

DIGIPASS 710

The ultimate security for online banking transactions: e-signature in a trusted environment

The DIGIPASS 710 (DP 710) ensures secure banking transactions across the Internet or any public network. DP 710 prevents sophisticated fraud schemes such as tampering, message forgery, malware or man-in-the middle attacks.

The patent-pending DIGIPASS 710 bank-to-customer authentication prevents attackers from impersonating financial institutions. A customer's account credentials can no longer be stolen. One-Time Password (OTP) and e-signature authentication methods prevent attackers from impersonating customers in an effort to process fraudulent transactions.

E-signature based on "What you see is what you sign" is considered as the ultimate level of security.

MUTUAL AUTHENTICATION

1. A bank customer identifies and connects to his bank server.
2. The bank server initiates the authentication by presenting a dynamic host verification code, which can only be generated by a valid bank server and therefore identifies the bank.
3. This code is verified by the DP 710 and when it matches,
4. The DP 710 generates a dynamic code (OTP) to validate the user's identity to the bank.

Both parties have proven their identity, resulting in mutual authentication. A secure channel has been created for any transaction between the bank and the end-user.

This process ensures that valid passwords are sent only to legitimate bank servers. All authentication codes rely on the proven DIGIPASS algorithm.

The initial bank server authentication can be done without user interaction when the DP 710 optical interface is used.

OPTICAL INTERFACE

The optical interface is a feature that automatically downloads encrypted data from the PC display into the DP 710. This feature increases the end-user acceptance dramatically since a data transfer is completed within 4 seconds.

The interface does not require any software or driver as the communication is established between a flashing pattern on the user's PC and the DP 710 photo-transistors. Customizable positioning icons on the DP 710 overlay enable the compatibility of the optical interface with any screen size and resolution.

The optical interface facts:

- No installation and support issues
- No hidden deployment cost
- Can be used on any platform (Windows, Linux, Mac)
- Compatible with any available browser
- Displays as a flashing pattern on the PC screen

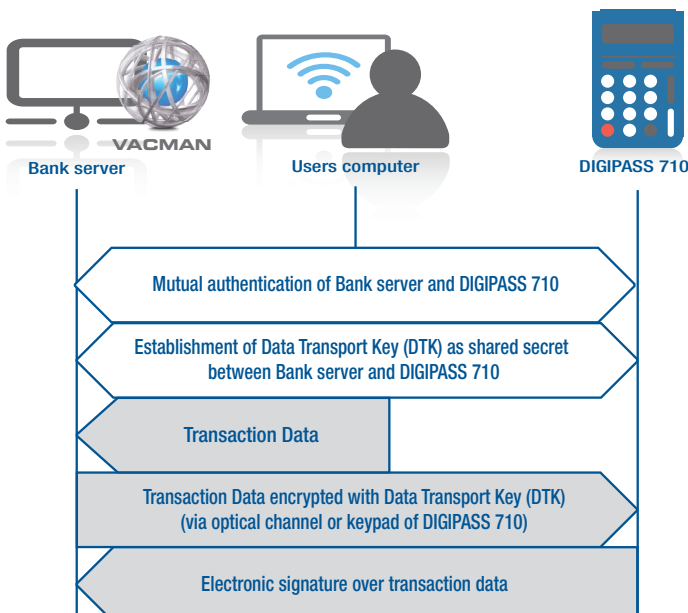
ZERO FOOT-PRINT

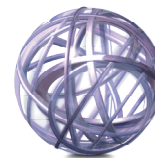
The DP 710 does not require any software or driver installation on the user's PC. This ensures that valuable data is never stored on the user's PC, thus eliminating a potential security threat.

E-SIGNATURE: WHAT YOU SEE IS WHAT YOU SIGN (WYSIWYS)

The DP 710 e-signature functionality automatically activates once the mutual authentication has been established between the bank and the end-user.

1. The bank server sends the user the encrypted transaction requiring an e-signature. This transaction is sent securely to the DP 710 encrypted by a Data Transport Key (DTK) only valid for this session. This encryption key was shared between the bank server and the DP 710 after having a successful mutual authentication.
2. The end-user loads his transaction into the DP 710 by one of the following methods:
 - Automatically through the optical interface of the device, or
 - Manually on his DP keypad.
3. This transaction is decrypted by the device and key transaction data is displayed for confirmation from the user by selecting "OK".
4. Once the user has approved all displayed data, the device generates an electronic signature, based on the original data sent to the bank server. This code is unique for each transaction.




FEATURES

- Customizable user interface and number of fields available for e-signature
- Adjustable PIN management to meet even the most stringent banking security policies: weak PIN protection, PIN length, maximum number of wrong PIN entries, time limits, unlock code, etc.
- Very user friendly
- Multiple languages available for the user interface
- Fully customizable labels displayed for the different transaction data (in e-signature mode)
- Any time labels can be defined by the authorized bank server: e.g. to enforce new security rules (in e-signature mode)
- Public internet access places are no longer a threat; a secure channel is established between the bank server and the DP 710


PHYSICAL FEATURES

Size	90x60x10 mm
Weight	46 g.
Battery Lifetime	5 years
Tactile 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
Display	80x16 dot matrix, 1 or 2-line mode

COMPLIANCE TO STANDARDS

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 60068-2-32
Emission		EN 55022
Immunity	4 kV contact discharges 8 kV air discharges 3 V/m from 80 to 1000 MHz	EN 61000 -4-2 EN 61000-4-3
Compliance to European directives (CE marking)		2004/108/EC (EMC directives) 2002/95/EC (RoHS directive) 2002/96/EC (WEEE directive)

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXs GUARD® authentication products for the financial world, remote access, e-business and e-commerce.

With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com
BRUSSELS (Europe)

phone: +32.2.609.97.00
email: info-europe@vasco.com

BOSTON (North America)

phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)

phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)

phone: +65.6323.0906
email: info-asia@vasco.com