

# Sipiro



## Contents

|                                       |   |
|---------------------------------------|---|
| Getting Started .....                 | 3 |
| Installation.....                     | 3 |
| Supported Card Types.....             | 3 |
| Belgian Eid Card detection .....      | 4 |
| Adjusting Contrast .....              | 4 |
| Calculator .....                      | 5 |
| Language .....                        | 5 |
| Authentication PIN .....              | 6 |
| Authentication Message .....          | 6 |
| Qualified Signature PIN.....          | 7 |
| Qualified Signature Message (1) ..... | 7 |
| Qualified Signature Message (2) ..... | 8 |
| EMV CAP authentication.....           | 8 |
| EMV CAP transactions.....             | 9 |
| Frequently Asked Questions .....      | 9 |

## Getting Started

The **Sipiro** is a portable and low-cost handheld smart card device that is capable of managing One Time Passwords (OTP), Challenge-response Authentication Codes, and Transaction Data Signing (PKI digital signatures) based on the security keys stored in the EMV cards and eID cards. The **Sipiro** is compliant with major federal, banking, computing and safety standards such as the Belgian eID card, MasterCard® Chip Authentication Program (**CAP**), MasterCard® Advanced Authentication for Chip (**AA4C/PLA**), VISA Dynamic Passcode Authentication (**DPA**) and **EMV Level 1**.

The **Sipiro** supports Secure PIN Entry (SPE) to assure secure PIN entry and PIN change while on PC-linked mode. On standalone mode, the PIN is securely entered into the device and kept from being exposed to vulnerable PC's or workstations, hence eliminating the possibility of a Virus/Trojan getting hold of the PIN.

Furthermore the **Sipiro** can be used as a compact OTP (One-time password) generator which can perform authentication for various applications either on PC-linked or standalone mode. It uses two-factor authentication which requires the cardholder to insert the EMV card (*something you have*) into the device and enter a PIN (*something you know*) using the built-in pin-pad. The display screen will then let somebody see a generated dynamic one-time password which can be used to perform secure online transactions, telephone orders or e-banking logons.

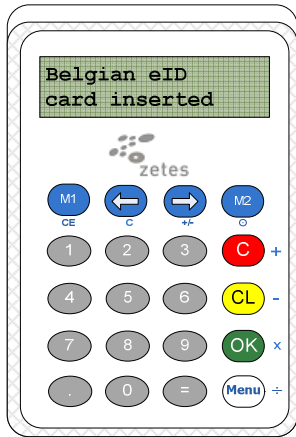
## Installation

- **Manual install:** download the driver as presented on [www.belgeid.be](http://www.belgeid.be) and follow these procedures:
  1. Do **NOT** connect the reader!
  2. Run setup.exe
  3. Follow instructions on screen
  4. Select destination folder or click next to confirm the default installation folder
  5. Once prompted that the operation is complete, click "Finish".
  6. After installation is complete, plugin the reader into an available USB port and wait until Windows finds the new hardware.
  7. Do not remove the reader until "Ready to use" message is shown by the windows device installation dialog.

## Supported Card Types

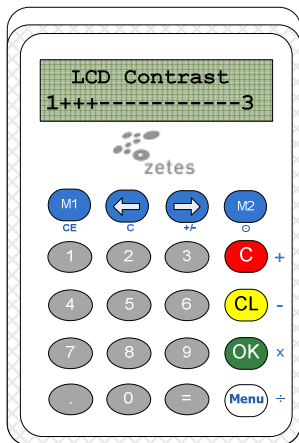
- ISO7816 cards like **Belgian eID card**
- CAP certified EMV contact card, including:
  - a. M/Chip Lite 2.1 with CAP personalization profile
  - b. M/Chip 4 with CAP personalization profile
  - c. M/Chip Select 2.05 with CAP personalization profile
- PLA/AA4C certified EMV contact card
- VISA DPA certified contact card

## Belgian Eid Card detection



In PC connected mode the Sipiro detects the Belgian eID card automatically and contains special functions for securing all of your eID transactions.

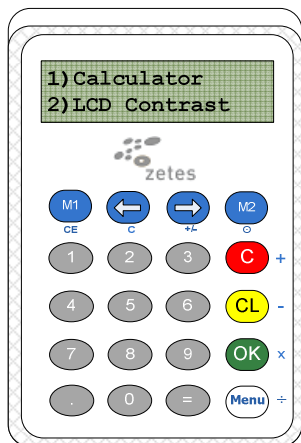
## Adjusting Contrast





In standalone mode (not connected to computer) you can adjust the contrast.

- Press **M2** and hold for 1-2 seconds to start up
- Press **Menu**
- Press **[2]** for selecting contrast
- Press **[1]** for less contrast
- Press **[3]** for more contrast

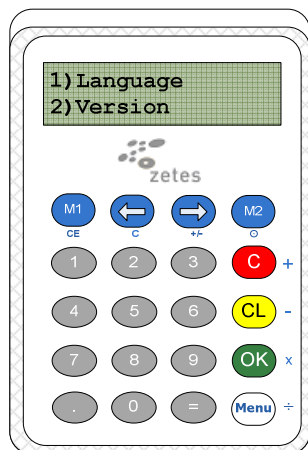
## Calculator






In standalone mode (not connected to computer) you can use the calculator function.

- Press  and hold for 1-2 seconds to start up
- Press 
- Press [1] for starting Calculator

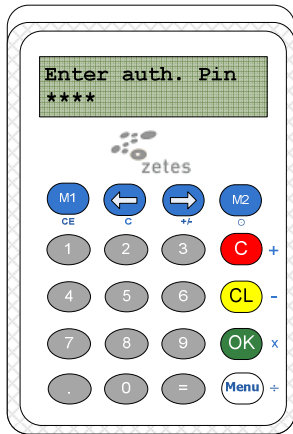
## Language




In standalone mode (not connected to computer) you can adjust the language. **In connected mode the application defines the language.**


- Press  and hold for 1-2 seconds to start up
- Press  **2 times**
- Press [1] to select language setting
- Select language or press  **again** to show other languages


## Authentication PIN



Whenever an application wants you to authenticate yourself, it first asks for your authentication PIN. This can be a standard application or a web-application using SSL. (eg. [HTTPS ://...](https://...)) the authentication pin protects the authentication key on your eID card.

After entering the pin, press  to confirm.

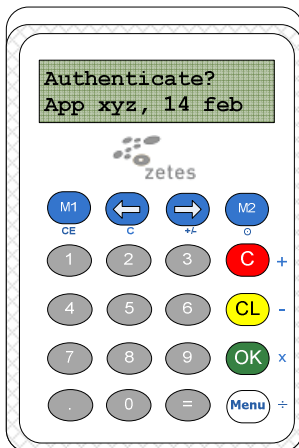
Press  to cancel the operation.

Press  for backspace.

The pin length of current auth. pin is between 4 and 12 digits in size.


**(For current eID cards, authentication PIN is the same as the non-repudiation PIN)**

## Authentication Message



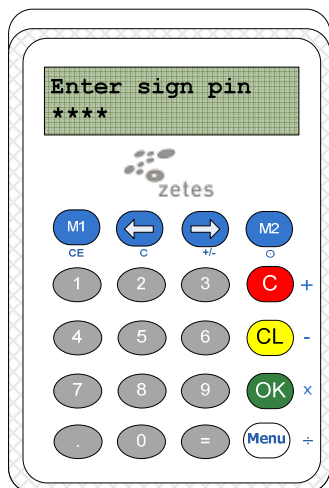
After entering the authentication pin, this message could appear. This means that App xyz wants you to authenticate by using your eID card. The application can display the same message so you can easily verify the application you are entering.

Press  to confirm.

Press  to cancel operation

In normal SSL connections ([https ://...](https://...)) this message will **NOT** appear.

## Qualified Signature PIN



When an application wants you to sign a document, it first asks you to enter the non-repudiation or signing pin. This pin protects the key you need for calculating official qualified signatures on documents.

After entering the pin, press **OK** to confirm.

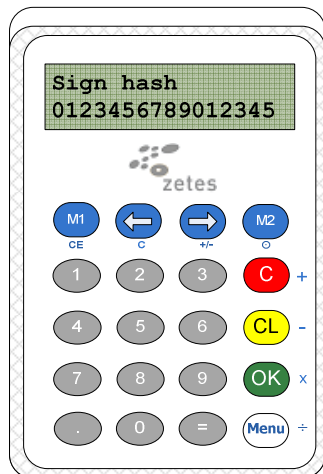
Press **C** to cancel the operation.

Press **CL** for backspace.

The pin length of current auth. pin is between 4 and 12 digits in size.

**(For current eID cards, authentication PIN is the same as the non-repudiation signing PIN)**

## Qualified Signature Message (1)



When an application wants you to sign a document with your eID card, it sends a small check value (hash) to your card reader. The card reader will display this value and asks you to confirm the check value. The application should display the same value and this way you know the value originates from the genuine application.

Press **OK** to confirm the check value.

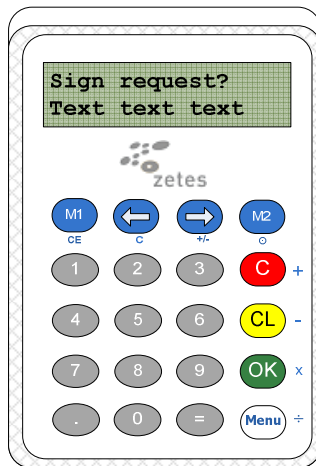
Press **C** to cancel the operation.

Press **←** or **→** to scroll the message.

**If the value does not correspond to the value on screen, cancel the operation!**

**If this message appears and you are not signing some document, cancel the operation!**

## Qualified Signature Message (2)



When an application wants you to sign a small text value with your eID card, it can send a small readable text message for you to confirm before signing. . The card reader will display this message and asks you to sign this message.

Press **OK** to confirm the text to sign.

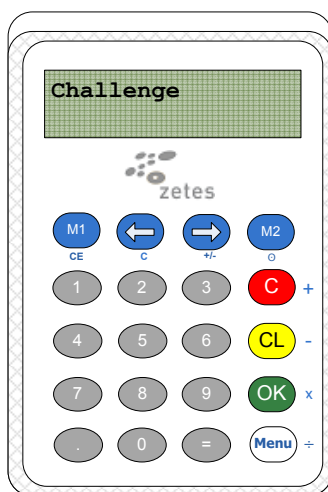
Press **C** to cancel the operation.

Press **←** or **→** to scroll the message.

**If the value does not correspond to the value on screen, cancel the operation!**

**If this message appears and you don't know why this appears, since you are not using an application that needs your eID card, cancel the operation!**

## EMV CAP authentication



The Sipiro supports EMV authentication as used in most online Belgian banking systems. When you insert your debit card in the reader, the display will show "Select menu". To authenticate in online banking applications:

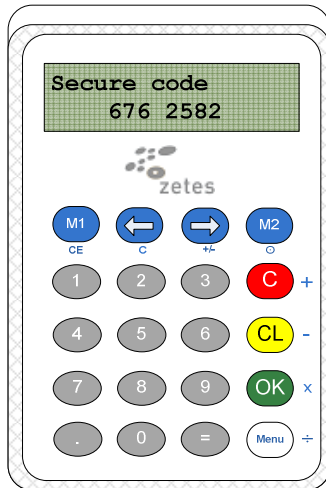
- Press **M1** to enter the challenge given by the online banking application and press **OK**
- Enter the PIN of your debit card.
- The display will show you the secure code to login in your banking application.

**CL** = backspace





**C** Cancel this operation and return to the menu



## EMV CAP transactions



The Sipiro supports EMV signing functions as used in most online Belgian banking systems. When you insert your debit card in the reader, the display will show **“Select menu”**. To sign a transaction in online banking applications with your debit card:

- Press 
  - Enter the PIN of your debit card.
  - **[Data: 1]** will show up in the display. Now enter the data as shown on screen by the banking application.
  - **[Data: 2 /OK?]** will show up. Enter the data as shown on screen by the banking application or press  when the banking application asks you to.
  - The display will show you the secure code to sign the transaction you are about to make.
-  = back space
-  Cancel this operation and return to the menu

## Frequently Asked Questions

**Q: How do I turn on/off the device when it is standalone?**

A: You can press the M2 button for few seconds, and it will be turned on/off.

**Q: What should I do if there is no response from Sipiro after card insertion?**

A: You can remove the card for a few seconds, reinsert it to the Sipiro. If it still doesn't work, check if the batteries are out of power.

**Q: How do I insert or replace the battery of the Sipiro?**

A: The battery of the Sipiro could be replaced or inserted through the following steps:

1. Pull out the battery case.
2. Insert 2 CR2032 batteries into the battery compartment.
3. Plug in the battery case.

