



SecureToken ST2

User's Guide

Version 1.1

Disclaimer

The information contained in this Software Development Kit is for general guidance on using SecureMetric products. While SecureMetric have made every attempt to ensure the information contained in this Software Development Kit is believed to be accurate and reliable, however SecureMetric is not responsible for any errors or omissions, or for any infringement of patents or other rights of third parties resulting from its use. Any third party trademarks or trade names are the property of their respective owners.

All the Products, Software Samples, Tools, Utilities and Documents contained in this Software Development Kit are the Intellectual Property of SecureMetric. SecureMetric reserves the right to make changes, updates, amendment, at anytime and without notice.

Copyright © 2008 SecureMetric Technology Sdn Bhd. All rights reserved.

Revision History:

| Date | Version | Description |
|--------------|----------------|--------------------|
| January 2007 | 1.0 | 1st Edition |
| July 2008 | 1.1 | 1st Revision |

Software Developer's Agreement

All Products of Securemetric Technology Sdn. Bhd. (Securemetric) including, but not limited to, evaluation copies, diskettes, CD-ROMs, hardware and documentation, and all future orders, are subject to the terms of this Agreement. If developers do not agree with the terms herein, please return the evaluation package to us, postage and insurance prepaid, within seven days of their receipt, and we will reimburse developers the cost of the Product, less freight and reasonable handling charges.

1. Allowable Use - Developers may merge and link the Software with other programs for the sole purpose of protecting those programs in accordance with the usage described in the Developer's Guide. Developers may make archival copies of the Software.

2. Prohibited Use - The Software or hardware or any other part of the Product may not be copied, reengineered, disassembled, decompiled, revised, enhanced or otherwise modified, except as specifically allowed in item 1. Developers may not reverse engineer the Software or any part of the product or attempt to discover the Software's source code. Developers may not use the magnetic or optical media included with the Product for the purposes of transferring or storing data that was not either an original part of the Product, or a Securemetric provided enhancement or upgrade to the Product.

3. Warranty - Securemetric warrants that the hardware and Software storage media are substantially free from significant defects of workmanship or materials for a time period of twelve (12) months from the date of delivery of the Product to developers.

4. Breach of Warranty - In the event of breach of this warranty, Securemetric's sole obligation is to replace or repair, at the discretion of Securemetric, any Product free of charge. Any replaced Product becomes the property of Securemetric.

Warranty claims must be made in writing to Securemetric during the warranty period and within fourteen (14) days after the observation of the defect. All warranty claims must be accompanied by evidence of the defect that is deemed satisfactory by Securemetric. Any Products that developers return to Securemetric, or a Securemetric authorized distributor, must be sent with freight and insurance prepaid.

EXCEPT AS STATED ABOVE, THERE IS NO OTHER WARRANTY OR REPRESENTATION OF THE PRODUCT, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. Limitation of Securemetric's Liability - Securemetric's entire liability to developers or any other party for any cause whatsoever, whether in contract or in tort, including negligence, shall not exceed the price developers paid for the unit of the Product that caused the damages or are the subject of, or indirectly related to the cause of action. In no event shall Securemetric be liable for any damages caused by developers failure to meet developer's obligations, nor for any loss of data, profit or savings, or any other consequential and incidental damages, even if Securemetric has been advised of the possibility of damages, or for any claim by developers based on any third-party claim.

6. Termination - This Agreement shall terminate if developers fail to comply with the terms herein. Items 2, 3, 4 and 5 shall survive any termination of this Agreement.

CE Attestation of Conformity



The equipment complies with the principal protection requirement of the EMC Directive (Directive 89/336/EEC relating to electromagnetic compatibility) based on a voluntary test.

This attestation applies only to the particular sample of the product and its technical documentation provided for testing and certification. The detailed test results and all standards used as well as the operation mode are listed in

Test report No.: 70407310011
Test standards: EN 55022/1998 EN 55024/1998

After preparation of the necessary technical documentation as well as the conformity declaration the CE marking as shown below can be affixed on the equipment as stipulated in Article 10.1 of the Directive. Other relevant Directives have to be observed.

FCC certificate of approval



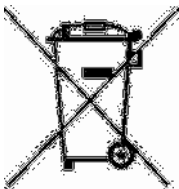
This Device is in conformance with Part 15 of the FCC Rules and Regulations for Information Technology Equipment.

USB



This equipment is USB based.

WEEE



Dispose in separate collection.



1 User Guide Summary

This User Guide provides the user friendly explanation and guidance on how to use SecureToken ST2 Token Manager which includes the following topics:

- Prerequisite
- Overview
- Login
- Certificate Management
- Change Token Name
- Change User PIN
- Diagnostic
- Slot/Token Information
- About

1.1 Prerequisite

User must correctly install SecureToken ST2 middleware into computer before start using the SecureToken ST2 Manager.

Inset SecureToken ST2 SDK CD and double click on ST2.exe in the root directory, the middleware will be installed follow the below screen.



Fig. 1.0 SecureToken ST2 auto setup wizard

Click on **Install** button to start SecureToken ST2 middleware installation.

1.2 Overview

1.2.1 Interface Before Connecting the Token

The shortcut for the Manager could be found under “Start” → “Programs” → “Securemetric” → “Secure Token (ST2)” → “Token Manager”. Click the shortcut to start the Manager tool. The following window appears without any USB token details.



Fig. 1.1

1.2.2 Interface After Connecting the USB Token

Right after user plug in the SecureToken ST2 USB token, all menus will be displayed as screen (Fig 1.2) below. The SecureToken ST2 Token Manager will recognize the basic information of the token automatically.



Fig. 1.2

1.2.3 Tree View Menus

The tree view menus on the main interface of the Manager includes the functions listed below (will cover into more details in later sections).

Configuration → Change Token Name

Facilitate user to change the identifier name of the SecureToken ST2.

Configuration → Change User PIN

Facilitate user to change the SecureToken ST2 User PIN.

Diagnostic

Facilitate user to diagnose SecureToken ST2 technical problem.

Slot/Token Information

Show basis Slot and Token information.

About

General information about SecureToken ST2.

1.3 Login

Before accessing SecureToken ST2 USB Token private zone that contains Private Key, Login with valid User PIN verification is necessary. Just click on the “Certificate” and a login dialog box appears as Fig 1.3.

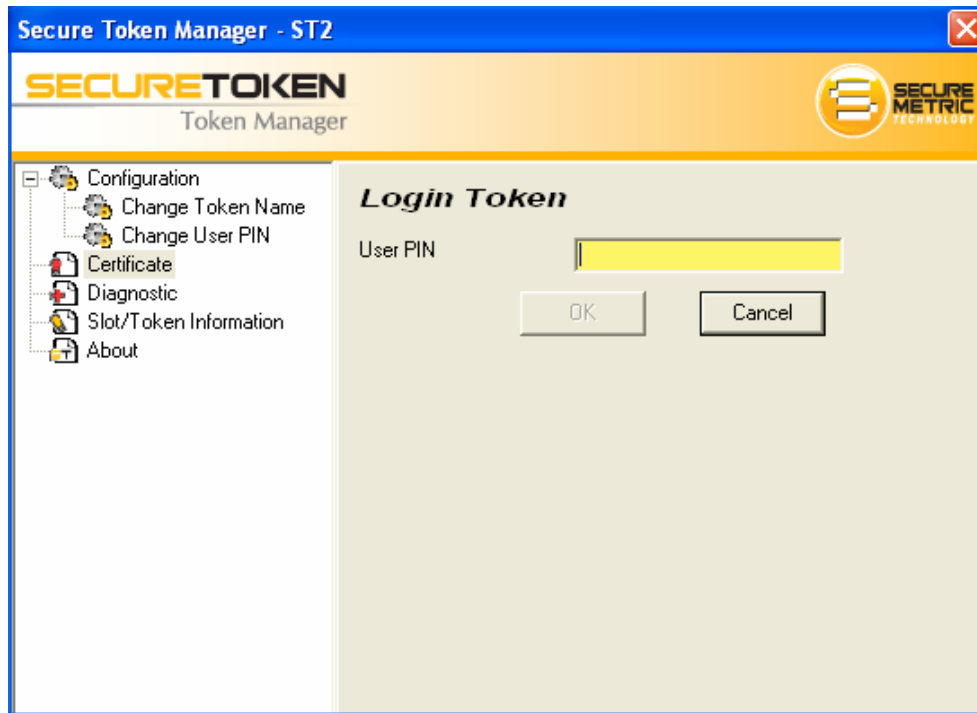


Fig. 1.3

After enter the correct User PIN and press the 'OK' button, the following window (Fig 1.4) appears. The certificate list is displayed on the top. Users can click to select either Certificate or Private Key or Public Key from the tree view to further view the object attributes. To exit, click “Logout” to close the active connection and safely exit.



Fig. 1.4

If users enter wrong PIN, a following dialog box appears to indicate incorrect User PIN (Fig 1.5). Press "OK" to get back to login dialog box in Figure 1.3 and retry login.

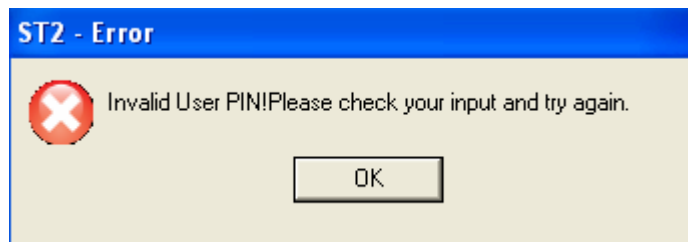


Fig. 1.5

If users enter incorrect User PIN for 2 times, a new error message window will appear like Fig 1.6

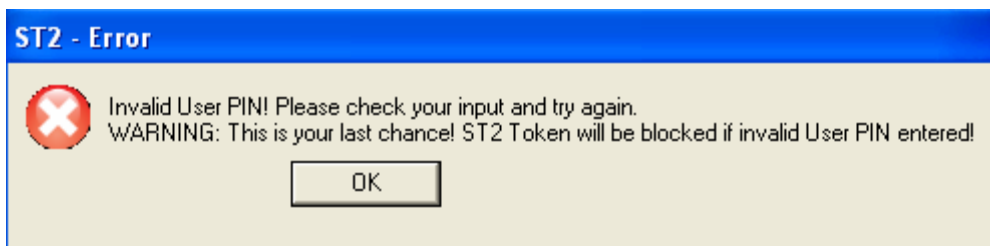


Fig. 1.6

Note: SecureToken ST2 come with the default 3 limited times of incorrect User PIN. If users enter incorrect User PIN for 3 times, SecureToken ST2 will be blocked (as shown by Fig 1.7). For any further operation, users might have to contact the system administrator to unblock it.



Fig. 1.7

1.4 Certificate Management

After Users successfully logged into SecureToken ST2 Manager, Users can perform the provided operations such as Viewing Certificate Information, Importing, and Deleting. Below sections will explain in more details.

1.4.1 Viewing Certificate Information

Certificate manager will display all certificates stored inside SecureToken ST2 token and sorting by same group of certificate, private key and public key. Click “+” sign on the left of any container to expand the treeview menu. After treeview menu has been expanded, Double click on the Object Icon (Certificate, Private Key, and Public Key) to view the attributes of each object.



Fig. 1.8

| Button | Description |
|--------|--|
| View | View particular object attributes in SecureToken ST2 token. For example certificate, private key and public key. |
| Delete | Delete an object in SecureToken ST2 token. For example certificate, private key and public key. |
| Import | Import certificate into SecureToken ST2 token. For example .cer, .der and .p12 certificate type. |
| Logout | Close active connection to SecureToken ST2 token and PIN verification is require during next login. |
| Close | Close Certificate Manger, PIN verification is not required during next time open token manager. |

Click “View” button on the selected Object, below Certificate View dialog box appears.

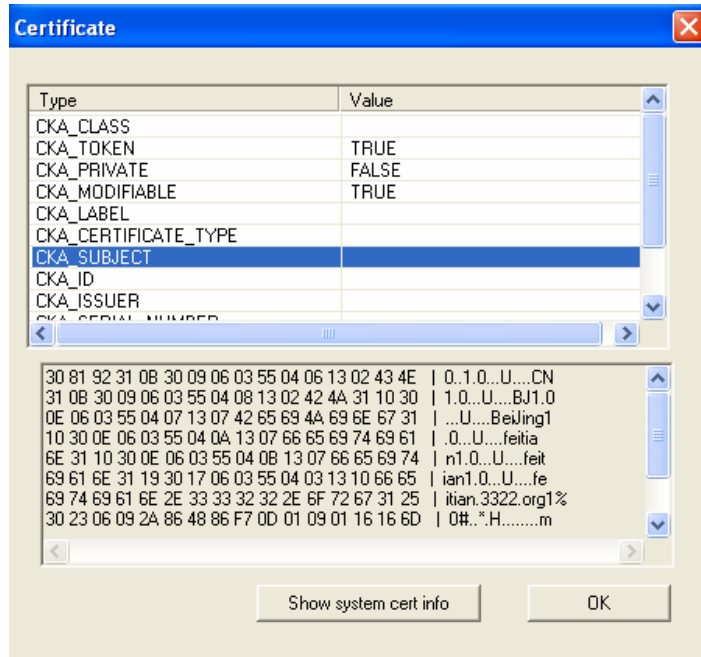


Fig. 1.9

Click “Show system cert info “, a different Certificate View dialog box appears as Fig 1.10. Users can click “General”, “Details” or “Certification Path” to view certificate information.

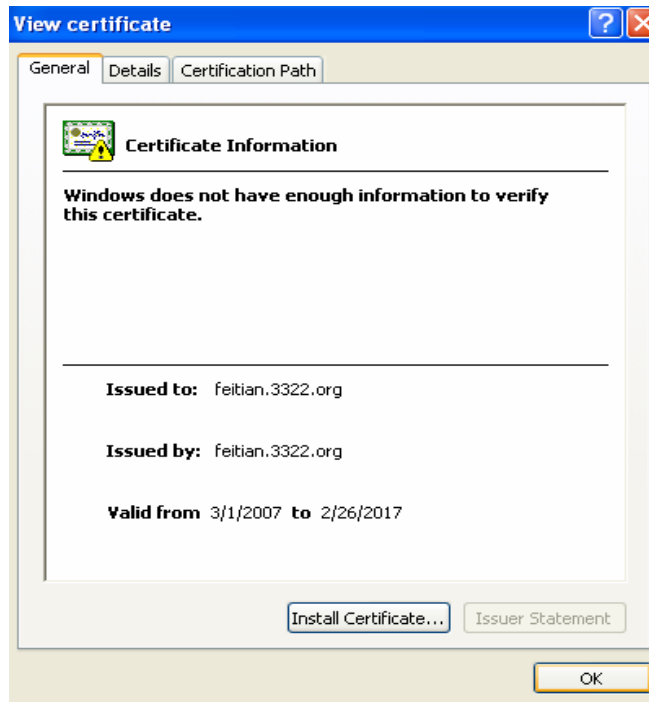


Fig. 1.10

1.5 Change Token Name

Generally, a token is identified by a Hardware ID (HID) which is a globally unique ID pre-burnt into the token chipset during production. HID cannot be changed even by the manufacturer. However, the HID can be difficult to memorize thus it offers another option to Users to set own prefer Token Name as identified. Users can change the Token Name anytime at their own choice.

1. Click “Change Token Name” button in the main window of the Manager. A window will appear like Fig 1.11.

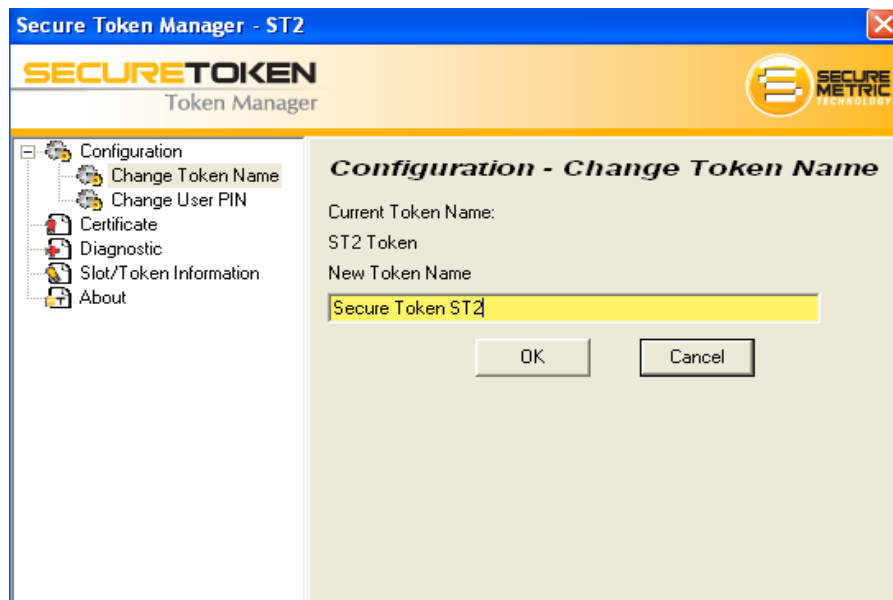


Fig. 1.11

2. Type a new Token Name in the text box, and click “OK”.
3. An information dialog will appear like Fig 1.12 after SecureToken ST2 Token Name changed successfully.

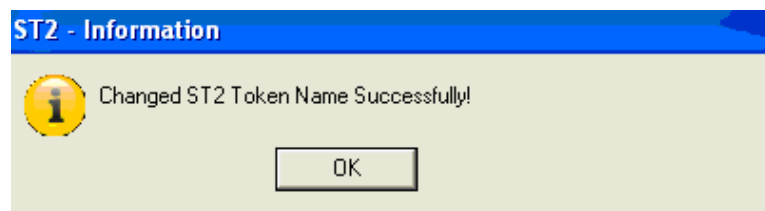


Fig. 1.12

Note: Token name must be less than of 32 characters.

1.6 Change User PIN

User could also change the SecureToken ST2's User PIN by using the Manager tool. Click the "Change User PIN" button in the main window, Change User PIN dialog will appear as Fig 1.13.

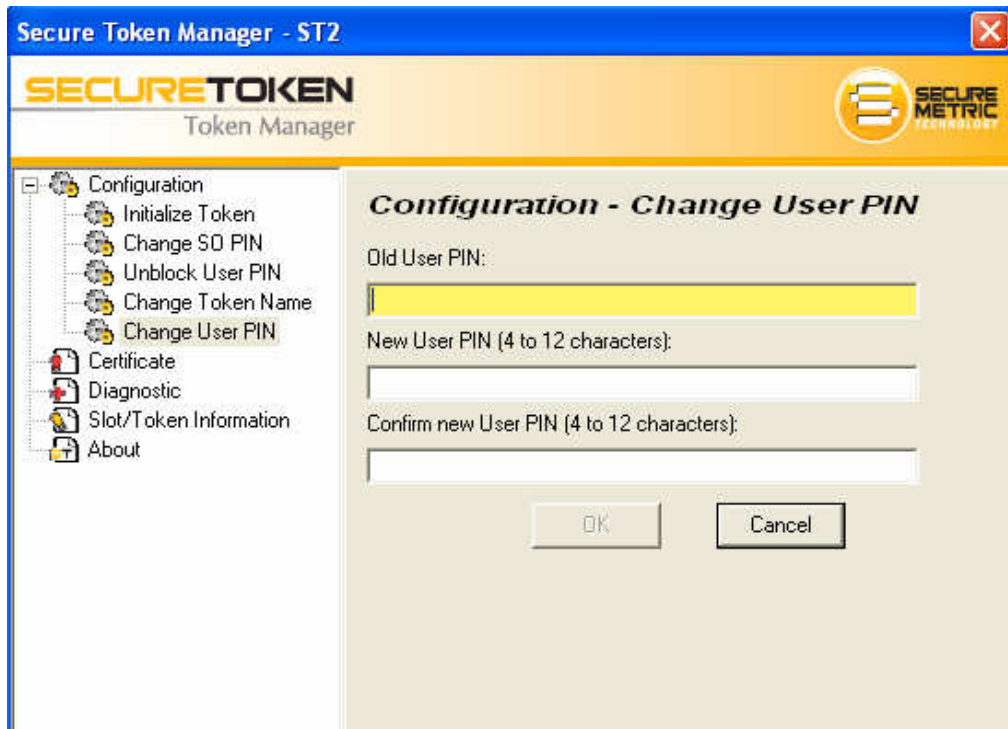


Fig. 1.13

Users require entering correct **Old User PIN**, followed by **New User PIN** and **Confirm new User PIN**. After that, click "OK" button to proceed. If the Change User PIN is done successfully, below notification message window will be shown as Fig 1.14.

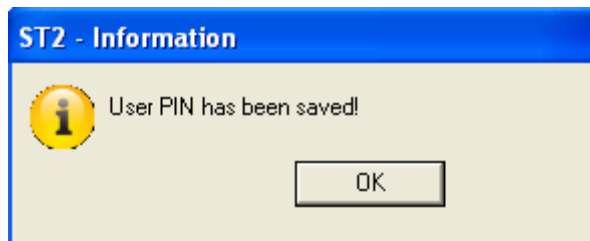


Fig. 1.14

1.7 Diagnostic

Click the “Diagnostic” menu on the left of the SecureToken ST2 Manager, A window will appear like Fig 1.15.

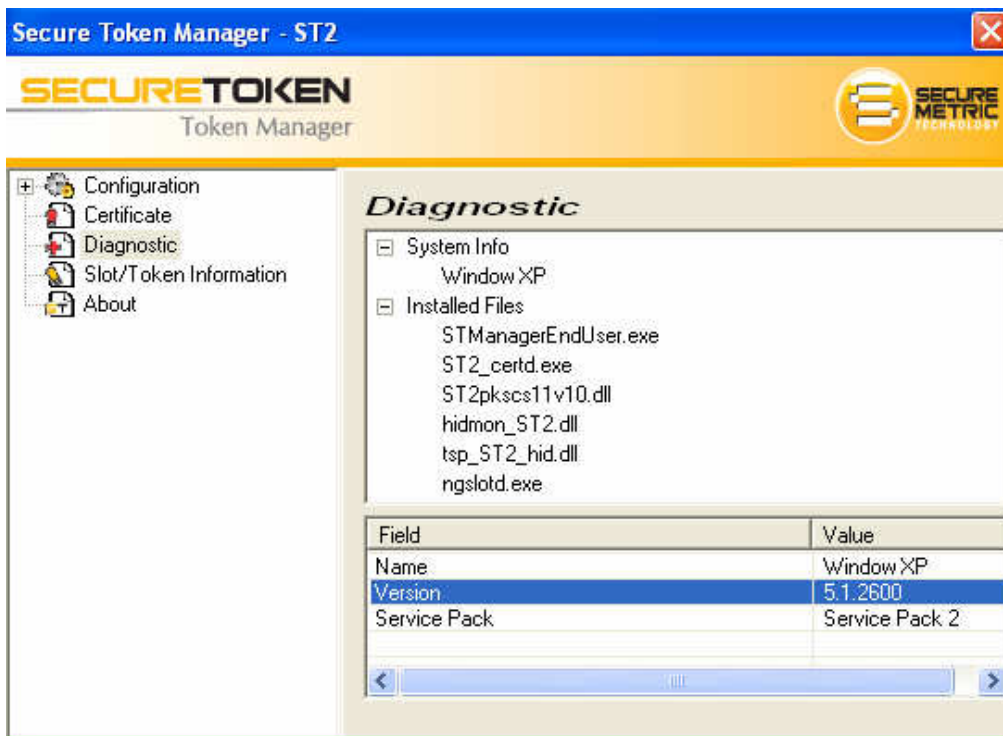


Fig. 1.15

Click “+” sign on the “System Info” menu or double-click the “System Info” menu to display submenus. Double click on the “Window XP” menu and panel below will display “Field” and “Value” attributes.

For example: Name, Version and Service Pack of Microsoft Windows.

Click “+” sign on the “Installed Files” menu or Double click the “Installed Files” menu to display submenus. Double click on the sub menu and panel below will display “Field” and “Value” attributes.

For example is to confirm whether all the needed SecureToken ST2 files have been installed properly.

Note: Details display from Diagnostic will be very helpful for remote technical support at end-user side.

1.8 Slot/Token information

Click the “Slot/Token Information” menu on the left side of the SecureToken ST2 token Manager, A window will appear like Fig 1.16 with Slot and Token information displayed.



Fig. 1.16

1.9 About

Click the “About” menu on the left side of the SecureToken ST2 Manager, the about SecureToken screen will be displayed like Fig 1.17.



Fig 1.17