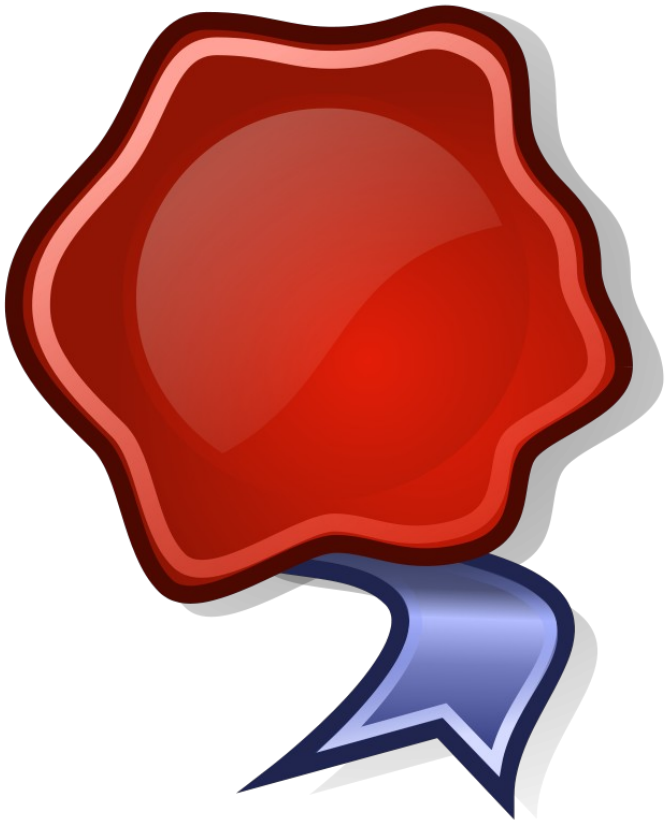

CAcert und das Audit

Was ist das Audit?

Was ist das Audit?

- **Auslöser:**
  - Aufnahme der Root-Zertifikate in die Browser

➔ Audit ist unabdingbar

  - Qualitätssicherung innerhalb der CA

- Unabhängige Prüfung durch einen Auditor
  - Systeme
  - Dokumente
    - Policies
  - Abläufe

Audit-Bereiche

Geschäftsbereiche von CAcert

- Aktuell 3 Aufgabenbereiche
  - Assurance (RA – Registration Authority)
  - Systeme (CA – Certificate Authority)
  - Community (Audit Background)

- Prüfung durch das Audit
  - Registration Authority
  - Certificate Authority

RA (Registration Authority)

- Assurance-Policy hat POLICY-Status erreicht
  - Dokument ist bindend für alle Assurer
  - Das Assurance-Prinzip kann geprüft werden
- Wichtige Punkte für die Prüfung:
  - CATS (Assurer-Challenge)
  - ATE (Assurer Training Events)
  - Co-Audit

CA (Certificate Authority)

- Security Policy
- Security Manual

- Prüfbereiche:
  - Systeme
  - Software

Wichtige Punkte für die Prüfung

CATS

- **C**Acert **A**utomated **T**esting **S**ystem
- Bestehend aus 25 Fragen
  - Multiple Choice
  - 80% müssen richtig beantwortet werden
- Kann beliebig oft wiederholt werden
- Minimaler Standard zur Qualitätssicherung
  - Aneignung des Wissens im Interesse der Community

Assurer Training Events

- Vortragsreihe für Assurer
  - Idealerweise werden alle Assurer erreicht
  - **2009**: 20 ATEs in Europa
  - **2010**: Bisher zwei Events (Sydney, Essen)
- Information über alle aktuellen Themen
  - Policies
  - Abläufe
  - Empfehlungen
- **Empfehlung:** Jährliche Teilnahme an einem ATE

Co-Audit

- Qualitätssicherung der Assurance
  - Als definierter Prozess in der Community
  - Essentiell für das Audit
- Statistische Erhebung
  - Umsetzung der Policies in der Praxis
  - Grundlegendes Wissen
  - Inhalt nach Absprache im Co-Audit-Team
- **Certificate Authority Review Checklist:**
  - *„The CP details how the CA verifies that RAs operate in accord with the CA's policies.„*

Einfluss auf den Bereich Assurance

Änderungen an der Assurance

- Bestätigung des Mitglieds (Assuree)
  - Persönliche Daten sind korrekt
  - Zustimmung zum CCA (CAcert Community Agreement)
- Bestätigung des Assurers
  - Assurance wurde entsprechend der Assurance Policy durchgeführt

- **CAcert Assurer Reliable Statement (CARS)**
  - Verpflichtung der Community gegenüber

Prüfung der Assurance

- **2009**
  - **Februar bis Juni:**
    Erhebung der Assurance-Qualität
  - Co-Audit als Maßnahme zur Prüfung abgesegnet
  - Audit aus anderen Gründen ausgesetzt
- **2010**
  - Assurance-Abläufe können nach Ende des Jahres geprüft werden
  - Co-Audit ist im März (CeBIT) angelaufen

Prüfung der Systeme

Prüfung der Systeme

- Sicheres Hosting seit Oktober 2008
  - Teams
  - Rechenzentrum
  - Server
- Security Policy (seit März 2009)
  - Bindende Policy für CAcert-Mitglieder in sicherheitskritischen Positionen
- Software
  - CPS (Certification Practice Statement)
  - Teams

Aktueller Stand der Systeme

- Teams
  - Kritische Systemadministration (Critical Sysadmins)
  - Physikalischer Zugang (Access Engineers)
- Security Policy im DRAFT-Status
  - Bindend für kritische Rollen
    - Systemadministratoren, Zugangsingenieure, Support, Software
- Systeme in sicherem Rechenzentrum
  - BIT, Ede, Niederlande

Aktuelle Vorhaben

- Unkritische Systeme
  - Reorganisation wird durchgeführt
- Root-Zertifikate
  - in Planung
- Notfallpläne / Disaster Recovery
  - in Planung
- Aufbau und Erweiterung von Teams
  - Software Assessment
  - ...

Software

- Erhebung des aktuellen Stands 2009 in Innsbruck
  - Erhebliche Probleme mit Wartung, Weiterentwicklung und Absicherung
  - Keine verlässlichen Aussagen möglich
- **Ansatz 1**
  - Neues Entwicklungsteam
  - Neues Design: **BirdShack**
- **Ansatz 2**
  - Alte Software im Wartungsmodus

Die Community und das Audit

Audit und die Community

- **Kriterien des Audits**
  - **DRC** (**D**avid **R**oss **C**riteria)
  - David Ross hat das Audit 2005 begonnen
- **Gegenstand der Kriterien**
  - Risiken
  - Haftung
  - Pflichten
- Transparente Darstellung der Außenwelt gegenüber

- Große Herausforderung für die CA

Herausforderungen

- Wie sind die Kriterien für CAcert definiert?
- Wer ist daran gebunden?
- Sind die Kriterien vernünftig?
- Wie können wir die Anforderungen umsetzen?

- **Ergebnis:**
  - CAcert Community Agreement (CCA)

Anforderungen an das CCA

- Aufbau einer Gemeinschaft, deren Mitglieder sich gegenseitig verpflichtet sind
- Aufzeigen der Risiken, Haftung und Pflichten
- Beschränkung der Haftung
  - Aktuell **1000 €** materielle Haftung
- Haftung an Mitglieder zurückgeben

Verantwortungen im CCA

- Wie wird die Haftung umgesetzt?
  - eigene Plattform zur Streitschlichtung
    - Arbitration
  - Einverständniserklärung der Mitglieder
    - CAcert Community Agreement 3.2
    - *„You agree, with CAcert and all of the Community, that all disputes arising out of or in connection to our use of CAcert services shall be referred to and finally resolved by Arbitration [...]“*
  - Regelung der Schlichtung durch Policy
    - Dispute Resolution Policy (DRP)

Arbitration

Gründe für die Arbitration

- Audit verlangt Offenlegung der Haftung
- **Lösungsansätze:**
  - Limitierung
  - Zuweisung
- Sicherer und effizienter Weg zur Umsetzung
  - Delegation an eigene Arbitration

Fragen?