

## **Guide to Obtaining Your Free WIS@Key CertifyID Personal Digital Certificate on Aladdin eToken (Personal eID)**

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

Date: September 2007  
Version: 1.0.0  
Authors: WIS@Key SA

## TABLE OF CONTENTS

<b>About this User Guide .....</b>	<b>1</b>
<i>About Personal eID (Digital Certificate) .....</i>	<i>1</i>
<i>Document Conventions.....</i>	<i>1</i>
<i>Copyright.....</i>	<i>2</i>
<i>Software and Hardware Requirements.....</i>	<i>2</i>
<b>Verify and Initialize your eToken .....</b>	<b>3</b>
Using your eToken for the First Time.....	3
Initializing a previously used eToken .....	4
<b>Free Secure e-Mail eID.....</b>	<b>6</b>
Creating your Profile .....	6
Email Verification .....	8
Keypair Generation .....	8
Install Certificate.....	10
<b>Support.....</b>	<b>12</b>

## 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 and to install it on an Aladdin eToken hardware device. Installing a digital certificate on a hardware device is preferable to storing it on your computer as it is much safer and can easily travel with you and thus allow you to use your certificate on different machines and environments.

### About Personal eID (Digital Certificate)

A digital certificate 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 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.

### 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.

## 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 WIS@key SA.



is a registered trademark of WIS@key SA.



is a registered trademark of WIS@key SA.

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

## Software and Hardware Requirements

Hardware	Description
Operating System	Microsoft Windows XP, 2000, 2003
Web Browser	Microsoft Internet Explorer version 5 and up
eToken Software	Aladdin eToken PKI Client version 4.5 and higher
Supported Aladdin eToken modules (SmartCard and USB) versions	eToken PRO 32k eToken PRO 64k eToken PRO 72k (Java)

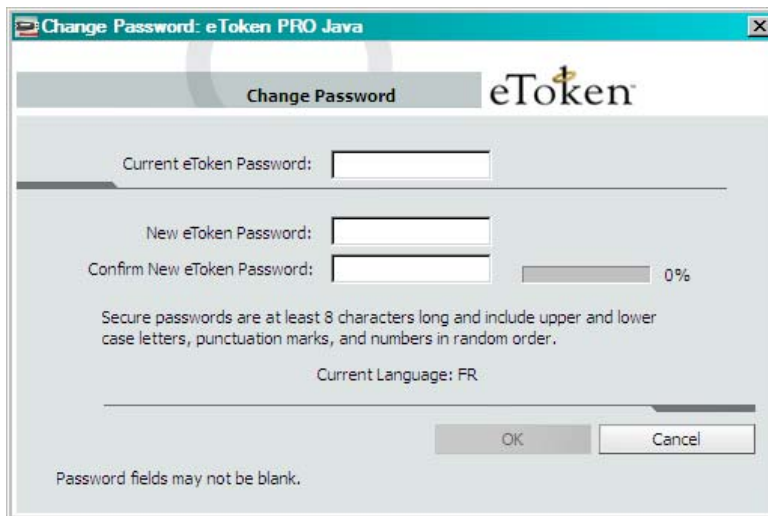
## Verify and Initialize your eToken

In this guide we assume that you have already successfully installed a version of the Aladdin eToken PKI Client software. For instructions on how to install the Aladdin software please refer to the Aladdin installation manuals.

### USING YOUR eTOKEN FOR THE FIRST TIME

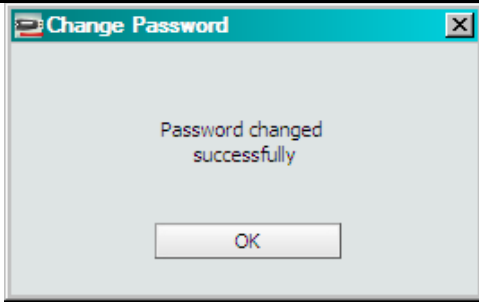
Once the Aladdin eToken PKI client is installed, you should verify that your token is correctly detected and initialized. This can be done by performing the following steps:

Steps	Instructions
1	Plug in your eToken into a free USB port
2	Check that the red light on the eToken is on. If so, the token is detected and the software is working fine. If the light does not show up it means that either the eToken software is not installed or it is recent enough to recognize the token (Please note that eToken PKI Client version 4.5 or higher is required for the eToken PRO 72k Java).
3	When you plug in the token for the first time, the eToken software will prompt you to modify the default password (Figure 1).



**Figure 1**

- a. Enter the default password
- b. Enter your new password twice
- c. Press OK (Figure 2)



**Figure 2**

Now your eToken is initialized and you are ready to install some certificates onto it.

### INITIALIZING A PREVIOUSLY USED ETOKEN

If you are using an eToken that has been used before, be sure that you know the token password, and that there is still space left on the device. If you do not remember the password or if the contents of the token are obsolete, you may wish to initialize the token to clear all the contents and set a new password.

Steps	Instructions
1	<p>Open the eToken Properties program (Figure 3)</p> <p><b>Figure 3</b></p>
2	Select "Advanced"
3	Select your token (Figure 4)

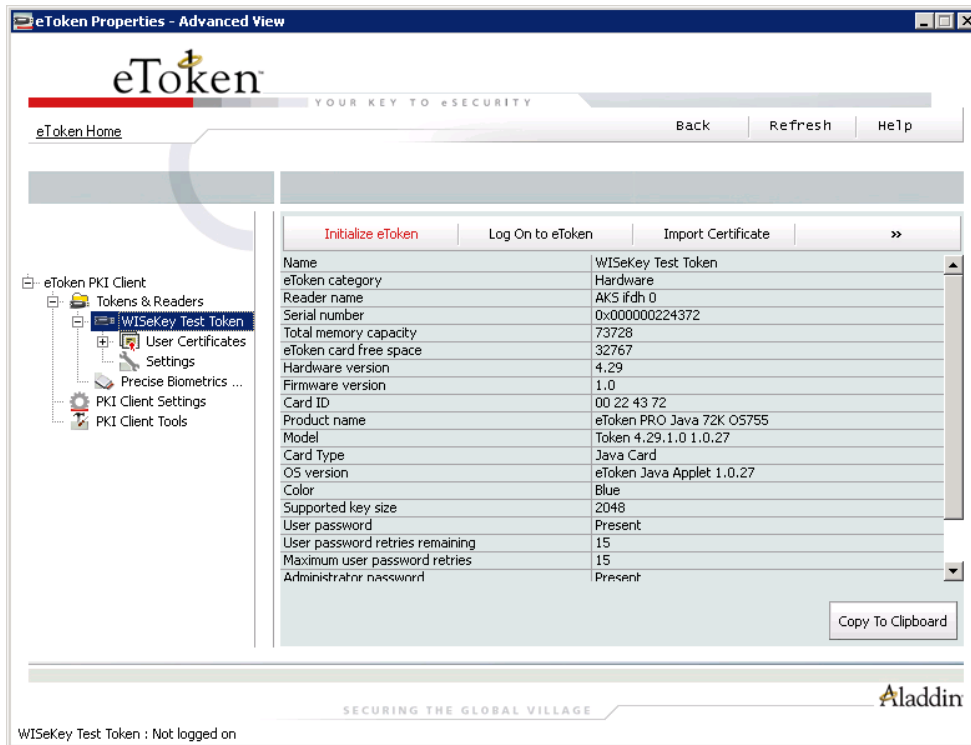


Figure 4

- 4 Select "Initialize eToken"
- 5 On the following dialog (Figure 5) please fill in a new name for the eToken, and select a new password. A click on "Start" will reinitialize the token. Please be aware that all data on the token will be lost, so this should only be performed if the current content is no longer needed.

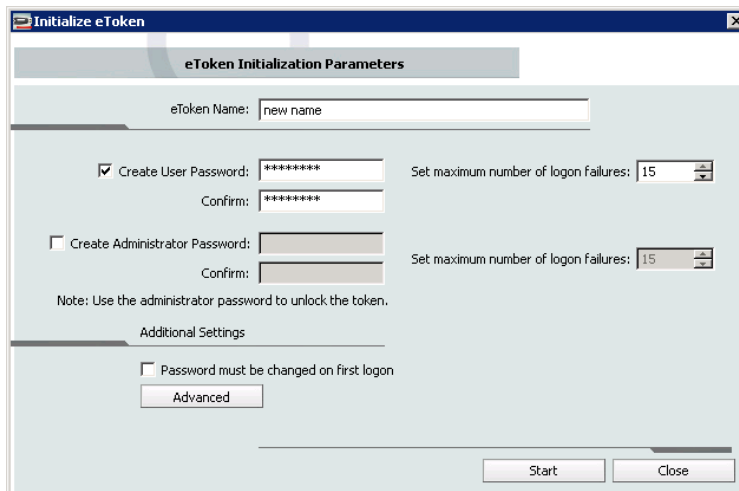



Figure 5

# Free Secure e-Mail eID

## CREATING YOUR PROFILE

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

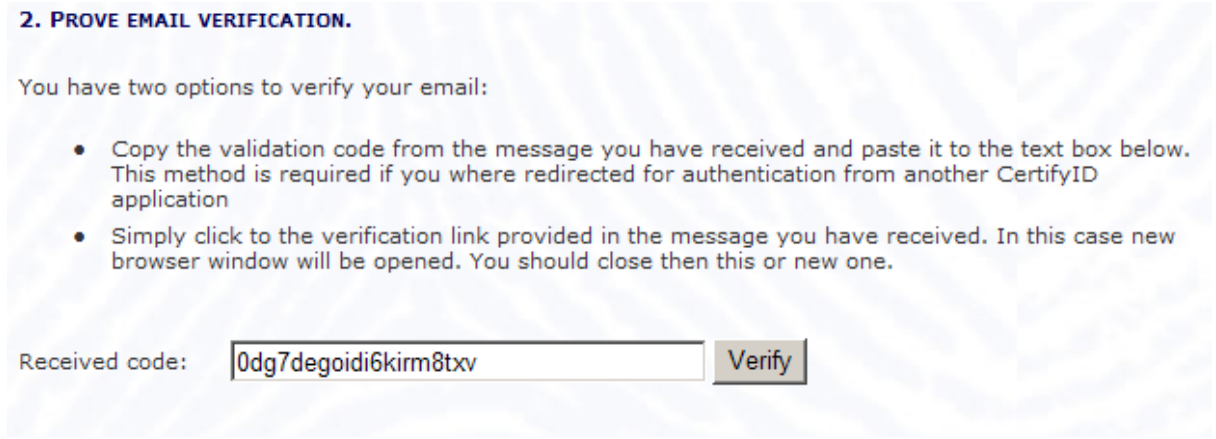
Please review the Account information you've entered above, and change it if necessary, then review the Privacy Policy below. [\[Printable version\]](#).

**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>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 you have not received your verification email, then click the browser's back button and check your email address in the <b>Create your CertifyID Account</b> page. If your email address is correct and you have not received your verification email, then go to the <b>CertifyID Account email verification</b> 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 <b>CertifyID Account email verification</b> page you can enter the verification code received in your email, then click the <b>Verify</b> Button to verify your email address.</p>  <p><b>2. PROVE EMAIL VERIFICATION.</b></p> <p>You have two options to verify your email:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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.</li> </ul> <p>Received code: <input type="text" value="0dg7degoidi6kirm8txv"/> <input type="button" value="Verify"/></p>

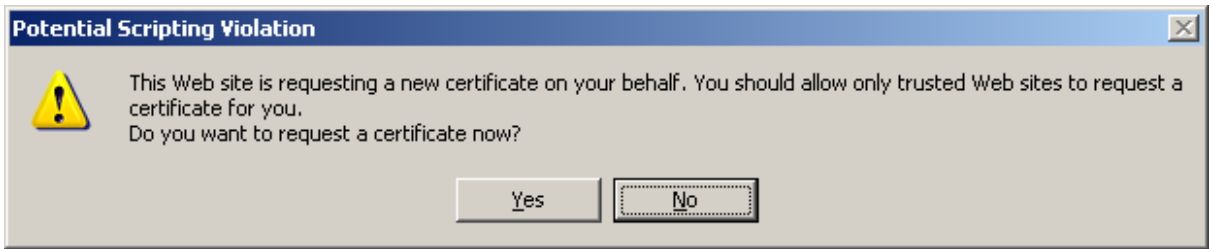
## KEYPAIR GENERATION

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 <b>Certificates</b> page.</p> <p>Click on the button title <b>Online Web Enrollment</b>, or the <b>Enroll</b> menu item. You will arrive in the <b>CertifyID Registered User</b> page. Now you need to select the <b>eToken Base Cryptographic Provider</b>. Once you made sure your correct eToken is plugged in (and you have no other eTokens connected to the system), you can click the <b>Generate</b> button.</p>  <p><b>CERTIFICATE WEB ENROLLMENT</b></p> <p>Click on "Generate" to get your certificate</p> <p><b>User Information</b></p> <p>First Name: JohnDoe          Last Name: [Empty]</p> <p><b>Certificate Template</b></p> <p>Certificate Template Name: CertifyID Standard User</p> <p><b>Subject [Identifying Information]</b></p> <p>EMAIL: john.doe@somecompany.com          COMMON_NAME: john.doe@somecompany.com          ORGANIZATIONAL_UNIT: Person's Identity not verified - Ce</p> <p><b>Key Options</b></p> <p>Cryptographic Service Provider (CSP): eToken Base Cryptographic 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"/></p> <p><b>Generate</b></p> <p><i>NOTE: If you do not select the eToken Base Cryptographic Provider while you generate the certificate request, the private key will be stored on your local machine and not on your eToken.</i></p>

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



**Figure 6**

3 Now you are prompted for your eToken password



**Figure 7**

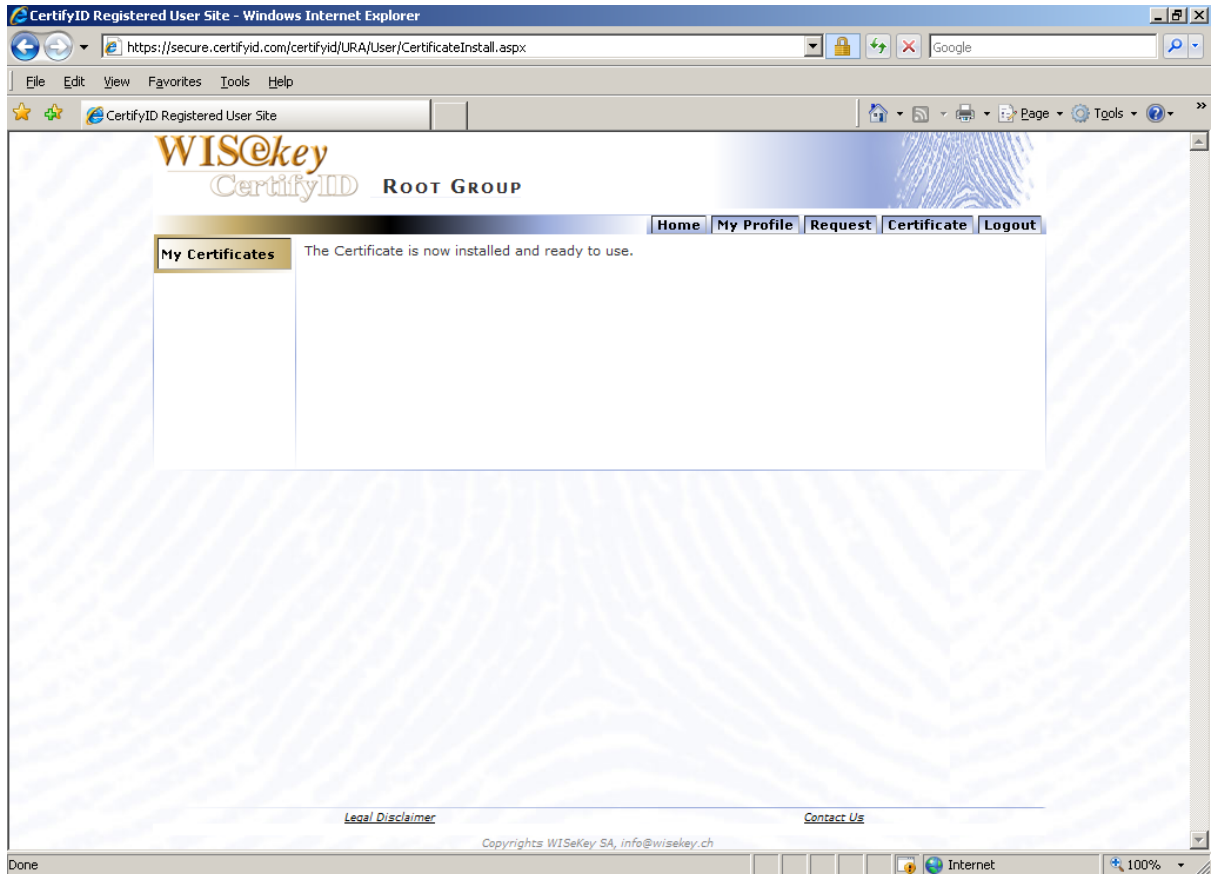
It takes a couple of seconds while the key pair is generated. During this time the red light on the eToken is blinking.

**INSTALL CERTIFICATE**

Steps	Instructions
1	The certificate should be immediately generated and the following prompt should appear in <b>CertifyID Registered User page</b> , click <b>Yes</b> in the Internet Explorer message box to install the entire certificate chain. On some setups this message will appear twice.



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.

Your WISEKey CertifyID Personal Digital Certificate is now successfully installed on your eToken. You can use it now to secure your email communication, to securely authenticate with certificate-enabled websites and to sign and encrypt documents.

## 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](mailto:support@wisekey.com)