CRYPTO-Server™

6.x

Smart Tokens

SC-1 Smart Card Token

QUICK Reference
# Table of Contents

OVERVIEW...................................................................................................................1
OPERATING MODES & OPTIONS..................................................................................2
USING THE SC-1...........................................................................................................6
    Generating a passcode (QuickLog™ mode) ............................................................6
    Using Manual Mode Authentication .......................................................................6
    Generating a passcode (Challenge-response mode) ................................................7
    User-changeable PIN .............................................................................................7
GENERATING DIGITAL SIGNATURES ............................................................................8
PASSWORD RESYNCHRONIZATION .............................................................................9
REMOVING SC-1 TOKEN(S) .......................................................................................9
HID/MiFare PROXIMITY DOOR ACCESS .................................................................10
PHOTO ID AND CUSTOM GRAPHICS .......................................................................10
LOADING CERTIFICATE(S) ON A SMART CARD (SCR331 USB SMART CARD) ..........12
    Section 1a .............................................................................................................12
    Section 1b .............................................................................................................13
Overview

The SC-1 token is an implementation of the CRYPTOCard software token on a Gemalto 64k V2 Cyberflex Java Smart Card with Prox HID access, and is designed for use with Windows 2000/2003/XP Professional, RHEL 3/4 and Mac OS X Tiger systems. The tokens can be used with CRYPTOCard PCCard (PCMCIA), external USB card readers, or third-party ISO 7816 compliant readers.

The SC-1 token generates a new, pseudo-random passcode each time the token is activated. An SC-1 PIN consists of a string of 3 to 8 alphanumeric characters that is used to guard against unauthorized use. If PIN protection is enabled, the user must provide a PIN with the one-time passcode to authenticate.

Multiple tokens, each protected by their own unique PIN, may reside on a single SC-1 token. The SC-1 can also store digital certificates (PKCS11) generated by third-party PKI products.

SC-1 tokens can support a combination of QUICKLog™ password, challenge-response password, and digital signature functions.

When CRYPTO-Logon for Microsoft Windows or CRYPTO-Logon for Mac OS X is deployed, the following actions can be tied to removal of the SC-1 from the reader or activation of a screen saver:

- Lock the keyboard, with unlock restricted to the locking user
- Lock keyboard, with unlock restricted to valid SC-1 card holders
- Log the user off (SC-1 removal only)
Operating Modes & Options

The SC-1 supports a wide range of operating modes that can be modified using the CRYPTO-Console GUI, according to organizational and security policy requirements. A brief list of the more common operating modes follows. Refer to the CRYPTO-Server Administrator Guide for a complete list of modes and options.

Display Type:

- **Hexadecimal**: token generates passcodes comprised of digits and letters from 0–9 and A–F.
- **Decimal**: token generates passcodes comprised of digits from 0–9.
- **Base32**: token generates passcodes comprised of digits and letters from 0–9 and A–Z.
- **Base64**: token generates passcodes comprised of digits and letters from 0–9 and Aa–Zz, as well as other printable characters available via Shift + 0–9.

Telephone mode:

- **Yes**: replaces the fourth character of a passcode with a dash (–). This is generally used in combination with **Response length**: 8 characters and **Display type**: Decimal to resemble the North American telephone number format.
- **No**: passcode is displayed as set by Response length and Display type.

Response Length:

- Determines the passcode length. Options are 5, 6, 7, or 8 characters.

PIN Style:

- **Fixed PIN**: the PIN created for the token at the time of initialization is permanent and cannot be modified by the user or operator. Fixed PIN can only be changed by re-initializing the token after selecting a new PIN value through this tab. This PIN must be entered into the token before a passcode is displayed.
- **User-changeable PIN**: the user may change the PIN at any time. The initial PIN set during initialization must be changed by the user on first use of the token. This PIN must be entered into the token before a passcode is displayed. The PIN value selected by the user must be within the limits set under the Min PIN Length, Characters allowed, Try Attempts, and Allow Trivial PINs options.
Initial PIN:

- The initial PIN value required for the token. The value is permanent if Fixed PIN is selected as the PIN Style. This value must be changed on first use of the token for User-changeable PIN. Use the Randomize button to change the initial value to a random number within the limits set under the Random PIN Length, Min PIN Length, and Characters allowed options.

Note that the minimum initial PIN length can be longer than the minimum PIN length required by the user.

Random PIN Length:

- The minimum PIN length generated when clicking the Randomize button. The valid range is 3–8 characters.

Minimum PIN Length:

- The minimum PIN length required to authenticate. The valid range is 1–8 characters.

Characters allowed:

- Digits only: permits the digits 0–9 in the PIN.
- Alpha-numeric: permits the digits 0–9 and the characters Aa–Zz in the PIN.
- Strong Alpha-numeric: requires at least one uppercase character, one lowercase character, and one digit in the PIN.

This setting is affected by the Allow Trivial PINs option.

Try Attempts:

- Number of consecutive incorrect PIN attempts permitted. The valid range is 1–7 attempts.

If this value is exceeded, the token will be locked and will not generate passcodes until it is re-initialized.
Allow Trivial PINs:

- **No**: prevents the use of sequences or consecutive digits/characters longer than 2. For example, 124 is permitted; 123 is not permitted.
- **Yes**: no sequence checking. For example, 123 is permitted.

Mode:

- **QUICKLog**: passcode is displayed immediately by token (or after Display Name, if this option is enabled on the Display tab).
- **Challenge-response**: requires the user to key a numeric challenge into the token before a response is generated.

*QUICKLog™* is the recommended mode for all token types.

Algorithm:

- **Mk 2 Algorithm**: supports DES. This mode is automatically selected for CRYPTO-Server 6.x SC-3 tokens (serial numbers beginning with 91).

Start date:

- The first date, in yyyymmdd format, that the token may be used to authenticate.

Expiry date:

- The last date, in yyyymmdd format, that the token may be used to authenticate.

When an operator changes the Expiry date, the change immediately becomes active on the server and valid for the affected token. This is often used for periodic access typical of contractors. It permits the token to be issued once, while ensuring that the user can only authenticate with an active token during the set periods.

Operational Flags:

- **Force PIN change on next use**: For SC-1 tokens, this flag is only valid for Initial PINs (i.e. PIN change after token initialization) and the flag is not cleared on PIN change.
Property Flags:

- **Delete token at expiry**: On expiry, this token is automatically removed from inventory, if checked.

- **Don’t change key at initialization**: the encryption key used for this token is reused during re-initialization, if checked. It is recommended that this box remain clear to ensure that keys are changed with every initialization.

Usage Flags:

- **Authentication enabled**: token can be used to authenticate, if checked.

- **Signature enabled**: token can be used to generate digital signatures, if checked.
Using the SC-1

Access to the SC-1 authentication and digital signature functions 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.

Generating a passcode (QuickLog™ mode)

The SC-1 automates authentication when used in conjunction with CRYPTOCard agents or compatible third-party plug-ins. The user simply enters his PIN and clicks OK when prompted and the SC-1 completes the authentication.

Using Manual Mode Authentication

In instances where a user is attempting to connect to a network entity or Web asset for which a CRYPTOCard agent or third-party plug-in does not exist, there is no automated means by which the Token Authenticator software can furnish the one-time password to the entity/asset for authentication. Therefore, SC-1 tokens enable the user to generate a one-time passcode that can then be entered manually when the user is prompted for a password by the application/entity interface.

1. Launch the Token Authenticator:
   - For Windows, click on the toolbar icon or use Start > Programs > CRYPTOCard Authenticator.
   - For Linux, type /user/bin/authenticator.
   - For Mac, click on the Dock icon or use Applications > CRYPTOCard > bin > Authenticator.

2. Select the token from the Token Name field (if more than one software token is installed) and click Generate Password.

3. Enter the PIN.

4. Cut and paste, or transcribe, the one-time passcode into the logon/password dialog of the application/entity interface you are authenticating against.
Generating a passcode (Challenge-response mode)

QuickLog™ is the recommended mode for all CRYPTOCard tokens. Challenge-response mode should only be used if required.

1. Launch the Token Authenticator:
   - For Windows, click on the toolbar icon or use Start > Programs > CRYPTOCard Authenticator.
   - For Linux, type /user/bin/authenticator.
   - For Mac, click on the Dock icon or use Applications > CRYPTOCard > bin > Authenticator.

2. When you attempt to log in to the application or entity interface, you will receive an 8-digit challenge.

3. Click Generate Password on the Token Authenticator dialog window.

4. Enter the PIN and 8-digit challenge. A response will be displayed.

5. Cut and paste, or transcribe, the response into the application or entity interface logon dialog.

User-changeable PIN

If the SC-1 token is configured with a PIN Style of User-changeable PIN, the user will be forced to change the initial deployment PIN on first use. Thereafter, the user can change the PIN at any time, within the established security policy parameters.

1. Launch the Token Authenticator:
   - For Windows, click on the toolbar icon or use Start > Programs > CRYPTOCard Authenticator.
   - For Linux, type /user/bin/authenticator.
   - For Mac, click on the Dock icon or use Applications > CRYPTOCard > bin > Authenticator.

2. Select Tools > Change PIN from the toolbar.

3. Enter the current PIN, new PIN, and new PIN confirmation. Click OK.
Generating Digital Signatures

SC-1 tokens are able to generate digital signatures:

1. Launch the Token Authenticator:
   - For Windows, click on the toolbar icon or use Start > Programs > CRYPTOCard Authenticator.
   - For Linux, type /user/bin/authenticator.
   - For Mac, click on the Dock icon or use Applications > CRYPTOCard > bin > Authenticator.

2. Select Tools > Signature from the toolbar.

3. Enter your PIN and the input data (i.e. the form hash/challenge) generated by the document to be signed.

4. Cut and paste, or transcribe, the digital signature that is displayed into the application/document.
Password Resynchronization

Token resynchronization may be required if the user has generated a large number of passcodes without logging on (authenticating). Token resynchronization requires the user to enter a “challenge” into the token. The challenge must be provided by the Help Desk or via a Web-based resynchronization page. In the unlikely event that the token requires resynchronization with the authentication server:

1. Launch the Token Authenticator:
   - For Windows, click on the toolbar icon or use Start > Programs > CRYPTOCard Authenticator.
   - For Linux, type /user/bin/authenticator.
   - For Mac, click on the Dock icon or use Applications > CRYPTOCard > bin > Authenticator.

2. Select Tools > Re-sync from the toolbar.

3. Enter your PIN and the resynchronization challenge.

Removing SC-1 Token(s)

Please ensure that the Smart Card is plugged into the smart card reader first, and see section 3.10 of the CRYPTO-Server 6.4 Administrator Manual on how to remove SC-1 Tokens from the CRYPTOCard Authenticator.
HID/Mifare Proximity Door Access

HID/Mifare proximity access technology is embedded in each SC-1 token. The HID format is type number H10301, the 26-bit 125 kHz open format that is widely used, especially in legacy systems. CRYPTOCard can provide cards in this format with any 8-bit Facility Code and any 16-bit User ID Number.

The 13.56 MHz MiFare includes 1 kB of memory, a unique 32-bit fixed serial number, and 16-sector multi-application memory.

There is no link between the smart card chip embedded in the card and the circuitry that provides proximity door access. Nor does CRYPTO-Server manage the HID/Mifare portion of the card. HID/Mifare programming or access control panel association must be handled by the existing door system.
Photo ID and Custom Graphics

Direct image printing using dye sublimation or direct image transfer printing can be done by CRYPTOCard, the customer, or third parties. There are no restrictions on the graphics that can be applied to the front face of the card within the printable area (shown below).

The card may be slot punched along the horizontal or vertical edges to accommodate clips.
Loading Certificate(s) on a Smart Card (SCR331 USB Smart Card)

This section is split into 2. Section 1a explains how to initialize a container and load a token onto the Smart Card Chip. Section 1b explains how to use the Cryptographic Object Viewer and Editor (COVE) to format the remaining space on the Smart Card Chip so a certificate can be loaded on.

Section 1a

To initialize a container on the Gemalto Smart Card, go to Control Panel > Token Manager

Click on Options > Container Manager

Highlight the “SCM Microsystems Inc. SCR331 USB Smart Card Reader 0” and select “Initialize Container”

If the container is initialized properly, the output at the bottom of the window should be displayed as follows.

```
Container initialization complete.
```
Highlight the “SCM Microsystems Inc. SCR331 USB Smart Card Reader 0” and then click on “Container Information”

If the container is initialized successfully then it should say “Container is available for normal use”. Unplug and plug the Gemalto token back in to make sure it re-detects properly.

Launch the CRYPTO-Console, and log in. Assign a token to a user and select an SC-3 Token from the list of tokens that are available and initialize it locally.

Section 1b

Launch the COVE Admin tools.

Click on the dropdown menu and select the the “SCM Microsystems Inc. SCR331 USB Smart Card Reader 0” and click the “Connect” button.
Click on the “Personalize” tab

Browse to the Cove directory on the left pane. Select the desired cpf in the list on the right pane, or you could import a cpf that has already been created with the “New” button.

Set the User PIN and Unblock PIN or you could leave it default.

Click the “Select Keys” button and select the default COVE.ksf file.

Select the Cyberflex Access 64k in the list.

Once that is done, click on the “Personalize” button to have it create the PKI applet and load the correct files.

Once it has finished personalizing the Smart Card Chip, Disconnect and Re-Connect to the “Gemplus USB Key Smart Card Reader 0”. It will ask you the PIN to gain access to the Smart Card.

Click on the “Card tab” and you will see the following:
Open up a browser and navigate to your CA server. Select “Request a certificate”

Click on “Advanced certificate request”

Select “Create and submit a request to this CA”

For the purpose of this document I have select the following:
Certificate Template – Select “Smartcard Logon”
CSP – Select “Axalto Cryptographic Service Provider”
Request Format – Select “PKCS10”

Once that is all selected, click “Submit”. It should then prompt you to enter your PIN (The PIN that was entered in COVE to access the Smart Card)

On the next screen, click “Install this certificate”

The message that is displayed at the last step should be “Your new certificate has been successfully installed”

To verify if the Certificate has been installed, log back into COVE and click on the “Card” tab again.