



**CAcert**

**Assurer**

**Handbuch**

### *Anforderungen:*

- In jedem CAcert Büro sollten mindestens 2 CAcert-Assurer zu den normalen Öffnungszeiten anwesend sein
- Die Assurer sollten bereits Übung haben, also am besten die eigene Familie und Arbeitskollegen assuren, um Übung mit den Ausweisen und Formularen zu bekommen.
- Die Adresse des Büros und die Öffnungszeiten sollten bei CAcert.at und bei CAcert.org bekanntgegeben werden. Bei einer Übersiedlung sollten auch beide benachrichtigt werden.

Für die Auflistung des Büros brauchen wir folgende Daten:

- Öffnungszeiten (bei denen Assurer da sind)
- Genaue Adresse
- Telefonnummer/Handynummer
- E-Mail Adresse
- Anfahrtsbeschreibung

## Assurance Vorgang:

### Vorbereitungen:

- Man sollte immer ein paar ausgedruckte Formulare zur Hand haben, hier der direkte Link:  
[http://www.cacert.org/cap.php&lang=de\\_DE](http://www.cacert.org/cap.php&lang=de_DE)  
Tip: Das Formular sollte als Drucker-Testseite verwendet werden
- Man sollte Kugelschreiber auf Lager haben, damit die Formulare ausgefüllt werden können

### Assurance:

- Zuerst soll der Kunde das Formular 2 mal ausfüllen (für jeden Assurer eines).
- Wenn der Kunde bereits mit einem selbst ausgedruckten, und korrekt ausgefüllten Formular kommt, kann dies akzeptiert werden. (Bitte aber aufpassen, daß das Formular richtig ist)
- Der Kunde muß den oberen Teil ausfüllen, Datum und Unterschrift nicht vergessen.
- Dann muß der Kunde die Ausweise herzeigen, die von beiden Assurern kontrolliert werden müssen:

- Mindestens 1 amtlicher Lichtbildausweis, möglichst mehrere:
  - Reisepass, Führerschein, Personalausweis
  - Studentenausweis gilt nicht als amtlicher Ausweis
- Zusätzlich können auch E-Card, Bank-Karten, Kreditkarten, Mitgliedskarten, ... als Indizien verwendet werden.

## **Kontrolliert werden müssen auf den Ausweisen:**

- Lichtbild
  - Weil Führerscheine nie ablaufen muß man hier mit sehr alten Bildern und Unterschriften rechnen
- Unterschrift:
  - Wenn die Unterschrift nicht mehr wieder zu erkennen ist, die Person auffordern, unten auf dem Formular noch eine Unterschriftenprobe zu machen, die mit den Unterschriften in den Ausweisen übereinstimmen sollte
  - Wenn auf einer Karte eine Unterschrift vorgesehen ist, aber keine Unterschrift drauf ist, sollte man den Kunden bitten, die Karte zu unterschreiben.
- Sicherheitsmerkmale
  - Stempel, die das Foto und den Ausweis darunter abgestempelt haben

- Hologramme
- Drucktechniken
- Stempelmarken
- Übereinstimmung der Daten mit der maschinenlesbaren Zone
- Ablaufdatum
  - Führerschein: hat normalerweise keines
  - Reisepass: hat ein Ablaufdatum
  - Bankkarten: Meistens nur eine Jahreszahl: z.B.: 05
  - Abgelaufene Ausweise sind als Indizien zulässig, ein Punkteabzug ist möglich
  - Man sollte die Kunden auf das baldige Ablauf der Ausweise hinweisen
  - Ergeben das Ablaufdatum mit dem Ausstellungsdatum eine sinnvolle Lebensdauer? (z.B.: 10 Jahre)
- Geburtsdatum
  - Bei CAcert (Australien) wird das Datum oft als Jahr-Monat-Tag (2005-06-12) im Gegensatz zum hier üblichen Tag.Monat.Jahr (12.6.2005) angegeben. (ISO-8601 Format)
  - Ist das Geburtsdatum plausibel?
  - Auch Kinder und Jugendliche können assured werden, CAcert hat kein Mindestalter
- Testfragen

- Geburtsort
- Künstlername (bei deutschen Personalausweisen)

**Wichtig: Man sollte sich zur Kontrolle der Ausweise mindestens 1 Minute Zeit nehmen!**

## **Kontrolliert werden muß beim Formular:**

- Wurde alles vom Kunden ausgefüllt? (Datum und Unterschrift werden oft vergessen)
- Stimmt das Geburtsdatum, der Name, die Unterschrift mit den Ausweisen überein?
- **Wichtig: Ist die E-Mail Adresse gut lesbar?**  
Sie müssen diese Adresse später korrekt auf [CAcert.org](http://CAcert.org) eingeben können. Im Zweifelsfall nachfragen, und die Adresse zusätzlich in Blockbuchstaben auf das Formular schreiben.

## **Formular ausfüllen**

- Name, Unterschrift, aktuelles Datum
- Bei den beiden Ausweisfeldern die Art der gesehenen Ausweise („Reisepass“, „Führerschein“), nicht jedoch die Ausweisnummern notieren. (Bei manchen anderen

CAs ist es üblich, daß die Ausweisnummern notiert werden müssen, bei CAcert ist es nicht erlaubt, weil der Mißbrauch von Identitäten in Amerika leider zu stark verbreitet ist.)

- Punkte: Hier sollte man nach eigenem Ermessen die Punkte vergeben:
  - Kenne ich die Identität der Person bereits?
  - Haben die Ausweise glaubwürdig die Identität bestätigt?
  - Wenn es Zweifel gibt, dann entsprechend weniger Punkte vergeben

Wie funktioniert das Punkte-Schema?

- **0-49 Punkte** – Die Person ist nicht-assured, und der Name ist nicht in den Zertifikaten enthalten. Man kann Client Zertifikate (E-Mail Signatur und Verschlüsselung) und Server Zertifikate (für SSL in den Webservern) bekommen, die maximal 6 Monate gültig sind.

Sobald man mehr als 0 Punkte hat kann man die persönlichen Details (Name, Geburtsdatum, ...) nicht mehr selbst ändern.

- **50 Punkte** – „Assured“ Der Name kann in den Zertifikaten enthalten sein. Ein [ServerZertifikat](#) ist 2 Jahre gültig. Man kann den PGP/GPG Key von CAcert signieren lassen.
- **100 Punkte** – „Assurer“ Dies ist das Maximum der Punkte, die man von anderen Assurern bekommen kann. Mit 100 Punkten ist man Assurer, und kann die

Identität von anderen Personen für CAcert kontrollieren, und seinen Namen im Assurer Verzeichnis auf [www.CAcert.org](http://www.CAcert.org) auflisten lassen. Man kann Code-Signatur beantragen.

- **150 Punkte** – „Vollständig assured“. Das Maximum der Punkte, die man durch das TTP Programm oder durch das Assurieren anderer erreichen kann. Man kann nun bis zu 35 Punkte an andere vergeben.
- **200 Punkte** - „Super Assurer“. Wird verwendet, um bei größeren Events Massen-Assurance zu machen. Um diesen zeitlich beschränkten Status zu erhalten, muss man bereits 150 Punkte haben, und braucht die Zustimmung von 2 Board Mitgliedern.

Dadurch ist ein durchgängiges 4-Augen-Prinzip gewährleistet: Damit man sich selbst Zertifikate ausstellen kann, muß man von mindestens 2 Assurern bestätigt worden sein.

Um Assurer zu werden, muß man von mindestens 3 anderen Assurern bestätigt werden und kann dann eine Zeit lang üben.

## Preis

- Zertifikate sind kostenlos (die stellen sich die Kunden dann selber aus)

Wieviel kostet die Assurance?

- CAcert hat die Regelung, daß der Assurer vor dem

Treffen bekannt geben muß, wieviel die Assurance kosten wird, ansonsten muß die Assurance gratis durchgeführt werden.

- Eine normale Doppel-Assurance in einem Büro (durch 2 Assurer bestätigt) kostet 25,- EUR
- Sollte nur ein Assurer vorhanden sein, und dadurch nicht genügend Punkte vergeben werden können, dann entsprechend die Hälfte, also 12,50 EUR
- Assurance „vor Ort beim Kunden“ kostet 50,- pro Person (da gehen wir davon aus, daß das 2 Assurer machen)
- Bei Studenten, Stammkunden, ... kann man den Preis nach eigenem Ermessen ermäßigen
- VIP Assurance sollte wenn möglich kostenlos gemacht werden. (VIP Assurance ist für wichtige Personen gedacht, bei denen es für CAcert wichtig ist, daß diese assured werden. Im Falle einer VIP Assurance wird man vorher von CAcert informiert, daß jemand kommen wird, und sollte es der Person dann möglichst einfach und angenehm machen. Wichtig ist, daß auch VIPs intensiv kontrolliert werden, schlampige Kontrollen von VIPs könnten fatale Folgen haben!)

## Bei Problemen

- Sollte eine Person mit gefälschten, stark widersprüchlichen Ausweisen, auftauchen, oder sich stark verdächtig benehmen, möglichst alle Fakten über diese Person sammeln
  - Formular möglichst ausfüllen lassen
  - mit den Ausweisen kontrollieren
  - das ausgefüllte Formular auf jeden Fall einbehalten
  - die Daten möglichst sofort an die CAcert Zentrale weiterleiten
  - möglichst genauen Beschreibung der Geschehnisse.

## Punkte übertragen

Die Punkte können je nach Andrang entweder direkt bei der Assurance übertragen werden, oder am Abend nach Geschäftsschluß.

- Nicht auf einem Computer der gerade unter Viren, Würmern, ... leidet! (Im Zweifelsfall von Knoppix booten)
- Einen neuen Browser (Internet Explorer, Konqueror, Firefox, Safari, ...) starten, und oben in der Adreßleiste <https://www.cacert.org/> eingeben.
- Rechts im Menü auf „Normal Login“

- E-Mail Adresse und Passwort eingeben
- Rechts unten auf „CAcert Web of Trust“
- Darunter auf [„Jemanden assuren“](#)
- Die E-Mail Adresse des Kunden eingeben
- Das Formular ausfüllen.
- Das Datum braucht nur angegeben werden, wenn das Treffen nicht am selben Tag war
- **Nach der Abmeldung von der CAcert Webseite bitte den Browser aus Sicherheitsgründen schließen!**

## Arbeit nach dem Treffen:

- Bei Leuten, die sich den Account noch nicht angelegt haben, muß der Assurer die nächsten Tage immer wieder schauen, ob der Account bereits angelegt wurde, und dann entsprechend die Punkte nachtragen
- Wenn ein Account erledigt wurde, sollte man das Formular „abhaken“
- Nicht vergessen: Die Formulare müssen dann 7 Jahre lang sicher aufbewahrt werden, der Assurer ist persönlich dafür verantwortlich.
- Sollte es Zweifel oder Probleme bei einer Assurance geben, wird sich die CAcert Zentrale melden, dann muß das Assurance Formular an CAcert gefaxt / geschickt werden.

## Zertifikate ausstellen

Genauere bebilderte Anleitungen, wie man Zertifikate mit den jeweiligen Browsern und E-Mail Clients ausstellt, sind unter <http://www.cacert.at/>. Hier folgt eine verallgemeinerte Anleitung:

Um ein Zertifikat für ihre E-Mail Adresse zu bekommen, gehen Sie wie folgt vor:

- Login auf <http://www.cacert.org/>

- E-Mail Adressen → Neu

- E-Mail Adresse eingeben, → Weiter

Nun bekommen Sie eine E-Mail an die angegebene Adresse, in der ein Link ist, auf den Sie draufdrücken müssen, damit Sie sich als Eigentümer ausweisen.

- E-Mail lesen, auf Link klicken

- E-Mail Adressen → Anzeigen

- Hier bitte kontrollieren, ob die E-Mail Adresse „verifiziert“ ist

- Rechts im Menü auf „Client Zertifikate“ → Neu

- Die E-Mail Adresse aussuchen.

- Mit der Auswahl des „Crypto-Service-Provider“ können Sie sich aussuchen, ob Sie den Schlüssel in

einer SmartCard, oder normal auf ihrem Computer erzeugen wollen.

- Suchen Sie sich aus, ob Sie Ihren Namen im Zertifikat haben wollen, oder ein anonymes Zertifikat haben wollen.
- Weiter → Zertifikat importieren
- Damit ist das Zertifikat nun ausgestellt.
- Je nach E-Mail Programm und Internet Browser können Sie das Zertifikat nun automatisch im Browser verwenden, oder müssen das Zertifikat vom Internet Browser exportieren, und in das E-Mail Programm importieren.
- Zum Exportieren gehen Sie in die Einstellungen vom Browser
- → Sicherheitseinstellungen
- → Zertifikatsmanager
- Selektieren Sie das Zertifikat, und exportieren Sie es in eine PKCS#12 (.p12 .pkcs) Datei.
- Diese PKCS#12 Datei können Sie nun in den Einstellungen des E-Mail Programmes importieren.

Im E-Mail Programm müssen 2 Einstellungen gemacht werden:

- Welches Zertifikat für die eigene E-Mail Adresse verwendet werden soll
- Ob ausgehende E-Mails normalerweise unterschrieben werden: Das sollte man aktivieren
- Ob ausgehende E-Mails normalerweise verschlüsselt werden sollten: Empfohlen

## Fragen und Antworten:

Wer ist CAcert?

- CAcert Inc. ist ein eingetragener Verein mit Sitz in Australien

Was ist eine CA?

- Eine CA bestätigt die Identität von Personen und Organisationen, und stellt digitale Zertifikate aus. („Personenbindung“)

Was hat CAcert für Ziele?

- Sicherheit für jeden erschwinglich und verfügbar machen
- Das Internet sicher und vertrauenswürdig machen
- Privatsphäre durch Verschlüsselung
- Sicherheit durch Authentifizierung
- Vertrauen in das Internet

Was macht CAcert?

- CAcert stellt SSL Zertifikate aus, ist ein sogenannter Zertifizierungsdienste-Anbieter (Amtsdeutsch)

Was ist der Unterschied zu anderen CA's?

- CAcert trennt die Assurance (Bestätigung der Identität

mittels amtlichen Lichtbild Ausweisen) von der Ausgabe der Zertifikate.

Dadurch muss man nur einmal bestätigt werden und kann sich dann jederzeit beliebig viele Zertifikate gratis selbst ausstellen

- CAcert ist sehr stark Community-basiert

Können auch Kinder assured werden?

- Ja. Personen unter 18 Jahren können auch selber Assurer werden, können aber maximal 10 Punkte vergeben.

Wie wird die Privatsphäre geschützt?

- Die Formulare werden vom Assurer aufbewahrt, und nur bei Bedarf an die Zentrale in Australien geschickt.
- Für Außenstehende ist nicht ersichtlich, wer wen assured hat.

Ist CAcert bereits in den Browsern drin?

- Aktueller Status:  
<http://wiki.cacert.org/wiki/InclusionStatus>

Haben Sie auch qualifizierte Zertifikate?

- Derzeit noch nicht, wir arbeiten daran

Was kann ich mit den Zertifikaten alles machen?

- Webserver mit HTTPS absichern (Webshops)
- E-Mails unterschreiben und verschlüsseln
- SSL/TLS
- Anmeldung bei Webseiten
- Anmeldung bei VPN's

Wie lautet der Fingerprint von CAcert?

- Steht auf dem Assurance Formular unten klein gedruckt drauf. Am besten dem Kunden ein leeres Formular mitgeben.
- Die meisten Programme verwenden diesen Fingerprint (MD5):  
A6 : 1B : 37 : 5E : 39 : 0D : 9C : 36 : 54 : EE : BD : 20 : 3  
1 : 46 : 1F : 6B
- Manche Programme verwenden diesen Fingerprint (SHA1):  
135C EC36 F49C B8E9 3B1A B270 CD80  
8846 76CE 8F33

Was ist 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 lebenslange Konto bei CAcert vergeben werden

Wie bekomme ich die Zertifikate in meinen Webserver Apache / IIS?

- <http://www.cacert.org/> → Deutsch → Anleitung

Welche Technologien werden verwendet/unterstützt?

- X.509 Zertifikate
  - Serverzertifikate
  - Clientzertifikate
  - Code-Signing
- OpenPGP
  - OpenPGP Signaturen (PGP + GnuPG)

Gibt es besondere Anforderungen für Zertifikate?

- Die folgenden Arten haben „erhöhten Sicherheitsbedarf“:
  - Code-Signing Zertifikate (Java, Active-X, Handys, ...)
  - Umlaut-Domänen (z.B.: österreich.at)
- Um diese Zertifikate ausstellen zu können, braucht man mindestens 100 Punkte, und muß eine Kopie des Lichtbildausweises an CAcert schicken und Code-Signing beantragen

Steht der Sourcecode von CAcert zur Verfügung?

- Der Sourcecode steht auf der Webseite für Audits zur

Verfügung, darf aber nicht für andere Zwecke verwendet werden.

Warum muss man immer von 2 Assurern bestätigt werden?

- Wegen des 4 Augen Prinzips. Sollte einer der Assurer ausfallen, ...
- Um die Sicherheit und das Vertrauen in das System zu erhöhen, ist es zwingend notwendig, dass jedes neue Mitglied von mindestens zwei Assurern überprüft wird.

Verwendet CAcert OCSP (Online Certificate Status Protocol)?

- Ja: <http://ocsp.cacert.org/>

Wieviele Leute verwenden CAcert schon?

Aktuelle Statistiken bitte von <http://www.cacert.org/stats.php> holen.

Stand Oktober 2006:

- Verifizierte User: > 70.000
- Ausgestellte Zertifikate: > 160.000
- Assurer: > 7000
- in über 30 Ländern
- in 25 Sprachen übersetzt

Was heißt Web of Trust? (WoT)

- Web of Trust heißt Vertrauensnetz. Durch die vielen Assurer weltweit, die sich und andere gegenseitig bestätigen, entsteht ein Vertrauensnetz.

Wo finde ich mehr Informationen?

- <http://www.cacert.at/>
- <http://www.cacert.org/>
- <http://wiki.cacert.org/>

## **Support:**

### ***CAcert Zentrale Australien:***

P.O. Box 81

2216 Banksia / NSW

AU - Australia

### ***CAcert Support Österreich:***

<http://www.cacert.at/>

[office@cacert.at](mailto:office@cacert.at) (jederzeit erreichbar)

Telefon:

### ***Im Internet:***

ICQ: 6588261

IRC: irc.cacert.org

Deutsch: #cacert.ger sourcerer, thesourcerer

Englisch: #cacert evilbuny, evilbunny

Skype: the\_sourcerer8