CANADIAN MOBILE CONNECT COMMERCIAL PILOT

CASE STUDY

Mobile Connect technology allows end users to login to online resources using their mobile device. The most wide spread computing device can be turned into an authentication token. The ability to use a device you carry with you at all times for online authentication can mitigate risk in online transactions and can improve customer experience and trust.

Usability

User acceptance through effortless registration and ease-of-use during authentication was seen as the key success factor in the Canadian pilot. A lot of emphasis was put on perfecting the user experience. One of the biggest obstacles in conversion for any online service is registration. The registration of the Mobile Connect user in the Canadian pilot is completely mobile centric and takes less than a minute.

Security and Trust

The Mobile Connect protocol itself is built based on a privacy-by-design approach. Beyond the Mobile Connect protocol there are steps that can be taken to bolster both security and the trust towards the end users even further. One of the biggest improvements over SIM based or SMS –type of authenticators in the Canadian pilot is the logo usage.

Due to the nature of the Mobile Connect ecosystem where the main actors are the online service, GSMA discovery service, the mobile network operator and the end user with the mobile device the authentication process might lose the information on where the end user is actually logging into. With the smartphone app authenticator and the identity gateway, the Canadian pilot allows the end user to see the identity provider (mobile network operator) and the target service logos during the authentication. This will create trust as the end users can verify that they are accessing the correct service.

The Canadian pilot uses a smartphone app authenticator from MePIN. The app itself uses multiple techniques to increase internal security and it has been audited several times. For the end user the app provides a very convenient way to authenticate themselves. The end user can use a PIN code or biometrics depending on the device capabilities. The PIN code (separate from the phone unlocking PIN) and the biometrics are only used to unlock the PKI private key for signing the authentication request. All transactions in the Canadian pilot are signed by a PKI private key.

EnStream UBISECURE mepin

The Canadian Mobile Connect Commercial Pilot led by EnStream LP – a joint venture of Bell Mobility, Rogers Communications and TELUS Communications is now in pilot phase for authentication in Canadian e-services using components provided by Ubisecure and MePIN. The service is the first Mobile Connect deployment in the world that uses a Smartphone App Authenticator (SAA) for registration, authentication and account recovery, and has deep integration into mobile operator subscriber verification services.

FOCUS GROUP FEEDBACK

In a study conducted by Akendy before the launch of the pilot, end users gave the grade of **8.6/10** for the usability of the smartphone app authenticator.

"Better than a password keeper"

"What can be better than a technology KEEPING all your data secret"

Consent

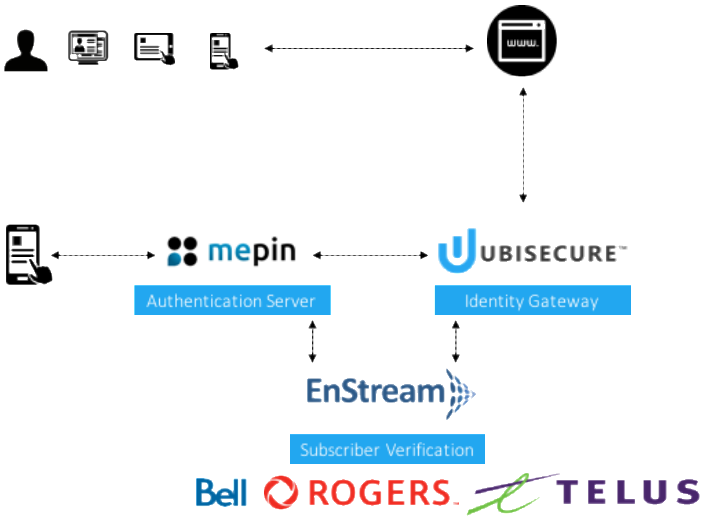
One key aspect of Mobile Connect is consent. When the end user allows that his mobile connect identity can be used to login into a service, he gives his consent. With the Canadian pilot, the end users can manage these consents through their smartphone app using the data provided by the identity gateway. This again increases trust.

Edge Cases

Mobile Connect is a protocol to implement global and federated authentication. Beyond Mobile Connect there are multiple edge cases that need to be supported to make the overall system usable. People lose their devices, they buy new ones and hand down their old one to a family member, they switch operators, have multiple devices etc.

Supporting these edge cases is essential for the success of the Mobile Connect adoption for a wider audience.

"The implementation reflects strong collaboration among the providers as well as the participating mobile network operators. We are all focused on developing an exceptional user experience that enhances convenience, security and privacy, while also integrating seamlessly into the online service providers' brand experiences," - Robert Blumenthal, Head of Digital Identity and Authentication Services at EnStream."



90% successful login and link to existing accounts

74% continue to use Mobile Connect

30% higher usage of TELUS.COM vs. previous usage

< 3 seconds latency for 90% of transactions

EnStream UBISECURE mepin

MINIMUM SOLUTION CRITERIA BY ENSTREAM

Broad coverage of mobile subscribers across Bell, Rogers & TELUS (together > 90% of Canada)

Easy to deploy

Easy integration with Relying party

Best in class user experience, security & privacy

Brand-friendly for Relying Parties

SPECIFICATIONS

Identity Gateway

Ubisecure Identity Server

Smartphone App Authenticator

Meontrust MePIN app for iOS and Android

02.2017