ATE Presentations SHORT Talk Script

1. Audit and Assurance

Slide 1.1
- CAcert want's the Roots into the Browser
- This requires Audit
  - Audit requires Policies (we have)
  -

Slide 1.2
- Audits Business Areas are
  1. Assurance (Registration Authority)
  2. Systems (Certificate Authority)
     a. Datacenter b. Software

We focus on 1. Assurance

Slide 1.3
- Policies:
  - CCA CAcert Community Agreement
  - AP Assurance Policy
    related documents:
    AH Assurance Handbook
    PoN Practice On Names
    AP-Subpolicies
    PoJAM Policy On Junior Assurers / Members
  - DRP Dispute Resolution Policy

Slide 1.4
- CAcert follows DRC Audit Criteria
  (David Ross Criteria)
  This defines
  R/L/O (Risks/Liabilities/Obligations)
  acceptance by each member
  This is specified in CCA
  So therefor in the Assurance process
  we have to check
  Does the user accepts CCA ?

Slide 1.5
  To check knowledge about:
  Risks: User can find himself subject to Arbitration
  Liabilities: Limited to 1000 Euro
  Obligations: to keep primary Email address in good working order

Slide 1.6
- Why CAcert Internal Arbitration ?
  to protect the Community
  to protect the member
  Arbitration is the general Fallback option
  for everything undefined
  eg policy exceptions, disputes between members, and much more

Slide 1.7
- CARS
  CAcert Assurer Reliable Statement
  Assurance Statement is an Assurer Reliable Statement
  CARS introduced within Arbitration

Slide 1.8
- AP Assurance Policy

Defines the process of Assurance

This follows the

Slide 1.9
The 5 Purposes of Assurance (Brick Policy to Practice)

Overview

Slide 1.10
1. Member
We have to do with a bonafide member

Slide 1.11
2. Account
As bonafide member, the user has an Account
with a verfied primary email address
(ask Assuree: Do you have an Account ?)
(ask Assuree: is the given email Address the primary email ?)

Slide 1.12
3. Certificate
With an Account, a user can issue certificates

If there is a problem with certificates,
with the unique serial number of each cert
this can be mapped to an account, so therefor

Slide 1.13
4. Arbitration
we can bring the member into arbitration
(check CCA acceptance -> bind user into Arbitration)

Slide 1.14
5. Data
there is some data known to the user
primary email, full name, secondary identification (-> DoB)

Further AP defines, what has to be onto a CAP form
(AP 4.5)

Slide 1.15 (Pictures)
- presenting CAP form ... with above topics
especialy CCA acceptance
(identify „new" CAP Form → 2 text blocks in Applicants block)

Slide 1.16 (Picture)
if CCA acceptance is not on CAP, write it
by hand
"I hereby accept CCA"

2. Assurance and Practice

Slide 2.1
- Names

5 simple strict rules
see current PracticeOnNames
-> Basic, Simple, Strict Rules

Rule 1: We assure only names, that we can find in at least one ID document.

Rule 2: Its allowed to reduce informations, but its prohibited to add informations.

(The data of the ID documents does not have to be used completely, that is not all given names have to be used and names may be abbreviated under certain circumstances.)

Rule 3: Document missing names on the CAP.

(A person may have multiple names as long as they are verifiable with official ID documents)

Rule 4: Transliterations are accepted (8bit to 7bit)
(because of technical reasons)

Rule 5: We use Case-Insensitive

```
Slide 2.2

  By international requirements, CAcert moves
  to the more "Relaxed Rules" (including Country variations)

  Can we handle names simply with the strict rules ?
  if yes: finished
  if no: continue with the relaxed rules
  Does a relaxed rule apply ?
  if yes: finished
  if no: rethink to file a dispute

Slide 2.3  (picture)
  We check twice
  Face-2-Face  ID doc to CAP
  @Home        CAP to Online-Account

Slide 2.4  (O->Ö sample picture)
  OE → Ö  (one sample for all rules)
  for: we check twice

Slide 2.5
  Documentation is Essential !
  write down full names as read in ID doxs
  identify givenname, lastname

  use backside of CAP form

Slide 2.6

- Signature

  Signatures may vary ..
  So we check the signature at F2F meeting


Slide 2.7

- DoB

  DoB errors 3 steps check
  50% error rate in first Audits
   1. Check date format (british, US, others)
      Identify: Year, Month, Day parts
   2. Check Number by Number → Order 10 → 01 (!)
   3. write down month in words -> 10 -> Oct
```

Slide 2.8

- Passports

  Security Features (UV, microscript, Holos, …)

  Known Security Features:
  - Hologramme
  - Micro Schrift
  - Wasserzeichen
  - Strukturen
  - Microlinien
  - Interferenzmuster
  - Ausstellungsdatum/Expiredatum different
  - UV Merkmale

Slide 2.9
  allowed Iddoxs (Issuer)
  what to do, if I did not have seen a document before ?
  Document all Security Features you'll find on backside of CAP

Slide 2.10
  check @home
  PRADO, CAcert Wiki: AcceptableDocuments

3. Evidence Gathering

Slide 3.1

- Evidence in Assurance Process

  Document, Document, Document

  eg write down full name, also if user wrotes down
     not all names

  If you feel, that there is something weak, document!

Slide 3.2
  CARS
  CARS is also needed in the Co-Audit process.
  We check the Assurers, results presented to Auditor with CARS
  The Assurer signs his CAP form. So this marks the CAP:
  This is a CAcert Assurer Reliable Statement.

  This information is correct and is
  verifyable. If you make false statements,
  you are bound to Arbitration.

  All "addtl." Documentation falls under this
  section.
  First used and spread out in Arbitration.

Slide 3.3
  So Arbitrators often request some infos
  about an assurance in an email with request
  for your CARS statement. This is given by:

Your Name
CARS

Slide 3.4
Advanced Assurance Processes, Procedures

- PoJAM
- Procedures
  - Missing CCA
  - Pwd Recovery w/ Assurance
  - Name Change after marriage w/ Assurance
  - Privacy Breach (asking Experienced Assurer)

PoJAM - Parental Consent
note that parental consent has been confirmed

Missing CCA acceptance line
write down by hand

Pwd Recovery w/ Assurance
exchange A-word Assurer/Assuree, give Assuree A-word, Assurers Name, Email
write down on CAP A-word
@home: write email to support with the infos collected

Name change after Marriage w/ Assurance
Name before/after marriage, if Arbitration case #, add onto CAP

Privacy Breach
eg Asking Experienced Assurer
Date, Time, Who, Reason (write on backside of CAP form)

Slide 4.1

- Helping CAcert

Audit
=====
Audit lief bis Mitte 2009
Einer der wesentlichen Gründe fuer den Abbruch
waren: fehlende Resourcen (Mitarbeit durch Board/Community)

(Abwaelzung der Arbeit auf den Auditor)
Board sowie Community dachten sich .. der Auditor
fuehrt das Audit schon durch …

Weit gefehlt ...

(Schlussfolgerung)

Der Auditor fuehrt das Audit nicht alleine
durch, es bedarf der Unterstuetzung durch das Board
und durch die Community

4.1 Mithilfe - Audit

In 2010 wurden bereits alle restlichen Policies verarbschiedet

Software-Assessment – die Basis damit die Software im Kritischen System gewartet, upgedated werden kann, gab es de facto nicht
Dieses Projekt laeuft seit Ende 2009 und hat mittlerweile eine Audit-faehige Prozedur fuer Software-Updates entwickelt, die unter anderem fuer das CCA Rollout notwendig sind - die Unterrichtung saemtlicher Mitglieder ueber das CAcert Community Agreement und die Zustimmung durch saemtliche Mitglieder.

Das Problem: Software-Assessment arbeitet nur schleppend.
Grund: Wir haben zwar ein Software-Testteam von 10-15 Leuten, wenn es aber zum Testaufruf kommt, passiert nichts.
Keine Tests.
Wir suchen daher dringend weiter nach
aktiven Software Tester

Audit over Assurance ist mit den Co-Audits seit Maerz 2010 am Laufen. Die Basis fuer die Co-Audits sind die Assurer Training Events. Wir brauchen mehr …
Bislang haben wir gerade mal 1 / 4 der Assurer geprueft die fuer ein Audit geprueft werden muessten.
Hier suchen wir Helfer, die zum einen ATEs lokal organisieren, so wie hier fuer Muenchen Frank das uebernommen hat, zum anderen Suchen wir aber auch finanzielle Unterstuetzung, insbesondere fuer ATEs in anderen Laendern

Mit Hilfe der ATEs haben wir aus den Erfahrungen aus der ATE Serie 2009 eine ganze Reihe neuer Helfer finden koennen, was wir zum Anlass genommen haben, hier auch die Helfer fuer die weiteren Tasks auf dem Weg zum Audit zu finden, um fuer die eigentlichen wesentlichen Projekte Spezialisten zu finden, die in der Lage sind, die anstehenden Projekte zu stemmen.

Eines der Projekte ist die Infrastruktur Seperation der Non-Critical Systeme.
Damit der Auditor nicht 10 bis 20 Systeme zu ueberpruefen hat, die in Ede im Rack zusammen stehen, sollen die Non-Critical Systeme in ein anderes Rechenzentrum ausgelagert werden.
Hier suchen wir weiterhin Hosting Provider, die den Infrastruktur Systemen ein neues Zuhause geben - Stichwort Sponsoring, zum anderen suchen wir Systemadministratoren mit Migrationserfahrungen und Systemadministratoren die Erfahrungen mit Virtualisierung haben.

Im April 2009 wurde beim Software-Camp Innsbruck zusammen mit dem Auditor die bisherige Software fuer nicht Auditierbar befunden.
Mit dem Software-Assessment Projekt wurde dies zu Teilen bereits widerlegt.
Das Ergebnis von Innsbruck war das Projekt „Birdshack“, die Software neu zu schreiben.
Beide Software Projekte laufen nun parallel.
Fuer Birdshack suchen wir Software Entwickler:
C/C++ fuer den Kernel, Python fuer den Dispatcher und Java fuer die Applikationsschicht.

Nun kommen wir langsam in die Regionen zur Vorbereitung
des eigentlichen Audits. Die Plaene gehen derzeit in die
Richtung das Audit aufzuteilen in das Audit over Assurance
und in Audit over Systeme …
Fuer beide Projekte werden Gelder benoetigt, die mit dem
Funding Projekt beschafft werden muessen.
Hier suchen wir Mitglieder mit Erfahrungen auf diesem Gebiet.

Einer der grundsaetzlichen Projekte auf dem Weg zum Audit
ist die Erstellung neuer Roots und das Finden einer
Sicherungsmassnahme (Escrow Projekt), um die Roots ueber
einen Zeitraum von vielleicht 30 Jahren zu sichern.
Das Generieren von neuen Roots wurde Ende 2008 schon einmal
durchgefuehrt, aber sowohl die alten Roots alsauch die Roots
von 2008 waren im Fruehjahr als Audit-fail eingestuft worden.
Die 2008er Roots Prozedur wurde zwar vom Auditor kontrolliert,
aber die nachfolgende Escrow Methode war Audit-fail.
Weswegen nun der Fokus auf der Entwicklung einer Escrow
Methode liegt, damit die zu generierenden Roots
auch bezueglich der Sicherungsmassnahmen
Audit-Bedingungen entsprechen.
Hier suchen wir Spezialisten im Crypto Bereich, die sich
mit den Sicherungsverfahren fuer Root Keys auskennen.
Die sich mit dem Thema „Risk-Analyse" auskennen, die
entweder ein Team beraten koennen, oder die selbst
in einem Team mitarbeiten koennen.

Und dann haben wir da noch das „CrowdIt" Projekt.
Das ist das Projekt die Audit Kriterien, die
David-Ross-Criterias vom rein theoretischen ins Praktische
zu uebersetzen und so mit Inhalt zu fuellen.
Sprich: jeder einzelne der Kritierien – lauter Fachchinesisch -
muss durch einen Spezialisten, der sich mit dem Vokabular
auskennt, in die entsprechende Praktische Entsprechung
uebersetzt werden. Die entsprechenden Team Mitglieder
muessen angesprochen werden, um die Ergebnisse dann
zusammentragen zu koennen. Jeder Punkt muss dann
mit einem CARS Statement in eine Datenbank eingetragen
werden, bis saemtliche der Audit-Kriterien abgearbeitet sind.

Slide 4.2

Um die bisherigen Team Mitglieder zu entlasten,
Zeit fuer Aufgaben im Audit Bereich zu uebernehmen
waere es auch hilfreich die laufenden Teams
zu unterstuetzen.
Hierzu zaehlt die Mithilfe bei der weiteren
Ueberarbeitung der Policies – einer der letzten
Anpassungen ist beispielsweise die Ueberarbeitung
der CCA
Einfache Aufgaben koennen bei Assurance Events
bei der Organisation derselben uebernommen werden.
Organisation von ATEs, Mithilfe im Bereich
Organisations-Assurance

Damit das Arbitration System weiterhin Arbeitsfaehig
bleiben kann suchen wir dringend neue Arbitrators
Ebenso um Support am Laufen zu halten suchen wir
dringend neue Triage Members und Support Engineers.
Fuer beide Bereiche ist die Mithilfe bei Uebersetzungen

gefragt.
Im Bereich Software Entwicklung suchen wir weitere Entwickler und Tester.
Aber auch weitere Systemadmins um die Infrastruktur Systeme zu betreuen.

(Ueberleitung zu Co-Audit)

In welchem Bereich kannst du hier weiterhelfen ?

Ok, die Frage braucht ihr jetzt nicht sofort beantworten … ihr koennt euch aber schon einmal Gedanken darueber machen . . .
Waehrend der Co-Audited Assurance koennt ihr dann das Thema genauer eroertern.