CAcert server/services arrangement at FunkFeuer (OxFF) , Vienna location

Abstract

This document has two target audiences:

1. *internal CAcert (Board, Management Sub-Committee, Auditor, and CAcert personnel mainly Philipp Gühring) and*
2. *external to CAcert (FunkFeuer as location and internet service provider and Sonance Verein as mediator of hosting provision).*

An overview is given of the current situation and arrangements for the CAcert critical systems located at FunkFeuer in Vienna.

The hosting is mediated by Sonance Verein. Reports of entrances to systems are outlined and a very basic dual control of physical access is proposed and should be implemented.

Access to entrance, access to CAcert critical services (access keys to systems), backup of access described is outlined. Needed actions as such providing reporting, logging and a minimum of dual control on physical access of the CAcert equipment.

This proposal respects that the FunkFeuer, Sonance and CAcert manpower resources are based on volunteers.

The arrangements as outlined in this document are temporary and limited to the interim period the systems reside in Vienna and will be voided when critical services have been moved to Holland. Expected end date: no later than the end of September 2008 (end of second half year of hosting arrangement at FunkFeuer).

The last two pages of this document are purely CAcert internal and are only of concern for CAcert.

Overview of actions and time table:

1. *Feedback on draft, acknowledge and acceptance by Sonance/FunkFeuer at end of June 2008: responsibilities, planning, contact information, extension of hosting period payment by CAcert;*
2. *Reporting and logging of access events by CAcert personnel, acknowledged by Sonance personnel (this is already started by 12th of June 2008, reporting format has been exercised);*
3. *Acknowledge of the key card logging implementation possibility and implementation/installation time frame (ca 15th of July 2008) and the key logging installation by FunkFeuer; CAcert contact needs to go via Sonance;*
4. *Evaluation of arrangements and reporting/logging 22th of July 2008;*
5. *Schedule for end of CAcert hosting at FunkFeuer at 1st of September 2008.*

Back grounds and Sonance/FunkFeuer contract situation

At 28th of October 2007 two CAcert servers (critical services: the data base / web service and signing service) have been installed at the FunkFeuer location under the contract arrangement of Sonance Verein with FunkFeuer. Two half high PCs are installed in a half high rack case in the cellar of the building. Doors of the rack case are sealed with security tape by Sonance.

The contract consists of a payment for two servers for 6 months, starting on 28th of October 2007 (there is one payment 480 Euro is made by CAcert on 12th of March 2008). Contract with FunkFeuer is a standard FunkFeuer contract and is signed by Sonance Directors (Simon Haefele and Michael Lamport). CAcert is paying the costs to Sonance for two servers (PC's). A one PC server hosting cost is 40 Euro per month. CAcert is providing Sonance logo advertisement on CAcert web site for this mediation support.

The arrangements had to be made around 15th of October 2007 in a rather short period. The problem was that FunkFeuer could not deal with CAcert directly due to contract policy requirement (hosting contract could only be done with Austrian entities), the payment requirement which did not allowing international cash transfers, and CAcert requirement to avoid direct personnel involvement of CAcert system administrator as contract mediator.

Sonance, acting as mediator for the hosting service, was able to provide a solution and support. The contract FunkFeuer/Sonance and Sonance/CAcert cover basic and standard ISP (e.g. fair use) arrangements as with other customers of FunkFeuer. Sonance is expected to put dual control on physical access using the routine FunkFeuer process of customer request for building entrance access. The CAcert Board accepted the Sonance hosting mediator contract and dual control physical access arrangement on 28th of October 2007.

CAcert expressed in October 2007 (CAcert staff meeting in Germany) that critical services rehosting to Holland location should have been finalized before 31st of December 2007. There are several reasons for failing this December deadline: failures within CAcert to solve technical problems relating to stability and reboot issues, lack of human resources and recruiting and training of a team with team member near the location in Amsterdam. At end of March 2008 the abandonment of an alternative plan Cachaca suggested as a solution caused another delay on final move of systems to Holland. Unintentionally the critical services are still (June 2008) running from Vienna.

On the 21st of May 2008 a request was made to the Sonance board to extent the first half year hosting provision for another half year, as well to highlight the need for enforcement of the dual control for physical access requirement.

As a last resort, at the end of May the *May 2008 Plan* was started to define the move of the critical systems to Holland. This May Plan is targeted for comfortable completion before the second half year period ending in November 2008, and is sent to the CAcert critical systems admin, auditor and board for acceptance on 18th of June 2008.

FunkFeuer/Sonance arrangements

Sonance is acting as billing agent for the CAcert server hosting provision, as well as the contact and control agent for the physical hosting arrangements. e.g. the minimal basic dual control on physical access to CAcert equipment.

Sonance, FunkFeuer and CAcert personnel are volunteers. Sonance and FunkFeuer personnel are well informed about the CAcert security technologies and needs. Volunteers act on the base of “best effort”.

Two arrangements are possible in order to facilitate and mandate the CAcert physical

access requirement of dual control:

1. Control and reporting via Sonance. This arrangement requires an appeal on manpower from Sonance: managing access requests, reports of access, supervision at the access times. This is the current situation, and has proven drawbacks and failures. Drawback: extra man power from Sonance. Advantage: control via the contractual line. Responsibilities and control are clearly defined.
2. Control and reporting via FunkFeuer. The management, reporting, and supervision are done via FunkFeuer directly with CAcert. Sonance mediates only for billing, administrative and contractual purposes. Advantage: shorter lines, less manpower requirement on Sonance. Drawback: FunkFeuer personnel comes closer to CAcert without legal control measures. This arrangement requires a good distance between FunkFeuer personnel and CAcert personnel. E.g. No involvement of CAcert personnel within FunkFeuer.

From October 2007 up to end of May 2008 there has been only two access reports received by CAcert. One in February 2008 and one in May 2008. In this period there must have been more access events at FunkFeuer by CAcert personnel. It is unclear if the original dual control requirements have been met. However there is no reason to believe that physical security access events have caused problems on the CAcert servers.

Sonance has indicated that they have difficulties in maintaining the dual control requirements from CAcert. This justified option 2) Control and CAcert investigated this option: reporting directly via FunkFeuer as possibility to solve the control problem as well it eases the late conflict of interest situation of Ian Grigg who has lately become a Sonance Board member. However FunkFeuer (information of Wolfgang Nagele in June 2008) is unable to provide physical access control arrangements, but can improve entrance card key use logging.

The control and reporting (option 1) has to go via Sonance. So far all reported access events (including the recent June event) Matthias Šubik from Sonance was able to help and managed the security sealing of the rack case.

The security measures:

- Card key locking mechanism of the entrance doors to FunkFeuer. The entrance access is logged (in and out entry) by a logging system. There is no entrance control by FunkFeuer personnel. Card keys have pin coverage but it is possible to use card key without the pin code.
- Web camera survey (movement triggered). Pictures are recorded and only deleted when resources are exhausted, so in general kept for months.
- personnel surveillance is not done. Visits to server rooms are done by FunkFeuer personnel and personnel from customers (volunteers, technicians). A list of key holders is maintained in a simple way.
- Security tape on CAcert servers is not provided by FunkFeuer but by Sonance. Damage control is done by CAcert personnel (at visits) and Sonance personnel. Sonance personnel is looking after security tape control.

Conclusions:

- The risk of damage to CAcert equipment can be taken till servers are moved to Nld.
- Current rack case, locking, and sealing of rack case for CAcert is for now sufficient. A door opening/closing event logging mechanism is suggested.
- The dual control for physical access needs to be improved. Help was and is provided by Sonance by Matthias Šubik. See CAcert internal and CAcert external access control procedures below. First step taken for this was on 12th of June 2008 (one

planned and one emergency visit).

- Logging of card key (in/out) usage and automatic report is possible as indicated by FunkFeuer and is suggested to be installed.
- Precautions can only be taken to minimize theft and damage of equipment and clear up events of physical access to CAcert equipment.

A simple procedure suited to this FunkFeuer/Sonance situation as well as simply enough for a short period of time should be possible and will only clear up physical access events at CAcert equipment. For CAcert it means that proper reports are possible and these reports will clear up physical situation at FunkFeuer location and will help to keep the CAcert Board informed on possible changes to services.

If FunkFeuer can do the dual control arrangements as described in 2) “Control and reporting via FunkFeuer”, Sonance can retreat from the dual control measurement and only help to solve the billing/contractual requirement of FunkFeuer (no involvement of Sonance personnel in access control; Sonance is the administrative support body). However FunkFeuer states clearly that FunkFeuer does not have these resources (17th of June 2008).

Ian Grigg has taken up in the end of 2006 the work in order to get the audit done for CAcert. As auditor Ian needs to stay independent from CAcert and its arrangements. The CAcert board, management committee and CAcert system administration personnel keeps a strong and powerful connection with Ian. In the beginning of 2008 Ian has started as board member in the board of Sonance. In order to respect his independence Ian should not be involved in decisions for the arrangements of this proposal.

Short period for CAcert critical systems at FunkFeuer physical access arrangements

The physical access control has three elements:

1. *Physical damage control*
   1.0. Breach event notice to CAcert (see contact list);
   1.1. Physical access prevention (controlled access to rack and access traced by logging);
   1.2. (Suggested) CAcert rack case door event logging and events notices to CAcert.
2. *Physical access control* to CAcert servers
   2.0. Event logging and notices (2.1 and 2.2):
      2.0.1. (Suggested) *Card key logging* of CAcert personnel will be sent separately to CAcert.
      2.0.2. (Suggested) CAcert *rack case door event*s logging.
      2.0.3. Reports and logging shall be sent via email (signed, encrypted) to contact persons and involved personnel.
   2.1. P*lanned visits*:
      2.1.1. Appointment of visit: at least one person of FunkFeuer or Sonance and CAcert person (logging of date/time visit, names of personnel, work task briefing and work time estimation);
      2.1.2. CAcert personnel entrance provision and work (physical) supervision by FunkFeuer/Sonance personnel to rack case and CAcert equipment.
      2.1.3. Reseal of rack case and supervision to leave of the location.
      2.1.4. Report will state physical materials entered and leaving the location, timings and names of personnel involved with the physical access. Report can be short and can be made by CAcert personnel and signed by FunkFeuer/Sonance personnel.
      2.1.5. Report is sent to FunkFeuer/Sonance and CAcert contact personnel via email.
   2.2. *Event visits*; supervision by FunkFeuer/Sonance personnel maybe omitted, but should be reported and avoided:
      2.2.1. If possible appointments (see 2.2.1) is made.
      2.2.2. Entrance log (see
      2.2.3. Leave log.
      2.2.4. Report (see 2.1.4). If not supervised by FunkFeuer/Sonance signature can be omitted, but should be logged as per 1.1.).
      2.2.5. Report is sent to FunkFeuer/Sonance and CAcert contact personnel.

Reports from CAcert personnel to CAcert internally will have also log the non physical arrangements made to the systems: topics, abstract of changes made, result of actions.

Contact information

***Contacts for FunkFeuer*:**
Administrative address: FunkFeuer OxFF, *street, location, phone number*.
Administrative contact: Wolfgang Nagele, mail@wnagele.com, *phone number*
Technical contact(s): Andreas Marksteiner, andreas@marksteiner.net, *phone number*
entrance key arrangement:
administrative reference number: 66

***Contacts for Sonance*:**
Administrative address: Sonance Verein, *street, location, phone number*.
Administrative contact: Simon Haefele <binsh@sonance.net>,
sonanceboard@lists.sonance.net, *phone number*
Technical contact(s): Matthias Subik, matthias@subik.at, *phone number*
entrance key arrangement:

***Contacts for CAcert*:**
Administrative address: CAcert Inc., PO Box 4107, Denistone East NSW 2112, Australia
http://www.cacert.org
Administrative contact: Teus Hagen, teus@theunis.org, +31 77 3270160, 08788722649@sip.xs4all.nl
Technical contact(s): Philipp Gühring, philipp@futureware.at, +43 66 49 953 109.

---------- *Only for internal CAcert use*

CAcert access arrangements to CAcert (critical) services

CAcert servers have self containing security measures: encrypted files systems, firewalling, and self shut down on illegal access attempts. Risks are theft or damage of CAcert equipment and reliable dual control on physical access for CAcert personnel.

Theft and damage risks are basic arguments to have both servers moved to a higher level secured facility as is available at the location in Holland, and this is the reason why the audit for part of CAcert critical servers for this location is stalled (already for a too long a period).

Up to now the passwords for data backup (filesystems, user database, access keys, ssh system access keys, root passwords and password CAcert Root Key, etc.) has been with **one** person from CAcert. At least access to critical services should be accessible to a second person if CAcert Board demands so.

Proper arrangements for services access credentials on board order shall be activated before 1st of July 2008. Action for CAcert personnel.

Options are: stored complete with usage description on data media at third party (e.g. for now in Vienna) or encrypted media.

Access for the Board shall be arranged such that at least any two Board members can order disclosure of the keys, disclosure of data backups and the use of keys is aided by documentation.

CAcert May plan

The CAcert May plan (under construction) is a *final attempt* to have the critical services of CAcert moved to Holland. This needs to be completed at the end of October 2008.

The FunkFeuer location will not be secure enough to pass an audit on system services/servers in order to fulfil the intention to have the CAcert Root Key incorporated in the main stream browsers. There is no alternative present in Vienna and CAcert should keep a proper distance from system admin a personnel interest in the servers. Thirdly the servers donated have been donated with the message that CAcert services will use this equipment (February 2007).

The May plan has the following basics:

- A technically feasible solution to communication channel between user data base service and signing service machine. Key issues are: stability, robustness, reliability, auto reboot, and security. Philipp has reported in May 2008 to be ready with this. Trial has been started already in an operational environment;
- Critical services team located in Holland and preferably on very short distance from location in Ede, Holland. Possible conflict of interest with Oophaga (CAcert server and location provider) is avoided by this separate CAcert NL team.

  Status: There is a list of about ten prospects. Second opinion of majority of the persons on the prospects list is ready. Possible interests have been investigated, but for some persons a final commitment is lacking. One person is highly experienced and located very near Ede, but only available for the first six months. One person is taken up in May 2008 as trainee and will be available for nearly 35% of his full time. One person committed work for infrastructure work

(located however 2 hours from BIT). Tunix will provide two persons.

One person living very close to BIT offered “reboot support”. One person familiar with FunkFeuer but now located in Amsterdam offered system admin help. Working plan needs to be defined, appointed and finally committed;

Funding is expected to be lower than financial arrangement and financial commitments for Cachaca project which was initiated in January 2008 and was dropped on 23rd of April 2008 for several reasons.

System Admin Manager task description and appointment

- Investigations have been started to have a CAcert general system admin. project manager appointed. The task of the system admin project (resource/task) manager is to manage the team: divide system admin work, manage definition of developments and prioritisation, acquire team members, create team cooperation, but will not be involved in technical work himself.
  Status: There are currently two prospects: one from Oophaga and one from Australia but working in Europe. Plan needs to be defined and then committed by the manager, Board, and system admins.
  If the critical system admin team plan is well defined and started, the delay of the start of the system management appointment will not be a stalling factor on the start of the completion to move the servers to Holland.

The May plan as well a System Admin Manager appointment and task description is currently defined and needs to be accepted by CAcert system admin personnel, CAcert Management Team and Board, and committed by new team members before it can be activated. Funding needs are far less as previous plan and committed budgets so the expectation is that finances will not be the bottleneck.

---------- end of CAcert internal part