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.

SEVENTH FRAMEWORK PROGRAMME

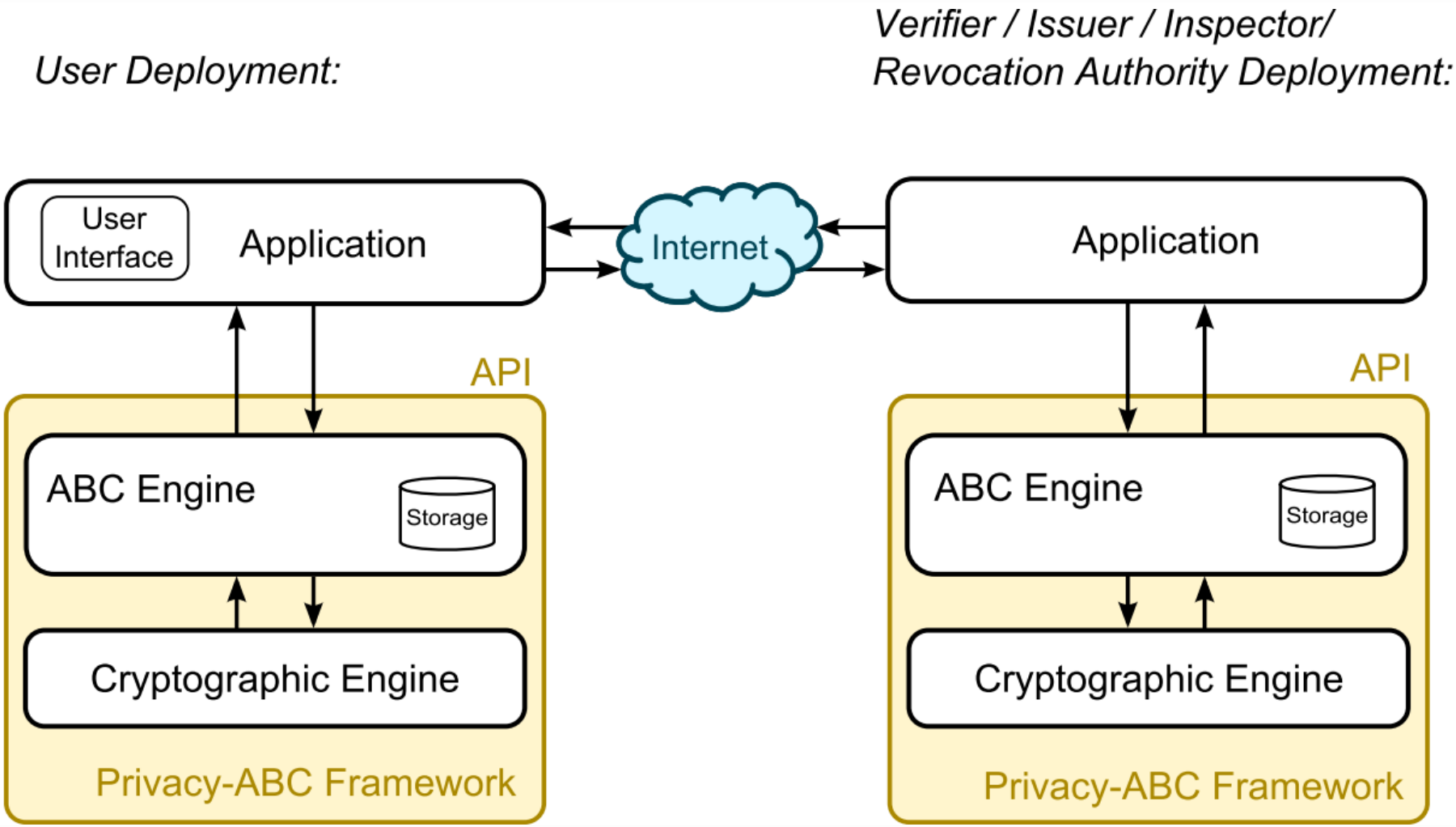
Agenda

- 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



Central Components

- core-abce
  - abc4trust-xml
    - Schema definitions for presentation policies, crendential 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

Data Flow

- 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

Data Flow

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 satisty 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

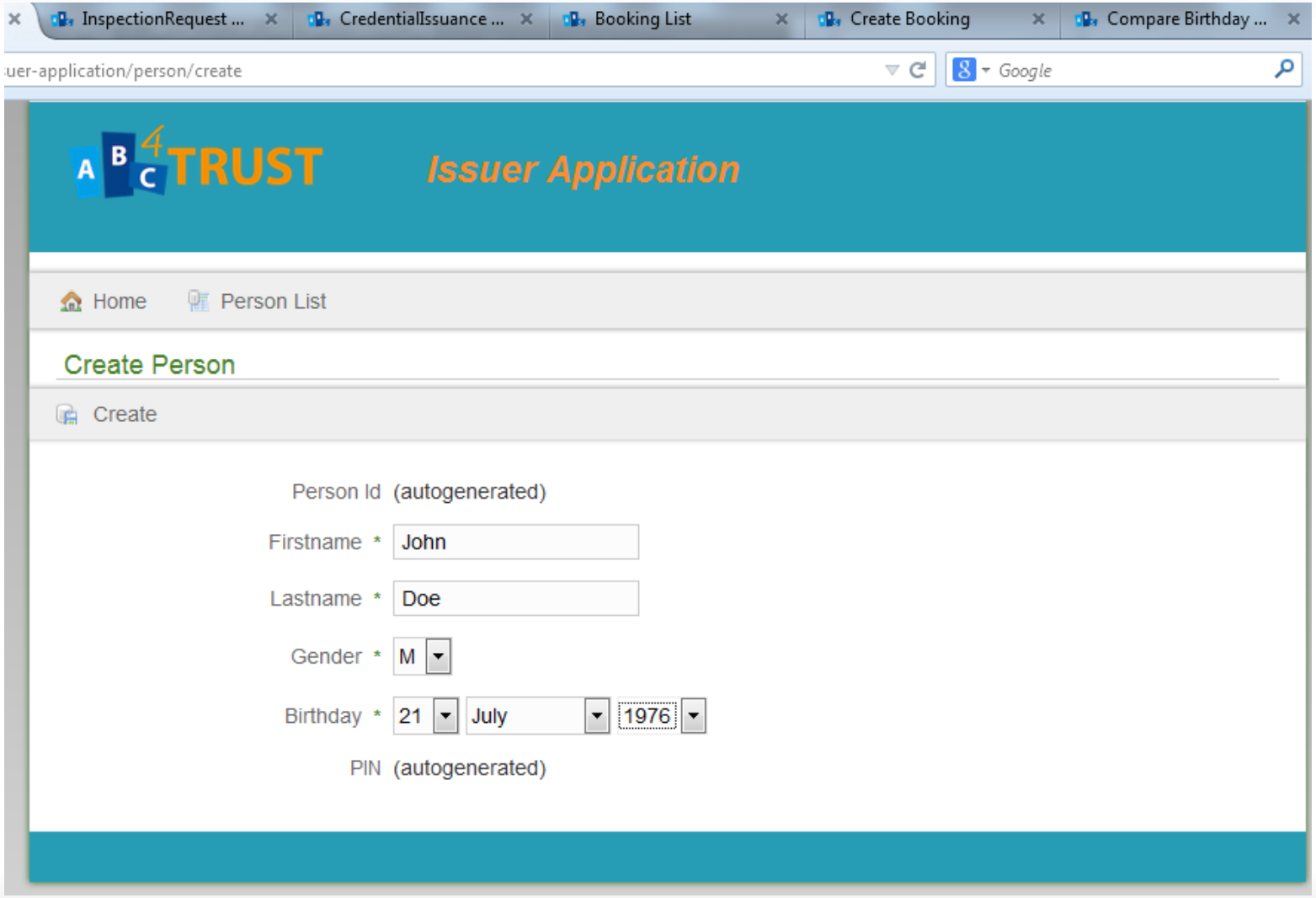
HOTEL BOOKING

Hotel Booking

ISSUER

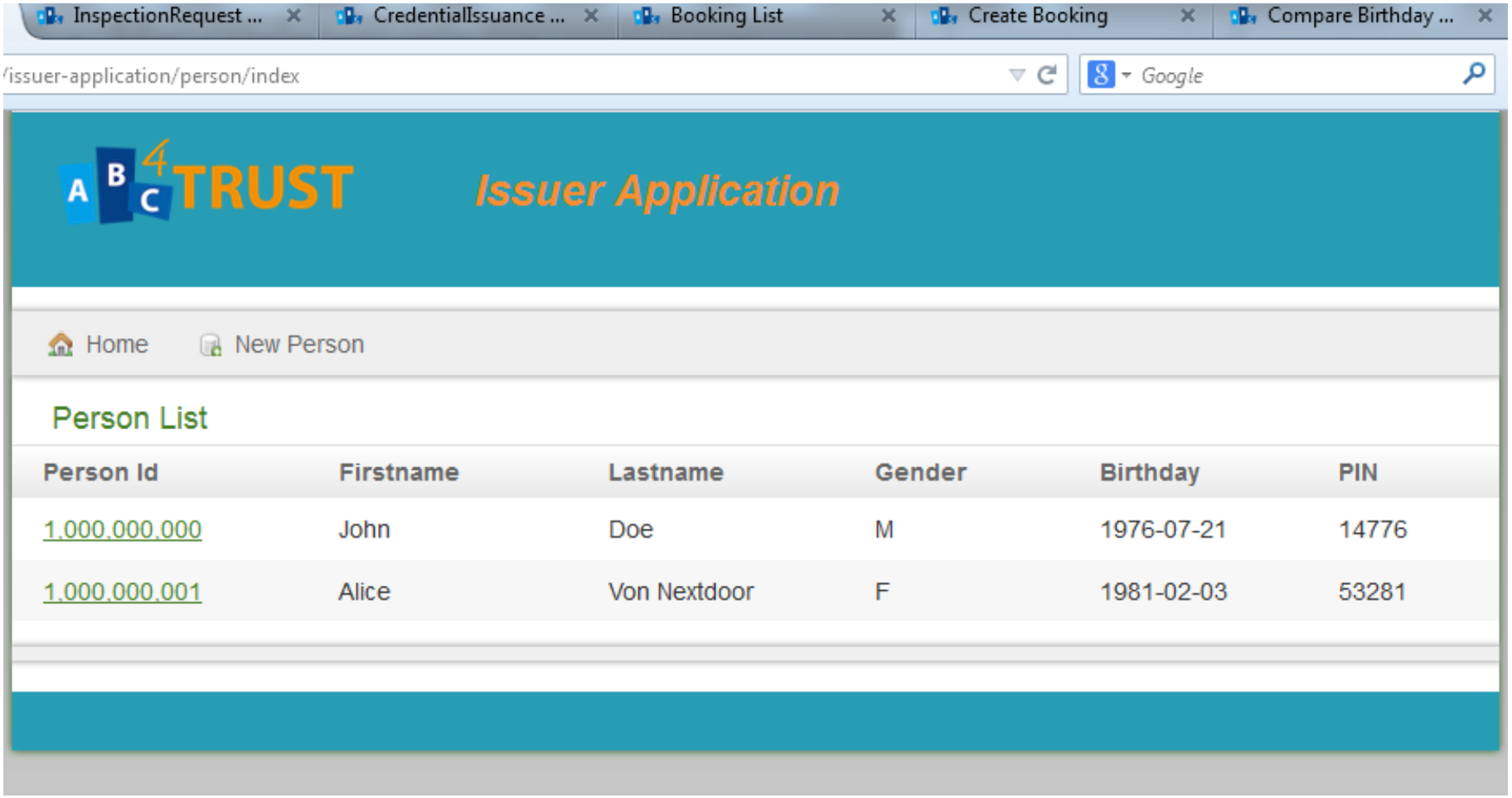
Issuer

Demo Application



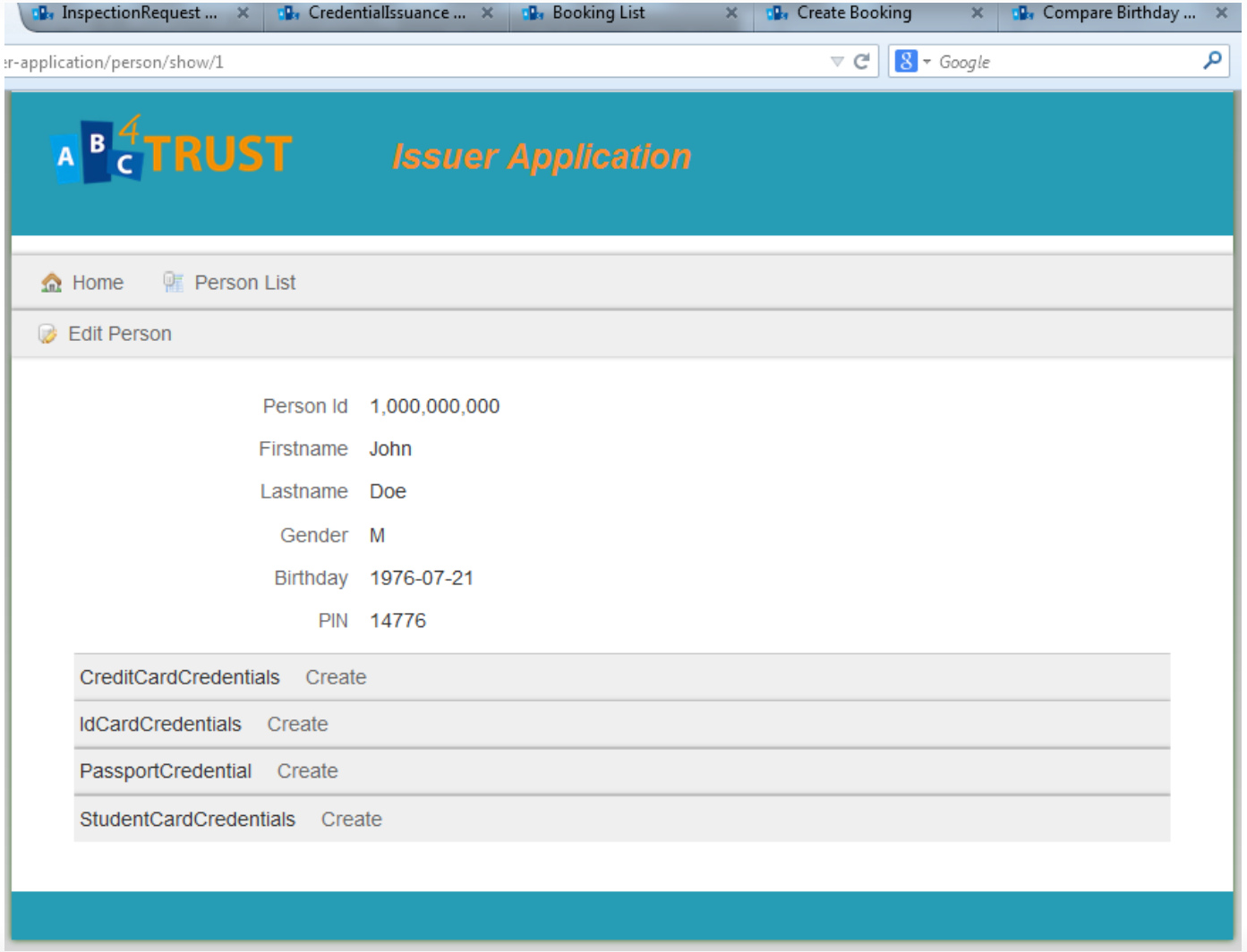
Issuer

Demo Application



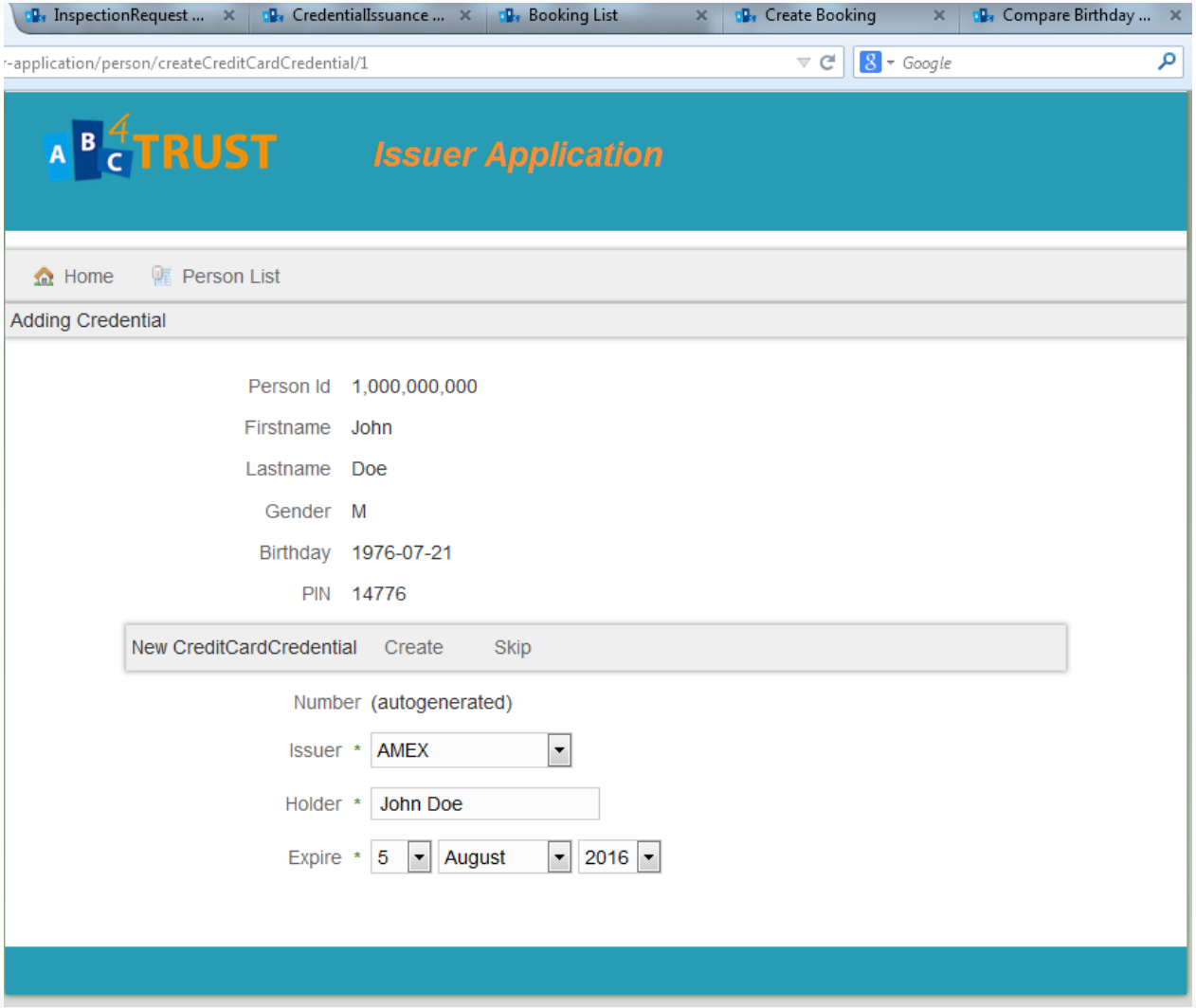
Issuer

Demo Application



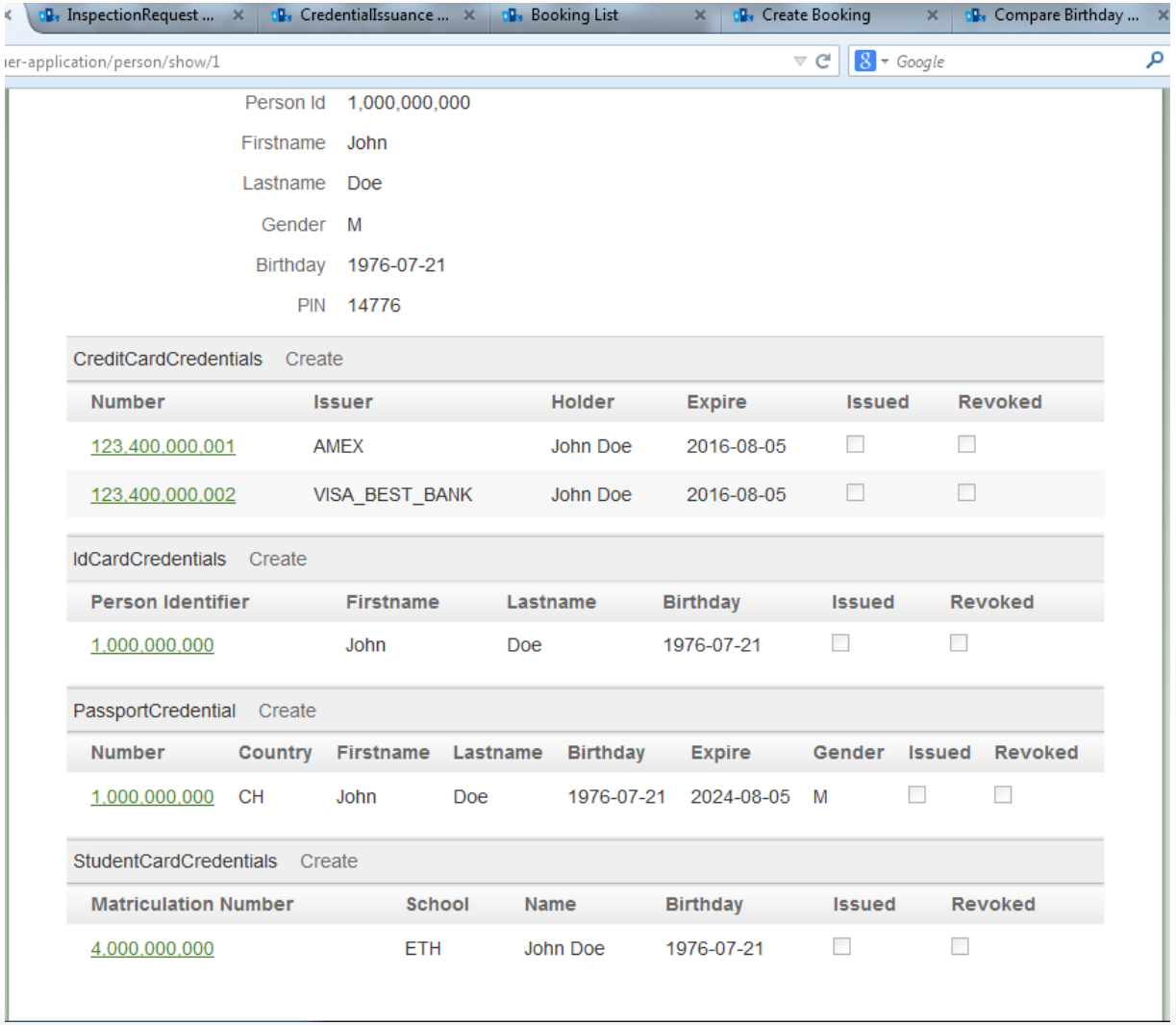
Issuer

Demo Application

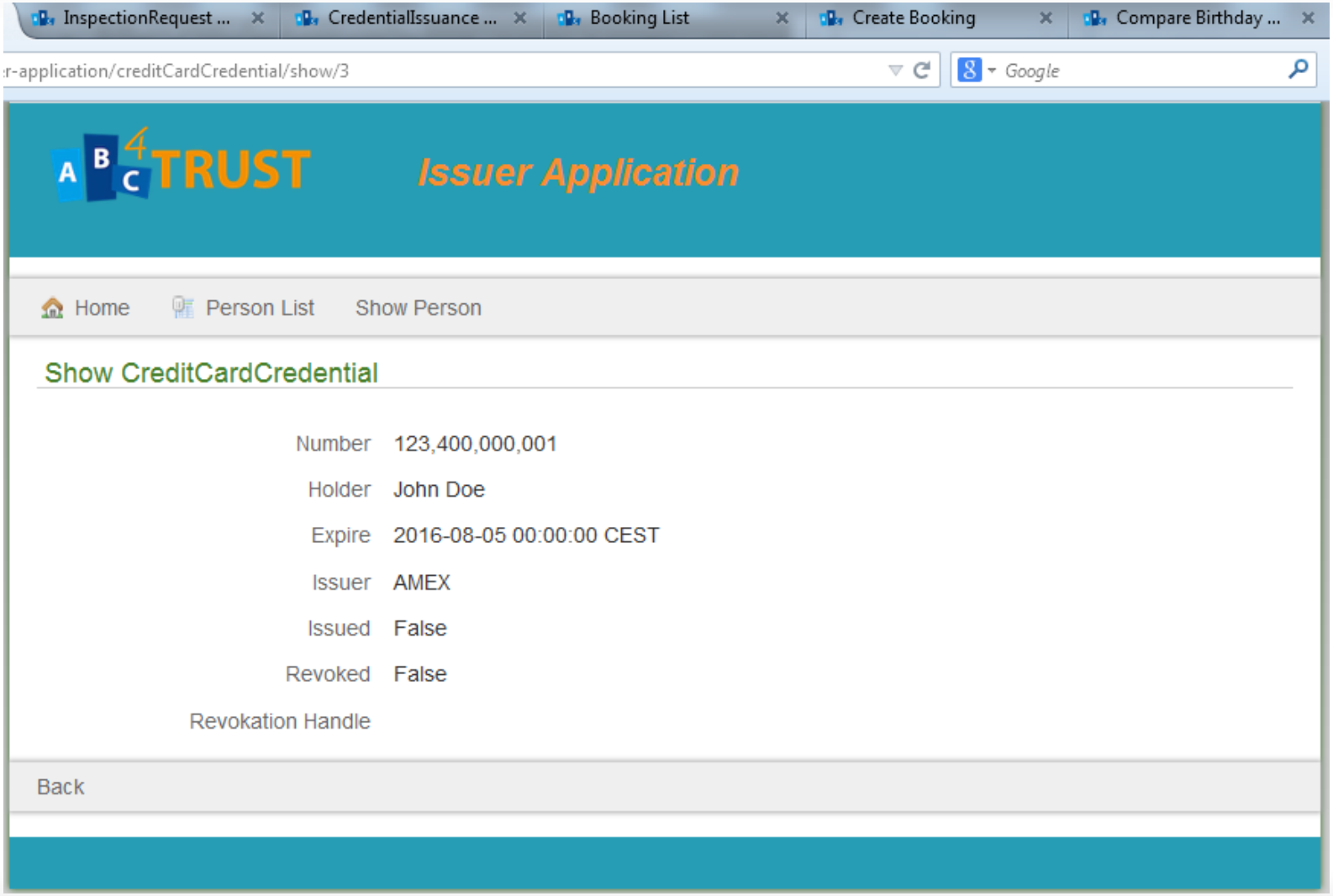


Issuer

Demo Application



Issuer
Demo Application

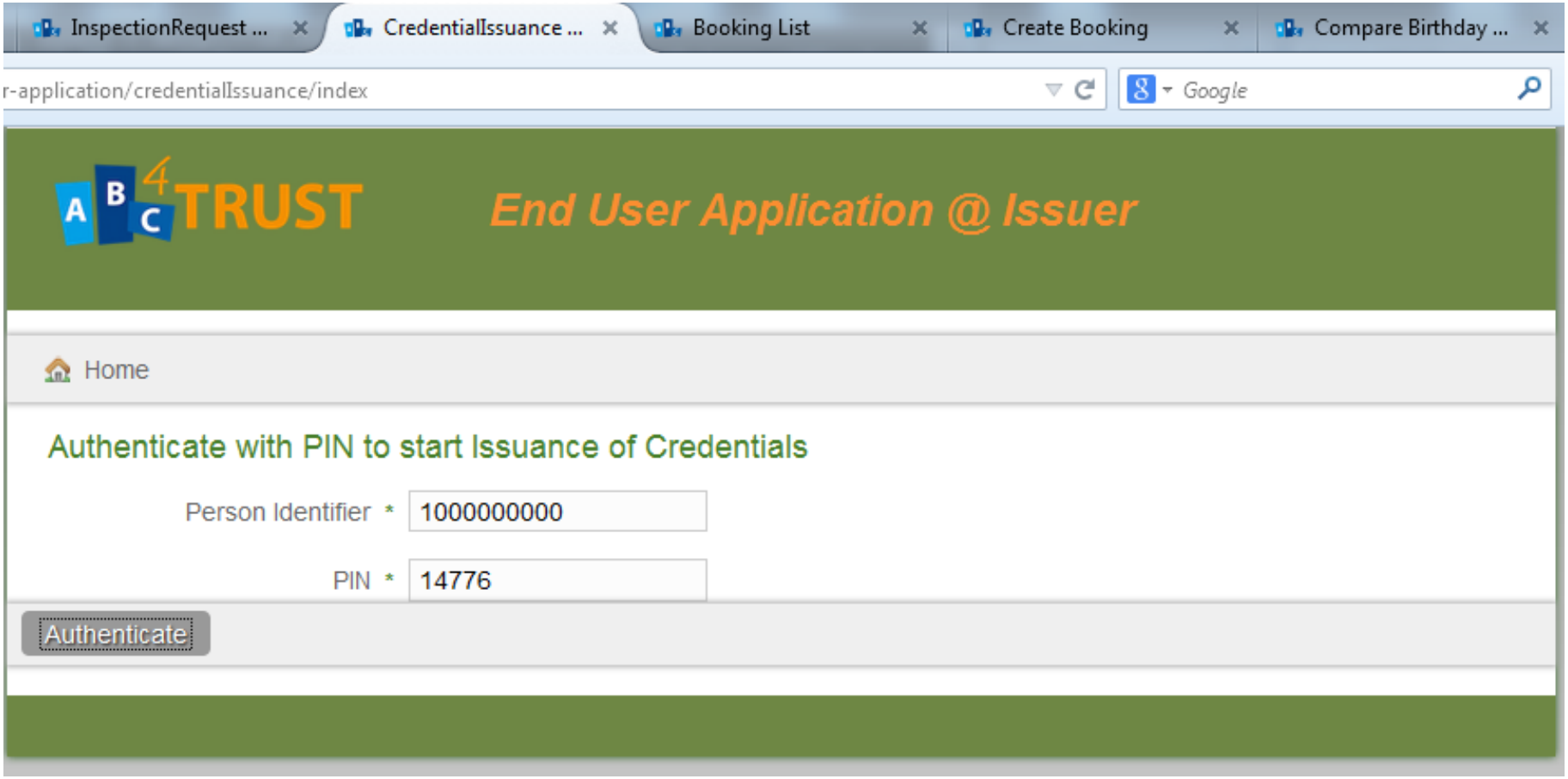


Hotel Booking

USER @ ISSUER

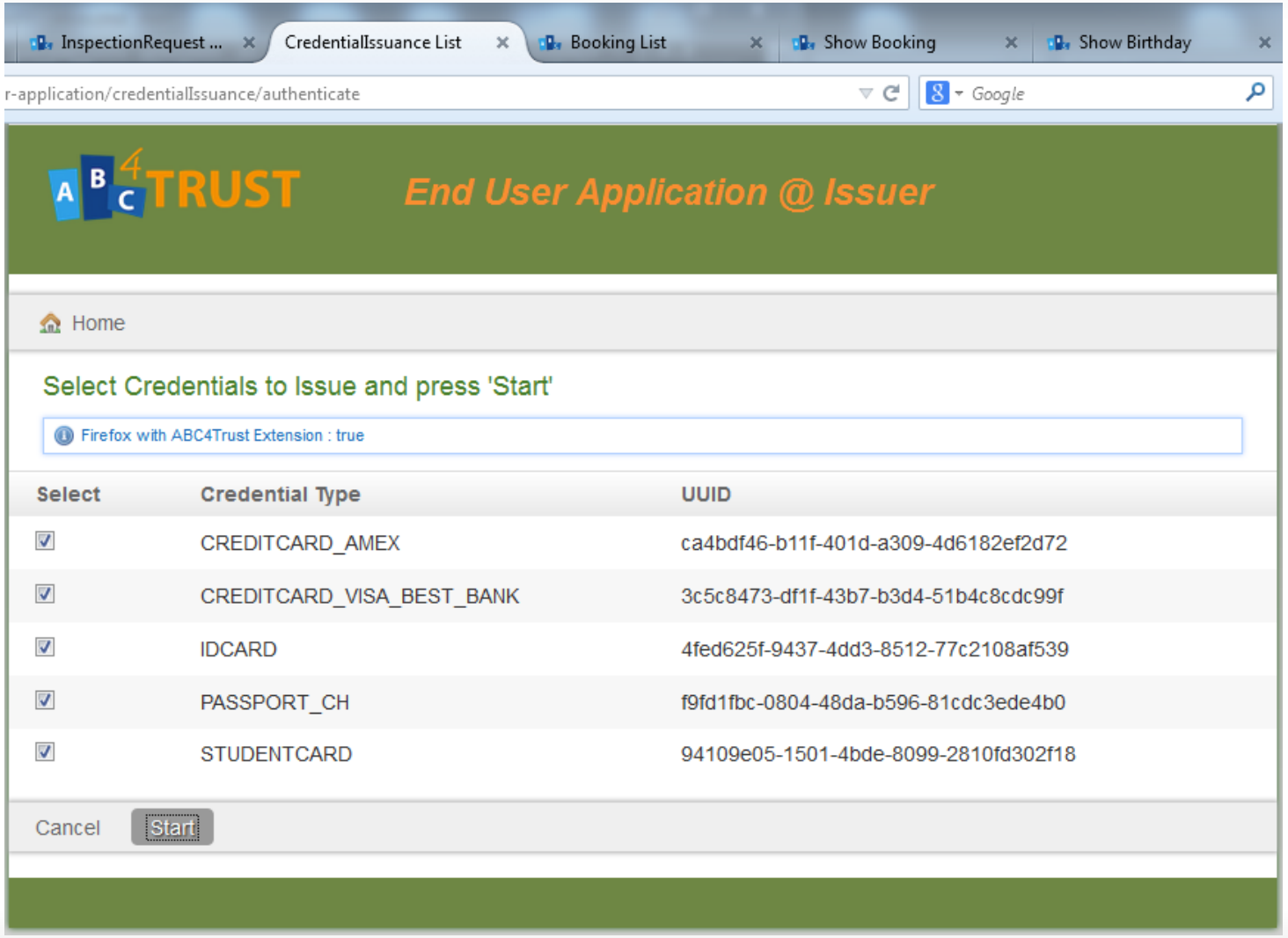
User @ Issuer

Demo Application



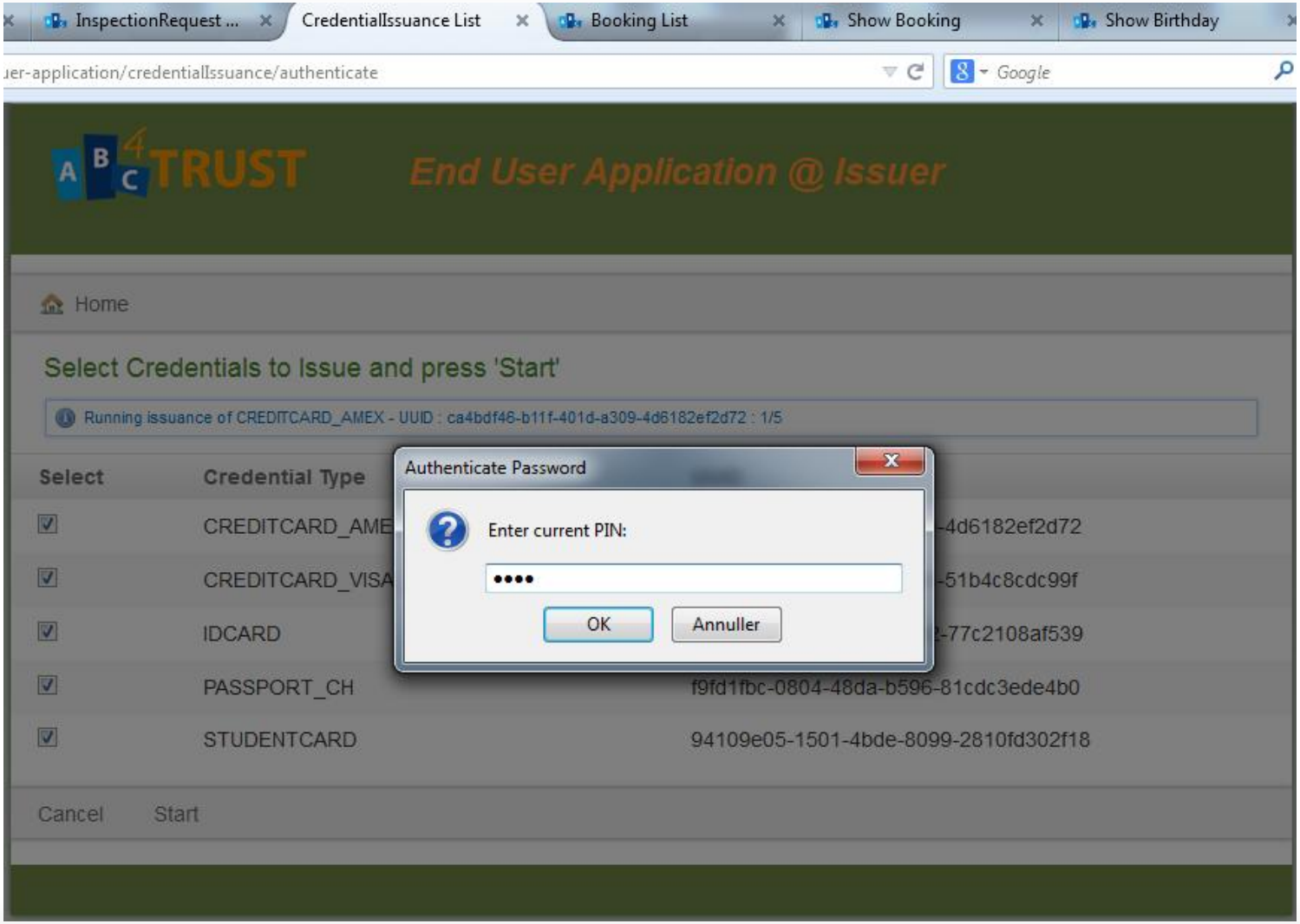
User @ Issuer

Demo Application



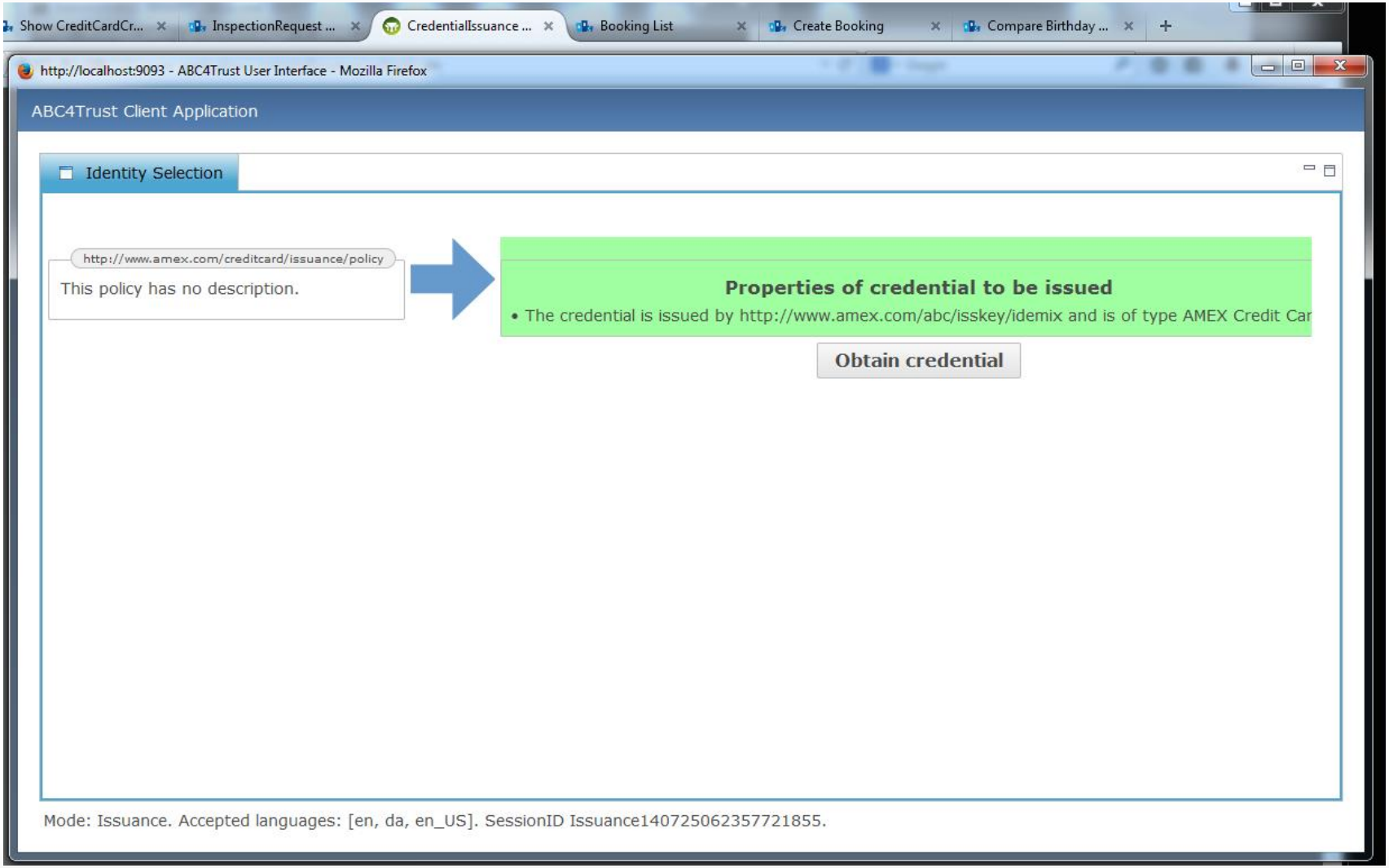
User @ Issuer

Demo Application



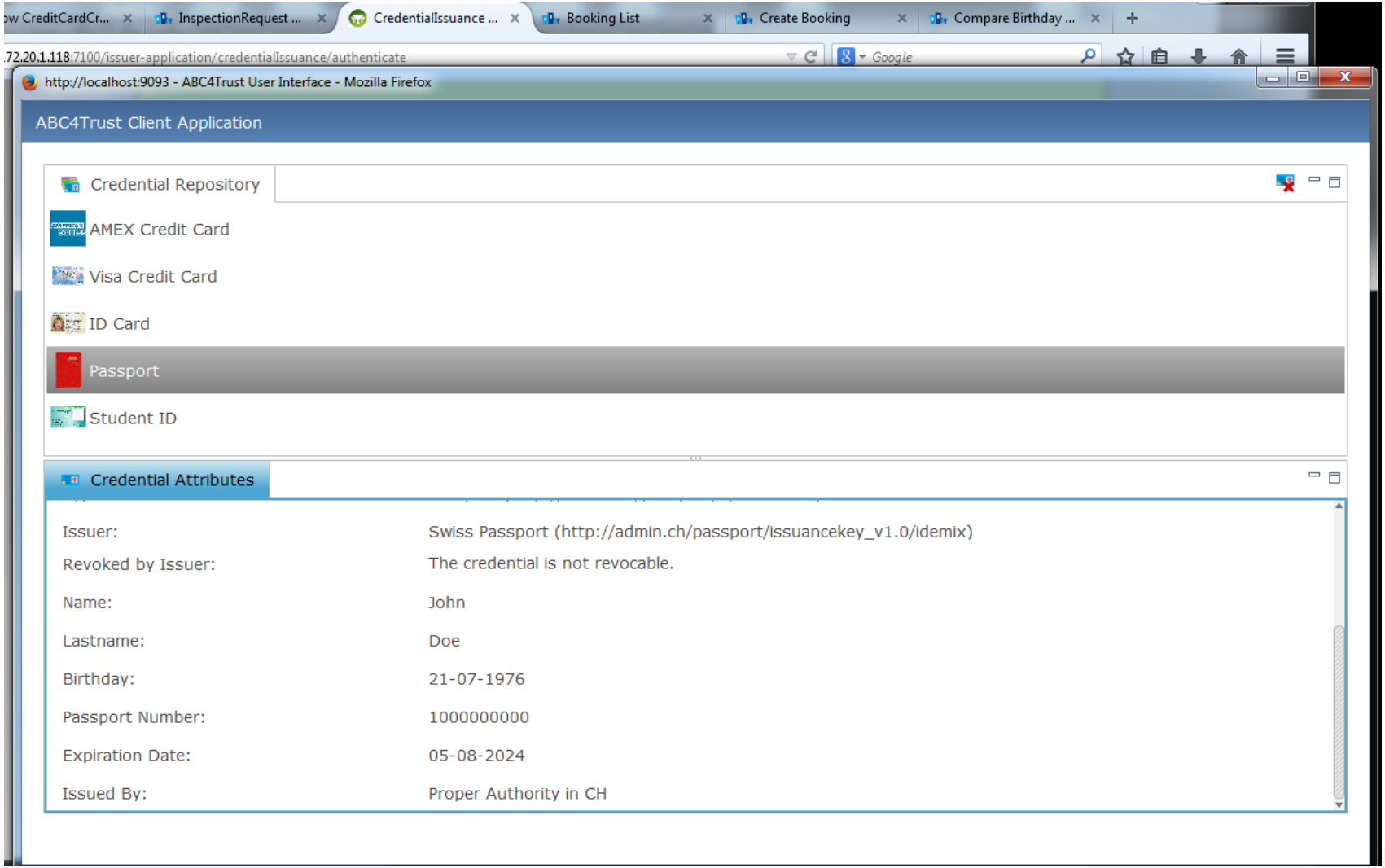
User @ Issuer

Demo Application



User @ Issuer

Demo Application

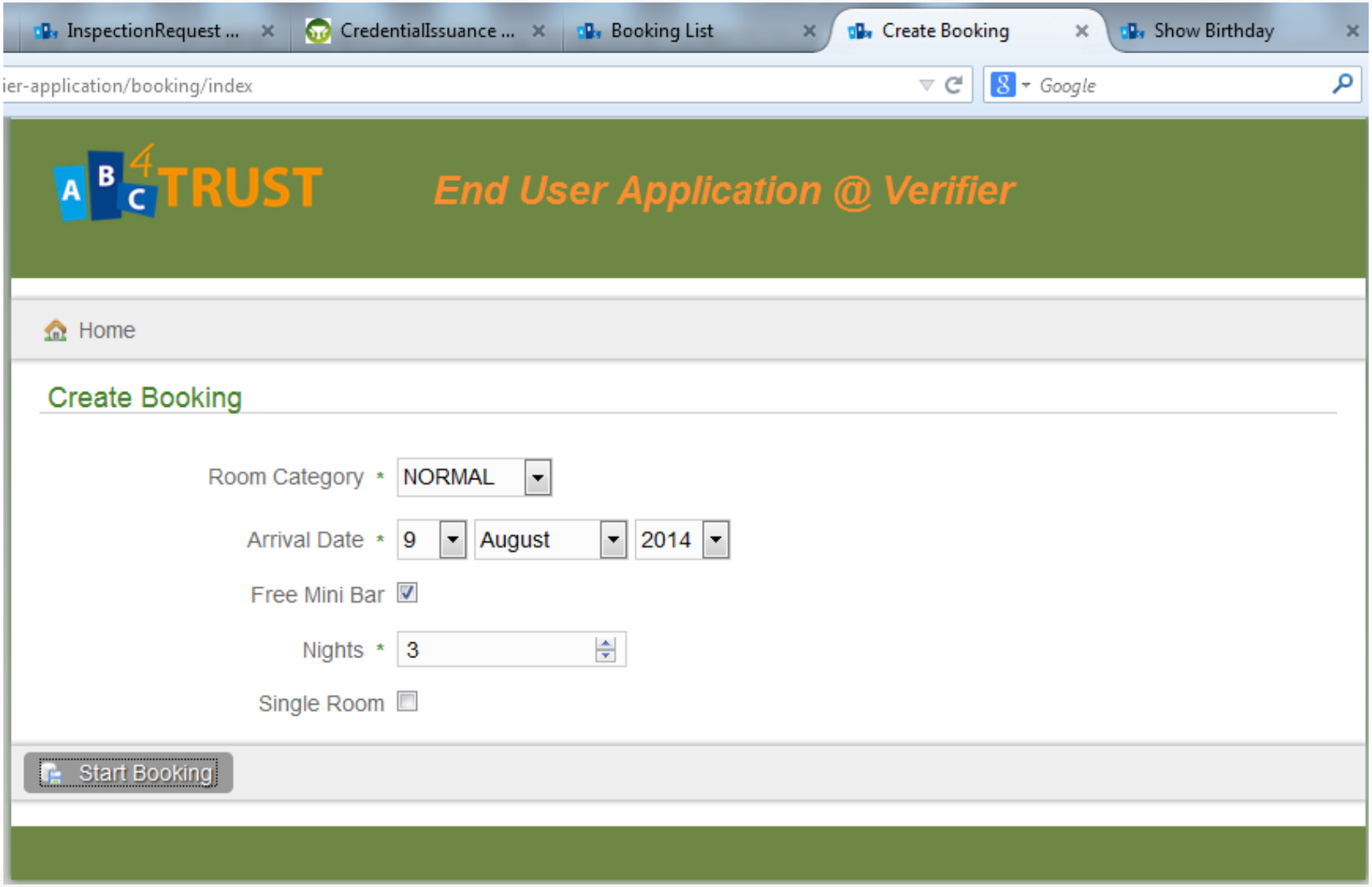


Hotel Booking

USER @ VERIFIER

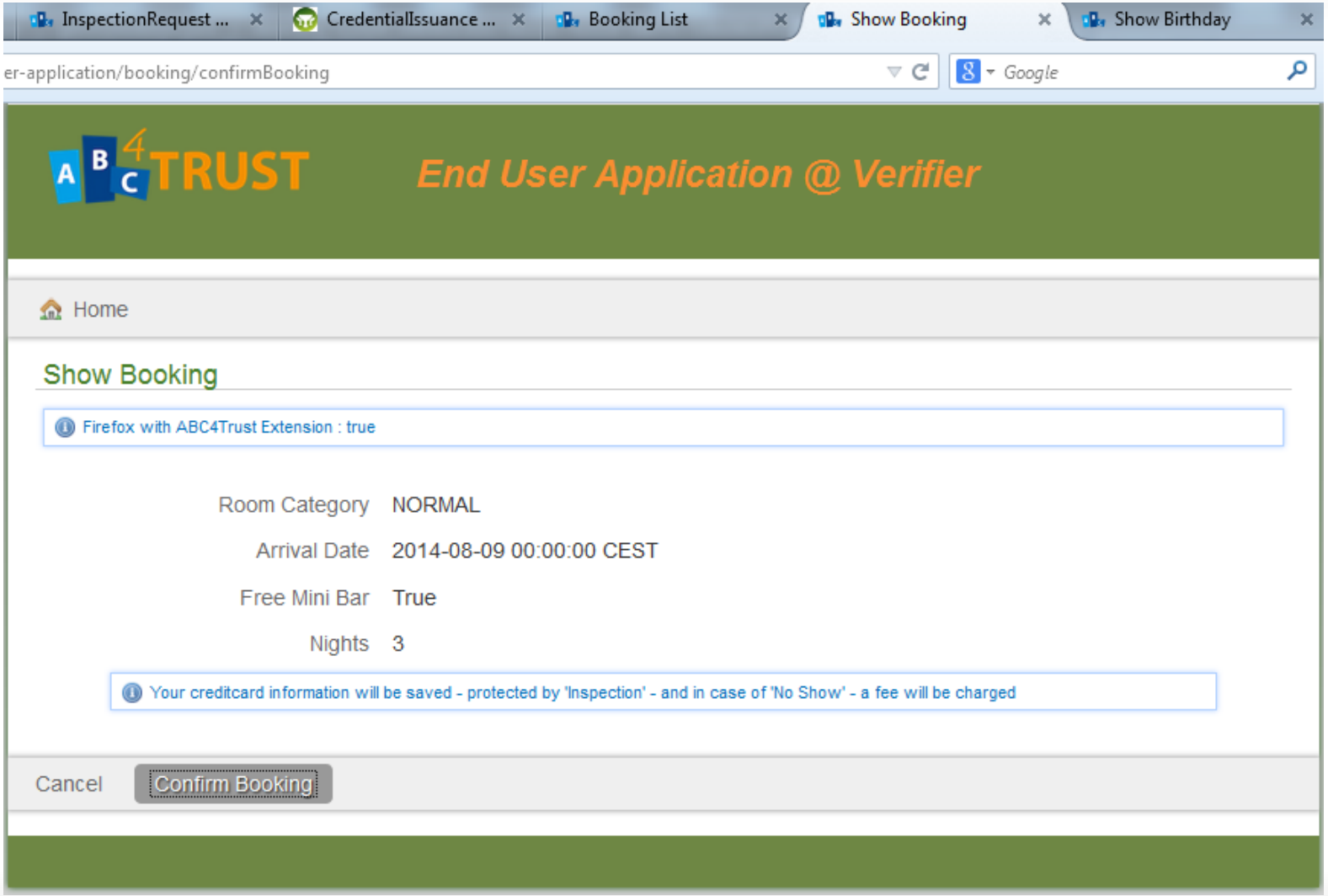
User @ Verifier

Demo Application



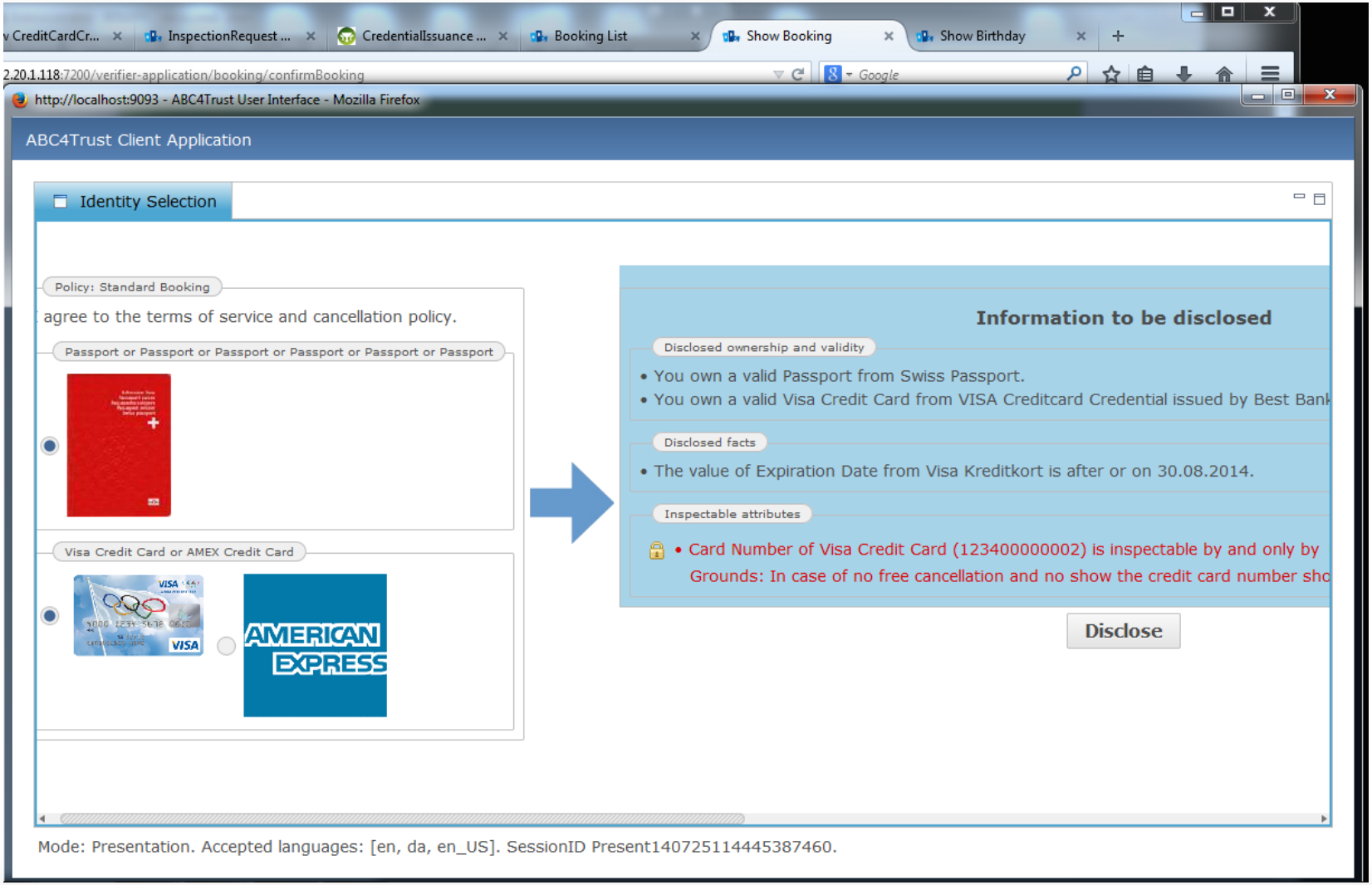
User @ Verifier

Demo Application



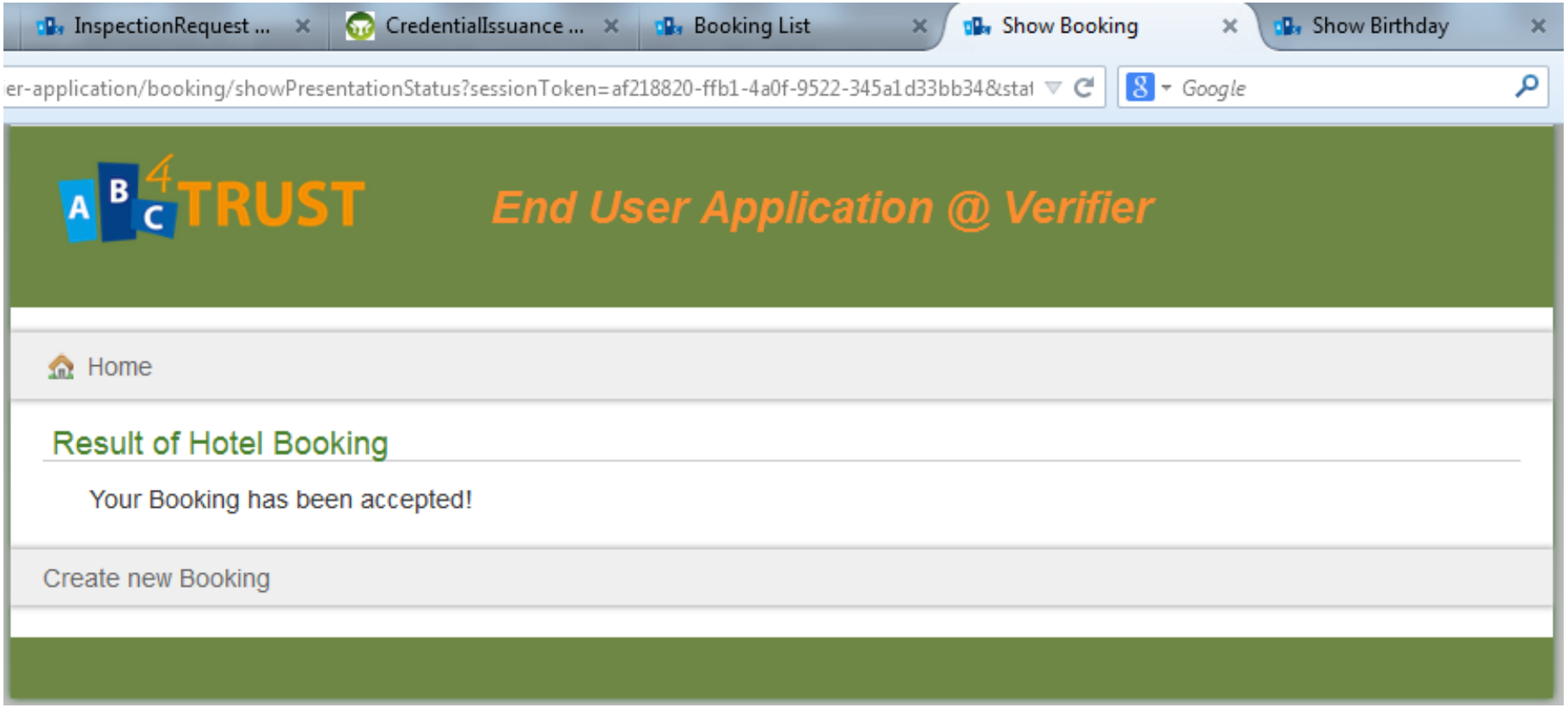
User @ Verifier

Demo Application



User @ Verifier

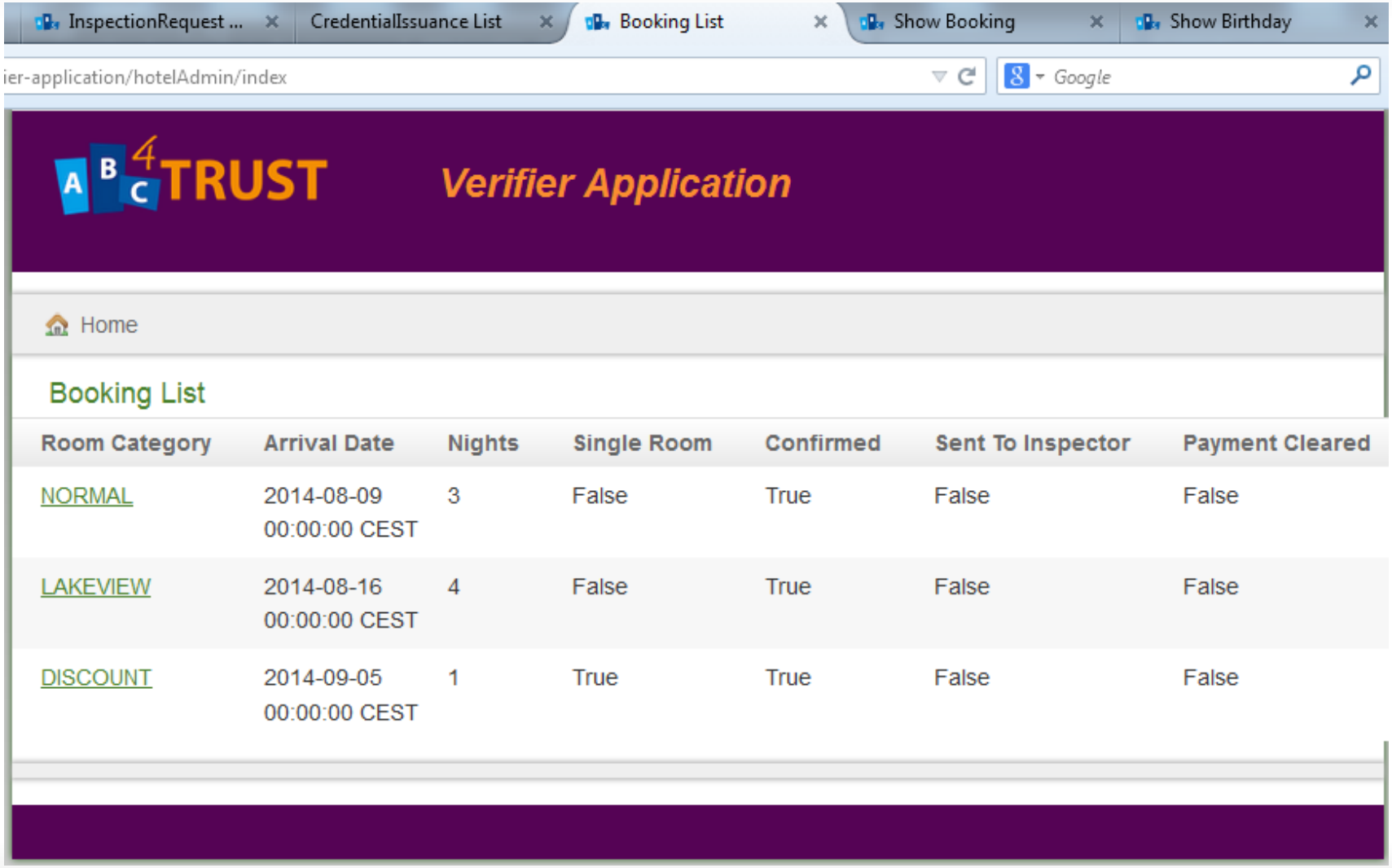
Demo Application



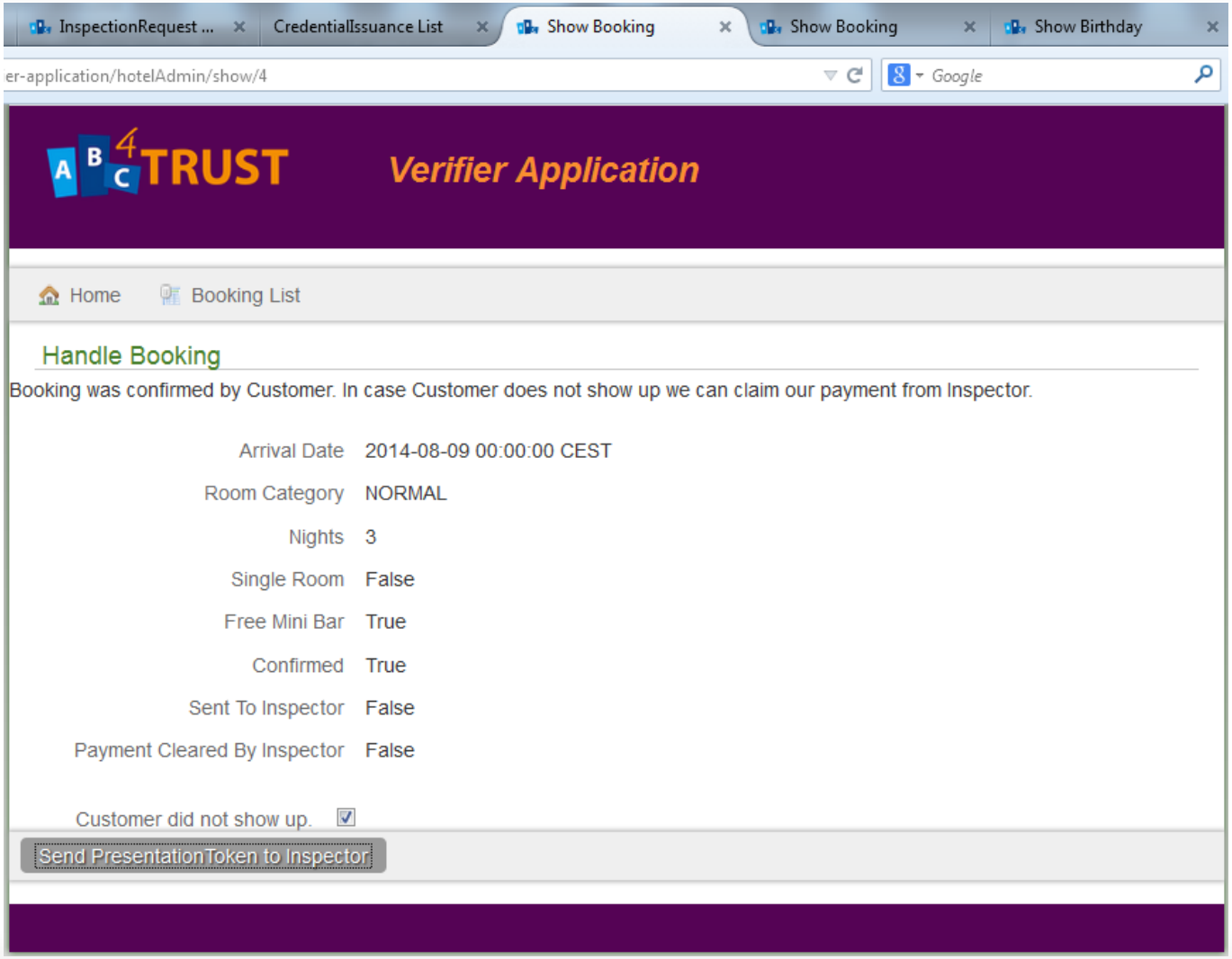
Hotel Booking

VERIFIER

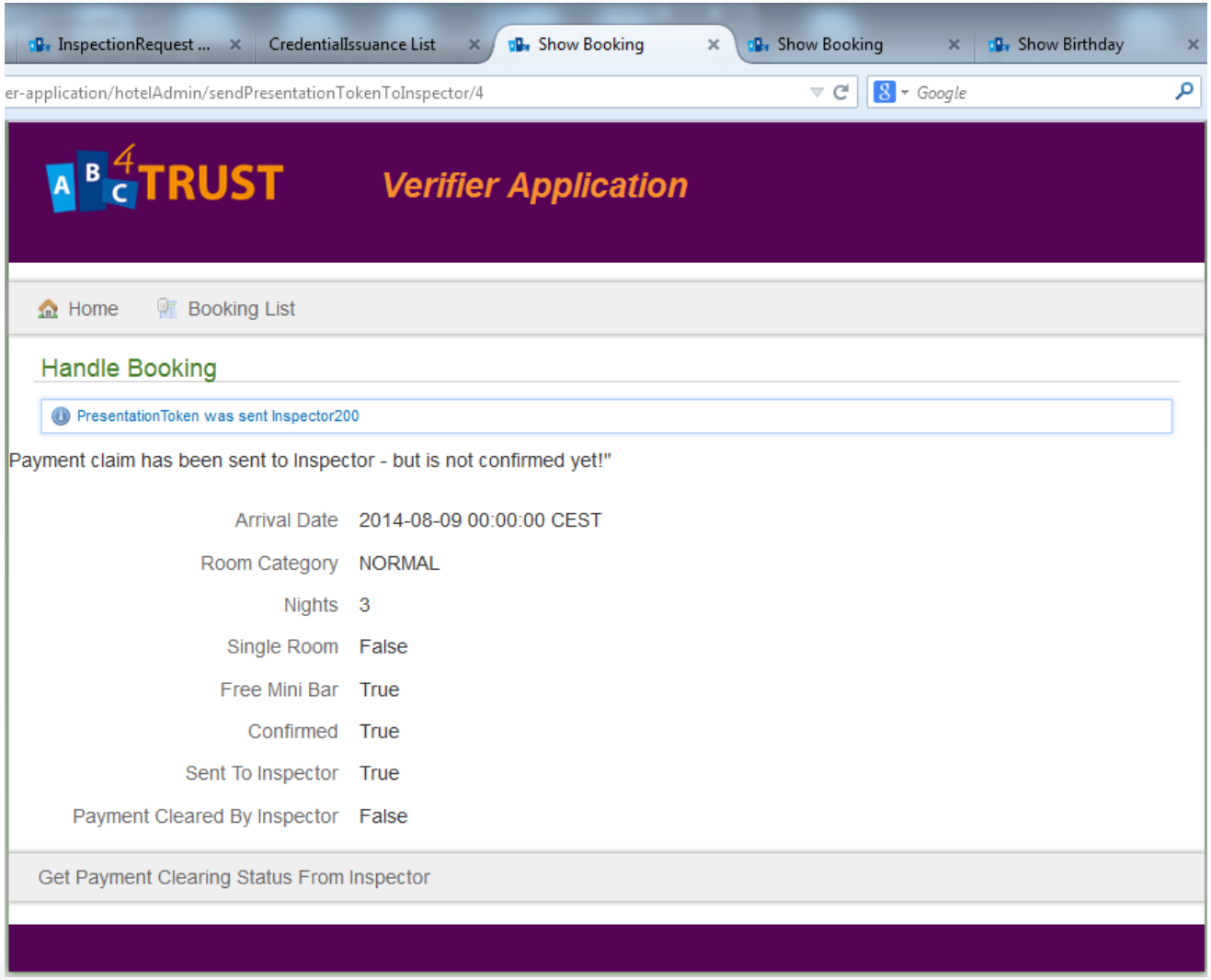
Verifier
Demo Application



Verifier
Demo Application



Verifier
Demo Application

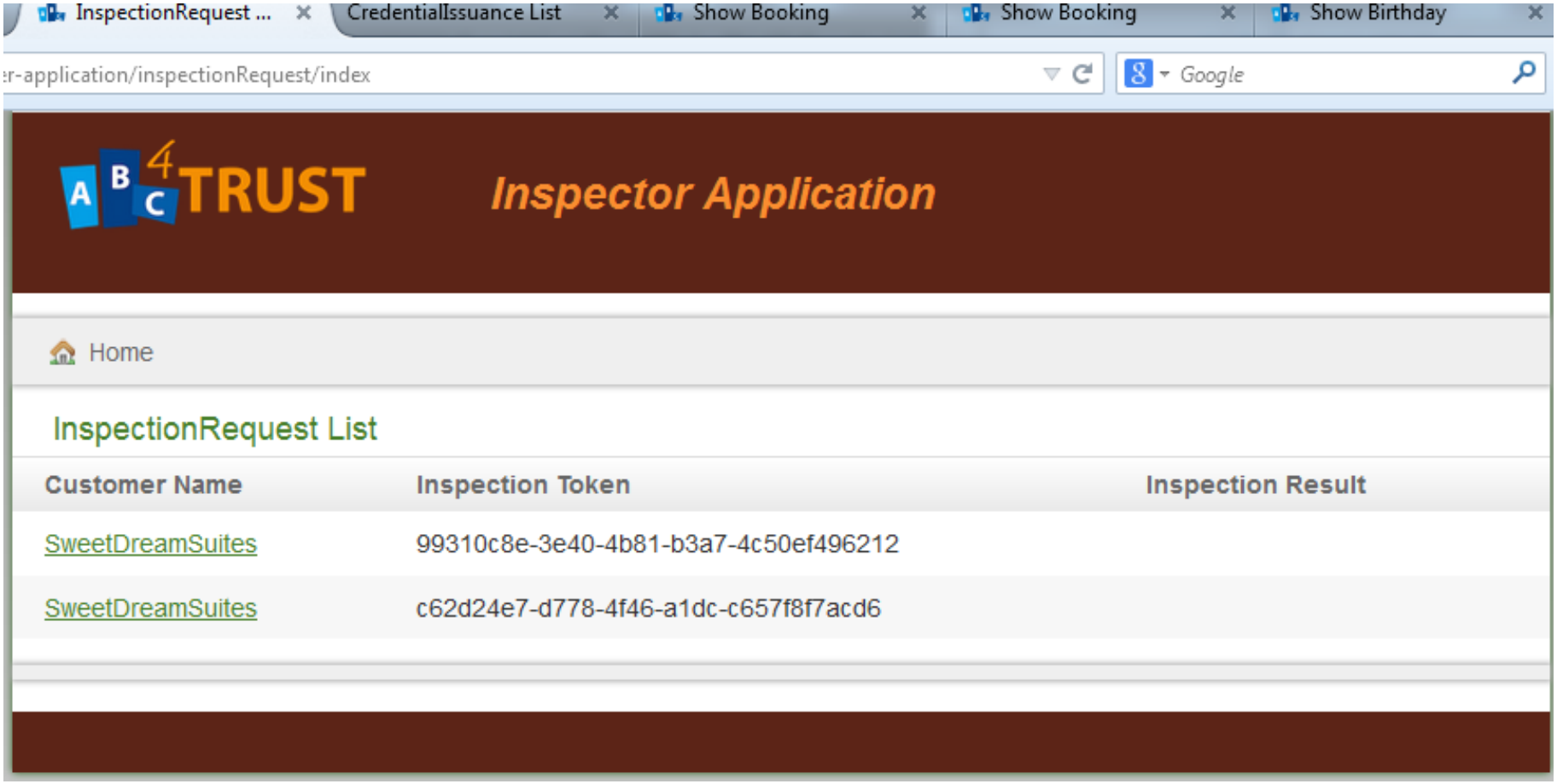


Hotel Booking

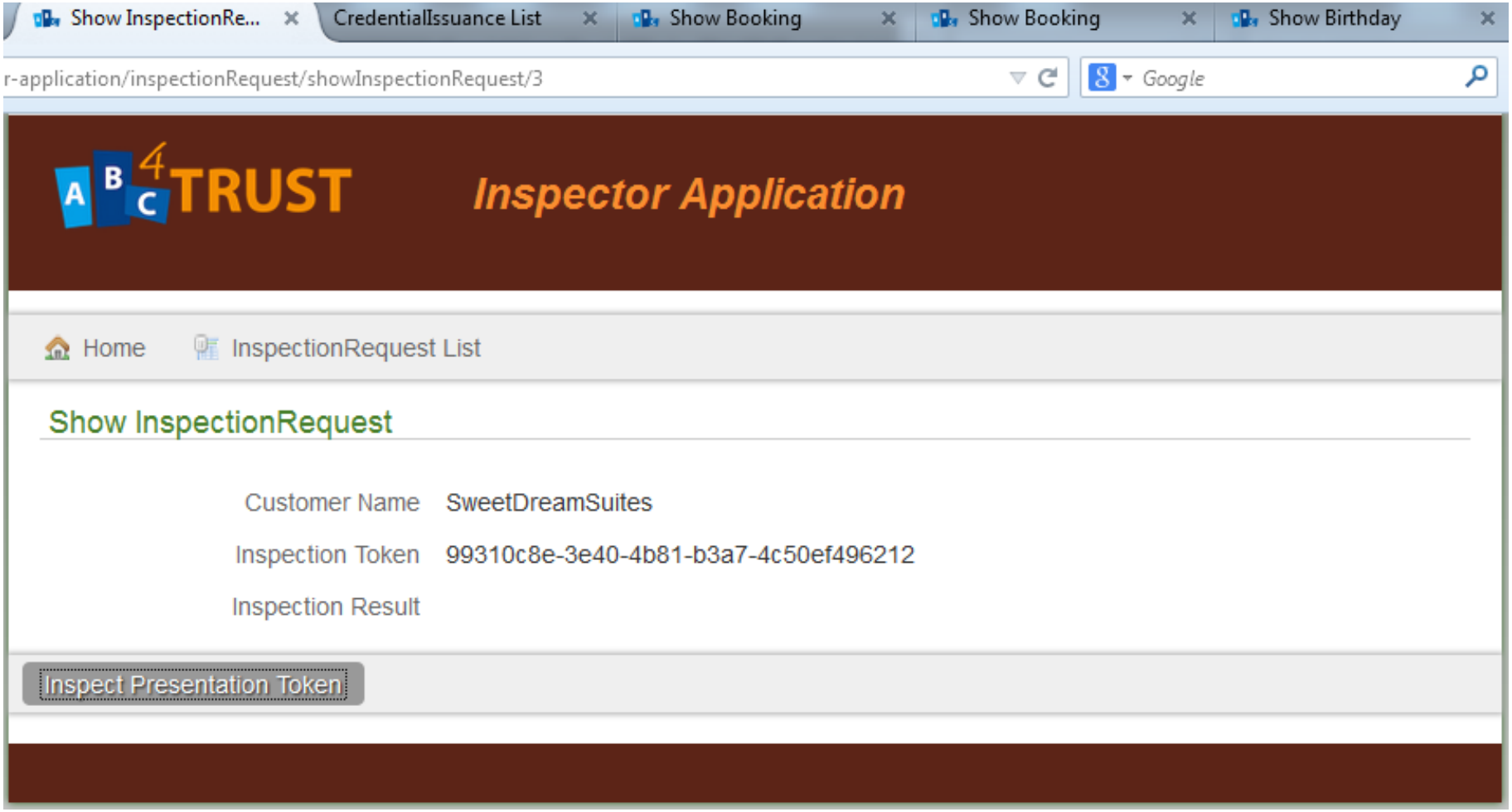
INSPECTOR

Michael Østergaard, Miracle A/S

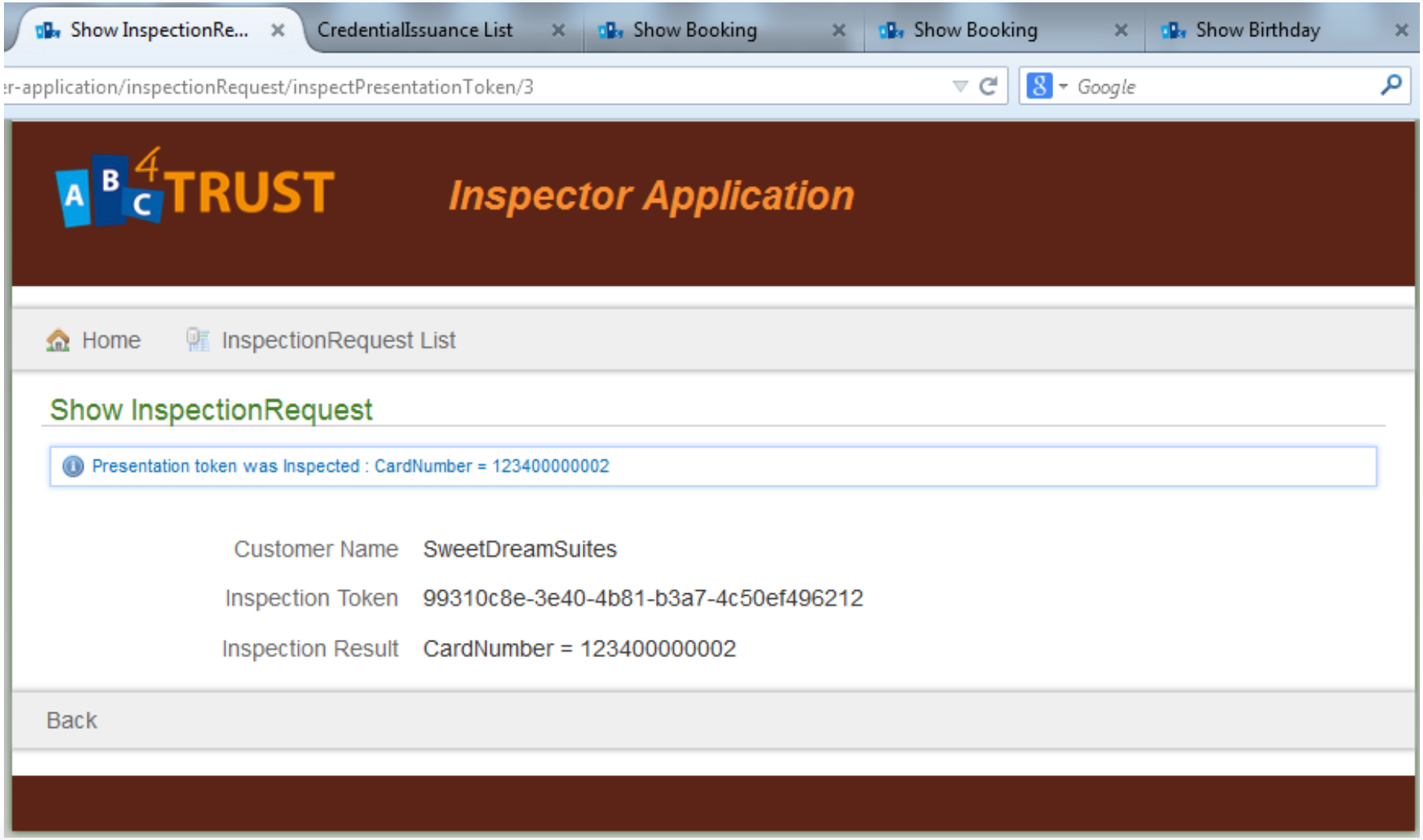
Inspector
Demo Application



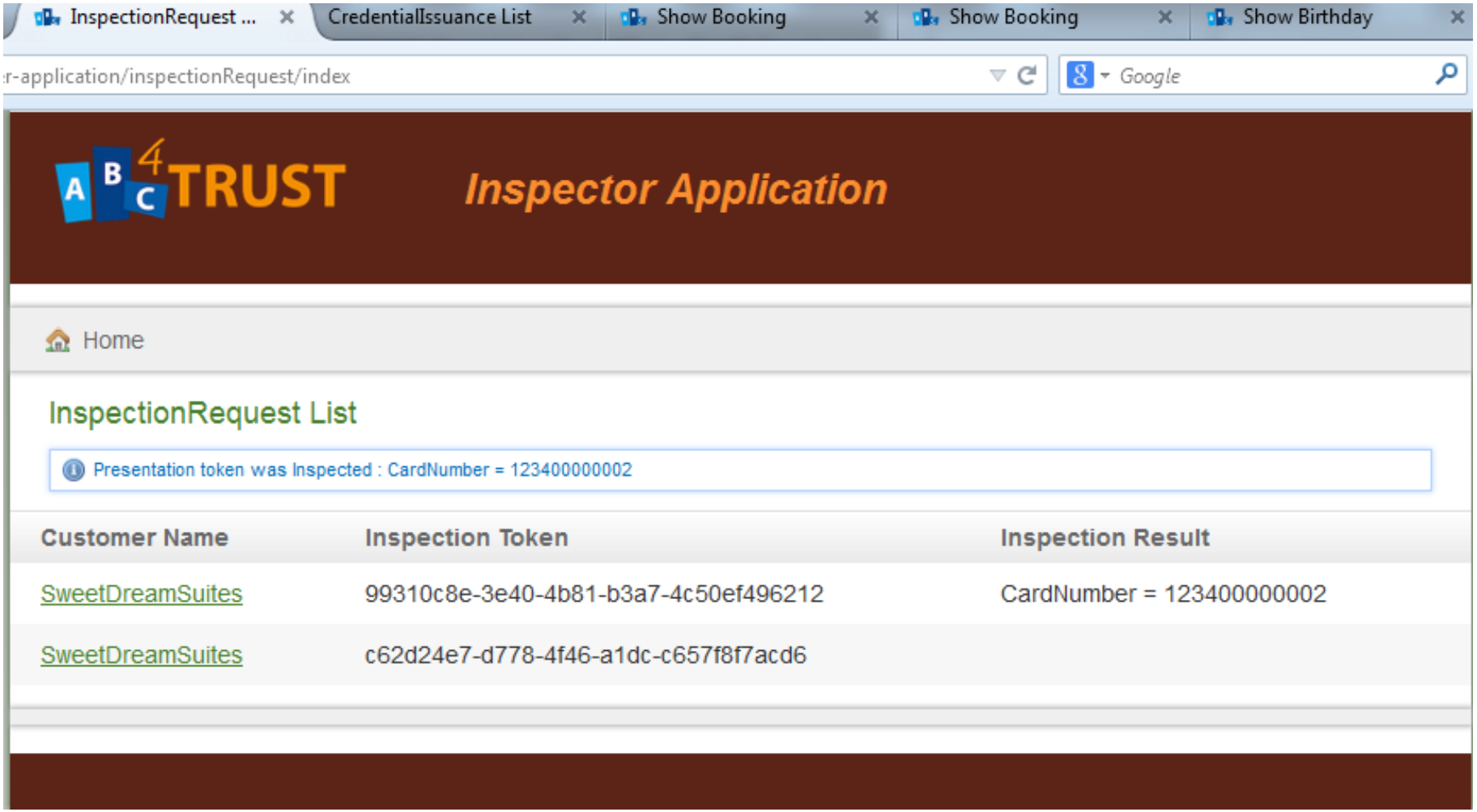
Inspector
Demo Application



Inspector
Demo Application



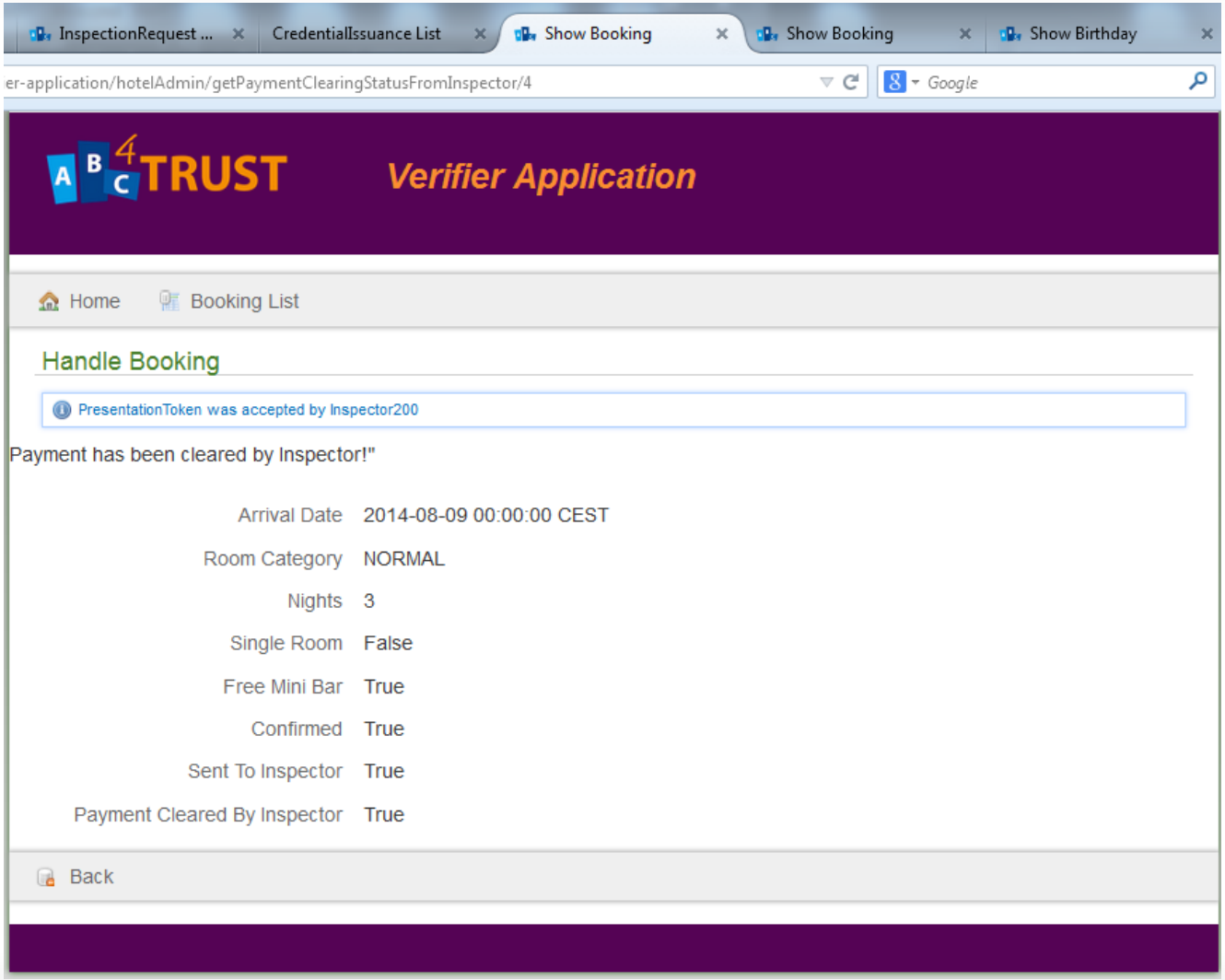
Inspector
Demo Application



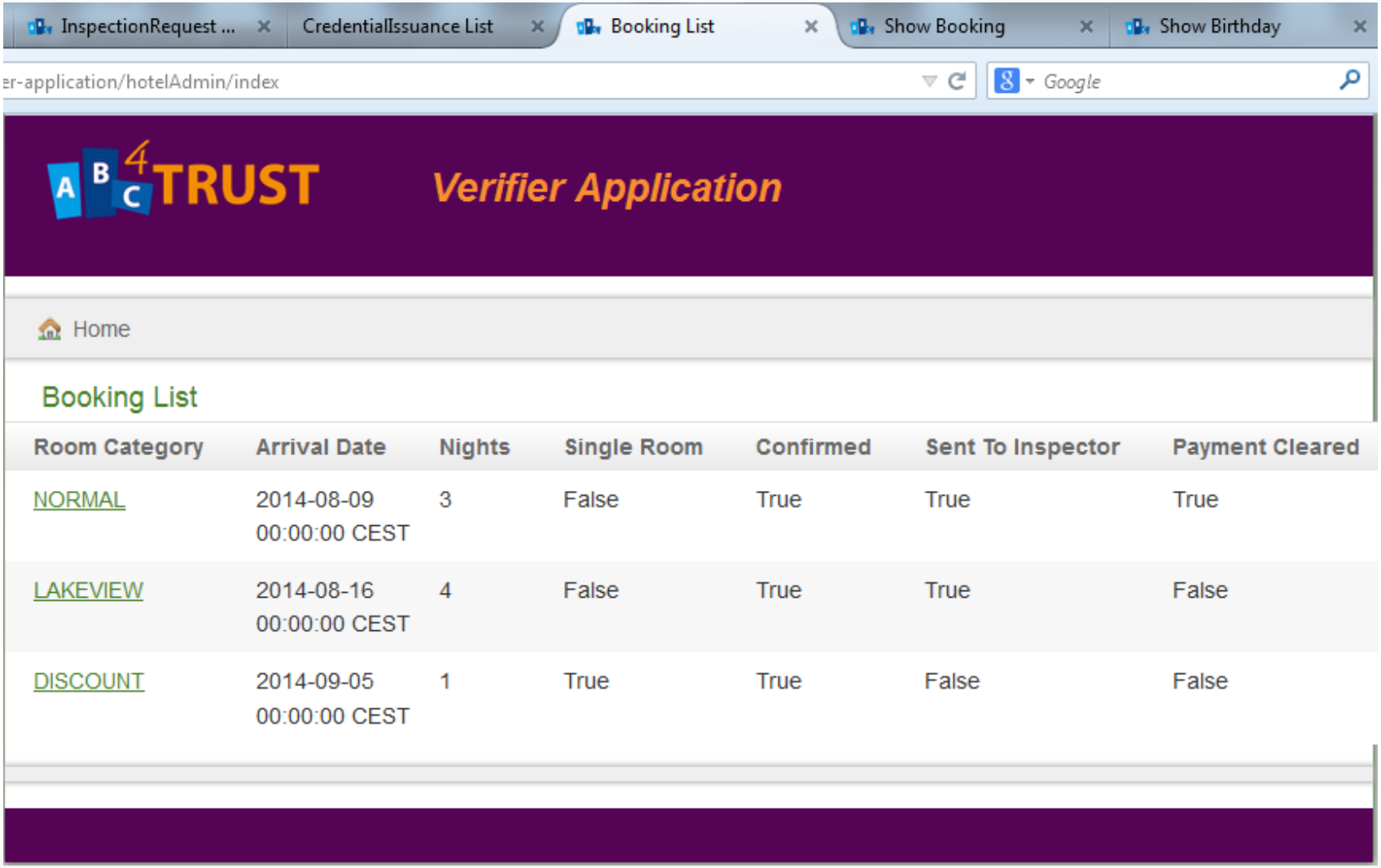
Hotel Booking

VERIFIER

Verifier
Demo Application



Verifier
Demo Application



Demo

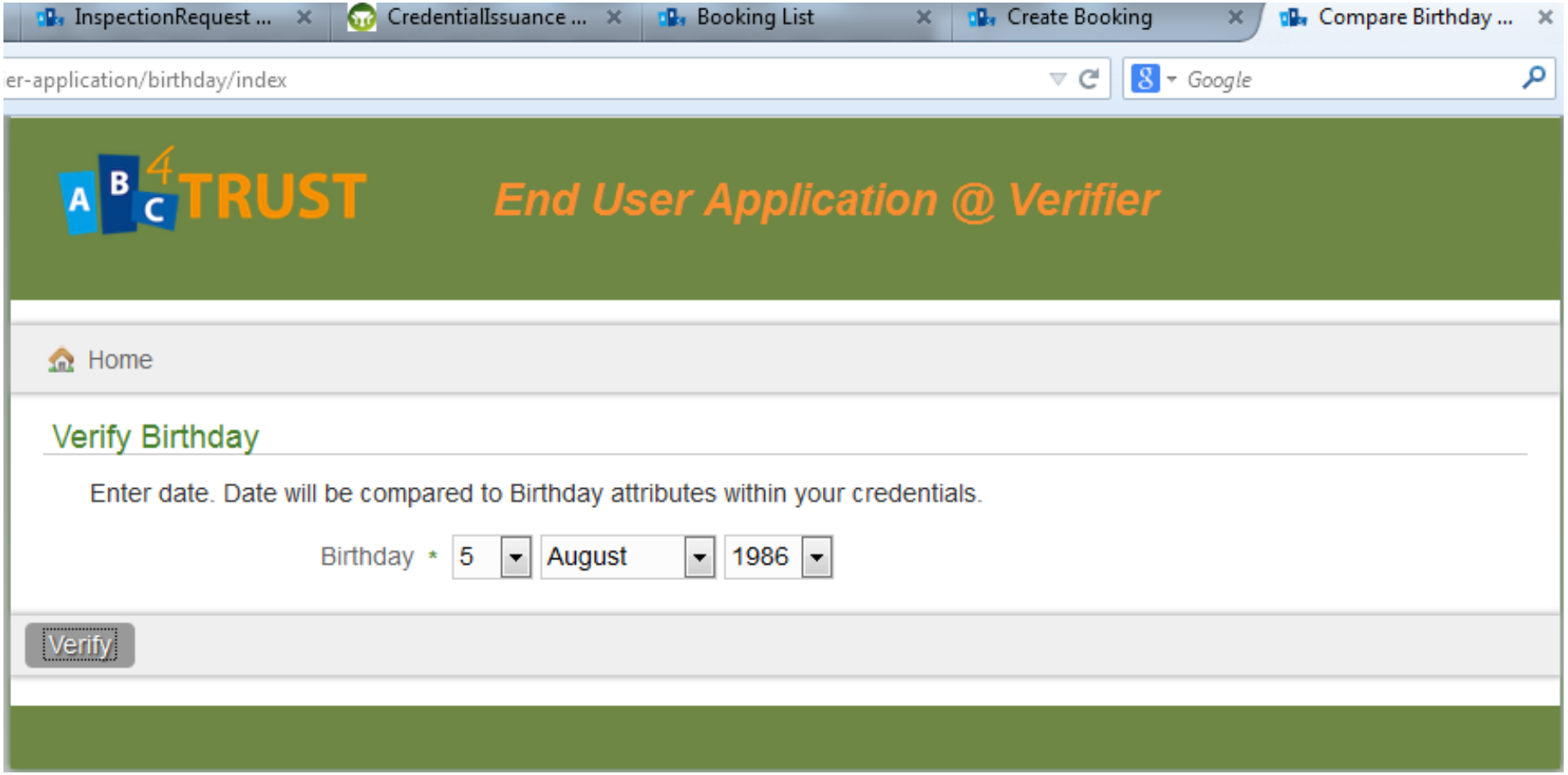
AGE VERIFICATION

Age Verification

USER @ VERIFIER

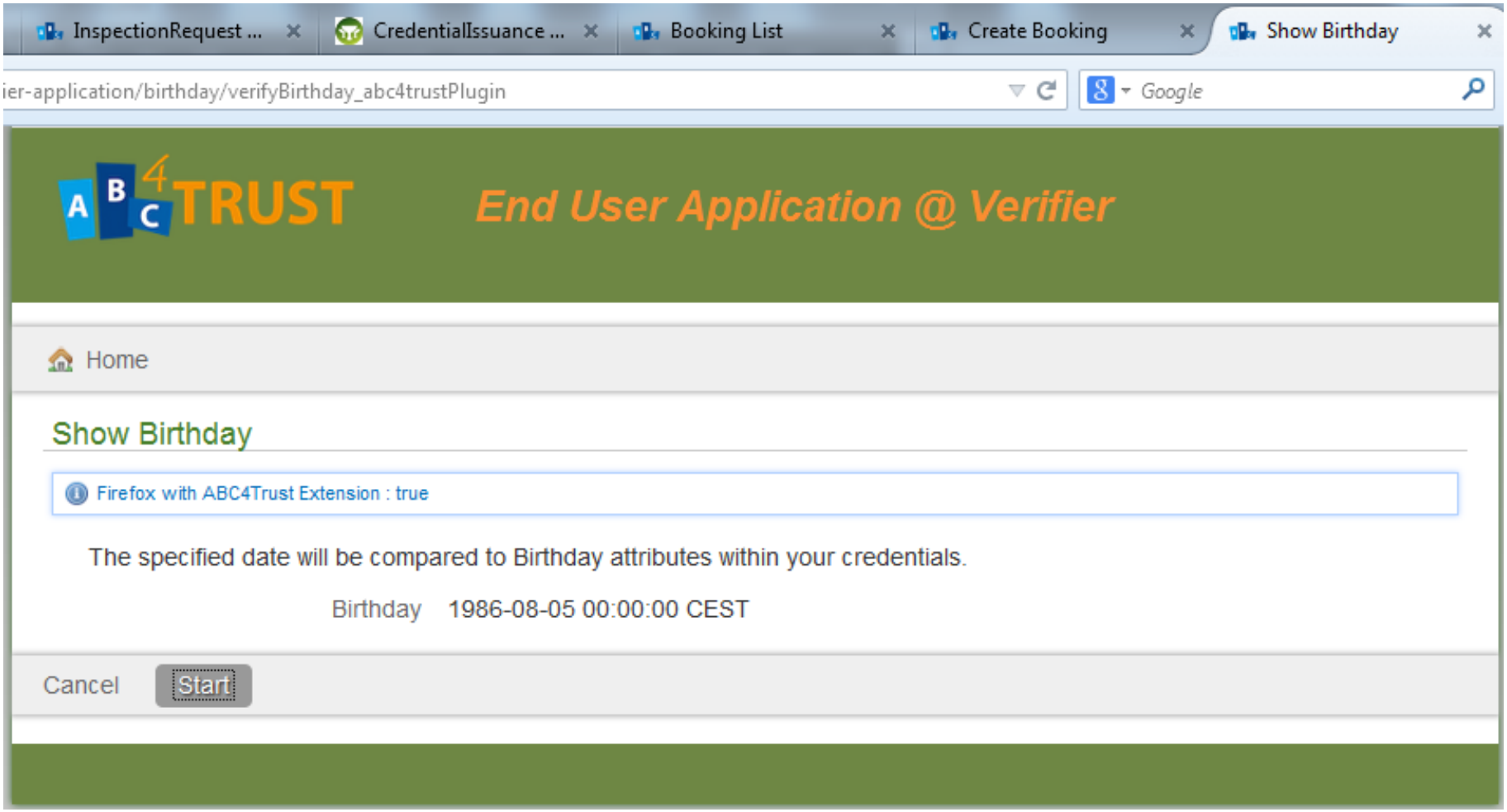
User @ Verifier

Demo Application



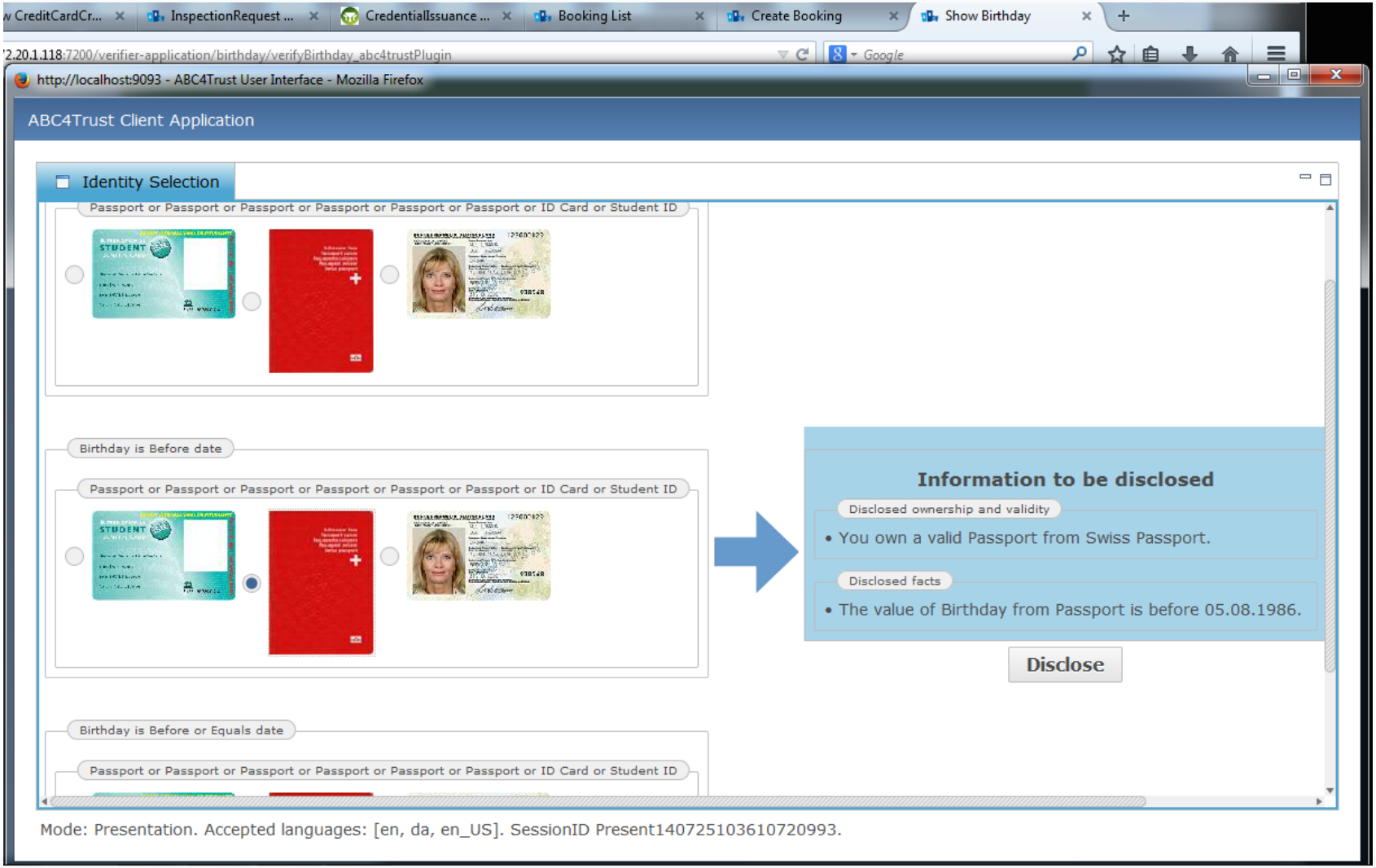
User @ Verifier

Demo Application



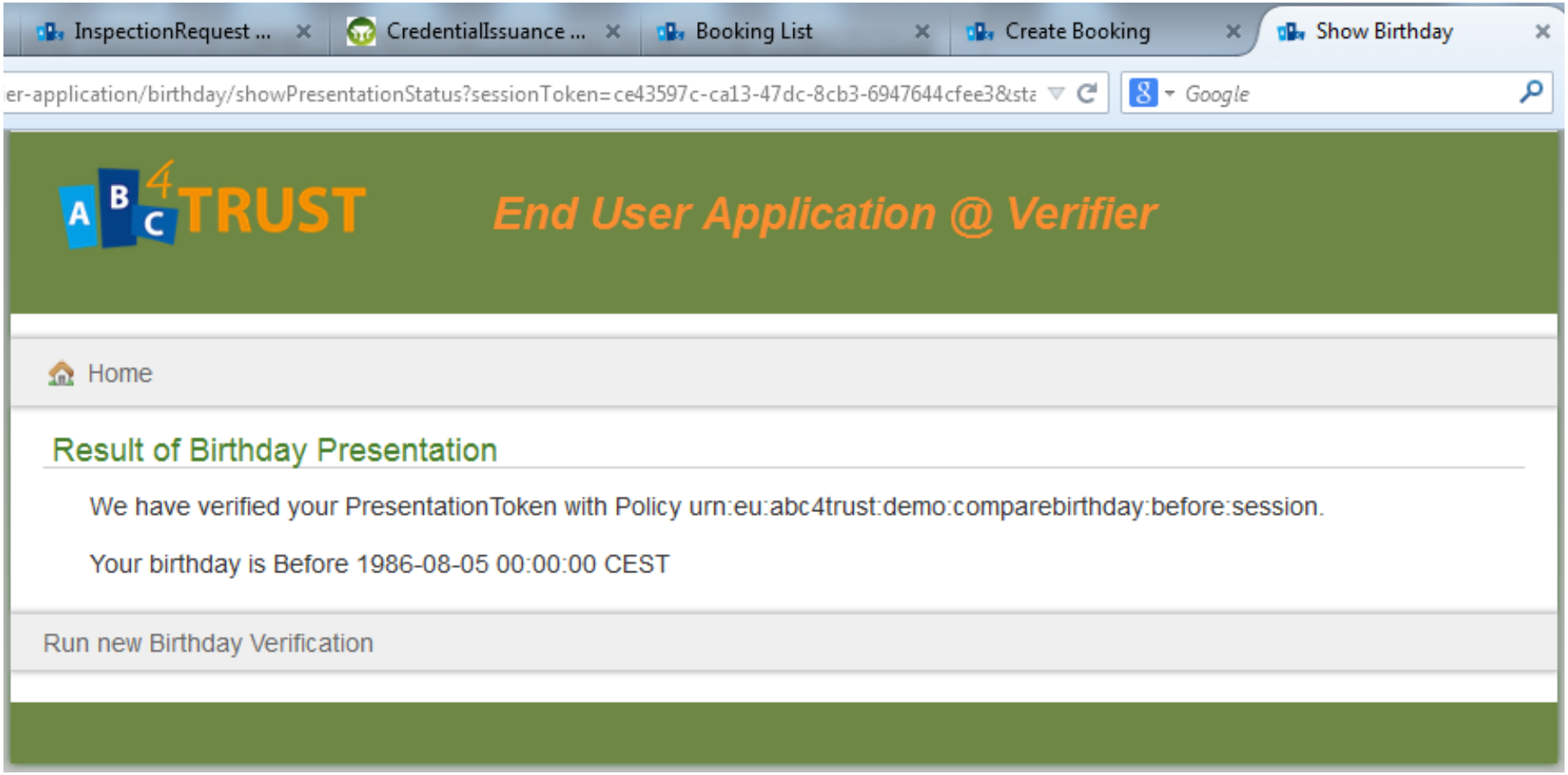
User @ Verifier

Demo Application



User @ Verifier

Demo Application



More Information

- My contact information
  - Michael Østergaard
  - mop@miracle.dk
- ABC4Trust website
  - www.abc4trust.eu