

**Guide to Obtaining Your
Free WIS@Key CertifyID
Personal Digital Certificate
(Personal eID)
WIS@Key 2010 / Alinghi 2010
Smartcards**

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

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>
Pre-Installation requirements	3
Install Smartcard reader	3
Install Smartcard Software	3
Free Secure e-Mail eID	4
<i>Creating your profile</i>	<i>4</i>
Creating your Profile	4
Email Verification	6
Keypair Generation	6
Install Certificate	8
Verify that your certificate has been installed	9
What Next?	11
Support	12

About this User Guide

This manual describes the steps followed to obtain a WISEKey CertifyID Digital Certificate (eID) for securing your e-mail transactions, on the Alinghi 2010 branded smartcard.

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.

Pre-Installation requirements

All software should be available on the WISEkey web site at the following location:

<http://www.wisekey.com/en/projects/alinghi/10/help/Pages/default.aspx>

INSTALL SMARTCARD READER

Before proceeding you should have installed your smartcard reader, and its software drivers.

Ensure you have installed a Smartcard reader.

If you have a WISEkey SCR3xxxx Smartcard reader then you can [download the smartcard drivers from the web site and install them](#).

INSTALL SMARTCARD SOFTWARE

Before proceeding you should have installed the WISEKey Smart Security Interface, please refer to its manual for installation instructions.

[Download and install the WISEKey Smart Security Interface software drivers](#) (Windows only). These drivers provide support for MS_CAPI, CSP and PKCS#11 cryptographic interfaces.


Please refer to the WSSI manual to install the software, and change the default PIN of your smartcard from 11111111 to your personal password.

After you have successfully installed your card reader, and inserted your card into your reader, and preferably changed the smartcard PIN, then please continue below to obtain your free digital certificate.

Free Secure e-Mail eID

Creating your profile

CREATING YOUR PROFILE

Steps	Instructions
1	Open Internet Explorer . Type https://secure.certifyid.com/certifyid/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>

Create your CertifyID Account - Windows Internet Explorer

https://secure.certifyid.com/certifyid/accounts/Register.aspx

WIS@key
CertifyID CREATE A CERTIFYID ACCOUNT

Please complete the form with the information that will be displayed in you Digital ID.

1. LOGON ID:

2. PASSWORD:
 Password confirmation:

3. EMAIL ADDRESS:

4. PASSWORD RECOVERY: I prefer NOT to use password recovery

Password recovery question 1:
 Your answer:
 Password recovery question 2:
 Your answer:

5. PROMO CODE (OPTIONAL)

IF YOU HAVE ANY PROMO CODE PLEASE ENTER IT.

Create your CertifyID Account - Windows Internet Explorer

https://secure.certifyid.com/certifyid/accounts/Register.aspx

4. PASSWORD RECOVERY: I prefer NOT to use password recovery

Password recovery question 1:
 Your answer:
 Password recovery question 2:
 Your answer:

5. PROMO CODE (OPTIONAL)

IF YOU HAVE ANY PROMO CODE PLEASE ENTER IT.

TERMS OF SERVICE

Please review the Account information you've entered above, and change it if necessary, then review the Privacy Policy below. [\[clickable version\]](#).

Important Note for Relying Parties
 Reliance on a certificate or certificate revocation list issued by the CertifyID CA that issued the certificate requires agreeing to the terms of the Relying Party Agreement and assessing whether such reliance is reasonable. In order to do so, it is essential to read and understand the provisions of this document, the CertifyID CA Certification Practice Statement (CPS) and Certificate Policy under which the certificate was issued (all of which are available at <http://www.wisekey.com/repository>).

By checking 'I accept' below, you are agreeing to the the Privacy Policy above.

I accept

EMAIL VERIFICATION

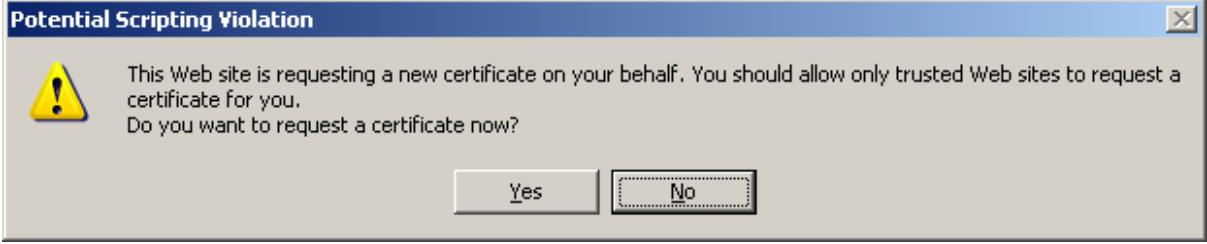
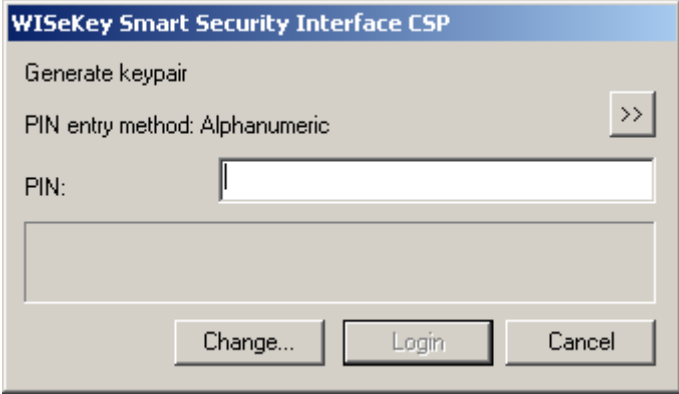
Steps	Instructions
1	<p>You must use a valid email address. An email verification code will be sent to this email address and you should check your email to retrieve the message.</p> <p><i>NOTE: Use an email address that is accessible from an S/MIME capable email application. Examples of S/MIME capable 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>jdove@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>jdove@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 where 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="512 1536 987 1576" type="text" value="0dg7degoidi6kirm8txv"/> <input data-bbox="997 1536 1090 1576" 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.

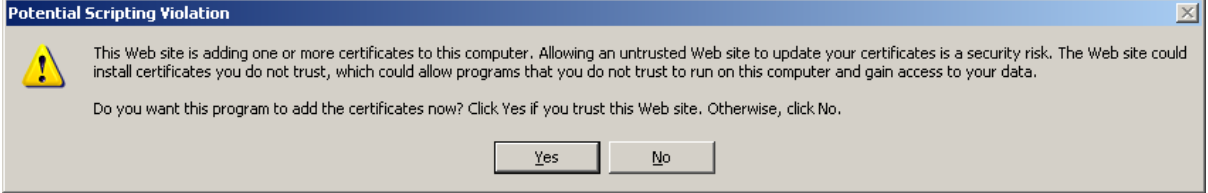
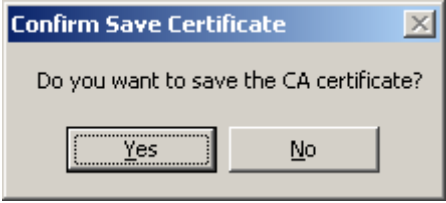

NOTE: Only CertifyID Account users that have verified their email address can obtain a digital certificate.

Steps	Instructions									
1	<p>Ensure that your smartcard is inserted properly in the smartcard reader, and that the smartcard reader is functioning properly.</p> <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. If necessary click on the Requests menu to arrive at the requests page.</p> <p>Check the box to agree with the CertifyID Subscriber Agreement.</p> <p>Select the WiseKey Smart Security Interface User (CSP) Cryptographic Provider 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="288 846 1481 1809" style="border: 1px solid black; padding: 10px;"> <p style="text-align: center;">SUBMIT NEW CERTIFICATE REQUEST</p> <p>Certificate Template Name: CertifyID Standard User</p> <hr/> <p style="text-align: center;">Subject</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Email</td> <td style="width: 60%;"><input type="text"/></td> <td style="width: 10%;"></td> </tr> <tr> <td>Common Name</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>Organizational Unit</td> <td>Person's Identity not Verified - CertifyID Standard User</td> <td style="text-align: center; color: red;">*</td> </tr> </table> <hr/> <p style="text-align: center;">Other Options</p> <p>Cryptographic Service Provider (CSP): WISEKey Smart Security Interface CSP</p> <p>Key Size: 2048</p> <p><input checked="" type="checkbox"/> Mark keys as exportable</p> <p><input checked="" type="checkbox"/> I ("certificate subscriber") hereby agree to the terms and conditions of the CertifyID Subscriber Agreement and to comply with its provisions.</p> <p style="text-align: center; margin-top: 20px;">Generate</p> </div>	Email	<input type="text"/>		Common Name	<input type="text"/>		Organizational Unit	Person's Identity not Verified - CertifyID Standard User	*
Email	<input type="text"/>									
Common Name	<input type="text"/>									
Organizational Unit	Person's Identity not Verified - CertifyID Standard User	*								
2	Click Yes in the Internet Explorer message box.									

	 <p>Potential Scripting Violation</p> <p>This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you. Do you want to request a certificate now?</p> <p>Yes No</p>
<p>3</p>	<p>If you have already changed your smartcard pin (see WSSI manual), then enter your new PIN, otherwise enter the default PIN in the WSSI CSP Generate keypair dialog box.</p> <p>Default PIN is 11111111</p> <p>When you have entered your PIN, click the Login button.</p>  <p>WiseKey Smart Security Interface CSP</p> <p>Generate keypair</p> <p>PIN entry method: Alphanumeric >></p> <p>PIN: <input type="text"/></p> <p>Change... Login Cancel</p>

INSTALL CERTIFICATE

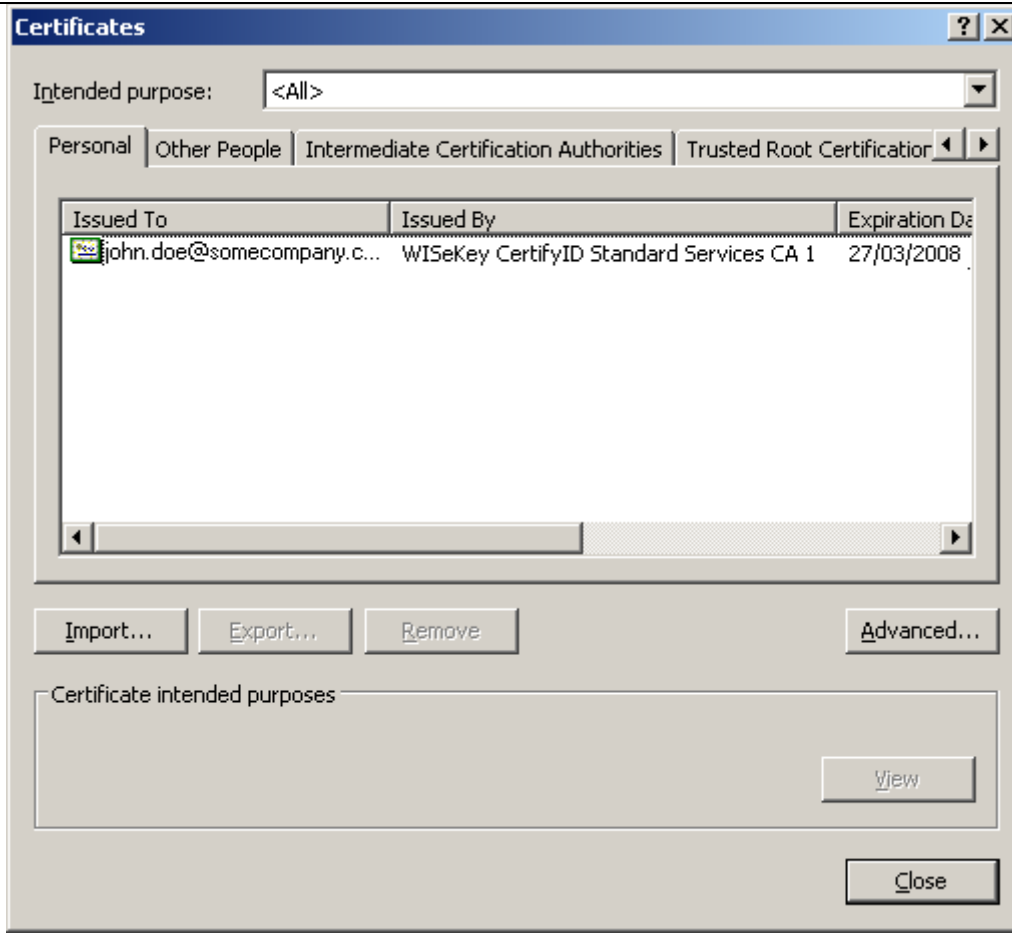
<i>Steps</i>	<i>Instructions</i>
<p>1</p>	<p>The certificate should be immediately generated and the following page should appear:</p> <p>Ensure that your card is still in the reader, and select Install to install the entire certificate chain to your smartcard.</p> <p>Your certificate (ID:5756) has been issued successfully</p> <p>Certificate details Download Install</p>  <p>You may see the following prompts several times, always click the Yes button when the following prompts appear.</p>

	 
<p>2</p>	<p>You should then see the following page, indicating that the certificate is installed and ready for use in your PKI enabled applications.</p> <p>Your certificate (ID:5756) has been issued successfully</p> <p style="text-align: center;"> <input type="button" value="Certificate details"/> <input type="button" value="Download"/> <input type="button" value="Install"/> </p> <p><i>The Certificate is now installed and ready to be used.</i></p> 
<p>3</p>	<p>Click Logout tab in the right hand top of the page to logout from the application.</p>

VERIFY THAT YOUR CERTIFICATE HAS BEEN INSTALLED

The digital certificate should also have been installed in your Windows operating system, and the Internet Explorer browser store.

<i>Steps</i>	<i>Instructions</i>
<p>1</p>	<p>Open Internet Explorer. Click Tools > Internet Options > Content > Certificates. You should see your certificate appear in the list, with your email address as the Common Name.</p>



What Next?

You can now use your digital certificate to

Access Web Sites securely

- <https://secure.certifyid.com/certifyid/accounts>
 - You should now be able to logon to your certifyid account using your digital certificate. Ensure that your certificate is inserted in your smartcard and have your PIN ready for this process.
- Accessing web-sites with your digital certificate offers the following advantages:
 - Increased authentication security – it is impossible for an imposter to access your account with a fake certificate, as your key and certificate are unique and are accessible only with your smartcard, or computer.
 - Increased communication security – in order to access a site with a digital certificate, a secure communications channel, called SSL is built. This assures you that your communications with that web site remain confidential.

Send digitally signed messages

- Configure your digital certificate in your email application. You should now be able to configure your digital certificate in your email application in order to use your digital certificate to send digitally signed messages. Digitally signed email has the following advantages:
 - Recipients are assured that the message is from you, and that it is not spam.
 - If the message was changed or tampered with during transit then the recipient will be automatically alerted.

Receive secure confidential messages

- Once you have configured your digital certificate in your email application, and have sent signed messages to recipients, those recipients can add your contact details to their address book, along with your digital certificate. They can thereafter send you encrypted S/MIME (secure email) messages. Such messages are confidential and can only be decrypted and read with your private key, which is stored on your computer or smartcard.
- Note that some email packages require that your recipient also obtains a digital certificate before they are able to send you encrypted email.

WISEkey provides some guides to configuring your digital certificate with some popular email applications. These guides can be found in the support section of WISEKey's web site <http://www.wisekey.com/en/support>.

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