Agenda

• Introduction
• Overview
  ▪ Components
  ▪ Interfaces
  ▪ Data Flow
• Demo application
At a Glance

- Implements the ABC4Trust architecture
- Written in Java
  - Most source code is available on GitHub
  - Uses maven as build tool
- Features
  - Designed for a typical desktop/server setup
  - Supports hardware and software smart cards
  - User interaction via a User Service and Browser Plugin
Central Components

• core-abce
  ▪ abc4trust-xml
    • Schema definitions for presentation policies, credential specifications, etc.
  ▪ abce-interfaces
    • Interfaces for abce-components
  ▪ abce-components
    • Implementation of core components
  ▪ abce-services
    • REST API for abce-components

• java-ui
  • User interface
Interfaces

- Java API for the ABC Engine
- RESTful web services
  - Mainly for demonstration and integration testing
  - Set up the ABC Engine
    - Import parameters from files
      - E.g. credential specifications and issuance policies
    - Perform simple cross validations
      - E.g. does there exist issuer parameters for the UID in the issuance policy?
    - Export parameters if needed
      - E.g. issuer parameters for other components
An issuance/presentation between a User and Issuer/Verifier involves communication between the following components:

- Issuer / Verifier Application
- Browser Plugin
- User Service
- Identity Selector
• The application notifies the Browser Plugin via JavaScript about the action to take, policies and endpoints.
• The Browser Plugin retrieves the resources and passes them to the User Service.
• The User Service computes the possible ways to satisfy the policy and returns the list to the Browser Plugin.
• The Browser Plugin passes this information to the Identity Selector which presents the choices to the user.
• Once the user has made a selection, the choice is returned to the Browser Plugin.
• The Browser Plugin passes the choice to the User Service.
• The User Service computes an ABC protocol message (issuance message) which is sent to the Browser Plugin.
The Browser Plugin sends this protocol message to the application, which can then act accordingly.
Building an Application

• Setup
  1. Define credential specification and policies
  2. Setup system parameters
  3. Setup issuer parameters
  4. Setup inspector / revocation authority parameters
  5. Distribute public parameters

• Runtime
  ▪ Call the ABC Engine interfaces (REST or Java)
  ▪ Keep track of sessions
Demo Application Flow

• Hotel booking
  - User gets credentials
  - User books a hotel room
  - User does not show up
  - Hotel asks inspector for gets credit card number
  - Inspector reveals credit card number
  - Hotel collects payment

• Age verification
  - User proves that he is over a certain age
Demo

HOTEL BOOKING
Hotel Booking

ISSUER
Create Person

Person Id: (autogenerated)
Firstname: John
Lastname: Doe
Gender: M
Birthday: 21 July 1976
PIN: (autogenerated)
## Issuer Application

### Person List

<table>
<thead>
<tr>
<th>Person Id</th>
<th>Firstname</th>
<th>Lastname</th>
<th>Gender</th>
<th>Birthday</th>
<th>PIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.000.000.000</td>
<td>John</td>
<td>Doe</td>
<td>M</td>
<td>1976-07-21</td>
<td>14776</td>
</tr>
<tr>
<td>1.000.000.001</td>
<td>Alice</td>
<td>Von Nextdoor</td>
<td>F</td>
<td>1981-02-03</td>
<td>53281</td>
</tr>
</tbody>
</table>
Issuer Application

Adding Credential

- Person Id: 1,000,000,000
- Firstname: John
- Lastname: Doe
- Gender: M
- Birthday: 1976-07-21
- PIN: 14776

New CreditCardCredential

- Number: (autogenerated)
- Issuer: AMEX
- Holder: John Doe
- Expire: 5 August 2016
### Issuer Demo Application

<table>
<thead>
<tr>
<th>Person ID</th>
<th>1,000,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firstname</td>
<td>John</td>
</tr>
<tr>
<td>Lastname</td>
<td>Doe</td>
</tr>
<tr>
<td>Gender</td>
<td>M</td>
</tr>
<tr>
<td>Birthday</td>
<td>1976-07-21</td>
</tr>
<tr>
<td>PIN</td>
<td>14776</td>
</tr>
</tbody>
</table>

#### CreditCardCredentials

<table>
<thead>
<tr>
<th>Number</th>
<th>Issuer</th>
<th>Holder</th>
<th>Expire</th>
<th>Issued</th>
<th>Revoked</th>
</tr>
</thead>
<tbody>
<tr>
<td>123,400,000,001</td>
<td>AMEX</td>
<td>John Doe</td>
<td>2016-08-05</td>
<td></td>
<td></td>
</tr>
<tr>
<td>123,400,000,002</td>
<td>VISA_BEST_BANK</td>
<td>John Doe</td>
<td>2016-08-05</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### IdCardCredentials

<table>
<thead>
<tr>
<th>Person ID</th>
<th>1,000,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firstname</td>
<td>John</td>
</tr>
<tr>
<td>Lastname</td>
<td>Doe</td>
</tr>
<tr>
<td>Birthday</td>
<td>1976-07-21</td>
</tr>
</tbody>
</table>

#### PassportCredential

<table>
<thead>
<tr>
<th>Number</th>
<th>Country</th>
<th>Firstname</th>
<th>Lastname</th>
<th>Birthday</th>
<th>Expire</th>
<th>Gender</th>
<th>Issued</th>
<th>Revoked</th>
</tr>
</thead>
<tbody>
<tr>
<td>1,000,000,000</td>
<td>CH</td>
<td>John</td>
<td>Doe</td>
<td>1976-07-21</td>
<td>2024-08-05</td>
<td>M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### StudentCardCredentials

<table>
<thead>
<tr>
<th>Matriculation Number</th>
<th>School</th>
<th>Name</th>
<th>Birthday</th>
<th>Issued</th>
<th>Revoked</th>
</tr>
</thead>
<tbody>
<tr>
<td>4,000,000,000</td>
<td>ETH</td>
<td>John Doe</td>
<td>1976-07-21</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hotel Booking

USER @ ISSUER
Authenticate with PIN to start issuance of Credentials

Person Identifier * 1000000000

PIN * 14776

Authenticate
## User @ Issuer
### Demo Application

**End User Application @ Issuer**

### Select Credentials to Issue and press 'Start'

- **Firefox with ABC4Trust Extension**: true

<table>
<thead>
<tr>
<th>Select</th>
<th>Credential Type</th>
<th>UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔️</td>
<td>CREDITCARD_AMEX</td>
<td>ca4bf46-b11f-401d-a309-4d5182ef2d72</td>
</tr>
<tr>
<td>✔️</td>
<td>CREDITCARD_VISA_BEST_BANK</td>
<td>3c5c6473-df1f-43b7-b3d4-51b4c8dc99f</td>
</tr>
<tr>
<td>✔️</td>
<td>ID CARD</td>
<td>4fed625f-0437-4dd3-8512-77c2108af539</td>
</tr>
<tr>
<td>✔️</td>
<td>PASSPORT_CH</td>
<td>f9f11bce-0804-48da-b596-81cdec3ede4b0</td>
</tr>
<tr>
<td>✔️</td>
<td>STUDENTCARD</td>
<td>94109e05-1501-4bde-8099-2810f302f18</td>
</tr>
</tbody>
</table>

**Cancel**  **Start**
User @ Issuer
Demo Application

ABC4Trust Client Application

Identity Selection

Properties of credential to be issued
- The credential is issued by http://www.amex.com/abc/isskey/idemix and is of type AMEX Credit Card

Obtain credential

Mode: Issuance. Accepted languages: [en, da, en_US]. SessionID Issuance1407250652357721855.
User @ Issuer
Demo Application
Hotel Booking

USER @ VERIFIER
User @ Verifier
Demo Application

Create Booking

Room Category: NORMAL
Arrival Date: 9 August 2014
Free Mini Bar: ✔
Nights: 3
Single Room: ☐

Start Booking
End User Application @ Verifier

Show Booking

Room Category: NORMAL
Arrival Date: 2014-08-09 00:00:00 CEST
Free Mini Bar: True
Nights: 3

Your creditcard information will be saved - protected by 'Inspection' - and in case of 'No Show' - a fee will be charged

Cancel  Confirm Booking
User @ Verifier
Demo Application

ABC4Trust Client Application

Identity Selection

Policy: Standard Booking

agree to the terms of service and cancellation policy.

Passport or Passport or Passport or Passport or Passport or Passport

View Credit Card or AMEX Credit Card

Information to be disclosed

- Disclosed ownership and validity
  - You own a valid Passport from Swiss Passport.
  - You own a valid Visa Credit Card from VISA Creditcard Credential issued by Best Bank

- Disclosed facts
  - The value of Expiration Date from Visa Kreditkort is after or on 30.08.2014.

- Inspectable attributes
  - Card Number of Visa Credit Card (123400000002) is inspectable by and only by
    Grounds: In case of no free cancellation and no show the credit card number should

Mode: Presentation. Accepted languages: [en, da, en_US]. SessionID Present1407251144453876460.
User @ Verifier
Demo Application

Result of Hotel Booking

Your Booking has been accepted!

Create new Booking
Hotel Booking

VERIFIER
## Booking List

<table>
<thead>
<tr>
<th>Room Category</th>
<th>Arrival Date</th>
<th>Nights</th>
<th>Single Room</th>
<th>Confirmed</th>
<th>Sent To Inspector</th>
<th>Payment Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td>2014-08-09 00:00:00 CEST</td>
<td>3</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>LAKEVIEW</td>
<td>2014-08-16 00:00:00 CEST</td>
<td>4</td>
<td>False</td>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>DISCOUNT</td>
<td>2014-09-05 00:00:00 CEST</td>
<td>1</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>
Verifier Application

Handle Booking
Booking was confirmed by Customer. In case Customer does not show up we can claim our payment from inspector.

Arrival Date: 2014-08-09 00:00:00 CEST
Room Category: NORMAL
Nights: 3
Single Room: False
Free Mini Bar: True
Confirmed: True
Sent To Inspector: False
Payment Cleared By inspector: False

Customer did not show up: False

Send Presentation Token to Inspector: Button
Verifier Application

Handle Booking

PresentationToken was sent: Inspector200

Payment claim has been sent to Inspector - but is not confirmed yet!

- Arrival Date: 2014-08-09 00:00:00 CEST
- Room Category: NORMAL
- Nights: 3
- Single Room: False
- Free Mini Bar: True
- Confirmed: True
- Sent To Inspector: True
- Payment Cleared By Inspector: False

Get Payment Clearing Status From Inspector
Hotel Booking

INSPECTOR
### Inspector Application

#### InspectionRequest List

<table>
<thead>
<tr>
<th>Customer Name</th>
<th>Inspection Token</th>
<th>Inspection Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SweetDreamSuites</td>
<td>99310c8e-3e40-4b81-b3a7-4c50ef496212</td>
<td></td>
</tr>
<tr>
<td>SweetDreamSuites</td>
<td>c62d24e7-d778-4f46-a1dc-c657f8f7acd6</td>
<td></td>
</tr>
</tbody>
</table>

Michael Østergaard, Miracle A/S
Inspector
Demo Application

Show InspectionRequest

Customer Name: SweetDreamSuites
Inspection Token: 99310c8e-3e40-4b81-b3a7-4c50ef496212
Inspection Result

Inspect Presentation Token
Inspector
Demo Application

Show InspectionRequest

Presentation token was inspected: CardNumber = 123400000002

Customer Name: SweetDreamSuites
Inspection Token: 99310c8e-3e40-4b81-b3a7-4c50ef496212
Inspection Result: CardNumber = 123400000002

Back
### Inspector Application

#### InspectionRequest List

- **Presentation token was inspected**: CardNumber = 123400000002

<table>
<thead>
<tr>
<th>Customer Name</th>
<th>Inspection Token</th>
<th>Inspection Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SweetDreamSuites</td>
<td>99310c8e-3e40-4b81-b3a7-4c50ef496212</td>
<td>CardNumber = 123400000002</td>
</tr>
<tr>
<td>SweetDreamSuites</td>
<td>c62d24e7-d778-4f46-a1dc-c657f8f7acd6</td>
<td></td>
</tr>
</tbody>
</table>
Hotel Booking

VERIFIER
Verifier
Demo Application

Verifier Application

Handle Booking

PresentationToken was accepted by Inspector200

Payment has been cleared by Inspector1

Arrival Date: 2014-08-09 00:00:00 CEST
Room Category: NORMAL
Nights: 3
Single Room: False
Free Mini Bar: True
Confirmed: True
Sent To Inspector: True
Payment Cleared By Inspector: True

Back
Verifier Application

Booking List

<table>
<thead>
<tr>
<th>Room Category</th>
<th>Arrival Date</th>
<th>Nights</th>
<th>Single Room</th>
<th>Confirmed</th>
<th>Sent To Inspector</th>
<th>Payment Cleared</th>
</tr>
</thead>
<tbody>
<tr>
<td>NORMAL</td>
<td>2014-08-09 00:00:00 CEST</td>
<td>3</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>LAKEVIEW</td>
<td>2014-08-16 00:00:00 CEST</td>
<td>4</td>
<td>False</td>
<td>True</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>DISCOUNT</td>
<td>2014-09-05 00:00:00 CEST</td>
<td>1</td>
<td>True</td>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
</tbody>
</table>
Demo

AGE VERIFICATION
Age Verification

USER @ VERIFIER
End User Application @ Verifier

Verify Birthday

Enter date. Date will be compared to Birthday attributes within your credentials.

Birthday * 5 ▼ August ▼ 1986 ▼

Verify
User @ Verifier
Demo Application

End User Application @ Verifier

Show Birthday

Firefox with ABC4Trust Extension: true

The specified date will be compared to Birthday attributes within your credentials.

Birthday 1986-08-05 00:00:00 CEST

Cancel  Start
Result of Birthday Presentation

We have verified your PresentationToken with Policy urn:eu:abc4trust:demo:comparebirthday:before:session.

Your birthday is Before 1986-08-05 00:00:00 CEST

Run new Birthday Verification
More Information

• My contact information
  ▪ Michael Østergaard
  ▪ mop@miracle.dk

• ABC4Trust website
  ▪ www.abc4trust.eu