



ABC4Trust Reference Implementation

Michael Østergaard, Miracle A/S

Dissemination Event

2014-09-29

Athens



A research project funded by the European Commission's 7th Framework Programme.



Agenda



- Introduction
- Overview
 - Components
 - Interfaces
 - Data Flow
- Demo application

At a Glance



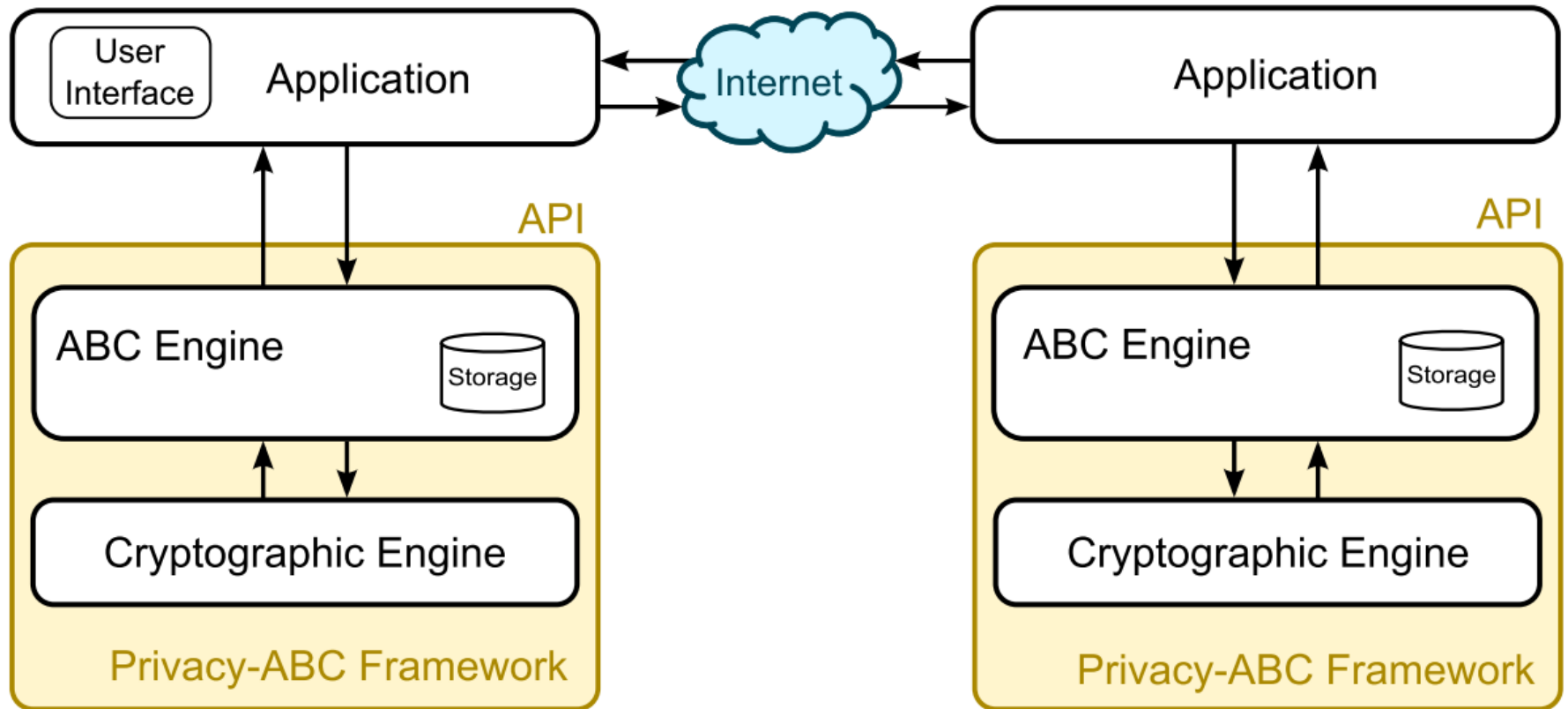
- Implements the ABC4Trust architecture
- Written in Java
 - Most source code is available on GitHub
 - Uses maven as build tool
- Features
 - Designed for a typical desktop/server setup
 - Supports hardware and software smart cards
 - User interaction via a User Service and Browser Plugin

Architecture Overview



User Deployment:

*Verifier / Issuer / Inspector/
Revocation Authority Deployment:*



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

- 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
 - Credential Selector
- And indirectly also
 - ABCE on both Issuer/Verifier and User side

1. The application notifies the Browser Plugin via JavaScript about the action to take, policies and endpoints.
2. The Browser Plugin retrieves the resources and passes them to the User Service.
3. The User Service computes the possible ways to satisfy the policy and returns the list to the Browser Plugin.
4. The Browser Plugin passes this information to the Credential Selector which presents the choices to the user.

Data Flow (cont.)



5. Once the user has made a selection, the choice is returned to the Browser Plugin.
6. The Browser Plugin passes the choice to the User Service.
7. The User Service computes an ABC protocol message (a presentation token or issuance message) which is sent to the Browser Plugin.
8. 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 inspector parameters*
 4. *Setup revocation authority parameters*
 5. Setup issuer 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

Issuer Demo Application



InspectionRequest ... CredentialIssuance ... Booking List Create Booking Compare Birthday ...

uer-application/person/create

Google

ABC4 TRUST Issuer Application

Home Person List

Create Person

Create

Person Id (autogenerated)

Firstname *

Lastname *

Gender *

Birthday *

PIN (autogenerated)

Issuer

Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Compare Birthday ... x

issuer-application/person/index

Home New Person

Person List

Person Id	Firstname	Lastname	Gender	Birthday	PIN
1.000.000.000	John	Doe	M	1976-07-21	14776
1.000.000.001	Alice	Von Nextdoor	F	1981-02-03	53281

Issuer

Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Compare Birthday ... x

tr-application/person/show/1

Google

Issuer Application

[Home](#) [Person List](#)

[Edit Person](#)

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

CreditCardCredentials [Create](#)

IdCardCredentials [Create](#)

PassportCredential [Create](#)

StudentCardCredentials [Create](#)

Issuer Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Compare Birthday ... x

application/person/createCreditCardCredential/1

ABC4 TRUST Issuer Application

Home Person List

Adding Credential

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

New CreditCardCredential Create Skip

Number (autogenerated)

Issuer * AMEX

Holder * John Doe

Expire * 5 August 2016

Issuer

Demo Application



InspectionRequest ... CredentialIssuance ... Booking List Create Booking Compare Birthday ...

ier-application/person/show/1

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

CreditCardCredentials Create

Number	Issuer	Holder	Expire	Issued	Revoked
123.400.000.001	AMEX	John Doe	2016-08-05	<input type="checkbox"/>	<input type="checkbox"/>
123.400.000.002	VISA_BEST_BANK	John Doe	2016-08-05	<input type="checkbox"/>	<input type="checkbox"/>

IdCardCredentials Create

Person Identifier	Firstname	Lastname	Birthday	Issued	Revoked
1.000.000.000	John	Doe	1976-07-21	<input type="checkbox"/>	<input type="checkbox"/>

PassportCredential Create

Number	Country	Firstname	Lastname	Birthday	Expire	Gender	Issued	Revoked
1.000.000.000	CH	John	Doe	1976-07-21	2024-08-05	M	<input type="checkbox"/>	<input type="checkbox"/>

StudentCardCredentials Create

Matriculation Number	School	Name	Birthday	Issued	Revoked
4.000.000.000	ETH	John Doe	1976-07-21	<input type="checkbox"/>	<input type="checkbox"/>

Issuer Demo Application



The screenshot shows a web browser window with several tabs: 'InspectionRequest ...', 'CredentialIssuance ...', 'Booking List', 'Create Booking', and 'Compare Birthday ...'. The address bar shows the URL 'r-application/creditCardCredential/show/3' and the search engine is set to Google.

The application header is teal and contains the ABC4 TRUST logo and the text 'Issuer Application'. Below the header is a navigation bar with links for 'Home', 'Person List', and 'Show Person'. The main content area is titled 'Show CreditCardCredential' and displays the following information:

Number	123,400,000,001
Holder	John Doe
Expire	2016-08-05 00:00:00 CEST
Issuer	AMEX
Issued	False
Revoked	False
Revocation Handle	

At the bottom of the content area is a 'Back' button.

Hotel Booking

USER @ ISSUER

User @ Issuer


Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Compare Birthday ... x

r-application/credentialIssuance/index

Google



End User Application @ Issuer

Home

Authenticate with PIN to start Issuance of Credentials

Person Identifier *

PIN *

User @ Issuer

Demo Application



InspectionRequest ... x CredentialIssuance List x Booking List x Show Booking x Show Birthday x

r-application/credentialIssuance/authenticate

ABC4 TRUST *End User Application @ Issuer*

Home

Select Credentials to Issue and press 'Start'

Select	Credential Type	UUID
<input checked="" type="checkbox"/>	CREDITCARD_AEMX	ca4bdf46-b11f-401d-a309-4d6182ef2d72
<input checked="" type="checkbox"/>	CREDITCARD_VISA_BEST_BANK	3c5c8473-df1f-43b7-b3d4-51b4c8cdc99f
<input checked="" type="checkbox"/>	IDCARD	4fed625f-9437-4dd3-8512-77c2108af539
<input checked="" type="checkbox"/>	PASSPORT_CH	f9fd1fbc-0804-48da-b596-81cdc3ede4b0
<input checked="" type="checkbox"/>	STUDENTCARD	94109e05-1501-4bde-8099-2810fd302f18

Cancel

User @ Issuer

Demo Application



The screenshot shows a web browser window with several tabs: 'InspectionRequest ...', 'CredentialIssuance List', 'Booking List', 'Show Booking', and 'Show Birthday'. The address bar shows the URL '...er-application/credentialIssuance/authenticate'. The page header includes the 'ABC4 TRUST' logo and the text 'End User Application @ Issuer'. Below the header is a navigation bar with a 'Home' link. The main content area is titled 'Select Credentials to Issue and press 'Start''. A status bar indicates 'Running issuance of CREDITCARD_AMEX - UUID : ca4bdf46-b11f-401d-a309-4d6182ef2d72 : 1/5'. A table lists credential types with checkboxes in the 'Select' column and UUIDs in the right column. An 'Authenticate Password' dialog box is overlaid on the table, prompting the user to 'Enter current PIN:' with a text input field and 'OK' and 'Annuler' buttons. At the bottom of the page are 'Cancel' and 'Start' buttons.

Select	Credential Type	UUID
<input checked="" type="checkbox"/>	CREDITCARD_AMEX	...4d6182ef2d72
<input checked="" type="checkbox"/>	CREDITCARD_VISA	...51b4c8cdc99f
<input checked="" type="checkbox"/>	IDCARD	...L-77c2108af539
<input checked="" type="checkbox"/>	PASSPORT_CH	f9fd1fbc-0804-48da-b596-81cdc3ede4b0
<input checked="" type="checkbox"/>	STUDENTCARD	94109e05-1501-4bde-8099-2810fd302f18

User @ Issuer

Demo Application



A screenshot of a web browser window showing the ABC4Trust Client Application. The browser tabs include 'Show CreditCardCr...', 'InspectionRequest ...', 'CredentialIssuance ...', 'Booking List', 'Create Booking', and 'Compare Birthday ...'. The application title is 'ABC4Trust Client Application'. A tab labeled 'Identity Selection' is active. On the left, a box contains the URL 'http://www.amex.com/creditcard/issuance/policy' and the text 'This policy has no description.' A blue arrow points from this box to a green box on the right. The green box is titled 'Properties of credential to be issued' and contains a bullet point: '• The credential is issued by http://www.amex.com/abc/isskey/idemix and is of type AMEX Credit Car'. Below the green box is a button labeled 'Obtain credential'. At the bottom of the application window, the text reads: 'Mode: Issuance. Accepted languages: [en, da, en_US]. SessionID Issuance140725062357721855.'

User @ Issuer

Demo Application



The screenshot shows a web browser window with several tabs open. The active tab is titled "CredentialIssuance ...". The browser address bar shows the URL "http://localhost:9093 - ABC4Trust User Interface - Mozilla Firefox". The application interface is titled "ABC4Trust Client Application" and features a "Credential Repository" section with a search bar and a list of credential types: AMEX Credit Card, Visa Credit Card, ID Card, Passport (highlighted), and Student ID. Below this is a "Credential Attributes" section displaying the following information:

Issuer:	Swiss Passport (http://admin.ch/passport/issuancekey_v1.0/idemix)
Revoked by Issuer:	The credential is not revocable.
Name:	John
Lastname:	Doe
Birthday:	21-07-1976
Passport Number:	1000000000
Expiration Date:	05-08-2024
Issued By:	Proper Authority in CH

Hotel Booking

USER @ VERIFIER

User @ Verifier

Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Show Birthday x

ier-application/booking/index Google

ABC⁴ TRUST *End User Application @ Verifier*

Home

Create Booking

Room Category * NORMAL

Arrival Date * 9 August 2014

Free Mini Bar

Nights * 3

Single Room

Start Booking

User @ Verifier

Demo Application



The screenshot shows a web browser window with several tabs: 'InspectionRequest ...', 'CredentialIssuance ...', 'Booking List', 'Show Booking', and 'Show Birthday'. The address bar shows the URL 'er-application/booking/confirmBooking' and a search engine 'Google'. The page content includes the ABC4 TRUST logo and the title 'End User Application @ Verifier'. A navigation bar contains a 'Home' link. The main content area is titled 'Show Booking' and displays booking details: 'Room Category NORMAL', 'Arrival Date 2014-08-09 00:00:00 CEST', 'Free Mini Bar True', and 'Nights 3'. A warning message states: 'Your creditcard information will be saved - protected by 'Inspection' - and in case of 'No Show' - a fee will be charged'. At the bottom, there are 'Cancel' and 'Confirm Booking' buttons.

User @ Verifier

Demo Application



The screenshot shows a web browser window displaying the ABC4Trust Client Application. The browser tabs include 'CreditCardCr...', 'InspectionRequest...', 'CredentialIssuance...', 'Booking List', 'Show Booking', and 'Show Birthday'. The address bar shows 'http://localhost:9093 - ABC4Trust User Interface - Mozilla Firefox'. The application header is 'ABC4Trust Client Application'.

The main content area is titled 'Identity Selection' and contains two sections:

- Policy: Standard Booking**: A text box containing 'agree to the terms of service and cancellation policy.' Below it is a radio button and the text 'Passport or Passport or Passport or Passport or Passport or Passport'.
- Visa Credit Card or AMEX Credit Card**: A radio button and two images: a Visa credit card and an American Express logo.

A large blue arrow points from the 'Passport or Passport...' section to a blue box titled 'Information to be disclosed'. This box contains three sections:

- 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 sho

A 'Disclose' button is located at the bottom right of the 'Information to be disclosed' box.

At the bottom of the application window, the text reads: 'Mode: Presentation. Accepted languages: [en, da, en_US]. SessionID Present140725114445387460.'

User @ Verifier

Demo Application

A screenshot of a web browser window. The browser has several tabs open: 'InspectionRequest ...', 'CredentialIssuance ...', 'Booking List', 'Show Booking', and 'Show Birthday'. The address bar shows a URL ending in '&stat' and a search bar with 'Google'. The page content is on a green background with the ABC4 TRUST logo and the text 'End User Application @ Verifier'. Below this is a navigation bar with a 'Home' link. The main content area is titled 'Result of Hotel Booking' and contains the message 'Your Booking has been accepted!'. At the bottom of the content area is a 'Create new Booking' link.

InspectionRequest ... x CredentialIssuance ... x Booking List x Show Booking x Show Birthday x

er-application/booking/showPresentationStatus?sessionToken=af218820-ffb1-4a0f-9522-345a1d33bb34&stat Google

ABC4 TRUST *End User Application @ Verifier*

Home

Result of Hotel Booking

Your Booking has been accepted!

Create new Booking

Hotel Booking

VERIFIER

Verifier

Demo Application



InspectionRequest ... x CredentialIssuance List x Booking List x Show Booking x Show Birthday x

ier-application/hotelAdmin/index

Google

ABC4 TRUST *Verifier Application*

Home

Booking List

Room Category	Arrival Date	Nights	Single Room	Confirmed	Sent To Inspector	Payment Cleared
NORMAL	2014-08-09 00:00:00 CEST	3	False	True	False	False
LAKEVIEW	2014-08-16 00:00:00 CEST	4	False	True	False	False
DISCOUNT	2014-09-05 00:00:00 CEST	1	True	True	False	False

Verifier

Demo Application



The screenshot shows a web browser window with several tabs: 'InspectionRequest ...', 'CredentialIssuance List', 'Show Booking', 'Show Booking', and 'Show Birthday'. The address bar shows 'er-application/hotelAdmin/show/4'. The page header features the ABC4 TRUST logo and the text 'Verifier Application'. Below the header is a navigation bar with 'Home' and 'Booking List'. The main content area is titled 'Handle Booking' and contains the text: 'Booking was confirmed by Customer. In case Customer does not show up we can claim our payment from Inspector.' Below this is a list of booking details: 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), and Payment Cleared By Inspector (False). At the bottom, there is a checkbox labeled 'Customer did not show up.' which is checked, and a button labeled 'Send PresentationToken to Inspector'.

er-application/hotelAdmin/show/4

ABC4 TRUST Verifier Application

Home Booking List

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.

Send PresentationToken to Inspector

Verifier

Demo Application



er-application/hotelAdmin/sendPresentationTokenToInspector/4

ABC4 TRUST *Verifier Application*

Home Booking List

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 Demo Application



InspectionRequest ... x CredentialIssuance List x Show Booking x Show Booking x Show Birthday x

er-application/inspectionRequest/index

Google



Inspector Application

[Home](#)

InspectionRequest List

Customer Name	Inspection Token	Inspection Result
SweetDreamSuites	99310c8e-3e40-4b81-b3a7-4c50ef496212	
SweetDreamSuites	c62d24e7-d778-4f46-a1dc-c657f8f7acd6	


Inspector Demo Application



Browser tabs: Show InspectionRe... x CredentialIssuance List x Show Booking x Show Booking x Show Birthday x

Address bar: r-application/inspectionRequest/showInspectionRequest/3

Search: Google



Inspector Application

Home | InspectionRequest List

Show InspectionRequest

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


Inspector Demo Application



Browser tabs: Show InspectionRe... x CredentialIssuance List x Show Booking x Show Booking x Show Birthday x

Address bar: er-application/inspectionRequest/inspectPresentationToken/3

Search: Google



Inspector Application

Home | InspectionRequest List

Show InspectionRequest

Information: Presentation token was Inspected : CardNumber = 123400000002

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

Back

Inspector Demo Application



InspectionRequest ... x CredentialIssuance List x Show Booking x Show Booking x Show Birthday x

...-application/inspectionRequest/index

Google

Inspector Application

Home

InspectionRequest List

Presentation token was Inspected : CardNumber = 123400000002

Customer Name	Inspection Token	Inspection Result
SweetDreamSuites	99310c8e-3e40-4b81-b3a7-4c50ef496212	CardNumber = 123400000002
SweetDreamSuites	c62d24e7-d778-4f46-a1dc-c657f8f7acd6	

Hotel Booking

VERIFIER

Verifier

Demo Application



The screenshot shows a web browser window with several tabs: 'InspectionRequest ...', 'CredentialIssuance List', 'Show Booking', 'Show Booking', and 'Show Birthday'. The address bar shows the URL 'er-application/hotelAdmin/getPaymentClearingStatusFromInspector/4'. The page header features the ABC4 TRUST logo and the text 'Verifier Application'. Below the header is a navigation bar with 'Home' and 'Booking List'. The main content area is titled 'Handle Booking' and contains a message box: 'PresentationToken was accepted by Inspector200'. Below this, a confirmation message reads: 'Payment has been cleared by Inspector!'. A list of booking details follows:

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

At the bottom of the content area is a 'Back' button.

Verifier

Demo Application



InspectionRequest ... x CredentialIssuance List x Booking List x Show Booking x Show Birthday x

er-application/hotelAdmin/index

Google

ABC⁴ TRUST *Verifier Application*

Home

Booking List

Room Category	Arrival Date	Nights	Single Room	Confirmed	Sent To Inspector	Payment Cleared
NORMAL	2014-08-09 00:00:00 CEST	3	False	True	True	True
LAKEVIEW	2014-08-16 00:00:00 CEST	4	False	True	True	False
DISCOUNT	2014-09-05 00:00:00 CEST	1	True	True	False	False

Demo

AGE VERIFICATION

Age Verification

USER @ VERIFIER

User @ Verifier


Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Compare Birthday ... x

er-application/birthday/index

Google



End User Application @ Verifier

[Home](#)

Verify Birthday

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

Birthday *

User @ Verifier


Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Show Birthday x

ier-application/birthday/verifyBirthday_abc4trustPlugin

Google



End User Application @ Verifier

Home

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

User @ Verifier

Demo Application



The screenshot shows a web browser window with the URL `http://localhost:9093 - ABC4Trust User Interface - Mozilla Firefox`. The application title is "ABC4Trust Client Application".

The main content area is titled "Identity Selection" and contains three identical sections. Each section has a header "Passport or Passport or Passport or Passport or Passport or Passport or ID Card or Student ID" and three image thumbnails: a blue student ID, a red passport cover, and a passport photo. Below each section is a date filter: "Birthday is Before date", "Birthday is Before or Equals date", and "Birthday is Before or Equals date".

A blue arrow points from the second section to a blue box titled "Information to be disclosed". This box contains two sections:

- Disclosed ownership and validity**
 - You own a valid Passport from Swiss Passport.
- Disclosed facts**
 - The value of Birthday from Passport is before 05.08.1986.

At the bottom of the disclosure box is a "Disclose" button.

At the bottom of the application window, the text reads: "Mode: Presentation. Accepted languages: [en, da, en_US]. SessionID Present140725103610720993."


User @ Verifier

Demo Application



InspectionRequest ... x CredentialIssuance ... x Booking List x Create Booking x Show Birthday x

er-application/birthday/showPresentationStatus?sessionToken=ce43597c-ca13-47dc-8cb3-6947644cfee3&sta Google



End User Application @ Verifier

Home

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