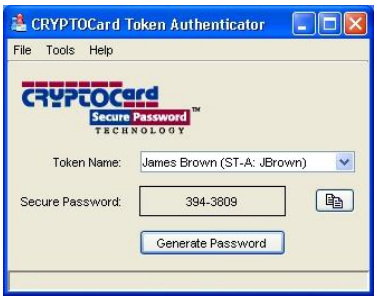
ST-1 Software Token

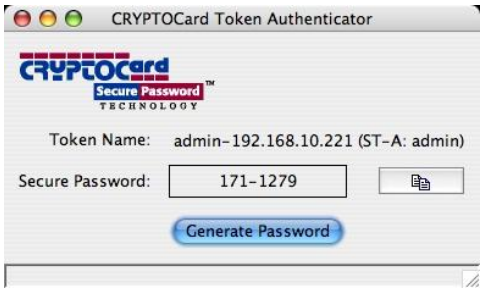
QUICK Reference

Overview

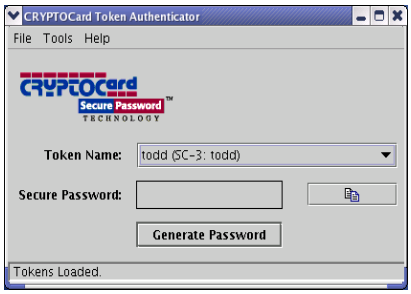
The ST-1 is a software implementation of an authentication token and is designed for installation on Microsoft® Windows®, Linux, and Mac OS X® computing platforms. The ST-1 token generates a new, random "one-time password" each time the token is activated.



ST-1 for Windows



ST-1 for Mac OS X



ST-1 for Linux

The ST-1 can be installed on Windows 2000/2003/XP Professional/Vista/7, RedHat 3.0, 4.0, SuSe 9.0, and Mac OS X systems.

The ST-1 requires the use of a PIN (personal identification number) to operate. Initially this PIN is "1234", and you will change it to a PIN known only to you on first use of the ST-1.

Install the Software Tools on a User's Computer

A program called CRYPTOCard Software Tools must be installed on your computer for you to use ST-1 tokens. This software provides an interface through which you generate one-time passwords from the token.

To install the Software Tools

1. Download the appropriate package (Windows, Linux or Mac) from the Software section of http://cryptocard.com/en/crypto-mas-v10
2. Run the program to install the Software Tools on your computer.
3. The installation wizard will prompt you to select an installation type. Choose "Typical".

The installation adds the following into Windows, Linux, Mac:

- CRYPTOCard Authenticator
- Token Manager

Installing Your ST-1 Token

You will receive your ST-1 software token in an email attachment. Save the attachment (initialization file) to a place on your hard disk. On all operating systems, the initialization file has a .token extension.

Windows and Mac: Double-click on the file to execute it.

Linux: Enter authenticator <token name>.token to execute the file. Alternatively, the token can be initialized using the Token Manager utility's Load Token button.

During installation, you will be asked to supply:

- A "friendly name" that you will use to identify that token (must be unique if you have multiple tokens).
- Your initial PIN ("1234").
- Your user name that you use to log on to your network.

When the installation is complete, the CRYPTOCard Token Authenticator window is displayed and the new token is shown in the Token Name field. The token is now ready for use.

Using the ST-1

To access the ST-1, you run the **CRYPTOCard Authenticator** program on your workstation. Access to the ST-1 requires the user to enter a 3 to 8 character PIN. The PIN is generally unique for each token and known only to the owner of the token. Your initial PIN will be "1234", and you will be prompted to change your PIN the first time you use the token.

Launch the CRYPTOCard Authenticator:

- For Windows, click on the toolbar icon or use:
  Start > All Programs > CRYPTOCard > Authenticator
- For Linux, type **`/usr/bin/./Authenticator.sh`**
- For Mac, click on the Dock icon or use:
  /Applications/CRYPTOCard Software Tool/bin/Authenticator

1. Select the token from the `Token Name` field (if more than one software token is installed) and click `Generate Password`.
2. Enter the PIN.
3. Cut and paste, or transcribe, the one-time passcode into the logon/password dialog of the application/entity interface you are authenticating against.

Changing Your PIN

You can change the PIN at any time, within the established security policy parameters.

1. Launch the CRYPTOCard Authenticator.
2. Select **Tools > Change PIN** from the toolbar.
3. Enter the current PIN, new PIN, and new PIN confirmation. Click OK.

Locked Token Removal

The purpose of this section is to instruct end-users and administrators how to remove a locked ST-1 token should too many incorrect PIN"s be entered into the Token Authenticator.

Go to the Control Panel and open up the 'Token Manager' application.

Highlight the token that is locked and click on 'Remove Token…'. You will be asked 'Do you really want to remove token – xxxx?. Select 'Yes'.

Follow the instructions above 'Installing Your ST-1 Token' when you receive a new token from the Administrator.

Token Resync

The purpose of this section is to instruct end-users and administrators how to resynchronize tokens using the on-line CRYPTO-MAS resynchronization tool.

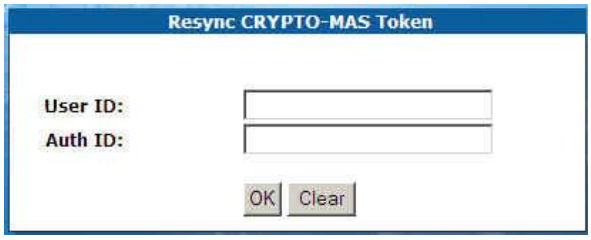
If too many One-time password Codes (OTP's) have been generated by a token since the last time the server received a correct OTP, the server will not recognize the OTP and the token and server are said to be "out of sync".

For CRYPTO-MAS, the number of OTPs that needs to be generated by the token to cause the server and the token to become out-of-sync is defaulted to 25.

Instructions

IMPORTANT: Please ensure that the user has only one token assigned to them. An 'Access Denied' message will appear if the user has multiple tokens.

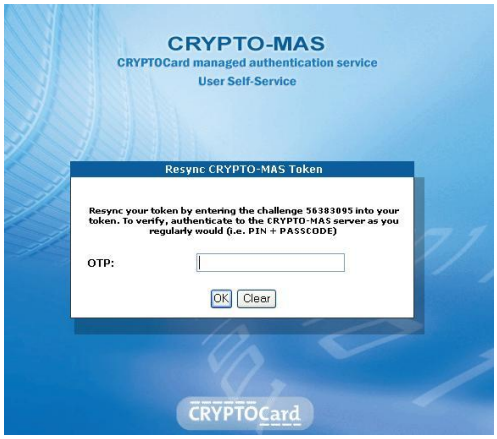
Step 1:
Open up a browser (IE6, IE7, Mozilla Firefox 1.5+) and go to http://resync.cryptocard.com/. The following dialog box will appear:



Step 2:
Enter the "User ID" and "Authentication ID" (Auth ID) and click OK.

Contact your MAS Administrator if you don't know the "Authentication ID'.

Step 3:
You will be presented with a challenge to be entered into your token, along with a field to enter your next OTP (after the resync process has been completed) (see below for instructions on entering a challenge into your token).



Enter your OTP displayed on your token and Click "OK".

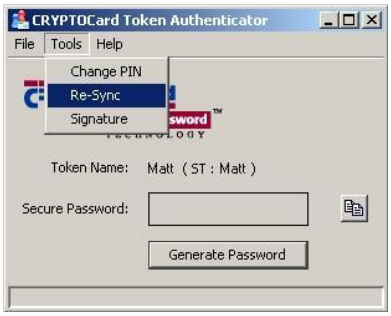
Your token should now be synchronized with the server.

Entering a Challenge into an ST-1 Token:

1. Open up the Token Authenticator on your PC by following these steps:
   - Go to "Start" in their Windows environment
   - Click "All Programs"
   - Click "CRYPTOCard"
   - Click "CRYPTOCard Authenticator"

2. A "CRYPTOCard Token Authenticator" window will appear on the User's terminal.

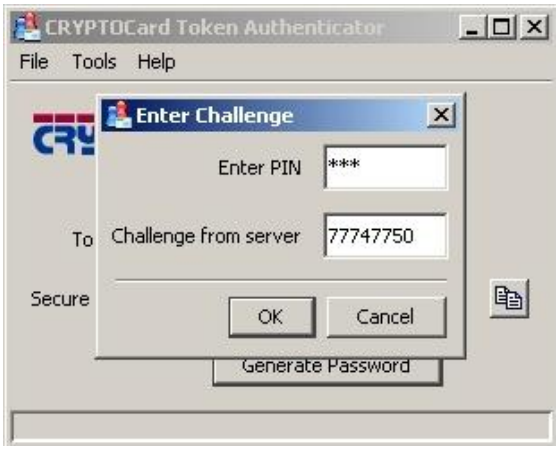
   In the new window, click on "**Tools**" > "**Re-Sync**".



3. An "Enter Challenge" window will then appear on the User's terminal.

   The User must then enter their PIN in the "Enter PIN" field, and the challenge number that was displayed in Step 3 above into the "Challenge from server" field.

   Click OK, and a new Secure Password ('response') will be generated.



MAS Token Template

The following table identifies the ST-1 token configuration:

MAS Token Attributes - ST-1	
Display	
Display Type	Base 32
Telephone Mode	No
Response Length	8 characters
Automatic Shut-off	N/A
PIN	
PIN Style	User-changeable PIN
Initial PIN	1234
Random PIN Length	4
Min PIN Length	3
Characters allowed	Digit only
Try Attempts	7
Allow Trivial PINs	Yes
Operation	
Mode	Quicklog
Passwords per power cycle	Single
User can turn token off	N/A
Usage	**Usage**
Operational Flags	Force PIN change on next use