THE HSL **SECURE** MULTI-DOMAIN **SMART CARD** READERS

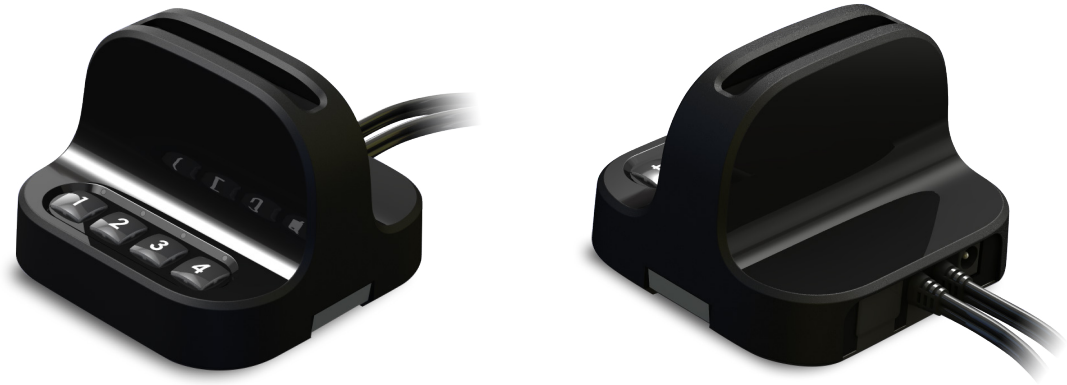
HighSecLabs
Highest Security Solutions Ltd.

HDC10275 Rev. 1.3

SMART CARD AUTHENTICATION BENEFITS

Provides unambiguous identification of users by the combination of two different components.

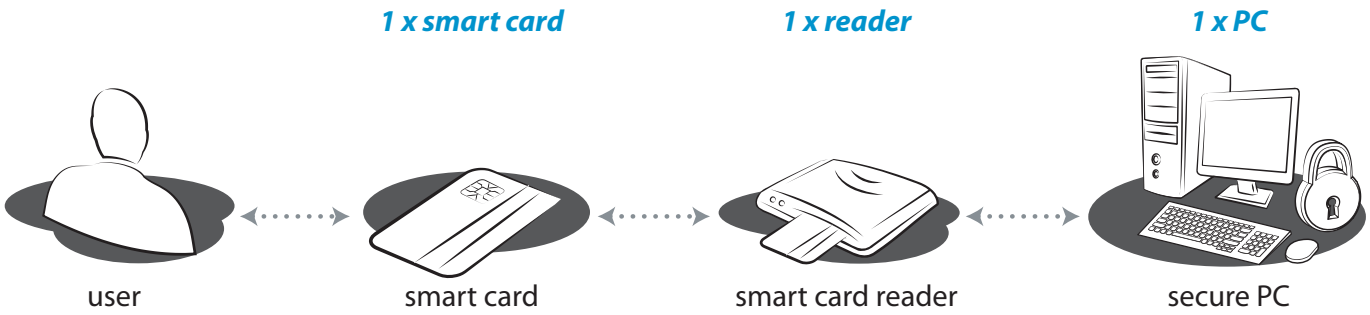
- Something the user possesses (e.g. Smart card).
- Something the user knows (e.g. PIN code).



COMMON AUTHENTICATION WORKFLOW

One-to-One scenario

1x user 1x smart card 1x smart card reader 1x PC



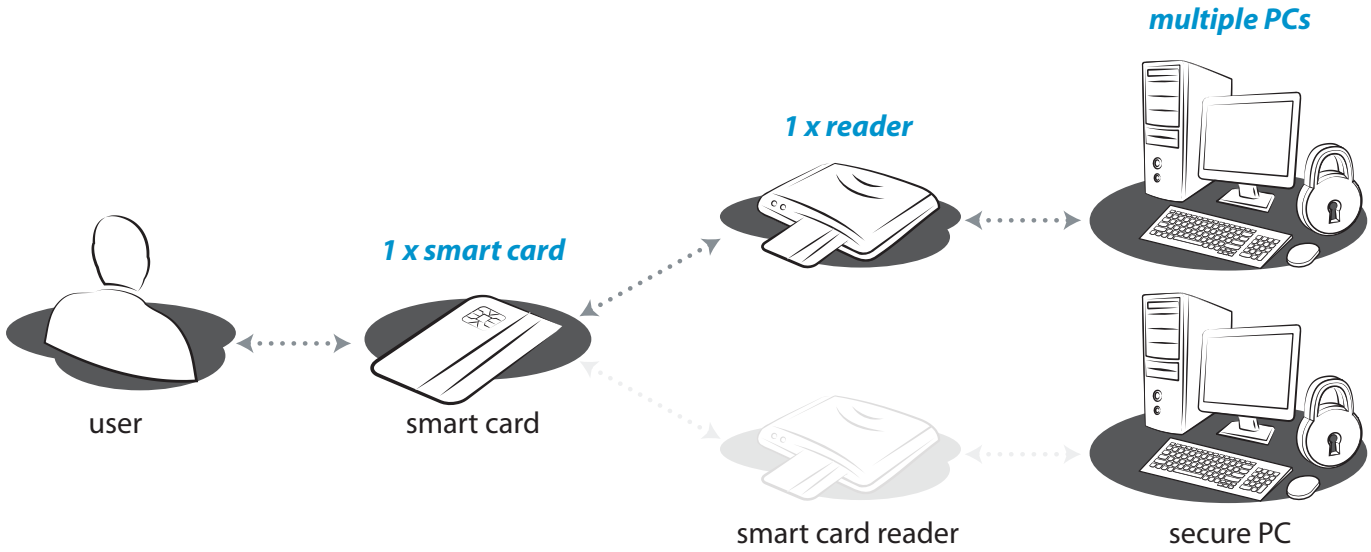
To work securely the user must insert the smart card and type the PIN code.

THE MULTIPLE PCS CHALLENGE

What if the user has to work simultaneously on multiple PCs?

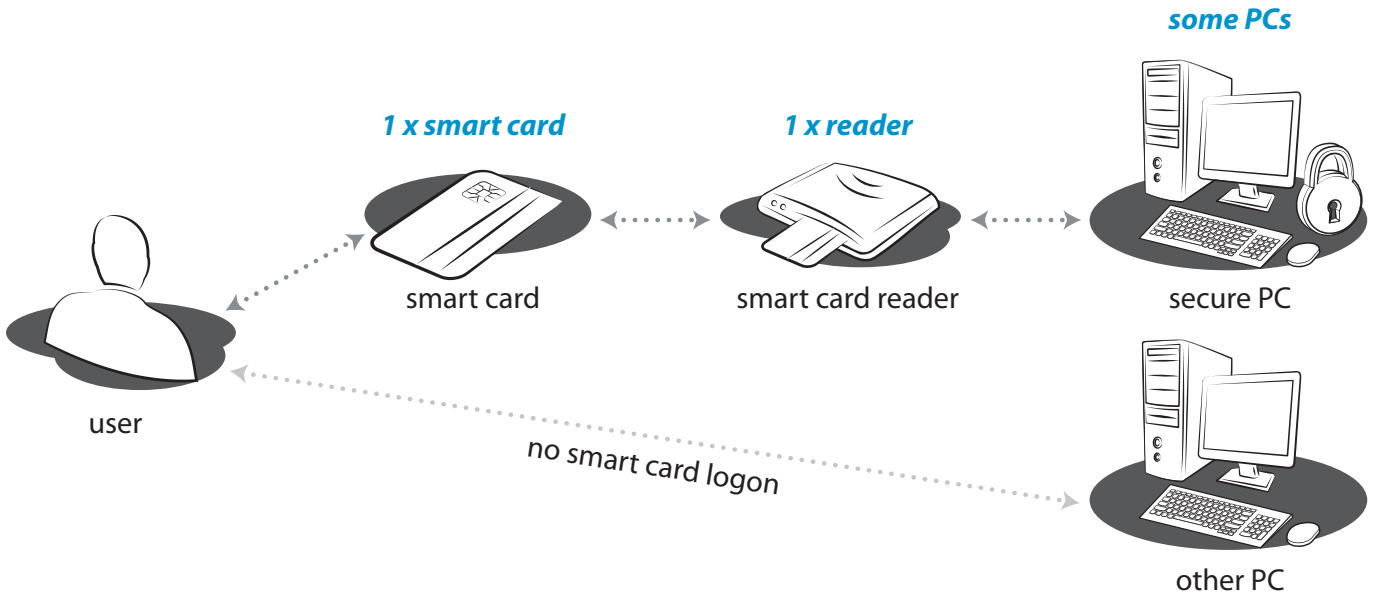
- **1# One-to-All Scenario (single session)**
  User has 1x smart card that can be used with all PCs, 1x PC at a time.
- **2# One-to-Some Scenario (single session)**
  User has 1x smart card that can be used with some PCs, 1x PC at a time.
  Smart card authentication is not implemented on all PCs.
- **3# Many-to-Many Scenario (multiple sessions)**
  User has multiple smart cards, one for each PC.
- **4# The HSL Solution: One-to-All Scenario (multiple sessions)**
  User has a single smart card for use with multiple PCs simultaneously.

One-to-All (Single Session) Drawbacks



- **Cost Overhead:**
  Each PC must have a dedicated smart card reader.
- **User Overhead:**
  User can't access PCs simultaneously. Only one PC at a time.
  User has to move the smart card between PCs.

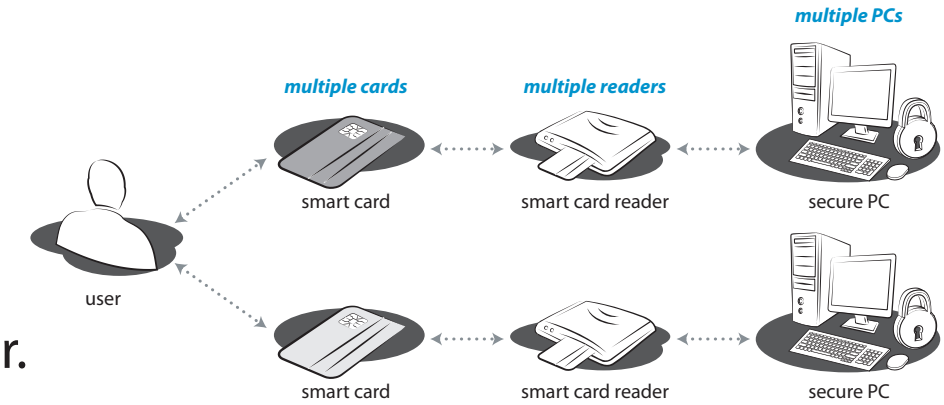
One-to-Some (Single Session) Drawbacks



Security Threat:

- User's work on other PC is not secure.
- User remains logged-on to other PC when smart card is removed.
- Asymmetric security policy is hard to justify and may not comply with organization policy.

Many-to-Many (Multiple Sessions) Drawback

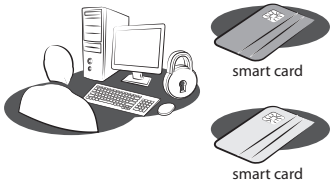


Administrative overhead:

- Administrators have to program and manage multiple smart cards for each user.

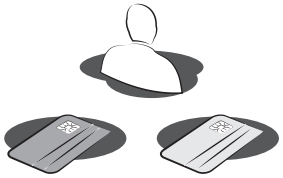
Cost overhead:

- Each PC must have a dedicated smart card reader.
- Multiple smart cards have to be purchased for each user.



User overhead:

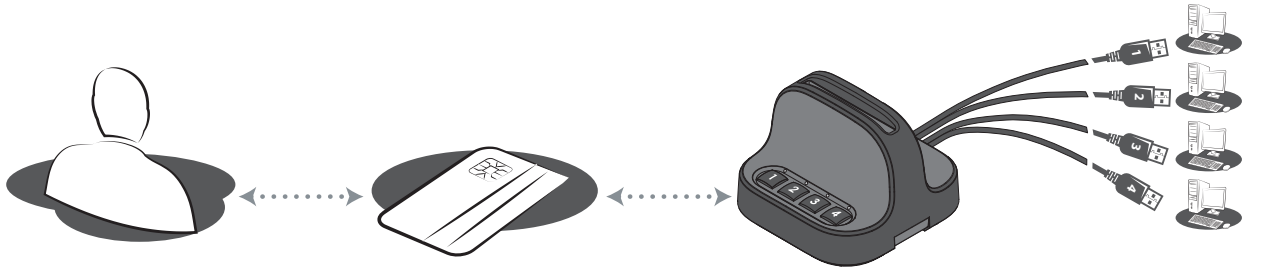
- The user must possess a smart card for each PC.
- Cards may get lost.
- Cards may be accidently left in the reader.



THE HSL SOLUTION

SECURE MDR SOLUTIONS

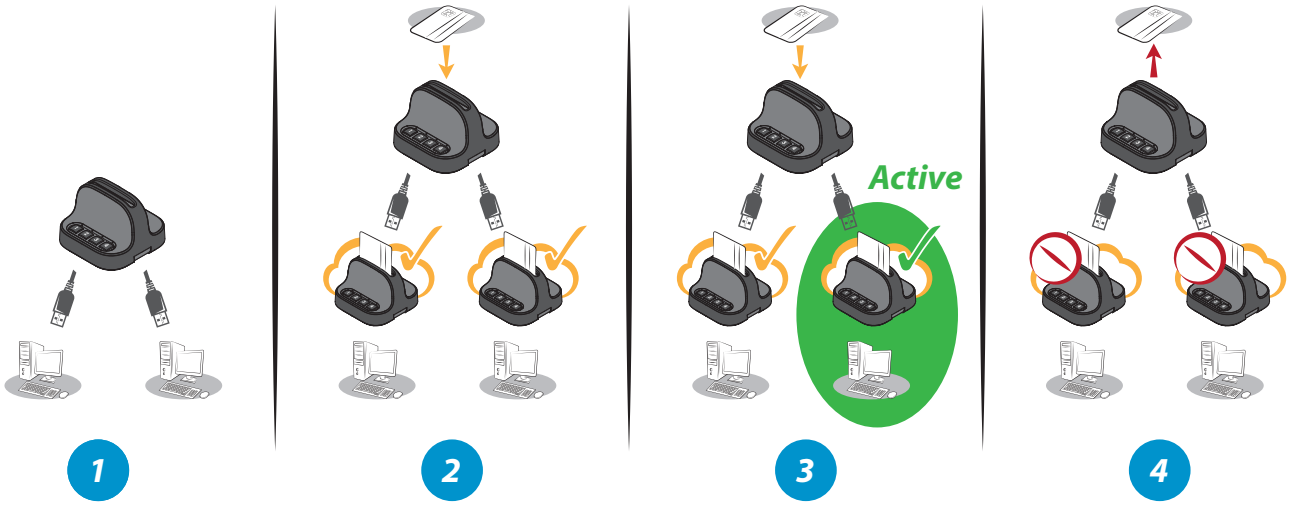
One-to-Many (Multiple Sessions)



Highlights:

- Unique: One-to-Many approach. Allowing 1x smart card and 1x Multi-Domain-Reader for simultaneous work on multiple PCs.
- Reduce overall smart card operational costs, buy fewer cards and readers..
- Minimize smart card administrative overhead.
- Increased security, easily enforce smart card authentication on all PCs.
- Increased security: card removal resets all PC session; no PC is left unsecured.
- Minimize user learning curve and overhead.
- Auto-association, dynamically map the smart card to the PC that requires access to it.

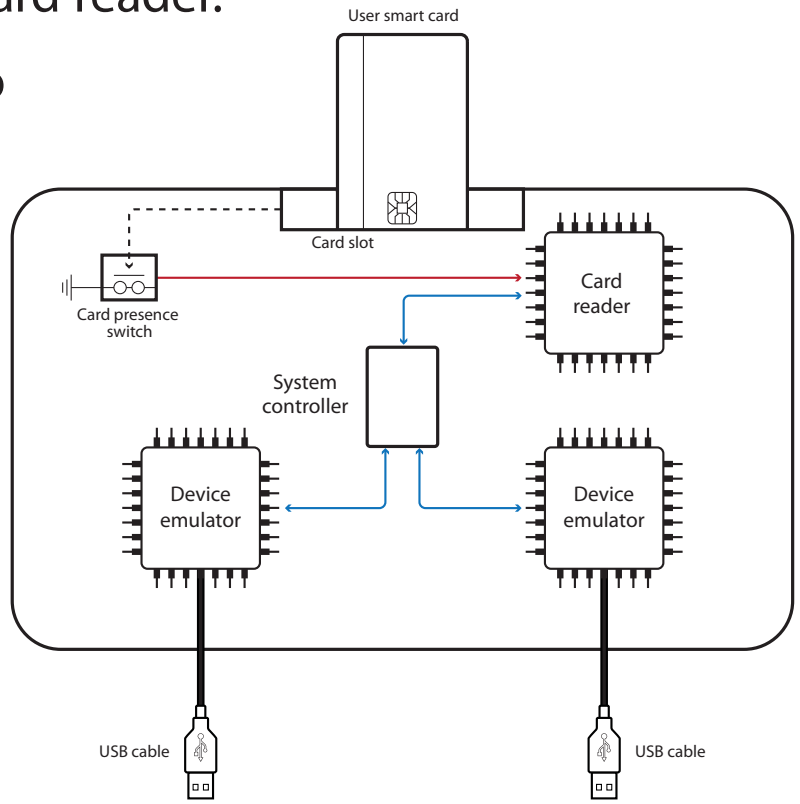
How it Works from a User's Perspective?



1. Connect the MDR to PCs
2. Insert the smart card and click the PC numbers to associate it with the computers
3. Smart card appears as available on all PCs simultaneously
   MDR dynamically associates the smart card to PCs that require smart card access (or user switches manually between PCs)
4. Smart card removal de-associates the MDR from all PCs

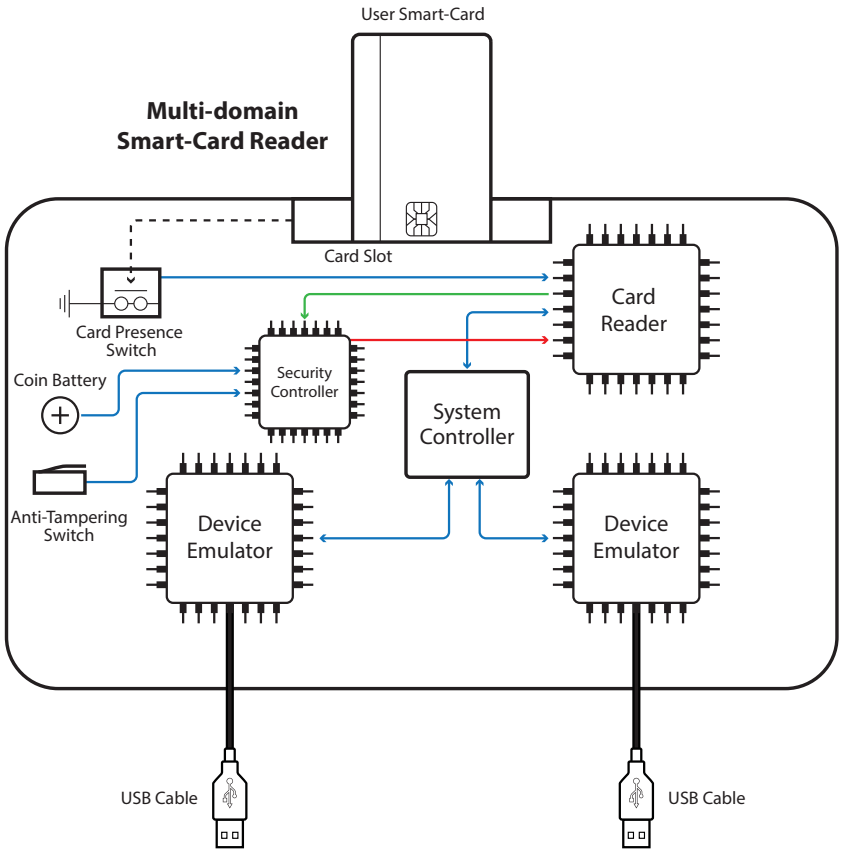
How it Works from a Design Perspective

- The MDR contains a standard smart card reader chip.
- A smart card reader chip assures 100% compatibility to existing and future cards, OSs and applications.
- The card presence sensor maps the smart card to the card reader.
- A system controller allows associating the smart card to the PCs on demand, by a logic requests queue.
- Each PC connects through device emulators to the system controller. The device emulator emulates the smart card reader to the host and assures the continuous connection between the PC and the card reader.
- The system controller arbitrates the different computers' CAC requests.



Design from Security Perspective

- Separate security controller arbitrates user and computer card requests.
- Holographic tamper evident labels.
- Security controller and smart card reader chip's firmware is in ROM. Code modification is not possible
- No card or user data is accessible to the MDR. No data can pass between coupled PCs.



HIGHLIGHTS SUMMARY

Feature	Benefit
Patent pending, unique solution on the market	Designed specifically to meet the need for secure simultaneous smart card access
Standard smart card reader chips (from SCM). No additional smart card reader drivers are needed	100% compatibility to existing and future cards, OSs and applications. Uses standard USB CCID drivers which are built into common computer operating systems.
Transparent to all participating PCs	PCs are unaware of their peers and can work seamlessly with the smart card.
Card removal de-associates the MDR from all PCs	Once the card is removed, all sessions are terminated at once.
Safe and Secure	No card or user data is accessible to the MDR. No data can pass between coupled PCs.
Once the MDR is associated with all PCs the user no longer has to deal with the smart card	MDR can automatically associate itself to the computer that requires smart card access, or it can be done manually. MDR includes auto-association with dynamic mapping of the smart card to the PC that requires secure access.
Reduce overall smart card operational and administrative costs without any security compromise	A single reader and card provide a solution for multiple PCs operated via smart card simultaneously and securely

SMART CARD READER - MODELS

Model	RS20N-4 	RS40N-4 
No. of computers	2	4
MDR ports	• 2 x USB Type-A to connect to computers, 1m long cable for each • 1 x DC power supply jack	• 4 x USB Type-A to connect to computers, 1m long cable for each • 1 x DC power supply jack
Controls and indications	• 2 x blue LEDs to indicate active channel • 2 x red LEDs to indicate tampering attempt or failure to read card • Sound transducer to provide user warnings (65dB maximum)	• 4 x blue LEDs to indicate active channel • 4 x red LEDs to indicate tampering attempt or failure to read card • Sound transducer to provide user warnings (65dB maximum)
Computer ports	• USB Type B ports	

THANK YOU

HighSecLabs
Highest Security Solutions Ltd.

For more information, please visit www.highseclabs.com