

Memorandum of Understanding

Between

CAcert Incorporated
and
secure-u! e.V.

PARTIES

This Memorandum of Understanding documents the agreement between the Australian Association **CAcert Incorporated**, NSW, Australia („CAcert“) and **secure-u e.V.**, Twistringen, Germany („secure-u!“).

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.

secure-u! stimulates and supports on a purely non-profit basis certification services, and agrees to provide the non-profit certification service provision to CAcert.

Technical Requirements

Appendix A „the Technical Requirements“ contains 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 secure-u!.

AGREEMENT

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

secure-u! will provide the server hardware, which is owned by secure-u!, 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 „secure-u!-CAcert Hardware and Configuration Specification“ (Appendix A of this Document).

Governance

CAcert and secure-u! agree on their non-profit status and agree to advise each other on any partnerships which challenge each others status. Should the commercial status of either parties change between entry into force and termination of this Memorandum of Understanding, Parties are obliged to promptly 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 to the servers (physical and remote) is governed by the CAcert Security Policy (<https://svn.cacert.org/CAcert/Policies/SecurityPolicy.html>) in the version

p20100510. Future versions of the CAcert Security Policy are automatically accepted by secure-u! unless opposed in writing within 30 days.

For the current list of control contacts see Appendix B of this Document.

Responsibilities

secure-u! is responsible for the certification services:

- Physical access control;
- Hardware parts, maintenance, replacement;

secure-u! 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;
- Firewall management to the servers;
- Security key management;
- Use of the servers is limited to non-profit Certificate Authority services and related web services.

Costs

secure-u! agrees to provide the hosting of services mentioned above for a yearly non-profit reimbursement of these costs by CAcert (for 2012: around 4000 euro).

Emerging arrangement

secure-u! is allowed at its discretion, and solely in the case of either an emergency or an urgent maintenance arrangement to temporarily disconnect the network from hardware needed to provide the certification service rendered. secure-u! 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 secure-u! agree to confirm this termination in writing at least ninety days ahead.

For full acceptance and usage of the hosting services,

location and date of signature

location and date of signature

location and date of signature

location and date of signature

secure-u! e.V.
(two board members secure-u!)

CAcert Inc
(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 700 GB disk space and backup facility;
- maximal 120G per day outbound traffic;
- maximal 10G per day inbound traffic;
- Access security measurements on firewall/router equipment managed by CAcert;
- 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 32 static, public IPv4 addresses (allocated by BIT for secure-u!).
- At least one public IPv6 /48 network (allocated by BIT for secure-u!)

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

These lists will be updated by CAcert in cooperation with secure-u!.

1. System administrators list, controlled by CAcert board:

(Remote) Access to the servers.

Firewall/OS Access List

- Wytze van der Raay <wytze@deboca.net>, <wytze@cacert.org>
- Mendel Mobach <mendel@mobach.nl>, <mendel@cacert.org>
- Martin Simons <martin@webhuis.nl>, <msimons@cacert.org>

Firewall/OS Contact List

- CAcert Support Team <support@cacert.org>
- Wytze van der Raay <wytze@deboca.net>, <wytze@cacert.org>

2. Access engineers list, controlled by secure-u! board:

Physical access to hardware.


Firewall/Site Access List

- Rudi van Drunen <rudi@xs4all.nl>
- Rudi Engelbertink <rudi@unsec.nl>
- Hans Verbeek <h.verbeek@hccnet.nl>, <h.j.verbeek@kader.hcc.nl>, <hans@cacert.org>
- Bas van den Dikkenberg <bas@dikkenberg.net>
- Stefan Kooman <stefan@bit.nl>, <stefan@kooman.org>, <stefan@cacert.org>


Firewall/Site Contact List

- Mark Overmeer <mark@overmeer.net>


This document is signed by

	Signatory	EMAILADDRESS=michael.taenzer@cacert.org, CN=Michael Tänzer
	Date/Time	Wed Jul 24 00:34:35 CEST 2013
	Issuer-Certificate	EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority, OU=http://www.cacert.org, O=Root CA
	Serial-No.	887874
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)
Note	This signature can be verified, if you open the document with Adobe Reader!	


This document is signed by

	Signatory	EMAILADDRESS=froehlich@secure-u.de, CN=Bernhard Froehlich
	Date/Time	Thu Jul 25 20:49:26 CEST 2013
	Issuer-Certificate	EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority, OU=http://www.cacert.org, O=Root CA
	Serial-No.	885586
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)
Note	This signature can be verified, if you open the document with Adobe Reader!	

This document is signed by

	Signatory	EMAILADDRESS=kueppers@secure-u.de, CN=Sebastian Küppers, O=secure-u e.V., L=Hamburg, ST=Hamburg, C=DE
	Date/Time	Thu Aug 01 08:30:13 CEST 2013
	Issuer-Certificate	CN=CAcert Class 3 Root, OU=http://www.CAcert.org, O=CAcert Inc.
	Serial-No.	72856
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)

This document is signed by

	Signatory	EMAILADDRESS=werner.dworak@cacert.org, CN=Werner Johannes Dworak
	Date/Time	Fri Aug 09 09:28:24 CEST 2013
	Issuer-Certificate	EMAILADDRESS=support@cacert.org, CN=CA Cert Signing Authority, OU=http://www.cacert.org, O=Root CA
	Serial-No.	877919
	Method	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)