



Token User Guide

Version 1.0/ July 2013

Index

Overview	3
Usage requirements	4
KIT contents	5
Smart Card installation	6
Reader driver installation	7
<i>In the case of Windows XP.....</i>	<i>7</i>
<i>In the case of Windows Windows 7</i>	<i>7</i>
Starting the device	8
<i>Auto-Start</i>	<i>9</i>
The taskbar	10
Application	12
Online authentication with Firefox	13
“Import” certificate	15
Management of Smart Card	21
<i>Change PIN Code</i>	<i>21</i>
<i>Unlock PIN.....</i>	<i>22</i>
<i>Change PUK Code</i>	<i>23</i>
<i>Smart Card Information.....</i>	<i>24</i>
<i>Smart Card Management error codes.....</i>	<i>25</i>
Auto-diagnosis of the Aruba Key device.....	27
Options	30
<i>Proxy Setting</i>	<i>30</i>
<i>Language Setting</i>	<i>32</i>

Overview

This section contains the User Manual of the TOKEN USB device “**Aruba KEY™**”. In the rest of this section it will be referred to simply as TOKEN.

It is recommended to read this manual before using the TOKEN.

The TOKEN is the ideal solution for who wants a **portable** and **install-free** digital signature tool, ready to be used in any moment and on any PC.

It is an advanced USB device, which looks like a standard USB memory key which allows to always have with you everything you need to:

- digitally sign documents;
- authenticate with strong encryption when accessing web sites (using the SSL protocol);
- surf the web (even web sites that use Java applets) with a built-in browser;
- save and always carry with you your documents and any kind of file.

The TOKEN contains:

- a **cryptographic chip** in which there are the user’s certificates protected by a PIN code;
- a 2 GB Flash memory that comes with the pre-installed apps that are described further on in this document.

To use the TOKEN it is **simply** to connect it to a PC’s USB port, activate your Internet connection and follow the instructions given in this manual.



Usage requirements

The TOKEN can be used on any PC equipped with the following requirements:

- Windows XP (with service pack 3), Vista, Windows 7, Windows Server 2003, Windows Server 2008 (32 and 64bit)
- one free USB 2.0 port;
- an Internet connection.

Although Windows Vista is supported by the token, it is not supported by TARGET2 -SSP platform.

We recommend using a high quality **antivirus** software.

In order to create digital signatures and to use strong on-line authentication, the cryptographic chip must contain the appropriate certificates.



In order to guarantee the correct operation of the TOKEN, the user shall not modify in any way the software that comes preinstalled on the device.

If you modify in any way the software pre-installed on the TOKEN device (eg: adding or removing apps or add-on/plugin) or modify the configuration, we do not guarantee the product will work.

KIT contents

The TOKEN is provided in a kit which also includes an envelope containing the cryptographic chip secret PIN and PUK codes.

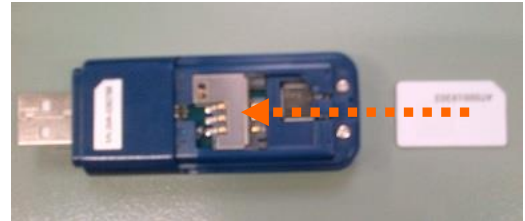
The user shall verify the contents of the KIT and the integrity of the envelope containing the secret codes. Important information on the PIN and PUK codes are in the chapter “Management of Smart Card”.

Smart Card installation

If the smart card is not already inserted remove the protective cover, on the back of the device, and slide it off. Once you have opened the smart card reader, insert the Digital Signature SIM, as shown below.

Step 1:

Insert the SIM card with the chip faced down as shown in the image.



Step 2:

After inserting the SIM card, put the cover back.



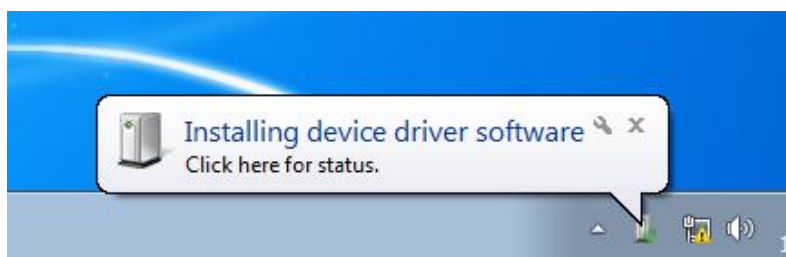
Reader driver installation

In the case of Windows XP

The installation is automatic and requires no user action

In the case of Windows Windows 7

The installation is automatic and requires no user action. After having inserted the TOKEN in the USB port, the following message (“Installing device driver”) will appear at the bottom right side of the screen:



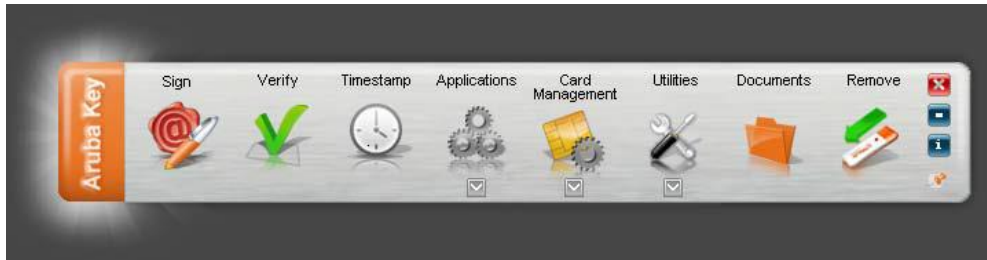
The TOKEN is identified by the PC as a HID (Human Interface Device), therefore the drivers are found in the device itself for it to be recognized correctly.



From this moment on, the TOKEN will be recognized by the operating system as a standard smart-card reader as well as a removable storage device.

Starting the device

If the PC has the Auto-run function active when connecting the TOKEN the toolbar will automatically come up as shown below.

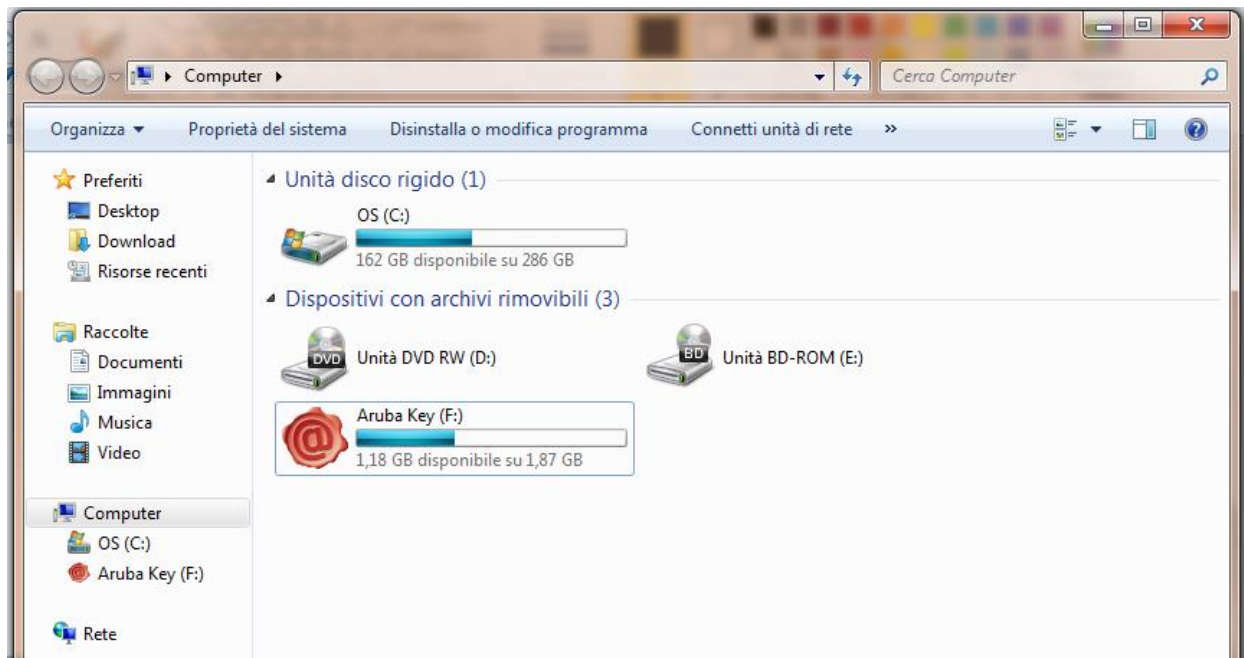


The “Autorun” feature of the Windows 7 operating system never suggests the start of Flash memory-resident software, so it cannot be used to start the TOKEN. In this case there are two possible solutions:

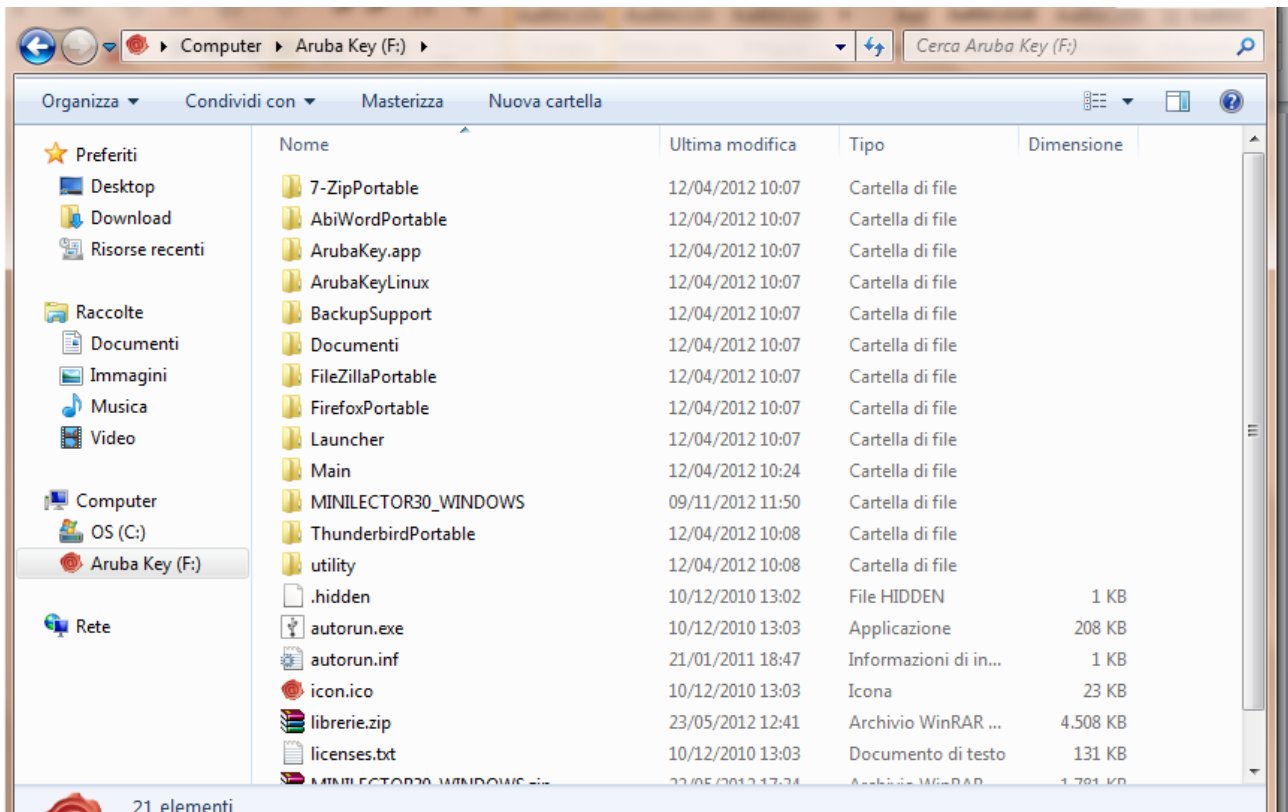
- 1) manual start;
- 2) use of the Auto-Start feature of Actalis (see following section).

To manually start the taskbar, follow these steps:

- view the resources of the computer (Windows key + E) and locate the removable device “Aruba Key” as shown in the figure below:



double click on the TOKEN (Aruba Key) to view its contents, as shown in the following figure:



- finally, double-click the autorun.exe file (“Application” Type) to start the Taskbar

Auto-Start

It is possible to make the taskbar start automatically when the TOKEN is inserted in the USB port, regardless of Windows’s Autorun/AutoPlay mechanism. To obtain this result, follow these steps:

- start the taskbar manually (Figure 1 page 16);
- select “Auto-start”;
- select “YES” in the dialogue box that appears:

From this moment on, the taskbar will start automatically when you insert the TOKEN in the USB port.

This procedure must be repeated on each PC on which you want to activate the Auto-Start.

To disable the Auto-Start of the TOKEN you must simply click on the Auto-Start icon again and select “YES” in the dialogue box which appears:

This feature is especially useful in Windows 7, for the reasons already mentioned in the previous section. However it can be used on Windows XP and Vista as well (in these cases we recommend to disable the Autorun/Auto Play feature to avoid interference).

The taskbar


After starting the TOKEN, as described previously, the following taskbar will appear on the PC Desktop:






Figure 1: The TOKEN taskbar

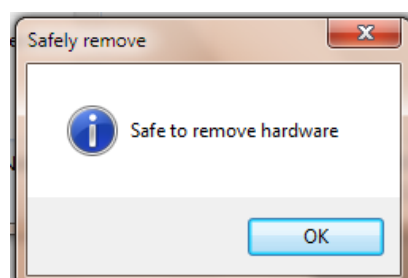
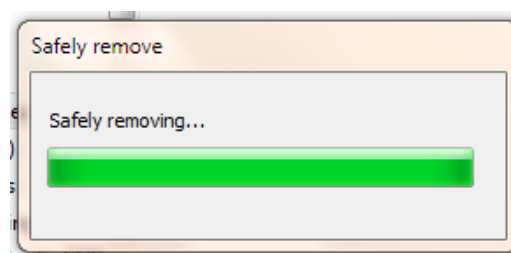
The bar allows you to start the desired application with a single click.

You can move the taskbar on your Desktop, dragging one side of the bar it with the mouse.




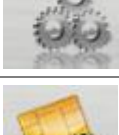



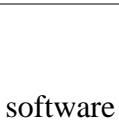
Clicking on the  in the upper right corner of the bar, the taskbar is closed but.

Clicking on the  in the upper right corner of the bar, the taskbar is hidden. To display it again just click once on the icon  that is in the notification area of Windows.

To remove the TOKEN, clicking on , the following figure appear:



The table below describes the applications normally installed on the TOKEN:

Icon	Application	Description
	Sign	Sign a File
	Verify	Verification of signed file
	Timestamp	Adding timestamps
	Application	Contains the application portable like FireFox.
	Card Management	Management of smart card.
	Utilities	Contains various utilities like Auto-diagnostic.
	Personal documents	Direct access to the TOKEN's "Documents" folder, where the user can store all documents and personal files.
	Safely remove hardware	Allows the "safe removal" of the device, to prevent data loss that may occur when pulling device out of the USB port suddenly.

All the software necessary for the operation of the TOKEN is in the \Aruba Key Flash Memory folder. Be careful not to alter the contents of that folder.

In general, instructions for the use of the various available applications (Sign, Verify, Firefox, etc.) are accessible directly from within the applications themselves.







The cryptographic TOKEN contains a microchip that is *identical* to the traditional **smartcard** one. With TOKEN is possible, among other things, authenticate on websites that require **access by smart card**.

Application

Clicking on “**Applications**” icon on taskbar the following figure appear:

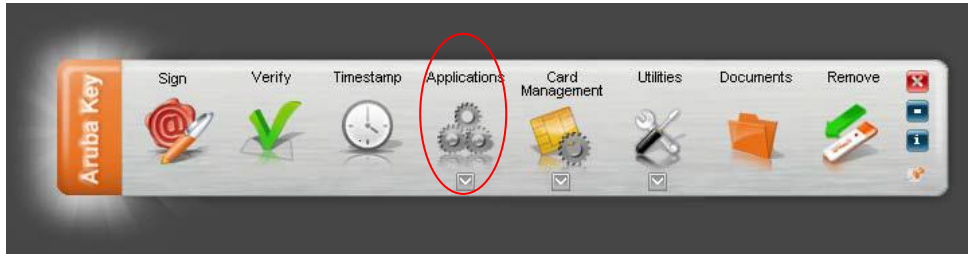


The table below describes the applications:

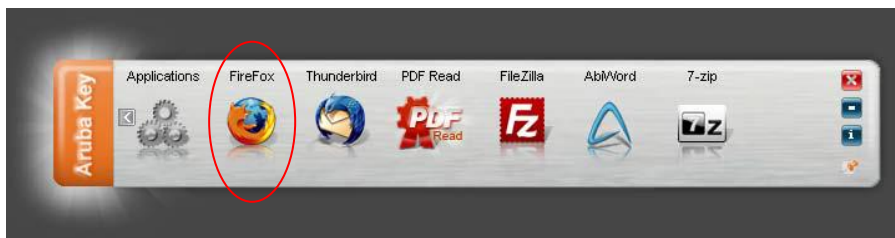
Icon	Application	Description
	Mozilla Firefox	High quality and safety web browser
	Thunderbird	Email client
	PDR Read	Pdf Reader
	FileZilla	FTP client
	AbiWord	Document processor in format compatible with Microsoft Word™.
	7-zip	File Archiver.

Online authentication with Firefox

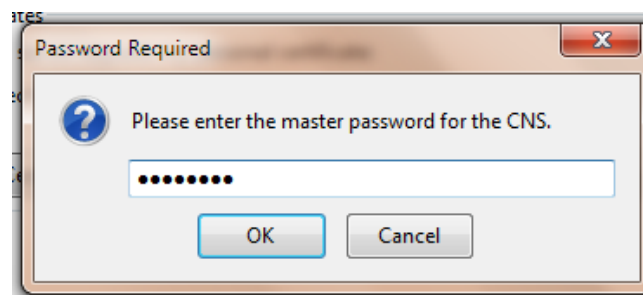
To access the “Mozilla FireFox Portable Edition” found in TOKEN click on the “**Applications**” icon.



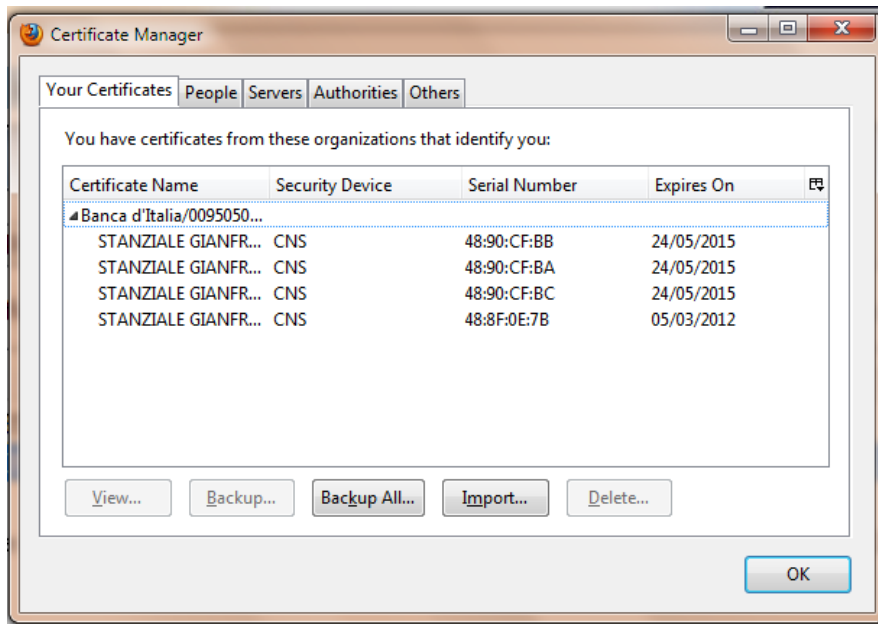
Click on **Firefox**:



Select Tools → Options → Advanced → Coding → “**Show Certificates**” and enter the PIN when requested



Your certificates, found TOKEN, are displayed in the ‘Personal certificates’ tab



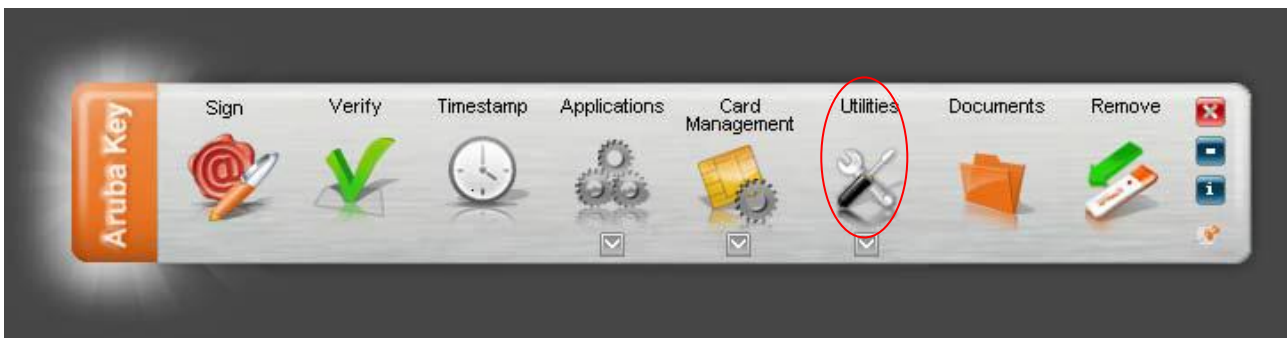
ATTENTION: Should the Qualified and authentication certificates be imported in the Mozilla FireFox Store you must not click on the "Delete.." button. This could cause the certificates to be deleted from the smartcard and not be recuperated.

“Import” certificate

The “Import” certificate function allows you to import TOKEN certificates in the local certificates store making it possible for the applications found in the host pc to interface with the device like for example: Internet Explorer, Adobe Reader (Professional), Safari, , etc...

NOTE: To activate this function you must have the PC administrator privileges.

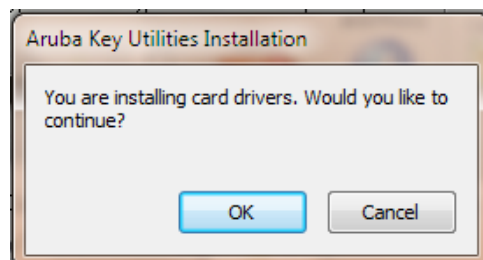
To activate the “import” of the certificate, click on “**Utilities**”.



Click on “**Import Certificate**”



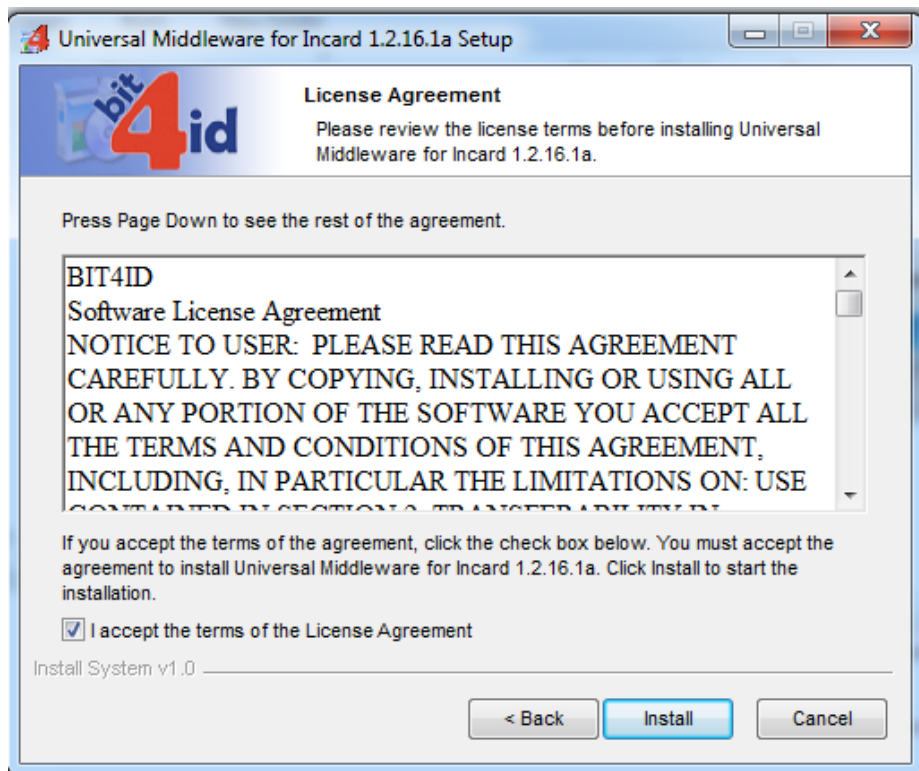
Follow the installation wizard accepting the contract conditions and clicking on OK in each page.



After a few seconds the following dialogue box will appear:

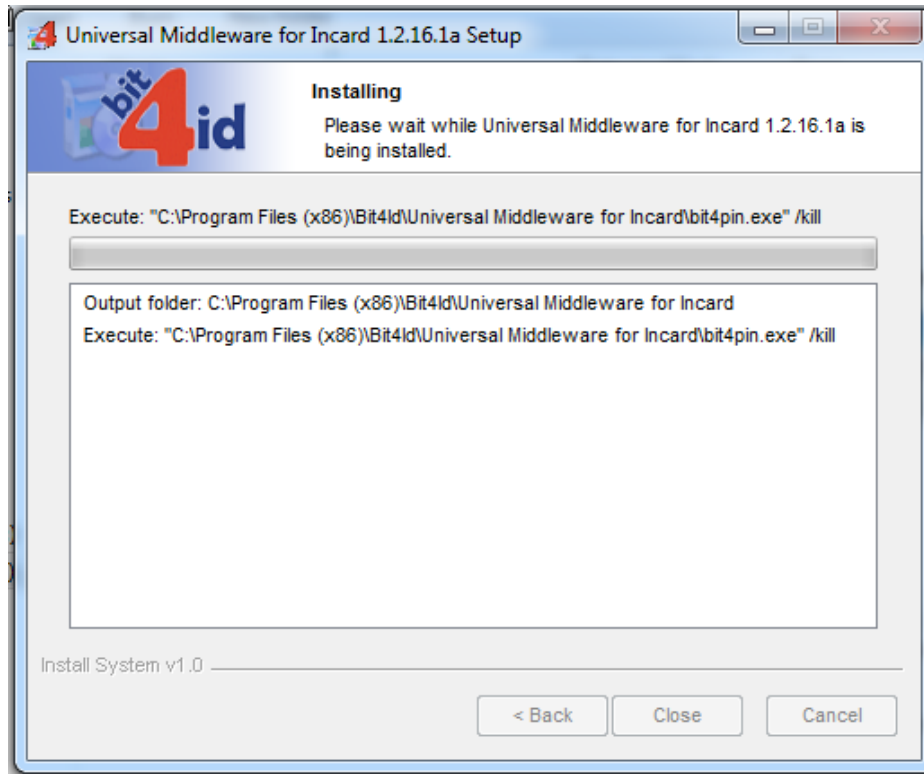


Clicking on "Next>" to proceed, the following window appears:

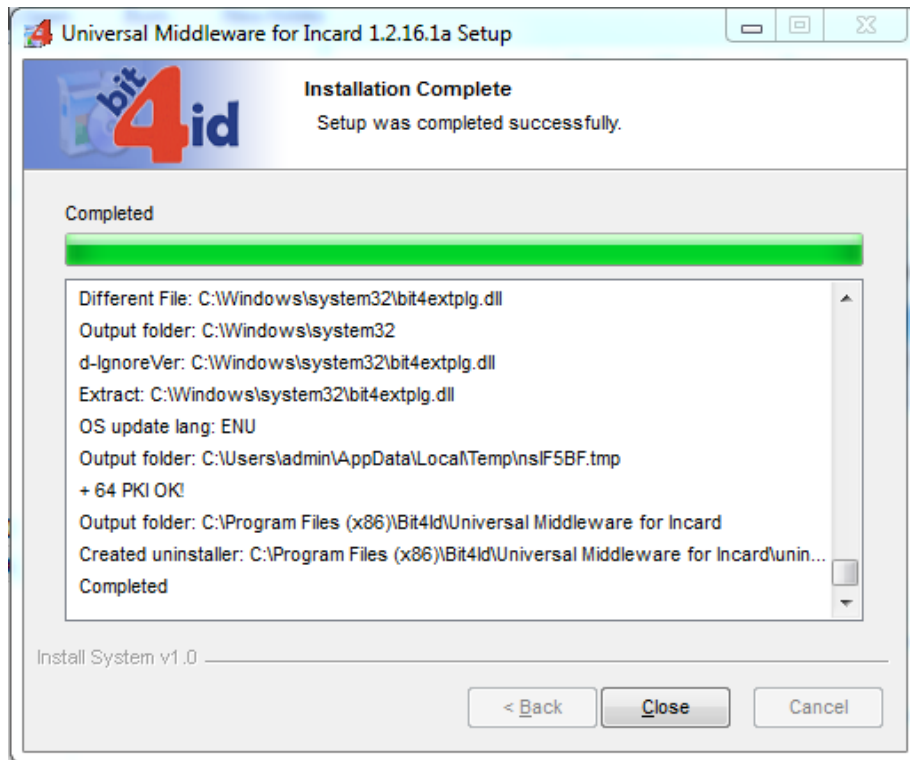


Check the flag 'I accept the terms of the License Agreement'.

Clicking on 'Install' to proceed, the following window appears:

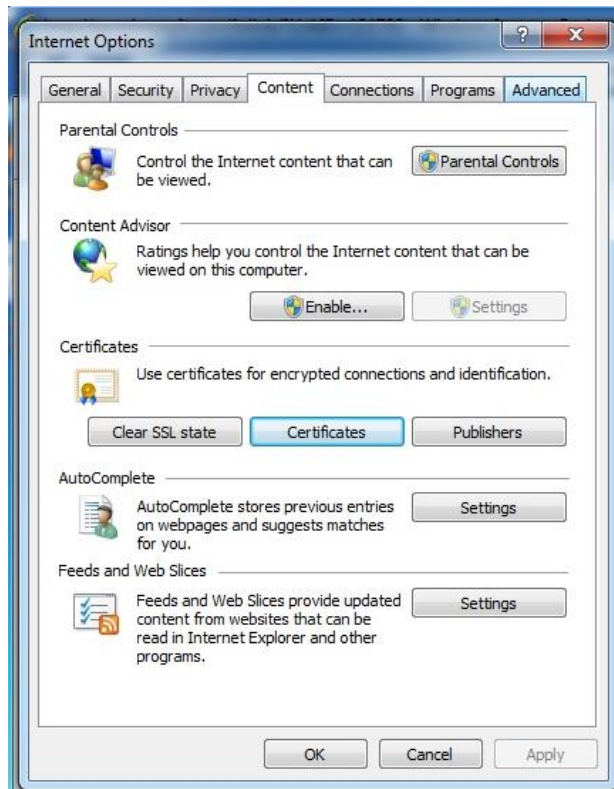


Within a few seconds (normally) the final window informing that the driver is installed appears. Click on "Close" to close the wizard.

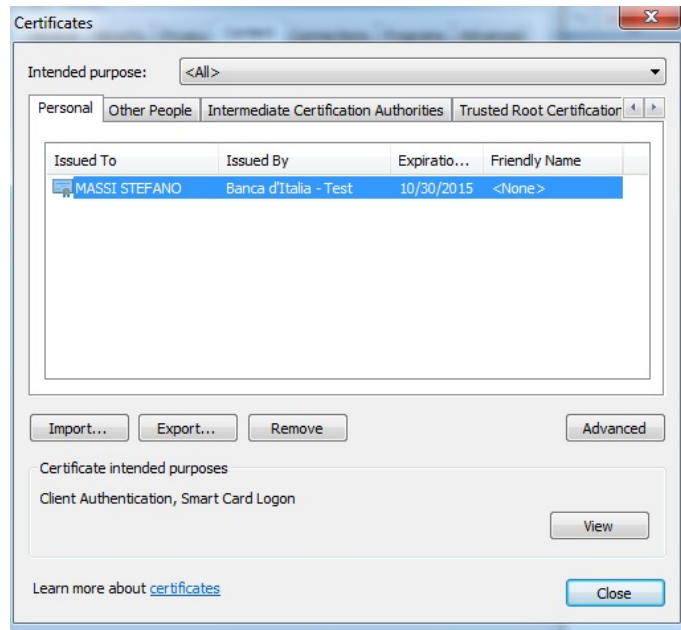


Verify that the certificate has been installed correctly by following these steps:

1. Start Microsoft Internet Explorer;
2. Select Tools → Internet Options;
3. Select the Content tab, click on the Certificates button and then the Personal tab.
4. Check that the certificates installed on TOKEN are listed
5. Click on “Close”

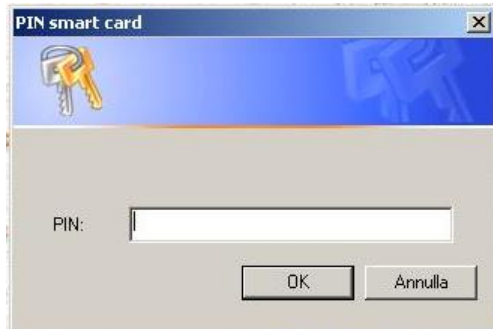


In this windows, click on 'Certificates', window like this appears:



When you connect to a web site requiring strong authentication (e.g. TARGET2 ICM), Microsoft IE shows the authentication certificate store on TOKEN.

Select the certificate and click on 'OK', the browser asks the PIN with a window like this:



Management of Smart Card

We have already said that the encryption chip built-in the TOKEN is technologically and functionally identical to a traditional smart card (we therefore use the term "smart card" as a synonym below). Therefore, it is also protected by a confidential code called PIN. As said before, the PIN code is part of the KIT.

The PIN allows you to carry out, in a secure way, operations, such as digital signature and authentication on-line. These operations use the user's private RSA key which is inside the encryption chip.

Keep your PIN in a safe place separate from the where you keep the TOKEN, to prevent its fraudulent use by unauthorized parties.

For security reasons, if you enter an incorrect PIN for more times in a row (three attempts) the PIN blocks. In this case, you cannot use the smart card until it is "unblocked".

To unlock the smart card, you must use the second secret code called **PUK** (unlock functionality is available within the application File Protector).

You must pay the utmost attention to entering the PUK code correctly, as this too is subject to block in case of repeated errors.

In the case of block of the PUK as well (maximum three attempts), *it is not possible* to restore the normal functioning of the cryptographic chip inside the TOKEN.

Change PIN Code

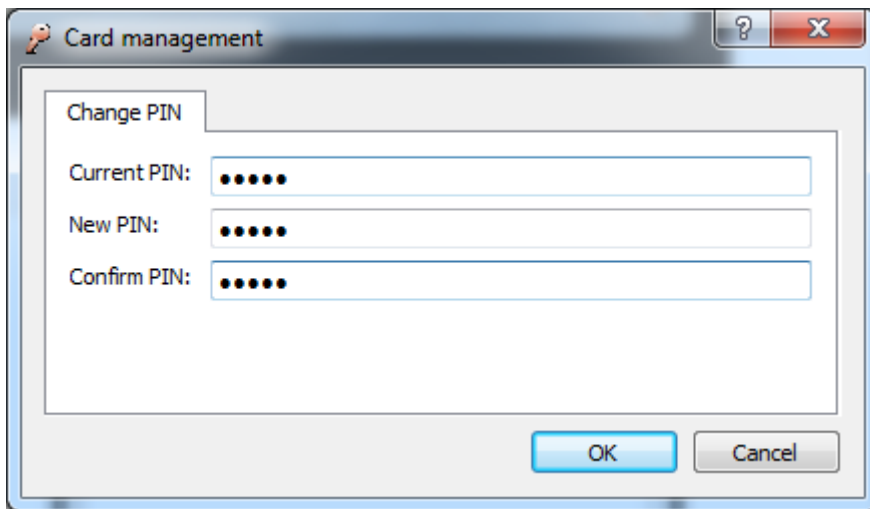
To change the PIN code of the smart card found in TOKEN click on the “**Card Management**” button.



Click on “**Change PIN**”.

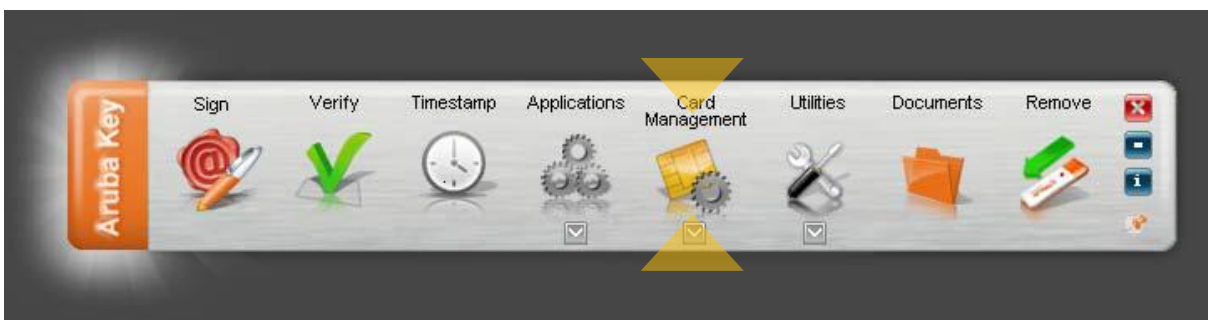


In the “**Change Pin**” window enter the previous PIN, then enter the new Pin and click on OK

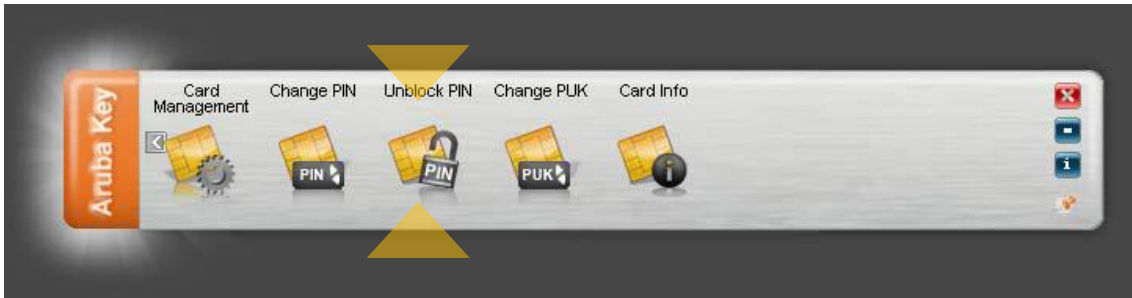


Unlock PIN

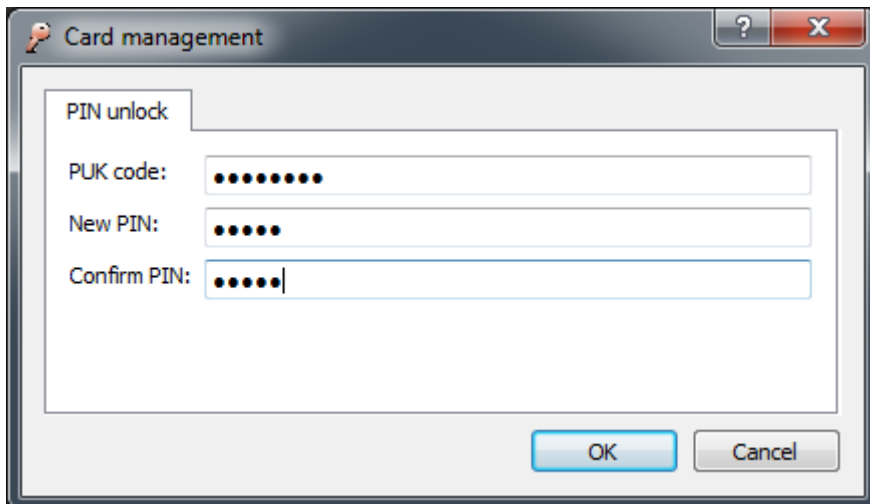
To unlock the PIN code of the smart card found in TOKEN click on the “**Card Management**” icon.



Click on the “**Unlock PIN**” icon.

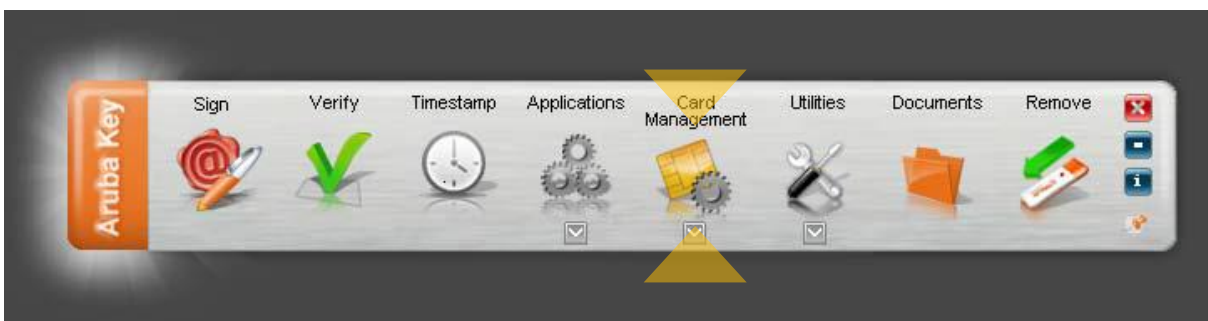


In the “**Unlock Pin**” window enter the PUK code, then enter the new PIN and click on OK.

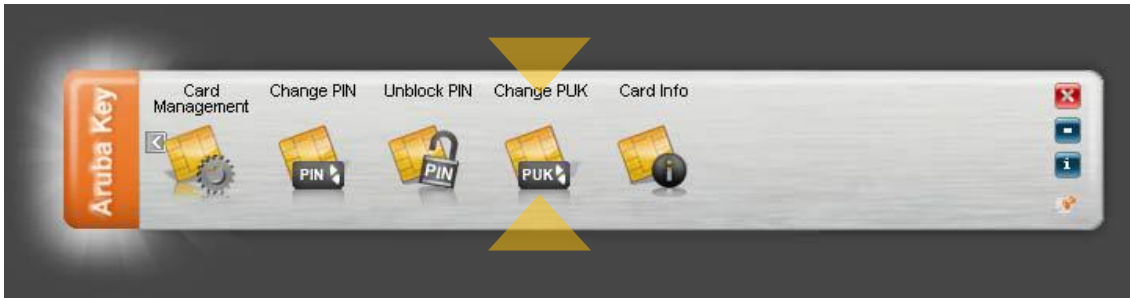


Change PUK Code

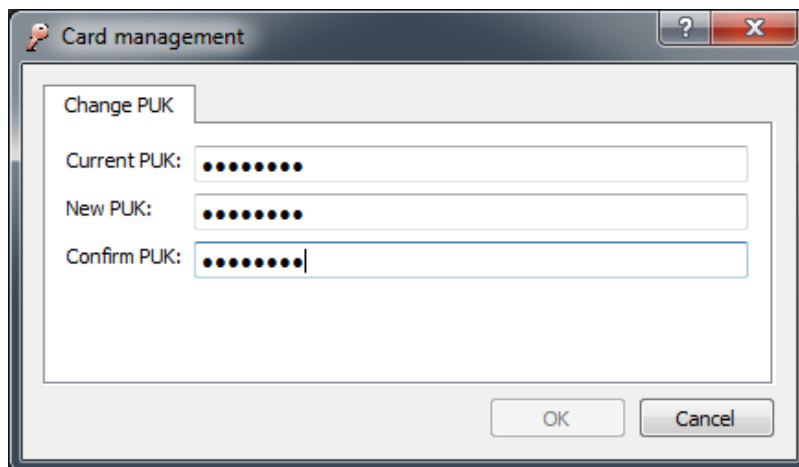
To change the PUK code of the smart card found in TOKEN click on the “**Card Management**” icon.



Click on “**Change PUK**”.

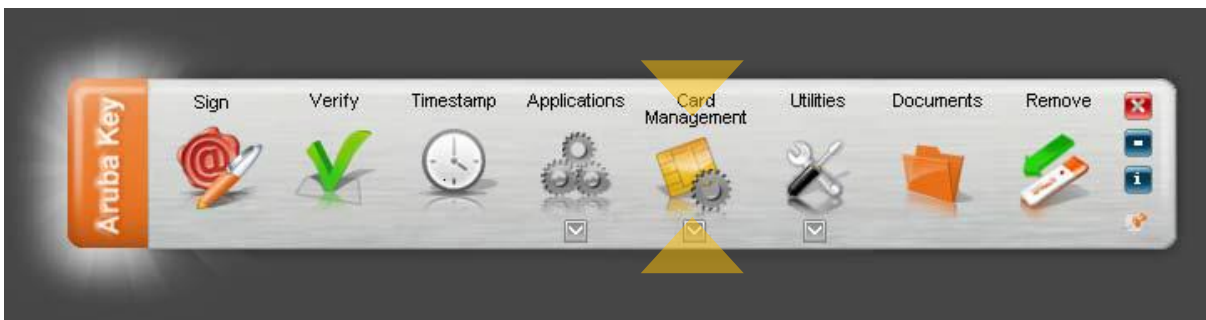


In the “**Change PUK**” window enter the previous PUK, then enter the new one and click on OK.



Smart Card Information

To get the information on the smart card found in the TOKEN click on “**Card Management**”.

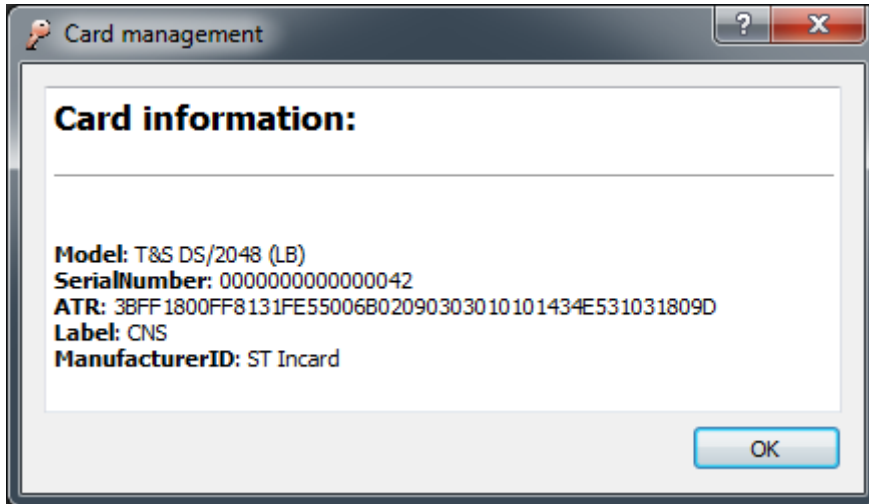


Click on “**Card Info**”

In the “Manage Smart Card” window you will find the following information:

- Model;

- Serial Number of the smart card;
- ATR of the smart card;
- Any Label that is associated to the smart card;
- Manufacturer of the smart card



Smart Card Management error codes

When **changing the PIN**, **unlocking the PIN** and **changing the PUK**, the TOKEN may give the following error messages:

<p>Error: <i>The current Pin is not correct.</i> Warning: <i>too many incorrect attempts may lock the PIN.</i></p>	<p>This message indicates that the “Old Pin” field of the “Change Pin” window, is not correct.</p> <p>In this case the user needs to bear in mind that by attempting to enter the incorrect PIN repeatedly may cause the PIN to lock and therefore the smart card.</p>
<p>Error: <i>The PIN is locked.</i></p>	<p>This message indicates that the PIN of the smart card is locked.</p> <p>You need to unlock the PIN by following the indications found in the “Unlock PIN” paragraph.</p>
<p>Error: <i>The PUK Code is not correct.</i> Warning: <i>too many incorrect attempts may</i></p>	<p>This message indicates that the “Puk” field of the “Unlock Pin” window, is not correct.</p>

<p><i>lock the PUK!</i></p>	<p>In this case the user needs to bear in mind that by attempting to enter the incorrect PUK repeatedly may cause the smart card to lock <u>permanently</u></p>
<p><i>Error: The current PUK is not correct.</i> <i>Warning: too many incorrect attempts may lock the PUK!</i></p>	<p>This message indicates that the “Puk” field of the “Change Puk” window, is not correct.</p> <p>In this case the user needs to bear in mind that by attempting to enter the incorrect PUK repeatedly may cause the smart card to lock <u>permanently</u></p>
<p><i>Error: The PUK is locked.</i></p>	<p>This message indicates that the PUK of the smart card is locked.</p> <p>The user needs to contact the Certification Authority in order to revoke the current certificates and purchasing a new smart card.</p>

Auto-diagnosis of the Aruba Key device

Step 1

To access the auto-diagnosis application found in the TOKEN click on “**Utilities**”.



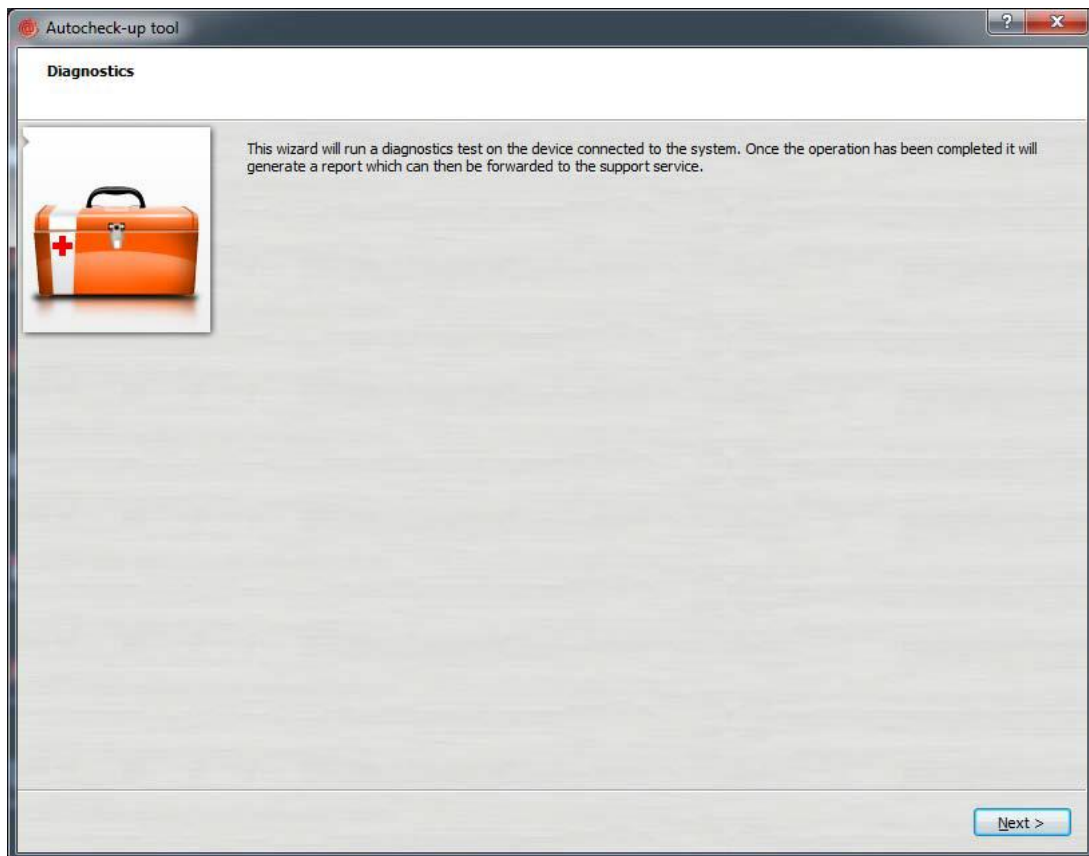
Step 2

Click on “**Autocheck-up**”



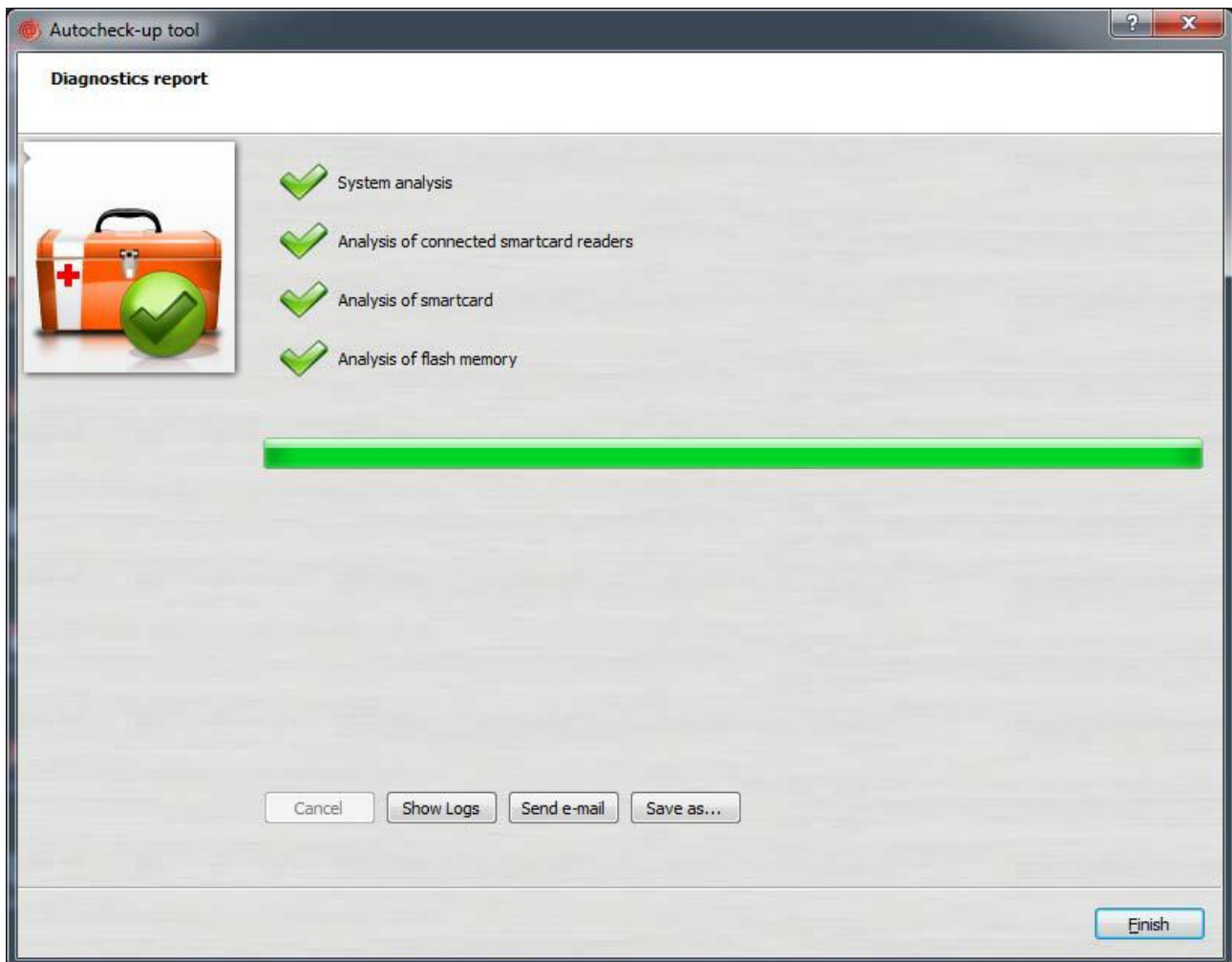
Step 3

Click on “**Next**” and wait for the TOKEN to complete the analysis of the device



Step 4

After completing the analysis, if faults are not found, a page like the following will appear.



The user will be able to send the result of the analysis via e-mail or save it in a .txt file.

Note: *To use this function of the TOKEN the user must have administrator privileges.*

Options

Proxy Setting

To use the TOKEN in a network protected by Proxy, follow these steps:

Step 1

Select the “Utilities” icon.



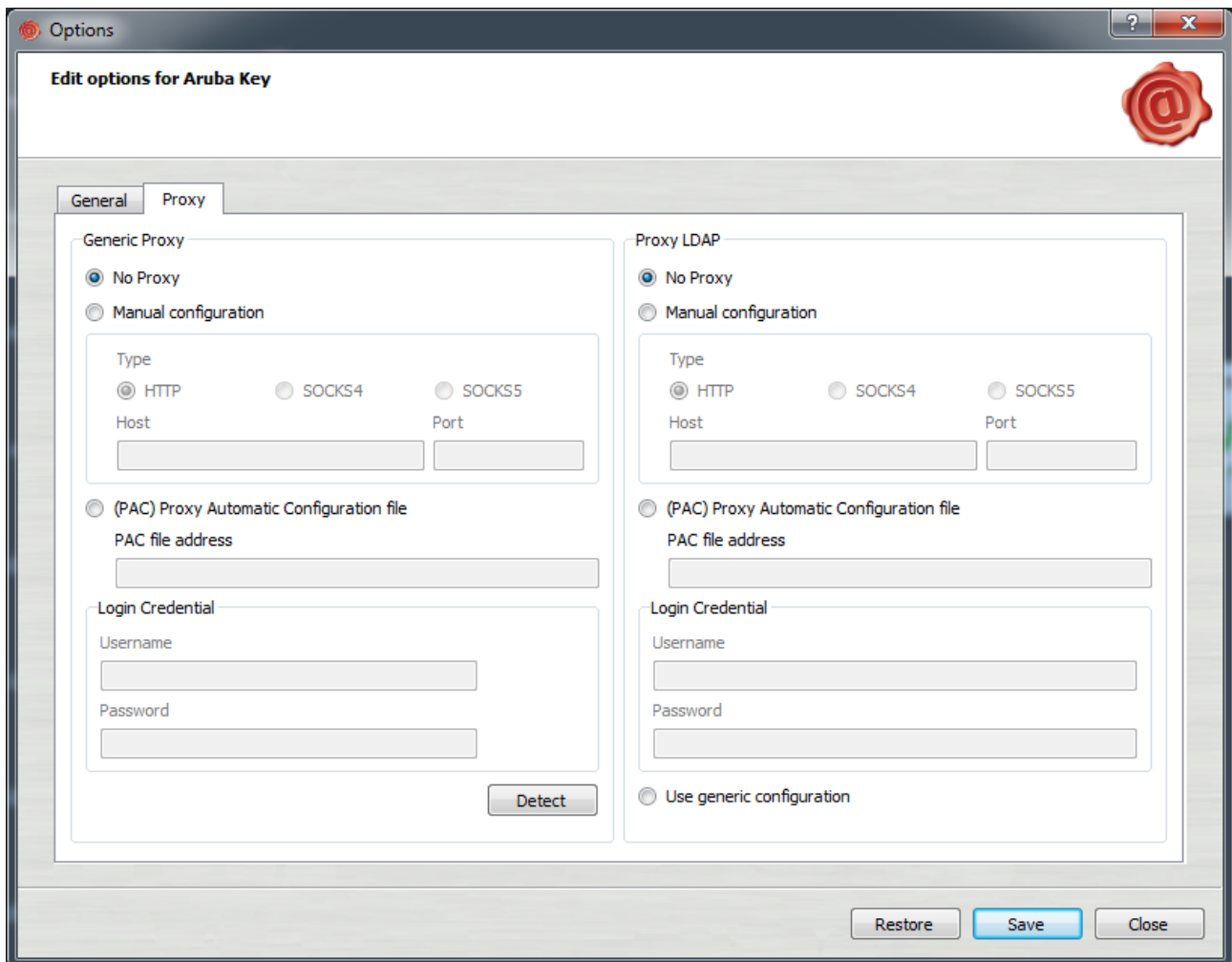
Step 2

Click on “Options and Proxy”



Step 3

Proceed with the configuration of the Proxy (HTTP/LDAP) section



For each configuration (generic Proxy and LDAP Proxy) it is possible to select the following options:

- **No proxy:** if selected no proxy is used;
- **Manual configuration:** if selected the proxy specified by 'Type', 'Host' and 'Port' is used;
- **Auto-configuration (PAC):** if selected you need to specify a valid address for the proxy auto-configuration (PAC) file in the 'PAC file address' field.

The address can be entered in the format *http://address/to/file* or *file://path/to/file*. Such file is used to determine the address of the proxy that will be used (or if not to use the proxy) for a specific address.

The access credentials specify the user name and password which should be used for the proxy authentication.

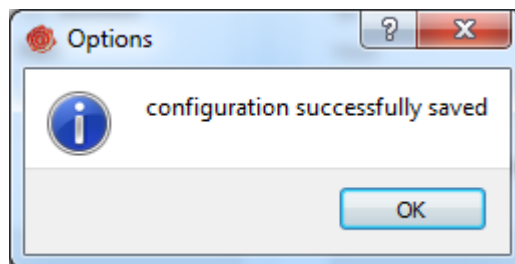
If not specified on Windows operating systems, the system will use, if possible, the credentials of the user that is currently logged in the system. If however, the credentials are not valid for the currently used proxy, each application will request the credentials when required.

For the 'Proxy LDAP' configuration it is also possible to select the **Use generic configuration** option so that for the LDAP addresses the same configuration specified in 'Generic Proxy' will be used.

NOTE: If the details relevant to either the HTTP or LDAP section are not available (e.g. because the network does not support both configurations), proceed only with the section relevant to the supported type of Proxy.

Step 4

If the configuration has been saved correctly the following window will appear.



Language Setting

To change the TOKEN language, follow these steps:

Step 1

Select the “Utilities” icon.



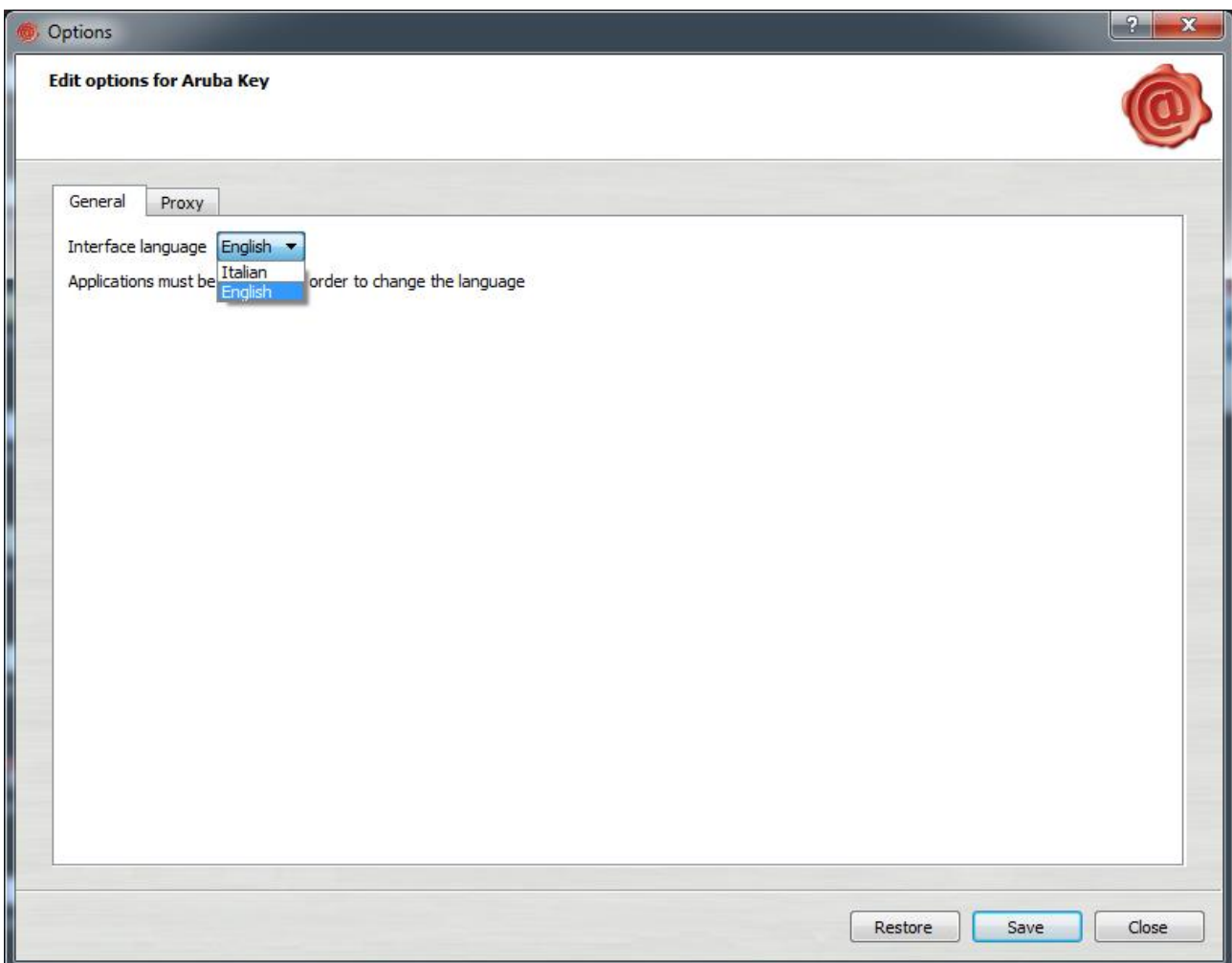
Step 2

Click on “Options and Proxy”



Step 3

Proceed with the configuration of the preferred Language



NOTE: Once you've changed the language settings you need to restart the Aruba Key software to activate them.

NOTE 2: In this version of the software the language settings do not apply to these applications:

- Firefox portable
- Thunderbird portable
- Filezilla portable
- AbiWord portable
- 7Zip