MOBILE CONNECT

THE SIMPLE, SECURE, UNIVERSAL LOGIN SOLUTION WITH PRIVACY PROTECTION

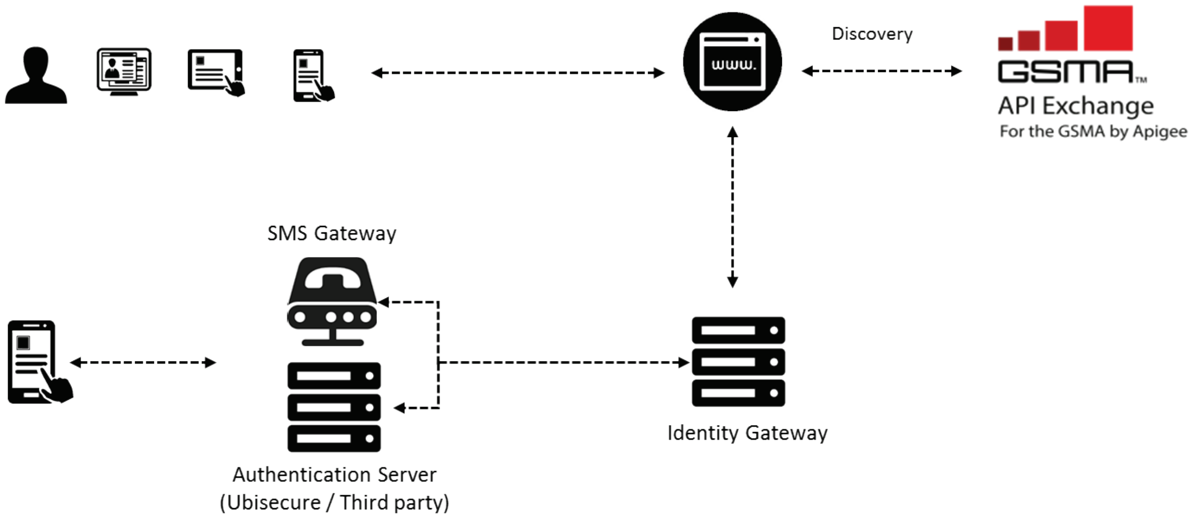
WHITE PAPER

UBISECURE™

Connecting Identity.
Transforming Digital Business.

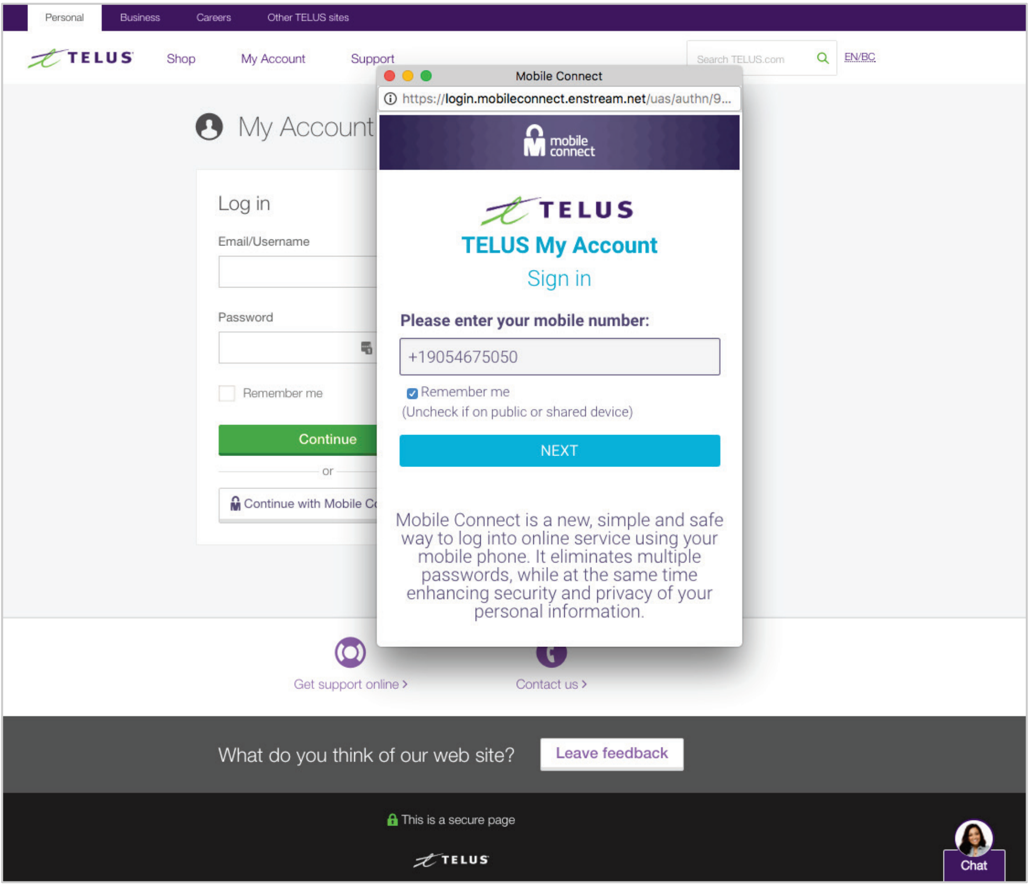
INTRODUCTION

There is no more ubiquitous computing device than a mobile phone. Mobile Connect is an emerging global standard led by the GSMA that turns your phone into a user-friendly identity and authentication device for a wide range of consumer and business applications. Currently supported in countries covering over 3 billion mobile users, Mobile Connect promises to provide a truly ubiquitous solution to help consumers and business alike improve access to online services by eliminating passwords, and providing increased security, privacy and identity assurance.



WHAT IS MOBILE CONNECT?

Mobile Connect is protocol based on OpenID Connect, that uses the mobile number (MSISDN) as the user ID for global and federated authentication. Mobile Connect standards are developed in the MODRNA group.



https://login.mobileconnect.enstream.net/uas/authn/9...

TELUS My Account

Sign in

Please enter your mobile number:

+19054675050

☑ Remember me

(Uncheck if on public or shared device)

NEXT

Mobile Connect is a new, simple and safe way to log into online service using your mobile phone. It eliminates multiple passwords, while at the same time enhancing security and privacy of your personal information.

What do you think of our web site?

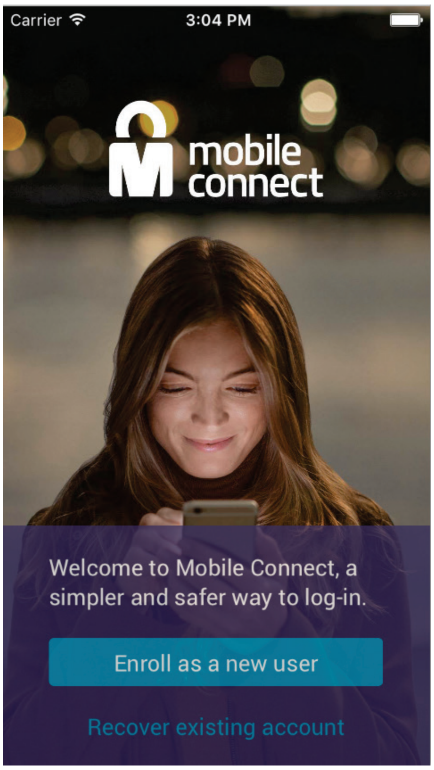
GLOBAL AND FEDERATED

Mobile numbers (MSISDN) are globally unique numbers issued mobile network operators. Mobile Connect allows online service providers to send authentication requests securely to mobile users on participating mobile networks with the help of the GSMA discovery service, which determines to which

mobile operator a mobile number belongs in real-time. For example, an online service located in Singapore can authenticate a Mobile Connect user from a Canadian mobile operator.

AUTHENTICATORS

Each market is different. In many developed countries, smart phone penetration is quickly approaching 100%, whereas in developing markets inexpensive feature phones are prevalent. Mobile Connect allows each mobile network operator to deploy a suitable authenticator for their subscribers based on market demand. The authenticators range from simple SMS –based methods to advanced smartphone app authenticators (SAA) using biometrics and PKI. It is up to the mobile network operator to select the appropriate authenticators for their markets, and there can be more than one authenticator deployed by an operator.



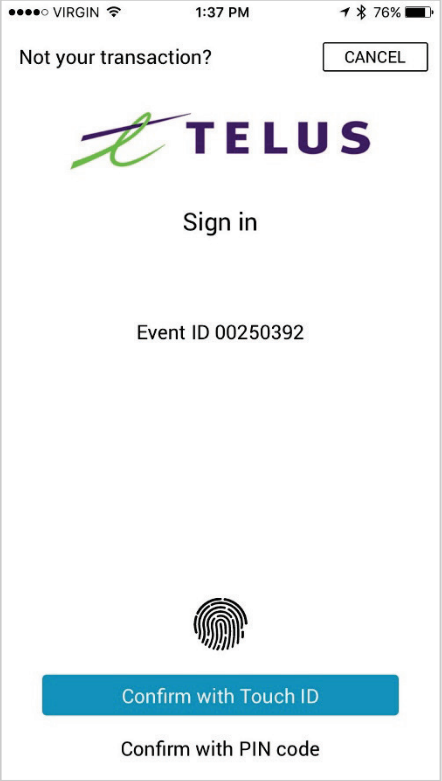
IDENTITY GATEWAY

The glue between the online service provider and the mobile device-based authenticator Identity Gateway. It is the primary interface for service providers to send requests for authentication and authorization by Mobile Connect users, routing the request to the appropriate authentication server corresponding to the particular user based on the capabilities of their device and how they enrolled with the Mobile Connect service. If the operator has chosen to deploy more than one authenticator, the Identity Gateway is responsible for sending these requests to the correct authenticators.

The Identity Gateway performs other important functions such as verifying subscriber status (phone number is active), collecting end-user consent, verifying identity, delivering identity attributes, providing geolocation data for the online service. It may also provide the mechanism to deliver media-rich branding in support of the online service provider and/or mobile operator.

BENEFITS OF MOBILE CONNECT

For mobile network operators, Mobile Connect represents a new business opportunity. Mobile network operators (MNOs) throughout the world possess a treasure trove of valid identity information including customers' the standard name, address, e-mail and phone number, but also data that can be mitigate risk in online transactions such as geolocation (phone is in another country than the transaction) or how long the user has been a customer (establish reputation score).



Mobile Connect can also help reduce friction and user engagement at the MNO's own services, by making it easier for customers to get access to online and mobile-based services. Better engagement and increased usage means greater potential to upsell new and enhanced services.

The true potential as a new business for the MNO lies in the combination of user friendly authentication and commercialising the identity information. End users will like the mobile oriented authentication that increases security. They will appreciate the smooth registration experience. They will trust the solution as it puts the end user in control of consents.

For the online service providers, Mobile Connect can already provide access to billions of enabled users globally with better, more secure, login to existing online services. Mobile Connect can also be used to streamline new user registration, using identity attributes verified by the mobile operator available through the Mobile Connect service, with integrated end-user consent. The result is lower abandonment rates, increased registration and customer satisfaction with a higher level of identity assurance to mitigate against identity fraud and account takeovers, and streamline account recovery.

TRUST, SECURITY AND PRIVACY

End-user consent is at the heart of Mobile Connect – providing trust and end-user control. Unless the user provides consent, no personal informational about a user is shared with the online service provider, including their mobile number. Each link created to an online service also requires consent. Consent is managed by users through a user interface provided by the Identity Gateway, allowing users to control where they go and what information is shared with whom at all times.

Mobile Connect also enhances privacy from the ground up. It uses anonymous identifiers (the Pseudo-anonymous Customer Reference, or PCR) as an alias to represent users at online service providers, which can be linked to existing or new accounts, effectively replacing existing password authentication mechanisms. PCRs are unique for each user at each online service provider in order to prevent link-ability and trace-ability of where users go when using Mobile Connect.

From a security perspective, Mobile Connect uses best-in-class technologies to ensure the highest level of authentication assurance. First, in addition to being convenient for users, the mobile device is an "out-of-band" authentication device, not susceptible to man-in-the-middle or man-in-the-browser attacks common with password as well as second factor OTP solutions. Second, the authenticator uses advanced security protocols such as PKI and biometrics to prevent the unauthorized device and users from authenticating or authorizing transactions, without compromising user convenience of a single tap, PIN or thumb to login.

EDGE CASES

Mobile Connect is a protocol. Implementing and deploying a solution that just implements the protocol is not enough for a successful Mobile Connect solution. Edge cases need to built-in to the final production deployment. The Mobile Connect deployment should support and survive cases where people lose their devices, hand them to someone else, switch operators, have multiple devices, change subscriptions etc.

CASE STUDY –TELECOMS COMMERCIAL PILOT

The Canadian Mobile Connect Commercial Pilot where Ubisecure Identity Platform provides the Identity Gateway functionality was nominated as a finalist in the Global Mobile Awards.

86%

FOCUS GROUP SCORE FOR THE IN THE CANADIAN MOBILE CONNECT COMMERCIAL PILOT USING SMARTPHONE APP AUTHENTICATOR (SAA)

30%

INCREASED USAGE OF ONLINE SERVICE APPLICATIONS BY MOBILE CONNECT USERS IN UBISECURE'S CANADIAN TELECOMS COMMERCIAL PILOT

74%

USERS CONTINUE TO USE MOBILE CONNECT AFTER THE FIRST TIME IN UBISECURE'S CANADIAN TELECOMS COMMERCIAL PILOT

CONCLUSION

Mobile Connect has the potential to change how we think about online authentication on a global basis. Mobile network operators can create new business and services with Mobile Connect. Online service providers have a real and already wide-spread alternative to implement not just convenient and secure authentication, but also smooth registration.

As a mobile network operator you need a feature rich and proven Identity Gateway solution that is easy and quick to deploy and supports the edge cases out of the box. Depending on your market you then need to select the appropriate authenticators to cover your subscriber base.

Contact Ubisecure today to hear how we can help you as a mobile network operator to become also an identity provider in your market.

UBISECURE™

Ubisecure is a pioneering European b2b and b2c Customer Identity & Access Management (CIAM) software provider and cloud identity services enabler dedicated to helping its customers realise the true potential of digital business.

Ubisecure provides a powerful Identity Platform to connect customer digital identities with customer-facing SaaS and enterprise applications in the cloud and on-premise. The platform consists of productised CIAM middleware and API tooling to help connect and enrich strong identity profiles; manage identity usage, authorisation and progressive authentication policies; secure and consolidate identity, privacy and consent data; and streamline identity based workflows and decision delegations. Uniquely, Ubisecure's Identity Platform connects digital services and Identity Providers, such as social networks, mobile networks, banks and Governments, to allow Service Providers to use rich, verified identities to create frictionless login, registration and customer engagement while improving privacy and consent around personal data sharing to meet requirements such as GDPR and PSD2.

Ubisecure is accredited by the Global Legal Entity Identifier Foundation (GLEIF) to issue Legal Entity Identifiers (LEI) under its RapidLEI brand, a cloud-based service that automates the LEI lifecycle to deliver LEIs quickly and easily. The company has offices in London and Finland.

To learn more about Customer IAM and Company Identity solutions visit www.ubisecure.com or contact us at info@ubisecure.com