Memorandum of Understanding

Between

CAcert Incorporated
and
Stichting Oophaga Foundation

I. PARTIES

This Memorandum of Understanding documents the agreement between the Australian Association **CAcert Incorporated**, NSW, Australia („CAcert“) and the foundation **Stichting Oophaga Foundation**, Amsterdam, the Netherlands („Oophaga“).

II. PURPOSE

Background

CAcert requires a service provision for its digital certification services to operate the non-profit CAcert.org website and other related free services.

Oophaga stimulates and provides on a purely non-profit basis certification services, and agrees to provide the non-profit certification service provision to CAcert.

Technical Requirements

In Appendix A „the Technical Requirements“ is the definition of the minimal technical requirements for hosting CAcert needs for its operations as of the date of this MoU. This list can only be updated by mutual agreement between CAcert and Oophaga.

III. AGREEMENT

CAcert agrees to have the physical hosting located at the ISP BIT premises in Ede, the Netherlands.

Oophaga will provide the server hardware, which is owned by Oophaga, and might be sponsored by other parties. The hardware and configuration conforms to the CAcert needs and specifications as specified in Appendix A. A description of the hardware and configuration adhering the minimal Technical Requirements list is provided and confirmed by writing by CAcert in a separate document „Oophaga-CAcert Hardware and Configuration Specification“ (Appendix A of this Document).

Governance

CAcert and Oophaga agree on their non-profit status and agree to advise eachother on any partnerships which challenge eachother status. Should the commercial status of either parties change between entry into force and termination of this Memorandum of Understanding, Parties are obliged to promply inform each other of this event. Failing to comply with this will result in the right to terminate this memorandum without any prior (written) confirmation. The results of a change as mentioned above will be further discussed between Parties and might induce a change in the status of this Agreement.

Contact and Access control

Access is controlled at two levels: *physical site and direct internet connectivity level* and *remote/virtual access level*. Each organization operates on one level. For each level there is a „Contact List“ for management and communication responsibilities and one list called „Access Lists“ for individuals who are allowed to access computer equipment and/or system administration running on that computer equipment:

1. *Remote and Virtual Access and Contact List*: for remote and virtual access and maintenance only of the Operating Systems (OS's) and firewall configuration (connectivity rules for OS and console remote access). CAcert is responsible for these Lists;
   and
2. *Physical and Direct internet Access and Contact List:* for direct access, internet configuration and connectivity rules for arrangements of the computer equipment and housing and for third party support arrangements (e.g. Tunix and BIT). Oophaga is responsible for these Lists.

Individuals on the Contact Lists:

- may change the particular Access List
- will sent a signed report for changes to individuals on both Contact and Access Lists
- will send signed report of architectural changes to all individuals on both Contact and Access Lists
- maintain a logging of events and reports.

Individuals on the Access List may:

- Instruct ISP personnel
- Access the servers for software maintenance
- Accompany appointed Third Parties.

The operation, reporting and event logging procedures for Access (contact arrangements, contact addresses, reports of events and reports of changes) is decribed in a separate document: „Procedures for Access“. All events and contact are logged for auditing of the procedures.

CAcert will require access by a CAcert appointed Third-Party Auditor. This party must only be allowed physical access to the servers in the presence of a trusted administrator of each of the Access Lists.
Other exceptions are only permitted under this agreement with a mutual and agreement in writing by the boards of each organisation.

Responsibilities
Oophaga is responsible for the certification services:

- Physical access control;
- Hardware parts, maintenance, replacement;
- Firewall management to the servers.

Oophaga makes an effort to provide the services at a reasonable level with:

- Environmental and physical safeguards;
- Fire prevention, Fire protection, Flood water protection;

CAcert is responsible for these services:

- On-site backup, storage and restoration procedures;
- Internal security management for the servers;
- Security key management;
- Use of the servers is limited to non-profit Certificate Authority services and related web services.

Costs

Oophaga agrees to provide the hosting of services mentioned above for a yearly (non-profit) nominal fee of 1500 euro per year.

Use of the name CAcert
CAcert Inc requests and Oophaga agrees that Oophaga will hold .NL domain names in CAcert's brand name, for use by mutual agreement. Oophaga agrees that CAcert owns the brand of 'CAcert' and has a final veto on any use of domains.

Emerging arrangement
Oophaga is allowed at its discretion, and solely in the case of either an emergency or an urgent maintenence arrangement to temporarily disconnect the network from hardware neede to provide the certification service rendered. Oophaga should contact CAcert personnel of the „Firewall/OS Contact List".

Termination
A termination of this hosting of services mentioned in this Memorandum can be executed by either party. Both Cacert and Oophaga agree to confirm this termination in writing at least sixty days ahead.

For full acceptance and usage of the hosting services,

Ede, 16th of Februari 2007	Ede, 16th of Februari 2007
Stichting Oophaga Foundation	CAcert Inc
two board members Oophaga	two board members CAcert

Appendix A – **Technical Requirements**

Minimal Technical Requirements

The Technical Requirements list is the definition of the minimal technical requirements for hosting CAcert needs for its operations as of the date of this MoU:

- Internet Service Provision („ISP“) for physical location of services;
- servers / firewalls / intelligent switches;
- at least 100 GB diskspace and backup facility;
- maximal 50-60G per month outbound traffic;
- maximal 3-4G per month inbound traffic;
- Access security measurements on firewall/router equipment managed by Oophaga;
- Access security measurements on certificate services managed by CAcert;
- 24x7 security control over physical access to equipment;
- Restricted access to the equipment, such that at least two authorized persons for access need to be on-site at the same time before access is granted;
- Physical security of our equipment from everyone but those that are authorized by our own audits and background checks of them;
- At least 3(?) static, public IPV4 addresses (allocated by BIT for Oophaga).

Appendix B – **Organisational Access List and Contact List**

1. CAcert Control and Access List, controlled by CAcert board:

Firewall/OS Access List

- Wytze van der Raay <wytze@deboca.net> <wytze@cacert.org>
- Mendel Mobach <mendel@mobach.nl> <mendel@cacert.org>
- Stefan Kooman <stefan@kooman.org>

Firewall/OS Contact List

- CAcert Support Team <support@cacert.org>
- Philipp Michael Gühring <pg@futureware.at> <philipp@cacert.org>
- Wytze van der Raay <wytze@deboca.net> <wytze@cacert.org>

2. Oophaga Contact and Access list, controlled by Oophaga executive board:

Firewall/Site Access List

- Rudi van Drunen <rudi@xs4all.nl> <rudi.vandrunen@oophaga.org>
- Rudolf Leonardi Maria Engelbertink <rudi@unsec.nl> <rudi.engelbertink@oophaga.org>
- Henri Johan Verbeek <h.verbeek@hccnet.nl> <hans.verbeek@oophaga.org>
- Bastiaan Franciscus van den Dikkenberg <bas@dikkenberg.net> <bas.vandendikkenberg@oophaga.org>

Firewall/Site Contact List

- Teunis Hagen <teus@theunis.org> <teus.hagen@oophaga.org>
- Robert Jan Nicolaas Kochheim <robert@hkochheim.org> <robert.kochheim@oophaga.org>

Appendix C Access Procedures

Procedures for access to equipment (physical access), access to firewall and computer consoles (KVM), and access to the operating systems.

Physical Access to equipment, firewall and console (under control by Oophaga):

- Physical* dual control access system is in place by means of at least one Oophaga representative (assurer grade) of the Firewall/Site Access List maintained by Oophaga;
- Report of access to site, firewall and console switch (KVM) is provided to the Contacts Lists;
- Logging of entrance to the location of the equipment is done by BIT for Oophaga.

Oophaga Access List members have eye scan and RF ID for entering BIT facilities and datacenter. Each Oophaga Access List member have one key for locks (front and back door) of the rack with Oophaga equipment. Oophaga Contact List safeguard a spare key of the rack locks.

Oophaga is the responsible agency for the procedures for physical access to equipment, access to firewall (surveillance done by Tunix), and access to cole (KVM switch).

Oophaga informs CAcert (CAcert Contact List member) about events before accessing the facilities at BIT and after the physical access. A third party who needs to be identified with formal ID, is only to have physical access when so reported in advance to the Contact Lists and only that person is accompanied with a Oophaga Access List member.

Oophaga maintains the Oophaga Contact List (management list) and Access List (individuals who have access) for site, firewall and console operations. Oophaga informs CAcert about changes on those list. The Contact List members are responsible for these communications.

Oophaga maintains and logs events and reports for firewall, console and site access.

Procedure for physical access to equipment at BIT location:

1. Oophaga Contact List member informs the day before the access event BIT, and informs CAcert Contact List about the access plan and name Oophaga Access List member and work to be done.
2. Oophaga Access List member identifies at BIT (eye scan and RF ID).
   The doors of the rack for the equipment are locked.
   BIT maintains a log with equipment (physical) access events. Evcents are sent to Oophaga Contact list members.
3. Oophaga List member sends signed report of operations to Oophaga and CAcert Contact List.

Secured remote and internet connectivty and configuration for virtual access to the operating systems

This is an Oophaga responsibility. For Firewall and for console (KVM switch) dual control access is in place via the Physical/Direct and Remote/Virtual Access and Contact Lists.

For access to the firewall Access List members have received security instructions, a security access token and pin from Tunix. A list of individuals with tokens is maintained by Oophaga. For Oophaga Tunix will maintain a list of pins for the token. Tunix maintains logging access events of the firewall.

For access to the KVM switch Cacert and Oophaga Access List members have received a KVM login account and password which should provide remote console access to the computer equipment.

Signed events, reports of events and changes to the firewall and KVM are sent to Oophaga and CAcert Contact and Access Lists. A record of events is kept by the Oophaga and Contact Lists members. Disputes are decided by the Oophaga board.

Tracking the tokens will be a requirement. The tokens for the firewall are "useless until enabled" by Tunix. Tunix will email (encrypted) out the enabling of every token, with the details as to who it thinks has the token. The Contact List memebrs of CAcert and Oophaga will be informed about the sending and receipt of the token codes.

Instructions for use are distributed by Tunix. Tunix is responsible for its operations to Oophaga.

Requirement and usage is a CAcert responsibility.

Procedures for remote and virtual access to and configuration of firewall and virtual monitoring of consoles (KVM switch):

1. Events: will be notified to and logged by Oophaga Contact List with a black carbon copy to the Cacert Contact List. Event will be bind to one member of Oophaga (control) and and one of CAcert Access List (operational).
2. Changes to the configuration either initiated from Tunix (firewall), Cacert or Oophaga: a plan will be notified to both Contact and Access List members. Ratification is needed from all parties. Disputes will be decided by Oophaga board. Operations are performed by one members of CAcert and one meber of Oophaga Access List members. One person of the two is designated as operational and one as controller.
3. After the operations and changes to the firewall or console switch configuration a report is sent to Oophaga Contact List (carbon copy to Cacert Contact List) and will be logged.

Operating and Software Access -- CAcert

Root access and software access to the servers is currently held on full reponsibility of Cacert (Cacert Contact List and Cacert Access List) responsibility.

Representatives

Oophaga representatives are also representatives of CAcert. The may need to be highly aware of the CAcert-controlled security plan.

Addendum Appendix B-1 to Appendix B of the contract.

Date: 15th of October 2008

This addendum describes access control to the critical servers (two computers): the web server with user database and the signing server for CAcert.

This is a practical implementation of four-eyes / dual control principle for system administration of CAcert's critical systems.

A) Web and database server

Remote access is available through ssh or KVM console server for CAcert sysadmins. All changes made to system configuration must be recorded through RCS. Dual control is not instantaneous but tracing back is possible in all cases.

Physical access is only possible through Oophaga, i.e. at least one Oophaga person and at least one CAcert sysadmin will be present at such visits. All visits will be logged by e-mail to the rehostingnl mailing list including a short description of activities performed.

B) Signing server

Remote access to this machine is ***not*** possible; its only data connection with the outside world is a serial/USB connection to the webserver running CAcert's webserver-signing server protocol.

Physical access is only possible through Oophaga. Oophaga will strive at putting an extra physical barrier in place around the signing server, e.g. a locked panel in front of its connectors or so.

For *simple maintenance actions*, at least one Oophaga person and at least one CAcert sysadmin will be present.
The Oophaga person will overview commands given at the signing server system console by the CAcert sysadmin in order to check whether operations performed are indeed simple maintenance actions, and raise a flag (both locally and later on the mailing list) when this is not the case.
Simple maintenance actions include things like:

- hookup console access
- hookup USB backup disk
- perform encrypted backup to USB backup disk (afterwards
- taken to safe storage by Oophaga)
- reboot server, including file system checks
- restart protocol software between signing server and webserver
- adjust date/time of server
- compress logfiles

Anything outside this scope is considered a complex maintenance action, and will require at least two CACert sysadmins to be present in addition to the Oophaga person.

All visits will be logged by e-mail to the rehostingnl mailing list including a short description of activities performed.

Passwords and passphrases entered into the systems will be kept private to CAcert sysadmins in all cases.