Certification Assurer
CACERT.AT
Österreich

CAcert.org

Certification Assurer
CACERT.AT
Österreich

CAcert

Fragen

- Warum verwenden die meisten Leute noch immer das elektronische Gegenstück der Postkarte?
- Warum verwenden die Leute noch immer Passwörter, und schicken sie im Klartext?
- Was kann ich tun, um mich und meine Privatsphäre zu schützen?

Certification Assurer
CACERT.AT
Österreich

CAcert

Langfristiges Ziel

- Privatsphäre durch Verschlüsselung
- Sicherheit durch Authentifizierung
- Vertrauen in das Internet
- Lösung für das Henne-Ei Problem: Zertifikate und Anwendungen

Certification Assurer
CACERT.AT
Österreich

Aufgabe einer CA

- „Zertifizierungsdiensteanbieter“
- Eine CA bestätigt die Identität von Personen und Organisationen auf digitalem Wege („Personenbindung“)
- Ausstellung von digitalen Zertifikaten

Certification Assurer
CACERT.AT
Österreich

Anwendungen

- Webserver mit HTTPS absichern
- Unterschreiben und Verschlüsseln von Emails

  - SSL/TLS Serverprogramme
  - Anmeldung bei Webseiten
  - Anmeldung bei VPN´s

Certification Assurer
CACERT.AT
Österreich

CAcert Inc.

- 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

Certification Assurer
CACERT.AT
Österreich

CAcert

Personenbindung

- Bisher: Kontrolle der Identität für jedes Zertifikat, dadurch Kosten pro Zertifikat von 200,- € pro Jahr
- Was hilft es mir, wenn ich mir ein Zertifikat leisten kann, aber der Rest der Welt nicht?
- CAcert trennt die Assurance (Bestätigung der Identität mittels amtlichen Lichtbild Ausweisen) von der Ausgabe der Zertifikate

Certification Assurer
CACERT.AT
Österreich

CAcert

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
- Freier Mark
- 5000 Assurer weltweit

Certification Assurer
CACERT.AT
Österreich

Punkteschema

- Ab 50 Punkten kann man Zertifikate ausstellen
- Ab 100 Punkten ist man Assurer, kann andere Personen Assuren, kann max. 10 Punkte vergeben, bekommt selber 2 Punkte dafür
- Bis 150 Punkte, da kann man 35 Punkte vergeben

Certification Assurer
CACERT.AT
Österreich

Organisationen

- 1. Variante: Die Leute werden normal von 2 Assurern bestätigt, und stellen sich selber Zertifikate aus
- 2. Variante: ein Zeichnungsberechtigter
  - Geschäftsführer, Prokurist, Vorstand, Rektor, ...
  - wird selbst Assurer (mit seinem **privaten Account**)
  - schickt den Handelsregisterauszug / Gründungs-urkunde / ... / amtliche Bestätigung an support@cacert.org
  - delegiert die Organisationsassurance dann an „Ad-ministratoren“ weiter
  - die dann Zertifikate mit dem Firmenwortlaut und der Firmenadresse direkt und einfach ausstellen können

Certification Assurer
CACERT.AT
Österreich

CAcert

Zertifikate

- Lebenslanger Account bei Cacert
- Zertifikate jederzeit selbst im Internet ausstellen
- Zertifikate sind kostenlos
- beliebige Menge von Zertifikaten
- dadurch nur Initialkosten, keine Folgekosten

Certification Assurer
CACERT.AT
Österreich

CAcert

Technologie

- X.509 Zertifikate
  - Serverzertifikate
  - Clientzertifikate
  - erhöhter Sicherheitsbedarf:
    - Code-Signing Zertifikate (Java, Active-X, Handys, ...)
    - Umlaut-Domänen
- OpenPGP
  - OpenPGP Signaturen

- CAcert eine plattform-übergreifende und technologie-neutrale CA!

Certification Assurer
CACERT.AT
Österreich

CAcert

Sicherheit

- CAcert wird durch einen WebTrust kompatiblen Audit überprüft
- Durchgängiges 4 Augen Prinzip
- Offene und transparente Strukturen
- Sourcecode steht für Audits zur Verfügung
- Sofortige Widerrufslisten + OCSP Live-Kontrolle

Certification Assurer
CACERT.AT
Österreich

CAcert

Signaturgesetz

- In der EU gibt es
  - Einfache Zertifikate
  - Fortgeschrittene Zertifikate
  - Qualifizierte Zertifikate
- Digitale Rechnungen
  - Österreich: mind. Fortgeschrittene Zertifikate
  - Deutschland: Qualifizierte
- CAcert
  - derzeit nur einfache Zertifikate
  - vielleicht bald fortgeschrittene
  - wenn Hardware verfügbar dann qualifizierte

Certification Assurer
CACERT.AT
Österreich

Client Zertifikate in der Praxis

- Firefox
  - Login
  - Email Adressen freischalten
  - Client Zertifikat beantragen
  - Zertifikat importieren
  - Zertifikat auf secure.cacert.org verwenden

Certification Assurer
CACERT.AT
Österreich

Server Zertifkat in der Praxis

- Apache
  - CSR generieren
  - Login
  - Domain freischalten
  - Server Zertifikat eantragen
- Vhosts:
  http://wiki.cacert.org/wiki/VhostTaskForce

Certification Assurer
CACERT.AT
Österreich

CAcert

Browser Security

- Sicherheitslücken:
  - Plugins
  - Browser Helper Objects (BHO)
  - DLL´s, Bibliotheken (modularität)
- Betroffene Browser
  - Internet Explorer / Win32
  - Firefox / Win32
  - andere werden folgen

Certification Assurer
CACERT.AT
Österreich

CAcert

Lösungen für Browser Security

- Sichere Plattform
  - Kein Windows
  - gehärtete Browser
    - CAcert Browser
  - Knoppix
    - CAcert Live-CD
- Zweiter Kanal
  - SMS
  - Anrufe

Certification Assurer
CACERT.AT
Österreich

CAcert

Erfolg?

- Verifizierte User: > 50.000
- Ausgestellte Zertifikate: > 105.000
- Assurer: > 5000
- Deutschland: >840 aktive Assurer (Platz 1!)
- in über 45 Ländern
- in 26 Sprachen

- http://www.cacert.org/stats.php

Certification Assurer
CACERT.AT
Österreich

CAcert

Danke

- http://www.cacert.org/
- http://wiki.cacert.org/

Noch Fragen?

Certification Assurer
CACERT.AT
Österreich

Wie krieg ich jetzt mein Zertifikat?

- Formular holen, oberen Teil ausfüllen
- Mit amtlichem Lichtbildausweis zu uns kommen
- Zertifikate selber über das WebInterface erstellen
- Freiwillige Spende
- Account anlegen auf www.cacert.org
  - Email Adresse innerhalb 24 Std. kontrollieren
  - Passwort: Groß+Klein+Ziffer+Sonderz.