
CAcert

*Überblick, Einblick, Ausblick
oder
Was war, was ist, was sein wird*

Henrik Heigl

initial Organisations Assurer & Public Relations Officer CAcert.org

Henrik@cacert.org

Übersicht

- CACert gegründet
- Was ist eine Certificate Authority? Was ist CACert?
- Wie wird hier die Identität verifiziert und warum?
- Wie nutze ich CACert (Beispiel E-Mail)?
- Was kann man noch machen?
- Was passiert gerade bei der Umstrukturierung und dem Audit?

Die Assurance

- Assurance ist die Dienstleistung, bei der ein Assurer die Identität einer Person mittels amtlichen Lichtbildausweis kontrolliert
- gegenüber CAcert bestätigt, und dafür Punkte auf das Konto bei CAcert vergeben werden
- Lebenslanger *Account* bei CAcert, *Zertifikate* müssen spätestens alle 2 Jahre erneuert werden
- Zertifikate jederzeit selbst im Internet ausstellbar
- Zertifikate sind kostenlos
- beliebige Menge von Zertifikaten
- dadurch nur Initialkosten, keine Folgekosten

Die Anfänge

CAcert Inc. ist ein eingetragener Non-Profit Verein mit Sitz in Australien, der die Regeln definiert, und die zentralen Server betreibt

Start www.CAcert.org: 2002

Gründung CAcert Inc.: 2003

2008: Umzug der Server in ein
RZ in den Niederlanden



CA Überblick



- Cacert (fortgeschrittene Zertifikate): Communitybasierend, kostenlos, SSL und Codesigning Zertifikate
- Z.B. Verisign, etc. (fortgeschrittene Zertifikate):
 - eMail-Zertifikat: 19,95\$ pro Jahr; Code Signing Zertifikat: 499,00\$ pro Jahr; SSL Zertifikat: 899,00\$ pro Jahr (incl. Versicherung)
- Z.B. D-Trust (Qualifizierte Zertifikate): eMail Signaturkarte (2048b): 139,00€ im ersten Jahr - 129,00€\$ pro Folgejahr
 - Klasse-3 Kartenlesegerät mit PIN-Eingabe: 99,00€ pro Gerät
 - Lotus Notes Plugin: 19,00€



CAcert

- Inhalt
 - Vertrauen (Trust)
 - X.509 digital certificates
 - CAcert community
 - CAcert services
 - das HowTo
 - Wieso sollte ich?
 - Ich auch!
 - Es ist FREI (unter GPL Lizenz)!



Ablauf

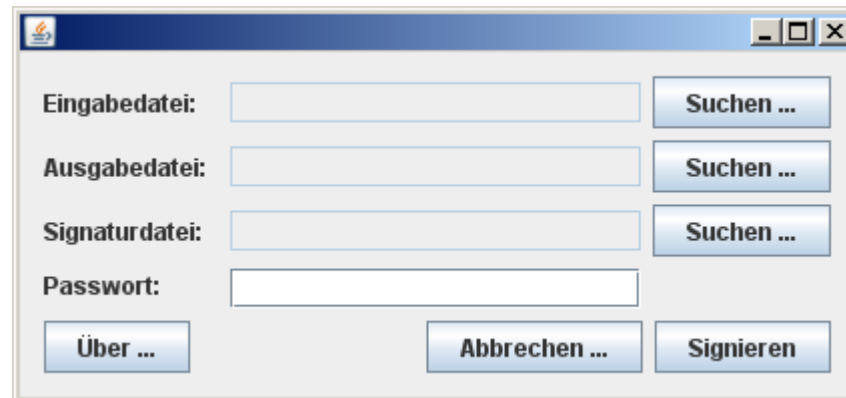
- Account anlegen unter CAcert.org
 - Zu diesem Zeitpunkt können schon (nichtbeglaubigte) Zertifikate ausgestellt und verwendet werden.
- Beglaubigungen (Assurances) einholen
 - Assurer suchen
 - Formular ausfüllen, CCA lesen
 - Ausweis dem Assurer zeigen
 - Formular unterschreiben und dem Assurer geben
- Beglaubigte Zertifikate ausstellen
 - E-Mail Zertifikat
 - SSL Zertifikat
 - Codesigning

Punkteschema

Punkte	Status	Punktevergabe (maximal)
0 – 49	unassured	–
50 – 99	assured	–
100 – 109	assurer	10
110 – 119	assurer	15
120 – 129	assurer	20
130 – 139	assurer	25
140 – 149	assurer	30
150	fully assured	35
200	super assurer	150

Portablesigner

PDF Signiertool (in Java, von Peter Pfläging - pfp@adv.magwien.gv.at)



Freeauth.org



Two-Factor Authentication
Safe, secure and easy to use. Free White Paper download.

Web-based Project Mgmt
Manage your project on the web. Easy to use, deploy & afford.

Ads by Google

[Login](#) | [Settings](#) | [Help/Guide](#) | [About Trac](#) | [My Notifications](#) | [Register](#)

[Wiki](#) | [Timeline](#) | [Roadmap](#) | [Browse Source](#) | [View Tickets](#) | [New Ticket](#) | [Search](#)

[Start Page](#) | [Index by Title](#) | [Index by Date](#) | [Last Change](#)

What is the Free Auth Project?

The Free Auth Project was born out of the need for cheap/free One Time Password authentication in any business or organisation where you need to manage keys between users. There is currently numerous systems for doing One Time Passwords in the enterprise but these are often very awkward, user unfriendly or expensive (or all the above).

All the pieces currently exist to build such systems, but there is currently no cohesive documentation on how to do it, you have to work it out for yourself as you go along, so the majority of this project is dedicated to documenting different software options and how it all fits together, and building or enhancing any software that doesn't exist such as management interfaces to make enterprise deployment easier.

Contact Us

Due to the nature of this project the best way to contact us is via [⇒ our mailing list](#)

Want to help us?

The biggest help people can be is in:

- ★ Spreading the word about the site/project
- ★ Helping with issues, feature requests and suggestions for improvements on [⇒ our mailing list](#)
- ★ Writing documentation and software
- ★ Testing software as much as possible for usability and bugs

Freeauth in action



Einmalpasswort Anmeldung - OTP

- Unter <http://www.freeauth.org/site/wiki/FreeAuth%20> die Anleitung zur Passwortgenerierung durchgehen
- Zeitzone UTC +3 (Europa)
- HASH unter cacert.org eintragen
- Einmalpasswort am Handy generieren und bei der Anmeldung im Passwortfeld eintragen

CAcert Freeauth

Meine Details	
Vorname:	Henrik
Mittlere Namen (wahlweise)	
Familienname:	Heigl
Suffix (wahlweise)	
Geburtsdatum (tt/mm/jjjj)	12 Juni 1972
OTP Hash (Not displayed)	<input type="text"/>
OTP PIN (Not displayed)	<input type="text"/>
Ich-habe-mein-Passwort-vergessen-Fragen	
1) <input type="text"/>	<input type="text"/>
2) <input type="text"/>	<input type="text"/>
3) <input type="text"/>	<input type="text"/>
4) <input type="text"/>	<input type="text"/>
5) <input type="text"/>	<input type="text"/>
<input type="button" value="Aktualisieren"/>	

Audit

- Ziel: Cacert Root Zertifikat im Browser
- Management
- Policies + Verfahrensanweisungen
- Audit der Geschäftsabläufe & Systeme
- gegenüber diesen Richtlinien und Verfahren
- Durchführung nach dem „David Ross Criteria (DRC) welches von Mozilla anerkannt wird

Audit DRC

- Die DRC haben eine solide Eigenschaft:
- sie verlangen, daß
 - alle Risiken,
 - jegliche Haftung und
 - alle Verpflichtungen
- klar gegenüber jedermann dargelegt werden!

Audit /2

- Unterteilung: Assurances und Systeme
- Assurance -> Assurer Policy
=> done

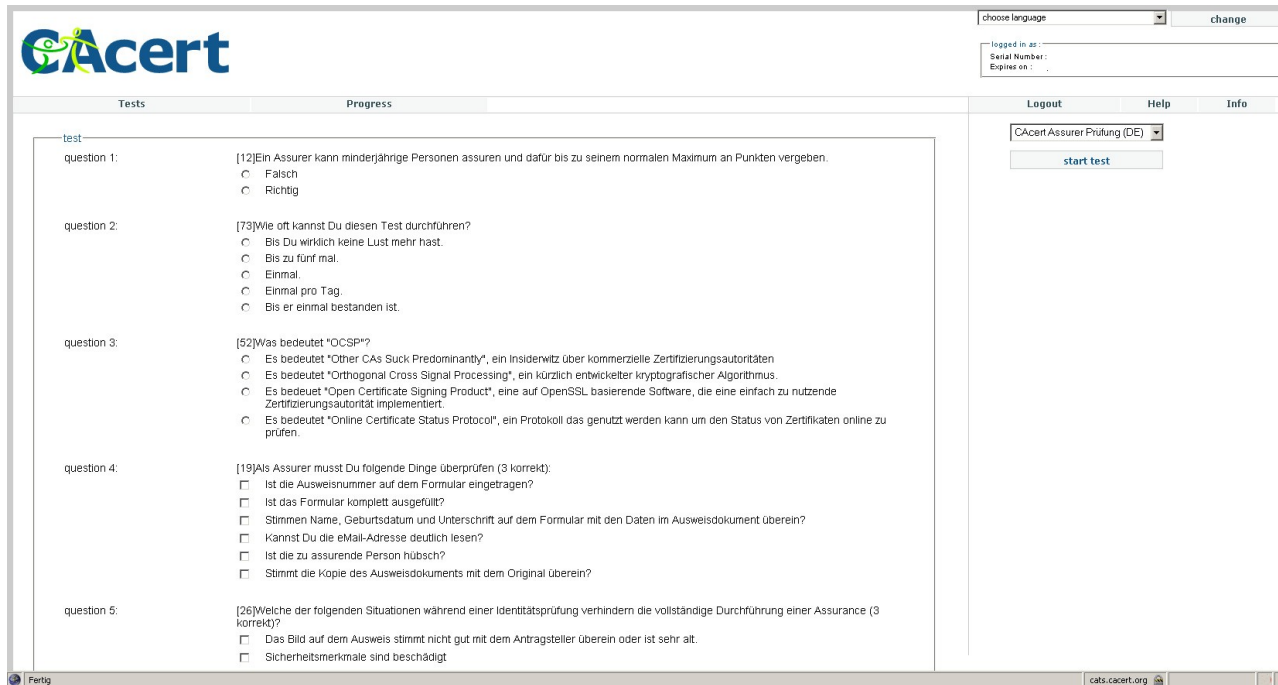
- Systeme: Umzug der Systeme aus Wien nach Ede zu BIT, Niederlande (Oktober 2008)
- Systemadministratoren Team gebildet
=> in Arbeit

Audit /3

- Zertifizierungs Verfahrensweisung
(Certification Practise Statement; CPS)
=> in Arbeit

- Software: Schwierigkeiten bei Wartung
und Sicherung
=> Neues Systemdesign; in Arbeit

CATS



The screenshot shows the CATS interface with the following content:

- Header:** CAcert logo, language dropdown (set to 'change'), and user information (logged in as, Serial Number, Expires on).
- Navigation:** 'Tests' and 'Progress' tabs, and 'Logout', 'Help', 'Info' links.
- Test Questions:**
 - question 1:** [12] Ein Assurer kann minderjährige Personen assuren und dafür bis zu seinem normalen Maximum an Punkten vergeben.
 - Falsch
 - Richtig
 - question 2:** [73] Wie oft kannst Du diesen Test durchführen?
 - Bis Du wirklich keine Lust mehr hast.
 - Bis zu fünf mal.
 - Einmal
 - Einmal pro Tag.
 - Bis er einmal bestanden ist.
 - question 3:** [52] Was bedeutet "OCSP"?
 - Es bedeutet "Other CAs Suck Predominantly", ein Insiderwitz über kommerzielle Zertifizierungsautoritäten
 - Es bedeutet "Orthogonal Cross Signal Processing", ein kürzlich entwickelter kryptografischer Algorithmus.
 - Es bedeutet "Open Certificate Signing Product", eine auf OpenSSL basierende Software, die eine einfach zu nutzende Zertifizierungsautorität implementiert.
 - Es bedeutet "Online Certificate Status Protocol", ein Protokoll das genutzt werden kann um den Status von Zertifikaten online zu prüfen.
 - question 4:** [19] Als Assurer musst Du folgende Dinge überprüfen (3 korrekt):
 - Ist die Ausweisnummer auf dem Formular eingetragen?
 - Ist das Formular komplett ausgefüllt?
 - Stimmen Name, Geburtsdatum und Unterschrift auf dem Formular mit den Daten im Ausweisdokument überein?
 - Kannst Du die eMail-Adresse deutlich lesen?
 - Ist die zu assurende Person hübsch?
 - Stimmt die Kopie des Ausweisdokuments mit dem Original überein?
 - question 5:** [26] Welche der folgenden Situationen während einer Identitätsprüfung verhindern die vollständige Durchführung einer Assurance (3 korrekt)?
 - Das Bild auf dem Ausweis stimmt nicht gut mit dem Antragsteller überein oder ist sehr alt.
 - Sicherheitsmerkmale sind beschädigt
- Footer:** 'Fertig' button and 'cats.cacert.org' URL.

Siehe: <https://cats.cacert.org>

Zertifikat



Hashserver

HashServer

This is a public service to detect compromised, weak SSL/X.509 keys.

-> HashServer for Users

You can check your certificate to see whether it is compromised.

-> HashServer for Certificate Authorities

Certificate Authorities can integrate HashServer into their workflow to avoid issuing certificates for already known to be compromised keys, and to

More information about this service: <http://wiki.cacert.org/wiki/HashServer>

This Hashserver is operated by CAcert.org

Redesign

- Neudesign des Logos im Zuge der Wahl des neuen Boards von CACert.Inc
- Einführung des CAcert-Styleguides

The CAcert logo with a stylized figure in green and yellow.The CAcert logo with a stylized figure in white.The CAcert logo with a stylized figure in green and yellow.The CAcert logo with a stylized figure in white.

cr-day

- Umzug der Server in ein Hochsicherheits Rechenzentrum in den Niederlanden, Oktober 2008
- Vom Audit beaufsichtigte Überführung der Serverplatten von der Schweiz nach den Niederlanden



Attention: The Servers of CAcert are moving to another Place. Therefore the Website and Services related to CAcert Certificates is temporarily offline, please try later.
 In the meantime you can look at our Blog or inform at our wiki about CAcert.

Progress status:

The sealed disks are opened and installed in the servers	Progress
The servers are booted and the data integrity is checked.	Progress (2008/10/01)
Root key is installed (or a new one is created if time permits us)	Progress (2008/10/01)
Operational Overview	Progress (2008/10/01)
Last checks	Progress (2008/10/01)
Website and Services Back on-line	Offline
Check with small group of "beta testers" around the world	Progress (2008/10/01)
Announcement to community and press release	Progress

For more information during the Movement you can also contact henrik@cacert.org

Do you want to help CAcert?
 We are facing an uphill battle to fund this service and could do with your help!
 If you can, please donate
 AU\$50 per year by this button



Policy

- Assurance Policy: hat vollen Policy Status und ist VERBINDLICH für alle Assurer

wichtiges

Assurance Policy (AP)

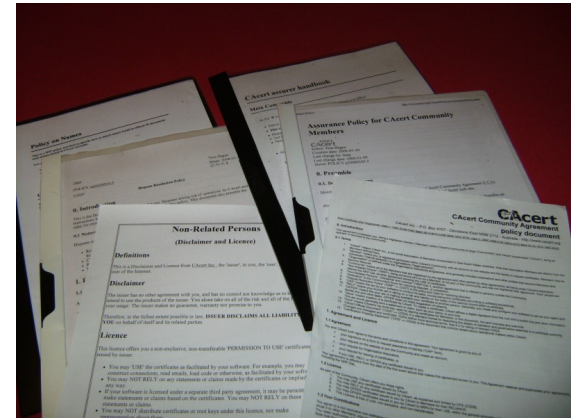
<http://www.cacert.org/policy/AssurancePolicy.php>

CAcert Community Agreement (CCA)

<http://www.cacert.org/policy/CacertCommunityAgreement.php>

Assurance Handbook (AH)

<http://wiki.cacert.org/wiki/AssuranceHandbook2>



Non-Related Persons (Disclaimer and Licence)(NRP-DaL)

Unabhängige Personen – Haftungssauschluß und Lizenz

<http://www.cacert.org/policy/NRPDisclaimerAndLicence.php>

ATE – Assurer Training Event

- Dient der Heranführung und Schulung neuer Assurer
- Qualitätssicherung
- Aufbessern des Wissens
 - Hamburg, Donnerstag 7. Mai
 - [<http://wiki.cacert.org/wiki/Events/20090507ATE-Hamburg>]
 - Düsseldorf, Dienstag 12. Mai
 - [<http://wiki.cacert.org/wiki/Events/20090514ATE-Duesseldorf>]
 - München, Samstag 16. Mai
 - [http://wiki.cacert.org/wiki/Events/20090509muc_AssurerTraining]
 - Stuttgart, Dienstag 26. Mai
 - [<http://wiki.cacert.org/wiki/Events/20090526ATE-Stuttgart>]

Weitere Infos

- Weitere Infos unter
 - <http://www.cacert.org>
 - <http://wiki.cacert.org>
 - <http://wiki.cacert.org/wiki/ClientCerts>
 - <http://blog.cacert.org>
 - <http://www.ivamp.de/cert>
- CACert im irc
 - Server: [irc.cacert.org](irc://irc.cacert.org)
 - Chanel: [#cacert](#) oder [#cacert.ger](#)

Fazit

- Es geschieht viel
- Es muss noch viel getan werden
- Vorrangig Audit abschliessen, Root zertifikat in Mozilla integrieren, Root Zertifikat in allen anderen Browsern integrieren (Mainstream)
- Personen und Geld wird benötigt

Anmerkungen

- Der Fingerprint des Root Zertifikates hier in der Präsentation rechts unten ist NOCH gültig. Wenn der neue Root Key installiert ist sollte man diesen neu verifizieren.
- Wer die Präsentation im Gesamten oder in Teilen verwenden möchte darf und soll dies gerne tun, aber mich bitte kurz darüber informieren. Danke.

Danke und Fragen

- Henrik Heigl – CAcert @ gmx . net

