OneSpan

Digipass® 870

Datasheet

Digipass® 870 helps banks and financial organizations eliminate smart card security gaps and build trust in every transaction. Its independent verification and signing process protect users from credential compromise while simplifying compliance and safeguarding high-value operations.

Strong protection for smart card–based authentication

Many online banking and PKI applications still depend on static PIN entry, leaving them exposed to malware and keylogging attacks. Digipass 870 eliminates this risk by enabling users to enter their PIN directly on the reader instead of the keyboard, keeping credentials fully isolated from the PC.
A built-in firewall mechanism prevents unauthorized card access, and secure PIN changes can be performed safely through the device's keypad.

This makes every authentication replay-resistant, even if intercepted, the code cannot be reused.
By introducing secure transaction signing, banks can prevent fraudulent transfers. The result is reduced fraud losses, stronger compliance with security regulations, and higher customer confidence in digital channels.

"What-you-see-is-what-you-sign" (WYSIWYS) assurance

The full dot-matrix display allows users to visually verify complete transaction details before signing. This WYSIWYS capability ensures that what the user sees on the device is exactly what they authorize, safeguarding against tampered data and reinforcing trust in digital signatures.

Reader signature and multi secure channel

Each Digipass 870 can be uniquely identified by the issuing bank, ensuring that only legitimate readers are used for signing. Any attempt to use an unauthorized reader is fully detectable.

During connected transactions, banks can communicate directly with the customer through a secure channel, providing an additional layer of verification and customer assurance.

Easy to deploy, manage and use

Digipass 870 uses standard drivers compatible with all major operating systems, including Windows, Linux, and macOS, no additional software installation required. Because the readers are not individually personalized, they can be easily distributed across large customer bases without compromising security. Banks may optionally enable secure firmware updates, allowing the device to be maintained and enhanced even after deployment using proven cryptographic mechanisms.

Highlights

Secure and convenient

- Reduces deployment and maintenance costs with postal distribution and zero software installation
- Supports multiple applications with a single device
- Simplifies customer experience with one-touch operation and clear guidance
- Supports compliance with banking security and strong customer authentication requirements
- Customizable branding

Firmware update optional

As an option, the Digipass 870 supports secure firmware update. Digipass 870 firmware and applications can be updated by the bank which issues the card reader at any time even when Digipass 870 has already been issued to the enduser, making use of proven and standard cryptographic mechanisms.

Flexible connected and unconnected operation

In connected mode, the reader interfaces directly with the bank system for automatic transaction display and signing. In unconnected mode, it functions as a standalone authenticator, supporting strong authentication and transaction signature generation for applications such as digital banking, e-commerce, and secure corporate access.

Digipass 870 supports a wide range of industry schemes including Mastercard CAP, Visa Dynamic Passcode Authentication, and proprietary domestic protocols, leveraging the security of chip cards for cryptographic key management and one-time password generation.

How it works

Connected mode – Transaction signing

1. The device displays transaction information (e.g., amount, account number).
2. The user confirms each data field or the full transaction as shown.
3. The user enters their PIN and confirms. The transaction is securely signed using WYSIWYS verification.

Unconnected mode – Secure login

1. The user inserts their card and selects the login function.
2. The challenge value from the bank's website is entered.
3. The user enters their PIN; the device generates a one-time password.
4. The response code is entered on the website to complete secure login.

CERTIFICATION AND COMPLIANCE		
Short-term Storage	-10°C to 50°C 90% RH non-condensing	IEC60068-2-78 (damp heat) IEC60068-2-1 (cold)
Operating Temperature	0°C to 45°C 85% RH non-condensing	IEC60068-2-78 (damp heat) IEC60068-2-1 (cold)
Vibration	10 to 75 Hz 10 m/s²	IEC60068-2-6
Drop	1 meter	IEC60068-2-31
Emission		EN55022
Immunity	4 kV contact discharges 8 kV air discharges 3 V/m from 80 to 1000 MHz	EN 61000-4-2 and EN 61000-4-3
Compliant with European Directives	CE: 89/336/EEC or 2004/108/EC RoHS: 2002/95/EC WEEE:2002/96/EC	

TECHNICAL SPECIFICATIONS	
Size	97 mm (L) x 61,7 mm cm (W) x 13,5 mm (H)
Weight	<80g
Display	102 * 46 full dot matrix display Up to 6 lines, 120 characters
Keypad	Tactile keypad with silicon rubber key printed with an epoxy layer. Resistant to over 100,000 rubbings. 10 numeric keys and 6 function keys
Battery	2 replaceable batteries
Power supply in connected mode	USB connection
Cable	1m long USB cable with type A connector
Standards	• Mastercard CAP (2004, 2007) • VISA dynamic passcode authenticatio version 1.1 • Belgian eID card • Connected EMV CAP • ISO 7816 • EMV2000 LEVEL 1 • USB 2.0 Full speed • PC/SC 2.01 • CCID

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
OneSpan.com/security

Contact us at
OneSpan.com/contact-us