Know Your Customer: Opening a new bank account online using UAAF

Romain Laborde, Arnaud Oglaza,
Samer Wazan, François Barrère,
Abdelmalek Benzekri,
University Toulouse III Paul Sabatier
{Romain.Laborde, Arnaud.Oglaza,
Samer-Ahmad.Wazan,
Francois.Barrere,
Abdelmalek.Benzekri}@irit.fr

David W. Chadwick
University of Kent
d.w.chadwick@kent.ac.uk

Rémi Venant
University of Le Mans
Remi.Venant@univ-lemans.fr

***Abstract*—Universal Authentication and Authorization Framework is a user-centric, privacy by design and decentralized system that allows anyone to easily benefit from a reliable digital identity made of multi-purpose and multi-origin attributes. In this article, we present the implementation of this framework in the context of online banking. We demonstrate how it can facilitate enforcing Know Your Customer when opening a new bank account online by allowing users to combine verifiable identity attributes issued by different organizations.**

***Keywords*—Know Your Customer, Federated Identity Management, FIDO UAF, Verifiable credentials**

I. Introduction

EU Directive 2015/2366 (Payment Service Directive 2 - PSD2) aims at making international payments easy, efficient and secure. It also seeks to open up payment markets to new entrants leading to more competition, greater choice and better prices for consumers. As consequence, European banks have to open their information systems and move to this new electronic payment market.

Nevertheless, the high level of security required by the regulations impacts the usability of the services. For instance, Know Your Customer guidelines require the banks to strongly verify the identity of its clients to prevent money laundering activities. As a consequence, opening a new bank account is a currently time-consuming and painful procedure for users even when it is done online. With the help of our partner iBP (Informatique Banque Populaire), we could study a process enforced by a French bank compliant with the related national and international regulations. In order to make the payment system highly secure, the current process for opening a new bank account online requires strong evidence about the identity of the future customers and relies on digital copies of official documents. However, uploading these documents during the registration is tedious and degrades the user experience, especially with mobile devices. In addition, the uploaded documents must be verified by human operators, which takes 4 or 5 days, before the bank account is created.

Federation of identities could facilitate this process. Users can authenticate using a single Identity Provider (IdP), that centralizes all the identity attributes of the user. Then, these attributes can be used to identify the user to a new bank that is in the same federation as the IdP. However, today's federated identity management (FIM) systems have a significant structural weakness, namely, the placement of the IdP at the centre of the identity ecosystem. First, the trust model requires the IdP to trust the Service Provider (SP) to preserve the privacy of the user's identity attributes that it is asserting, and the SP to trust that the IdP is the authoritative source of (all of) the user's identity attributes. Both of these trust requirements are unreasonable. Secondly, the IdPs are the centre of the identity eco-system, and issue short-lived identity assertions or tokens on demand to trusted SPs. Consequently, they know when and which SPs the user is visiting, and thus are able to track the user. Finally, users cannot easily combine attributes from multiple IdPs which constrains users to centralize all their attributes in a unique IdP.

We think that 1) placing the user at the centre of the identity ecosystem, and 2) splitting omnipotent IdPs into small and specialized Attribute Authorities (AA) or Issuers is the only architecture that can ubiquitously succeed in the long term. Hence, we have built a user and privacy-friendly identity system, called Universal Authentication and Authorization Framework (UAAF), that places the user at the centre and allows combining reliable attributes from multiple attributes issuers. It implements the new W3C Verifiable Credentials standard [1] using an extension of the FIDO UAF protocol [2]. More information about UAAF can be found in [3].

II. Demonstration

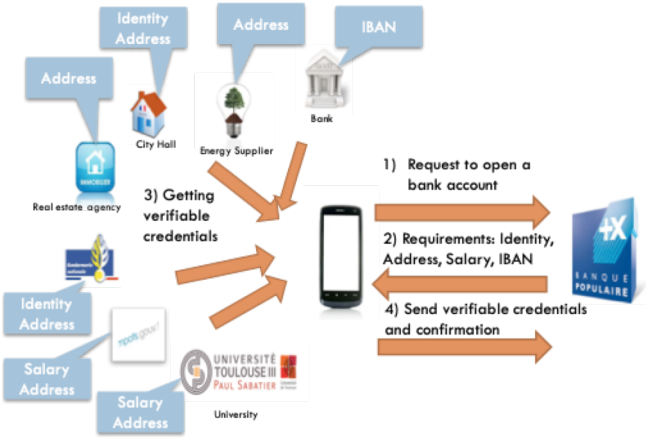
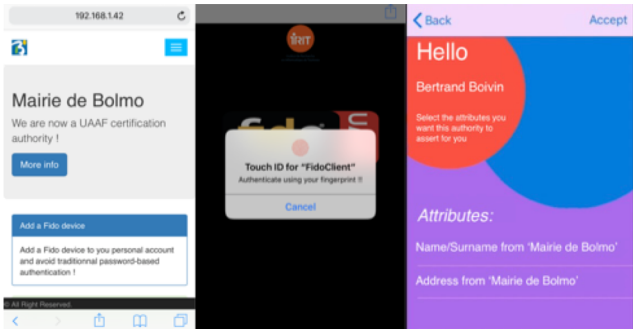


Figure 1: The "opening a new bank account" use-case

The scenario of our demonstration use case changes the current online bank account opening process which consists in the following steps. The future client starts by filling manually forms to provide all the information requested by the bank. Since all this information needs to be verified, the client has to provide digital copies of official documents and upload them to the bank server. However,

these documents contain much more information than actually needed by the bank.



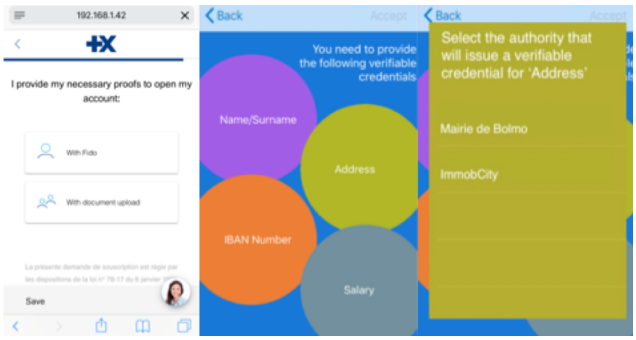
(a) (b) (c)

Figure 2: Screenshots of the enrollment process on the AA "Mairie de Bolmo"

Instead of providing documents, users present fine grained certified identity attributes such as name/surname rather than the ID card. A lot of existing organizations can assert verifiable credentials in our daily life. For instance, Universities assert diplomas or student status, utility companies or city hall can assert user's name or address, etc. In our ecosystem, all these organizations can become Attribute Authorities (AA) and provide certified attributes. In our new process (fig. 1) used in the demonstration, the user starts by registering her device on each AA she already knows. For instance, she can go to her city hall and register her device using an OTP provided by a city official (Fig. 2(a)). The user is then asked to authenticate (here using TouchID) to create the FIDO key pair for the city hall (Fig. 2(b)). When the city hall receives the public key, it sends the list of assertable attributes back to the user (see fig. 2(c)). In our demonstration, the user registers her device at her city hall (here Mairie de Bolmo), an energy supplier (here GreenElectricity), her current bank (here 'my online bank'), and her real estate agency (here ImmobCity).

- When the user wants to open a new bank account, she connects to the new bank web site. After asking some legal questions, the new bank website will start the UAAF process (fig. 3(a)). The UAAF client of the user then creates a key pair for the new bank website and transmits the public key to the web site. Then, the new bank web site sends its authorization policy to the user (fig. 3(b)) where it asks for four verifiable credentials:
- a proof of identity (name/surname) issued by either a city hall or the National Gendarmerie;
- a proof of address issued by either an energy supplier, a city hall, an accredited real estate agency, the French National Gendarmerie, the French tax department or a University;
- a proof of salary issued by either the French tax department or a University;
- and the IBAN number of the current user's bank account.

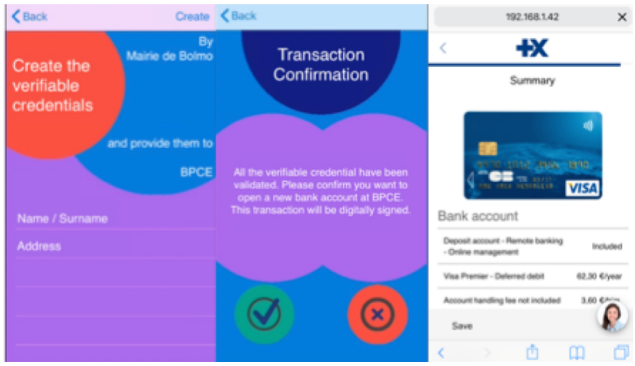
For each requested attribute, the user can select the AA that will issue the related verifiable credential (fig. 3(c)). The UAAF client only presents the list of AAs trusted by the SP that matches the registered AAs. In our case, the user can only select Mairie de Bolmo or ImmobCity (fig. 3(c)). Once the AAs are selected, the user will generate signed verifiable credential requests (fig. 4(a)). For each request, the user will be asked to authenticate using the TouchID or other authentication methods so that the UAAF client can use the private key for the respective AA to sign the messages. When all the verifiable credentials have been retrieved, they are transmitted to the new bank web site. In our use-case, the new bank website shows a transaction confirmation message (fig. 4(b)) once it verified the credentials. If accepted, the user signs the transaction confirmation using her new bank's private key. She is seamlessly redirected to the bank website, all her information is automatically extracted from the verifiable credentials. Finally, she can use her new bank account straightaway (fig. 4(c)).



(a) (b) (c)

Figure 3: Screenshots of the SP's authorization policy

We implemented the AA and SP servers using the popular Spring framework. The FIDO UAAF client is available on Android (version 6.0 and higher) and iOS (version 10.3 and higher).



(a) (b) (c)

Figure 4: Screenshots of the verifiable credentials' creation and transaction confirmation

References

[1] W3C, « Verifiable Credentials Data Model 1.0 - Expressing verifiable information on the Web », February 2019

[2] FIDO Alliance. « FIDO UAF Architectural Overview. » FIDO Alliance Proposed Standard. 8 December 2014

[3] R. Laborde, A. Oglaza, D. W. Chadwick, R. Venant, S. Wazan, F. Barrère, A. Benzekri, "A User-Centric Identity Management Framework based on the W3C Verifiable Credentials and the FIDO Universal Authentication Framework", In CCNC 2020, to appear