



# Middleware manual

Idoneum Electronic Identity, S.A

# Índice

<b>1 Introduction</b> .....	<b>3</b>
1.1 About the product.....	3
1.2 To whom is it addressed.....	4
1.3 How to read this manual.....	4
1.3.1 Conventions.....	4
1.3.2 Support.....	4
<b>2 System requirements</b> .....	<b>7</b>
2.1 Hardware.....	7
2.2 Software.....	7
<b>3 Software installation</b> .....	<b>9</b>
3.1 Windows.....	9
<b>4 Exacard monitor</b> .....	<b>15</b>
4.1 Status icons.....	16
4.1.1 Empty reader.....	16
4.1.2 Unknown card.....	16
4.1.3 Card analysis in progress.....	17
4.1.4 Card detected and analyzed successfully.....	17
4.1.5 Locked card.....	18
4.2 Using Exacard monitor.....	19
4.2.1 Deleting certificates.....	20
4.2.2 Importing certificates.....	20
4.2.3 PIN change.....	22
<b>5 Glossary</b> .....	<b>23</b>
<b>6 Licencia de uso y condiciones de garantía</b> .....	<b>25</b>

---

# 1 Introduction

Thank you for purchasing the advanced cryptographic card *Exacard*.

This is the installation manual for the *Exacard* middleware, specifying the instructions for proper installation of the cryptographic modules CSP and PKCS#11, as well as the use of the application *Exacard* monitor.

## 1.1 About the product

The product contains the following elements:

- *Exacard*.
- Software installation and user manual.

*Exacard*, as a SSCD (Secure Signature Creation Device) in a PKI (Public Key Infrastructure), incorporates into applications that support it the following features: strong authentication, electronic signature, generation and secure export of cryptographic keys, and confidentiality, integrity and protection of personal data.

## 1.2 To whom is it addressed

This manual is designed for people with basic knowledge regarding the use of smart cards, electronic signature and PKI certificates.

## 1.3 How to read this manual

The manual specifies the installation and use of the *Exacard* middleware. It is structured in a first part which deals with the software installation, and a second part which discusses the use of the application *Exacard* monitor.

### 1.3.1 Conventions

The convention used to ease the understanding of the steps to follow is indicated by:

- ◆ **Bold**: The label of the buttons pressed during the installation and use.
- ◆ *Italic*: Trademarks.
- ◆ {}: Indicates directories that must be replaced by the user.
- ◆ →: indicates a sequence of menus.

### 1.3.2 Support

You can have support through:

<http://www.idoneum.net/contacta.html>

For more information, please contact:

**IDONEUM Electronic Identity, S.A.**

Calmell Group

Polígono Industrial Pla d'en Coll

C/ Fresser 12 C

08110 Montcada i Reixac (BARCELONA)

Tel: +34 93 564 14 00

Fax +34 93 564 58 22



---

## *2 System requirements*

It's imperative to verify that the computer where you install the *Exacard* middleware meets the minimum requirements in both the software and the hardware.

### **2.1 Hardware**

- ◆ 50 MB of free space on your hard drive.
- ◆ 25 MB of RAM for Exacard monitor.
- ◆ Smart card reader compliant with ISO/IEC 7816 and PC/SC (Personal Computer Smart Card).

### **2.2 Software**

- ◆ *Microsoft Windows XP/Vista/7* for the CSP (Cryptographic Service Provider) cryptographic module.
- ◆ *Microsoft Windows XP/Vista/7, GNU/Linux or Mac OS X* for the PKCS#11 cryptographic module.
- ◆ *Microsoft Windows XP/Vista/7, GNU/Linux or Mac OS X* for the *Exacard* monitor.



## 3 Software installation

### 3.1 Windows

The installer for *Windows XP/Vista/7* includes the cryptographic modules CSP and PKCS#11 together with the application *Exacard* monitor.

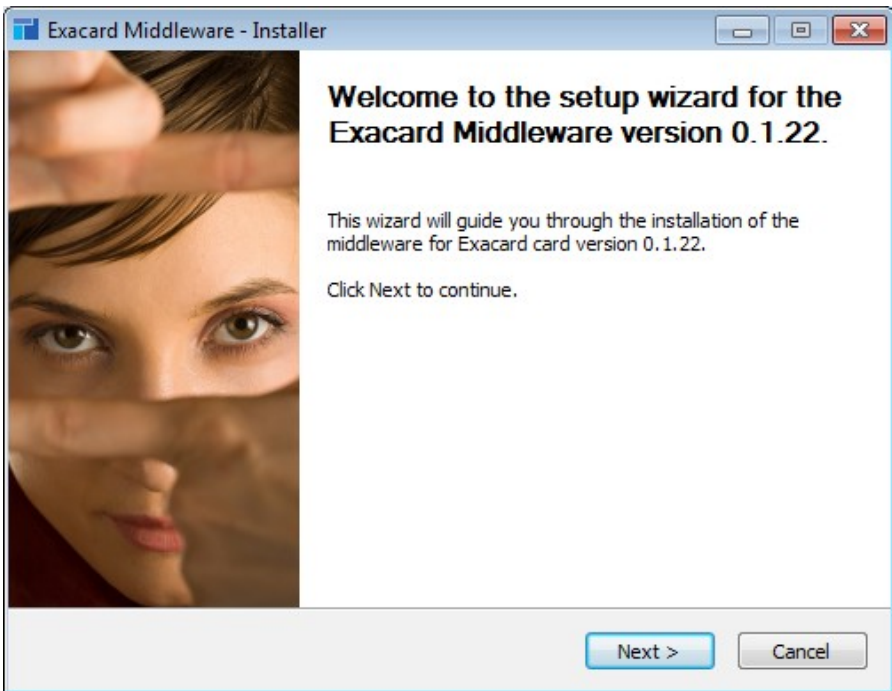


Figure 1: Exacard Middleware installer

## Installation

- Continuing with the installation process is subject to the agreement of the terms and conditions of use.

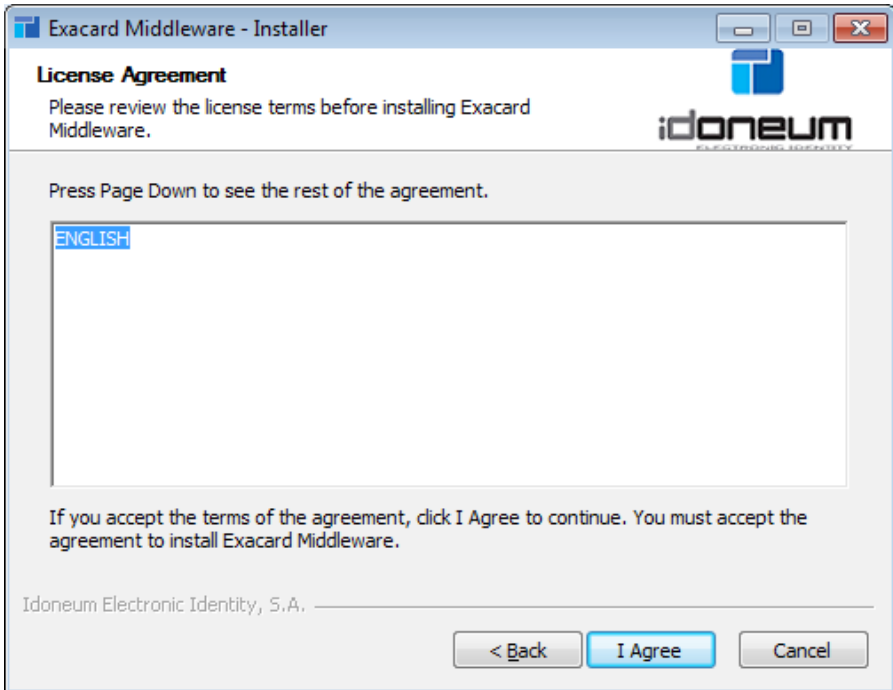


Figure 2: Terms and conditions of use

- Then proceed to the selection of components to install.

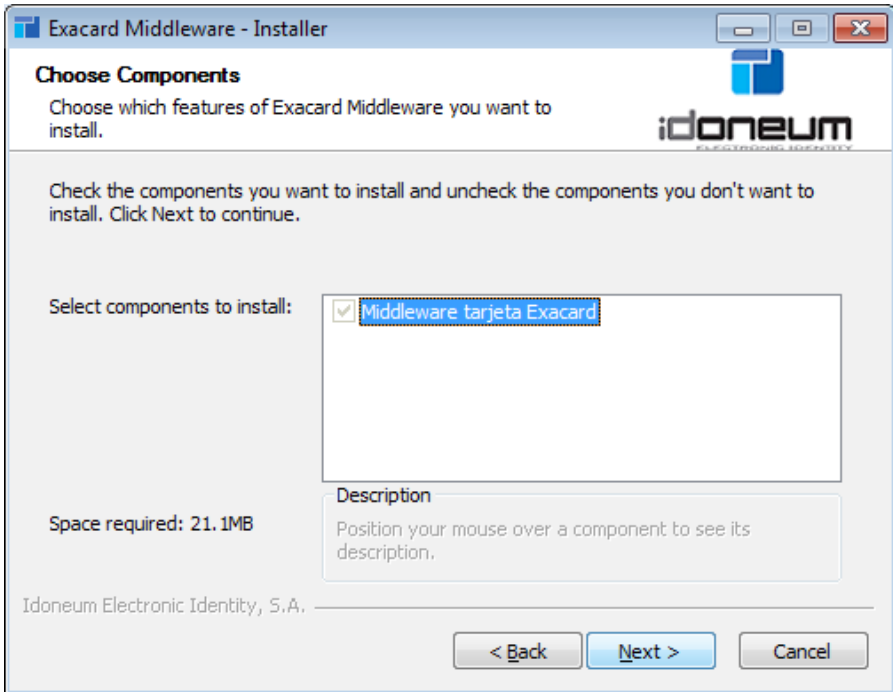


Figure 3: Installation options

**Note:** This window, though titled as "Component Selection" and given that only one global component is installed, does not allow selection or deselection of it. This may change in future releases.

- After choosing the components you can select the installation path.

**Note:** During the process being described the installation of the *Microsoft Visual C++ 2008 Redistributable* is started. This package has a separate installer that will run externally to the *Exacard* Middleware.

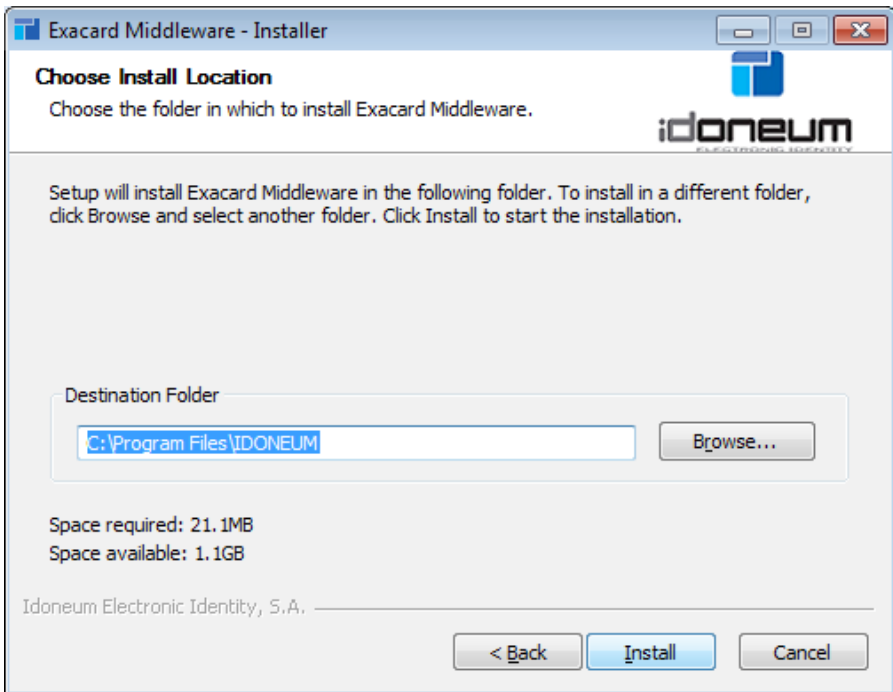


Figure 4: Installation path

- Press **Close** after the installation has finished.

## Uninstallation

- The uninstall process will remove from the system the installed components.

*Figure 5: Uninstallation*

- Press **Close** after the uninstallation has finished.



---

## 4 *Exacard monitor*

After installing the *Exacard* middleware the application *Exacard monitor* is automatically launched. It becomes visible from its icon in the notification area of the operating system.

Exacard monitor offers the following features:

- It detects and enumerates all smart card readers installed in the system, displaying an icon for each reader.
- Detects and check the status (locked, enabled, etc.). Of the *Exacard* inserted into the readers.
- Load the certificates contained in the *Exacard* directly to the system certificate store (*Windows XP/Vista/7* only)
- Import and delete certificates in the *Exacard*.
- Change of user's PIN.

## 4.1 Status icons

Here are the different icons that can take *Exacard* monitor during its execution.

### 4.1.1 Empty reader

There is an icon of this type for every reader installed on your system.



*Figure 6 Empty reader detected*

### 4.1.2 Unknown card

This icon is displayed when the card inserted into the reader was not recognized or it not was properly inserted.



*Figure 7 Unknown card*

### 4.1.3 Card analysis in progress

In this case the card has been recognized and its certificates are enumerating and loading in the system certificate store (*Windows XP/Vista/7*).



*Figure 8 Card analysis*

### 4.1.4 Card detected and analyzed successfully

Once the certificates are enumerated and loaded into the system certificate store (*Windows XP/Vista/7*) this icon is displayed.

At this point pressing the right mouse button over the icon displays a context menu that allows the user to operate interactively with *Exacard* (see 4.2 Using Exacard monitor)



*Figure 9 Card detected and analyzed successfully*

## 4.1.5 Locked card

This icon indicates that the *Exacard* was detected successfully but it's locked for transport for safety reasons. To use it you need to enter the corresponding transport PIN individually generated and sent by Idoneum Electronic Identity.



Figure 10 Card locked for transport

To enter the the transport code open the context menu of this icon and select **Unlock Transport Code...**

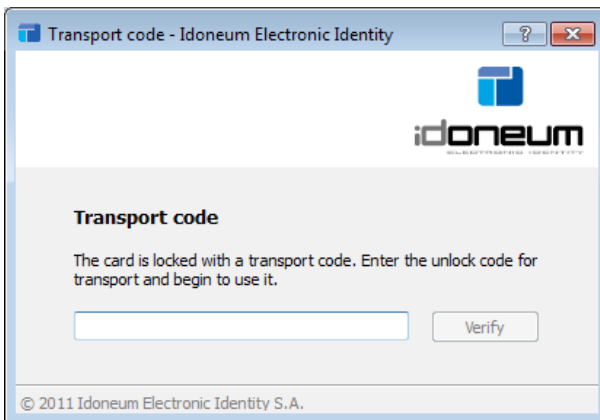


Figure 11 Unlock card

## 4.2 Using Exacard monitor

Once the *Exacard* is inserted into the reader and successfully recognized, from the context menu icon in the notification area the following operations are enabled:

- Delete certificates
- Import PKCS#12 certificates
- Change PIN

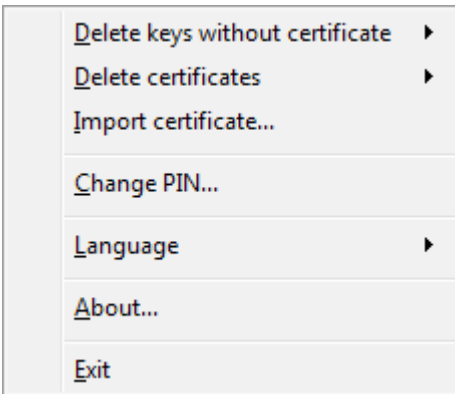


Figure 12 Exacard monitor operations

## 4.2.1 Deleting certificates

This operation lets you view and delete any personal certificate, along with its key pair, from the *Exacard*.

To perform this operation is required the presentation of the user PIN.

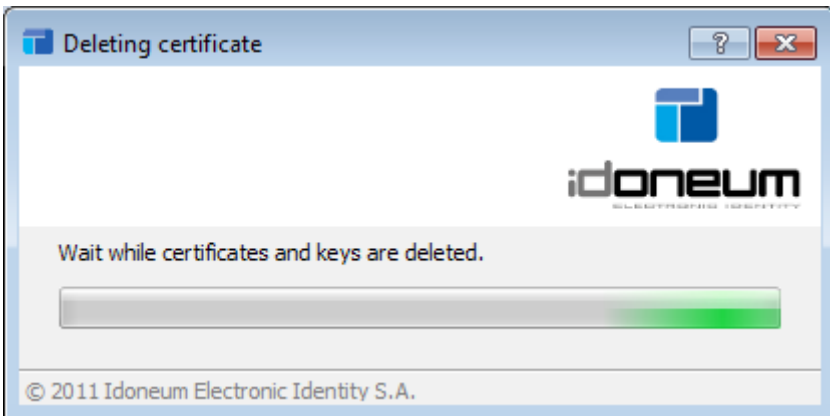


Figure 13 Deleting certificates

## 4.2.2 Importing certificates

This operation allows you to import a personal certificate to the *Exacard*, along with its private key, stored in the system.

It supports PKCS#12 certificates with extensions \*.pfx and \*.p12.

As in the previous operation the user PIN must be presented to import a certificate.

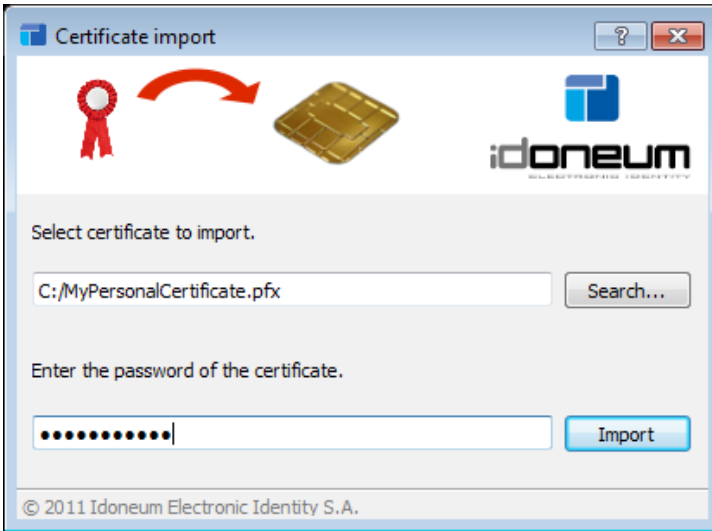


Figure 14 Importing certificates

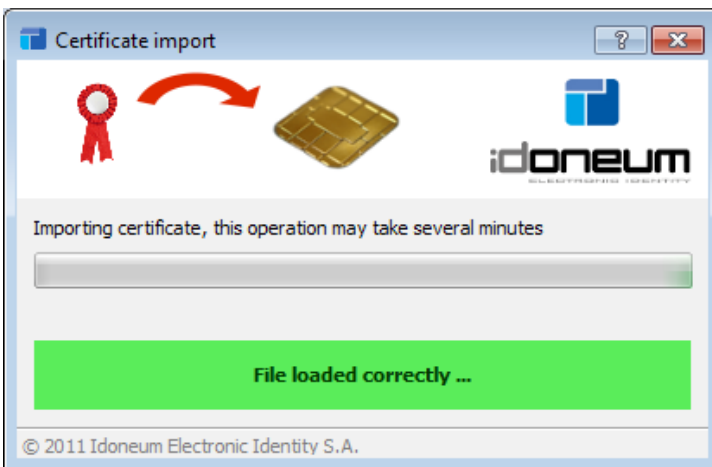


Figure 15 Certificate imported successfully

### 4.2.3 PIN change

With the PIN change operation it's possible to change the current user PIN, if desired.

The new PIN must consist of a string of 6 or more alphanumeric characters up to 20.

To change the PIN is required to present the current stored on the *Exacard*.

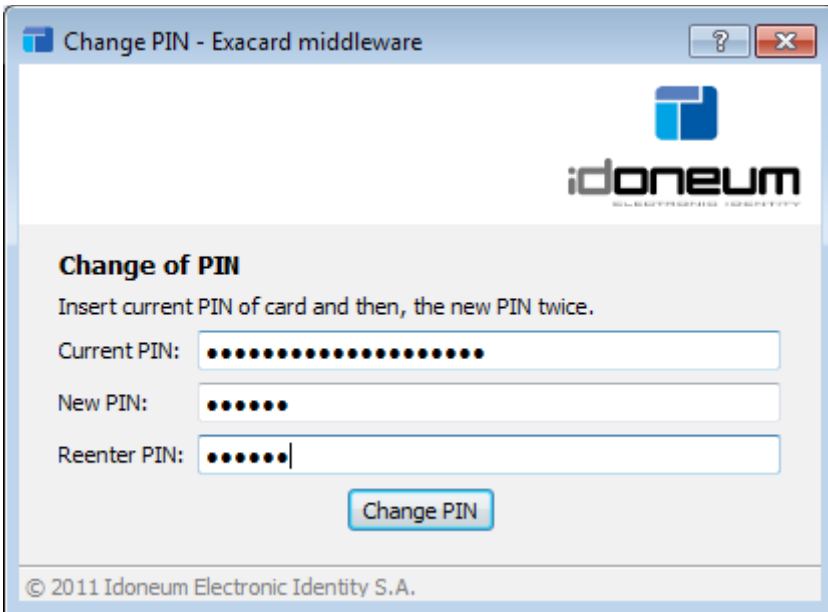


Figure 16 PIN change

---

## 5 Glossary

- **Strong Authentication:** Using this type of authentication provides more protection of private information than a simple username and password can provide. Using a smart card with a corresponding private key and certificate allows a user to be identified by strong authentication.
- **Digital certificate:** A digital document by which a trusted third party (certification authority, certification service provider) ensures the linkage between the identity of a person or entity (name, address, etc.) and a public key.
- **Private key:** In asymmetric cryptography, secret and private component of the key pair that the user protects (e.g. using a Exacard). With this key it's possible to sign documents and decrypt messages.
- **Public key:** In asymmetric cryptography, public component that is normally distributed within its associated digital certificate. With this key other individuals or entities can verify signatures on documents and encrypt messages.
- **Digital Signature:** The digital signature of a document is the result of applying mathematical algorithms to its content using a private key that only the user knows.
- **ISO 7816:** International standard for electronic identification cards, especially smart cards. It's an extension of ISO 7810.
- **Smart Card:** Card with the size of a credit card. They have a microchip for electronic transactions such as electronic identification or financial transactions.



---

## *6 License of use and warranty conditions*

### **Idoneum Electronic Identity, S.A – Exacard Middleware**

Before installing, loading or using this software, please read the terms of use listed below. These conditions define the legal regime which is subjected the cession made of the rights to the software. If you disagree with these conditions, you must return the software.

The installation, loading or use of this software is under total and unconditional acceptance of the usage regime of the software and leads to the agreement of a contract between you and Idoneum Electronic Identity, S.A., governed by the terms and conditions listed below.

Idoneum Electronic Identity, S.A. grants you a non-exclusive, nontransferable right to use the software on one computer and for one user. The authorization extends to the conduct of all operations of software playback (installation, loading and execution) required for use.

The technical and use information that comes with the software, have the same consideration as the contract, and enjoys the same protection provided to the software.

Ownership of the software is not passed by this document, granting a mere right of use. This right of use will last as long as you have installed the software on a computer that is under your possession. If the computer where the software is installed will cease to be in your possession and you were not going to install the software on another computer, you must destroy the copy of the software, and

proceed to it's removal.

During the term of the contract, you agree to the following:

- a. Not to deliver the software to others and to take measures to preserve confidentiality.
- b. Not to modify, copy, or allow others to modify or copy the software or technical documentation in whole or in part.
- c. Not to decompile, disassemble, or allow third parties to decompile or disassemble all or part of the software.
- d. Not to use or permit others to use the software for any purpose other than the mere installation, loading and running on your computer, in the same conditions as it is today.

### **Warranty conditions**

- Idoneum Electronic Identity, S.A., guarantees that the product presents no malfunction and has a warranty of 24 months from the date of acquisition.
- Given the product's functionality, the authorized user must use it only for the purpose stated in the manuals supplied with the product and always following the same instructions.
- Idoneum Electronic Identity, S.A., is committed to repairing the product or where applicable, to replacement thereof, without any charge to the customer during the warranty period, excluding shipping charges, which are always to be borne by the customer. Damage caused during transport or the loss of the product are not covered by this warranty. Also, the following are not covered by this warranty:
  - Damage caused by misuse or negligence caused by the authorized user or third parties.
  - Damage caused by using excessive voltage, leakage of liquid or solid, rust or corrosion.

- Wear produced by normal use of the product.
- Alteration on the product label or serial number.
- Alterations in the exposed parts of the product such as scratches or damage resulting from use.
- Damage caused by the installation, maintenance, operation or defective modification by third parties or by the authorized user, without the express written permission of Idoneum Electronic Identity, S.A..
- Fortuitous event or force majeure. In any case, Idoneum Electronic Identity, S.A., is not responsible in front of the subject or authorized distributors of loss of profits, loss of the product, or the deactivation of the same.
- Obtaining warranty service:
  - To qualify for warranty service of the product will be essential to have the number and invoice date of purchase.
  - Our after-sales service:
    - Our site on the Internet  
<http://www.idoneum.net/>
    - Contact our technical department by mail:  
[suport@idoneum.net](mailto:suport@idoneum.net)