

Solutions for Security

Guide to Obtaining Your Free WIS@key CertifyID Personal Digital Certificate (Personal eID) on WIS@key Smart Cards

*Wherever Security relies on Identity,
WIS@key has the solution.*

Date: September 2007
Version: 0.1.1
Authors: WIS@key SA

TABLE OF CONTENTS

About this User Guide	1
<i>About Personal eID (Digital Certificate)</i>	<i>1</i>
<i>About WISEKey Smartcards and USB Tokens</i>	<i>1</i>
<i>Copyright</i>	<i>3</i>
<i>Document Conventions</i>	<i>4</i>
Free Secure e-Mail eID on WISEKey Smart Card	5
<i>Associating WISEKey Smart Card and Reader</i>	<i>5</i>
Pre-requisites	5
Installing SafeSign Identity Client	5
Initialising the Smart Card / Token	5
<i>Creating your profile</i>	<i>7</i>
Creating your Profile	7
Email Verification	9
Keypair Generation on Smart Card	9
Install Certificate	12
<i>Generating an Exportable Key Pair for Backup before storage in the Smart Card</i>	<i>13</i>
Keypair Generation	13
Install Certificate	15
Export Key and Certificate to File	15
Import Key (PFX) File into Smart Card	19
Support	21

About this User Guide

This manual describes the steps followed to obtain a free WISEKey CertifyID Digital Certificate (eID) for securing your e-mail transactions.

About Personal eID (Digital Certificate)

A digital certificate provides the individual user with the highest level of security; enabling identification, authentication, secure encrypted communications (e-mail, web site etc.), electronic signatures, and non-repudiation.

WISEKey Personal eIDs associate the identity of a person with a digital identity. On one hand a digital ID, or eID can be viewed as Digital Passports that inform Internet users about their interlocutors' identity and ensure electronic messages confidentiality.

Those certificates integrate seamlessly with the majority of existing systems. They are user-friendly, each action being performed via Windows-like active icons.

An eID enables you to:

- Create digital signatures on electronic mail messages, thus ensuring message integrity and authenticity with your correspondents;
- Receive confidential information from any of your correspondents that only you can decrypt and read using S/MIME (You can also send confidential information to other eID users);
- Increase security for your applications, replacing passwords with eID authentication protection (for PKI enabled applications);
- Securely encrypt files and share them with other eID holders using available applications such as the free WISECrypt Personal Edition, available from WISEKey's web site.

About WISEKey Smartcards and USB Tokens

WISEKey provides smartcards, readers, and secure USB tokens for individuals and enterprises. WISEKey smart cards are high quality multipurpose cards that can be used for a variety of purposes including:

- Secure files and documents
- Securely exchange information
- Secure electronic email
- Securely access facilities (wireless proximity access – special version)
- Securely access desktops and servers
- Digital sign documents and files for more efficient electronic workflow and approvals
- In addition to signature and PKI applications, and access control systems, the smart card can be used to secure many other sensitive applications, such as payment systems.

The Alinghi Smartcard 2007 is a WISEKey card that has been co-branded by Alinghi for their use the Defense of the 32nd Americas Cup, in which they were successful.

The WISEKey Smart Card (2007) is implemented using a Philips P8WE5032 integrated circuit, which has been certified as ITSEC E4 high.

Features:

- ISO/IEC compatibility
- Secure messaging
- Hierarchical ISO file system
- DES, 3DES
- State machine
- Logical channel support
- Deletion of files (EF) and applications (DF)
- Enhanced hardware security
- High performance
- Implementation of various access controls (authentication)
- Data encryption with asymmetric RSA keys up to a key length of 1,024 bits
- Generation and verification of digital signatures with RSA and DSA
- On-card RSA key generation up to a key length of 1,024 bits
- Digital signature application can be certified ITSEC E4 high

The provided middleware allows smart card or tokens to be used in all conventional PKI applications such as secure mail, SSL or network login. The smart card middleware consists of an easy-to-use installation routine and the middleware itself. This serves to connect the hardware to applications and operating systems. A utility for token management is also included.

To achieve optimum interoperability the smart card middleware supports more than 70 different smart card operating systems (Starcos, JCOP, CardOS, Multos, SmartCafe, etc.), thus ensuring future longevity and flexibility of the deployed infrastructure.

Supported operating systems:

- Windows 98/ME/NT 4.0/2000/XP/2003 server
- MAC OS X
- Linux
- Solaris
- Windows CE

A selection of the supported applications:

- MS Windows 2000/XP log-on
- MS Windows terminal server/Citrix
- Secure e-mail clients, e.g. MS Outlook (Express, 98, 2000, XP), Netscape Messenger, Novell Groupwise 6, Baltimore Mail-Secure, Utimaco Sign & Crypt, Entrust Entelligence
- Secure e-mail plug-ins for Lotus Notes from Utimaco, Secude, SSE, Baltimore
- WISECrypt
- SSL authentication with browsers such as MS Internet Explorer, Netscape Navigator
- WISEKey PKI, Baltimore PKI, Entrust PKI, RSA Keon PKI, VeriSign PKI or GlobalSign PKI
- VPN clients from Microsoft, NCP, Cisco, Checkpoint, SafeNet
- SSH Secure Shell clients
- PGP, RSA SecurID, Celo eSigner, Lotus Notes Rnext, Citrix Metaframe, Novell NMAS
- SSO from eTrust, Protocom

The following interfaces are supported:

- PKCS#11 meeting the RSA specification
- PKCS#12 transport format
- PKCS#15 token information syntax format
- CSP for MS CryptoAPI
- PC/SC 1.0 several class 2/3 readers
- A004

Token management utility

- Token initialization (incl. loading of applets in the case of a Java™-based token)
- PIN definition
- Key generation
- Multi-language support
- Automatic registration of certificates in MS applications
- Customized adaptations (e.g. menu options on/off)

Copyright

No part of the contents of this document may be reproduced or distributed in any form or by any means without the prior written permission of WISeKey SA.



is a registered trademark of WISeKey SA.



is a registered trademark of WISeKey SA.

Written and published in Geneva, Switzerland, by WISeKey SA.
Copyright © 2007 WISeKey SA.
All Rights Reserved.

Document Conventions

This User Guide uses the following conventions:

- **NOTE** means *reader take note*. Notes contain helpful suggestions.
- **IMPORTANT** means the reader must follow the instructions strictly.
- Descriptions for significant fields are available.

Free Secure e-Mail eID on WISEKey Smart Card

Associating WISEKey Smart Card and Reader

PRE-REQUISITES

WISEKey Smart Card and Reader works with the Windows Operating Systems defined in the latest product description: Windows 2000, Windows XP Professional, Windows 2003 Server, and Windows Vista. Windows NT and Windows 98 / ME are not supported.

Note that in order to install WISEKey Smart Card reader, card and SafeSign Identity Client; you will need to have local administrator rights on the (local) computer itself. This is because upon installing SafeSign Identity Client, access to the registry is required, which a user without local administrator rights is not granted access to. When SafeSign Identity Client is installed, any user can use it.

Before being able to use smart card readers and smart cards, you should have Microsoft Smart Card Base Components and its update, the Smart Card Driver Library installed, for all non-Windows 2000 / XP / 2003 versions.

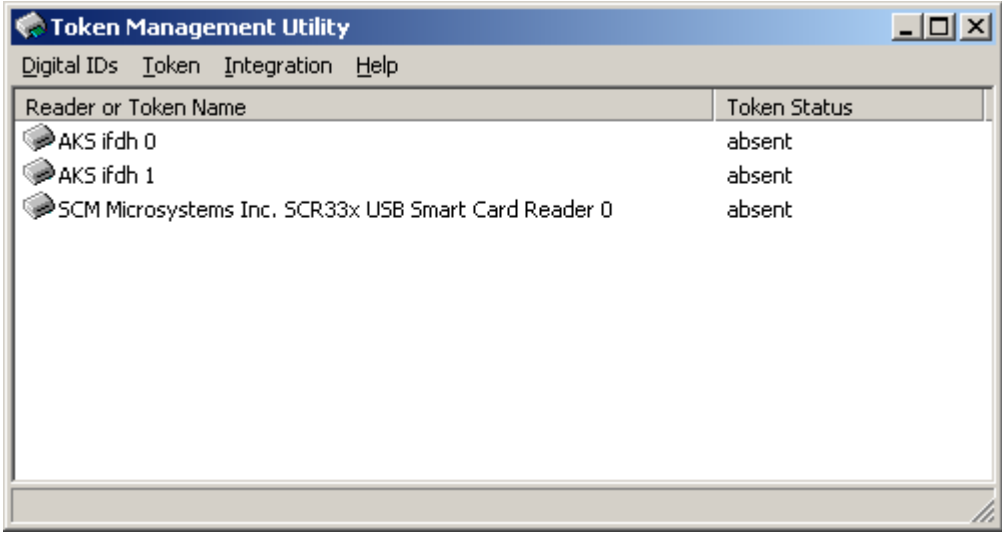
INSTALLING SAFESIGN IDENTITY CLIENT

SafeSign Identity Client installation is quick and straightforward. The installation program will lead you through all steps necessary to install SafeSign Identity Client. The installation program will also allow you to install SafeSign Identity Client in Firefox (and/or Netscape and Mozilla) and Entrust, when these are available on your system and selected as program features to be installed.

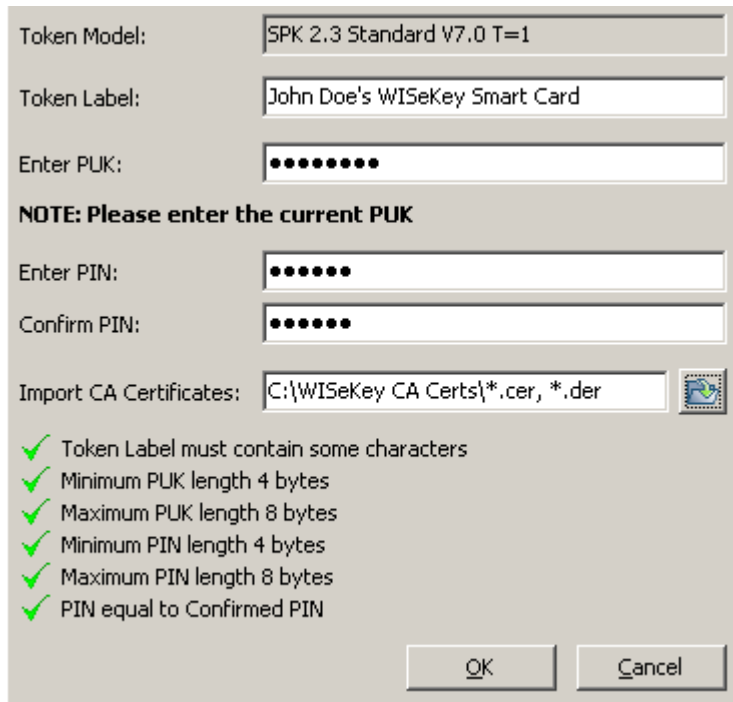
The detailed steps for installation are described in SafeSign Identity Client Installation Guide.

INITIALISING THE SMART CARD / TOKEN

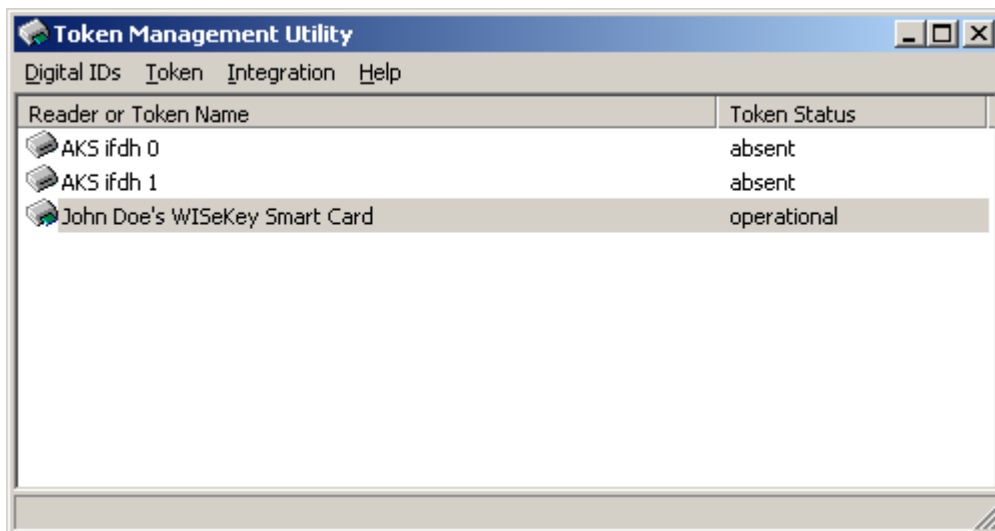
The smart card needs to be initialised before generating key pairs and storing digital certificates in it. You can assign your PIN for the smart card during this procedure.

Steps	Instructions								
1	<p>Open Token Management from Start Menu > Programs > SafeSign Standard.</p>  <table border="1" data-bbox="288 1458 1294 1989"> <thead> <tr> <th data-bbox="300 1547 1002 1576">Reader or Token Name</th> <th data-bbox="1002 1547 1283 1576">Token Status</th> </tr> </thead> <tbody> <tr> <td data-bbox="300 1576 1002 1606">AKS ifdh 0</td> <td data-bbox="1002 1576 1283 1606">absent</td> </tr> <tr> <td data-bbox="300 1606 1002 1635">AKS ifdh 1</td> <td data-bbox="1002 1606 1283 1635">absent</td> </tr> <tr> <td data-bbox="300 1635 1002 1664">SCM Microsystems Inc. SCR33x USB Smart Card Reader 0</td> <td data-bbox="1002 1635 1283 1664">absent</td> </tr> </tbody> </table>	Reader or Token Name	Token Status	AKS ifdh 0	absent	AKS ifdh 1	absent	SCM Microsystems Inc. SCR33x USB Smart Card Reader 0	absent
Reader or Token Name	Token Status								
AKS ifdh 0	absent								
AKS ifdh 1	absent								
SCM Microsystems Inc. SCR33x USB Smart Card Reader 0	absent								

- Insert Smart Card in the reader. Click **Initialise Token...** in the **Token** menu.
 Enter a suitable label for your card in the **Token Label** field.
 Enter an appropriate PUK in the **Enter PUK** field. Remember this PUK because it will be useful for unblocking the card if required later. PUK shall be minimum 4 and maximum 8 characters (numeric or alphanumeric).
 Enter your PIN in the **Enter PIN** and **Confirm PIN** fields. PIN shall be minimum 4 and maximum 8 characters (numeric or alphanumeric).
 You can import CA certificates at this time. Copy all CA certificates in one folder and browse to the folder using the button adjacent to **Import CA Certificates** field.
 Click **OK** to initialise the token.




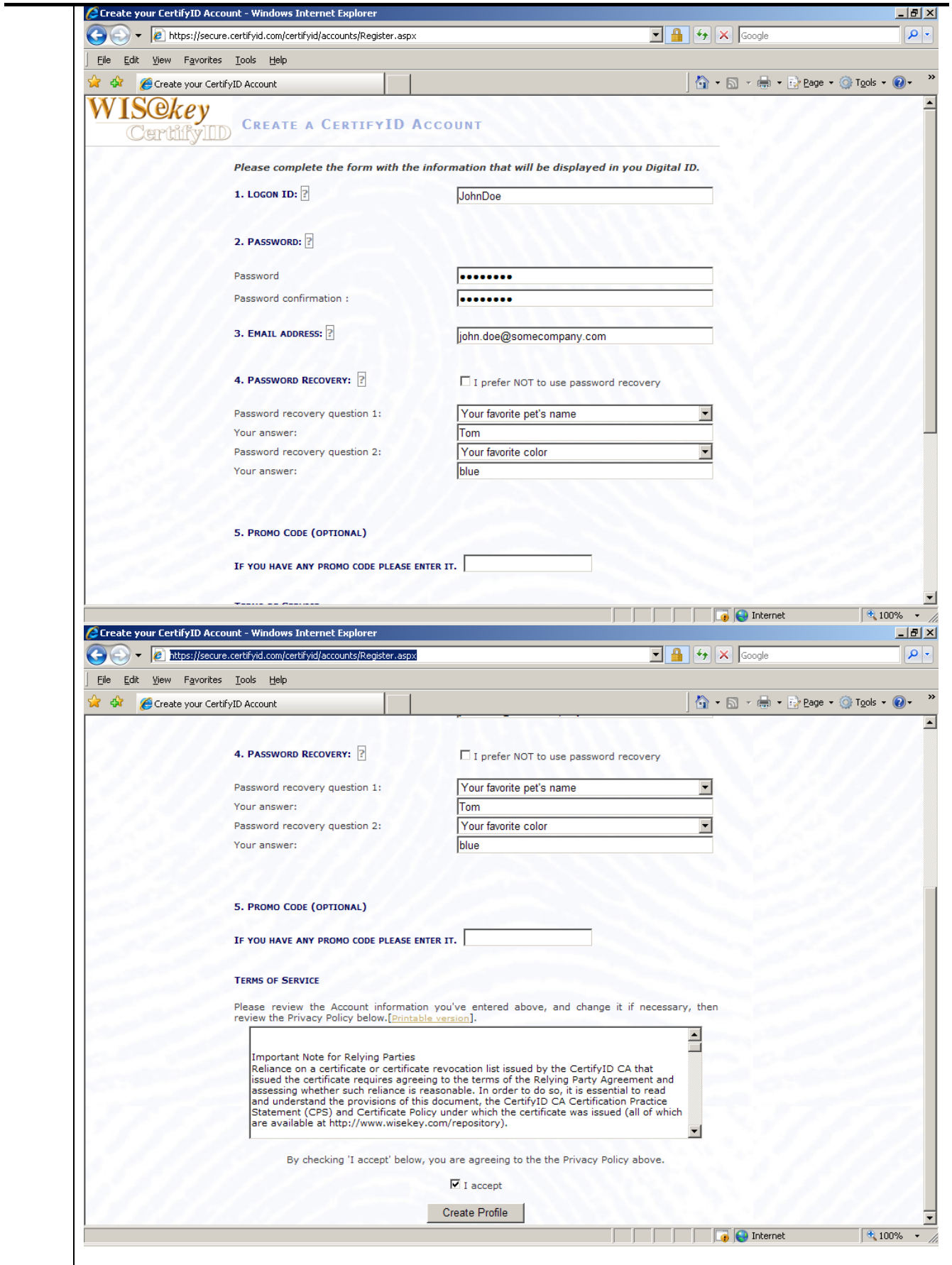
- Click **OK** in the Message Box. Your card is ready to create key pairs and store digital certificates.



Creating your profile

CREATING YOUR PROFILE

Steps	Instructions
<p>1</p> <p>2</p>	<p>Open Internet Explorer. Type https://secure.certifyid.com/accounts in the address bar.</p> <p>Click Sign Up to CertifyID Account link in the homepage.</p>
	
<p>3</p>	<p>In the Create your CertifyID Account page, fill in the details according to your choice.</p> <p><i>Note: Enter a valid email address in the Email Address field. Your password will be sent to this email address.</i></p> <p>Accept the terms and conditions by enabling I Accept check box. Click Create Profile button to create your profile.</p>



EMAIL VERIFICATION

Steps	Instructions
1	<p>You must use a valid email address. An email verification code will be sent to this email address and you should check your email to retrieve the message.</p> <p><i>NOTE: Use an email address that is accessible from an S/MIME capable email application. Examples of S/MIME capable applications include Outlook, Outlook Express, and Mozilla Thunderbird. The email address you submit must be in the exact form as used by your email application, do not use mapped emails. E.g. if your email application accesses your account using <u>jd@somecompany.com</u>, then please use this address for your CertifyID Account. Even though <u>john.doe@somecompany.com</u> may be a working alias for <u>jd@somecompany.com</u>, it will not work in some SMIME capable applications.</i></p> <p>You will receive two emails notifying you of the registration on the address that you provided. One of these messages will be titled: "CertifyID Account email verification".</p> <p><i>Note: As these emails are automated messages, some Email providers may identify them as SPAM, so if you fail to receive them, make sure to check in your spam folder.</i></p> <p>If it has not been received, click browser's back button and check your email address in the Create your CertifyID Account page. If the email is correct and you have not received a your verification email, then go to the CertifyID Account email verification page and click the Send verification code again button in order to send a new verification code to your email account.</p>
2	<p>In the CertifyID Account email verification, you can click on the email verification link. Or you may log on to CertifyID Account, and in the CertifyID Account email verification page you can enter the verification code received in your email, then click the Verify Button to verify your email address.</p> <p>2. PROVE EMAIL VERIFICATION.</p> <p>You have two options to verify your email:</p> <ul style="list-style-type: none"> • Copy the validation code from the message you have received and paste it to the text box below. This method is required if you were redirected for authentication from another CertifyID application • Simply click to the verification link provided in the message you have received. In this case new browser window will be opened. You should close then this or new one. <p>Received code: <input data-bbox="513 1469 991 1509" type="text" value="0dg7degoidi6kirm8txv"/> <input data-bbox="999 1469 1091 1509" type="button" value="Verify"/></p>

KEYPAIR GENERATION ON SMART CARD

The following procedure should be used to generate a non-repudiable cryptographic key pair on the smart card, and obtaining your digital certificate from WISEKey.

Important: If you wish to save a backup of your key pair before saving it to the smartcard then please skip to the section titled Generating an Exportable Key Pair for Backup before storage in the Smart Card.

Generating a key pair within a smart card is the most secure form of key generation. The key pair cannot be extracted from the smart card, and thus a user requires the smart card and the password

for the card in order to use the private key to encrypt or decrypt information, or generate digital signatures. This is called strong authentication, because two factors of authentication are involved.

Signatures created by keys generated on a smart card are also referred to as “non-repudiable”, because relying parties can be sure that the user possessing the smart card can be proved to be responsible for the digital signatures generated by it. Those signatures cannot be repudiated.

NOTE: If you wish to use your certificate and key pair for encryption, you may wish to consider generating an exportable key pair in your browser key store, and storing your certificate in this store. Then you can export your key pair to a password protected file, which you can store safely on some media, before you import it into the smart card for further use.

Please see further in this guide for instructions on performing this procedure using the WISEKey CertifyID system and smart card.

NOTE: Only CertifyID Account users that have verified their email address can obtain a digital certificate.

Steps	Instructions
1	<p>Log on to CertifyID Account, and go to the Certificates page.</p> <p>Click on the button titled Online Web Enrolment, or the Enrol menu item. You will arrive in the CertifyID Registered User page. Select the appropriate Cryptographic Provider (CSP), for the WISEKey smart card this should be the “SafeSign Standard Cryptographic Service Provider”, and then click the Generate button.</p> <p><i>Note: You should select SafeSign Standard Cryptographic Service Provider in order to generate your key pair and certificate on your WISEKey smart card.</i></p>

CERTIFICATE WEB ENROLLMENT

Click on "Generate" to get your certificate

User Information

First Name	JohnDoe
Last Name	

Certificate Template

Certificate Template Name	CertifyID Standard User
---------------------------	-------------------------

Subject [Identifying Information]

EMAIL	john.doe@somecompany.com
COMMON_NAME	john.doe@somecompany.com
ORGANIZATIONAL_UNIT	Person's Identity not verified - Ce

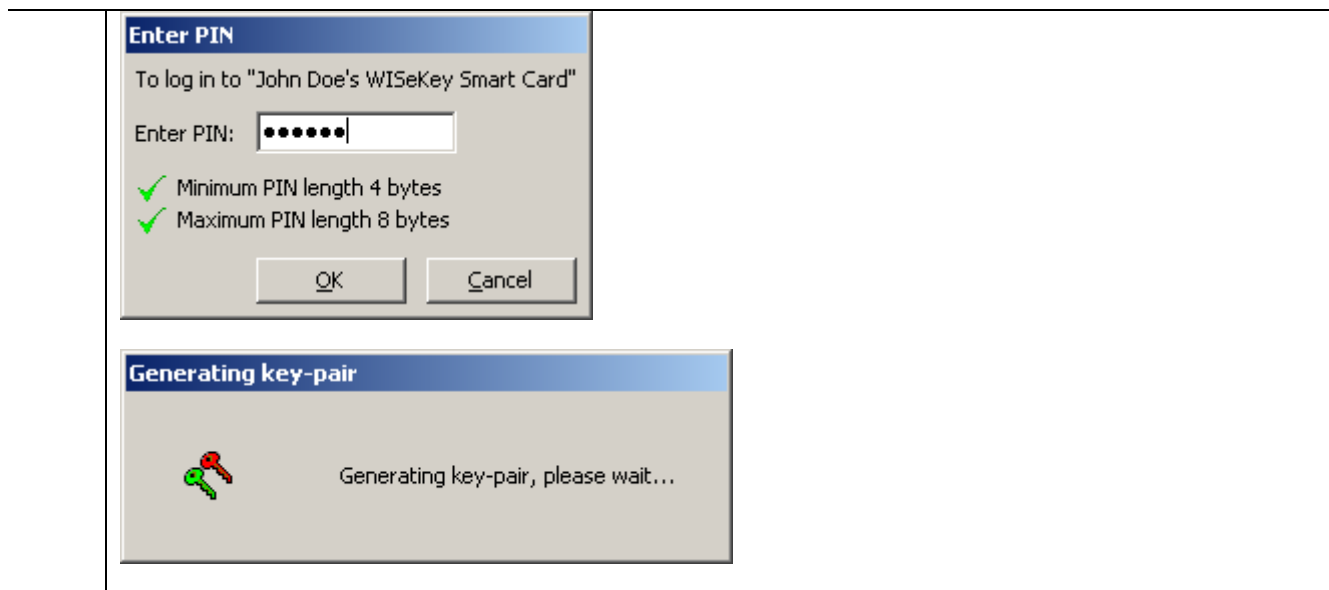
Key Options

Cryptographic Service Provider (CSP)	SafeSign Standard Cryptographic Service Provider
Key Usage	<input type="radio"/> Exchange <input type="radio"/> Signature <input checked="" type="radio"/> Both
Key Size	1024
Exportable Private Key (Allows you to transfer your certificate)	<input checked="" type="checkbox"/>
Protected private key	<input checked="" type="checkbox"/>
SMIME Capability	<input checked="" type="checkbox"/>

Generate

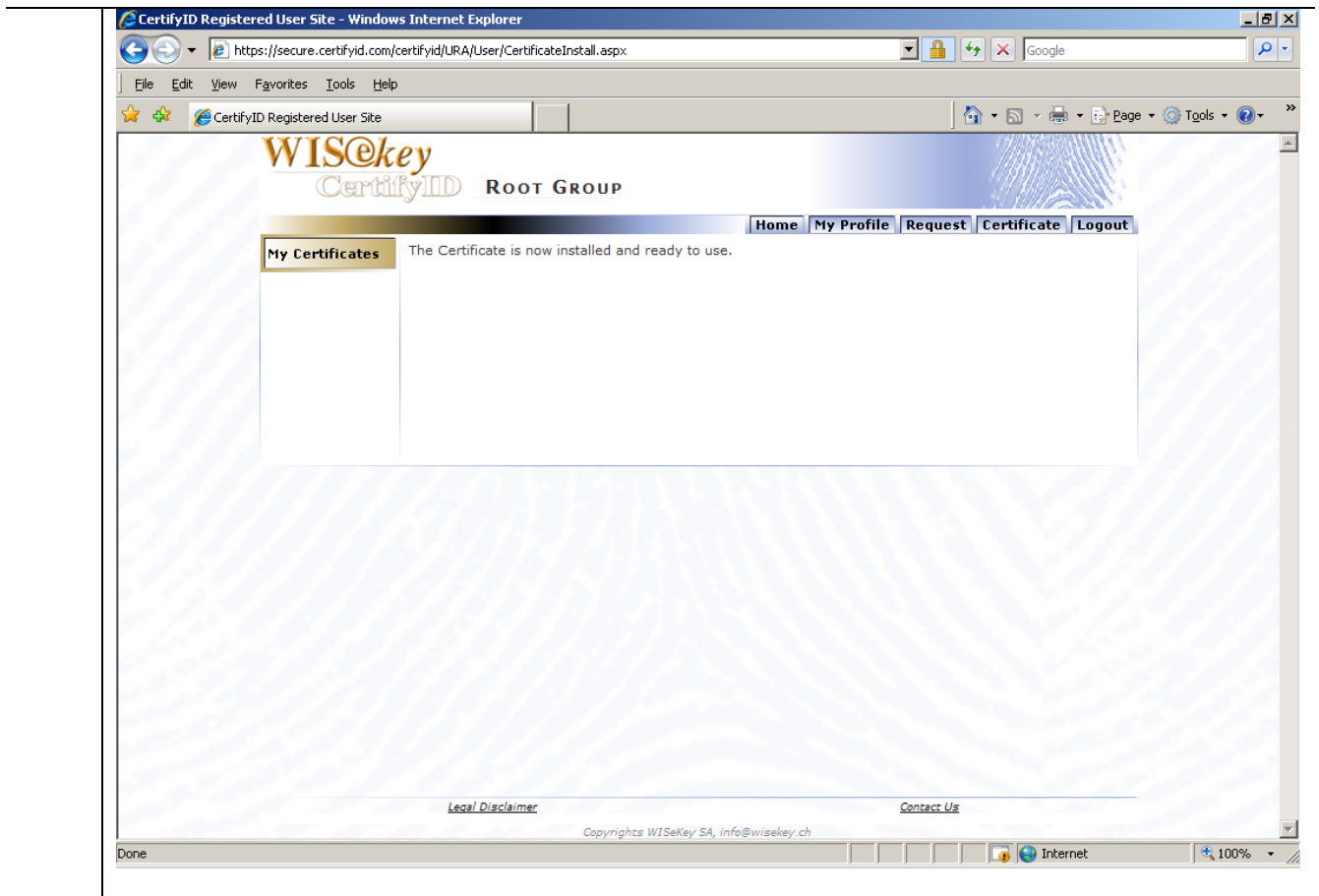
- Click **Yes** in the Internet Explorer message box.
- Enter your smart card PIN in the **Enter PIN** dialog box and click **OK**. The key pair will be generated in the smart card.

Important: Don't remove smart card from the reader during key generation.



INSTALL CERTIFICATE

Steps	Instructions
1	<p>The certificate should be immediately generated and the following prompt should appear in CertifyID Registered User page, click Yes in the Internet Explorer message box to install the entire certificate chain.</p>
2	<p>The certificate should now be available for your use in PKI enabled applications.</p>



3 Click **Logout** tab in the right hand top of the page to logout from the application.

Generating an Exportable Key Pair for Backup before storage in the Smart Card

If you wish to use your certificate and key pair for encryption, you should consider generating an exportable key pair in your browser key store, and storing your certificate in this store. Then you can export your key pair to a password protected file, which you can store safely on some media, before you import it into the smart card for further use.

KEYPAIR GENERATION

The following procedure should be used to generate an exportable cryptographic key pair using the browser key store. You should only follow the instructions in this section if you wish to save a backup of your key pair. Otherwise please generate the key pair as described in the previous section.

Steps	Instructions
1	<p>Log on to CertifyID Account, and go to the Certificates page.</p> <p>Click on the button title Online Web Enrollment, or the Enroll menu item. You will arrive in the CertifyID Registered User page. Select the appropriate Cryptographic Provider (CSP) and click Generate button.</p> <p><i>Note: You should select Microsoft Enhanced Cryptographic Provider v1.0 in to generate your key pair and certificate in your current user account and PC using Internet Explorer browser.</i></p>

Also ensure that the **exportable private key** checkbox is selected.

CERTIFICATE WEB ENROLLMENT

Click on "Generate" to get your certificate

User Information

First Name	JohnDoe
Last Name	

Certificate Template

Certificate Template Name	CertifyID Standard User
---------------------------	-------------------------

Subject [Identifying Information]

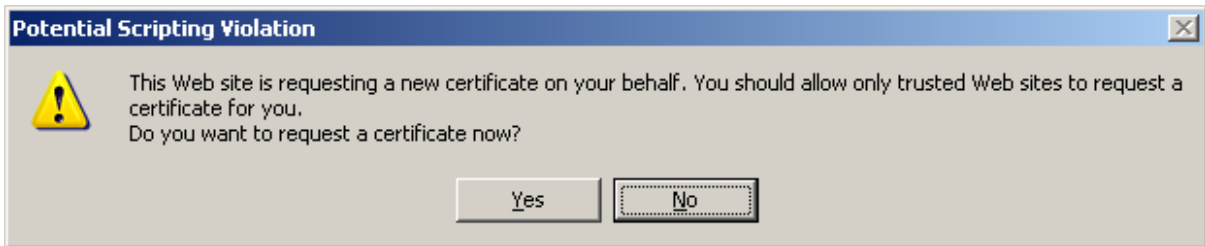
EMAIL	john.doe@somecompany.com
COMMON_NAME	john.doe@somecompany.com
ORGANIZATIONAL_UNIT	Person's Identity not verified - Ce

Key Options

Cryptographic Service Provider (CSP)	Microsoft Enhanced Cryptographic Provider v1.0
Key Usage	<input type="radio"/> Exchange <input type="radio"/> Signature <input checked="" type="radio"/> Both
Key Size	1024
Exportable Private Key (Allows you to transfer your certificate)	<input checked="" type="checkbox"/>
Protected private key	<input checked="" type="checkbox"/>
SMIME Capability	<input checked="" type="checkbox"/>

Generate

2 Click **Yes** in the Internet Explorer message box.



3 Click OK in the **Creating a new RSA exchange key** dialog box.



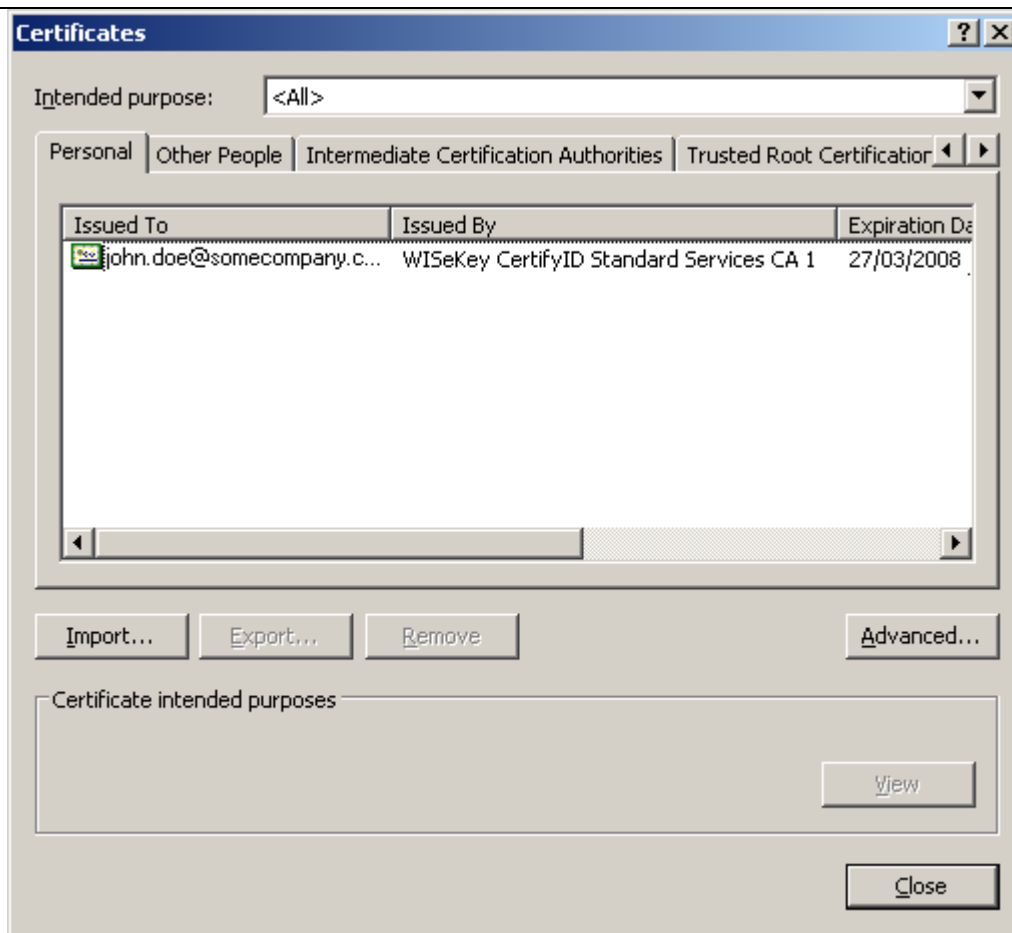
INSTALL CERTIFICATE

<i>Steps</i>	<i>Instructions</i>
1	<p>The certificate should be immediately generated and the following prompt should appear in CertifyID Registered User page, click Yes in the Internet Explorer message box to install the entire certificate chain.</p> 

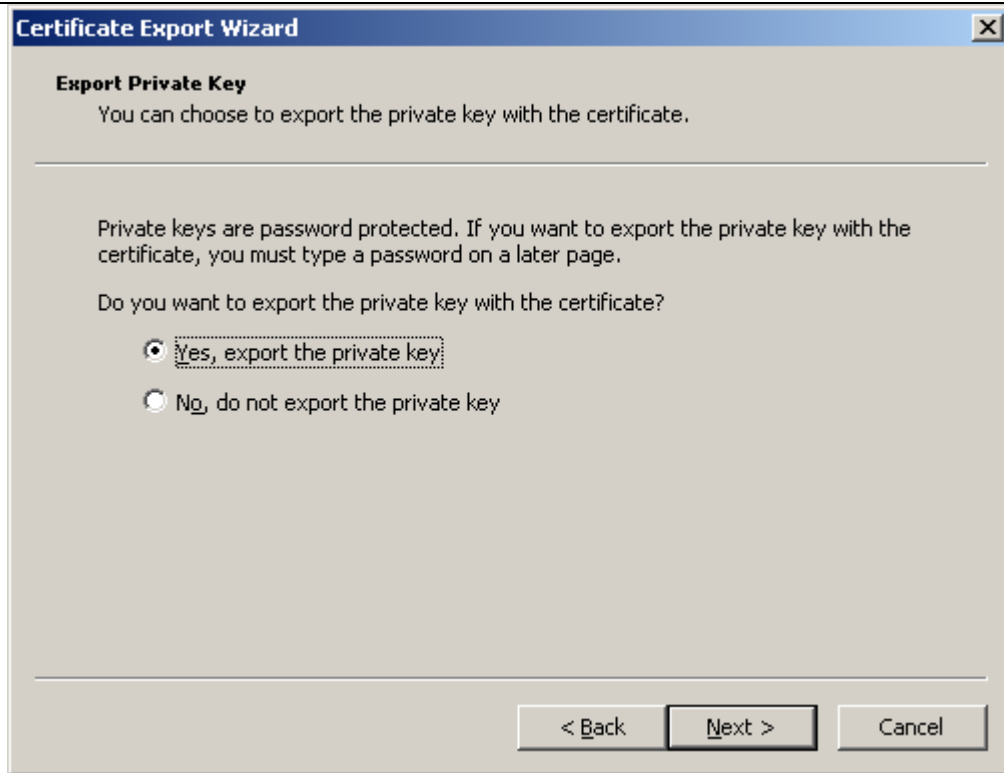
EXPORT KEY AND CERTIFICATE TO FILE

The digital certificate will be installed in your Internet Explorer browser store. It shall be exported into a file securely by protecting with a password.

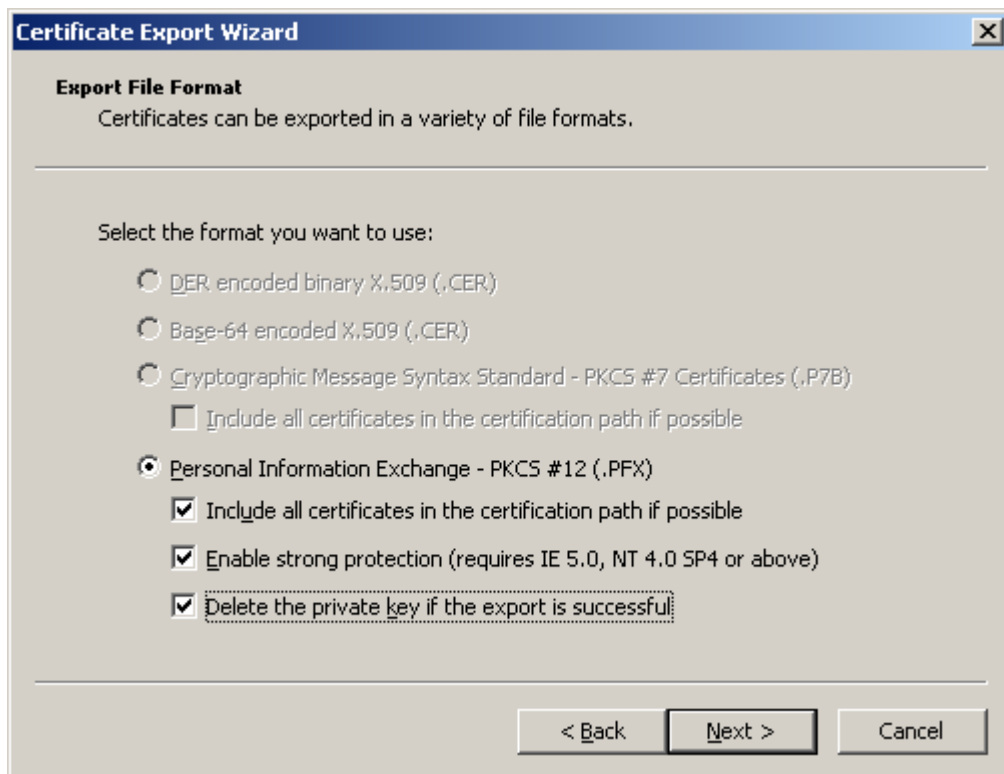
<i>Steps</i>	<i>Instructions</i>
1	<p>Open Internet Explorer. Click Tools > Internet Options > Content > Certificates. Select your certificate and click Export... button.</p>



- 2 Certificate Export Wizard dialog box will open. Click **Next** in the welcome screen. In the **Export Private Key** screen, select the **Yes, export the private key** option. Click **Next** button.



- 3 In the **Export File Format** screen, select all three check boxes under **Personal Information Exchange – PKCS #12 (.PFX)** option. Click **Next** button.

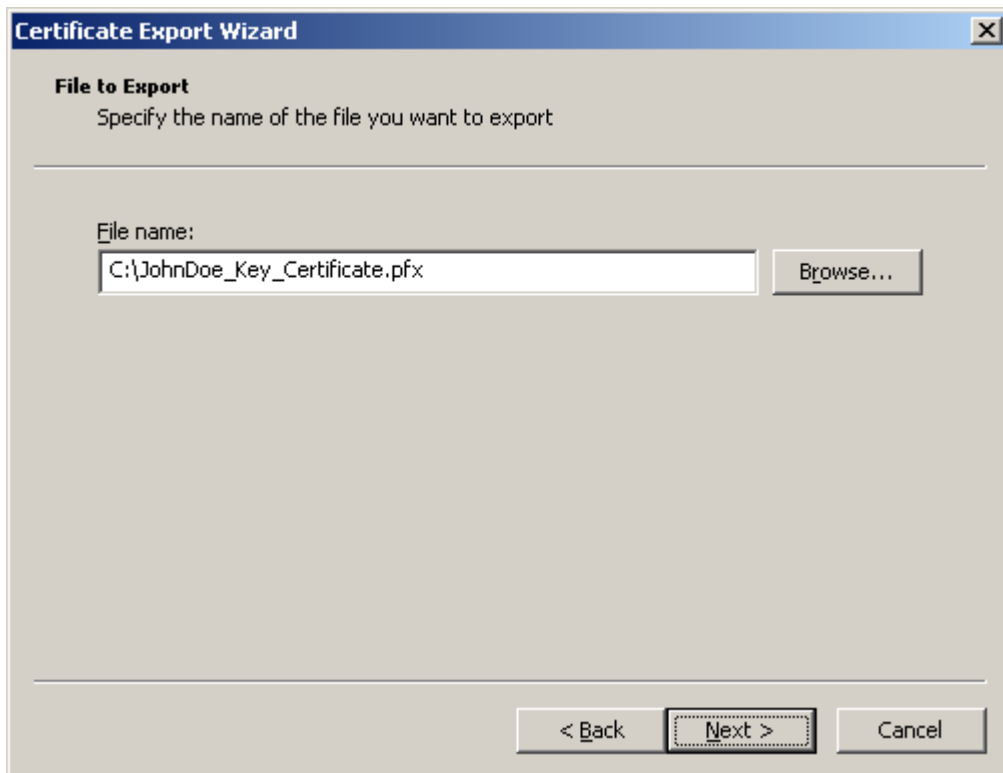


- 4 In the **Password** screen, enter a password to secure the PFX file (containing your private key and certificate) in the **Password** and **Confirm password** fields. Click **Next** button.

Important: Remember this password. You require this password for importing PFX file into the smart card.

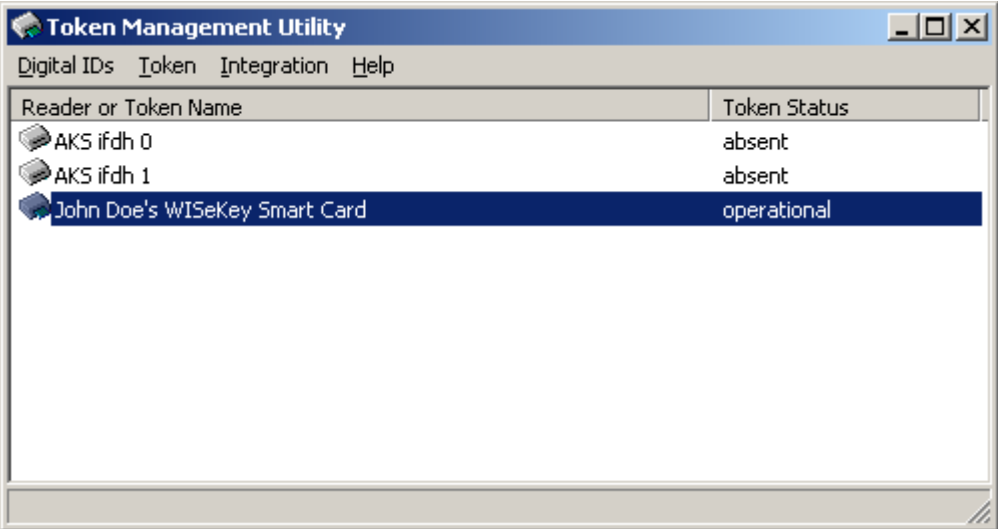



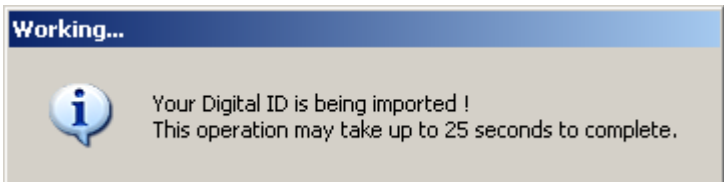
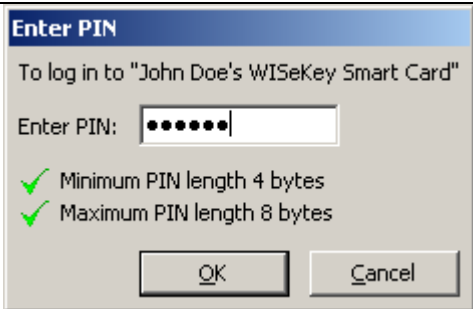
- 5 In the File to Export screen, type the file name of the pfx file to be created. You can also click the **Browse...** button, select the folder and enter the file name in the file dialog. Click **Next** button. Click Finish button in the **Completing the Certificate Export Wizard** screen. Click **OK** in the message box to complete the procedure.



IMPORT KEY (PFX) FILE INTO SMART CARD

The digital certificate will be exported and deleted from your Internet Explorer browser store. It shall be exported into a file, and will be secured by the password.

Steps	Instructions
1	<p>Open Token Management from Start Menu > Programs > SafeSign Standard.</p> <p><i>Note: You should initialise the smart card as mentioned earlier in the document before importing pfx file into smart card.</i></p> 
2	<p>Click Import Digital ID... from the Digital IDs menu. Click the button adjacent to Digital ID file field and select the PFX file. You can enter a label for certificate in the Label on token field by enabling Set the label of the ID on the token to a non default-value checkbox. Enter the password of PFX file in the Digital ID password field. Click OK to import PFX file into smart card.</p>  <p>Enter the smart card PIN in the Enter PIN dialog box.</p>



Your key and certificate will be imported into the smart card.

Note: Check the browser store after successfully completing this operation whether the Certificate and Key is deleted completely to ensure security.

Support

Should you require support at any stage of this procedure then please contact WISEKey SA :-

WISEKey SA
WTC II / 29 Rte de Pré Bois
Geneva CH-1215
Tel. +41 22 594 3000
Email : support@wisekey.com