Attribute Based Credentials for Trust: towards the privacy preserving eIdentity management of the future

ABC4Trust EU project

https://abc4trust.eu/
More and more business/government services are migrated online
  - Improves convenience
  - Reduces costs

High-value transactions require high-level of identity assurance
  - Usernames/passwords are ubiquitous, but provide low-security
  - Conventional “enterprise” solutions (e.g., Kerberos, PKI) don’t scale or are not flexible enough for an internet-wide system
  - How can you show some ID (identifier) online, just like in real life?
Identity federation

• Most popular proposed architecture
  ▪ Very flexible
  ▪ Easy to deploy
  ▪ Many protocols: WS-Federation/Trust, SAML, Information Cards, OpenID, OAuth, ...

• But many challenges
  ▪ Security
  ▪ Privacy
  ▪ Scalability
What’s new? Minimal disclosure!

- ABC tokens cannot be combined and lead to the revelation of identity
  - Token issuance and presentation are unlinkable
  - Think “coins” (cannot be distinguished) vs. “bills” (have a serial number!)

- Users can disclose a *subset* of the encoded claims
  - To respond to unanticipated requests of RPs
  - Without invalidating the token integrity
An example of minimal disclosure:

Name: Alice Smith
Address: 1234 Pine,
        Seattle, WA
Over-21: true

Coho Winery
Prove that you are over 21 and from WA

Which adult from WA is this?

Coho Winery

State

Name: [redacted]
Address: [redacted] WA
Over-21: true

Minimal disclosure illustrated
### ABC4Trust participants:

<table>
<thead>
<tr>
<th>Participant No.</th>
<th>Participant organization name</th>
<th>Participant short name</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Goethe-Universität Frankfurt am Main</td>
<td>GUF</td>
<td>Germany</td>
</tr>
<tr>
<td>2</td>
<td>Alexandra Institute AS</td>
<td>ALX</td>
<td>Denmark</td>
</tr>
<tr>
<td>3</td>
<td>Research Academic Computer Technology Institute</td>
<td>CTI</td>
<td>Greece</td>
</tr>
<tr>
<td>4</td>
<td>IBM Research GmbH</td>
<td>IBM</td>
<td>Switzerland</td>
</tr>
<tr>
<td>5</td>
<td>Miracle A/S</td>
<td>MIR</td>
<td>Denmark</td>
</tr>
<tr>
<td>6</td>
<td>Nokia Siemens Networks GmbH &amp; Co. KG</td>
<td>NSN</td>
<td>Germany</td>
</tr>
<tr>
<td>7</td>
<td>Technische Universität Darmstadt</td>
<td>TUD</td>
<td>Germany</td>
</tr>
<tr>
<td>8</td>
<td>Unabhängiges Landeszentrum für Datenschutz</td>
<td>ULD</td>
<td>Germany</td>
</tr>
<tr>
<td>9</td>
<td>Eurodocs AB</td>
<td>EDOC</td>
<td>Sweden</td>
</tr>
<tr>
<td>10</td>
<td>CryptoExperts</td>
<td>CRX</td>
<td>France</td>
</tr>
<tr>
<td>11</td>
<td>Microsoft Research and Development France</td>
<td>MS</td>
<td>France</td>
</tr>
<tr>
<td>12</td>
<td>Municipality of Söderhamn</td>
<td>CSH</td>
<td>Sweden</td>
</tr>
</tbody>
</table>
Visit: https://abc4trust.eu/

ABC4Trust
Attribute-based Credentials for Trust

Welcome to the web presence of the EU-funded research and development project ABC4Trust!

On this website, you will find project-related information and research results as well as media material for educational purposes. If you have any further questions, please do not hesitate to contact us.
1. You will Meet the privacy-ABCs Technology

- Crypto technology combining the security of PKI with the flexibility of federation, providing user-centric, privacy-by-design
- It is planned be the future e-identity standard (applications include: e-commerce, e-government, e-voting, blogging, e-consultation, financial applications like lotteries)
By joining our Pilot:

2. You will participate in a lottery using this unique technology.

The winner receives:

- A registration for two people for the upcoming **International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies in September 2014**
By joining our Pilot

3. You will also be rewarded with a bonus mark for your final grade at the “Distributed Systems I” course:
   - If you sign the distributed User Consent Form
   - If you have participated at the course evaluation in the end of the semester
   - If you join the lottery
   - If you deliver a questionnaire of your feedback on the usability of the privacy-ABCs technology
By joining our Pilot:

4. You get:

- The **smart card reader & your eIdentity smart card** loaded with your privacy ABC-credentials

- The book: “**The Future of Identity in the Information Society: Challenges and Opportunities**” written by some of the leader in the eIdentity domain
A group of 60 students will take part in the evaluation of two courses they have attended at a University Department.
It will take place in the Computer Engineering and Informatics Department of the University of Patras in Greece.
A group of 60 students will take part in the evaluation of the following two courses:

- Distributed Systems I
University Pilot will realize a trial where university students can anonymously rate courses they took while ensuring that:

1. students have indeed taken the course and have had sufficient attendance
2. can only rate the course once, without keeping list of students who have already rated the courses, so as to protect student anonymity.
3. Can join a lottery
Students of Computer Engineering and Informatics Department will be issued credentials that certify a number of facts about them e.g.:

- year of study
- major
- percentage of attendance of a course (5 attendance units).
A student can be eligible to participate the course evaluation:

☑ by using his credentials with ABC technologies in order to prove some facts about him, i.e.:
  ☑ whether he took the course,
  ☑ the year of his first registration to the university department
  ☑ his course attendance ratio.
The sufficiency of attendance will not be proved by revealing the exact attendance percentage (as this might be used to identify students)

it just shows that is above the predefined attendance threshold that allows the student to enter the evaluation process (or to get a bonus ).
• All the students can also prove that they participated in the course evaluation, in order to have access to a Tombola lottery.

• A participated student in lottery will win a prize.

A registration for two people for the upcoming International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies in September 2014.
Course Rating by Certified Students

LEGEND

- Storage of information
- Request/data flow
- Network link

User (student) -> Smart card reader with Smart card storing student ABCs

1. Request ABC
2. Send ABC
3. Request Course evaluation form
4. Request proof of eligibility
5. ZKIP of eligibility
6. Allow access if ZKIP correct
University Pilot Portal

- University Pilot Portal is an information web portal (https://ces.cti.gr/Portal/Portal.html)
University Pilot Portal

- University Pilot Portal consists of three blocks:
  - Get Credentials
  - Evaluation
  - General Info
  - User Manual
  - Join Tombola lottery
  - All the necessary software
Today

• We will make a short introduction in the aspects of ABC4Trust Pilot
• We will distribute the User Consent Form in order to sign it
• You will get Your SC
• You will collect your first attendance Unit
Participating in the Pilot

Beginning of the Semester (Red Phase)
- Get Your Smart Card
- Setup Your PC
- Unistall ABC4Trust User Service
- Register Your Smart Card
- Get a University Credential
- Get a Course Registration Credential
- Test Your Smart Card

During the Semester (Blue Phase)
- Collect Class Attendance Evidence
- View Attendance Units
- Periodic Backup of Your Smart Card
- Smart Card Restore in Case Needed
- Change Your PIN
- Unlock Your card
- View Your Credentials
- Delete Your Credentials

In the end of the Semester (Green Phase)
- Participate in the Course Evaluation
- Join the Tombola lottery
Today

- We will provide you with:
  - A smart card (*You can keep it in the end*)
  - A sealed envelope that is marked with the smart card ID and contains your smart card’s PIN and PUK.
You will obtain your attendance data:

- You have to wave your smart cart in front of a contactless NFC reader
On 11/11/2013

• We will provide you with:

☑ A smart card reader (*You can keep it in the end*)
☑ A slip of paper containing a one-time-password (OTP)
You will be able to:

**Beginning of the Semester (Red Phase):**
- Get Your Smart Card
- Setup Your PC
- Unistall ABC4Trust User Service
- Register Your Smart Card
- Get a University Credential
- Get a Course Registration Credential
- Test Your Smart Card

**During the Semester (Blue Phase):**
- Collect Class Attendance Evidence
- View Attendance Units
- Periodic Backup of Your Smart Card
- Smart Card Restore in Case Needed
- Change Your PIN
- Unlock Your card
- View Your Credentials
- Delete Your Credentials

**In the end of the Semester (Green Phase):**
- Participate in the Course Evaluation
- Join the Tombola lottery
Pilot’s Information

• Take a look at:
• Patras Portal
• Course’s Forum
• User manual
• User Consent Form