





CAcert Annual Report 2013

Table of Contents

Contents

1. 1. CAcert Annual Report 2013
2. From the Committee of CAcert
 1. Terms
 2. Governance Statement
 3. The Committee's Year in Brief
 4. The Committee's Forward-Looking Statement
2. Financial Report 2012-2013
 1. Currency Rates
 2. Summary
 3. Current Assets
 4. Current Liabilities
 5. Equity
 6. Income
 7. Expenses
 8. Profit
 9. Conclusion
3. Team Reports 2013
 1. Policy Group
 1. Policy Directory Migration Project
 2. Decisions reached by Policy Group in 2012/2013 period
 3. Policy Group Work To Do
 2. Audit Team
 1. Report
 2. Outlook
 3. Infrastructure
 1. Blog
 2. Mail
 3. SVN
 4. Wiki
 4. Arbitration
 1. Precedent Cases Overview
 2. Arbitration Statistics
 5. Software Development Team
 1. Team
 2. Statistics
 3. Achievements Unlocked
 4. New Achievements Available
 6. Critical System Administrator Team Report July 2012 - June 2013
 1. Hardware changes
 2. On-site activity
 3. Off-site activity
 4. Webdb server
 5. DNS service
 6. OCSP and CRL service
 7. Backup service
 8. Firewall
 9. Infrastructure support
 10. Software Assessment Team support
 11. Events team support
 12. Interaction with other teams
 13. Team changes
 14. Plans
 7. PublicRelations
 1. Overall status
 2. Not directly connected to Public Relations, yet performed by Head of PR team
 3. Plans for the future
 8. Education
 1. Report
 2. Prospects for next year
 9. EventsTeam
 10. ATE Team
 1. Co-Audit results
 11. Assurance
 1. The Individual Assurance Program
 2. TTP-assisted-assurance Program
 12. Organisation Assurance Team
 13. New Root & Escrow Project (NRE)
 1. Building Team
 2. Outlook
 14. BirdShack
4. CAcert Members Report 2013
 1. <your name>

- This page  APPROVED in m2013?????
-  Stuff that needs completion is in Bold XXXXX 
- Reflecting headings from  last year

From the Committee of CAcert

Hereby, the Committee of CAcert Inc presents its executive report to the members of Association, and by extension, to the entire Community of CAcert. This report is over the customary period of 1st July 2012 to 30th June 2013.

In addition to that defined period, the Committee presents a Forward Looking Statement that covers 1st July 2013 and beyond. Note also that Team Reports are not so constrained by fixed periods.

Terms

The terms committee and board are used interchangeably. The terms CAcert Inc. and the Association are used interchangeably. The term Member means a member of the Community under the CCA where unqualified, and a member of the Association or the committee where qualified.

Governance Statement

CAcert Inc. is incorporated under the Associations Incorporation Act, 2009 of NSW, Australia. The members of the Association are our registered participants in the governance of our wider Community. Total Association membership at 30th June 2011 was **90**. As of time of writing, association membership stands at **100**. The wider Community outside the association currently numbers some 5,200 Assurers, around 22,000 end-users with some assurance, and over 200,000 accounts with zero assurance.

CAcert Inc. has no employees – we rely fully on a cadre of volunteers to carry out all functions.

CAcert Inc. operates under the rules of the Association, as adopted by the Association members, November 2011. In addition, CAcert Inc also binds itself by means of the CAcert Community Agreement and prior decisions at AGM and Committee to the policies of the community. Under these combined rules, the affairs of CAcert Inc. are managed by the Committee.

The Committee is elected each year at the annual general meeting. The Committee comprises the president, the vice-president, treasurer, secretary and three ordinary members. The Committee also forms a sub-committee under the rules, and incorporates the sub-committee into deliberations. The Committee meets on the Internet once or twice per month. Meetings are generally open, minuted on the wiki, and publically readable.

The Committee's primary role is to manage the services and teams of the Community. The Committee is assisted by 2 other main groups, being the Arbitration Forum for the resolution of disputes and the policy group for the creation and approval of formal policies. The Committee directly manages the many teams of CAcert, each of which work within the policy framework of CAcert, document their activities and processes on the wiki, report to the Committee, and abide by rulings of the Arbitration Forum.

The outgoing Committee provides the annual report to members at the annual general meeting. The annual report includes a financial report, team reports, a summary of the year's events and a forward looking statement to assist the incoming Committee.

The Committee's Year in Brief

All minutes can be found on the wiki:

- <https://wiki.cacert.org/Brain/CAcertInc/Committee/MeetingAgendasAndMinutes/yyyymddd>

There is a summary of the Board's activities extracted from the minutes:

- <https://wiki.cacert.org/AGM/Diary/2013>

Strategy

In response to two factors (being, moves by the CA industry, and accusations in the previous year impacted over future auditors), the board took on a far-reaching reconsideration of the primary mission of CAcert, being in short to 'get into the browsers.' This should be an important goal but not dominate everything else.

The CA industry has now imposed multiple audits on the process, and browser vendors (Mozilla and others) have followed suit without any apparent question as to the costs and competitive nature of the process. The increased costs in the process are perhaps doubling and tripling that which we have faced in the past.

As it was already in our minds that the cost of even one audit was unreachable, we are now faced with a dramatic challenge to the mission. There are yet rumours a sponsor could be found.

This has far-reaching implications. In order to address this, the committee discussed some ways to better utilise the community to get the root into the browsers on a manual basis, including browser plugins and contract changes to facilitate member-empowerment.

Before we can get external audits, we need to have internal audits. In spring 2013 a member showed up that is able and willing to do regular internal audits. In 2013 he did some preparation and will start in the beginning of 2014. Some areas of CAcert are ready for audit or have already passed an audit, in other areas essential work has to be done to be auditable.

Location of CAcert

CAcert Inc is incorporated in Australia, the original location of its founding as a community. However it has been for many years clear that the centre of members and activity for the community is located in Western Europe, mainly in Netherlands, Swiss, Austria and Germany. France becomes more important too.

Efforts to enhance the Australian base have worked partially, here Ian did an excellent work. But since Ian is no longer in Australia, the situation is very deplorable.

It is therefore our emerging view that we need to move CAcert's intellectual property and management vehicle to Europe, in order to better align with the strength of the community. In this board time there was no real progress. But just during the preparation of this AGM it became obvious that we must enforce it, maybe very fast. No Australian member showed up and was nominated till the final date. So, some of them can only be nominated during the AGM.

The Committee's Forward-Looking Statement

July 2013 to November 2013 (AGM Time)

This period has already passed, and this section can be seen as a preliminary briefing on the period. However, the next year's full report will properly replace this entire section with a formal report.

- The participation of the Australian Board members has been worse and worse during that time, but sadly no one really responded in good time.
- We finally appointed more arbitrators and some new arbitrators did good work. But still we need more arbitrators. Many old arbitrators are very busy with other tasks and are no longer active.
- The software team was rather active and some important patches are settled now. We now ask for confirmation to CCA on all sensible occasions, so at least all active members agreed the CCA now.
- There have been enhancements to the support console and precedent cases, so more cases can be handled now without explicit arbitration.
- Since it became important to get a new root certificate with a SHA256 hash and we need an auditable escrow method, we started a "New Roots & Escrow project".

December 2013 to End-2014

Looking forward, the Committee has to face one giant challenge, that is to move CAcert from the present Australian CAcert Inc. to an European incorporated association or similar form of organisation.

Even if at the moment some Australian members would show up, I have no hope that we get a well working Australian community in the long term. Besides that most members are in Europe and opposed to most other parts of the world, in Europe we have a well working and cheap banking system established, so we would save an enormous amount of bank transfer costs and exchange costs if our main account is there. And we have many active people nearby, so many travels are just some dozen or hundreds of kilometres.

As we can see at present, nearly all contracts can be easily transferred. But the community and the CCA are the stumbling block. It looks like we need a consent of each community member to transfer the legal binding to the new association, but many are nor very responsive and maybe a lot of email addresses do not exist any more.

[CategoryCAcertInc](#)

[To AGM](#) - [To AGM/Next](#) - [To Financial Reports Overview](#) - [To AGM Board Report 2013](#)

Financial Report 2012-2013

Currency Rates

Currency rates at the end of the fiscal year:

- USD: 0.923012
- EUR: 0.705667

Summary

Description	2012/2013	Diff.	2011/2012
Current Assets	9474.17 AUD	-35.2%	14613.19 AUD
Current Liabilities	3873.55 AUD	+2.7%	3772.41 AUD
Equity	5600.62 AUD	-48.3%	10840.78 AUD
Income	3336.77 AUD	-16.5%	3995.90 AUD
Expenses	8576.93 AUD	+83.1%	4684.08 AUD
Profit	-5240.16 AUD	+661.5%	-688.18 AUD

Current Assets

Acc. No.	Account Name	2012/2013	Diff.	2011/2012
B212	Accounts Receivable USD	523.93 USD is 567.63 AUD	+302.4%	143.93 USD is 141.06 AUD
B421	Westpac Transaction Account	286.10 AUD	-17.2%	345.68 AUD

B422	Westpac Savings Account	3220.24 AUD	-70.8%	11042.51 AUD
B423	Credit Union Australia	137.25 AUD	+0.0%	137.25 AUD
B431	PayPal AUD	3058.16 AUD	+56.4%	1954.80 AUD
B432	PayPal USD	1969.22 USD is 2133.47 AUD	+132.6%	935.84 USD is 917.18 AUD
B433	PayPal EUR	50.33 EUR is 71.32 AUD	-4.5%	60.55 EUR is 74.71 AUD
	Total Current Assets	9474.17 AUD	-35.2%	14613.19 AUD

Current Liabilities

Acc. No.	Account Name	2012/2013	Diff.	2011/2012
E113	Accounts Payable EUR	456.00 EUR is 646.20 AUD ²	-126.1%	-2000.00 EUR is -2467.80 AUD
E32	Provisions for bills to receive	3227.35 AUD ³	-48.3%	6240.21 AUD
	Total Current Liabilities	3873.55 AUD	+2.7%	3772.41 AUD

2: Contains the contribution to the new infrastructure server.

3: Contains the anticipated hosting costs for the first half of 2013 and additionally anticipated power and phone line costs for the end of 2012.

Equity

Acc. No.	Account Name	2012/2013	Diff.	2011/2012
C3	Retained earnings (last year)	10840.78 AUD	-6.0%	11528.96 AUD
PNL	Retained earnings (this year)	-5240.16 AUD	+661.5%	-688.18 AUD
	Total Equity	5600.62 AUD	-48.3%	10840.78 AUD

Income

Acc. No.	Account Name	2012/2013	Diff.	2011/2012
F1	Donations	1391.72 AUD	+4.1%	1337.00 AUD
F21	Membership Fees	924.88 AUD	+101.3%	459.54 AUD
F22	Assurer Certificates	49.78 AUD	-60.0%	124.59 AUD
F23	Password Reset Service	492.79 AUD	-33.1%	736.28 AUD
F3	Advertising Income	449.95 AUD ⁵	-60.7%	1145.98 AUD
	=> Total Own Income	3309.12 AUD	-13.0%	3803.39 AUD
G1	Interest Income	8.39 AUD	-94.5%	153.85 AUD
G2	Income Suspense	19.26 AUD	-50.2%	38.66 AUD
	=> Total Other Income	27.65 AUD	-85.6%	192.51 AUD
	Total Income	3336.77 AUD	-16.5%	3995.90 AUD

5: Main reason for the decline is that dental trade didn't book an advertisement this and the previous year

Expenses

Acc. No.	Account Name	2012/2013	Diff.	2011/2012
I22	Events	476.42 AUD ⁶	-	-
I74	Hosting	6937.05 AUD ⁷	+54.1%	4500.30 AUD
I75	Other Computer Costs	561.24 AUD ⁸	-	-
I82	Bank Service Charges	652.41 AUD ⁷	+372.0%	138.23 AUD
I83	Exchange Variance	-50.19 AUD	-210.2%	45.55 AUD
	Total Expenses	8576.93 AUD	+83.1%	4684.08 AUD

6: Contains the costs of the **BarCamp Melbourne, Australia, decided by the previous board** and the **ATE in Manchester, UK also decided in the previous FY**

7: Anticipated hosting costs from the previous years didn't fully cover the actual hosting costs billed in this FY. So the increased hosting account from too low hosting costs in past years and increased hosting costs for FY12/13. Also a lot of banking charges are associated with the actual payment of these costs. Some of these banking charges are actually charges from past years (we sent money to Oophaga some time back (2011-11-28) but **PayPal** charges were applied on the way resulting in less money actually

available to Oophaga (105€ less), now we paid some more to cover these).

8: Contains the contribution to the new infrastructure server.

Profit

2012/2013	Diff.	2011/2012
-5240.16 AUD	+661.5%	-688.18 AUD

Conclusion

















The increased loss is mainly due to exceptional costs for the hosting payment but other things like less advertising income, the supported events and the investment in the new infrastructure server did also contribute to this situation. In the long run we need to cut the hosting costs on one hand (we plan to reduce our rack space to half a rack and get rid of the phone line), bank transfer charges (I'm currently investigating a bank account in Europe but that comes with some fees and bureaucracy too) and on the other hand increase our income. Question is, if we want to do that through donations or go the advertisement route again.

CategoryCAcertInc

[To AGM](#) - [To AGM/Next](#) - [To AGM TeamReports Overview](#) - [To AGM Members Reports Overview](#)
[To AGM Members Report 2013](#)

Team Reports 2013

Team Leaders are encouraged to present a report for their team.

1.	#PolicyGroup	
2.	#AuditTeam	
3.	#Infrastructure	
4.	#Arbitration	
5.	#SoftwareDevelopment	
6.	#Critical	
7.	#PublicRelations	
8.	#Education	
9.	#EventsTeam	
10.	#ATE	
11.	#Assurance	
12.	#OrganisationAssurance	
13.	#SupportTeam	
14.	#AffiliateProgramme	
15.	#New Roots & Escrow Project Team	
16.	#BirdShack	

Policy Group

The year in Policy showed some activity. The main work was focused to fix specific sentences that have moved over the past few years since the initial start of the policies. Assurance subpolicy POJAM moved to status POLICY after a quite long period in DRAFT (since February 2010) while we've collected experience in practice in the assurance area and we did receive all good feedback.

Policy Directory Migration Project

Since the initial start of the [PolicyOfPolicy](#) the location of all Policy's in DRAFT or status POLICY to be placed into a subdirectory of the critical system turns into a complicated process, that turns into a backlog of 4 years of update changes that requires to be transferred into the critical system.

Since December 2009 the Software Assessment project team deployed a running infrastructure to write patches and move them to the critical team. This process is now running in a good shape. But the backlog of Policy update changes didn't make it yet under the main CAcert website.

With a potential conflict of authorities between two teams - Software Assessment vs. Policy Group, one problem has been fixed first by Policy Group, to allow updates of the Policy documents under the Critical System so that the collected required Policy updates can be transferred by the Software Assessment team without further big discussions and each individual voting in Policy Group ([p20130223](#)).

This effects Policy updates that have been voted in effect by Policy Group long time ago, but didn't find its way into the "officially" listed Policy in the Critical system. Also link fixes and reference updates (eg. the RDL that replaced NRP-DaL in 2010) and other "minor" changes, that didn't change the policy text and their meaning. The collection of Policy Updates patches running under [Bug #1131](#) "Rename _all_ Policies from .php to .html and fix all links"

Decisions reached by Policy Group in 2012/2013 period

p20121113 DRP - minor clarifications to parties, etc	Motion FAILED
p20121213 DRP - minor changes, excluding controversial issues	Motion CARRIED . Consensus of 30:0
p20130116 DRP - drop three references to Board's role in Appeal	Motion CARRIED , (20:1)
p20130222 PoJAM to POLICY	Motion CARRIED with consensus of 21:0
p20130223 Several minor changes to PoP to DRAFT	Motion CARRIED . Consensus of 19:0 reached

Policy Group Work To Do

1. New Legacy Policy - how to handle "old" assurance and experience points, eg a fade-out? revocation of points? cut of old Superassurance Points down to 35 Pts?
2. CCA review / rework - still WIP (75% finished)
3. DRP review / rework - still WIP
4. CPS review / rework
5. TTP-assisted-assurance Sub Policy to POLICY (once TOPUP program is activated)
6. RDL to POLICY
7. Security Policy review (to POLICY?) (defining Escrow role?)
8. CCS to POLICY
9. Organisation-Assurance Policy review / rework (requires some preparation by the OA team)

Audit Team

Report

Audit Activities in FY 2012 / 2013 had been limited to case handling on request, since the master plan to get CAcert Audit ready was not executed as planned.

Since April 2013, [Benedikt Heintel](#) is working as internal Auditor for CAcert. Between April and June no request was handled.

Outlook

Starting in January 2014, it is planned to conduct a yearly internal Audit over CAcert. For this reason, an Audit plan will be created in January 2014 containing especially, but not limited to, Audit over CCA, Critical Infrastructure, Arbitration, and New Roots & Escrow Processes.

To build a strong audit capability, further internal Auditors shall be included in the Audit Team.

Benedikt Heintel
CAcert Lead Auditor

Infrastructure

Team members, Admins, Others - Feel free to add anything you think is worth mentioning. Either as text or bullet list. The report will be edited in time before the AGM.

This report does not necessarily cover CAcert's financial year, but the period from last AGM until now.

- Current (active) team members
- Maintenance on many VMs has stalled, outdated OS releases, list added to Systems somewhen
- New server / hosting
 - Dev

Blog

After resignation of Daniel as Infrastructure Team Leader and admin, maintenance on Blog was stalled - the system was still running Debian Lenny and almost no updates and security updates were applied. In July 2013 Mario did a complete new setup of the system now running Debian Wheezy and migrated the old Wordpress 2.5 installation to the most recent Wordpress 3.5.2 vanilla version. The new installation features a working media gallery that allows authors to upload images and to include them in their posts and an update function

that can easily install updates for Wordpress and plugins from the web admin interface. To ensure compatibility with the new wordpress version, a new theme was hacked up, and the client certificate authentication plugin was reimplemented and is now available from the [wordpress plugin directory](#). The Client Certificate Authentication plugin allows users to login based on a matching email address in the client certificate and in wordpress, and creates new users automatically and grants them author privileges. Also, SSL related issues were fixed with the upgrade. The admin list in the application was cleaned and privileges have been granted to Marcus Mängel and Alexander Bahlo (in addition to the system admins) allowing them to initiate Wordpress and plugin updates, and to manage plugins. Martin was appointed as system administrator for Blog and will care about keeping the Blog up, running and updated. Changes in the output of the RSS feed [broke the display of the news item teasers on the CAcert start page](#). Martin prepared a patch for LibreSSL that features proper XML parsing of the news feed.

Mail

- ABC on Jochim

SVN

In May 2013, Jan updated SVN to the latest Debian release Wheezy. The upgrade went very smooth without any problems.

Wiki

From April 2013 until July 2013 we were experiencing severe load problems caused by the wiki being hit by bots. By using files as data storage, MoinMoin got very slow on some actions. We have taken several counter measures, including: backported a fix from an upcoming MoinMoin version that improves the performance for the action rss_rc for single pages to which a link is included in every wiki page, remove the link to a fullsearch on the current page in the breadcrumb, run moin maint cleanpage to remove deleted and spam pages from the system, run custom deleteusers.py script that deletes all users that have not subscribed to or edited any page (in total a number of ~8000 users were deleted, less than 1000 remaining). In June 2013, Martin performed an upgrade of the system to Wheezy and updated MoinMoin to the latest version.

Arbitration

Alex Robertson took over the role of DRO just prior to the last AGM

It appears that only four arbitrators (two regularly active, one is busy but doing some work and another appears sporadically and then disappears again!) and one arbitrator in training are currently active. This means that long delays are likely to occur before non-urgent cases get processed. All of the currently active arbitrators have a caseload. There are several very old cases stalled because the arbitrators who have taken them on have not been seen in either team meetings or in relevant wiki updates.

Subsequent to the reporting period, one new arbitrator (Eva Stöwe) has joined the team and one (Joel Hatsch) has resigned.

Six team meetings were held during the report period – but attendance dwindled over time and it seemed pointless holding a formal meeting with only two attendees for after the report period.

The proposed rewrite of the DRP (mentioned in last year's report) has stalled) – the person who volunteered to do this has not been heard from for many months.

Currently the arbitration team is struggling to cope with the flow of cases which means that the backlog is increasing and there is a desperate need to get more active arbitrators but there is the additional issue of having sufficient active experienced arbitrators available to effectively mentor new candidates.

Alex Robertson DRO

Arbitration Statistics 01 July 2012 to 30 June 2013		
Cases Opened	28	
Cases Closed	19	
	From 2013	2
	From 2012	11
	From 2011	4
	From 2010	2

Current Status as at 5 Nov 2013	
Cases currently in Arbitration	61
Cases awaiting Arbitration (< 1 year)	11
Cases awaiting Arbitration (> 1 year)	30

Precedent Cases Overview

Cases handled by support under precedent rulings	
Arbitration Precedent Case	Handled following precedent by Support or Critical team
a20090525.1 Events scripted mailings	7
a20100210.2 Revoke assurance 24 hours / 3 days / 7 days after an event	2
a20111128.3 Delete Account cases which may be handled by SE - No Assurances given, no certs or certs expired	69
a20111204.3 Minor account data differences which may be handled by SE	1
a20101025.1 Removal of posts from mailing list archives	3
Total	82

Arbitration Statistics

Statistics by Year (FY)

FY 2012-2013

Cases closed from year	2012						2013						Still open/running totals
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	
2009	0	0	0	0	0	0	0	0	0	0	0	0	5 (-0)
2010	0	0	0	0	0	0	0	1	1	0	0	0	18 (-3)
2011	0	0	0	0	0	0	2	0	2	0	0	0	27 (-5)
2012	1	1	1	2	1	2	0	0	3	0	0	0	37 (+4)
2013							0	1	0	0	1	0	7
Total	1	1	1	2	1	2	2	2	6	0	1	0	94 (+3)
Total New	6	2	0	1	6	1	1	1	1	3	2	1	25
Active Arbitrators	1	1	1	1	1	0	1	2	2	0	1	0	1-2

Arbitration table 1

Statistics period July 2012 - June 2013

Arbitration	2012			2012				2013			2013			Sum			
	Jul	Aug	Sep	Q3	Oct	Nov	Dec	Q4	Jan	Feb	Mar	Q1	Apr		May	Jun	Q2
New = Total	6	2	0	8	1	6	1	8	1	1	1	3	3	2	1	6	25
Running	4	0	0	4	0	5	1	5	1	0	1	2	3	1	1	5	16; Ø 4/month
Closed new	1	1	1	3	1	1	0	2	0	1	0	1	0	1	0	1	7
Closed total	1	1	1	3	2	1	2	5	2	2	6	10	0	1	0	1	19
Total	6	2	0	8	1	6	1	8	1	1	1	3	3	2	1	6	25

Arbitration table 2: statistics per period (seperated into quarters)

Number Arbitrators																		
Arbitration	2012			2012				2012			2013			2013			2013	
	Jul	Aug	Sep	Q3	Oct	Nov	Dec	Q4	Jan	Feb	Mar	Q1	Apr	May	Jun	Q2		
on list	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15	15
inactive	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
busy	9	9	9	9	9	9	10	9	9	8	8	8	10	9	10	9	10	9
active	1	1	1	1	1	1	0	1	1	2	2	2	0	1	0	1	0	1

Arbitration table 3: Arbitrators active/busy/inactive

Long term statistics 2008 - 2013

Arbitration	2007		2008		2008		2009		2009		2010		2010		2011		2011		2012		2012		2013	
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
New = Total	2	2	0	3	1	0	8	38	29	33	55	16	23	17	35	24	17	33	20	19	8	8	3	6
Running	0	0	0	0	0	0	2	11	11	12	42	15	20	11	14	4	15	4	20	16	4	5	2	5
Closed new	2	2	0	3	1	0	6	27	18	21	14	1	3	6	21	6	2	4	1	3	3	2	1	1

Closed total	2	2	0	3														48	20	14	18	17	7	3	5	10	1
Total	2	2	0	3	1	0	8	38	29	33	55	16	23	17	35	24	17	33	20	19	8	8	8	8	3	6	

Arbitration table 4: Long term Arbitration statistics new/running/closed

Number Arbitrators																								
Arbitration	2007		2008		2008		2009		2009		2010		2010		2011		2011		2012		2012		2013	
	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
on list											14	14	12	12	12	12	12	12	12	13	15	15	15	15
inactive											4	4	3	3	3	4	5	5	5	5	5	5	5	5
busy											7	6	5	5	6	6	6	5	6	7	9	9	8	9
active	1	1	0	3							3	4	5	5	3	2	1	2	1	1	1	1	2	1

Arbitration table 5: Long term statistics Arbitrators active/busy/inactive

Software Development Team

The software development team including software testers, developers and assessors continued their work to improve and fix the existing CAcert software.

Team

Some testers were coming and going while there's a core tester group which continues to work away in each weekly "software assessment" meeting. So tests were done in a timely fashion. Marcus and Magu, who previously were mainly involved in testing the software, now did more development work, preparing changes for later review by the software assessors. With about 2.5 active software assessors, proposed changes get reviewed continuously but there is certainly room for improvement (mea culpa).

Statistics

Over the past year we have resolved 165 issues while "only" 93 new ones were opened. That means we are down 72 open issues compared to last year. Of these 165 resolved issues, 58 resulted in a patch request to the critical admin team. But we can certainly improve on the average time until a bug gets fixed, which is 1,180 days at the moment. If you need more statistics, just head to the [statistics page on our bug tracker](#).

Achievements Unlocked

- Submit 50 patches within one year
- Add support for the new TTP programme
- Lots of small UI improvements
- In-browser key generation for Internet Explorer on Windows Vista and beyond (yes, it's 2013)
- MSI package for easier installation of the CAcert root certificates on Windows
- Easier account deletion for support

New Achievements Available

- Submit 75 patches within one year
- Add and record CCA confirmation to all relevant parts of the software (ca. 90% complete)
- Use the new point calculation in all relevant parts of the software (ca. 15% complete)
- Rewrite signer and [CommModule](#)
- Support the new roots project
- Load balancing and traffic optimisations for revocation information (OCSP and CRLs)
- Prepare the software to remove legacy PHP features
- Implement the password reset by Assurance in the system

Michael Tänzer
Software Assessment Team Leader

Critical System Administrator Team Report July 2012 - June 2013

Hardware changes

A major change made to the hardware infrastructure for the CAcert servers in the past reporting period was the phasing out of the original webdb box (an old Intel Pentium 4 based PC) by migrating the webdb services to sun2. Otherwise, there were no component failures requiring a hardware replacement in the reporting period.

On-site activity

The log of visits to the hosting facility shows the following "on site" activities:

- [03.07.2012] retire old signing server drive

- [27.07.2012] install software patch on signing server
- [07.02.2013] install cables and patch signer
- [03.04.2013] upgrade/migrate webdb server
- [13.05.2013] take spare switch cisco2 offsite for reconfiguration
- [19.06.2013] restore correct operation of CAcert signing server
- [20.06.2013] restore correct operation of CAcert signing server

The total number of visits (7) was somewhat smaller than in the previous year (9), and only 2 of these 7 visits could be labelled emergency visits. These two consecutive visits, on 19 & 20 June 2013, were caused by a flaw in the serial number administration of the Class 3 certificates which had been introduced there many years ago (around May 2005) by the original operator of the service. After analysing the results of the first visit, another visit was made the next day to permanently solve the problem.

Off-site activity

All other (i.e. most!) system administration work has been performed remotely. Issues directly affecting the operation of the webdb server continue to be logged to the [✉ cacert-systemlog@lists.cacert.org](mailto:cacert-systemlog@lists.cacert.org) mailing list (archived at [🔗 https://lists.cacert.org/www/arc/cacert-systemlog](https://lists.cacert.org/www/arc/cacert-systemlog)) with headings like "configuration change webdb server", "security upgrades webdb server" or "cvs.cacert.org checkin notification". This logging is also used for changes to all other services like DNS, OCSP etc. under critical-admin management. A total of 107 messages were posted on this mailing list during the year.

Webdb server

At the start of April 2013 the webdb server has been migrated to another hardware platform (sun2), with much better performance characteristics for this critical server. With 4 AMD Opteron cpus, 4 GB of internal memory and two 15000 rpm disks in mirror configuration, the response time of this system has improved tremendously.

In conjunction with the hardware migration, a software upgrade from the no longer supported Debian "Lenny" release to Debian "Squeeze" (oldstable) was performed, both for the system itself and for the chroot environment in which the web server runs.

The three disks of the old webdb server have been shredded meticulously with the GNU shred utility. They are still present in the locked hosting cabinet, awaiting removal to secure-u secure storage and eventually controlled destruction.

Other maintenance work on the webdb server during the reporting period involved:

- 7 installations of one or more Debian security updates
- 5 configuration changes
- 54 application software patch installations

thus making a total of 66 critical admin interventions for this server (previous year: 102).

DNS service

The DNS service has been continued in the same configuration as the previous year. Maintenance activities for this server boiled down to:

- 4 DNS software version updates
- 1 configuration change
- 6 installations of one or more OpenSuSE security updates
- 1 Key Signing Key rollover (for each of 3 zones)
- 8 zone file changes

thus making a total of 20 critical admin interventions for this server (previous year: 30).

OCSP and CRL service

The OCSP service and CRL services have also been continued in the same configuration as the previous year. Maintenance activities for these services boiled down to:

- 1 OCSP software changes
- 5 installations of one or more OpenSuSE security updates

thus making a total of 6 critical admin interventions for this server (previous year: 13).

The availability of the CRL service has been decreasing over the year. This is caused by a number of factors:

- the CRLs are growing larger and larger as more certificates are revoked, but all revocations are kept on the CRLs, including those for certificates which have expired;
- the number of consumers for these CRLs is increasing, in particular a number of consumers which attempt to retrieve the CRLs at a much higher frequency than really sensible (once per week should be OK for most purposes);
- the resulting heavy traffic is causing congestion in the external firewall from time to time.

Note that we are routinely pushing out over 100 GB of data *per day* from just this server. Plans are being made to improve the situation in the next year, in a number of ways:

- reduce the size of the CRLs by excluding expired certificates;
- provide an rsync service for retrieving fresh CRLs much more efficiently than with http;
- replace the external firewall by a modern more efficient engine.

Backup service

The boxbackup server has also been continued unchanged, with maintenance activities limited to installing a number of OS updates:

- 1 installation of one or more Debian security updates

thus making a total of 1 critical admin interventions for this server (previous year: 7).

Firewall

The external firewall is managed and operated by Tunix, as a donation to CAcert. However, the critical admin team is responsible for providing the correct configuration instructions to Tunix for the firewall mgmt. In the past year 3 firewall change requests were generated and monitored (previous year: 6). In addition a discussion has been conducted with Tunix regarding the disappearance of the backup telephone line to the firewall.

A project has been started to replace the complete Tunix firewall by a new small-footprint and energy efficient setup based on two Alix cards. We hope to be able to complete the replacement before the end of 2013. In conjunction with this change, the switch configuration will be overhauled, in order to reduce the number of hardware components employed, and improve the redundancy in case of failure.

Infrastructure support

After migrating all (non-critical) infrastructure services to infra01 in the previous reporting year and providing it with its own external USB backup drive, very little support has been required from the critical admin team for this server.

Recommendations have been made for the acquisition of a more powerful and energy-efficient infrastructure server, to be donated by a hardware vendor. This new server will be deployed at the end of 2013.

Software Assessment Team support

We continued to support the Software Assessment Team by maintaining a test server (on a virtual machine) which looks as closely as possible to the production webdb server. A second similar test server is also maintained for special critical system tests and preparation of major software upgrades.

The patch process developed by the Software Assessment Team has resulted again in a significant number (54) of successful patch updates to the production server (previous year: 60).

Events team support

From time to time the events team wants to inform CAcert members about important events like Assurer Training Events and the like. These mailings are performed by adding a custom script to the webdb server and running it against the current database. Based on arbitration <http://wiki.cacert.org/Arbitrations/a20090525.1>, such scripts are prepared by the events team and handed over to the critical admin team for installation and execution. 8 cases were handled in the past year.

Interaction with other teams

From time to time the critical admin team also receives requests from other CAcert teams like Support and Arbitration, which we try to handle as quickly as possible. The total number of e-mails processed or generated by the critical admin team during the reporting year amounts to around 1000.

Team changes

In March 2012 we found Martin Simons as a suitable candidate for reinforcing the critical sysadmin team, but due to the long time it took for the required ABC to complete, we could finally welcome him on November 1, 2012.

Plans

Plans for the coming year include:

- migrate entire server cabinet to a half-height cabinet to reduce hosting costs
- implement and deploy a new energy-efficient and well-performing external firewall based on Alix cards to replace the ageing Tunix firewall
- upgrade webdb server and boxbackup server to Debian Wheezy
- improve availability of OCSP and CRL services
- prepare system software upgrades (Debian Wheezy, OpenSuSE 12.3)
- improve system monitoring
- expand and improve server documentation
- look for strengthening of the sysadmin team

Wytze van der Raay, Mendel Mobach, Martin Simons
Critical System Administrator Team

PublicRelations

Overall status

- Starting in July 2013 with professional layout
- Sending press releases every 1-2 months

- Extending the list of press release recipients by many times
- Supporting fair events, namely [LinuxTag](#), and FOSDEM by answering detailed enquiries from our customers about the current status of CAcert development to make them understand that CAcert is not stuck at some point or taking the wrong direction, as well as supporting FrOSCon, and [OpenRheinRuhr](#) for building networks

Not directly connected to Public Relations, yet performed by Head of PR team

- Application, Planning, Organisation and event presentation for CAcert at [LinuxTag](#) Berlin (luckily less work this year due to better communication from [LinuxTag](#) staff and, of course, experience from last year).
- Suggestion for the correct wording of a mailing to secondary mail addresses of members with Lavabit primary mail address.
- Supporting non-yet-SSL-ready websites which are trying to implement SSL in order to use CAcert certs (unfortunately without success because CAcert is not in browsers).
- Presenting CAcert attendance on events to common social websites like XING, [LinkedIn](#), Google+ and starting Facebook, as long as event owners inform us about the event and they cannot do themselves. Especially for international events and ATEs in general there is no information on both these medias and information to me, so just by accidentally finding out that there is an event about to start I advertise most of these events.

Plans for the future

- Getting the account of a Twitter account named "CAcert" with the help of Dirk Astrath. Presently it's practically unused and owner is unknown. This user would give a better chance to publish news on Twitter rather than with the present account "CAcert_ATE".
- There is an account of CAcert Inc. on [LinkedIn](#) (<http://www.linkedin.com/company/cacert-inc.>) which I got access to from Martin Gummi, but unfortunately I got no information about what board wants to show there. Is board aware of this company profile?
- Building a new community besides the page profile of CAcert on Google+, probably presenting as "secure-u".
- Building up an existing profile on Facebook.
- Creation of a mobile game about security and CAcert certificates. We do have a developer reader for programming but we need more ideas on how to make the importance of encryption easily understood.

Any help is appreciated!

Alexander Bahlo
Officer for Public Relations

Education

Report

Management of CATS and the Assurer Challenge

Not many news this year.

The CATS repository has been moved to github (<https://github.com/CAcertOrg/cats>) and documentation of the installation procedure has been created. Currently there is a problem with the question management, probably since the OS upgrade to Debian Wheezy. Every modification to a question's text seems to set the text to empty! I hope I get to analyzing and fixing this soon...

No progress with translations.

During 2012 (numbers only available per calendar year), 72 PDF certificates and 10 printed certificates for passed Assurer Challenges have been issued.

Still there's no interface for Education to verify that a certificate applicant has collected 100 Assurance Points, so Support has to be contacted for every certificate request.

Some statistics for the time July 2012 to June 2013:

- 1842 test have been made, 744 english Assurer Challenges, 942 german ones and 78 Triage Challenges
- 692 of the Assurer Challenges has at least 80% correct answers and are therefor counted as passed
- 609 different users (that is, different certificates used to login) have passed the test at least once
- 120 users tried the test at least once but don't have a successful test recorded
- On the average those who passed the test had about one (more exactly: 0.92, compared to last year's 0.91) unseccessful tries before passing.

Prospects for next year

The same as last year:

- Finish the started translations of CATS test and user interface.
- Extend and update the pool of questions for the Assurer Challenge, especially in the area of Arbitration
- Support Event Organisation in improving and extending the present materials for ATEs (see SVN)
- Improve the CATS admin interface so editing questions and answers is a bit more comfortable.
- Improve the CATS database structure and admin interface to give better support for handling questionnaires in different languages

Bernhard Fröhlich

Events Team

In 2012/2013 we had 26 Events listed in total.

- 21 announced Assurance Events where 19 did happen. Only one out of 19 Events Reports received.
 - 5 ATE's have been announced. 2 out of 5 Events Reports received.
 - 7 scripted mailings (including 5 ATE invitations) for 3 countries (DE, US, AU) have been executed by the Critical team under Arbitration [a20090525.1](#) to support the 26 events. 6276 recipients have been notified of events in their near by the 7 mailings (ranging from 8 to 3467 recipients in a script)
-

ATE Team

The ATE team consists of a mixture from several other teams. Education team, Audit team, Co-Audit team, Assurance team. The Assurer Training Events are an event form, to bring Assurers together, to get them trained and co-audited.

With a decrease in Audit activities (by several reasons) also the ATE activities decreased to ATE's by request.

Finally we did run 5 ATE's. 3 in Germany, 1 in the United States and 1 in Australia.

ATE presentations are still based on the German "Bonn" presentation and English the "Manchester" presentations. Both can be found in the SVN under Education - Material

- ATE-Duesseldorf, DE: 21 attendees
- ATE-Melbourne, AU: 4 attendees
- ATE-Raleigh, US: 7 attendees
- ATE-Kiel, DE: 12 attendees
- ATE-Luebeck, DE: 12 attendees

Co-Audit results

The server that was used in the past to enter co-audit results has been shut down. A backup is currently held by Iang. With the new infrastructure machine, the hope is, to get a machine with some webspace for the internal audit and also for the co-audited assurance program.

Assurance

The Assurance area covers several related areas: Events, ATE's, [Organisation Assurance](#), TTP-assisted-assurance-Program, but also Audit, Policies. Some have their own reports, some are incorporated under this combined Assurance report.

In general: Assurance area is in good working order. Some sub areas may run better.

POJAM - the Policy on Junior Assurers/Members has been voted to status POLICY after 4 years of experience in practice with this policy (first voted to DRAFT in February 2010)

The TTP-assisted-assurance Policy was long time blocked by the lack of support in Software Updates. The first patches have been installed to production earlier this year, so the requirements given by the policy now could be processed in practice. A downer remains: the TOPUP program of the TTP-assisted-assurance Policy cannot be set active, until further Software updates will be implemented into the production system. The new TTP-assisted assurance Subpolicy program under Assurance Policy officially started in May 2013.

An update or review of Organisation-Assurance Policy is still in the work queue to be prepared by the Organisation-Assurance team.

An update of the CCA is still in the work queue of Policy Group.

The Individual Assurance Program

Short: **The Assurance Program** receives reports from the Events organizers and ATE teams. The lack of event reports reaches a new high score in the negative - only 1 of 19 Assurance Events organizers and only 2 of 5 ATE Event organizers delivered event reports, that gives some feedback about current status of the assurance program.

The CAcert statistics counts approx 400 new assurers in the period 2012/2013 (520 in 2011).

TTP-assisted-assurance Program

The *old* TTP program has been stopped back in 2009 in the Assurance Policy rollout that results in a termination of a couple of *old* Special Assurance Programs. One of these programs was the TTP program.

A new starter for a TTP-assisted-assurance Policy has been made at [Assurance MiniTOP Hamburg, Dec 2009](#).

The policy did pass Policy Group in 2010-09-13 [p20100913 TTP Assisted Assurance Subpolicy to DRAFT](#)

TTP-assisted-assurance Program deployment

Current state of the overall TTP-assisted-assurance program is, that part I, two TTP-assurances can be entered into the online system. Part II of the program, the TOPUP program can not.

Activation of the TTP-assisted-assurance program was most time blocked by Software developments to implement the new TTP assisted assurance program into the running software. From current state of writing, the TTP-assurance can be entered into the

system. TOPUP's can not, so the TOPUP program currently is still blocked until a patch has been applied into the system. Reasons why it is blocked can be summarized with: Old TTP program software code did allow easy implementation by recycling code for part I of the new TTP-assisted-assurance program, but there is still no code written, to implement part II, the TOPUP program into software.

The TTP-assisted-assurance deployment team decided, to go an intermediate step with the first step way, so that members can receive at least 50 assurance points and others, who have been assured in one Face-2-Face meeting by a CAcert assurer, can reach the 100 Assurance points barrier with 2 TTP-assisted-assurances. This doesn't help much, to seed the CAcert desert, but

- a. we receive experience with the TTP-assisted-assurances
- b. members with other assurance points collected can probably reach the 100 AP barrier by other ways

At Software-Assessment [patch day 2013-01-17](#) and [patch day 2013-04-24](#) two patches have been moved to production, that allows entering TTP assisted assurances into the system under the new TTP-assisted-assurance Subpolicy program.

Before that, a system cleanup (removing old TTP-admins/assurers) under the permissions stocktaking script project (initiated by board [m20120122.1](#) and [m20120122.2](#), conducted by [arbitration](#)) did happen.

New TTP-assurers have still been nominated and approved under board motion [m20120325.2](#) (2012-03-18) by board of 2011-2012.

Since the software blocking to enter TTP-assisted-assurances into the production system has been solved, the return of the TTP-assisted-assurance program has been official announced <http://blog.cacert.org/2013/05/cacert-is-proud-to-announce-that-the-trusted-third-party-programme-is-back-to-life/> at May 14, 2013

The first real TTP assisted assurances has been entered into the production system, so we can see, that the TTP-assisted-assurance procedure as deployed works as expected.

Documentation for TTP Users, TTP's, TTP assurers have been finished under the Wiki [TTP](#) tree.

Now the TTP deployment team still works on the TOPUP part of the TTP-assisted-assurance program.

TTP-assisted-assurances TOPUP program

An initial starter has been made by nomination and acceptance by CAcert Board for the seeding TOPUP assurers by board motion [m20130616.2](#).

A proposal workplan for giving TOPUP assurances is documented under the [wiki TTP/TTPtopup](#) page, but as long the required software patches haven't been implemented to production, the work with TOPUP candidates still makes not much sense, going through the procedure with the potential candidates now, but cannot enter a successful passed TOPUP into the production system (despite the fact we did received a couple of TOPUP requests by TTPusers). So this process stalls currently.

TTP-assurers seeding

The [TTP-assisted-assurance Subpolicy](#) doesn't define in full, how we bring in new TTP assurers except two requirements given:

- a. the Assurer must be a Senior Assurer ([Senior Assurer](#) definition in AH)
- b. The Assurer must be familiar with the local language and customs (to be checked individually)

This task has been picked up by the TTP deployment team and we now have two proposals to bring in new TTP assurers into the TTPadmin team:

- a. new TTP assurers gets nominated by the TTPadmin team, presented before CAcert Board and CAcert Board accepts nominations -or-
- b. new TTP assurers gets nominated by the TTPadmin team. CAcert Board delegates acceptance of new TTP assurers to the AO and OAO

TTP-assisted-assurances statistics

[from period 2013-05-14 until 2013-08-22]

	TTP-assisted-assurance program back online	2013-05-14
1.	TTP-assisted-assurances finished (total)	5
	- TTP-assurance US	4
	- TTP-assurance PR	1
2.	TTP-assisted-assurances WIP	17
	Total requests: 1 + 2	22
3.	TTP-assurances awaiting TOPUP (also under 1.)	4

TTP assurance requests by country

US	20
AU	1
PR	1
Total	22

Approved TTP's by Countries

Currently we have [approved TTP's](#) from 3 countries

Organisation Assurance Team

New Root & Escrow Project (NRE)

Building Team

In relation of discuss about New Roots in several board meetings the NRE Team was built in mid Jun 2013. The NRE team have an initial meeting with a board member to discuss about next steps

- The team started with 3 members
- A first proposal was written "New Root Certificates for CAcert proposal".
- The NRE team finished this document and sent to board.
- Board appoint the New Roots & Escrow project leader motion m20130729.2
- Project Charter signed by CAcert's President
- WBS & Time Planning created, project ready to start

Outlook

- Team meetings weekly to track communicate the current status of the project, monthly reporting to board planned.
- The team currently consist of 4 members
- Build New Roots

Martin Gummi - NRE Project Manager

BirdShack

Ada Lovelace, a Computer Science student from UNC-Chapell Hill, did an internship on the [BirdShack](#) project over the (northern) summer period, being May 2012 to August 2012, inclusive.

Ada worked with Iang on the middleware server. We implemented a first cut of a REST-based middleware server in Java. This involved creation of objects to match all the Birdshack resources, objects to implement the REST pattern (create, read, update, delete), testing them for network sending and recoverability (a process we called the Ouroboros pattern), and construction of an object database that could store and recover the REST resources. Piers was press-ganged into final review of Ada's code.

During the process we discovered several issues.

1. REST has no security architecture. As we were using techniques and network framework from an existing project called SOX, we inherited its security model. It remains to be seen if there are better options, but SOX is far better than nothing, and probably better than password / usernames over TLS. The choice of security model has many implications. For website language, Java is easier; the ability of other languages to contribute a website is somewhat reduced because of the lack of bindings, and if another model were used, we would need to align that with both languages.
2. REST has no state, so state-rich transactions are difficult. For example, it is impossible in pure REST to create two objects that link to each other at the same time, as an atomic transaction (which is more or less a requirement of the original [BirdShack](#) design). To address this, we created two variations:
 - a. promiscuous resources that could be created in advance, linked into other objects, and then changed to be a different final object.
 - b. expiries on objects, such that if a failure to finalise a transaction occurs, the initial object will be cleaned up automatically by the backend database.

The combination of these two extensions allows transactions to be implemented with REST commands.

1. It is not entirely clear that the REST model buys us much. From the perspective of security and state, once a proper model is implemented, it is also clear that implementing specialist access requests to do the specific [BirdShack](#) requirements is not that much more work, and gives great benefits in code solidity, reliability and especially security.

The next step in the [BirdShack](#) project would be to create a website that drives the REST-based interface according to user demands. This would be best in Java as the object bindings are already done, and we have the secure communications architecture in place.

The challenge would be to get enough of a website up and working to allow the whole site to be seen, and then features could be added incrementally by different programmers.

[CategoryCAcertInc](#)

[CategoryCommunity](#)

[To AGM](#) - [To AGM/Next](#) - [To AGM TeamReports Overview](#) - [To AGM Members Reports Overview](#)

[To AGM Team Report 2013](#)

CAcert Members Report 2013

Below is the report of the CAcert association members to itself. Please write about how you have contributed to CAcert over the year 2012-2013.

(Editors note - please place in alphabetical order)

<your name>

CategoryCAcertInc
CategoryCommunity

CategoryCAcertInc
CategoryCommunity

AGM/AGM20131117/CAcert_Annual_Report_2013 (last edited 2013-11-14 23:46:27 by [UlrichSchroeter](#))