The May (critical systems) Project proposal

Abstract

Description of requisites and tasks for rehosting the CAcert critical systems to a secure and maintainable location. Appointment of NL-part of critical systems (sub-)team: ordered list of prospects located in Nld and time line of the rehosting.

A longer term follow-up plan when services have been rehosted with a full critical systems admin (NL sub-)team, short term software developments for taking up software support for policies accepted, short term development due to policy changes and longer term developments (distribution of services and servers to other locations).

Dead line of rehosting completion is 30st of September 2008.

This plan is last attempt to move critical systems to a more secure location suited for systems server audit success. This plan is vital for CAcert (as is the success of the CAcert audit project funded by NLnet).

Goal

Establish on short time frame a completion of rehosting of CAcert critical services with a move of these services of CAcert to the Oophaga servers in Holland before the 30th of September 2008.

Installation of a system admin sub-team for “physical”-support located in Holland. Due to the short term need at first an very experienced person to help in the intermediate period till other NL system admins are evaluated to take over.

Installation of software changes due to changes in the CAcert policies needed to pass the audit.

Initiation of the formation of a (critical services) system admin team and acquisition and instalment of a system admin manager.

Oophaga Foundation situation

The servers as supported by Stichting Oophaga Foundation (contract is due since April 2007, signed by CAcert in November 2007).

Oophaga Foundation is providing on contractual (non-profit) base a rack with 2 firewall PC's in 24/7 hours external management support, 4 SUN/AMD based with hardware maintenance support and 2 Intel based (Debian) servers, KVM console switch (12 ports), NAS disks and managed switches for the CAcert services. The equipment is owned and services by Oophaga Foundation.

The servers are located with BIT ISP in Ede, Holland. Physical access is only allowed when guided by Oophaga personnel. There is an individual secured access control and logging provided by BIT.

Current hosting situation in Vienna:

The two (remaining) critical services/servers, which basically services the user database/web service and signing service) are hosted via Sonance Verein at FunkFeuer internet service provision in Austria. FunkFeuer is providing internet hosting provision for Austrian groups on a non-profit base. FunkFeuer and Sonance is supported by a group of (technical professionals) volunteers. The FunkFeuer/Sonance contracts awaiting the completion of the rehosting will end at the end of October 2008.

CAcert has two half tower PC's in a half high rack case hosting the critical services (user database/web service and signing server). Only the web/user database server has access to internet. The other is running the signing service and is connected with a dedicated communication channel to the user data base server.

Oophaga Foundation has been set up in January 2007 with the goal to have all CAcert services to be relocated in Holland. For this Oophaga has received donations, made promises to funding providers and donating manufactures and initiated arrangements and commitments. The critical systems could not be move up to now due to several technical and manpower resource problems.

The secure physical access problem at FunkFeuer:
The provision lacks the strong security CAcert requirements which are also needed if CAcert wants to pass the audit of the CAcert systems. CAcert is currently being audited and received funding for this audit project in order to get the CAcert Root Key accepted into the browser mainstream.

The main technical problem:
In operation is a dedicated and specialized “serial” (COM port) protocol between web/user data base server and the signing server. The signing Debian based server has no remote console, nor a tcp/ip stack service. The serial protocol (implemented in Perl) is the only dedicated connection to the out side world, in this case the web/user data base service. The signing server needs special care on reboot (synchronisation) and is secured for unexpected and failures on access and connectivity.

The manpower resource problem:
The systems installed in Vienna due to an emergency problem by dropping the server provision allowance in Sidney, Australia in the end of 2006, Philipp Gühring was luckily able to take over the services from Duane Groth and located within a week time the services to Vienna. End of summer 2007 the non-critical services were rehosted in Holland. Philipp located in Vienna is the sole person maintaining the two remaining critical servers and has the sole control over these CAcert critical services in Vienna.

Current software used on these Debian based systems is: Apache, PHP, OpenSSL, GNUpg, Debian-tooling, and Perl. The signing service has an updated serial proprietary protocol which is current running quite stable (last down time was 3 months ago). However due to lack of COM ports on the SUN systems from Oophaga there will be a change in hardware (eg USB serial or USB link hardware). This USB-link solution needs is currently tested and is expected to be stable and should have less failures at the communication synchronisation (reboot) phase.

Prerequisites of the rehosting of (critical) services action

The rehosting to a more secure and better (access) controlled location has to meet several prerequisites:

- *secure physical access*
  There need to be an independent control on physical access and reliable reporting/logging

structure. This is more as providing means to avoid theft and damage to equipment where CAcert critical services reside. E.g. On site ISP personnel for access overview and maintenance. The dual control for physical access is arranged by Oophaga Foundation in contract with BIT as well as with CAcert. Only Oophaga and BIT personnel have a key to the doors of the server rack. Only Oophaga personnel has physical access to BIT and the servers room. Procedures are in place as described in the CAcert-Oophaga contract.

The secure physical access (audit systems) prerequisite is accomplished.

- *Server availability*
  Currently the rack has 6 servers. There is not much room in the rack left. All non-critical servers are running from BIT location for now more as one year. The 4 SUN/AMD rack servers (the main machines) have no (COM) serial ports, but have USB ports. The non-critical services (can) run as virtual hosts (or virtual machines) for CAcert services.

  The server (room) availability for critical service/server prerequisite is accomplished.

- *Signing server protocol stability*
  Initially the protocol was using a dedicated serial (COM-)port based communication protocol. The serial protocol is causing currently manual support on reboot events (protocol synchronisation problems). However due to improvements in the protocol software the stability has been significatly improved in the start of 2008.

  Due to lack of COM port hardware and bandwidth limitations a USB-link based connectivity and protocol adaptation has been developed. This USB set-up is ready for operational use and will be tried on the current running servers in Vienna. USB-links have been installed at the servers located in Holland. This is reported by Philipp Gühring in April and May 2008. The signing server protocol plays a vital role for the CAcert certificate management and signing services.

  A review of the the Perl implementation of the protocol software is initiated in May 2008 and is done by Mark Overmeer <Mark@Overmeer.net> (Holland).

  Conclusion: the signing server protocol installation is feasible and can go to the final and operational test phase.

- *Critical services system admin team*
  The (critical) services system admin team needs to be extended. These vital services of CAcert should not depend on a single person.
  Due to the signing server dedicated server situation (signing server protocol stability, security restrictions, etc.) there is a high chance that manual intervention eg on reboots is needed and so it is required that some of the CAcert personnel is located on acceptable distance from the (critical) servers hosting location. At least one team member needs to be located on maximal 1 hour distance from the location of the signing server.

  The signing server has a self securing feature, as well the filesystems are fully encrypted. So equipment theft and damage is not the big issue but systems credits provided by CAcert personnel is an issue to take care of. This technology and policy nature requires a trusted and experienced system admin team.

  (Critical) services system admin team requires expansion of CAcert team, and a part of the team members should be located near the signing server location (BIT ISP, Ede in Holland). The latter has a high priority and is critical in order to complete the rehosting of the remaining CAcert (critical) services.

Tasks for the (critical) services system admin team

Local CAcert personnel assistance

Local physical assistance (physical access to equipment) on critical services supervised by a third independent party as Oophaga engineers (dual control on physical access or four eyes principle), eg. when systems are needed manual intervention eg on synchronisation protocol problems of the critical services/servers.

On the longer term providing support for system admin maintenance for both critical and non-critical services in cooperation with CAcert system administrators for the non-critical services (wiki, bugs, blog, revocation, backups, email lists, checking services, etc.).

Resource solution on the very short term

One very experienced person familiar with security software, situated very near the location (maximal 30 minutes distance), has spare time to get acquainted to the signing server software architecture and used applications, and can optionally visit the Vienna location. The person should be able to inform the NL team members later. This person has a high priority on commitments, needs to be experienced, secure, trustful and being able to dig in the critical services technology without too much help, fairly quickly.

As soon as the critical services have been rehosted, and up and running, as well as the other team members are getting up introduced to the critical systems architecture and behaviour of the systems the time spend by this intermediate person will rapidly decrease and system admin support tasks can be redirected to the other team members located in Holland.

Secondly to this person there needs to be a less experienced person trained by taking up tasks eg on the non-critical systems system admin. The is first step to install an experienced and cooperating (critical) system admin team.

Resource solution on the longer term

Improvement of security to a distributed management situation for the secure and non-secure services. E.g. distributed key management, distributed secure and secured backup, distributed revocation services, encryption hardware if insight can be obtained, etc. This will be a challenge for CAcert and for the CAcert (critical) system admin team.

The first and high priority tasks will be to have implemented and installed the new policy schemes for CAcert assurances, Assurance and Experience Point system and the certificate issue requirements.

Recruitment of new system admin team members located in Holland, but also located elsewhere.

Tasks are the installation of secured remote system OS access, development and installation of stopped services (time stamping service, improved and more secure OpenPG signing service, etc.) and new services. Updates and upgrades of software installation and OS (Debian). The tasks are not limited to critical systems administration tasks.

Cooperation with the CAcert development team (to be installed on a later time frame) in order to get more services operational or improved.

Project Management

The current non-critical and critical system administrator teams, support team operate in a flat organisation. There is a back log in division of tasks, separation of roles, reports, development tasks, and decision taking, alignment and prioritisation of actions to be taken by the available system administrators. The new critical systems team needs to be guided. A CAcert (security) system admin project manager is needed to manage the system administrators.

The current number of system administrators is less as minimal.

A plan and proposal for a system admin project manager is being defined and is separate from this May Plan. The start of the May Plan work is independent from this but needs to fit in the total picture together with non-critical systems, critical systems admin and development team set up as soon possible.

The Project Management plan is currently defined and two prospects for the management has been found but they have not yet committed to the (undefined) task.

Current systems administrators situation:

Basically there are four persons involved in the current CAcert service system admin tasks:

Philipp Gühring < philipp@cacert.org, pg@futureware.at> is involved with *all* services and systems located in Holland as well as in Austria. Philipp is doing development, security handbook definition, CAcert-help desk, user support system admin help desk, and technical consultation as well. Philipp took over the lonely job of Duane in December 2006. Philipp is the solely person for system administration for critical services/servers under Sonance at FunkFeuer in Vienna, Austria. Philipp is the person who will have the main benefit of real team for system admins of the critical services. Philipp is located in Vienna/Austria. Philipp is full time busy with CAcert and is doing security consulting. Philipp has spend a long time with CAcert.

Guillaume Rogmany <guillaume@cacert.org, guillaume@tiebogos.fr>, mostly working at CAcert-help desk, and user support system admin. Guillaume is CAcert board member. He is located in Paris/France. Guillaume has full time job as system admin. Guillaume has spend a long time with CAcert.

Evaldo Gardenali <evaldo@cacert.org, evaldo@gardenali.biz> is system admin for the CAcert system development test system and CATS (Assurer Challenge) system admin and system hosting. He is located in Brazil. Evaldo is finishing his computer science study specialized in computer security at the university in Sao Poalo/Brazil. Evaldo is at CAcert Management Sub-Committee (M-SC) and the Board (secretary). Evaldo has spend a long time with CAcert.

Daniel Black <daniel@cacert.org, dragonheart@gentoo.org> is doing all system admin for email (list) service. He is located in Australia. Daniel has a job as system admin. Daniel is involved with CAcert system admin task from about January 2008.

Critical systems admin team, the (urgent) part of the team located in Holland

For the system administrators it is strongly advised that tall system administrators are full (at least 50 Experience Points) CAcert Assurers, and CAcert Association members.

At 15th of May 2008 a call for systems administrators for the Critical Systems have been made on the NLUUG conference. Several persons have answered on this call. Numerous talks and discussions have been held with Teus Hagen and members of the Oophaga Foundation.

All prospects are full (at least 50 experience points) CAcert assurers and are Community Members of CAcert for mostly several years. Quite some have been involved with CAcert assurance events and all of them have been involved with Open Source (Linux) operating system, system admin tasks and system application for a long time. None of them are directly involved with the Oophaga Foundation so conflict of interest areas are omitted. All persons are in a distance from Ede of less as 150 km.

For some of the Dutch prospects still a final commitment is lacking. This is why those persons are lowered in priority proposal fir the NL sub-team to take them up in the team formation. The NL-sub-team formation is prioritized as well on short term requirements and the longer term requirements.

The following list of prospects will have a very short overview and will be prioritized. This list with opinions is separated from this report and is summarized in the appendix. The comments in the appendix are seconded by a second opinions from Ian Grigg, Philipp Gühring, Rudi van Drunen and Robert Kochheim in order to get some independent input and feedback. The second opinion(s) were given only for those persons they are familiar with the prospects. The appendix with opinions is confidential and not free for distribution. Board, auditor and Philipp will be the only persons who have access to this information.

The ordered (very short term, longer term, reserve) prospect list:

1. Wytze van de Raay <wytze@deboca.net> is very experienced, more as 20 years of experience with security and Un*x/Linux system admin. Wytze is retired. Wytze lives 17 km from BIT. Is only available for short term. Is very precise.
2. Brenno de Winter <brenno@dewinter.com> is well experienced with Linux OS. Has written a lot of articles on Linux and security. Has committed only to help occasionally e.g. rebooting the systems. He is located in Ede and knows BIT well. Conclusion on for short term and only for real emergencies.

3. Mendel Mobach <mendel@mobach.nl> has more as 7 years professional Linux system administration experience at a Linux system house and Uni*x service provision, and Linux consultancy. His father is well known in the Linux community. He has committed for 33% part time to work for CAcert. He has been taken up as trainee on the CAcert non-critical systems in the end of May 2008. Mendel is living 25 km from Ede.
4. Wolfgang Nagele <mail@wnagele.com> has long time experience with Linux systems at FunkFeuer, Vienna. Has been cooperating with Philipp at FunkFeuer. Wolfgang is now working in Amsterdam at RIPE NCC, 75 km from Ede.
5. Marco Hermans <marco@mhermans.nl> has 8 year network engineer experience. Has B-screening. Experienced with Cisco equipment and SUN systems. His target is network infrastructure. Marco is located 160 km from Ede.

6. Two engineers from Tunix, under supervision from Ruud Kenbeek <ruud@tunix.nl>. Ruud is supervisor of the engineers and chief developer for the Tunix firewalls. The CAcert firewall are managed by Tunix. Tunix is located in Nijmegen, 33 km from Ede.

7. Jacco de Leeuw <jacco2@dds.nl> . Jacco has finished his computer science study at Free Universiity in Amsterdam. Jacco has not yet taken up a full time job. He has been involved with CAcert assurances and help on technology from 2004. Jacco is located in Amsterdam 75 km from Ede.
8. Two others in discussion and cannot yet be disclosed. Distance to Ede will be in 100-150 km range.

Conclusions:

- T*he short term* solutions for setting up critical systems in Holland is feasible (Wytze seconded by Brenno on short term for reboot support). Note the limited period that Wytze is able to help out.
- For *the longer term* several (critical) system admin prospects located in Holland are possible. One person is already in training. Others are well experienced but tasks need to be divided and prioritized (Mendel, Wolfgang, and Marco).
- Philipp needs to talk to the prospects (located in Holland as well other prospects from applications received in January 2008 by Evaldo) and get them informed, as well allow exercises on the test systems so a selection from those can take up operational work just after summer time.
- The other prospects (on the list at 6) to 8)) mentioned can fill gaps if they occur.

Planning

The following time schedule and milestones are planned:

1. Signing server protocol review completed, exercised and tried in operational environment in Vienna ended 15th of July 2008
2. Signing server protocol installed at BIT in test ending by 15th of August 2008. Involvement of Wytze and maybe Brenno for briefing how to deal with emergencies. Oophaga Foundation is assisting for dual control.

   Involves travel by Philipp to Ede.
3. Optionally: If needed prepare rack space in Ede and extra server buy. Ending end of July 2008.
4. Document server configurations and administration tasks for move and setup Ending 15th of July 2008.
5. Domain name transfer to IP numbers from BIT (DNS TTL decrease, transfer).
6. PR plan preparation for new Root Key installation on 15th of August.
7. Test servers ready to switch over. Ending 10th of August 2008.
8. Migrate data securely to Holland. Ending 14th of August 2008.
9. Switch over to BIT fully. Redirect domain name to Ede at 13/14th of August 2008.
10. Installation of Root Key at 15th of August 2008. Controlled by auditor, Oophaga, and CAcert.

Involves travel of Ian and Philipp to Ede.

11. 15th of October 2008 evaluation of critical systems operations. First long term critical system engineers are starting to take over system management.

    Involves a final meeting and get CAcert critical team acquainted to each other.

12. 31st of October 2008 dead line of completion of CAcert services move to Holland.

Finances of the May project

Foreseen are travel and hotel costs for Philipp (3 X) and Ian (2 X) to Holland. Costs 5 X 400 Euro. Kick off meeting costs on 15th of October 500 Euro. Spurious travel costs within Holland by critical system engineers of about 400 Euro. PR materials (t-shirts, press release) 200 Euro. Unforeseen 100 Euro.

Total on travel and PR: 3200 Euro.

Optional equipment: one server and disks: 2000 Euro.

A question needs to be made if the Audit project funded by NLnet and targeted to get CAcert audited allows 3000 Euro to spend on the May Plan.

History notes

In January the idea was proposed to have the signing protocol and the initial instalment of the critical services by a security expert and CAcert system administration expert in a 3 month spare time. This project was called Cachaca. The CAcert Board accepted a total of 3000 Euro on this projected, as well funding was committed to this project of a Dutch firm. This project did not come to concreteness and was withdrawn by the CAcert expert on 23th of April 2008. The need to drop this project was demotivating to the CAcert system administrator and a disappointment to several others.

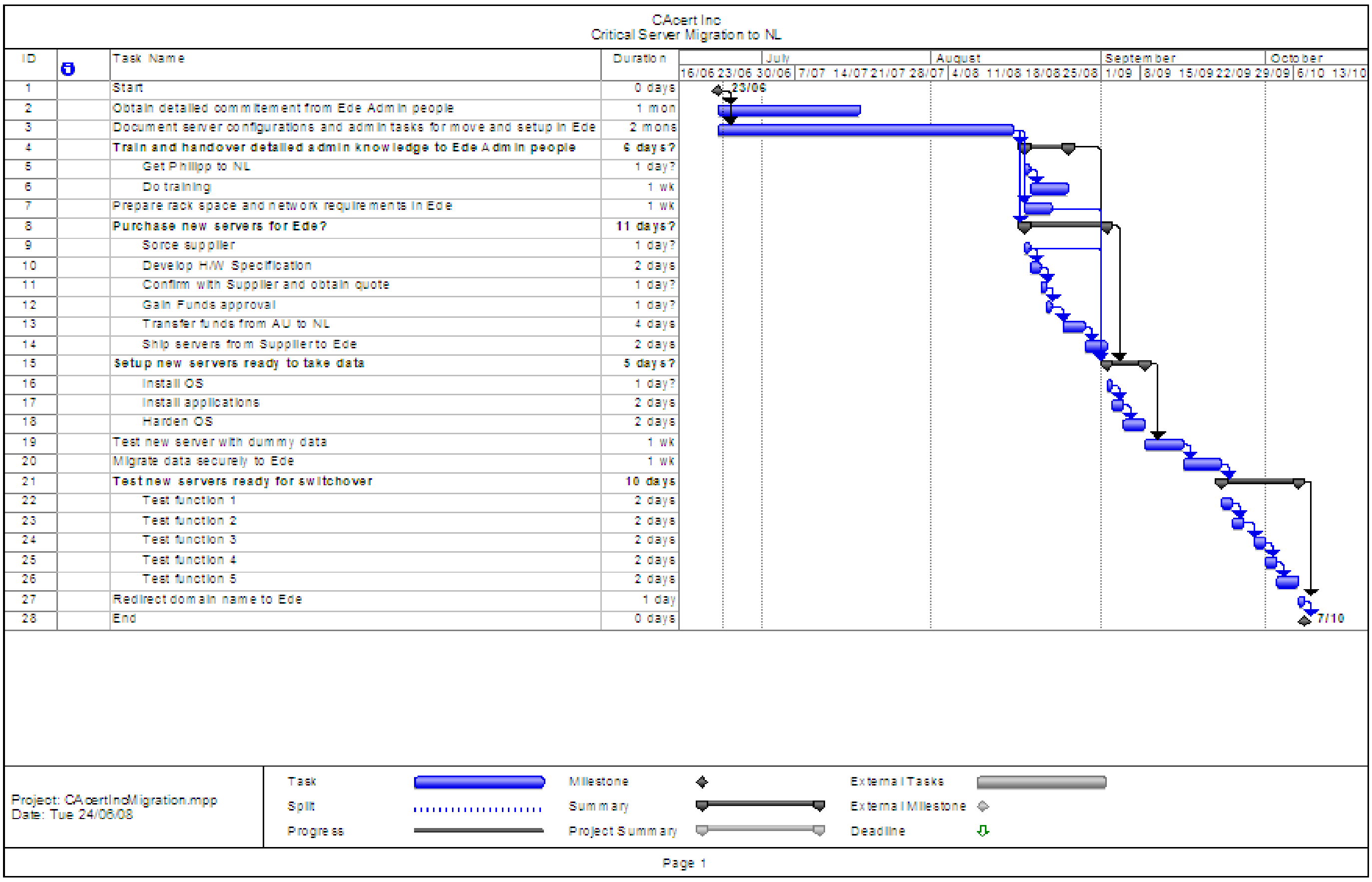
On the 29th of Februari 2008 a call has been made to apply for CAcert system administration work. At least six persons replied on the call and sent their CV. To M-SC and Board it is unclear what the follow up was and what the state now is. So it is unclear if some of these applicants can still be approached for system administration tasks for CAcert and so form a general CAcert administration team. However all of these applicants were not located in Holland so are not suited for emergency support at the server locations (Vienna/Austria or Ede/Holland).

Importance of success for this May Plan

This May plan is a attempt as last resort to get the critical services moved to a secure location. The audit of the CAcert services and systems is demanding a secure location and there is no other concrete alternative currently available. Another part of the audit is the CAcert organisation (structuring work), formal user and non-user agreements, certificate usage licensing and claim provision and the CAcert policy frame work, policies and sub-policies on different CAcert services for a CA. This audit project is funded by NLnet foundation and managed by Ian Grigg.

If the May Plans fails to succeed, CAcert will fail to pass the audit on the systems and with that will not be able to achieve CAcert Root Key inclusion in the main stream browsers by the end of this year. This will not be a good mark to the CAcert goodwill.

May Plan grand overview & table of actions, dependences and timings



CAcert Inc
Critical Server Migration to NL

ID	ⓘ	Task Name	Duration
1		Start	0 days
2		Obtain detailed commitement from Ede Admin people	1 mon
3		Document server configurations and admin tasks for move and setup in Ede	2 mons
4		**Train and handover detailed admin knowledge to Ede Admin people**	**6 days?**
5		Get Philipp to NL	1 day?
6		Do training	1 wk
7		Prepare rack space and network requirements in Ede	1 wk
8		**Purchase new servers for Ede?**	**11 days?**
9		Sorce supplier	1 day?
10		Develop H/W Specification	2 days
11		Confirm with Supplier and obtain quote	1 day?
12		Gain Funds approval	1 day?
13		Transfer funds from AU to NL	4 days
14		Ship servers from Supplier to Ede	2 days
15		**Setup new servers ready to take data**	**5 days?**
16		Install OS	1 day?
17		Install applications	2 days
18		Harden OS	2 days
19		Test new server with dummy data	1 wk
20		Migrate data securely to Ede	1 wk
21		**Test new servers ready for switchover**	**10 days**
22		Test function 1	2 days
23		Test function 2	2 days
24		Test function 3	2 days
25		Test function 4	2 days
26		Test function 5	2 days
27		Redirect domain name to Ede	1 day
28		End	0 days

Project: CAcertIncMigration.mpp
Date: Tue 24/06/08

Page 1

The project tabel has been created by Robert Cruikshank and needs to be completed by the project. This project plan will change. Suggested is to use Planner (Open Source tooling available on major distributions).

List of applicants to the February 2008 call for CAcert system admins

> CAcert Blog Posted by Evaldo Gardenali February 29th, 2008
>
> Recruiting System Administrators
>
> Calling all system administrators in the CAcert Community! We have need of help in running services like web, svn, wiki. Please contact evaldo@cacert.org if you can help.

Applicants have received on 3rd of March 2008 a more detailed overview of requirements and request for C (email from Evaldo, cc'd to Management Sub-Committee).

Ordered list of applicants:

- Nagy Gergely <nagy.gergely@gnanet.net> . System admin at Hungarian Linux company with internet servers and various Linux distributions. Involved with open source development projects.
- Matthias Diener <mdiener@macarony.de>. Works at government plant. Familiar with Linmux OS and system admin. Active CAcert Assurer.
- Charlie Garrison <garrison@zeta.org.au>. Interested to work on open source project. 8 years experience on Linux sys admin and MoinMoin/WordPress system admin.
- Jacob Steenhagen <Jacob.Steenhagen@us.hilite.com>. Experience with subversion, WordPress and MoinMoin and CAcert certificate management. Working at commercial enterprise.
- Thomas Widhalm <widhalmt@edv-widhalm.com>. System admin on mid size plant at University of Salzburg. Is CAcert Assurer.
- Matthijs Mohlmann <matthijs@cacholong.nl> System admin in north of the Netherlands. Apllied due to message on Debian email list.
- David Smith <dave@technopagan.org>. Sys admin at a small ISP. Is not anxious to take up more responsibilites.
- Ishbir Singh <ishbir24@gmail.com> . Not well experienced in CAcert technologies. Is interested to work on non-critical systems.
- Prem Vilas Fortran M. Rara <premrara@ieee.org>. Interested, no more information.
- Dirk Astrath <dastrath@gmx.de>. Is familiar with system admin, mainly with Windows system admin and less with Linux system admin (charity organisation and at home).