BlackShield ID MP Token Guide

for Java Enabled Phones

Copyright © 2010 CRYPTOCard Inc.

Trademarks

CRYPTOCard and the CRYPTOCard logo are registered trademarks of CRYPTOCard Corp. in the Canada and/or other countries. All other goods and/or services mentioned are trademarks of their respective companies.

License agreement

This software and the associated documentation are proprietary and confidential to CRYPTOCard, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by CRYPTOCard.

Third-party licenses

This product may include software developed by parties other than CRYPTOCard. The text of the license agreements applicable to third-party software in this product may be viewed in the \\CRYPTOCard\BlackShield ID\Open Source Licenses folder of a default BlackShield ID installation.

Note on encryption technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Contact Information

CRYPTOCard's technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

CRYPTOCard works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your partner directly for support needs.

To contact CRYPTOCard directly:

International Voice: +1-613-599-2441

North America Toll Free: 1-800-307-7042

Email: support@cryptocard.com

For information about obtaining a support contract, see our Support Web page at http://www.cryptocard.com.

Go to the CRYPTOCard corporate web site for regional Customer Support telephone and fax numbers: http://www.cryptocard.com

Publication History

Date	Changes
January 27, 2010	Initial release

Table of Contents

Overview

Security Administrators can transform Java ME mobile phones into tokens that will generate PIN protected one-time passwords valid for strong authentication at VPNs, Web applications, Citrix and any other BlackShield ID protected on-line resources.

The MP software token provides the advantages of AES-256 bit encryption-based hardware tokens without the associated cost and distribution issues. As an application installed on the mobile device it provides a viable alternative for organizations that do not want to rely on the availability of an SMS network for secure delivery of One-time passcodes.

Applicability

Summary		
Authentication Server	BlackShield ID	
Version	2.6.392 or higher	
Supported Java Phones	DLDC 1.1 or higher MICP 2.0 or higher	
Supported Token PIN Mode	No PIN Fixed PIN User selected PIN	Server-side Fixed Server-side User Select
Supported Token Code Complexity	Decimal Hexadecimal	Base32 Base64

Note: Multiple MP tokens cannot be installed in the same Java enabled phone.

Preparation and Prerequisites

1. BlackShield ID must be licensed for MP token capacity.
2. Users receiving an MP token for their Java phones must have a valid email address and mobile phone number defined within BlackShield ID.
3. The Mail Settings section within the System Admin tab of the BlackShield ID Manager must be configured and operational. Refer to the BlackShield ID Administrator's Guide for additional information.
4. The Self-enrollment section within the System Admin tab of the BlackShield ID Manager must be configured and operational. Refer to the BlackShield ID Administrator's Guide for additional information.
5. Depending on the deployment method, the BlackShield Self-enrollment site must be externally accessible to Java phones.
6. Depending on the deployment method, the SMS Settings section within the System Admin tab of the BlackShield ID Manager must be configured and operational.

MP Token Deployment methods

BlackShield ID supports two MP token deployment methods for Java enabled phones:

- Over-the Air (OTA) installation of the BlackShield Java ME Authenticator and MP Token file via the BlackShield ID Self-enrollment website.
- Desktop Suite installation of the BlackShield Java ME Authenticator and MP Token file using a third party vendor's installation tool.

Configuration

Over-The Air (OTA) method

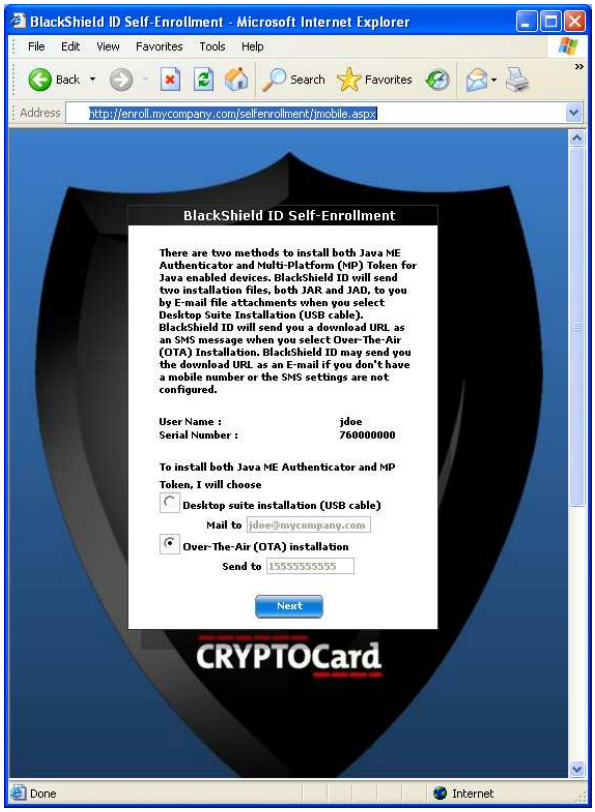
1. In the BlackShield ID Manager browse to the Assignment tab, create an MP token, find a user then select the Self-Enroll button or create an MP token Auto-Provisioning rule for a specific LDAP group with in System Admin Tab.

2. The user will receive a self-enrollment email directing them to the BlackShield ID Self-enrollment website.

> John Doe:
> Your self-enrollment account has been created.
> To activate your token, you will need the following:
>
> 1. User Name: jdoe
> 2. Token serial number: 760000000
> 3. Activation code: 93286288290946061171
>
> Please, go to the following URL to activate your token:
>
> http://enroll.mycompany.com/selfenrollment/index.aspx?user=amRvZQ==&serial=NzYwMD
>
> AwMDA3&code=OTMyODYyODgyOTA5NDYwNjExNzE=&date=2/4/2010
>
> If the above link does not work, please copy and paste this url to your web browser.

3. User selects **Java Enabled Phone** (installation options visible to the user can be customized).

4. User selects **Over-The Air (OTA)** installation. Depending on the settings within the BlackShield server, the user may modify their mobile number otherwise a predetermined mobile number is displayed on the web page.



5. User receives an SMS message on their mobile phone, which contains their **Initial PIN** and a **Download URL**.
6. User browses to the URL on their Java phone and is prompted to download and install the BlackShield Java ME Authenticator.
7. User launches the BlackShield Java ME Authenticator, enters their **Initial PIN** then prompted to **change their PIN**.
8. User logs on to the CRYPTOCard protected resource using the **Token Code** generated by their mobile phone.

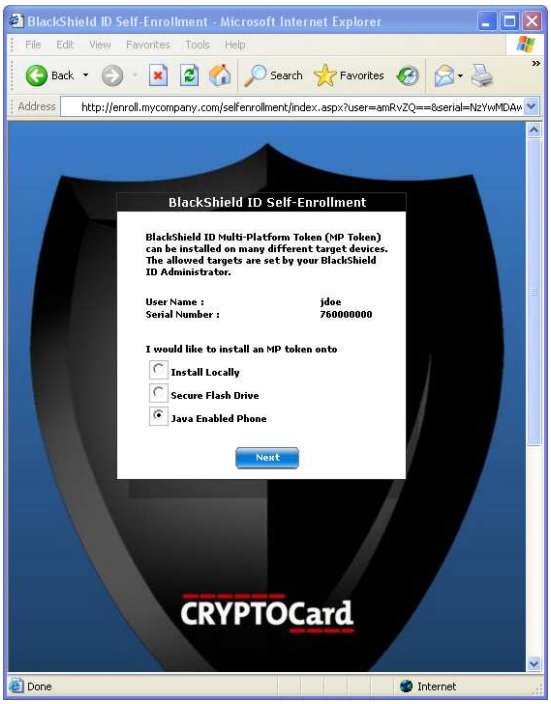
Desktop Suite method

1. The BlackShield Administrator creates an MP token, finds a user, selects the Self-Enroll button or creates an MP token Auto-Provisioning rule for a specific LDAP group.

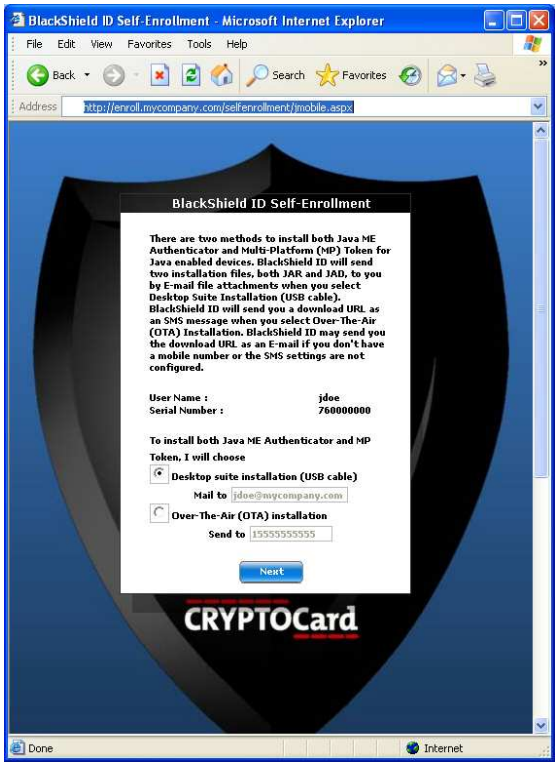
2. The user receives a self-enrollment email directing them to the BlackShield ID Self-enrollment website.

> John Doe:
> Your self-enrollment account has been created.
> To activate your token, you will need the following:
>
> 1. User Name: jdoe
> 2. Token serial number: 760000000
> 3. Activation code: 93286288290946061171
>
> Please, go to the following URL to activate your token:
>
> http://enroll.mycompany.com/selfenrollment/index.aspx?user=amRvZQ==&serial=NzYwMD
> AwMDA3&code=OTMyODYyODgyOTA5NDYwNjExNzE=&date=2/4/2010
>
> If the above link does not work, please copy and paste this url to your web browser.

3. User selects **Java Enabled Phone** (installation options visible to the user can be customized).



4. User selects **Desktop Suite Installation (USB)**. Depending on the settings within the BlackShield server, the user may modify their email address otherwise a predetermined email address is displayed on the web page.



5. User receives an email, which contains their **Initial PIN**, the BlackShield Java ME Authenticator application files and various links to third party vendor mobile phone installation tools.
6. User installs the BlackShield Java ME Authenticator using the third party mobile phone installation tool.
7. User launches the BlackShield Java ME Authenticator, enters their **Initial PIN** then prompted to **change their PIN**.
8. User logs on to the CRYPTOCard protected resource using the **Token Code** generated by their mobile phone.

Using the MP Token a Java Enabled Phone

Generating a Token Code (QuickLog™ mode)

MP tokens enable the user to generate a one-time Token Code that can then be entered manually when the user is prompted for a password by a CRYPTOCard protected resource.

1. On the Java enabled phone, launch the **Authenticator** application.
2. Enter the **PIN** (if required).
3. Enter the one-time **Token Code** into the logon/password dialog of the CRYPTOCard protected resource you are authenticating against.

Generating a Token Code (Challenge-response mode)

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

1. On the Java enabled phone, launch the **Authenticator** application.
2. When you attempt to log in to the CRYPTOCard protected resource, you will receive an 8-digit challenge.
3. Click **Generate Token Code** on the Authenticator dialog window.
4. Enter the **PIN** and 8-digit challenge. A **Token Code** will be displayed.
5. Enter the one-time **Token Code** into the logon/password dialog of the CRYPTOCard protected resource you are authenticating against.

User-changeable PIN

If the MP token is configured with a PIN Style of **User Select 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. On the Java enabled phone, launch the **Authenticator** application.
2. Select **Tools|Change PIN**.

3. Enter the **Current PIN**, **New PIN**, and **Verify new PIN**.

Token Code Resynchronization

Token resynchronization may be required if the user has generated a large number of token codes 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. On the Java enabled phone, launch the **Authenticator** application.
2. Select **Tools|Resync Token**.
3. Enter your **PIN** and the resynchronization **Challenge**.
4. Enter the one-time **Token Code** into the logon/password dialog of the CRYPTOCard protected resource you are authenticating against.

Unlock Token (Remote Unlock)

If the Max PIN Attempts threshold is exceeded, an MP token will enter a 'Locked' state and cannot be used for authentication. The Unlock Token option allows for a token to be enabled without having to redeploy the token file to the user.

1. On the Java enabled phone, launch the **Authenticator** application**.**
2. Select **Tools|Unlock Token**.
3. Provide the **Unlock Challenge** to the CRYPTOCard Administrator then enter the **Server Response** provided to you.
4. Enter the **New PIN**, and **Verify new PIN**.
5. A Token Unlocked message will appear. The MP token may now be used to generated Token Codes.

Customizing Email and Self-Enrollment messages

The email templates and text used during Self-Enrollment can be found in the \Program Files\CRYPTOCard\BlackShield ID\Languages\en directory.

The **JavaMEOTA.emt** template file contains the first name, last name, message body, Initial PIN and Download URL sent to the user when Over-The Air (OTA) installation is selected during enrollment.

The **JavaMEUSB.emt** template file contains the first name, last name, message body, Initial PIN and Download URL sent to the user when Desktop Suite installation is selected during enrollment.

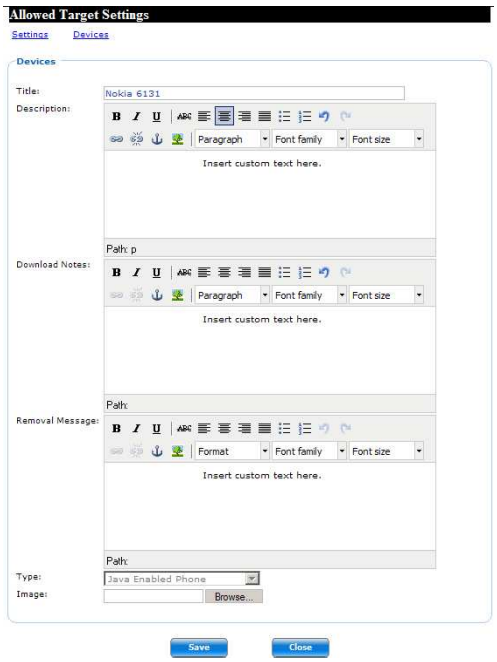
The **selfEnrollment.ccl** file displays the Self-Enrollment text that appears on the web site during Java phone enrollment. The text can be modified and will take effect when the IIS Admin Service is restarted.

Any information contained with < /> is dynamically generated by the BlackShield server and should not be modified.

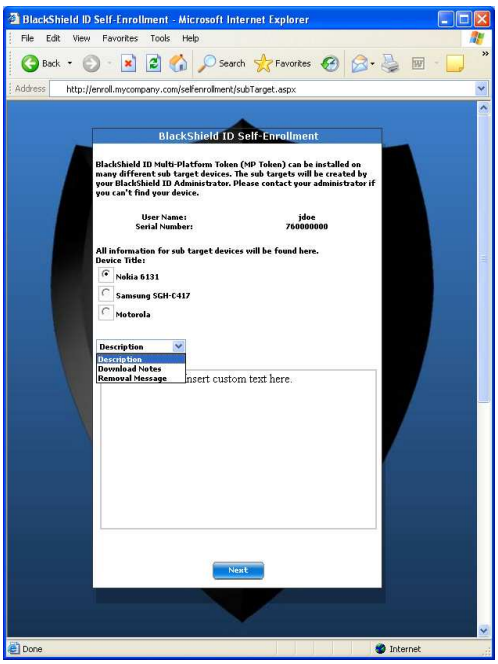
For more information on the customization of Self-enrollment, default BlackShield email templates and SMS messages; please refer to the BlackShield Administrators Guide.

Customizing Self-enrollment instructions for specific Java Phones

The BlackShield Server can provide a list of custom Self-enrollment instructions for specific Java Phones. A dropdown can appear during Self-enrollment and display multiple Java Phone types or vendors. Selecting an entry from the dropdown list will display custom messages to the users.



Policy Admin – Allowed Targets



BlackShield Self-Enrollment Web Site

For more in-depth information, please refer to the BlackShield Administrators Guide.