HighSecLabs
Highest Security Solutions

Secure Multi-Domain Smart Card Reader

Models:
RS20N-4 – Secure 2-Port Multi-Domain Smart Card Reader
RS40N-4 – Secure 4-Port Multi-Domain Smart Card Reader

Intended Audience

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

Objectives

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

Prerequisites

- Obtain and install the applications, drivers and files of the cryptographic software (CSP) corresponding to the smart card vendor.
- Obtain a smart card from the smart card vendor.
- Verify that the smart card setup works correctly on each PC using a standard smart card reader before to connecting the MDR.

Hardware Terms

The following terms are used to describe hardware elements in this document:
1. Numbered USB Cables: USB Cables with numbered connectors.
2. Card Reader Slot
3. PC Association LED
4. PC Button
5. PC Button LED
6. DIP Switch
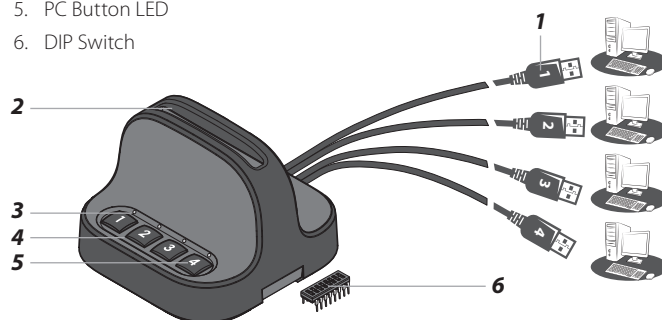
Initial MDR Configuration Steps

Table 1 - MDR Configuration Steps

#	Action	Action Description	Expected Behavior
1	Install Smart Card Applications	Verify that the applications, drivers and files of the cryptographic software (CSP) that corresponds to the smart card vendor are installed on all the computers connected to the MDR. **Note**: If necessary, restart the PCs to complete the smart card application installation.	
2	Turn PCs ON	Make sure that all the PCs are turned ON.	
3	Test Smart Card using a Standard Reader	Verify that the smart card setup works correctly on each PC using a standard smart card reader before connecting the MDR.	
4	Connect MDR to Power	Connect the MDR to a power source.	
5	Connect USB Cables to PCs	Connect the MDR USB cables to the computers. The cable numbers correspond to the PC Number Buttons.	All PC Button LEDs blink constantly.
6	Insert Smart Card into the MDR	Insert a smart card into the MDR's Card Reader Slot. **Note**: Make sure the smart card chip is facing the PC Buttons.	1 second beep sound. All LEDs are blinking.
7	Initial Association with PC #1	Press PC Button #1 to initialize the MDR on PC #1.	PC Button #1's LED blinks for 5 seconds, then remains ON. The MDR appears as a smart card reader under PC #1's device manager.
8	Initial Association with PC #2	Press PC Button #2 to initialize the MDR on PC #2. **Note**: Repeat the process on the remaining PCs.	PC Button #1's LED turns OFF. PC Button #2's LED blinks for 5 seconds, then remains ON. The MDR appears as a smart card reader under PC #2's device manager.

Working with the MDR

Once the initial configuration is complete, the MDR is ready to operate.

Pressing the MDR's PC Buttons switches the MDR to the associated PC.

Smart Card Removal Behavior

Removing the smart card from the MDR immediately de-associates the MDR from all coupled PCs. As a result, smart card-aware will notice the smart card's absence and respond accordingly.

For example, a Windows PC that requires a smart card for user logon may be set to lock the user's desktop once the smart card is removed.

Re-associating the MDR after Smart Card Removal

To use a smart card after it has been removed from the MDR, insert the smart card into the MDR's Card Reader Slot and complete configuration steps 6-8 to re-associate the MDR with the connected PCs.

De-associating the MDR from a Specific PC

In some cases, such as when one computer must be locked while still operating on the others, it can be useful to disconnect the MDR from a specific computer.
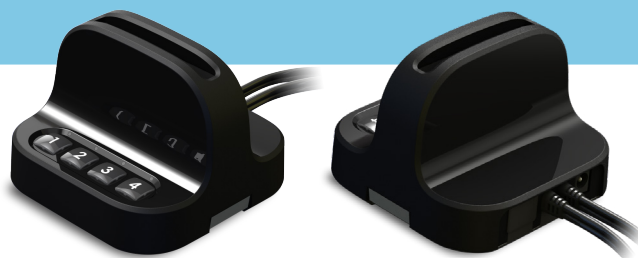
To do this, press and hold the PC Button for that computer for three seconds. The MDR will de-associate with that computer as if the smart card had been removed, but will remain associated with all other connected computers.

To re-associate the MDR with the computer, press the corresponding PC Button again.

Reset

Press and hold one of the MDR's PC Buttons for 7 seconds to reset the device and its association with the PCs.
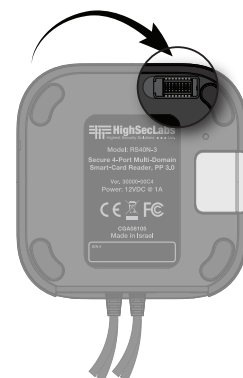
MDR Operational Modes

The MDR has three Operational Modes which determine how it interacts with the connected PCs: Manual Association, Single-Channel Association, and Automatic Association.

In Manual Association Mode, the channels to each computer must be opened or closed manually and individually. Single-Channel Association opens only the channel to the selected computer and closes all others. Automatic Association opens all channels to the connected computers and associates them with the MDR automatically.
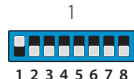
The MDR's Operating Mode can be configured using the Dual In-Line Package (DIP) switch located on the MDR's underside. The DIP switch includes 8 slides, numbered 1-8 from left to right. If a slide is in the up position, its status is ON. If a slide is in the down position, its status is OFF.

DIP Switch Configuration

1. Locate the DIP switch in the upper-right corner of the MDR's underside.

2. Gently remove the DIP switch cover.

3. Activate an Operational Mode by adjusting the slides according to the corresponding configuration in Table 2.

Table 2 - MDR Operational Modes:

#	Mode	Description	DIP Switch
1	Manual Association	The channels to each computer must be opened manually by pressing their associated PC Button. The channels will remain open unless they are closed manually by pressing the corresponding PC Button again.	1 1 2 3 4 5 6 7 8
7	Single Channel Association	Pressing a PC Button will open the channel between the MDR and the associated computer and close all others. Pressing another PC button will open the corresponding channel and close the previous one.	1 + 7 1 2 3 4 5 6 7 8
8	Automatic Association	Pressing PC Button #1 will open all channels between the MDR and the connected computers, associating the MDR with them automatically.	1 + 8 1 2 3 4 5 6 7 8

Power Requirements: External, wall-mounted power supply 12VDC, 5W maximum

HighSecLabs
Highest Security Solutions

Safety and Regulatory Statements

Safety Symbols

One or more of the following symbols may be included on the product and/or in its documentation.

Instructions: This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the product user manual.

Dangerous Voltage: This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

Power On: This symbol indicates the principal on/off switch is in the ON position.

Power Off: This symbol indicates the principal on/off switch is in the OFF position.

Protective Grounding Terminal: This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

Safety Precautions

WARNING: To avoid a potentially fatal shock hazard and possible damage to equipment, please observe the following precautions.

- Instructions: Do not disable the power grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) outlet that is easily accessible at all times.
- Disconnect the power from the product by unplugging the power cord from either the electrical outlet or the product. The AC inlet is the main disconnect for removing power to this product. For products that have more than one AC inlet, to remove power completely, all AC line cords must be disconnected.
- This product has no serviceable parts inside the product enclosure. Do not open or remove product cover.

CAUTION: Some HSL products contain a lithium battery. This battery is not a field replaceable item, and replacement should not be attempted by a user. If errors occur when using the product and the battery is suspected, contact HSL Technical Support.

WARNING: For Service Personnel Only - There is a risk of explosion if the battery is replaced with an incorrect type. Dispose of used batteries according to the manufacturer's instructions.

This product is for use with other products that are Listed or Certified by a Nationally Recognized Testing Laboratory (NRTL).

Installation Precautions

Do not connect this product to computing devices that:

- are TEMPEST computers
- include telecommunication equipment
- include frame grabber video cards
- include special audio processing cards.

Security Vulnerability

If a security vulnerability appears while installing this product, contact HSL Technical Support immediately:

- Web form: www.highseclabs.com/support/case/
- Email: security@highseclabs.com
- Tel: +972-4-9591191/2

WARNING: Unit Enclosure Warning - If the unit's enclosure appears disrupted or if all LEDs flash continuously, remove the product from service immediately and contact Technical Support.

Change Management

For change management tracking, perform a quarterly log check to verify that the RFD was not improperly used to override the current device policy by an unauthorized person.