ATTPS | Achieving The Trust Paradigm Shift

Deliverable D3.5
Harmonised e-authentication architecture in collaboration with STORK platform (M40)

Version 1.0
Author: Bharadwaj Pulugundla (Verizon)

25.10.2015

Table of content

1. Introduction

In this demonstrator, the STORK platform is integrated with the existing solution D3.2 as a new Identity and authentication provider. For readability reasons, we have decided to reuse some of the content and explanations from D3.2.

Within the existing solution, the user is now provided with a choice to select STORK log in and authenticate against it for accessing the services from the service provider for both mobile and web application.

This document provides a background to the live demonstrator.

According to the ATTPS project Task 3.5 description:

Task 3.5: Technology test bed (M1 – M40, task leader: BIC)
In this task, a limited TDL real life test bed environment will be implemented using the current and future available hard and software components contributed from TDL partners and integration based upon the developed trust architecture principles of the TDL community. This will be called from now on as Generic Trust Architecture Center (GTAC). The test bed supports generic trust architectures (developed in WP3 of ATTPS) and allows other TDL members to integrate & test their state of the art solutions. ATTPS will implement two separate forums: Certified hackers to test provided Trustworthy ICT solutions and the ICT expert forum to support providers of Trustworthy ICT solutions on integration and deployment aspects. The GTAC infrastructure consists of a technology platform provided and composed by:

- TDL members for enabling infrastructure on: communication level (Internet; Telecom) and on trustworthy platforms such as the e-authentication framework architecture, and
- TDL members providing trustworthy ICT solutions for integration and deployment on the enabling infrastructure

ATTPS will provide the overall design of the GTAC, taking into account the preparedness of TDL members to provide the necessary technology. ATTPS will operate and maintain the GTAC and provide access:

- To providers of trustworthy components with access to the TDL test bed infrastructure by providing user groups and ethical hackers in order to validate and test modules, systems, concepts and services,
- To support new developments of TDL members for innovative ICT concepts,
- To realize a harmonized-European e-authentication architecture, by close collaboration with the STORK platform, and
- To test the components of generic trust architecture of Work Package 3, i.e., mobile service and platform integrity, trusted stack and data life cycle management.

During the course of the ATTPS project, the GTAC can be found at: https://attps-survey.nlehd.de/gtac/ . After the end of the project GTAC will be taken over by TDL and accessed via the TDL website.

This deliverable provides a "Demonstrator allowing validation of interoperability allowing the private and public identity providers to offer their technologies to a variety of relying parties.

2. Demonstrator Objectives

This project aims to test and demonstrate the feasibility of technical solution for a cross country identity assurance ecosystem with government issued identity consumed by a third party service provider.

3. State of the Art Analysis

With the increase in the number of identity providers, the consumer ends up with more than one digital identity. For the ease of transaction between service provider and end consumer, various federation techniques are applied. Eg, service providers nowadays provide options to log in with Facebook account or google account etc. In addition there are solutions such as OpenID account chooser[1] that allow user to choose the type of identity for authentication.

Referring to the genetic trust architecture principles, in this demonstration, we aimed to test a solution where the user has a choice to select a government issued ID to complete a commercial transaction such as buying an offer online.

The key differentiator is that our solution is integrated with the STORK platform to show the federation between private and public sector identity providers. The user can select an identity provider and in addition has full control over his personal data. He decides what data should be shared with whom. Using such a solution, it is possible to facilitate private and public sector collaboration and demonstrate an improved level of trust for consuming online digital services.

4. Followed Approach

This demonstrator uses an existing solution built for ISIC business users (Students, Merchants and Issuers) in Europe and employs a collaborative approach across all ecosystem

[1] https://www.accountchooser.com/learnmore.html

participants such as Relying Parties, Identity and Attribute Providers. For this reason, the solution is developed referencing the TDL framework and is contextualized for this pilot.

Verizon plays the role of technology enabler and solution integrator for this project. In addition to the existing Verizon credential issuance and authentication system called Universal Identity Services (UIS), the STORK platform is added as a new identity and authentication provider. A hub is deployed that offers proxy service and user interface applications for access on mobile and laptop/pc devices.

Verizon is working with the International Student ID Card (ISIC) Association [2] that will provide a real life context for this pilot within its community.

This pilot has two tracks. The technical track covers defining use cases, hosting the technology components, and integrating the solution. Due to the open architecture, the solution is scalable using APIs, making its design flexible for integration with different types of platforms. In the second track, the commercial model will be developed and tested within the ISIC community. This includes developing revenue models and a going-to-market strategy to develop the eco system.

4.1 High Level Design of the Solution

As mentioned in section 4, the solution has the hub and spoke model architecture detailed in the TDL research paper "Architecture Serving complex identity infrastructures"[3]. This demonstrator implements user authentication with the STORK platform in conjunction with the following key services:

- Credential life cycle management for digitizing student identities (defining user enrolment/registration processes, issuance, renewing and/or revoking identity credentials)
- Authentication utilizing a wide variety of second form factors such as SMS, email, Voice based OTP, Software token, or Hardware Token
- Consumer consent and privacy management
- Attribute Verification (e.g., student status or age)
- Integrate with multiple identity/attribute providers, and various relying parties
- Campaign management

[2] http://www.isic.org/about/about-the-isic-association.html
[3] http://www.trustindigitallife.eu/uploads/Architecture%20serving%20complex%20Identity%20Infrastructures.pdf

4.2 Components of the Solution

The following diagram gives an overview of the key components in this solution.

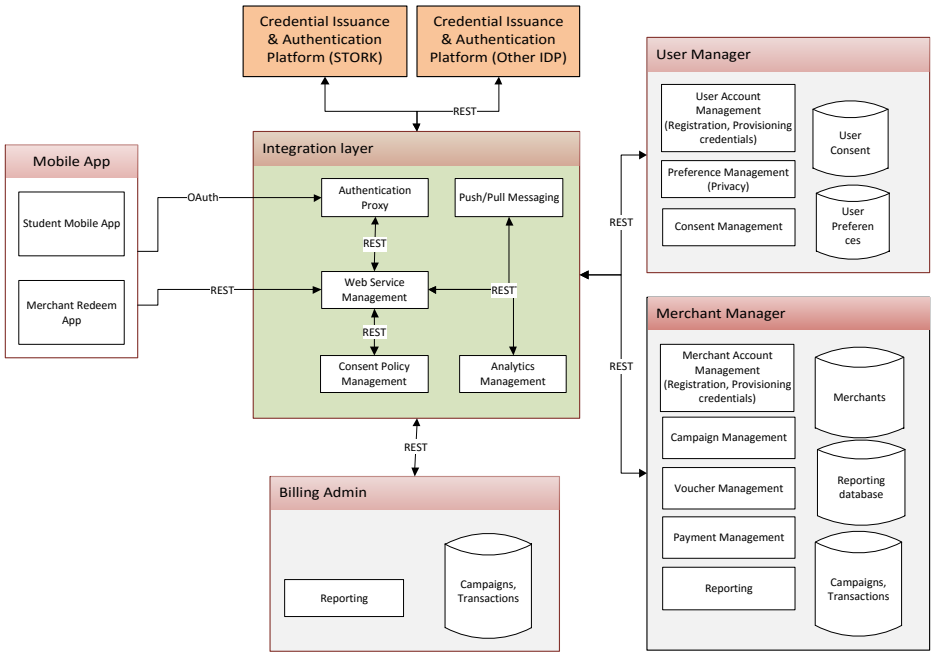


Figure 1: High Level Design of the overall Solution

STORK Platform: The STORK based ID is used as an identity provider for this demonstration. STORK is a protocol to allow authentication across national borders. The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. The role of the STORK platform is to identify a user who is in a session with a service provider and to send his data to this service.

Verizon Universal Identity Services (UIS): It is a cloud based identity management system that supports multi factor authentication mechanism. This is used as another identity provider in this solution.

Mobile applications: There are two mobile applications one for the student and one for the merchant. The student mobile app offers the feature to access the benefits or discounts. All the purchased offers are stored in user profile. The user can redeem such a voucher at the merchant location. The user can also manage his preferences and privacy settings through this mobile app. In addition, the solution aims for a better user experience, since this is one of the critical criteria for gaining students to use this platform.

For the merchant, can scan the purchased offer and also verify the student status.

Integration layer: The integration layer contains the consent policy management, databases and push/pull messaging services. These databases are used to draw reports on transactions for billing. Through analytics, the merchant is able to introduce context based promotions based on various factors such as past buying behavior of the student, his/her purchasing preferences, and geo location based services. For such analytics, only the aggregated data is used removing individual user names, to protect user privacy. Since the service is offered as "opt-in" to the user, in addition to the explanation of what kind of data are captured from the user and how they will be used, users will be asked explicitly to provide consent for using any specific attributes.

In addition, there is an authentication proxy in the integration layer that is capable of adding more Identity providers, making the solution scalable.

Billing Admin: creates reports from the system for transaction based revenue sharing amongst the parties involved. The billing admin team will only able to view the transactions happened in that period, and calculate the invoice amount for the service provider.

User Manager: Using the user manager, the student user can log into the application to manage his/her profile, preferences, privacy settings etc. Whilst the service provider may request various data items, the user always controls the data to be sent. The explicit consent of the owner of the data, the user, is always required before his data can be sent to the service provider.

Merchant manager, the issuer can manage the user registration process for both student and merchants. Merchants can log into their own accounts to perform activities such as adding a new payment provider, manage campaigns etc. The merchant registration also needs to be approved by Issuer. The merchant can create campaigns using this portal and run reports to analyze the campaign performance. There is also a mobile app that the merchant can use to scan and redeem the purchased voucher. Through this app, the merchant can also validate the student ID by scanning the QR code based student ID. Campaign Manager (Web Application).

The back end application is hosted on the Verizon cloud environment.

In this particular demonstration, referring to the STORK set up, we have installed STORK Local Pan-European Proxy Services model (PEPS), STORK Foreign PEPS and emulated country specific authentication portal. STORK proxy used is a custom implementation of Verizon that does not offer an open source version. During the course, we encountered several issues

with the deployment and configuration of the OpenAM based STORK proxy which were overcome; More details on the generic STORK implementation can be found here[4].

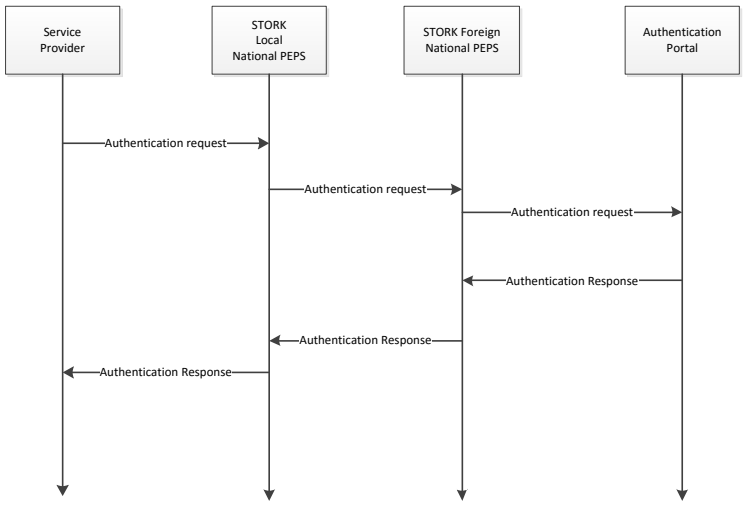


Figure 2 Authentication Sequence with STORK ID

There are two scenarios in this use case. In scenario one, the student user logs in to the mobile application and browses for the offers. In the second case, this user will log into the web application to manage his profile. In both cases, at the beginning of the workflow, the user is presented with a screen to select the authentication method. After the user selects STORK authentication method, the request is routed to STORK National PEPS. The service provider and the National PEPS belong to the same country. When the user tries to access the service provider application, by default the request goes to the authentication portal via local national PEPS in the country. In cases when the user is from a different country, then the national PEPS reroutes the authentication request to the authentication portal via foreign PEPS.

5. Demo Setup

The platform is hosted in the Verizon Cloud in the proof of concept environment. This can be accessed from the GTAC. To setup the demo, two smartphones (android based), one PC, and Wi-Fi Internet connection are needed. On one smartphone, the student (user) mobile

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_04_15_letter_artwp_atos_origin_annex_en.pdf

app should be installed and on the other device the merchant redeem application. Various users (Student, Merchant, Issuer, and Billing Admin) should be created.

6. Storyline of the D3.5 Demonstrator

In this deliverable, the following use case is demonstrated.

- A Netherlands citizen (Student) wants to access a third party application from ISIC issuer which supports STORK. A test user is created for this purpose.

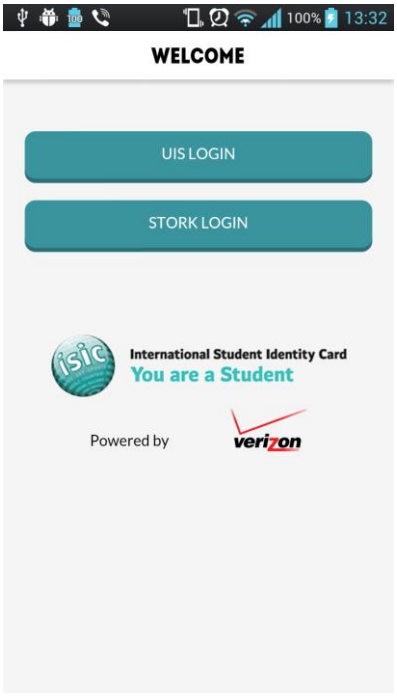
Following is the demo script for the technical proof of concept:

Table 1: Demonstrator Storyline

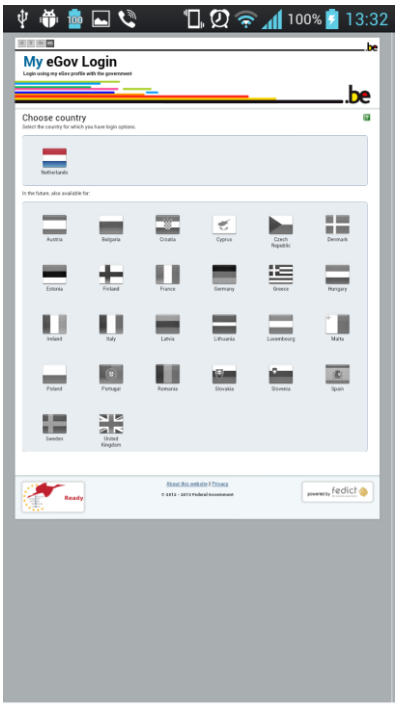
Serial #	Activity	Comments
Log in to mobile application		
1	Launch the mobile application	STORK ID configured for the Netherlands
2	Select STORK Authentication	
3	Select NL flag	
4	Enter the log in ID and Password	On successful authentication, user is able to see the home screen of the app to browse offers
Log in to the web application		
5	Launch the web application	
6	Select STORK Authentication	
7	Select NL flag	
8	Enter the log in ID and Password	On successful authentication, user is able to see the home page.

7. Demonstrator Screenshots

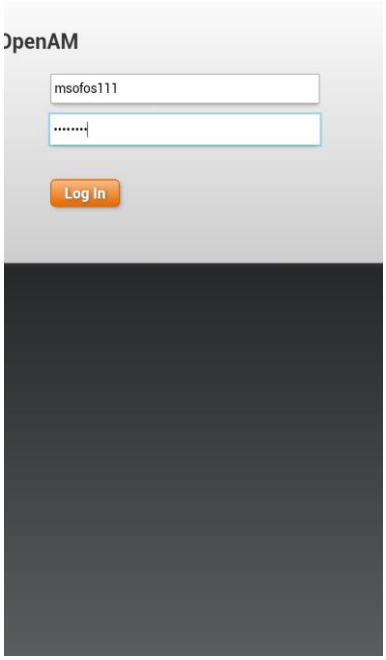
7.1 Student mobile Application



Select Authentication method



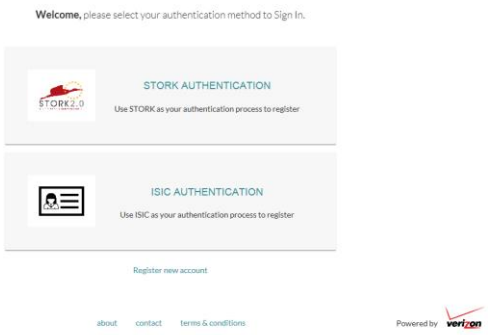
Select Country



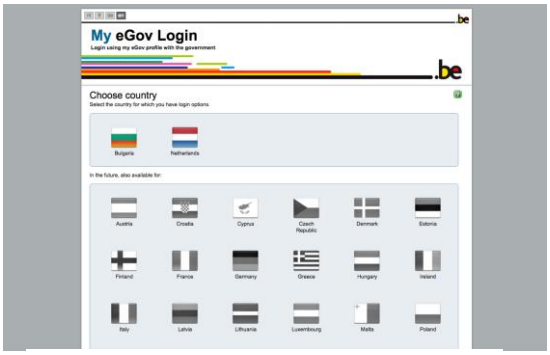
Log In

Application Home Page

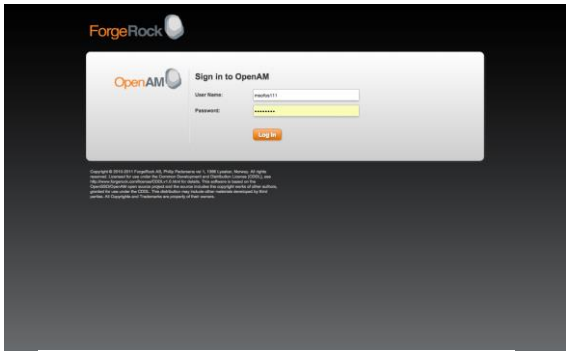
7.2 Web Application for Student Profile and, Consent Management



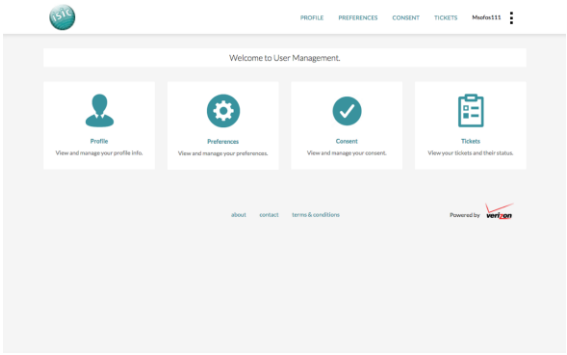
Select Authentication method



Select the country



Log In



Home Page of the application

8. Deviations from the DoW

None

9. Corrective Actions

None

10. Conclusion and Outlook

Verizon has developed a prototype to implement a real-time use case for identity federation with government identity providers and able to demonstrate that how private service providers can use the stork identity. This solution is scalable and can be integrated with more number of identity providers and service providers

.

This is a Verizon sandbox demonstrator, which can also serve as a test bed, where different aspects of the solution can be tested such as security, privacy and interoperability. From the user point of view; it offers flexibility to authenticate against an existing national ID. For the service providers, it saves a lot of infrastructure costs for managing the identity lifecycle of the users by simply integrating with the STORK platform.

In the first run, we demonstrated a cloud based identity management system where the user can select the second factor authentication method. In the second run, we demonstrated the use of a government issued National ID as an authentication option for a commercial transaction. The key achievement is that we were able to develop a technical solution is based on a real use case within the guidelines of Generic Architecture principles.

As a next step, any service provider who is interested in such an implementation can reference to this prototype concept of federation between governments and private enterprises and approach the local governments for integrating the applications with STORK authentication.