Mo's for the glory details.

From 16th of December 2008 Philipp Dunkel took over the liaison between Board and Ian Grigg. Basically for Phase B (and C).

An overview of work accomplished for the audit project can be found on the CAcert wiki Auditor reports page . The up to date cost overview wiki page of Ian Grigg state of expenditure and committed expenses.

The periodic reports of Ian Grigg on this audit project:

- Report to Community April 2009 (blog)
- Report to Community January 2009
- (short) Report for AGM and (long) Report to Community October 2008
- interim comments on the critical systems move to Holland October 2008
- Report to Community Sepotember 2008 (blog 1, blog 2)
- Report to Community June 2008 (blog)
- Report to Community March 2008 (blog)
- Report to Community January 2008 (blog)

Milestones

Milestones *major review*	**planned date**	**expected date**	**description**
A	Jan 2008	Sep 2008	Approval remaining policies, security manual
B	Jul 2008	+ 6 months Mar 2009? pending	Documentation DRC-A,B, stop old assurances, system and compliance evaluation, writeup major short falls (management letter)
C	Jan 2009	await start	Audit completion (opinion and management letter), presentation to browsers, check compliance

Remarks on the milestones planning dates

Major review A work started from 3rd of March 2008 and should have ended 6 months later by August 2008. The audit preparations and work started already in September 2007. Reported date was in early October 2008, 2 month later as planned. Security manual work started in July 2008 and ended in January 2009 with the Security Policy and Security Manual.

Major review B work was by the planning as made in November 2007, taking into account the two months delay of Phase A to be ended by March 2009.

Audit for CAcert Project finances/budgeting

Underestimation of time and work to get policies/documentation accepted

From the start of the Audit Project planning and work the issue of delays caused by discussions, debates, repeated argumentation, delays in decision taking over sub-parts and in the end the policy and/or documentation was known, anticipated for in the planning but too much underestimated. The start of policy and agreement definitions and documentation was with small groups and a funded face-to-face meeting in September 2007 made it possible to minimize the time in the beginning. Bringing the policy to a much wider audience was not to avoid (the CAcert Community needed voice) and merely created a delay already in Phase A.

This emphasizes the underestimated time needed to reach consensus also severely for Phase B, for which there was no “flying start” as with Phase A (majority of documentation written).

CAcert is based on volunteer work. This puts the burden on a very small group of people. Their contribution work is limited and the longer the project work continues the risk of “putting more work into it” is getting much to high. The effect is a delay known as the “pig breeding cycle”. This issue was not taken into account with the original project planning.

The policies are proposed, discussed and accepted via the CAcert Policy group (an email list). The group has about 180 readers. The amount of votes for acceptation is low: ca 5.

Conclusion: audit work for Phase B was doubled, time delay is another six month for Phase B.

Underestimation of needed documents and policies

At the start of this type of project it is unknown to the Community, the Association as well auditor which policies and documents are needed for the audit. The majority of work is showing up when details are going to be defined. As well the requirements of the browsers evolve in time and came only late (end of 2008) to a more precise and stable definition.

The Security Policy and Manual readied only by March 2009, which is one of the two large documents of about 20 pages text. The usual size of a policy document is one to two pages. The Certificate Policy Statements Policy document is the other oversized document and is still in work in progress.

Current work in progress policies are: trusted third party for assurances, third party CA's, organisation sub-policies, junior assurances. One need to take into account the experience with getting policies accepted from the past...

Conclusion: to get these remaining and last documents accepted will take four months of elapsed time and one months of audit work.

Organisation Assurance

The “audit for CAcert” Project was created due to the problem of “*lack of browser representation is the number one request for the users*”. The browser “popup” message “this server certificate is signed by a non trusted CA” is stalling the CAcert Community acceptance. In essence this means that server certificates (mainly from organisations) need to be signed by a CA which is in the browser “root lists”.

Hence CAcert Organisation Assurance needs to be taken up in the audit. However the needed audit work and involved time delay aspects influence a very unfortunate proposal by the auditor to not include Organisation Assistance into the audit project work.

The documentation work needed for Organisation Assurance is limited: Organisation Assurer Manual, and Organisation Assurer Challenge, which content can be based on the (Individual) Assurer Manual and (Individual) Assurer Challenge.

Similar as for CAcert individual Members, organisations should be able to login into the account and have a similar Assurance Policy as for individuals. The work in progress document has been defined, but there it has to be accepted, as well the software needs to be updated to allow organisations to login.

Conclusion: one month work for finalizing the Organisation Assurance Manual and Challenge. This allows Organisations to use server certificates signed by the audited CAcert key.

Audit travel and meeting costs

In the Audit for CAcert Project planning the audit restriction "testing of all Assurers" has been described. The Assurer Challenge (funded by a third party) has been developed and is fully operational. CAcert has been changed considerable due to taking into effect the new policies ("the new regime"). Assurer Training Events, combined with audit assurance compliance check, was felt necessary, but was not taken into account in the planning and cost plannings at all. These events started early 2009. However the financial room for this was not fully available.

Conclusion: 3.000 Euro budget for travel etc costs in Phase B are sufficient to allow a successful audit of practice. This should be doubled to 6.000 Euro.

Conclusion on the finances

The amount of work in time for Phase B should be extended with ten month which increases the work costs with +4.000 Euro (in total 7.000 Euro).

The travel, etc. costs budgets needs to be increased with 3.000 Euro (in total 6.000 Euro).

Some Remarks

On Financial budget

Work plan and associated costs can be more detailed when the project proceeds. However financial implications for the project and CAcert should be continuously monitored by the CAcert treasurer. The information to and the acceptance by the treasurer needs to be improved in order to avoid late discovered problems in the financial liquidity of the project and too late rescheduling of event arrangements.

On workplanning

Plans and changes thereof should be more frequently as when work is half finished more details of the planning are becoming known and successive actions can be planned better (notifying Members, marketing and PR, etc.). The work plan of e.g. Phase B was not very well known to the board, as well changes thereof from December 2008. One should avoid "surprises" to the Community as well the board who remains responsible (the board should be able to carry its responsibility).

Proposal

As the financial liquidity of CAcert Inc. does not allow this radical increase of costs, nor is the current funding of the audit project is allowing sufficient cost coverage, the time needed to end Phase B of the project plan, the "Audit for CAcert" project plan needs to be updated and extended.

Proposed is to adapt the above mentioned time and cost generalized numbers into the project plan. As auditor is with the past experience good informed on a more detailed schedule and costs, he is asked to plan a more detailed Phase B and when Phase C starts, similar under the restrictions of the 9.000 Euro historical budget (?).

This renewal of the "Audit for CAcert" Project plan will be offered on the short term (one month) for appropriate funding by NLnet.

An action has been initiated to negotiate this project plan renewal with NLnet in order to see if they feel that this request is feasible.

CA operational work funding/budget requirements

In order to fulfill browser requirements, to fulfill operational arrangements due to accepted policies and reorganisation of CAcert operations which can stall the audit or enable CAcert to survive from passing the audit some projects which need external funding need to be planned:

- **Web account software development**:
  - for the short term: patches to the current software in order to incorporate just enough functionality to support the accepted policies (Community Agreement mark, new pointing system, multiple individual names, organisation accounts, ...). Estimated effort is 2 months of software and test work. Risk: multiple names will change data base structure). Error rate in the estimation: 1 month. Funding estimate: 5000 Euro.
  - For longer term: rewrite of the CAcert account / web software. Estimated work 1 year (2 months design, 8 month development, 2 months testing). Risk: rollover to new software, security of software. Error rate in the estimation: 6 months. Funding estimate: 25.000 Euro.

  Need: urgently as this is another stalling factor of the audit.
- Face-to-face meetings. Board, officers and managers, support and system admins need one yearly meeting(s). International traveling and hotel accommodation needs to be funded. Funding estimation: 4 meetings, 3 days per meeting, 6 persons per meeting: 4 X 4000 Euro.
- PR. CAcert is much too technical oriented. So is the documentation. Policies are written "for lawyers", the changes in CAcert as well explanation of how-to with certificates for common end users need to be devices as well proper PR need to be done to those who volunteer (t-shirts, brochures, etc.). Funding estimate: 5.000 Euro.
- Marketing: assurance events with major conferences and exhibitions. Budget estimation: 5.000 Euro.