verizon

ReCRED

Verizon Enterprise Solutions

Towards a password-less OpenID Connect Experience

OpenID Connect integration with FIDO for submission to OpenID foundation EAP working group from ReCRED project

Project[1] **Number:** 653417
Project Acronym: ReCRED
Project title: [From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control]

[1]The term 'project' used in this template equates to an 'action' in certain other Horizon 2020 documentation

Table of Contents

1. INTRODUCTION

The OpenID Connect specification (http://openid.net/connect/) enables services, called Service Providers (SP), to delegate the authentication of users to other entities, called Identity Providers (IdP). This is particularly useful for various reasons:

- users do not need to remember the authentication credentials for all the services but instead they authenticate using the credentials that they have for specific IdPs.
- Service Providers do not need to worry about providing strong authentication mechanisms for their users.

In the OpenID Connect context, the authentication mechanism is entirely up-to the Identity Providers. Typically, popular IdPs such as Facebook and Google, use the traditional username/password authentication mechanism. The fundamental problem with that scheme is that it is either insecure because users choose to use easy-to-remember passwords (and therefore insecure passwords) or it is not easy-to-use because users need to remember difficult passwords (secure passwords). Recently, new specifications arose that aim to provide secure authentication while being easy-to-use. Specifically, the FIDO Alliance provides the FIDO UAF specification (https://fidoalliance.org/specifications/overview/) which is a passwordless solution that enables IdPs to authenticate users using strong authenticators, such as biometrics (e.g., fingerprint). By combining the concepts of strong authentication (FIDO UAF) alongside with the delegation of authentication to IdPs allow for a more user-friendly and secure solution for end-users.

The OpenID Foundation identified the possibilities of the combination of these concepts and has recruited a working group, called Enhanced Authentication Profile (EAP) Working Group that aims to enhance the OpenID Connect specification in order to enable IdP's to use strong authentication specifications. Our current work in the ReCRED project (http://www.recred.eu/) aligns with this working group. To this end, we provide a proof-of-concept implementation of an OpenID Connect implementation that is used in conjunction with a strong authentication specification, namely FIDO UAF. Below we provide an overview of the proposed solution with adequate technical details that can be of great significance for the OpenID Foundation and specifically for the EAP Working Group. Furthermore, we make our code publicly available under Apache 2.0 license. The code is publicly available on GitHub (https://github.com/zsavvas/ReCRED_FIDO_UAF_OIDC) with sufficient documentation for the installation of the different components

2. ARCHITECTURAL OVERVIEW

In this work, we focus on the architecture of the IdPs. The IdPs need to provide the OpenID Connect Provider functionalities while at the same time providing strong authentication mechanisms. Due to this, we propose the deployment of 2 different components on IdPs; the OpenID Connect Provider and the FIDO UAF Server. Figure 1 depicts the proposed architecture for the Identity Providers

.

- **OpenID Connect Provider:** The OpenID Connect Provider functionality is realized by deploying the OpenAM software (https://forgerock.org/openam/). In our deployment, within the OpenAM software, we have implemented a custom authentication module, called FIDO UAF Custom Authentication Module, which is responsible for undertaking the authentication of the users according to the FIDO UAF specification. To achieve this, the custom authentication module communicates with the FIDO UAF Server using a REST interface.
- **FIDO UAF Server:** The FIDO UAF Server is responsible for performing the authentication of the user by communicating with the FIDO UAF client that runs on users' devices. We have a FIDO UAF implementation, inspired from the Ebay's implementation (https://github.com/eBay/UAF), and we plan to refine it and submit

it for certification during the next certification session of the FIDO Alliance (December 2016). Our implementation of the FIDO UAF Server is designed in a way that all operations are exposed using a REST interface. In that way, communication between OpenAM's FIDO UAF Custom Authentication Module and the FIDO UAF Server implementation is done in a straightforward manner.

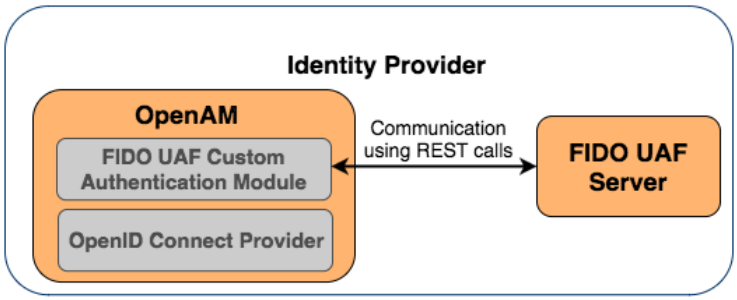

Figure 1: Identity Providers architectural components

3. DETAILED FLOW FOR AUTHORIZATION AND AUTHENTICATION

Figure 2 depicts the flow for the Authorization and Authentication of the user using the OpenID Connect and FIDO UAF specifications. Initially, the user use his device in order to visit a particular Service Provider *(Step 1)*. As the user tries to access a private area of the Service Provider available only to authenticated users, the Service Provider redirects the user to an Identity Provider that runs the OpenAM software *(Steps 2 and 3)*. Subsequently, OpenAM requires the user's username and the user provides it using his mobile app *(Steps 4 and 5)*. After the provision of the username, OpenAM provides the FIDO endpoint, which the user should use in order to authenticate *(Step 6)*. This allows enough flexibility to the Identity Provider as the FIDO Server instance might be running on another provider or on another server. The mobile app, make use of the FIDO client implementation to communicate with the FIDO Server, which was provided by OpenAM, in order to perform the authentication according to the FIDO UAF specification *(Steps 7-10)*. Note that during these steps, the FIDO UAF Server and Client implementation exchange an Authentication ID (authID). This unique identifier is generated by the FIDO Server and it is used to uniquely identify an authenticated session. This authID is returned to the user's device *(Step 10)* and it is then provided to the OpenAM instance *(Step 11)* so that the OpenAM FIDO UAF Custom Authentication can verify that the user is authenticated *(Step 12)* by calling the /isAuthenticated endpoint on the FIDO UAF Server. If the user is authenticated with the specific authentication ID then the FIDO UAF Server returns a success message to the OpenAM *(Step 13)*, which subsequently ask for the user's consent to reveal attributes to the specific Service Provider *(Step 14)*. After the provision of the user's consent to the Identity Provider (Step 15) the user receives a TokenID from OpenAM (Step 16). Then the TokenID is provided to the Service Provider *(Step 17)* so that it can be used to get an authorization code from OpenAM. This is achieved by calling OpenAM's /authorize endpoint and providing a valid TokenID *(Step 18)*. Afterwards, OpenAM provides the authorization code to the Service Provider *(Step 19)*, which again calls OpenAM so that it can gain an Access Token. This is accomplished by calling OpenAM's /access_token endpoint *(Step 20)*. Subsequently, the Service Provider receives the Access Token from OpenAM *(Step 21)* and then it make use of the Access Token to retrieve the user's attributes by calling the /userinfo endpoint on OpenAM *(Steps 22 and 23)*.

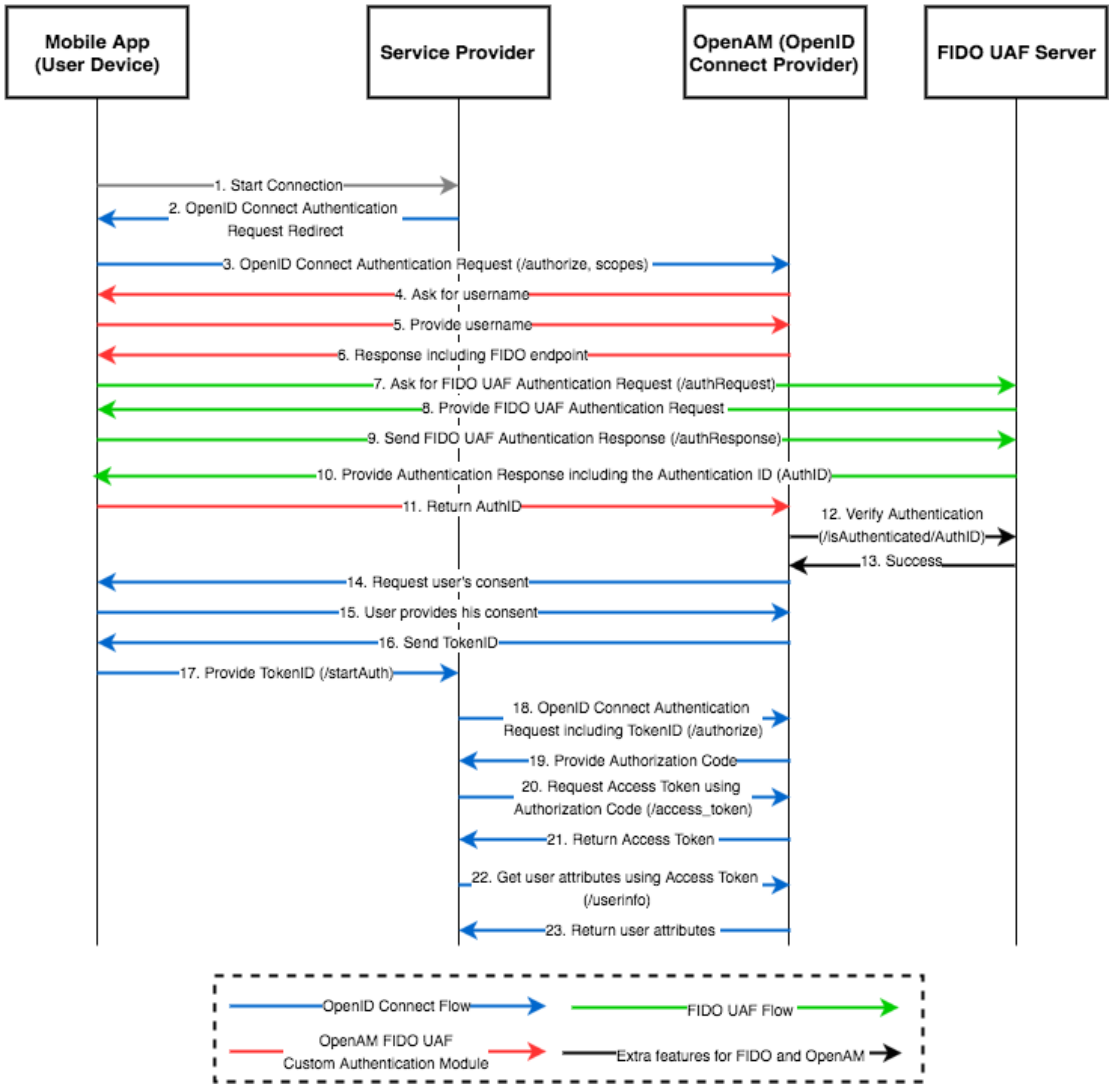

Figure 2:Authorization and Authentication flow using OpenAM and the FIDO UAF specification

4. CONCLUSION

In this document we describe the architectural design of the integration between two popular specifications, the OpenID Connect and the FIDO UAF. This integration enables the easy and secure delegation of authentication to Identity Providers. Furthermore, we make the code for providing this functionality publicly available (https://github.com/zsavvas/ReCRED_FIDO_UAF_OIDC). We argue that this work can be of great significance for the Identity Providers, for the OpenID Foundation and for the FIDO Alliance. To conclude, we encourage interested parties, irrespectively of organization and affiliation, to contact the consortium if they are interested to use, contribute or provide feedback to our implementation.

5. ACKNOWLEDGMENTS

This research has been fully funded by the European Commission as part of the ReCRED project (Horizon H2020 Framework Programme of the European Union under GA number 653417).