Implementation Guide for the

Command Line Interface (CLI)

with

BlackShield ID

http:// www.cryptocard.com

Copyright

Trademarks

Additional Information, Assistance, or Comments

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

support@cryptocard.com

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

Related Documentation

Refer to the Support & Downloads section of the CRYPTOCard website for additional documentation and interoperability guides: http://www.cryptocard.com.

Publication History

Date	Changes	Version
January 26, 2009	Document created	1.0
July 9, 2009	Copyright year updated	1.1
October 16, 2009	Minor updates	1.2

Table of Contents

Overview

By default, the BlackShield ID server uses a web based administration console, to manage users and tokens. You have the option of using a command line interface to send the servers commands and options, which can manipulate users and/or tokens.

Applicability

This integration guide is applicable to:

CRYPTOCard Server	
Authentication Server	BlackShield ID
Version	Professional Edition 2.3+

CRYPTOCard Agent	
Agent	BlackShield ID Command Line Interface
Version	2.x
Operating System 32-bit	Windows 2003, Windows 2008
Operating System 64-bit	Windows 2003, Windows 2008

Assumptions

BlackShield ID has been installed, fully configured within the System Admin tab, and you have tokens and users available within the assignment tab.

Operation

The command line interface can be used to perform many operations that normally are done from within the GUI management web interface.

The operator runs the CLI from the command prompt with a series of switches or options. The operator then can issue commands, which can perform actions such as adding users, deleting users, assigning tokens or performing actions in bulk

Preparation and Prerequisites

1. The BlackShield ID Command Line Interface.exe has been installed.
2. You have adequate licensing to support the functionality you are attempting to perform.
3. You have an operator who has at minimum, permission to use 'Remote Management'
4. If you are using a non-default agent key file, ensure to have this on hand to place into the key file directory within the CLI installation directory.
5. A valid SMTP server has been specified in the System Admin tab, and has been confirmed to be working by using the test functionality.

Installation

1. Run the BlackShield ID Command Line Interface.exe installer.
2. Click the 'Next' buttons to advance through the installer options.
3. To avoid misplacing the command line interface, it's recommended that you keep all default installation locations.
4. When you finish the installer, you will now have the command line interface installed.

Note: If you use your own key file, you will need to place it into the key file directory within the CLI directory before proceeding to the 'Usage' section.

Usage

Bulk self enrollment

Bulk self enrollment takes a group of users you specify and will automatically assign them all a token, and will put their accounts into 'Self Enrollment' mode. Refer to the Administrators guide for a verbose explanation of 'Self Enrollment'.

Here is how to self enroll a bulk number of users.

Creating user enrollment file

1. Create a plain text file.
   Using notepad or an equivalent text editor will do.
2. Copy and paste the template text below into your text editor.

3. Edit the user names and token types as necessary.
4. Save the text file to the installation path of the CLI.
   Normally this is C:\Program Files\CRYPTOCard\BlackShield ID\CLI
   Naming the file enrolledUsers.txt will assist in performing these procedures.

Using user enrollment file

1. Open a command prompt and change directory to C:\Program Files\CRYPTOCard\BlackShield ID\CLI.
2. Issue command: bsidcli.exe –f userEnrollmentFile.txt > enrolledUsers.txt
3. The command line should simply go to the next line.
4. There should be a file named enrolledUsers.txt in the C:\Program Files\CRYPTOCard\BlackShield ID\CLI directory. This file will show you the results of bulk enrollment, including all the serial numbers, which were assigned to each user.
5. Each user you self enrolled will receive a self enrollment e-mail from the BlackShield ID server.

Bulk import text template

```
Connect [ip address of BsID server] [Operator user name] [OTP or password]
enroll user1 –type KT
enrol user 2 –type KT
enrol user 3 –type RB
enrol user 4 –type MP
enrol user 5 –type KT
```

Troubleshooting

Failed logons

Symptom:	Every time you run the bsidcli.exe –f userEnrollmentFile.txt, it indicates that your authentication request has failed.
Possible Causes:	1. The user name you are attempting to use is not an operator 2. The operator account does not have the '**Remote Management'** access control permission.
Solution:	Login to the BlackShield ID manager, and browse to the Operators tab. Search for the operator you are attempting to use. • If the user does not appear in your search results, this user is not a secured user. • If the user does not have the '**Remote Management'** access control enabled, check the box, and then click Apply.

Agent Upgrade

To upgrade this Agent, uninstall the current version then run a newer version of the Agent installer.

For more information, please refer to the BlackShield ID Admin Guide located at: **http://www.cryptocard.com**