

GMSA MOBILE CONNECT IDENTITY GATEWAY

PRODUCT DATASHEET

Powering how Mobile Network Operators & Service Providers benefit from the new standard in digital authentication

In the world of digital business, nothing is more prevalent than the mobile phone. The GSMA Mobile Connect program can turn this ubiquitous device and the mobile identity it holds into a versatile, easy to use authentication device for billions of people. Mobile Connect allows people to log-in to websites and applications quickly without the need to remember multiple usernames and passwords. It's safe, secure and no personal information is shared without permission.

UbiSecure's Mobile Connect solution, built on the scalable identity management and authentication solution available through the UbiSecure Identity Platform, allows Mobile Network Operators (MNOs) to quickly deploy feature rich Mobile Connect services. Such MNOs become true identity providers and can leverage new revenue streams and offer increased customer convenience across large numbers of service providers.

UBISECURE MOBILE CONNECT IDENTITY GATEWAY BENEFITS

- Product based solution and no custom development needed enabling quick deployment
- Enables the mobile network operator to become a true identity provider
- Both on-premise and MCX deployments supported
- Out of the box support for mobile specific use cases outside of Mobile Connect
- Authenticators can be deployed or changed in seconds
- Supports online services, desktop applications, mobile apps and IoT

SUCCESS STORY

Mobile Connect Canada Pilot

The service is powered by an Identity Gateway provided by UbiSecure and the smartphone app authenticator by MePIN. The combination enables users to get started quickly and incorporates the mobile network operator brand as well as the e-service brand to be visible throughout the authentication event. This increases brand recognition for the participating providers and enhances trust as the end user is properly informed to which service they are logging into.

"The <Mobile Connect> 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



FOR MOBILE NETWORK OPERATORS

Mobile Connect provides mobile networks operators with the possibility of offering convenient end-user authentication services to their service provider customers from local e-commerce sites to online banking. By adding Mobile Connect to the product portfolio mobile network operators can become a true identity providers. With Ubisecure Identity Gateway, mobile network operators can become a central hub of identities for online commerce, banking and insurance, e-government, apps, Internet of Things (IoT), APIs, or anything digital that requires authentication of users or entities.

Ubisecure's proven Mobile Connect Identity Gateway can be easily integrated to mobile network operators' CRM, or other back-end systems, enabling the enrichment of user data and attribute services and provide online services the GSMA defined (Mobile Connect Release 2) products "Identity" and "Sign Up". Beyond authentication these products allow online services to streamline their registration flows and reduce the #1 reason for cart abandonment and therefore increase their revenue. Online services that require strong user authentication will benefit from the authenticators available through mobile network operators and provide their own customers a cost efficient, convenient and secure authentication.

Finance, insurance, energy, healthcare, and many other vertical industries demand convenient, yet secure alternatives to passwords. The authentication and identity verification options with Mobile Connect offer a toolkit to implement multiple levels of authentication and identity vetting for the online users from a simple swipe of the screen to biometrics, all of them utilizing the mobile phone of the end-user or the verified identity attributes of the subscriber.

For the Mobile Network Operator, Ubisecure brings in over 15 years of experience in delivering Identity and Access Management solutions to the service providers. Our customers spanning multiple verticals have created new online services and business models with help of our solutions. They have created considerable cost savings, improved customer experience, mitigated risk, achieved strategic goals, created world firsts, received awards for their innovations and more. A mobile network operator that wishes to become a trusted identity provider in their market will benefit from this experience.

GET STARTED WITH MOBILE CONNECT TODAY!

Get demos and more information at www.ubisecure.com or sales@ubisecure.com



About Ubisecure Inc

Founded in 2002, 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.

Tekniikantie 14 Espoo, 02150 Finland | The Granary, Hermitage Court, Maidstone Kent, ME16 9NT, UK
E: sales@ubisecure.com | T: +358 9 251 77250 | www.ubisecure.com

SPECIFICATIONS

Mobile Authentication

Swipe/Tap to Confirm (iOS, Android)*

HTTP Header silent authentication

USSD

PIN (iOS, Android)*

SMS+URL

SMS OTP (all platforms)

Fingerprint (iOS, Android)*

Face recognition (iOS, Android)*

FIDO U2F (iOS, Android)*

Mobile PKI (SIM based, ETSI MSS, all platforms)

Offline methods: TOTP (Time-based One-Time-Password, does not require a mobile network connection)*

*Uses Smartphone App Authenticator

Other Authentication Methods

Username and password

Social login (Facebook, Google, LinkedIn, Twitter...)

Business login (Office365/Azure, Google for Business, Windows AD, smart card / token)

National eIDs (BankIDs, eID cards, Mobile PKI)

OTP print-out list

Supported WebSSO and Federation protocols

SAML, WS-Federation, OpenID, OAuth,
OpenID Connect, Mobile Connect