OneSpan

FIDO Authentication

A complete portfolio of mobile and hardware solutions based on FIDO standards for simpler, stronger authentication using an open, scalable, and interoperable approach

HIGHLIGHTS

Solutions based on FIDO standards provide you with simpler, stronger authentication using an open, scalable, and interoperable approach. Easily implement FIDO enabled authentication while ensuring a superb user convenience.

- Support for mobile and/or hardware deployments
- Supports major operating systems including Android and iOS
- Easy to integrate
- Future proof
- Central management of all authentication channels

OneSpan FIDO Authentication addresses the challenges banks and financial institutions face to offer secure mobile or online applications without compromising user convenience. Reducing end user friction is key to the success of any mobile and online application and has a profound impact on customer loyalty, satisfaction and new business opportunities.

The FIDO ecosystem

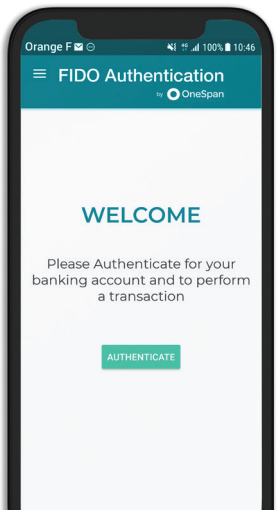
Organizations looking to replace traditional static passwords are confronted with a myriad of different proprietary clients and protocols. That is why the FIDO Alliance was founded. The idea was to create an interoperable ecosystem of hardware, mobile and biometrics-based authentication that can be used with a variety of online and mobile services. With this standards-based approach, any application can work with any device and any authenticator.

Create an unrivalled user experience

Reduce end user friction by offering your users the flexibility to use any FIDO compatible authenticator. OneSpan FIDO Authentication replaces traditional complex passwords with advanced authentication options, including biometrics, PIN and second factors. Mobile FIDO authentication enables passwordless experiences by using the native security capabilities present on end users' devices such as face recognition or fingerprint.

Strong security with privacy in mind

The different FIDO protocols use asymmetric public key cryptography. Upon registration, a private and public key pair is generated whereby the private key never leaves the device. As such, there are no server-side secrets to steal. There is also no linkability between the different series which means that no information is provided that would allow user tracking across different services. Biometric information is captured, stored and verified on the device and never sent to a server.



Cost reduction as an added bonus

Since you don't need to develop proprietary or in-house solutions your time to market for your online and mobile services offering will be shortened and development and maintenance costs will be reduced. OneSpan FIDO Authentication can be easily integrated alongside your existing mobile and web applications. By leveraging the end user's mobile device or using a second factor, provisioning cost are second to none. OneSpan FIDO Authentication eliminates the dependency on traditional complex passwords and as such severely reduces customer support for costly password resets..

Key benefits

- **Ease of use:** remove friction and offer your user the flexibility to use any FIDO-compatible authenticator or device
- **Standardization:** take advantage of the FIDO ecosystem that ensures interoperability of hardware, software and biometric authentication
- **Cost reduction:** use FIDO certified solutions and reduce operational costs while ensuring a faster time to market
- **Privacy and security:** provide stronger authentication with FIDO public key cryptography. Protect your apps against phishing, Man-in-the-Middle and replay attacks
- **Compliant with PSD2 and GDPR:** alleviate compliancy concerns and rely on standardized authentication to help you meet regulatory requirements
- **Future proof:** OneSpan Authentication is a standards based solution that allows you to deploy FIDO authentication to your customer base on multiple devices. New authentication methods will be natively supported as they come onto the market.

OneSpan FIDO Authentication solutions

OneSpan FIDO Authentication solutions enable you to provide your user with a universal second factor (hardware) or passwordless (mobile) user experience by using the native security features present on the user's device. OneSpan's FIDO solution suite easily allows you to mix and match software and hardware to fit your authentication needs.

Mobile

FIDO capabilities are integrated into OneSpan Mobile Security Suite. This is a comprehensive developer's toolkit (SDK) and unique single framework that natively integrates application security, FIDO authentication and electronic signing into your mobile applications. This allows you to benefit, besides FIDO authentication, from all features that OneSpan Mobile Security Suite offers, and flexible deploy the security features your offering requires (i.e. geolocation, jailbreaking, device binding, secure storage and application shielding with RASP).

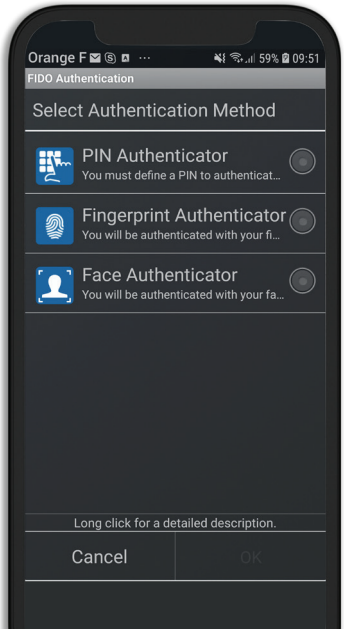
Hardware

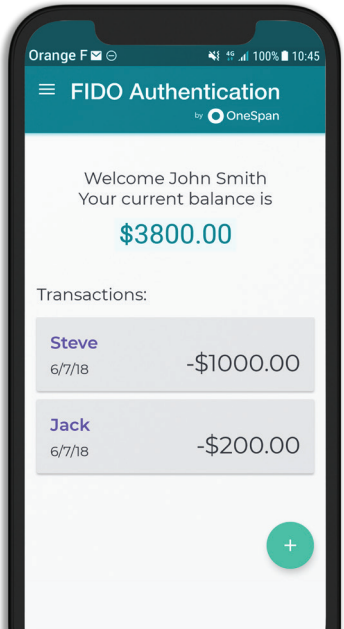
Digipass SecureClick is a FIDO U2F certified device, enabling users – with the single push of a button – to securely complete access to their online applications.

How it works

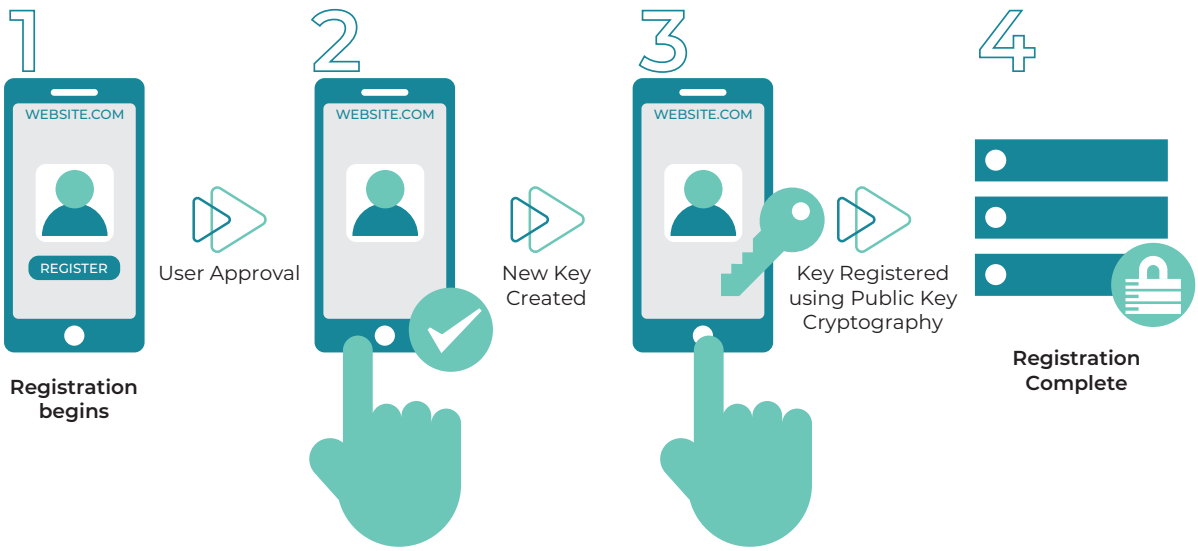
FIDO is a password replacement solution based on public key cryptography where the key stays on the device (whether it is hardware or mobile). There are no server-side secrets to steal and there is no link-ability between services or accounts.

In order to use FIDO authentication, the user must first register himself before logging on or validating transactions.





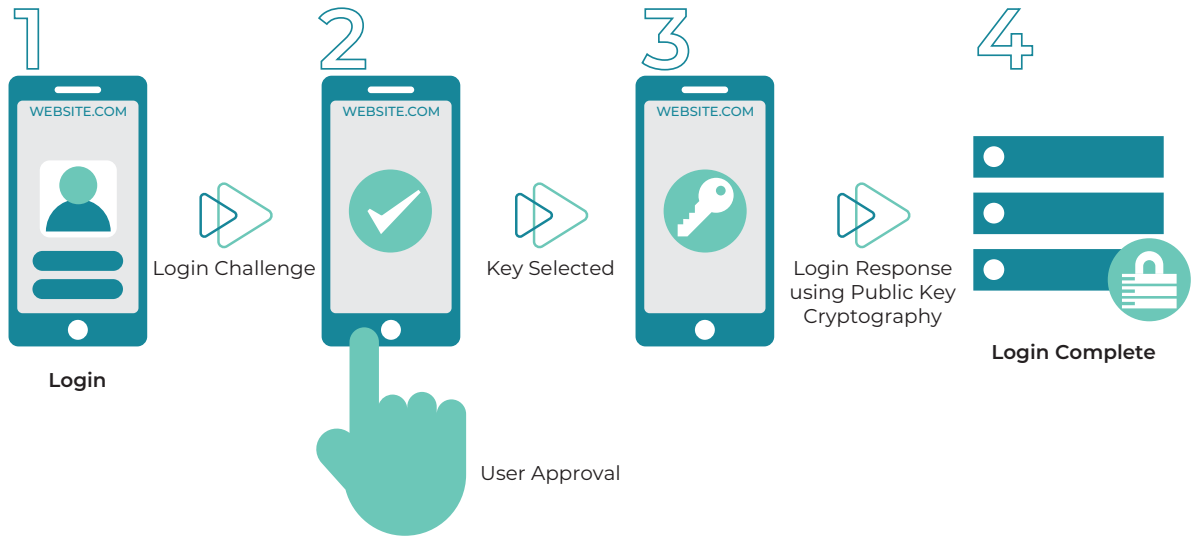
FIDO Registration



Registration

1. Request your user to choose an available FIDO authenticator in line with your acceptance policy.
2. Your user unlocks the mobile FIDO authenticator with a fingerprint reader or PIN; or with a button in case of a hardware second-factor device.
3. The user's device creates a unique private and public key pair for the local device, the user's account and your online or mobile service.
4. The public key associated with the user's account is sent to the server. The private key is stored on the local device in the cryptographic secure key store.
5. Your user unlocks his FIDO authenticator in the same manner as they did for registration (e.g. face recognition, fingerprint, PIN, second factor)

FIDO Authentication



Login

1. Your mobile or online service challenges the user to log in with a previously registered device.
2. Your user unlocks his FIDO authenticator in the same manner as they did for registration (e.g. face recognition, fingerprint, PIN, second factor).
3. The FIDO server creates a random challenge. To sign that challenge, the device uses an account identifier to select the correct key.
4. The signed challenge is sent back to the server where it's matched against the public stored key and the user is authorized to log in.

FIDO Transaction Verification

Transaction verification

1. After logging on, your user enters the transaction information which is sent to the relaying party.
2. A random challenge as well as the transaction information are created by the FIDO server and sent to the device for user approval.
3. Your user verifies the transaction on the display of the device. To sign that transaction, the device uses an account identifier to select the correct key.
4. The signed transaction is sent back to the server where it's verified against the public key and the transaction is validated.

About OneSpan

OneSpan, the digital agreements security company™, helps organizations accelerate digital transformations by enabling secure, compliant, and refreshingly easy customer agreements and transaction experiences. Organizations requiring high assurance security, including the integrity of end-users and the fidelity of transaction records behind every agreement, choose OneSpan to simplify and secure business processes with their partners and customers. Trusted by global blue-chip enterprises, including more than 60% of the world's largest 100 banks, OneSpan processes millions of digital agreements and billions of transactions in 100+ countries annually.

Learn more at **OneSpan.com**
Contact us at **www.onespan.com/contact-us**
Reseller: Ergonomics AG, Uetlibergstrasse 132, 8045 Zürich, Switzerland, +41 58 311 1000, sales@ergonomics.ch