



ASX

AUSTRALIAN SECURITIES EXCHANGE

# ASXAustraclear System

Client Side Digital Certificates (CSDC)

User Enrolment Guide

This information is proprietary and confidential to the SFE Corporation and copyright is strictly reserved. No part of this document may be reproduced or copied in any form or by any means without prior written permission by SFE Corporation.

# TABLE OF CONTENTS

<b>1 INTRODUCTION.....</b>	<b>3</b>
<b>USER ENROLMENT .....</b>	<b>3</b>
2.1 USER INFORMATION.....	3
2.2 ENROLMENT PROCEDURE .....	3
2.3 NEXT STEP .....	9
<b>PASSCODE EXPIRATION AND LOCKOUT.....</b>	<b>9</b>
<b>VALIDATING THE ENROLMENT WEB SITE.....</b>	<b>9</b>

# INTRODUCTION

The users require a client side digital certificate to access the new SFE Austraclear system. This document is a digital certificate enrolment guide and it details the information required and provides a step-by-step procedure for obtaining a digital certificate.

Please be aware that a digital certificate can only be downloaded from the Verisign webpage once. Please refer to the CSDS Import and Export guide for further information on how to export a certificate.

## USER ENROLMENT

### 2.1 USER INFORMATION

The following user information is required to complete the user enrolment process:

- First Name (User Id)
- Last Name (First and Last name of User)
- E-mail Address
- Passcode
- Participant Id
- Username (User Id)

The above information is verified against the registration information entered by the ASX during user registration.

### 2.2 ENROLMENT PROCEDURE

Please note that in the XP environment, login under the User Id and not as an administrator, otherwise the Digital Certificate will be enrolled without the private key.

The enrolment page is accessed through the Digital ID Centre secure website hosted by VeriSign. The enrolment website can be accessed either from the Austraclear webpage <https://exigo.austraclear.com.au/> or by entering the URL directly into the browser.

- 1) <https://exigo.austraclear.com.au/> for the Production Environment or <https://exigota.austraclear.com.au/> for the Test Bed Environment.

Please then click on the Digital Certificate Enrolment link. (Please note that the URL is case-sensitive)

- 2) Or go directly to the Verisign webpage via the link below.

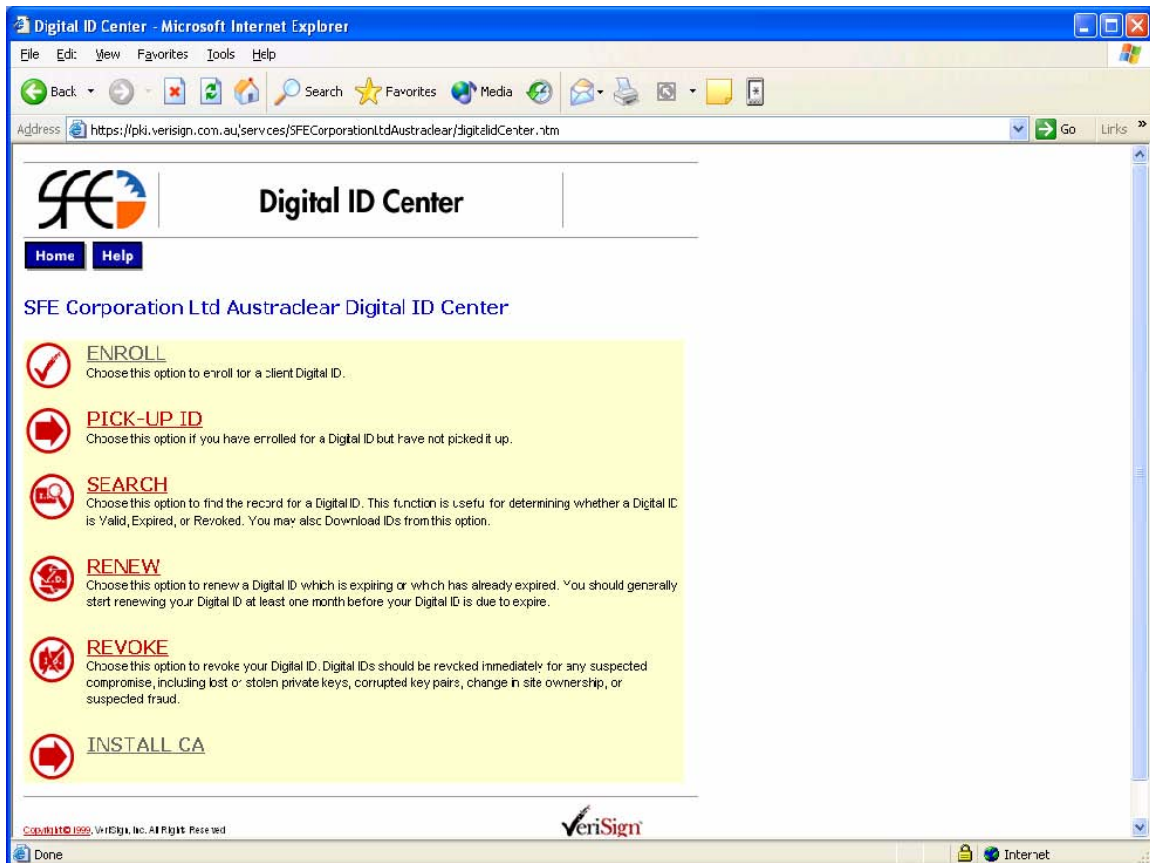
<https://pki.verisign.com.au/services/SFECorporationLtdAustraclear/digitalidCenter.htm>

When loading the enrolment page for the first time, you will see a **Security Warning** dialog for a program digitally signed by Microsoft. This program is required to enrol for a certificate. It is safe to run it on your computer and its authenticity is proven by a digital signature. Click **Yes**

(This window will not appear if Verisign is already listed a trusted site)



The following screen is displayed and the **ENROLL** option is used to display the Enrolment Form (Click on **ENROLL**)



The following fields must be entered exactly as advised by your Password Administrator:

- First Name (User Id)
- Last Name (First and Last name of User)
- E-mail Address
- Passcode
- Participant Id
- Username (User Id)


The only field not case sensitive is the Passcode.

Microsoft end-user Enrollment - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media

Address <https://pki.verisign.com.au/services/SFECorporationLtdAustralclear/client/userEnrollMS.htm> Go Links >>

 **Enrollment**

**Help with this Page**

**Complete Enrollment Form**

**Enter your Digital ID information**

Fill in all required fields. Fields marked with an asterisk (\*) are included with your Digital ID and are viewable in the certificate's details.

<b>First Name: *</b> (required) Nickname or middle initial allowed (Example: <b>Jack B.</b> )	<input type="text" value="aaaa2015"/>
<b>Last Name: *</b> (required) (example -- Doe)	<input type="text" value="john smith"/>
<b>Your E-mail Address: *</b> (required) (example -- jdoe@verisign.com)	<input type="text" value="jith@participant.com.au"/>
<b>Passcode:</b> (required)	<input type="text" value="BB094BF7"/>
<b>Participant Id: *</b> (required)	<input type="text" value="aaaa20"/>
<b>Username: *</b> (required)	<input type="text" value="aaaa2015"/>

Done Internet

The **Challenge Phrase** is a unique phrase set by the user and not shared with anyone. If you forget this phrase you will be required to apply for a new Digital Certificate by completing the Digital Certificate request form and faxing to the ASX

The ASX has allowed users to select the **Cryptographic Service Provider** in compliance with your organization's security policies and procedures. This allows users to store their generated digital certificates to the local PC, a smartcard, or a USB device. If the destination is the local PC, the default selection is **Microsoft Base Cryptographic Provider**.

**Additional Security for Your Private Key** selection allows you to select additional security for your private key. **Please DO NOT select the option to protect the private key**, by ticking this box you will not be able to export the Digital Certificate.

Microsoft end-user Enrollment - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media History

Address <https://pki.verisign.com.au/services/SFECorporationLtdAustralclear/client/userEnrollMS.htm> Go Links

**Challenge Phrase**  
This unique phrase protects you against unauthorized action on your Digital ID and should not be shared with anyone. Do not lose it! It is required to revoke and renew your Digital ID.

**Enter Challenge Phrase:** (required)  
Do not use any punctuation.

**Optional: Select The Cryptographic Service**  
If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.

**Cryptographic Service Provider Name** Microsoft Base Cryptographic Provider v1.0

**Additional Security for Your Private Key**  
We recommend that you protect the private key associated with your digital ID. Checking the box below will provide you with security options for your private key. [Click Here](#) for additional information.

**Check this Box to Protect Your Private Key**  [Do not check this box](#)

**Optional: Enter Comments**  
In some cases, your Administrator will instruct you to enter *Shared Secret* (information known only to you and the Administrator) information in this field. The Administrator uses this shared secret to verify that it

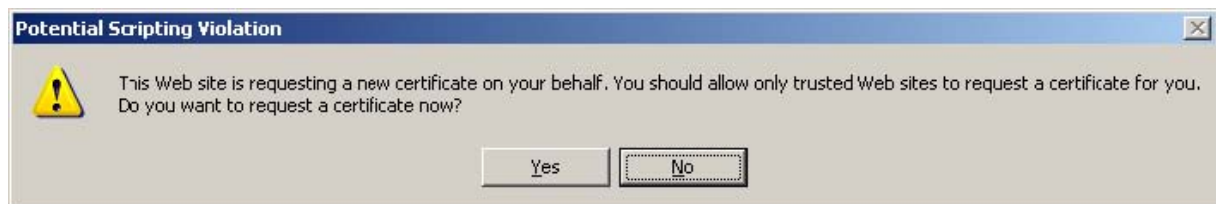
When all the fields have been entered, click on **Accept**.

Done Internet

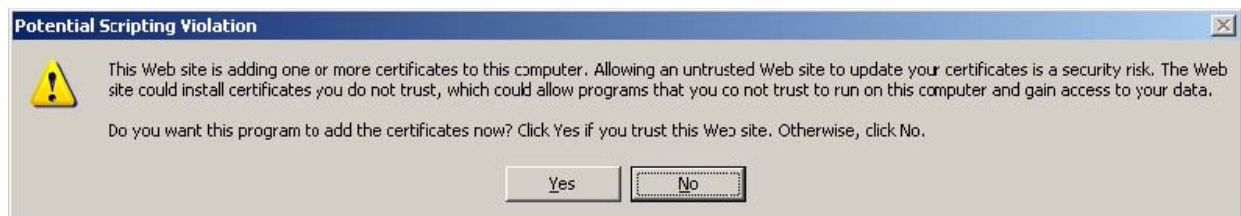
The popup window appears asking the confirmation of your e-mail address.



If the address is correct click on OK The warning window "Potential Scripting Violation" appears.

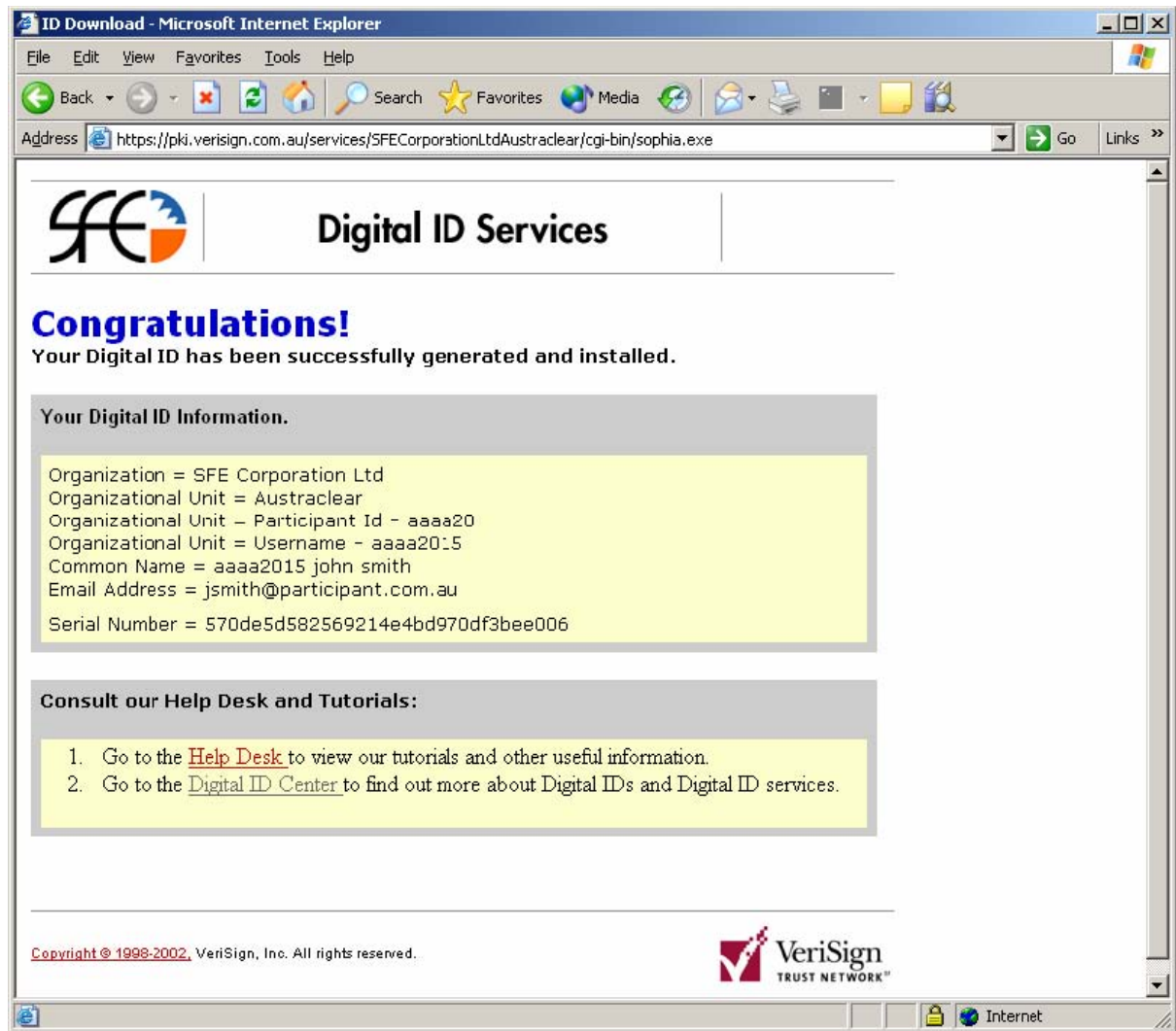


If you have confirmed that the web site is authentic, click on **Yes** to request the certificate. The following warning window appears:

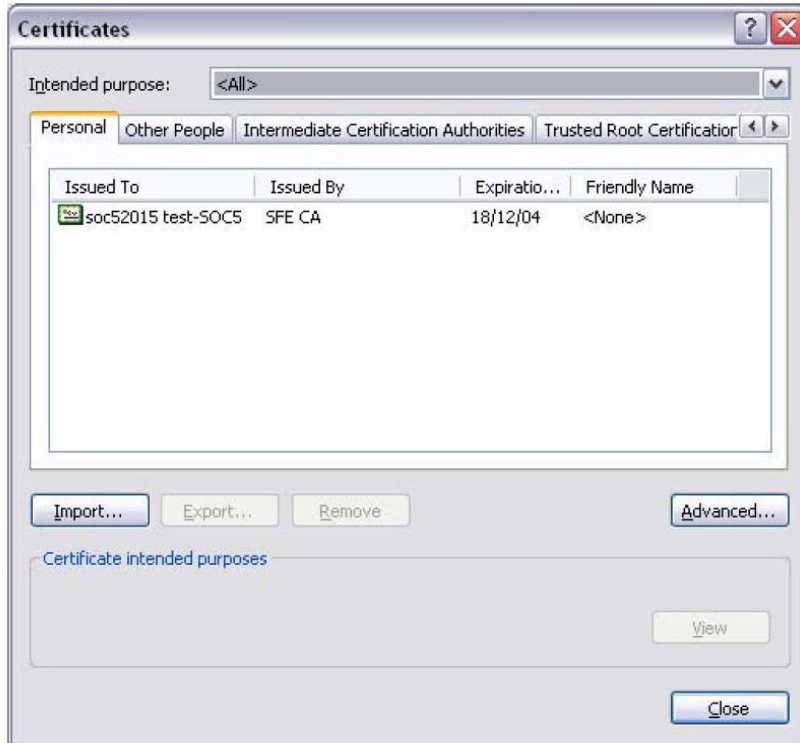


Click on **Yes** to add the certificate to your computer.

After the certificate is successfully installed the following Confirmation page is shown:



To confirm that the certificate has been successfully installed, open the Internet Explorer browser and click on: \Tools\Internet Options...\Content\Certificates...and check that the expiry date is one year out.



 Digital Certificate Successfully enrolled

### 2.3 NEXT STEP

Once the Digital Certificate has been successfully installed, please refer back to your Deployment User Guide for the procedures to deploy the software for the new system, using either the file or browser deployment method.

The SFE has configured the following policy relating to the Passcode expiry period and the lockout threshold for invalid entries:

- The Passcode expiration for enrolment is set to one month from the date of issue.
- The lockout threshold is set to three attempts. Fourth invalid entry will lockout the registration record and will require the SFE to reset the Passcode for the user.

## VALIDATING THE ENROLMENT WEB SITE

You can validate the web server's certificate before you enrol by clicking the security lock icon at the bottom right corner of the Internet Explorer window. The web server's certificate should show the following information:

**Issued to:**  
pki.verisign.com.au

**Issued by:**  
Secure Server Certification Authority

**Valid from:**  
[Check that the certificate is valid]