OneSpan

DATASHEET

DIGIPASS FIDO TOUCH

DIGIPASS FIDO TOUCH

Passwordless authentication for online services in mobile and desktop environments with Digipass FIDO Touch, a FIDO2-certified device. Protect your accounts against social engineering and replay attacks with FIDO-enabled multifactor authentication.

HIGHLIGHTS

- **FIDO2-certified device**
  Enable passwordless authentication directly in the browser
- **Highly secure**
  Protection against man-in-the-middle and phishing attacks eliminating shared secrets vulnerabilities
- **User convenience first**
  PIN-protected FIDO authenticator with touch screen to enable convenient registration, authentication, and transaction validation for any FIDO2-enabled service
- **PSD2 compliance ready**
  Digipass FIDO Touch satisfies all Strong Customer Authentication and RTS requirements

Move beyond passwords

Passwords are cumbersome, and we hate to remember them. Users struggle to remember passwords for different accounts resulting in password resets and costly helpdesk calls. Password reuse offers no solution and puts user accounts at risk for account takeover once the password is compromised. As much as 80% of large-scale data breaches and credential thefts can be attributed to insecure passwords. The answer to this dilemma: forget passwords!

Digipass FIDO Touch provides passwordless authentication allowing users to securely logon to online services and perform banking transactions via mobile or desktop. Digipass FIDO Touch works out-of-the-box with any service supporting FIDO2 authentication protocols.

Simplify the customer experience

Digipass FIDO Touch is designed with the user in mind. Passwordless authentication removes the first and often largest hurdle — remembering passwords. The touch screen offers an intuitive user experience. Digipass FIDO Touch is a USB and Bluetooth-enabled authenticator giving customers the choice to select their preferred authentication method. It also enables the device to be used with any other mobile device as a USB port.

How it works

Passwordless authentication puts an effective end to phishing and other social engineering attacks as hackers are unable to phish usernames or passwords. The physical possession of your Digipass FIDO Touch is required to gain access to the online service.

The passwordless login relies on FIDO2, an open standard supported by Google Chrome, Apple, Mozilla Firefox, and Microsoft Edge, and uses public key cryptography.

fido CERTIFIED L1 FIDO2

Your personal private keys live on Digipass FIDO Touch while the public keys are stored on the FIDO2-enabled servers. For each service, a unique key pair is created. Simply connect Digipass FIDO Touch to any device via USB or Bluetooth and enter your PIN on the touch screen. In the background, your private key will be used to sign a challenge and is sent back and matched with the public key stored on the server.

Enhanced security

Digipass FIDO Touch provides secure modern authentication with a high level of security using public key cryptography. Credentials are never exposed over any network and are protected with the PIN as a second factor. The PIN is entered directly on the display of the device which increases overall security.

Digipass FIDO Touch provides the maximum level of protection. Cryptographic private keys are generated onboard in the embedded hardware security element and never leave the device.

The solution protects against a variety of known and potential attacks, including PIN brute-force attacks. After too many incorrect guesses, the device is locked.

Enable PSD2 compliancy

Digipass FIDO Touch provides a fast and simple way to help you meet PSD2 compliancy by eliminating passwords and shared secrets. Fulfilling PSD2's Strong Customer Authentication requirements across your mobile and web applications is a breeze. Logging on with Digipass FIDO Touch satisfies the possession factor and the local PIN verification constitutes a second factor as mandated by PSD2. Digipass FIDO Touch equally supports dynamic linking for transaction authorization as transaction details can be presented on the display for user approval. Created with privacy and security in mind, no personal identifiable information is ever stored on the device or sent to the server.

Logon to Windows and Microsoft Azure AD

Digipass FIDO Touch replaces the username and password combo to sign-in to Windows 10 and the cloud version of Microsoft Azure AD. Via the display, the end-user can select his credential to log on to multiple domains or applications. Off-line connection is also supported.

Easy to setup

Digipass FIDO Touch is a Bluetooth enabled hardware device and can be connected to your desktop via USB. Installation via PC is straightforward; simply connect the device to the computer via USB. To enable Bluetooth, you will need to pair your device with the mobile, PC, or platform you wish to connect to.

Upon first use, you will be asked to set your PIN code. After the PIN is set, you will be able to log on or sign transactions on any FIDO2-enabled service. No additional drivers need to be installed, ensuring a frictionless and intuitive user experience, which in turn results in a higher user acceptance.

Cost-efficient solution

FIDO authentication offers an interoperable and standardized ecosystem of authenticators for use with mobile and online applications. It enables organizations to deploy strong authentication for login and transaction validation, without the incremental cost of in-house development.

TECHNICAL SPECIFICATIONS		
Display	1,77 in. TFT color display (128 x 160 dots)	
Size	76 mm (L); 42 mm (W);	
8,5 mm (H)	90.22 mm (L) 42 mm (W) 9-16.88 mm (H)	
Weight	25 gr	
Languages	Multilanguage support	
Batteries	Rechargeable*	
Cable	1m long USB detachable cable with type A connector	
Power Supply in connected mode	Only in USB connected mode, in BLE connected mode power from batteries	
Bluetooth	Standard 4.1 LE (Low Energy) Multiple Host handling: Up to 8 hosts with automatic selection Maximum output power : -16dBm Gatt profile and Service implementation	
Operating Systems	Bluetooth 4.1 LE (2) : iOS 10+, Android 7+, Mac OS X 10.12, windows 10?	
Tampering	Tamper evident	ISO 13491-1

CERTIFICATION AND COMPLIANCE		
Short storage temperature*	-10° C to 50° C; 90% RH non condensing	IEC 60068-2-78 (Damp heat) IEC 60068-2-1 (Cold)
Operating temperature	0° C to 45° C; 85% RH non-condensing	IEC 60068-2-78 (Damp heat) IEC 60068-2-1 (Cold)
Vibration	10 to 75 Hz; 10 m/s^2	IEC 60068-2-6
Drop	1 meter	IEC 60068-2-31
Compliant with	CE, FCC (FCC ID: 2AH88-785)	
FIDO certification	FIDO2 LEVEL 1	
FIDO protocol	FIDO2 and U2F	

**Long term storage for devices with rechargeable batteries should be limited to 1 year after production date. After each year, the battery of the unit must be fully recharged before it can be stored for another year. It is not recommended to fully charge a LiPo for storage. It is bad for the cell to store it fully charged. Charge to 3.8V for storage.*

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com