

MOBILE CONNECT

THE SIMPLE, SECURE, UNIVERSAL LOGIN SOLUTION
WITH PRIVACY PROTECTION

FEATURING THE CANADIAN MOBILE CONNECT COMMERCIAL PILOT

UBISECURE WHITE PAPER

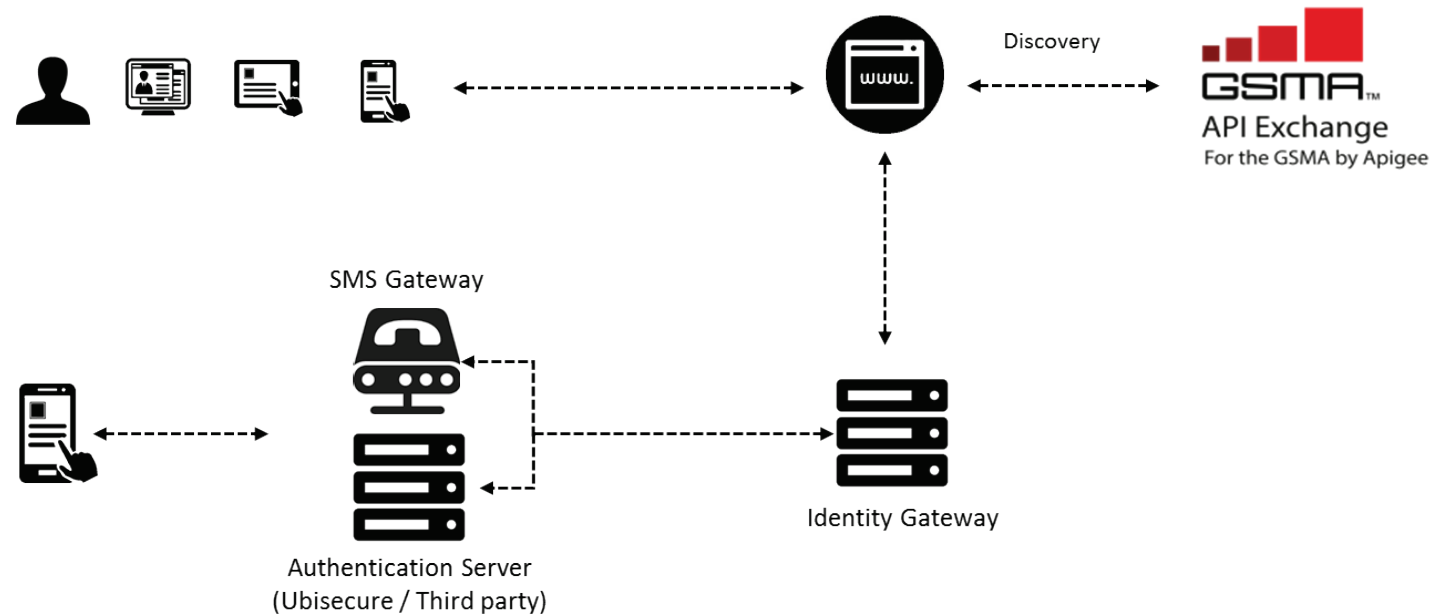


8,64 / 10

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

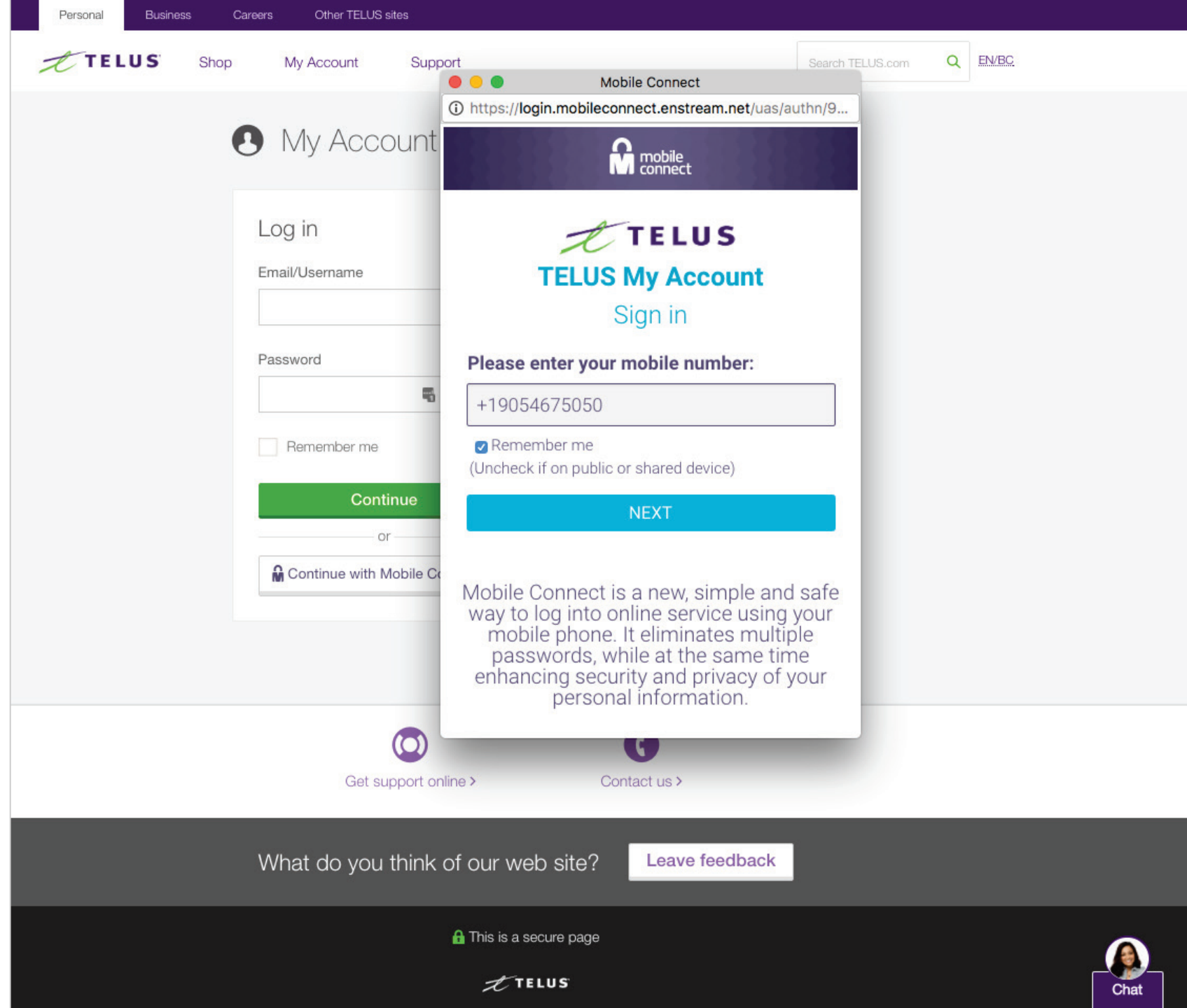
INTRODUCTION

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](#).





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

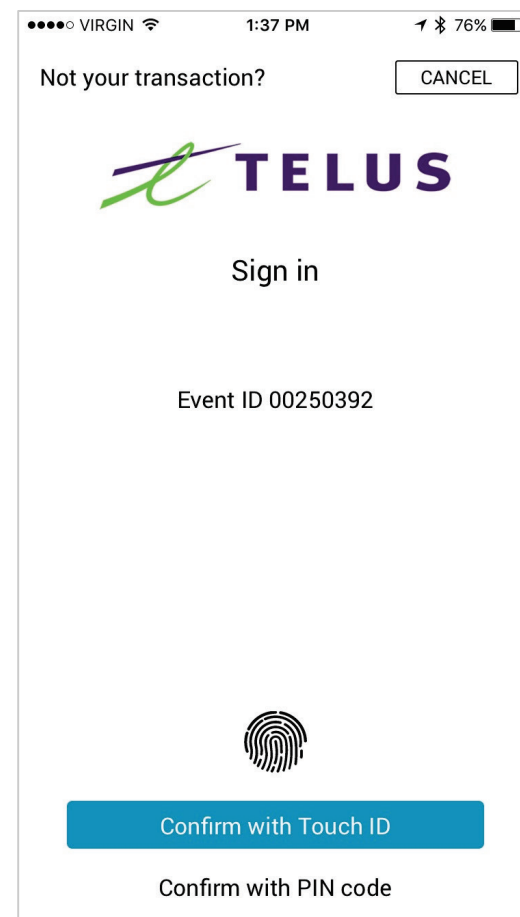
Each market is different. In many developed countries, smart phone penetration is quickly approaching 100%, whereas in developing markets inexpensive feature phones are prevalent. Mobile Connect allows each mobile network operator to deploy a suitable authenticator for their subscribers based on market 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.



30%

INCREASED USAGE OF
ONLINE SERVICE
APPLICATIONS BY MOBILE
CONNECT USERS IN THE
CANADIAN COMMERCIAL
PILOT



BENEFIT 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.

74%
OF USERS CONTINUE TO USE
MOBILE CONNECT
AFTER THE FIRST TIME IN THE
CANADIAN COMMERCIAL
PILOT

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 information 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.

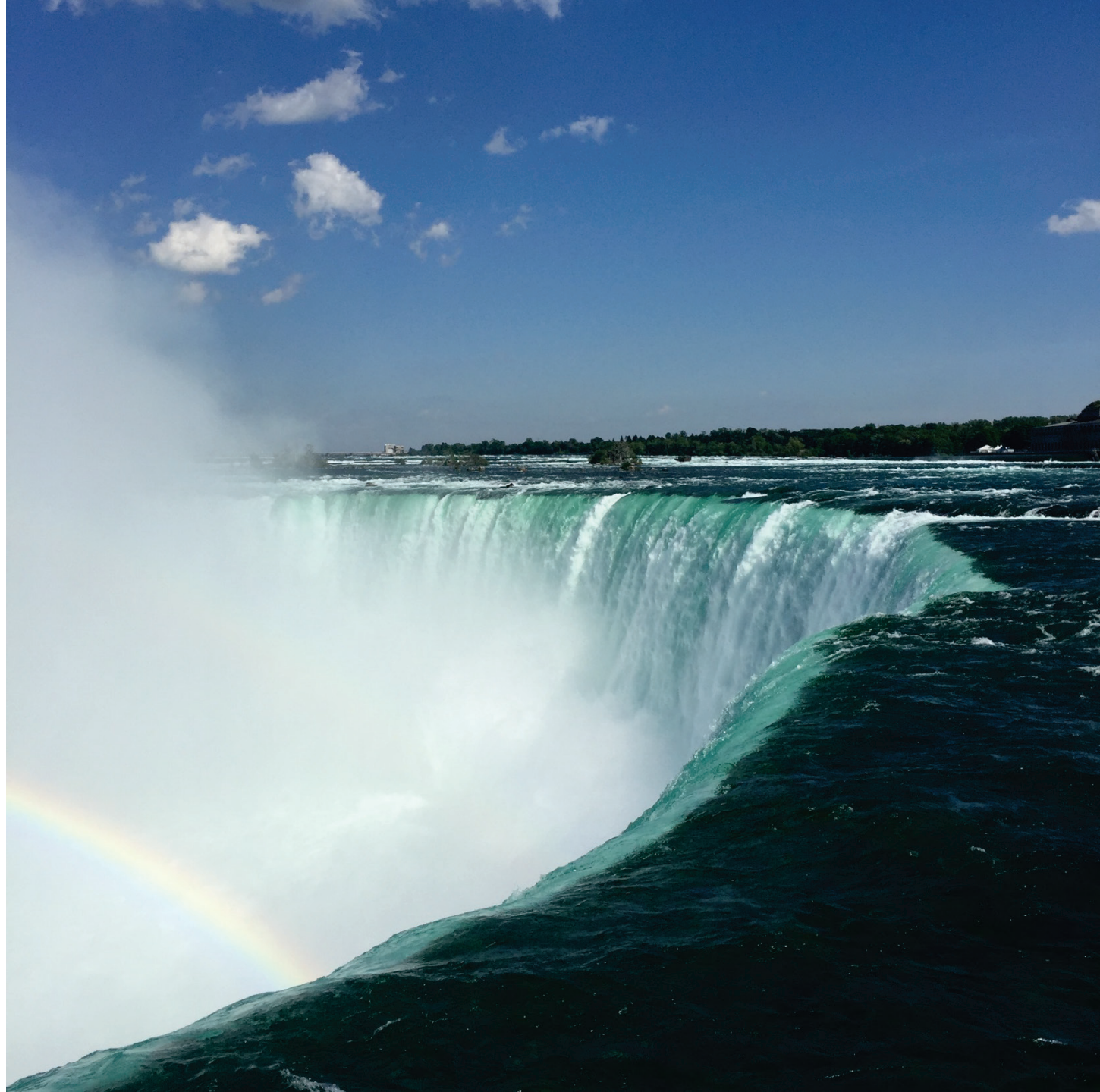
Mobile Connect also enhances privacy from the ground up. It uses anonymous identifiers (the Pseudo-anonymous Customer Reference, or PCR) as an alias to represent users at online service providers, which can be linked to existing or new accounts, effectively replacing existing password authentication 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 be 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.





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.

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



“

THERE ARE BILLIONS OF ONLINE AND MOBILE IDENTITIES AND THEY EXIST IN FRAGMENTED DOMAINS, SEPARATE ECOSYSTEMS DESIGNED FOR INDIVIDUAL PURPOSES.

WE SEE A WORLD OF DIGITAL TRANSFORMATION DRIVEN BY THE NEED FOR CUSTOMER/USER SERVICE. KEY TO THAT PROCESS ARE THE TENANTS OF SECURITY AND SIMPLICITY. SERVICE PROVIDERS ARE LOOKING TO EVOLVE, EMBRACE AND EMPOWER THEIR USERS, AND IN DOING SO INCREASE THE EFFICIENCY AND PROFITABILITY OF THEIR CUSTOMERS.

THE ABILITY TO OUTSOURCE IDENTITY, LEVERAGE THE SECURITY OF PROVEN PLAYERS, AUTOMATE THE MAINTENANCE AND ONBOARDING OF NEW IDENTITIES IS KEY TO THE EFFICIENT AND COST EFFECTIVE IMPLEMENTATION OF A DIGITAL TRANSFORMATION STRATEGY.

UBISECURE HAS PROVEN CAPABILITIES TO PUT IDENTITY AT THE BEGINNING OF EVERY DIGITAL TRANSFORMATION.

Simon Wood
Group CEO, Ubisecure



ABOUT UBISECURE

UbiSecure is a global Identity & Access Management software and cloud services provider. UbiSecure technology makes using online identities easier, safer and more private for consumers. It helps businesses improve user experience and reduce costs through increased customer engagement, loyalty and insight and it helps service providers benefit from simplified registration, login and attribute sharing from the rich identities already being used online. It helps create trusted connections between digital services, devices and mobile identity. When these modern aspects of identity management are combined, UbiSecure enables the true potential of digital business. The company headquartered in Finland works through a network of local and global system integrator partners and has offices in the UK.

CONTACT US

www.ubisecure.com
sales@ubisecure.com

Tekniikantie 14
02150 Espoo
Finland

The Granary, Hermitage Court
Hermitage Lane, Maidstone
Kent, ME16 9NT, UK

