Secure Multi-Domain Smart Card Reader

Models:

RS20N-3 (MDR102) – Secure 2-Port Multi-Domain Smart Card Reader
RS40N-3 (MDR104) – 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.

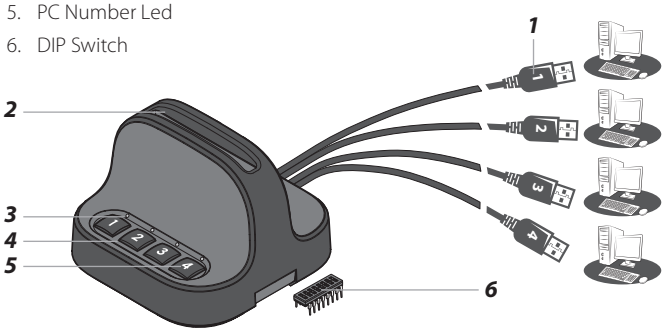
Prerequisites

- 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.
- Verify that your smart card setup works correctly on each PC using a standard smart card reader prior to connecting the MDR.

Hardware Terms

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

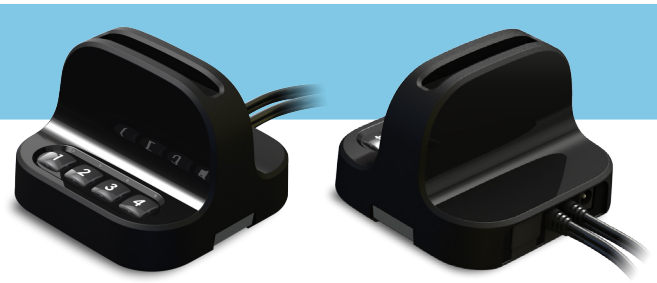
1. Numbered USB Cables: USB Cables with numbered connectors.
2. Card Reader Slot
3. PC Association Led
4. PC Number Button
5. PC Number Led
6. DIP Switch



Initial MDR Configuration Steps

Table 01 describes the initial 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 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 smart card application installation.	
2	Turn PC ON	Make sure that all the PCs are turned ON.	
3	Test Smart Card using a Standard Reader	Verify that your smart card setup works correctly on each PC using a standard smart card reader prior to connecting the MDR.	
4	Connect MDR to Power	Connect the MDR to Power	1 second beep sound. All 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 Smart Card into the MDR	Insert your smart card into the MDR reader socket. **Note**: Make sure the smart card chip is facing towards 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. The MDR appears as a smart card reader under PC#1 device manager.
8	Initial Association with PC#2	Press PC Number Button#2 to initialize the MDR on PC#2. **Notes**: Repeat the process on the remaining PCs.	PC Number Button#1 light turns OFF. PC Number Button#2 light turns ON. The MDR appears as a smart card reader under PC#2 device manager.



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 6-8 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.

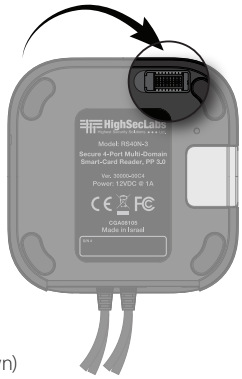
For example, when a user has to lock PC#1 by removing the smartcard yet remain logged-on to PC#2, or when a certain PC is not successfully associated with the MDR and the user wants to re-associate it.

MDR Operational Modes

Operational Mode settings determines 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, auto-association methods are used to determine which PC will be set as Active.
For example, when the MDR operational mode is set to Activity-Detection Auto Association, the MDR will automatically actively associate itself to the computer which requires smart card access based on an activity detection algorithm.
To preset which MDR Operational Mode is in use (Manual / Auto...etc), there is a hardware dual in-line package (DIP) switch situated in the underside of the base. See the switch configuration settings in Table 02, column DIP Switch.

DIP Switch Configuration



1. To change the DIP switch settings, hold the MDR with the underside facing you. In this position, the DIP switch should be at the upper right corner.
2. Gently remove the DIP switch cover.
3. The switch includes 8 slides numbered from 1 to 8, ordered from left to right.
4. When pulled down, slide status is OFF. When pulled up, slide status is ON.
5. To activate an operation mode, pull down its corresponding slide.
6. Multiple slides can be turned OFF (pulled down) at the same time.
7. Refer to Table 02 to adjust DIP switch settings with your work scenario.

Table 02 Operational Modes:

#	Mode	Description	DIP Switch
1	Manual	The user has to manually press the PC Number Button corresponding to the PC that requires access to the smart card. For example: Once the MDR is simultaneously connected to two computers (PC#1 and PC#2) and a user needs to authenticate securely via smart card in front of PC#1, by pressing PC Number Button #1 the MDR becomes actively associated with PC#1 and the user can authenticate 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 smart card available to the email application on that computer.	1 
2	Activity-Detection Auto Association	MDR will automatically associate itself to the computer which requires smart card access based on its activity-detection algorithm. Once an application attempts to interact with the smart card the MDR automatically associates itself to the computer that hosts it.	2 
3	Power-Detection Auto Association	MDR will automatically associate itself to the computer which requires smart card access based on its power-detection algorithm. Once the MDR detects an increase in power it automatically associates itself to the computer that initiated it.	3 
4	Device Manager Mode	Determines whether the MDR remains mapped to the computer's device manager, or not, upon smart card removal. Once enabled, the MDR remains mapped to the computer's device manager upon smartcard removal, just as a standard smart card reader would. When not in use, the MDR is disconnected from the computer's device manager upon smart card removal. This equals to disconnecting the USB cables between the MDR and the associated PCs but might cause computability issues with some smart card applications.	4  This option is only applicable when used in conjunction with other modes, for example 2+4.
5	Auto-Association Safe Mode	Application errors and usability issues may occur due to the smart card being switched to another computer in the middle of a smart card operation running on the active computer. When enabled, automatic switching of the smart card between computers will only occur when the smart card is idle (not in use). Auto-Association Safe Mode prevents the Auto-Association algorithm from switching the smart card in case it is busy – hence being used. When disabled, upon the detection of a smart card request the MDR immediately switches the smart card to the requesting computer, regardless of whether the smart card is in use by the currently active computer or not.	5  This option is only applicable when used in conjunction with other modes, for example 2+4+5
6	Activity & Power Auto Association with Device Manager Mode and Safe Mode (This is the default mode)	MDR will automatically associate itself to the computer which requires smart card access based on either activity or power detection (depending on the smart card type). Automatic switching of the smart card between computers will only occur when the smart card is idle (not in use). Upon smart card removal the MDR remains mapped to the computer's device manager, just as a standard smart card reader would.	2 + 3 + 4 + 5 

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