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 1+2
The magnificent seven (AP 4.5)
7 topics to check on Assuree
7 topics to check on Assurer

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 runs till mid 2009
Stopped mostly by lack of Resources
by Board, by Community

Community thoughts, the Auditor will do the work

Auditor does not do the audit alone
Audit needs work by the Community

4.1 Helping - Audit

In 2010 the last policies comes in effect at least to DRAFT

Software-Assessment, groundbase for Software updates on the critical system comes to work - slowly – but it works. One audit blocking factor: CCA Rollout needs patches. The notification to all members about the CAcert Community Agreement

Software-Assessment works slowly caused by not effective working Testteam.
We need: aktive Software Tester

Audit over Assurance (RA) is still running since March 2010 with the co-audited assurance program. With the Assurer Training Events we hope to find the resources we need for the special projects on the agenda
Co-audited Assurances we had only a quarter tested. We need to test more, especialy countries outside Germany and the Netherlands
So here we need support for the Co-Auditors team (travel expenses)

Infrastructure Admins with migration skills to help in the Infrastructure project to move the non-critical systems into another hosting center
Here we search for hosting providers sponsoring and / or groups who can deal with running the non-critical systems in a hosting center

In April 2009 at the Innsbruck Software Camp
the Software was attested to be non auditable
With the Software-Assessment project, we've got an update procedure.
Despite the fact, a new project has been started – Birdshack to rewrite the software. So here we search developers and teams

To bring in an Auditor for Audit over Assurance (first step) and for the Audit over Systems (second step), we need Audit funding.
We search consultants and specialists with skills in this area

New Roots & Escrow project …
We search experts in this area, familiar with the Escrow methods, skills in riscs analyze who can bring forward this project

And we have the CrowdIt project.
This is the project to „translate" the audit criterias into a database of results.
A consultants, familiar with the Audit terminological terms who can translate the criteria into „practical" topics, who can request from the teams and groups the required content. Push them to fill the database.

Slide 4.2 Helping the teams
to relieve the existing team members, to pickup other audit related tasks, we need also new team members in the running teams:
Helping on Policy group – eg CCA needs some updates
Helping on Assurance Events, organzing ATEs, helping in OA and TTP program

We need more Support team members, starting with Triage, moving to Support-Engineers
We need more Arbitrators

For both, Support and Arbitration we search translators as more and more foreign languages comes in

Software-Developer, Software-Testers, Infrastructure Admins

(transition to Co-Audit)

In which are you can help ?

Ok, you have not to answer this question right now,
but you can talk with the Co-Auditor later in the face-2-face
interview. But you can please rethink right now, in which
area you might can help