



Manual del Middleware

Idoneum Electronic Identity, S.A

Índice

1	Introducción.....	3
1.1	Sobre el producto.....	3
1.2	A quién va a dirigido.....	4
1.3	Cómo leer este manual.....	4
1.3.1	<i>Convenciones</i>	4
1.3.2	<i>Soporte</i>	4
2	Requisitos del sistema.....	7
2.1	Hardware.....	7
2.2	Software.....	7
3	Instalación software.....	9
3.1	Windows.....	9
4	Exacard monitor.....	15
4.1	Iconos de estado.....	16
4.1.1	<i>Lector sin tarjeta</i>	16
4.1.2	<i>Tarjeta no reconocida</i>	16
4.1.3	<i>Análisis de tarjeta en curso</i>	17
4.1.4	<i>Tarjeta detectada y analizada con éxito</i>	17
4.1.5	<i>Tarjeta bloqueada</i>	18
4.2	Uso de Exacard monitor.....	19
4.2.1	<i>Eliminación de certificados</i>	20
4.2.2	<i>Importación de certificados</i>	20
4.2.3	<i>Cambio de PIN</i>	22
5	Glosario.....	23
6	Licencia de uso y condiciones de garantía.....	25

1 *Introducción*

Gracias por adquirir la tarjeta criptográfica avanzada *Exacard*.

Este es el manual de instalación para el middleware de la tarjeta *Exacard*, donde se especifican las instrucciones para una correcta instalación de los módulos criptográficos CSP y PKCS#11, así como para el uso de la aplicación *Exacard* monitor.

1.1 Sobre el producto

El producto contiene los siguientes elementos:

- Tarjeta *Exacard*.
- Software de instalación y manual de usuario.

La tarjeta *Exacard*, en cuanto a su calidad de Dispositivo Seguro de Creación de Firma (DSCF – SSCD por sus siglas en inglés) en un sistema PKI (*Public Key Infrastructure*), incorpora a las aplicaciones que lo soporten las funcionalidades de autenticación fuerte, firma electrónica, generación y exportación segura de claves criptográficas, y confidencialidad, integridad y protección de sus datos personales.

1.2 A quién va a dirigido

Este manual está pensado para personas con conocimientos básicos respecto al uso de tarjetas inteligentes (smart cards), firma electrónica y certificados PKI.

1.3 Cómo leer este manual

El manual especifica la instalación y uso del middleware de la tarjeta *Exacard*. Está estructurado en una primera parte donde se trata la instalación del software, y una segunda parte donde se trata el uso de la aplicación *Exacard* monitor.

1.3.1 Convenciones

La convención usada para facilitar y resaltar el entendimiento de los pasos a seguir está marcada por:

- ◆ **Negrita**: Indica la etiqueta de los botones que se pulsan durante la instalación y uso.
- ◆ *Cursiva*: Marcas registradas.
- ◆ {}: Indican directorios que se tendrán que sustituir por los correspondientes del usuario.
- ◆ →: Indica la secuencia de menús que se siguen.

1.3.2 Soporte

Puede disponer de soporte técnico a través de:

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

Para más información, por favor, contacte con:

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 Requisitos del sistema

Es imprescindible comprobar que el equipo donde se instala el middleware de la tarjeta *Exacard* cumple con los requisitos mínimos tanto en el software como con el hardware.

2.1 Hardware

- ◆ 50 MB de espacio libre en el disco duro.
- ◆ 25 MB de RAM para *Exacard* monitor.
- ◆ Lector de tarjetas inteligentes que cumpla con la normativa ISO/IEC 7816 y PC/SC (Personal Computer Smart Card).

2.2 Software

- ◆ *Microsoft Windows 7 o XP* para el módulo criptográfico CSP (Cryptographic Service Provider).
- ◆ *Microsoft Windows 7 o XP, GNU/Linux o Mac OS X* para el módulo criptográfico PKCS#11.
- ◆ *Microsoft Windows 7 o XP, GNU/Linux o Mac OS X* para *Exacard* monitor.

3 Instalación software

3.1 Windows

El instalador para *Windows XP* incluye los módulos criptográficos CSP y PKCS#11 junto a la aplicación *Exacard monitor*.



Figura 1: Instalador Exacard Middleware

Instalación

- Continuar con el proceso de instalación está sujeto a la aceptación de los términos y condiciones de uso.

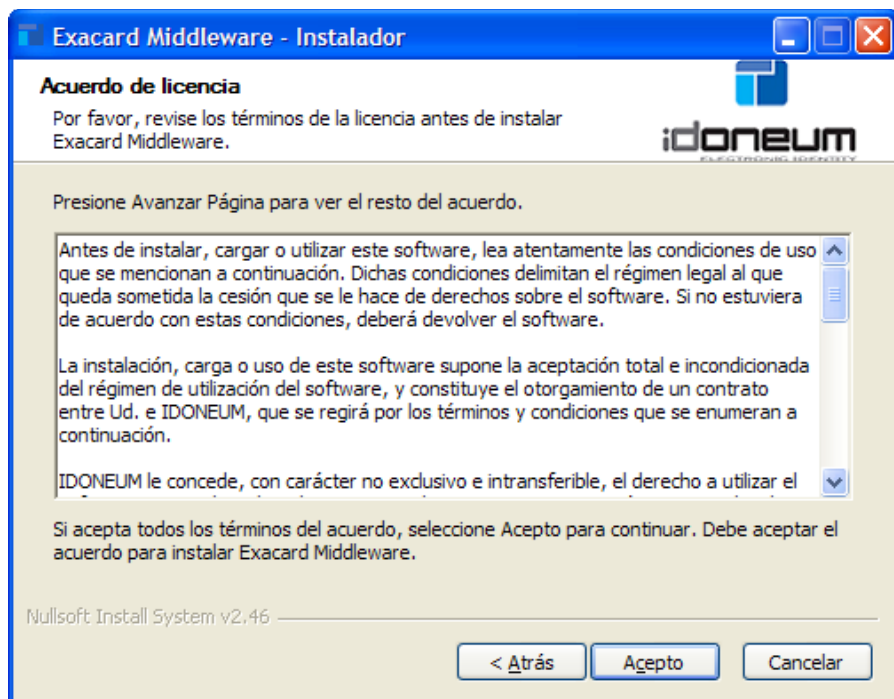


Figura 2: Términos y condiciones de uso

- A continuación se procederá a la selección de los componentes a instalar.

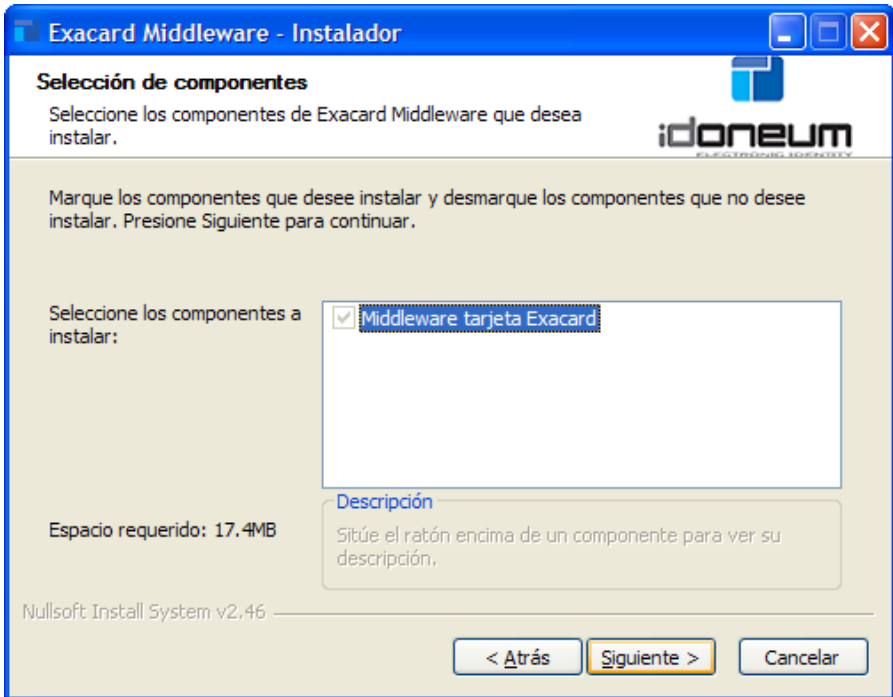


Figura 3: Opciones de instalación

Nota: Esta ventana, a pesar de titularse como “Selección de componentes” y dado que sólo se instala uno global, no permite la selección o deselección del mismo. Esto puede cambiar en futuras versiones.

- Una vez escogidas las opciones se podrá seleccionar la ruta de instalación.

Nota: Durante el proceso que se está describiendo se inicia la instalación del paquete *Microsoft Visual C++ 2008 Redistributable*. Éste paquete tiene un instalador independiente que se ejecutará de forma externa al de *Exacard Middleware*.

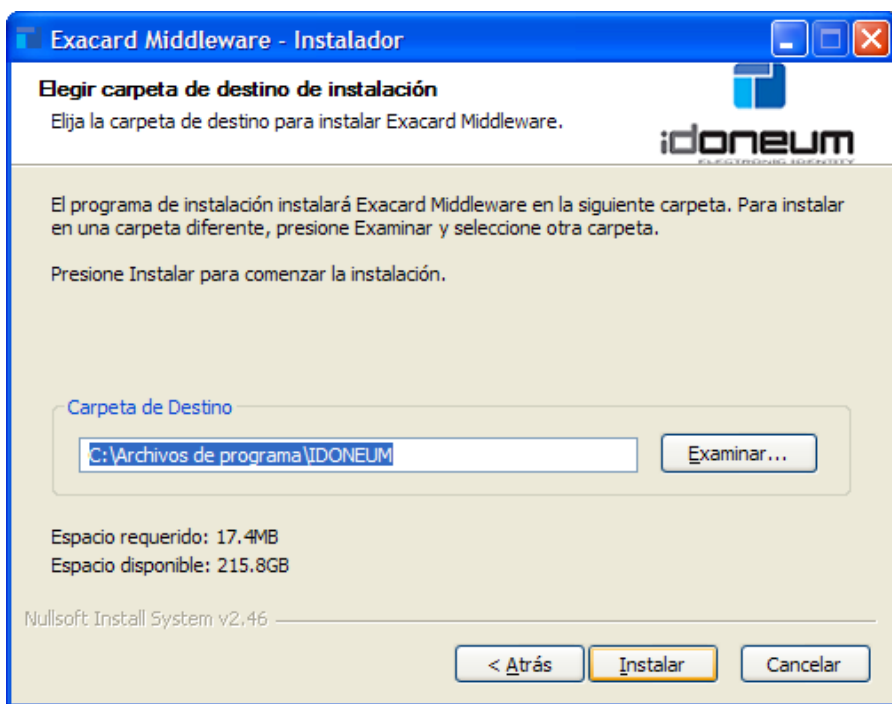


Figura 4: Ruta de instalación

- Pulsar Terminar una vez ha finalizado la instalación.

Desinstalación

- El proceso de desinstalación eliminará del equipo los componentes instalados.

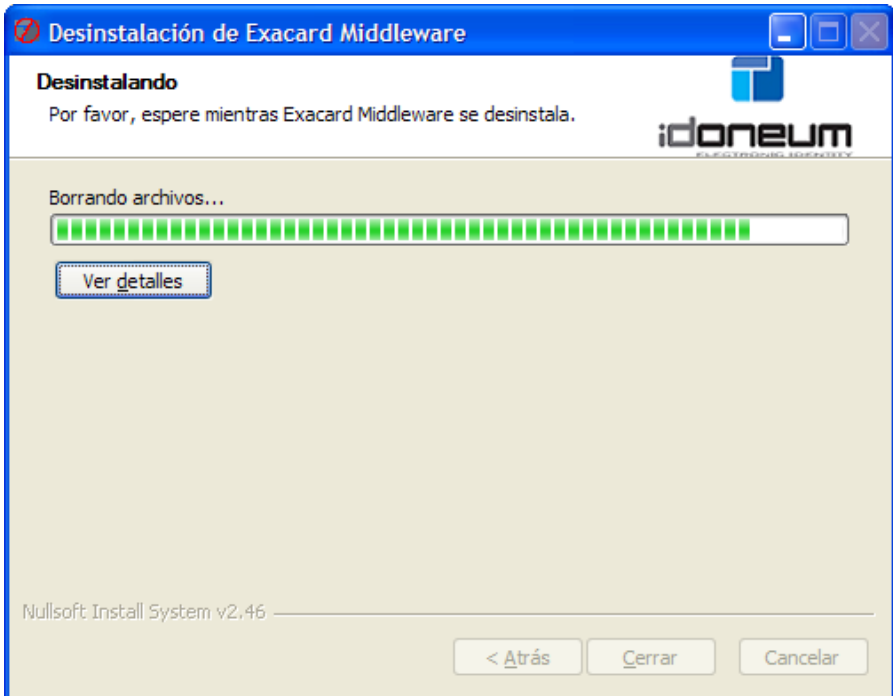


Figura 5: Desinstalación

- Pulsar Terminar una vez ha finalizado la desinstalación.



4 *Exacard monitor*

Una vez instalado el middleware de la tarjeta *Exacard* se lanzará automáticamente la aplicación *Exacard monitor* que será visible a partir de su icono en el área de notificación del sistema operativo.

Exacard monitor ofrece las siguientes funcionalidades:

- Detecta y enumera todos los lectores de tarjeta inteligente instalados en el sistema, mostrando un icono por cada lector.
- Detecta y comprueba el estado (bloqueada, activada, etc.) de las *Exacard* insertadas en los lectores.
- Carga los certificados contenidos en la tarjeta *Exacard* directamente al almacén de certificados del sistema (sólo *Windows 7* y *XP*)
- Importación y eliminación interactiva de certificados en la tarjeta *Exacard*.
- Cambio de PIN de usuario.

4.1 Iconos de estado

A continuación se describen los diferentes iconos que puede adoptar *Exacard* monitor durante su ejecución.

4.1.1 Lector sin tarjeta

Se muestra un icono de este tipo por cada lector instalado en el sistema.



Figura 6 Lector detectado sin tarjeta

4.1.2 Tarjeta no reconocida

Este icono se muestra cuando se ha insertado en el lector una tarjeta no reconocida o se ha insertado de forma incorrecta.



Figura 7 Tarjeta no reconocida

4.1.3 Análisis de tarjeta en curso

En este caso se ha reconocido la tarjeta y se están enumerando y cargando los certificados en el almacén de certificados del sistema (sólo *Windows 7, XP*).



Figura 8 Analizando tarjeta

4.1.4 Tarjeta detectada y analizada con éxito

Una vez enumerados los certificados y cargados en el almacén de certificados del sistema (sólo *Windows 7, XP*) se muestra este icono.

A partir de este momento si se pulsa el botón derecho del ratón sobre el icono se muestra un menú contextual que permite al usuario operar de forma interactiva con la tarjeta *Exacard* (ver 4.2 Uso de Exacard monitor)



Figura 9 Tarjeta detectada y analizada correctamente

4.1.5 Tarjeta bloqueada

Este icono indica que la tarjeta *Exacard* se ha detectado correctamente pero está bloqueada para su transporte por motivos de seguridad. Para poder utilizarla es necesario introducir el correspondiente PIN de transporte generado individualmente y enviado por Idoneum Electronic Identity.



Figura 10 Tarjeta bloqueada para su transporte

Para introducir el código de transporte se ha de abrir el menú contextual de este icono y seleccionar **Desbloquear Código de Transporte...**



Código de transporte - Idoneum Electronic Identity



Código de transporte

La tarjeta está bloqueada con un código de transporte.
Introduzca el código de transporte para desbloquearla y empezar a hacer uso de ella.

Verifica

Encontrará el código de transporte en la documentación suministrada con la tarjeta.

Figura 11 Desbloquear tarjeta

4.2 Uso de Exacard monitor

Una vez insertada la tarjeta *Exacard* en el lector y reconocida correctamente, desde el menú contextual del icono del área de notificación se habilitan las siguientes operaciones:

- Eliminación de certificados
- Importación de certificados PKCS#12
- Cambio de PIN

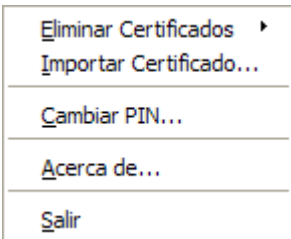


Figura 12 Operaciones Exacard monitor

4.2.1 Eliminación de certificados

Esta operación permite visualizar y eliminar cualquier certificado personal, junto con su par de claves, contenido en la tarjeta *Exacard*.

Para poder efectuar esta operación es necesaria una correcta presentación del PIN de usuario.

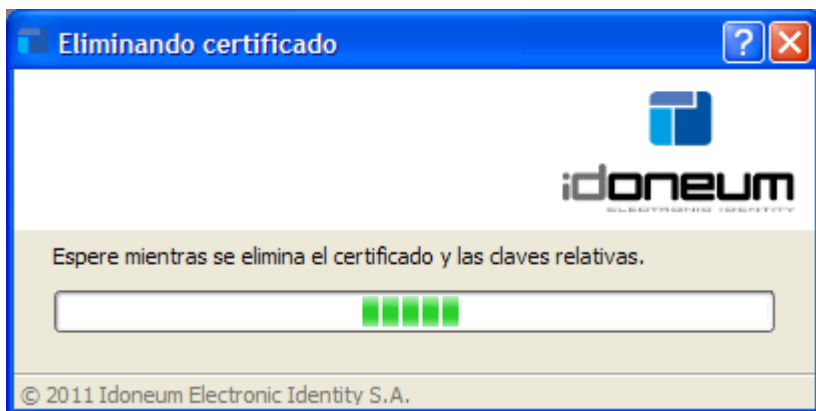


Figura 13 Eliminación de certificados

4.2.2 Importación de certificados

Esta operación permite importar a la tarjeta *Exacard* certificados personales, junto con su clave privada, almacenados en el sistema.

Se soportan certificados PKCS#12 con extensiones *.pfx y *.p12.

Al igual que en la operación anterior es necesaria una correcta presentación del PIN de usuario para poder importar un certificado.



Figura 14 Importación de certificados

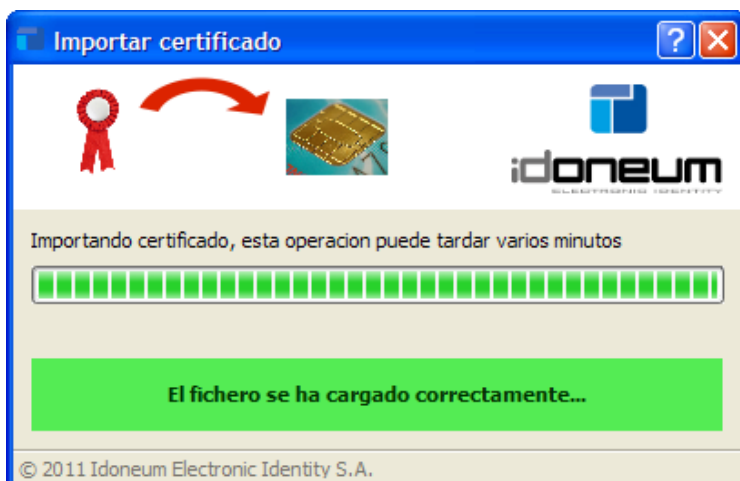


Figura 15 Certificado importado con éxito

4.2.3 Cambio de PIN

Con la operación de cambio de PIN es posible cambiar el PIN actual de usuario, siempre que se desee.

El nuevo PIN ha de estar formado por una cadena de 6 o más caracteres alfanuméricos hasta un máximo de 20.

Para poder cambiar el PIN es necesario presentar el actual almacenado en la tarjeta *Exacard*.

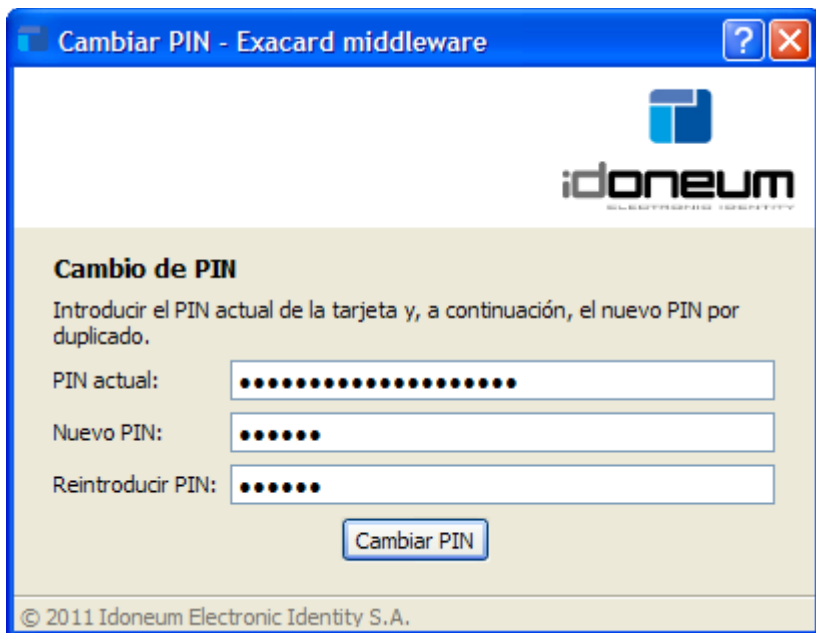


Figura 16 Cambio de PIN

5 Glosario

- **Autenticación fuerte:** El uso de este tipo de autenticación proporciona más protección de la información privada que la que un simple username y password pueden proporcionar. El uso de una tarjeta inteligente con un clave privada y su correspondiente certificado permite a un usuario identificarse mediante autenticación fuerte.
- **Certificado digital:** Documento digital mediante el cual un tercero de confianza (autoridad de certificación, prestador de servicios de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (nombre, dirección, etc.) y una clave pública.
- **Clave privada:** En criptografía asimétrica componente secreto y privado del par de claves que su usuario protege (por ejemplo con una tarjeta inteligente criptográfica Exacard). Con esta clave se pueden firmar documentos y descifrar mensajes.
- **Clave pública:** En criptografía asimétrica componente público del par de claves que normalmente se distribuye dentro de su certificado digital asociado. Con esta clave otros sujetos o entidades pueden verificar firmas de documentos y cifrar mensajes.
- **Firma digital:** La firma digital de un documento es el resultado de aplicar una serie de algoritmos matemáticos a su contenido empleando una clave privada que sólo su usuario conoce.
- **ISO 7816:** Estándar internacional para las tarjetas de

identificación electrónicas, especialmente tarjetas inteligentes. Es una extensión de la ISO 7810.

- **Tarjeta Inteligente (Smart Card):** Tarjeta del tamaño de una tarjeta de crédito. Disponen de un microchip para realizar transacciones electrónicas tales como identificación electrónica u operaciones financieras.

6 Licencia de uso y condiciones de garantía

Idoneum Electronic Identity, S.A – Exacard Middleware

Antes de instalar, cargar o utilizar este software, lea atentamente las condiciones de uso que se mencionan a continuación. Dichas condiciones delimitan el régimen legal al que queda sometida la cesión que se le hace de derechos sobre el software. Si no estuviera de acuerdo con estas condiciones, deberá devolver el software.

La instalación, carga o uso de este software supone la aceptación total e incondicionada del régimen de utilización del software, y constituye el otorgamiento de un contrato entre Ud. e Idoneum Electronic Identity, S.A., que se regirá por los términos y condiciones que se enumeran a continuación.

Idoneum Electronic Identity, S.A. le concede, con carácter no exclusivo e intransferible, el derecho a utilizar el software en un solo ordenador y por un solo usuario. La autorización se extiende a la realización de todas aquellas operaciones de reproducción del software (instalación, carga y ejecución), necesarias para su uso.

La información técnica y uso que se entrega junto con el software, tienen su misma consideración como objeto del contrato, y goza de la misma protección que se dispensa al software.

La propiedad del software no se le transmite por el presente documento, concediéndose un mero derecho de uso. Este derecho de uso durará mientras tenga instalado el software en un equipo que se encuentre bajo su posesión. En caso de que el equipo

donde esté instalado el software, vaya a dejar de estar bajo su posesión y Ud. no fuera a instalar el software en otro equipo, debe destruir la copia del software, y proceder a su desinstalación.

Durante la vigencia del contrato, Ud. se compromete a lo siguiente:

- a. A no entregar el software a terceros y a tomar las debidas precauciones para preservar su carácter confidencial.
- b. A no modificar ni copiar, ni permitir que terceros modifiquen o copien el software ni la documentación técnica en su totalidad o parcialmente.
- c. A no descompilar, desensamblar, ni permitir que terceros descompilen o desensamblen total o parcialmente el software.
- d. A no usar ni permitir que terceros usen el software para una finalidad distinta de su mera instalación, carga y ejecución en su equipo, en las mismas condiciones en que se encuentra actualmente.

Condiciones de garantía

- Idoneum Electronic Identity, S.A., garantiza que el producto no presenta ningún defecto de funcionamiento y cuenta con una garantía de 24 meses a contar desde la fecha de adquisición.
- Teniendo en cuenta la funcionalidad del producto, el usuario autorizado deberá utilizarlo únicamente para la finalidad que se indica en los manuales suministrados con el producto y siguiendo en todo momento las instrucciones de los mismos.
- Idoneum Electronic Identity, S.A., se compromete a la reparación del producto o en su caso, a la sustitución del mismo, sin cargo para el cliente durante la vigencia de la garantía, a excepción de los gastos de envío, que serán siempre a cuenta del cliente. Los daños ocasionados durante el transporte o el extravío del producto no quedan

cubiertos por esta garantía. Del mismo modo que no queda cubierto por esta garantía:

- Daños ocasionados por uso indebido o negligente por parte del usuario autorizado o terceros.
 - Daños ocasionados por uso de voltaje excesivo, derrames de líquidos o sólidos, oxidación o corrosión.
 - Desgaste normal por el uso del producto.
 - Alteración de la etiqueta del producto o de su número de serie.
 - Alteraciones en las partes expuestas del producto tales como rayadas o daños derivados del uso.
 - Daños ocasionados por la instalación, mantenimiento, operación o modificación defectuosa, realizados por terceros o por el usuario autorizado, sin la autorización expresa y por escrito de Idoneum Electronic Identity, S.A..
 - Caso fortuito o fuerza mayor. En ningún caso, Idoneum Electronic Identity, S.A., se responsabilizará frente al interesado o distribuidores autorizados de lucro cesante o de la pérdida del producto, así como de la inutilización del mismo.
- Obtención del servicio de garantía:
 - Para acogerse al servicio de garantía del producto, será imprescindible disponer del número y fecha de la factura de compra del producto.
 - Nuestros servicios post-venta:
 - Nuestra web en Internet
<http://www.idoneum.net/>

- Contacto con nuestro departamento técnico por correo:
suport@idoneum.net