

Solutions for Security

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

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

Date: September 2007
Version: 0.1.2
Authors: WIS@key SA

TABLE OF CONTENTS

About this User Guide	1
<i>About Personal eID (Digital Certificate)</i>	<i>1</i>
<i>Copyright.....</i>	<i>1</i>
<i>Document Conventions.....</i>	<i>2</i>
Free Secure e-Mail eID.....	3
<i>Creating your profile.....</i>	<i>3</i>
Creating your Profile	3
Email Verification	5
Keypair Generation	5
Install Certificate.....	7
Export Key and Certificate to File as a Backup.....	8
Support.....	13

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)

Digital certificates provides users 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 informs Internet users about their interlocutors' identity and ensures electronic message confidentiality.

Digital 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.

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:

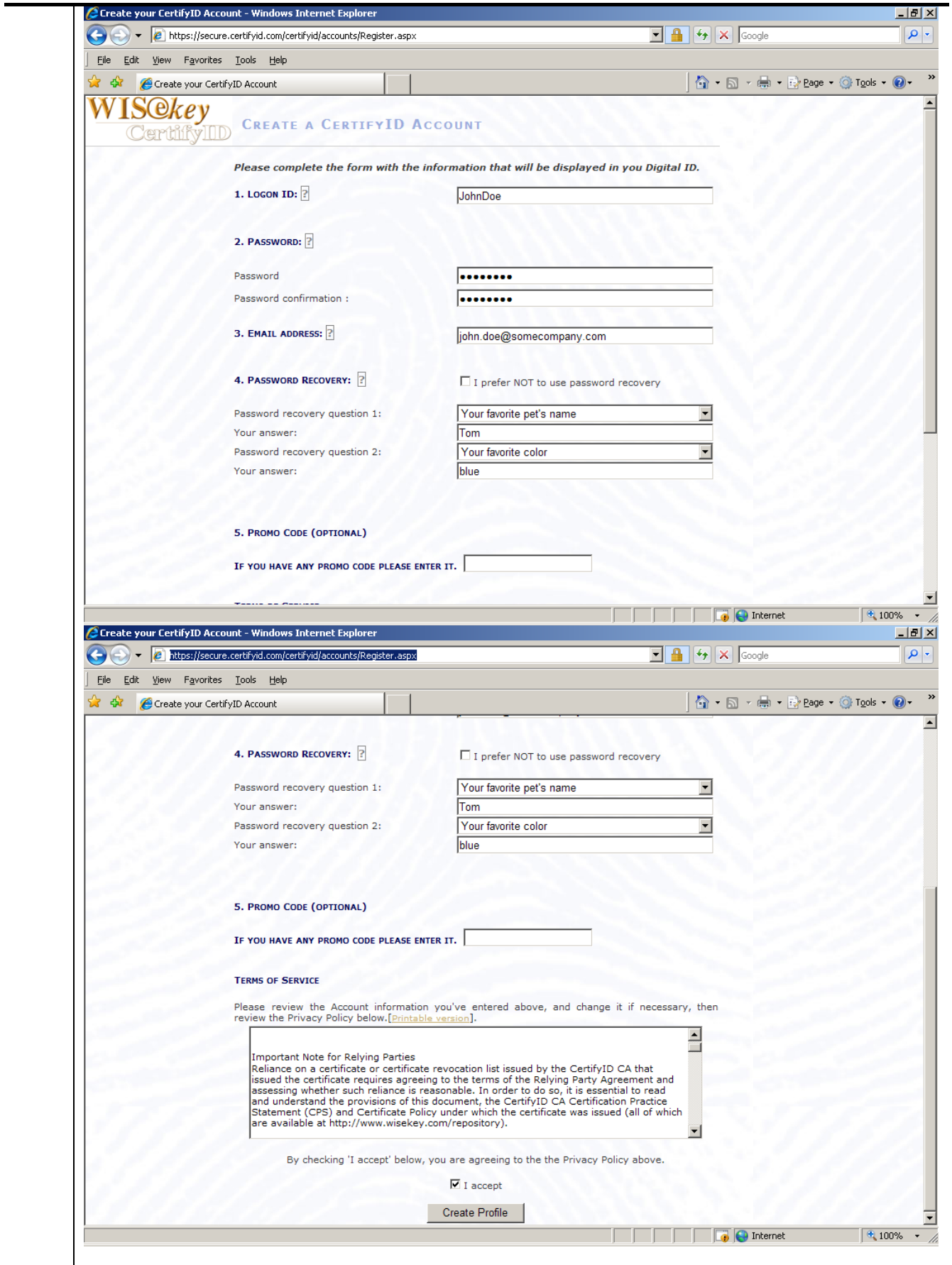
- **NOTE** means *reader take note*. Notes contain helpful suggestions.
- **IMPORTANT** means the reader must follow the instructions strictly.
- Descriptions for significant fields are available.

Free Secure e-Mail eID

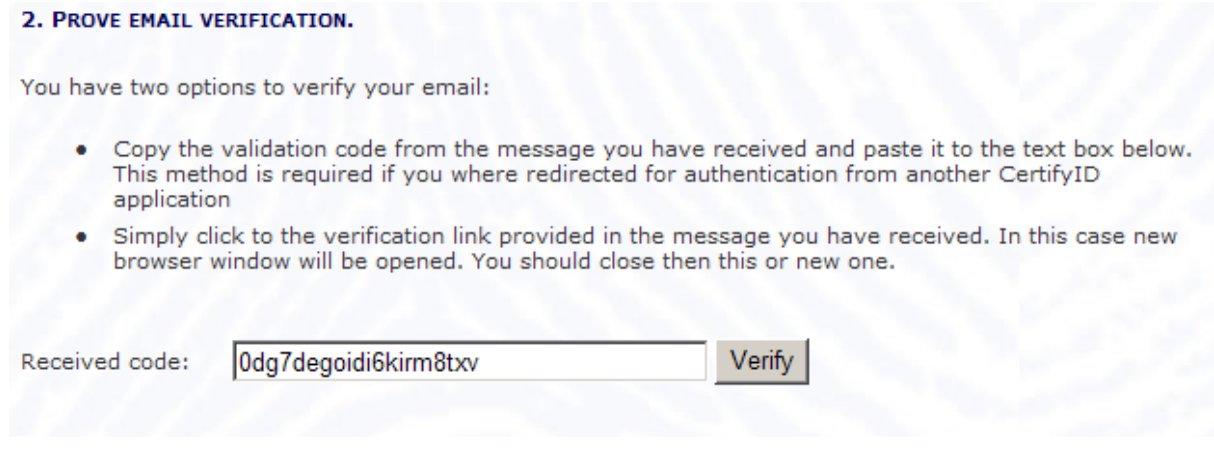
Creating your profile

CREATING YOUR PROFILE

Steps	Instructions
1	Open Internet Explorer . Type https://secure.certifyid.com/accounts in the address bar.
2	Click Sign Up to CertifyID Account link in the homepage.
	
3	<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

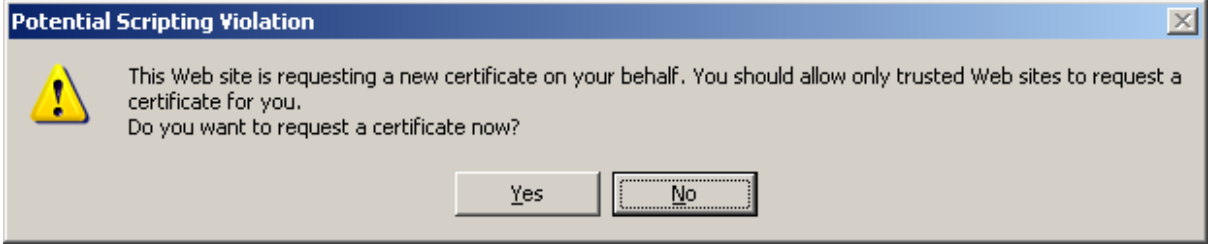

Steps	Instructions
1	<p>You must use a valid email address. An email verification code will be sent to this email address and you should check your email to retrieve the message.</p> <p><i>NOTE: Use an email address that is accessible from an S/MIME capable email application. Examples of S/MIME capable 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 type="text" value="0dg7degoidi6kirm8txv"/> <input type="button" value="Verify"/></p>

KEYPAIR GENERATION


The following procedure should be used to generate your cryptographic key pairs, and request your digital certificate from WISeKey.

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

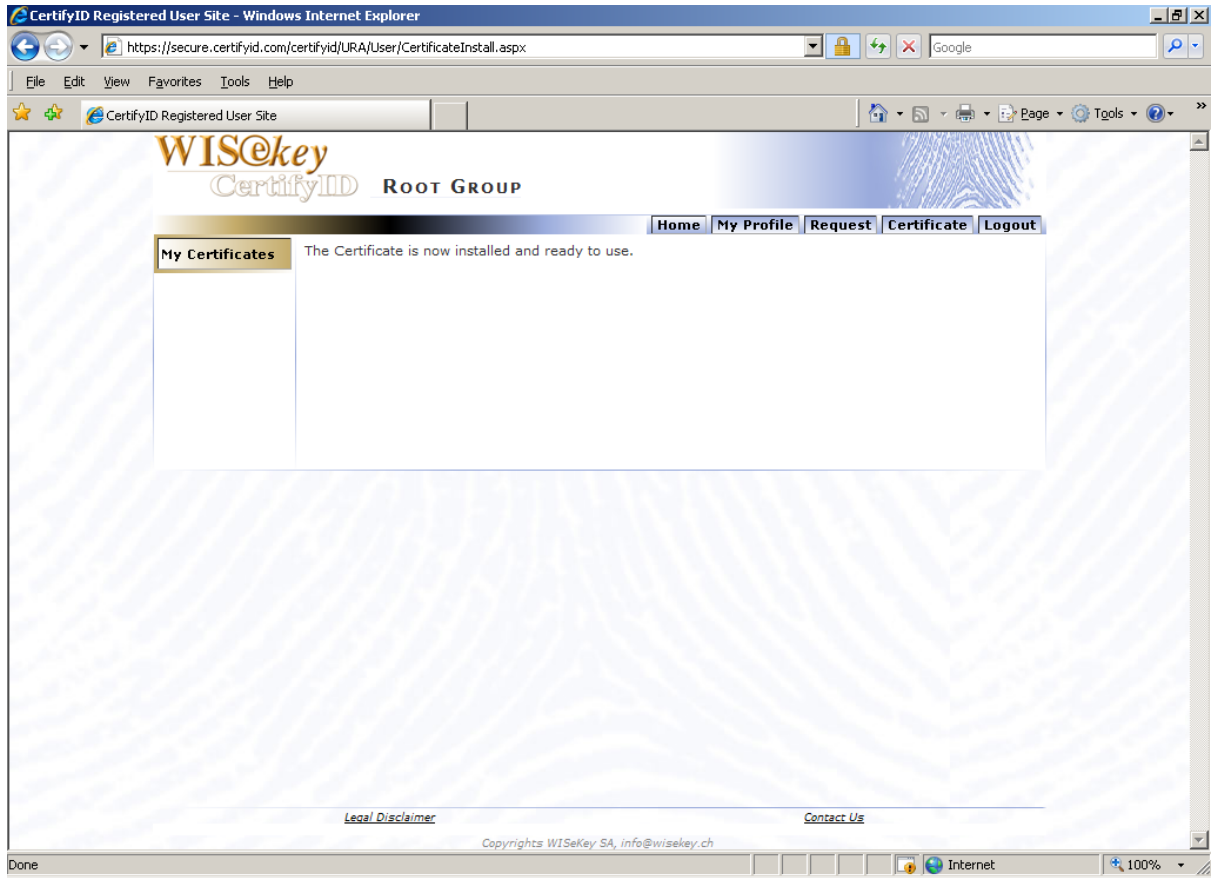
Steps	Instructions																								
1	<p>Log on to CertifyID Account, and go to the Certificates page.</p> <p>Click on the button title Online Web Enrollment, or the Enroll menu item. You will arrive in the CertifyID Registered User page. Select the appropriate Cryptographic Provider (CSP) and click Generate button.</p> <p><i>Note: If you would like to store your private key on your current computer, you can select Microsoft Enhanced Cryptographic Provider v1.0 (which is the default). Your key pair and certificate will be generated and stored in your current user account and PC using Internet Explorer browser</i></p> <div data-bbox="300 593 1342 1720" style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center;">CERTIFICATE WEB ENROLLMENT</p> <p style="text-align: center;">Click on "Generate" to get your certificate</p> <hr/> <p style="text-align: center;">User Information</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%;">First Name</td> <td>JohnDoe</td> </tr> <tr> <td>Last Name</td> <td></td> </tr> </table> <hr/> <p style="text-align: center;">Certificate Template</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Certificate Template Name</td> <td>CertifyID Standard User ▼</td> </tr> </table> <hr/> <p style="text-align: center;">Subject [Identifying Information]</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>EMAIL</td> <td>john.doe@somecompany.com</td> </tr> <tr> <td>COMMON_NAME</td> <td>john.doe@somecompany.com</td> </tr> <tr> <td>ORGANIZATIONAL_UNIT</td> <td>Person's Identity not verified - Ce</td> </tr> </table> <hr/> <p style="text-align: center;">Key Options</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td>Cryptographic Service Provider (CSP)</td> <td>Microsoft Enhanced Cryptographic Provider v1.0 ▼</td> </tr> <tr> <td>Key Usage</td> <td> <input checked="" type="radio"/> Exchange <input type="radio"/> Signature <input type="radio"/> Both </td> </tr> <tr> <td>Key Size</td> <td>1024 ▼</td> </tr> <tr> <td>Exportable Private Key (Allows you to transfer your certificate)</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Protected private key</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>SMIME Capability</td> <td><input checked="" type="checkbox"/></td> </tr> </table> <div style="text-align: center; margin-top: 10px;"> <div style="border: 1px solid #ccc; padding: 5px 20px; display: inline-block; background-color: #f0f0f0;">Generate</div> </div> </div>	First Name	JohnDoe	Last Name		Certificate Template Name	CertifyID Standard User ▼	EMAIL	john.doe@somecompany.com	COMMON_NAME	john.doe@somecompany.com	ORGANIZATIONAL_UNIT	Person's Identity not verified - Ce	Cryptographic Service Provider (CSP)	Microsoft Enhanced Cryptographic Provider v1.0 ▼	Key Usage	<input checked="" type="radio"/> Exchange <input type="radio"/> Signature <input 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"/>
First Name	JohnDoe																								
Last Name																									
Certificate Template Name	CertifyID Standard User ▼																								
EMAIL	john.doe@somecompany.com																								
COMMON_NAME	john.doe@somecompany.com																								
ORGANIZATIONAL_UNIT	Person's Identity not verified - Ce																								
Cryptographic Service Provider (CSP)	Microsoft Enhanced Cryptographic Provider v1.0 ▼																								
Key Usage	<input checked="" type="radio"/> Exchange <input type="radio"/> Signature <input 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"/>																								

2	<p>Click Yes in the Internet Explorer message box.</p> 
3	<p>Click OK in the Creating a new RSA exchange key dialog box.</p> 

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> 

2 The certificate should now be available for your use in PKI enabled applications.



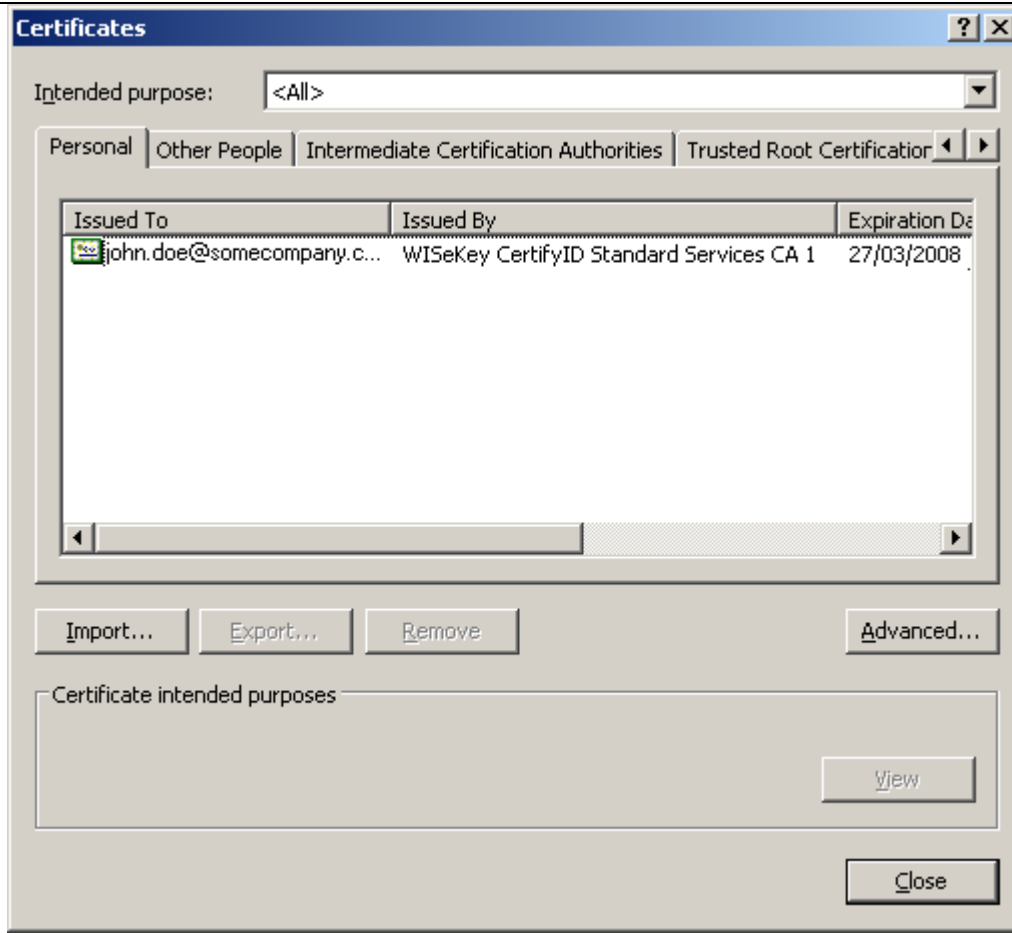
3 Click **Logout** tab in the right hand top of the page to logout from the application.

EXPORT KEY AND CERTIFICATE TO FILE AS A BACKUP

The digital certificate will be installed in your Internet Explorer browser store. It can be securely exported into a file protected with a password so that you can recover your key and certificate in case of exigency.

Important: Store the PFX file generated during this procedure in secure media to prevent unauthorised access.

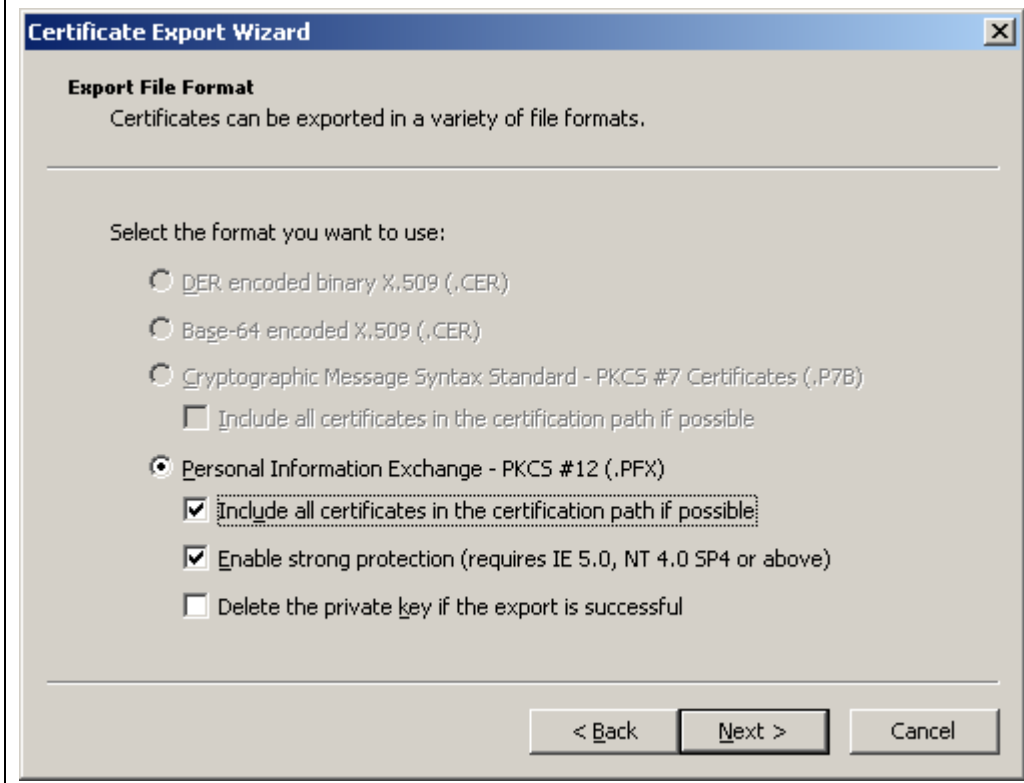
Steps	Instructions
1	Open Internet Explorer . Click Tools > Internet Options > Content > Certificates. Select your certificate and click the Export... button.



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



- 3 In the **Export File Format** screen, select check boxes **Include all certificate in the certification path if possible** and **Enable strong protection** under the **Personal Information Exchange – PKCS #12 (.PFX)** option. Click **Next**.

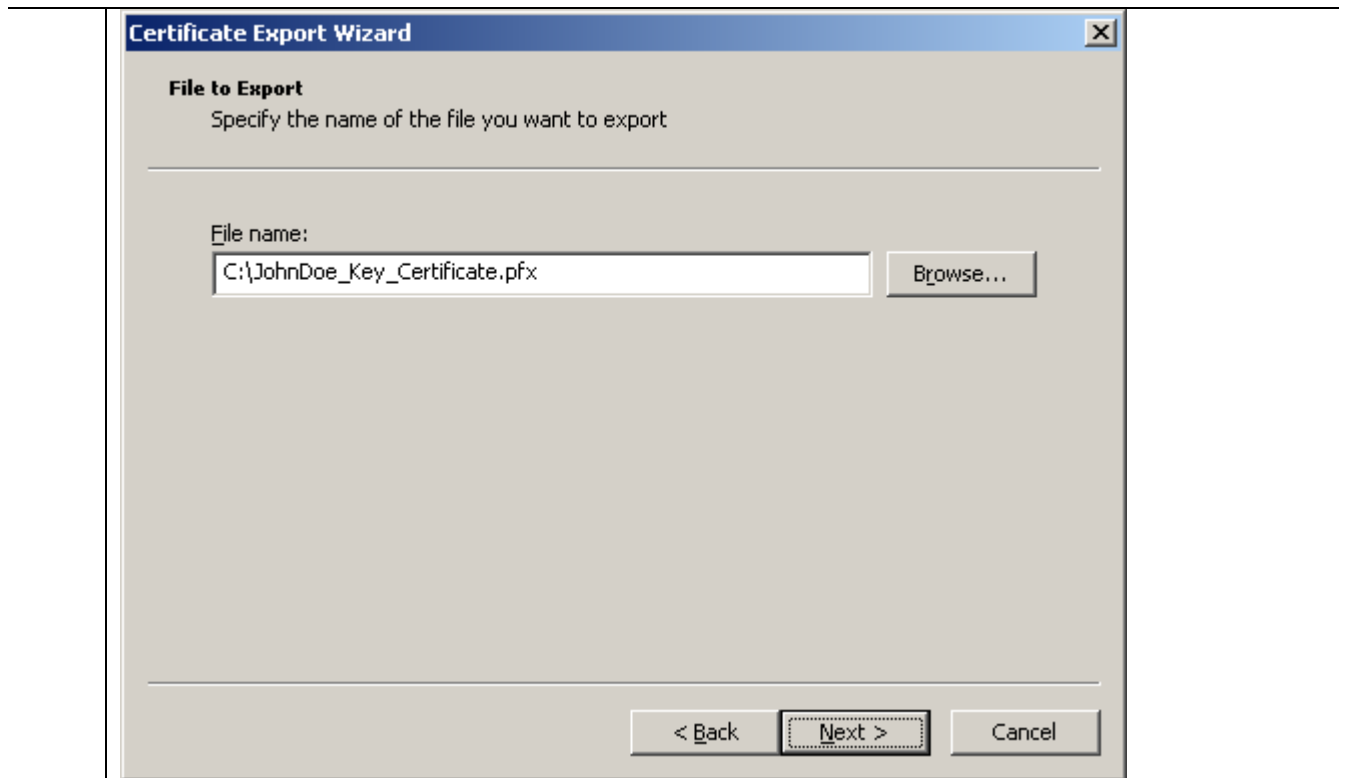


- 4 In the **Password** screen, enter a password to secure the PFX file (containing your private key and certificate) in the **Password** and **Confirm password** fields. Click **Next**.

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**. Click **Finish** in the **Completing the Certificate Export Wizard** screen. Click **OK** in the message box to complete the procedure.



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