GrIĐsure Token Guide for
BlackShield ID
Trademarks

CRYPTOCOard 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 \CRYPTOCOard\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

CRYPTOCOard’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.

CRYPTOCOard 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

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

Publication History

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 4, 2010</td>
<td>Initial release</td>
</tr>
</tbody>
</table>
Table of Contents

Overview ........................................................................................................................................................................1

How does GrIDsure work ? ............................................................................................................................................1

Compatible Network Access Points ...............................................................................................................................3

Creation and Deployment .............................................................................................................................................3
  Creating a token .......................................................................................................................................................3
  Issuing a token ...........................................................................................................................................................4

Token options ................................................................................................................................................................6
  Policy options ...........................................................................................................................................................6
  Token template options ...........................................................................................................................................6

Authentication sequence with a GrIDsure token ...........................................................................................................7
Overview

GrIDsure is a way of providing an end-user the ability to generate a one-time password, without requiring the end-user to have any additional hardware or software applications. GrIDsure presents the end-user with a grid of cells containing random characters, from which the end-user selects their ‘personal identification pattern’ (PIP). Each time the end-user needs to authenticate the grid will display a random / unique set of characters. The end-user then just needs to remember their PIP and provide the specific characters within those cells that make up their PIP in order to securely authenticate to the protected network resource.

How does GrIDsure work?

GrIDsure displays a grid of cells containing random characters to an end-user. As shapes and patterns are remembered more simply than words and numbers, GrIDsure involves the end-user to remember a sequence of cells in a pattern on the grid that is easily recognizable to them.

The end-user chooses their ‘personal identification pattern’ (PIP) from the arrangement and sequence of the cells from the grid.
When the end-user is required to authenticate securely to a protected network resource, they select the characters that match their PIP from the unique characters shown to them by the grid.

In this example, the end-user’s PIP would be a value of 5582. This is seen in the highlighted cells below.

Therefore to authenticate, the end-user would enter 5582 as their one-time password value. The next time the end-user needs to authenticate, the characters displayed by the grid will be different, but the PIP remains the same. The end-user just needs to enter the new characters in their PIP displayed by the grid.
In this example, the end-user would now enter 0182 as their one-time password to authenticate.

Compatible Network Access Points

Currently only web based resources protected by the BlackShield 2.6 IIS6 agent can be used with the Gridsure token. This includes virtual sites, Outlook Web Access 2003 using forms, SharePoint 2003/3.0 and Remote Web Workplace.

Creation and Deployment

As with all tokens in BlackShield, most of the procedures will take place on the Assignment tab.

Creating a token

When a BlackShield operator clicks on the 'Create' button in the Assignment tab, the option to create a Gridsure token is available.
Note: From the Assignment tab, BlackShield 2.6 sees GrIDsure tokens as a 'Custom' type, with serial numbers starting with 'GSxxxxxx'.

A GrIDsure token can only be issued to an end-user via the Self-Enrollment process.

BlackShield ID must be licensed for Custom token capacity.

Issuing a token

From within the Assignment tab, select your chosen user on the left and then select a GrIDsure token on the right. You can now self-enroll this user and token by clicking the ‘Enroll’ button.
After selecting the self-enrollment link in their email, the end-user will be presented with a grid. From this grid they must select their PIP and enter it into the 'Response' field.

So long as the end-user supplies a PIP that meets the GrIDsure token options selected by the BlackShield operator, the self-enrollment will complete and the GrIDsure token is ready for authentication.
Token options

Policy options

From the BlackShield Policy Admin tab, the authentication options for the GrIDsure tokens can be customized.

- Allow trivial PIPs: when enabled, allows the end-user to select a PIP consisting of a diagonal line, straight line, or the four corners of the grid
- Use Numbers: when enabled, the grid will display numbers (0-9).
- Use upper case letters: when enabled, the grid will display upper case letters (A-Z)
- Use lower case letters: when enabled, the grid will display lower case letters (a-z)
- Use special/symbolic characters: when enabled, the grid will display special characters (!@#$%^&*?)

Token template options

From the BlackShield Policy Admin tab, the GrIDsure token template can be edited.
The following options are supported:

- PIN Type: No PIN, Server-side user select, Server-side server select, Server-side fixed.
- Initial PIN: can be random, or a fixed value.
- Grid size: controls the number of columns and rows presented by the grid. Can be 5x5, 6x6, or 7x7

**Authentication sequence with a GrIDsure token**

The following example shows an end-user accessing a web site protected with the BlackShield 2.6 IIS 6.0 agent configured to authenticate against a BlackShield ID 2.6 server.

**Step 1:** The end-user launches their web browser and enters the protected web site address. They are presented with the BlackShield IIS 6.0 logon page.

**Step 2:** The end-user now provides their User name, and static password, followed by clicking the 'Log On' button. The OTP field is left empty.
Step 3: The end-user is now ‘challenged’ with the GrIDsure token.

The end-user now provides their PIP value into the OTP field. After clicking the 'Log On' button if the credentials provided are correct the end-user will be authenticated and gain access to the protected web site resource.

Note: The grid which is displayed in this example has highlighted green squares showing the PIP. In an actual scenario, the users PIP would never be revealed and the OTP would be masked.