

# DIGIPASS<sup>®</sup> 850 Secure Reader

*Standard Secure PINpad Reader with USB interface*



## **Application Area: Protecting smart card PIN**

Today more and more systems are using smart cards that are protected with static PIN. These can be PKI, e-wallet or e-banking applications. If these applications are relying on the static PIN of the smart card being entered on the PC-keyboard, then this PIN is vulnerable to Trojans or any other kind of keyboard logging tools. Due to the current vulnerability of the PC platform in the Internet environment, the practice of entering the PIN in this insecure way has become unacceptable from a security point of view.

The solution is easy: replace the insecure transparent smart card reader by a secure PINpad reader. The vulnerable PIN will now be entered on the keyboard of the reader itself so that the PIN is never available on the PC platform.

However, besides the security argument, people still choose transparent readers because:

- Secure PINpad readers are too expensive.
- Secure PINpad readers do not always support legacy applications.
- The extra development effort is too costly and too long.
- One loses too much flexibility for product enhancement/correction.

The DP850 solves these problems and becomes a real solution for enhancing the security of your system. When plugged into the USB port of a PC, the Digipass Desk 850 is:

- a fully PC/SC compliant smart card reader with local PIN entry
- a cost effective solution
- a backward compatible solution
- easy to configure & easy to integrate
- offering a maximum of flexibility

## DP850: A cost effective solution

- Secure PINpad readers used to have a cost that was a multiple of the cost of transparent smart card readers. This was due to the fact that they were derived from expensive point of sales terminals.
- The DP850 Secure PINpad Reader has been developed from scratch with the aim to be a cost effective reader for the private and consumer market.
- The DP850 offers the essential security functionality to have local PIN entry on the reader, without fully incorporating all expensive technologies of point of sales terminals. After all, the risk of physical tampering at home or office is completely different from a shop or petrol station.

**Conclusion: cost is not a reason anymore to keep using insecure readers.**

## DP850: A backward-compatible solution

- Secure PINpad readers do not always support older legacy applications that are based upon a transparent reader. This creates problems during migration or when new high security applications need to co-exist with older low security applications.
- This backward incompatibility forces people sometimes to have two readers connected at the same time, which in turn causes other issues such as missing PC connection ports, end-user confusion or conflicts on the ports.
- The DP850 reader solves this backward incompatibility problem as it can still behave as a transparent smart card reader for all old applications that do not require the extra security possibilities of the DP850. This gives a migration path for upgrading existing customer groups from an old insecure system (PIN entry on the PC) towards a new secure system (PIN entry on the reader).

- The level of backward compatibility can be tailored by selecting the correct settings for the DP850 firewall. This firewall defines the commands that may still be used in transparent mode.
- In cases where a huge investment was already made in insecure readers, one can still issue secure DP850 readers for new or for the most important customers. The application simply checks which reader type is being used and then activates the secure PIN entry or not.

**Conclusion: Migration and backward compatibility is no problem.**

## DP850: Easy configuration & easy integration

- Our "standard" secure PINpad reader contains firmware that is customer independent. So there is no extra cost involved to adapt the code inside the reader to your application and smart card. This "standard" secure PINpad reader is deliverable from stock in small quantity (minimum 2, maximum 100 pieces).
- Configuration of the behaviour is done via parameter settings in the embedded, battery backed-up, RAM. This flexibility allows one to:
  - Set the display messages. The standard DP850 supports 2 sets of loadable languages. The user of the DP850 secure PINpad reader can select the language by using the Menu button (while reader is disconnected).
  - Define the character set (e.g. support local special characters) or incorporate the Logo of the application of the customer on the display of the DP850.
  - Customize the firewall behaviour. This defines the usage as transparent reader.
  - Restrict the possibility of the PC to show messages and questions on the DP850 local reader display.

All tools needed for doing these RAM based configurations are supplied with the integration toolkit for the standard DP850.

- Using the sample program it takes less than 1 day to upgrade your existing insecure application into a "secure" application using PIN entry on the DP850 reader. No extra new tools or libraries are needed as the access to the security functions of DP850 secure reader is done using the PC/SC smart card interface.

**Conclusion: Integration and customisation cost is very low, making it possible to use secure readers for proof of concepts or demo's.**

## DP850: Maintaining maximum flexibility

- The DP850 leaves the majority of the smart card based functionality on the PC. Only the security related PIN entry or PIN change is done locally. This keeps flexibility at the place where it belongs: inside the PC program.
- The DP850 has incorporated the possibility to interface a whole range of smart cards with each having their own specific PIN entry method. All these methods are already incorporated so that not only your current smart card is supported, but also a wide group of other smart cards.
- As your application remains completely on the PC, there is no problem of adding new customer applications for the same reader. This avoids the need for firmware upgrades in the reader.

**Conclusion: The standard DP850 secure reader does not limit the flexibility of developing PC based applications.**

## DP850 Secure PINpad reader: How does it Work?

### What do you need to install?

As for other USB smart card readers, there is a specific DP850 USB-driver (Microsoft certified) that needs to be installed. Using the smart card reader name that appears in the Operating System, one can recognise that this is the VASCO secure PINpad reader. Using the "get

version" and "get firewall" special commands, the application can verify that the correct or compatible firmware version and RAM configuration is found. The reader can be accessed using the PC/SC interface.

### How to access the extra reader functionality?

No communication with the reader is possible as long as no valid smart card is inserted. Once the smartcard has been powered and reset, the communication with the smart card is opened and the security functionality of the DP850 is accessible. The DP850 security functionality can be fine-tuned using commands that look like normal smart card APDU's, except that the CLA and INS byte have values that are not used for ISO7816 smart cards. Because of these special CLA and INS values, the DP850 reader can at all times distinguish between reader commands and smart card commands. The DP850 reader will answer the reader commands in full compliance with the APDU interfacing rules.

### How does the firewall work?

All APDU's sent to the reader and intended for the smart card are compared with a list of allowed or forbidden INS bytes. This list is called the firewall and is normally part of the RAM customisations. This list can enumerate 15 allowed INS bytes (positive firewall) or it can enumerate 16 forbidden INS bytes (negative firewall). If the firewall rejects the INS command, then an error code (SW1-SW2) is returned to the PC. If the firewall permits the INS command, then the APDU is sent to the smart card and the smart card answer is returned to the PC.

### What extra reader functionality is available?

We have the following groups of commands:

- Status and Version commands. They allow one to get:
  - The current firmware version of the reader
  - The current status of the reader (waiting for or doing a local action).
  - The status of the firewall (defines the transparency of the reader).
- Commands for starting up secure PIN Entry or secure PIN Change. Also commands for retrieving the result of secure PIN Entry and secure PIN Change (=SW1-SW2 code).

- Commands for using the reader as a terminal:
  - Show message and ask confirmation
  - Show message + number and ask confirmation
  - Show message + ask to enter a number
  - Show message + ask to accept or modify a number
- Commands for changing the firewall.

Note that these "terminal" and "firewall" commands can be tailored by settings stored in RAM. Three options exist:

- These commands can be disabled = Impossible to use.
- These commands can be restricted = Only a well-defined list of commands stored in RAM is allowed (e.g. Only allow terminal messages "PIN LOCKED" and "LAST PIN TRY" and "OK TO SIGN ?").
- These commands can be free to use. This is useful for a proof of concept phase (e.g. a signature can be emulated with the Terminal mode command, but the composition of the smart card signature APDU + datablock is still done by the PC).

For medium and large systems, Vasco can easily add custom reader functionality to the DP850 reader platform. However, the standard DP850 secure PINpad reader will always remain the starting point in order to develop the concept and for doing the first pilot tests.

Example: Do secure PIN entry

1. First the PC powers the smart card and does a number of operations as for a fully transparent smart card reader. For instance, select the correct file and check the PIN status (Locked, PIN error count, etc...). If needed, the reader transparency can be limited with the "Reset Firewall" values that were selected during RAM configuration.
2. If wanted, the PC can use a special DP850 APDU that causes warning or error messages to be displayed (e.g. message "last PIN try").
3. Then the PC sends the "Start PIN entry" reader command followed by a data block that contains all parameters to customise PIN entry (e.g. length of PIN that should be used, etc....).

4. While the local PIN entry is busy, the PC application is waiting in a loop and polls the PIN entry progress using a Status retrieval reader command.
5. When finished, the PC can send the reader command for retrieving the result of the PIN entry process. This result is the SW1-SW2 that was answered by the smart card upon the PIN entry reader APDU sent by the reader to the smart card.
6. Now the PC can again access the smart card in a transparent way. If needed, the reader transparency can be limited with the "PIN-OK Firewall" as defined in the RAM configuration.

## Can we change the firmware of the DP850?

The standard DP850 secure PIN pad reader contains fixed firmware that cannot be changed or updated. If future upgrades are done of this firmware, then Vasco will take care that the new version is backward compatible with the existing version. For instance, this "standard DP850" firmware version is backward compatible with the "evaluation DP850" that was distributed before (firmware version 1C52).

If needed for larger systems or if a custom security level is needed, then Vasco can offer a cost-effective firmware customisation. For this customisation we start from the firmware of our standard reader and change only the customer specific items (e.g. automatic recognition of the card by the reader and selection of the correct firewall in function of the card found). But even in this case, we propose to start with the standard DP850 for initial testing and for proof of concept. As such, this work and cost can be delayed until the moment that the project has proven to become a success.

The DP850 hardware and firmware platform are fully compatible with the Vasco family of Digipass tokens. This gives the possibility to include in the DP850 firmware any functionality (=code) of any other Vasco token. This makes it possible, for example, to use the DP850 off-line as password

password generator for all cases where a USB interface is not available, or to add functionality like EMV-CAP password generation. Please contact Vasco for a reference list of customisations that have been performed.

## Hardware Features

- High-contrast, 12-character, 2-line LCD (1 continuous 7 x 60 dot matrix line + 1 line of 12 7-segment characters)
- Tactile keypad with silicon rubber keys
- Intelligent battery management (providing 5-year service life in standalone mode)
- Internal real-time clock
- Compatible with ISO7816 and EMV smart cards
- Comes with detachable USB cable of 150cm.
- Size: 63 x 95 x 16 mm
- Weight: 62 gr

## Software Features

- Character set can be adapted (battery backup RAM).
- Two independent languages can be loaded
- Menu button allows to select Language or to display version
- Values of the Firewall can be selected.
- Secure PIN entry and secure PIN change (multiple formats are possible, except for hashed PIN formats).
- Usage as "Terminal" (allows the user to confirm amounts or other values).

**For regional offices or to learn more about us, visit our web site at [www.vasco.com](http://www.vasco.com)**



### EMEA

VASCO Data Security nv/sa  
Koningin Astridlaan 164  
B-1780 Wemmel, Belgium  
phone: +32.2.456.98.10  
fax: +32.2.456.98.20  
email: [info\\_europe@vasco.com](mailto:info_europe@vasco.com)

### APAC

VASCO Data Security Asia-Pacific Pte Ltd.  
#15-03 Prudential Tower, 30 Cecil Street  
049712 Singapore  
phone: +65.6.232.2727  
fax: +65.6.232.2888  
email: [info\\_asia@vasco.com](mailto:info_asia@vasco.com)

### AMERICA

VASCO Data Security Inc.  
1901 South Meyers Road, Suite 210  
Oakbrook Terrace, Illinois 60181, USA  
phone: +1.630.932.8844  
fax: +1.630.932.8852  
email: [info\\_usa@vasco.com](mailto:info_usa@vasco.com)

All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for any infringement of patents or other rights of third parties resulting from its use.