BlackShield Authentication Service

Guide for

Users of CRYPTOCard MP-1 Software Tokens on Smart Phones

Protecting Your On-line Identity

Authentication Service Delivery Made EASY™
Copyright

Copyright © 2011. CRYPTOCard Inc. All rights reserved. The information contained herein is subject to change without notice. Proprietary Information of CRYPTOCard Inc.

Disclaimer

The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than CRYPTOCard Inc. While every effort is made to ensure the accuracy of content offered on these pages, CRYPTOCard Inc. shall have no liability for errors, omissions or inadequacies in the content contained herein or for interpretations thereof.

Use of this information constitutes acceptance for use in an “AS IS” condition, without warranties of any kind, and any use of this information is at the user’s own risk.

No part of this documentation may be reproduced without the prior written permission of the copyright owner. CRYPTOCard Inc. disclaims all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall CRYPTOCard Inc. be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if CRYPTOCard Inc. has been advised of the possibility of such damages. Some provinces, states or countries do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents CRYPTOCard Inc. from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behaviour to support@cryptocard.com.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of the license.

Trademarks

BlackShield ID, BlackShield Cloud, BlackShield Server, CRYPTOCard and the CRYPTOCard logo are trademarks and/or registered trademarks of CRYPTOCard Inc. in Canada and/or other countries. All other goods and/or services mentioned are trademarks of their respective holders.
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:

<table>
<thead>
<tr>
<th>United Kingdom</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td>Venture House, Downshire Way</td>
<td>600-340 March Road, Kanata, Ontario, Canada K2K 2E4</td>
</tr>
<tr>
<td>Arlington Square, Bracknell</td>
<td></td>
</tr>
<tr>
<td>RG12 1WA</td>
<td></td>
</tr>
<tr>
<td>Freephone: 0800 694 1000 (UK)</td>
<td>Toll Free: 800-307-7042</td>
</tr>
<tr>
<td>Phone: +44 870 7077 700</td>
<td>Phone: +1 613 599 2441</td>
</tr>
<tr>
<td>Fax: +44 870 70770711</td>
<td>Fax: +1 613 599 2442</td>
</tr>
<tr>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
<td><a href="mailto:support@cryptocard.com">support@cryptocard.com</a></td>
</tr>
</tbody>
</table>

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

Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011.06.01</td>
<td>Initial release</td>
<td>1.0</td>
</tr>
</tbody>
</table>
**Contents**

Welcome .................................................................................................................................................. 5

What is a MP-1 Software Token? ........................................................................................................ 5

How does it protect me? ......................................................................................................................... 5

Can anybody use my MP-1? .................................................................................................................. 6

How does it work? ................................................................................................................................ 6

How do I create a Security PIN? ........................................................................................................... 6

What is Self-Enrollment ....................................................................................................................... 6

I have not received an Enrollment E-mail ............................................................................................ 6

The Self-enrollment process .................................................................................................................. 6

How do I use my MP-1 .......................................................................................................................... 10

What if my token shuts off while I’m entering the token code? ............................................................. 10

What are my responsibilities? .............................................................................................................. 10

  Protect your Security PIN .................................................................................................................. 10

  How can I change my PIN? ................................................................................................................. 10

  What if I forget my PIN? .................................................................................................................... 11

  What if my token is “Locked” ........................................................................................................... 11

What should I do if I can’t logon using my token? ............................................................................... 11

How long will my token continue to operate? ..................................................................................... 11

Customizing Your Token ..................................................................................................................... 11
Welcome

In this package you will find instructions for installing and activating your MP-1 token. Once activated you will use your MP-1 token every time you logon.

![One-time Password](image)

Figure 1: MP-1 Software Token for Smart Phones

What is a MP-1 Software Token?

Up until now, you’ve logged on with your User Name and Password. The problem is that passwords are easily compromised, putting your identity and the resources you access at risk. By using a MP-1 you will be able to generate a “One-time Password” or “OTP”. As the name implies, an OTP can only be used once. Each time you logon you will use your MP-1 to generate a new OTP.

How does it protect me?

Password theft is the single most common way thieves and hackers steal identities and gain unauthorized access to networks and resources. While they have many ways to steal a password, success depends on the stolen password being valid, much the way credit card theft relies on the card being usable until you report it as stolen. The problem of course is that it is almost impossible for you or the security professionals that manage your network to discover your password has been compromised until long after damage has been done.

The MP-1 solves this problem because the instant you logon with your OTP, it is no longer valid. Any attempt to logon by reusing the OTP will not only fail, but also instantly alert your network security professionals to a possible attack on your identity.
Can anybody use my MP-1?

Your MP-1 is protected against unauthorized use by a Security PIN only you know. Again, much like a bank card or “Chip and PIN” credit card, the thief not only needs access to your MP-1 but must know your PIN as well. Any attempt to use the MP-1 with and incorrect PIN will fail. Successive attempts to guess your PIN will automatically “Lock” your MP-1, effectively disabling it, giving you and your network security professionals time to deal with the threat.

How does it work?

Each time you need an OTP, the MP-1 will prompt you to enter your Security PIN. For example:

<table>
<thead>
<tr>
<th>Security PIN</th>
<th>OTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1427</td>
<td>48466628</td>
</tr>
<tr>
<td>1427</td>
<td>4Kz6371R</td>
</tr>
<tr>
<td>1427</td>
<td>669-9487</td>
</tr>
</tbody>
</table>

How do I create a Security PIN?

You have or will shortly receive a “Self-enrollment Email” from your company which contains a unique URL to the self-enrollment web site and instructions for installing the MP-1 software, enrolling and activating your token. You will create a Security PIN that only you know during self-enrollment.

What is Self-Enrollment

Self-enrollment is a simple process for activating your token and creating your PIN. When you complete this process you will be able to use your token when you logon.

I have not received an Enrollment E-mail

If you have not received your self-enrollment email, contact your help desk to arrange for a new self-enrollment email to be sent to you.

The Self-enrollment process

The process begins when you receive your self-enrollment e-mail notification containing instructions and an enrollment URL.
Welcome Guide for Users of CRYPTOCard MP-1 Software Tokens on Smart Phones

What is Self-Enrollment?

Read the instructions then using a browser, navigate to the URL in the message.

The enrollment web site will display a list of devices or “Targets” approved by your security administrator such as iPhone, Android, Blackberry and laptops upon which the MP-1 can be installed. Choose a smart phone device from the list that will give you the most convenience and be readily available every time you need to logon, and then click the “Next” button.

Figure 2: Example Self-enrollment e-mail

The next page displays the email address to which the “Over the Air” token installation instructions will be delivered. These messages must be retrieved from the Smart Phone using the native email client.

Figure 3: Select Target Device
NOTE: Do not retrieve this message on your smart phone using a browser or Web Mail.

Figure 4: Confirm Enrollment Delivery Address

Retrieve the Over-the-Air installation instructions using an email client on your smart phone. Do not use a browser / web mail. The instructions contain 2 steps:

1. Downloading the MP-1 application. This step will install the application by retrieving it from the appropriate source such as iTunes or Android Market. When this step is completed, the MP-1 launch icon will appear on your smart phone.

2. The 2nd step completes the installation of the token.

Figure 5: Install MP-1 Application
When installation is complete, the token name and serial number will be displayed in a tile in the MP-1 application. Multiple tokens can be loaded into the application following this method.

![MP-1 with multiple tokens installed](image)

Each token is displayed in its own tile (1). Tap the tile to activate the token.

Edit (2) allows the token name, PIN and other functions to be modified.

Tap the information button (3) to retrieve information about the MP-1 application and version.

On first use of the token you will be required to create and confirm a security PIN. The Security PIN must meet the requirements set by your security administrator for length and composition.

![Create a New PIN](image)

![Confirm New PIN](image)

Your token is now installed and ready to use.
How do I use my MP-1

Every time you need an OTP to logon, begin by tapping the MP-1 icon and then enter your Security PIN. If you have more than one token loaded you must select a before you will be prompted to enter your PIN.

Figure 9: Using the MP-1 OTP

Remember, every time you logon you will enter your Security PIN to generate an OTP, then type or copy the OTP into the appropriate password or OTP field. OTPs are displayed for approximately 60 seconds.

What if my token shuts off while I’m entering the token code?

Simply generate a new token code by clicking the Generate Token Code button and then enter your Security PIN. Enter the Token Code into the appropriate password field and logon as normal.

What are my responsibilities?

Using the MP-1 will not only provide security, it will simplify your life by reducing or eliminating the need to remember or periodically change passwords. Your token will do this for you, every time you logon. However, you do have a few simple obligations:

Protect your Security PIN

Protect your Security PIN just as you would the PIN for your bank or credit card. Never share it with anybody, including people you trust. Your network security administrator and help desk will never ask for your PIN and you should never reveal it to them. Never write down your PIN.

How can I change my PIN?

If you wish to change your PIN or are concerned that it has been compromised tap the “Edit” button (Figure 6: MP-1 with multiple tokens installed on page 9), then tap the blue token tile, then enter your
What should I do if I can’t logon using my to
ken?

The most common cause of failed logon is entering an incorrect OTP. Never attempt to reuse a token code and ensure that you enter the code exactly as displayed on the token, including any upper and lower case letters and punctuation that it may contain.

Your account will automatically lock for a period of time if more than the allowed number of consecutive logon attempts fail. You must wait this amount of time before your account will unlock. Contact your help desk to resolve logon problems.

How long will my token continue to operate?

Your token will be able to generate OTPs until it is revoked by your Security administrator.

Customizing Your Token

You can customize your token in several ways: Change your PIN, Resync the token, Rename the token, Turn Signature mode on/off, and review the tokens operating parameters. To access any of these functions, begin by tapping the Edit button then tapping a token. Enter your PIN, then tap Done.
Customizing Your Token

**CHANGE PIN**
Tap the Change PIN option, enter a new PIN value and tap Done. Confirm your new PIN by re-entering the value when prompted, then tap Done.

**RESYNC TOKEN**
Tap the Resync Token option, then enter the 8 digit challenge provided by your Security administrator or by the Self-service page. Give the Resync Response Code to your Security administrator or enter it when prompted on the Self-service page. Tap Done to exit.

**RENAME TOKEN**
Tap the Rename Token option, then enter a new name, then tap Done.

**SIGNATURE ON/OFF**
The signature function is off by default and should not be enabled unless advised by your Security administrator. To enable, tap the Signature option, then set to On, then tap Done.

**OPERATION**
To view the token operating parameters, tap the Operation option. To exit tap Done.

**REMOVE A TOKEN**
Tap the red symbol to the left of the token, then tap Delete. Tap the confirmation delete message to confirm removal of the token, then enter your PIN.
UNLOCK A TOKEN
If the maximum number of incorrect PIN entry attempts is exceeded, your token will display the message "Locked". Tap the token. If the unlock option has been enabled by your security administrator, the token will display an unlock code. Give this code to your security administrator who will then give you an unlock code to enter into the token. Enter the code, then tap Done. Enter a new PIN value, then confirm the value by re-entering the PIN. Tap Done to complete the unlock process.