Secure Multi-Domain Smart Card Reader

User Manual

Models:
RS20N-3 (MDR102) – Secure 2-Port Multi-Domain Smart Card Reader
RS40N-3 (MDR104) – Secure 4-Port Multi-Domain Smart Card Reader
# Table of Contents

## Introduction .......................... 2

## Overview ............................. 3
   - Hardware Terms ................................. 4
   - PC Modes ........................................ 5
   - PC Modes Description ............................ 5

## Operation ............................. 6
   - MDR Operational Modes ............................. 6
   - Initial MDR Configuration Steps ..................... 7
   - Working with the MDR ............................ 9

## Information .......................... 10
   - High Sec Labs Warranty Programs .............................. 10
   - High Sec Labs Limited Warranty Terms and Conditions .................. 10
   - Limited Warranty Types .................................. 11
   - High Sec Labs Security Procedures ............................. 12
   - Copyright and Legal Notice ............................ 13
INTRODUCTION

**Intended Audience**
This document is targeted at the following professionals:
- System Administrators.
- IT Managers with adequate knowledge of PKI architecture.
- End Users.

**Objectives**
- This document describes the fundamental configuration procedures that are required to install the HSL Multi-Domain Smart Card Reader.

**Prerequisites**
- Obtain and install the applications, drivers and files of the cryptographic software (CSP) which corresponds to your selected smart card vendor.
- Obtain a smartcard from your selected smart card vendor.
Overview

Background
In organizations where users simultaneously work on multiple computer environments, the use of smartcards to secure logons and applications (such as email encryption) generates a costly and administrative-intensive overhead.

The Challenge
Due to the fact that a dedicated smartcard and smartcard reader have to be purchased, programmed and installed on both per user and computer bases multiplied by the number of computers and users in the organization, the TCO and administrative effort required to support such environments is extremely high.

For example, an employee that has to access 3 computers simultaneously would need to have 3 smartcards, one for every computer environment (domain) plus 3 smartcard readers, each reader connected to a separate computer.

The HSL Solution
HSL developed the Secure Multi-Domain Smartcard Reader (MDR) technology to provide a simple and yet secure solution to this common problem.

The HSL Multi-Domain Smartcard Reader (MDR) is a single secure smartcard reader which connects simultaneously to multiple computers thus allowing a user to utilize a single smartcard while working securely on multiple computer environments at the same time.
Hardware Terms

The following terms are used to describe hardware elements in this document:

1. Numbered USB Cables: USB Cables with numbered connectors.
2. Smartcard Reader
3. PC Association Led
4. PC Number Button
5. PC Number Led
PC Modes

Overview
The MDR has a built-in association mechanism which allows the smartcard to be concurrently mapped to multiple PCs. PC Modes determines which of the associated PCs is set as Active, while others are set as Passive. An Active PC has full (read/write) access to the smartcard which is inserted into the MDR. A Passive PC recognizes the smartcard but has no access to it until it is made Active. At any given time only one PC can be set as Active.

PC Modes Description

Active Mode
- The smartcard is inserted into the MDR.
- The PC Association Led is ON.
- The PC Number Led is ON.
- The MDR appears under the computer’s operating system device manager as a smartcard reader.
- The computer’s OS and applications have full (read/write) access to the smartcard.

Passive Mode
- The smartcard is inserted into the MDR.
- The PC Association Led is ON.
- The PC Number Led is OFF.
- The MDR appears under the computer’s operating system device manager as a smartcard reader.
- The computer’s OS and applications have NO access to the smartcard.
MDR Operational Modes

Operational Mode settings determine how Active/Passive PC Modes are set. For example, when the MDR Operational Mode is set to Manual, the user has to manually press the PC Number Button corresponding to the PC that requires access to the smartcard.

When the MDR Operational Mode is set to dynamic, association methods are used to determine which PC will be set as Active. For example, when the MDR operational Mode is set to LED Auto Association, the MDR will automatically actively associate itself to the computer which requires smartcard access based on a led-light activity detection algorithm.

To preset which MDR Operational Mode is in use (Manual / Auto…etc), a hardware dual in-line package (DIP) switch has to be configured. See the switch configuration settings in Table 01.

<table>
<thead>
<tr>
<th>#</th>
<th>Mode</th>
<th>Description</th>
<th>DIP Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Manual</td>
<td>The user has to manually press the PC Number Button corresponding to the PC that requires access to the smartcard. For example: Once the MDR is simultaneously connected to two computers (PC#1 and PC#2) and a user needs to authenticate securely via smartcard in front of PC#1, by pressing PC Number Button #1 the MDR becomes actively associated with PC#1 and the user can authentication successfully. Then when the user wants to digitally sign an email on PC#2, pressing PC Number Button #2 will actively associate the MDR to PC#2 making the smartcard available to the email application on that computer.</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>LED Auto Association</td>
<td>MDR will automatically associate itself to the computer which requires smartcard access based on its led-light activity detection algorithm. Some smartcard applications trigger the reader’s led-light to blink while attempting to communicate with the smartcard. Once the MDR detects such a trigger, it automatically actively associates itself to the computer that initiated it.</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Power Auto Association</td>
<td>MDR will automatically associate itself to the computer which requires smartcard access based on a power-detection algorithm. Some smartcard applications increase the reader’s power consumption while attempting to communicate with the smartcard. Once the MDR detects an increase in power, it automatically associates itself to the computer that initiated it.</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>LED &amp; Power Auto Association</td>
<td>MDR will automatically associate itself to the computer which requires smartcard access based on both led-light and power activity detection.</td>
<td>2 + 3</td>
</tr>
</tbody>
</table>
## Initial MDR Configuration Steps

*Table 02* describes the initial MDR configuration steps.

<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Action Description</th>
<th>Expected Behavior</th>
</tr>
</thead>
</table>
| 1  | Install Smartcard Applications | Verify that the applications, drivers and files of the cryptographic software (CSP) that corresponds to your selected smart card vendor are installed on all the computers that you plan to connect to the MDR.  
**Note:** Perform a computer restart in case needed to complete the smartcard application installation. |                                                                                  |
| 2  | Select MDR Operational Mode    | Operational Mode selection is controlled by a hardware dual in-line package (DIP) switch.  
Led Auto Association is the default mode.  
In this mode, PIN number 2 is pulled down and other PINs are up.  
**Note:** Read the Understanding the MDR Operational Mode section for further details. |                                                                                  |
| 3  | Turn PC ON                     | Make sure that all the PCs are turned ON.                                          | 1 second beep sound.  
All PC Association Led lights blink once.                                               |
| 4  | Connect MDR to Power           | Connect the MDR to Power                                                           | 1 second beep sound.  
All PC Association Led lights blink once.                                               |
| 5  | Connect USB Cables to PCs      | Connect the MDR USB cables to the computers. Cable numbers correspond to the numbered MDR buttons. | All PC Number Led lights blink constantly.                                         |
| 6  | Insert Smartcard into the MDR  | Insert your smartcard into the MDR reader socket.  
**Note:** Make sure the smartcard chip is facing away from you.                      | 1 second beep sound.  
All lights are OFF.                                                                     |
| 7  | Initial Association with PC#1  | Press PC Number Button#1 to initialize the MDR on PC#1.                           | PC Number Button#1 light turns ON.  
PC Association Led#1 blinks and then turns ON.  
The MDR appears as a smartcard reader under PC#1 device manager.                      |
<table>
<thead>
<tr>
<th>#</th>
<th>Action</th>
<th>Action Description</th>
<th>Expected Behavior</th>
</tr>
</thead>
</table>
| 8  | Initial Association with PC#2 | Press PC Number Button#2 to initialize the MDR on PC#2.                           | PC Association Led#1 remains ON.  
PC Number Button#1 light turns OFF.  
PC Number Button#2 light turns ON.  
PC Association Led #2 blinks and then turns ON.  
The MDR appears as a smartcard reader under PC#2 device manager. |
|    | Notes:                        | Once pressing Button#2, the green led light aligned with Button#1 remains ON, indicating that the MDR is still recognized by PC#1.  
Repeat the process on the remaining PCs.                                                                                                                                       |
| 9  | Verify all PCs are Initialized|                                                                                  | All PC Association Led lights are ON.  
One of the PC Number Buttons is ON indicating that the MDR is actively associated with the PC that corresponds to it. |
Working with the MDR

One completing the initial MDR configuration steps the MDR is ready for use allowing simultaneous usage of a single smartcard with multiple PCs.

Smartcard Removal Behavior
Removing the smartcard from the MDR immediately de-associates the MDR from all coupled PCs. As a result, smartcard-aware applications will notice the smartcard absence and respond accordingly.

For example, a Windows PC that is configured to require smartcards for user logon may be set to lock the user’s desktop once the smartcard is removed.

Re-associating the MDR after Smartcard Removal
In order to continue using the smartcard (after it’s been removed from the MDR), the user has to insert the smartcard into the MDR and complete steps 7-9 in order to re-associated the MDR with all the corresponding PCs.

De-associating the MDR from a Specific PC
Long pressing a PC Number Button is the equivalent of removing the smartcard only from the PC which corresponds to that button without effecting other associated PCs. To re-associate that PC with the MDR, press the PC Number Button to initialize the MDR (as described in step 7).

The de-association option is useful in any case a user wants to de-associate the MDR from a specific PC, without interfering with other PCs which are associated with the MDR.

For example, when a user has to lock PC#1 by removing the smartcard yet remain logged-on to PC#2, or when a certain PC is not successfully associated with the MDR and the user wants to re-associate it.
High Sec Labs Warranty Programs

Hardware Service Coverage
All HSL hardware comes with a two-year, return-to-depot warranty at no extra charge. This limited warranty covers 100% of parts and workmanship on any required repairs. However, repair turnaround times average two weeks, so the purchase of enhanced hardware service coverage is highly recommended for all mission-critical applications. The PREMIUM program provides next day replacement service and 24x7 telephone support. Both of these programs are available in US, Canada and in Europe.

<table>
<thead>
<tr>
<th>Program</th>
<th>Service Level</th>
<th>Technical Support Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>STANDARD</td>
<td>Return-to-Depot Repair</td>
<td>Email 24/7, phone 9 am - 5:30 pm,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Eastern, Monday to Friday</td>
</tr>
<tr>
<td>PREMIUM</td>
<td>Next Day Advance Replacement</td>
<td>24x7</td>
</tr>
</tbody>
</table>

All HSL hardware are designed and tested for at least 10 years of maintenance-free operation. HSL will be pleased to extend your STANDARD warranty for up to 7 years after purchase and to extend PREMIUM warranty for up to 10 years after purchase.

It is beneficial to purchase enhanced coverage at the same time as the hardware. Doing so ensures that the hardware is continuously protected. Although it is possible to obtain enhanced coverage at a later date, such contracts are subject to a blackout period which delays the start of any coverage by 60 days.

High Sec Labs Limited Warranty Terms and Conditions
High Sec Labs warrants that the product you have purchased from High Sec Labs or from an authorized High Sec Labs reseller is free from defects in material and workmanship under normal use during the Limited Warranty period. The warranty period commences on the date of purchase. Your sales receipt showing the date of purchase of the High Sec Labs product is your proof of the date of purchase. This warranty is not transferable to anyone who subsequently purchases the product from you. This Limited Warranty does not include expandable parts.

Never open the product’s enclosure and never attempt to replace or fix any internal part! Any attempt to repair the product, install or replace components by an unauthorized person could expose that person to risk electrical shock and will cause the product warranty to be void immediately. Should the product require service during the term of the Limited Warranty, High Sec Labs would provide either mail-in or carry-in service.

High Sec Labs will repair or replace according to its own discretion the defective products or parts with new products or parts. All exchanged parts and products replaced under this warranty will become the property of High Sec Labs.

TO OBTAIN SERVICE UNDER THIS LIMITED WARRANTY for mail-in or carry-in you must return the product, freight prepaid and insured (or assume the risk of loss or damage during shipment) in the original container or an equivalent, to a High Sec Labs Service Center. If the unit was not registered, you should enclose a written receipt for the product, showing the date of purchase, distributor’s or dealer’s name from whom you purchased the product, and both the model and serial number of the product. High Sec Labs will pay the return ground shipping charge within the continental United States, Canada and Europe.
Limitations of Remedy

THIS LIMITED WARRANTY COVERS repair or replacement at the discretion of High Sec Labs of the High Sec Labs product device purchased from High Sec Labs. THIS LIMITED WARRANTY DOES NOT COVER losses or damages that occurred as a result of shipping; improper installation or maintenance by anyone other than an authorized representative of High Sec Labs; acts of God or accident; misuse, neglect, or misapplication of the product; installation of options or parts by anyone other than High Sec Labs; exposure to extremes of temperature or humidity; or improper electrical power. Products returned to High Sec Labs for service, in warranty and post warranty that are diagnosed as No Fault Found will be subject to a diagnostic fee.

The Limited Warranty will be void in case of mechanical damage to the product, High voltage electrical pulse or lightning induced damage.

Product may have special Tampering Evident Labels that will provide clear indications if removed or tampered with. This will void High Sec Labs product warranty. Product may also have battery powered active anti-tampering function. Any attempt to remove enclosure screws or to open product enclosure may trigger this function and void product warranty.

This warranty excludes power supply, cables, mouse and adapters purchased with the device.

THIS LIMITED WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, REMEDIES OR CONDITIONS, WHETHER ORAL OR WRITTEN, EXPRESSED OR IMPLIED. THERE ARE NO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. HIGH SEC LABS WARRANTY OBLIGATIONS AND BUYER’S REMEDIES ARE EXCLUSIVELY STATED HEREIN. HIGH SEC LABS LIABILITY, WHETHER BASED ON CONTRACT, TORT, WARRANTY, STRICT LIABILITY OR ANY OTHER THEORY, SHALL NOT EXCEED THE PRICE OF THE INDIVIDUAL UNIT WHOSE DEFECT OR DAMAGE IS THE BASIS FOR THE CLAIM. IN NO EVENT SHALL HIGH SEC LABS BE LIABLE FOR ANY SPECIAL OR CONSEQUENTIAL DAMAGES. HIGH SEC LABS SPECIFICALLY DOES NOT REPRESENT THAT IT WILL BE ABLE TO REPAIR ANY PRODUCT UNDER THIS WARRANTY OR MAKE A PRODUCT EXCHANGE WITHOUT RISK TO OR LOSS OF PROGRAMS OR DATA.

U.S.A. State Laws

Some states do not allow limitations on how long an implied warranty lasts, or allow the exclusion or limitation of incidental or consequential damages, so the above limitations may not apply to you. This warranty gives you specific legal rights, and you may also have other rights, which vary from state to state.

Limited Warranty Types

Mail-In Coverage

The Customer will make the initial service request to the High Sec Labs Customer Service. If High Sec Labs determines that a repair is required, the Customer will receive instructions on returning the Product to High Sec Labs. The customer will return the product in its original package or an equivalent. The Customer will pay incoming freight charges and is responsible for any loss or damage to the Product while it is in transit. Upon completion of the repair, High Sec Labs will return the Product to the Customer, freight prepaid. A copy of your Warranty Certificate must accompany the Product. All non-High Sec Labs Product, accessories, attachments, modifications and all programs, data, and storage media must be removed from the Product before it is mailed in for service. High Sec Labs shall not be responsible for items that are not removed.
Carry-In Coverage
The Customer will make the initial service request to the High Sec Labs Customer Service depending on the product covered. If High Sec Labs determines that a repair is required, the Customer must deliver the Product to a High Sec Labs Authorized Service Provider, make arrangements and pay for the transport of Product to Customer after its repair. A copy of the Customer’s Warranty Certificate must accompany the Product. All non-High Sec Labs Product, accessories, attachments, modifications and all programs, data, and storage media must be removed from the Product prior to taking Product to the High Sec Labs Authorized Service Provider. High Sec Labs or High Sec Labs Authorized Service Provider shall not be responsible for items that are not removed or that are damaged before they are received by High Sec Labs or the Service Provider.

Upgrade Commitment on behalf of Customer
In case High Sec Labs discovers some failure in its Software (e.g. Firmware, Operating System, Management Software, Plug-Ins or any other aspect of its Software), the customer might be required to upgrade his software to a specific software version within a reasonable period of time. After the specified time has passed, High Sec Labs will not be held obligated to support the product under its Warranty or Extended Warranty terms and conditions.

High Sec Labs Security Procedures

Reporting HSL Product Security Vulnerability
If you are aware of potential security vulnerability with any HSL product, we encourage you to contact us immediately at the following email address: security@highseclabs.com or our technical support line at: +972 4 9591191

After your communication is received, HSL personnel will contact you to follow up. To ensure confidentiality, HSL encourages you to use our PGP encryption key. The security@highseclabs.com email address is not intended to reach technical support on HSL products or services. Any support inquiries should be directed to support@highseclabs.com or support web-form indicated above.

Responsible Disclosure
Notifying a vendor prior to releasing information publicly about vulnerability is standard practice in the security industry and is known as “responsible disclosure.” This advance notice allows vendors to research and fix vulnerabilities before potential attackers are notified of their existence – keeping the product install base secure. We appreciate your assistance in ensuring that HSL products and services are secure.

Receiving a notification about Product Vulnerability / Solution
HSL security policy and internal system provides quick response in case that product security vulnerability is found. Once product vulnerability is found and confirmed by HSL QA, HSL provides an email to the following list of users based on affected product:

1. All users who registered their product and provided a valid email address.
2. All users who registered for Premium product warranty coverage.
3. All users that reported same security vulnerability.
4. Users that requested information about specific product vulnerability.

Once a solution is found – HSL will send an email to the same distribution list within 24 hours.
Copyright and Legal Notice

© 2015 High Sec Labs Ltd all rights reserved.

This product and/or associated software are protected by copyright, international treaties and various patents.

This manual and the software, firmware and/or hardware described in it are copyrighted. You may not reproduce, transmit, transcribe, store in a retrieval system, or translate into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, any part of this publication without express written permission from High Sec Labs.

HIGH SEC LABS SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN; NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

The information contained in this document represents the current view of High Sec Labs on the issues discussed as of the date of publication. Because High Sec Labs must respond to changing market conditions, it should not be interpreted to be a commitment on the part of High Sec Labs, and High Sec Labs cannot guarantee the accuracy of any information presented after the date of publication. PRODUCT DESIGN AND SPECIFICATION IS SUBJECT TO CHANGES WITHOUT NOTICE

This Guide is for informational purposes only. HIGH SEC LABS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

PATENTS AND TRADEMARKS

The products described in this manual are protected by multiple patents.

High Sec Labs, KVM Combiner, and the High Sec Labs logo are either trademarks or registered trademarks of High Sec Labs Ltd.

Products mentioned in this document may be registered trademarks or trademarks of their respective owners.

The Energy Star emblem does not represent endorsement of any product or service.

U.S. GOVERNMENT RESTRICTED RIGHTS

The Software and documentation are provided with RESTRICTED RIGHTS.

You agree to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

The information and specifications in this document are subject to change without prior notice.

Images are for demonstration purposes only.