Smart Card Deployment in the Data Center:

Best Practices for Integrating Smart Card Authentication in a Secure KVM Environment

Executive Summary

While many organizations have employed smart card identification to enhance their physical security infrastructure, KVM (Keyboard, Video & Mouse) system users in particular can benefit greatly from the two-factor authentication that a smart card inherently provides to the logical realm (access to software and application systems on servers).

However, whereas a physical security system that incorporates smart cards is straightforward to implement, logical security using PKI-based authentication (Public Key Infrastructure) incurs very specific practical obstacles during implementation in a data center, network operating center, lab or any facility that relies on a KVM system for efficient operation. While smart card readers themselves are inexpensive, 1-to-1 mapping of card readers to server hardware neutralizes many of the efficiencies that a high-density server environment with few user touchpoints provides. IT managers thus face a difficult decision: greater security or greater convenience.

A similar problem has been faced previously. Before the modern server boom, most computer rooms employed a keyboard and monitor for each server – a 1-to-1 mapping. But KVM switching technology later eliminated this inefficient deployment, allowing one set of keyboard, monitor and mouse peripherals to be deployed to many servers at once. **By extending its peripheral set to include smart card readers, modern KVM switches with smart card capabilities can allow data center managers to enjoy the best of both worlds: greater security and greater convenience.**

The objective of this document is to provide insight into smart card support within a KVM system, enabling servers with PKI authentication to be deployed without sacrificing efficiency and convenience. We explore several points to consider when adding or deploying this functionality.

Note that this white paper provides perspective on the implementation of smart card readers for the purpose of accessing servers and PC's via a KVM switch, not the use of smart cards to log into the KVM system itself.

Introduction

The use of integrated PKI and smart card authentication infrastructure for strengthening user identification credentials is growing worldwide. Driving the demand is an increased need for greater physical security along with the requirement for stronger authentication of individuals accessing networks, often referred to as "logical access control." For logical access, smart cards provide additional security to organizations that require multifactor authentication without hampering user convenience.

Managing employee credentials for physical access to facilities and logical access to IT infrastructure can be burdensome and expensive – even simple tasks such as password resets and reminders can incur nontrivial costs in a large organization. Smart cards provide a form of identification that can be used to secure both physical and logical access while combining other business benefits. Thus, many organizations have employed secure, portable and multipurpose employee badges to enable an efficient and cost-effective identity management system. A sound understanding of the business processes and goals within an enterprise is a key to the most successful implementations of smart cards.

Global Smart Card Shipments by Sector (millions of units)

	2008 Global Shipment November 2008 Forecast		2009 Global Forecast	
Sectors	Memory	Microprocessor	Memory	Microprocessor
Telecom	380	3200	300	3600
Financial services / Retail / Loyalty	30	610	30	700
Government / Healthcare	250	140	170	160
Transport	160	30	160	30
Pay TV		100		100
Other (including corporate security)	80	65	80	70
Total	900	4145	740	4660
Aggregate Total	**5045**		**5400**	

Source: www.EuroSmart.com

A pioneer in the adoption of smart card infrastructure is the United States Department of Defense (DoD), which has 3.8 million smart card users as a result of its Common Access Card (CAC) program[1], an initiative motivated by HSPD-12. This presidential mandate intends to achieve improved physical and logical security of Federal defense employees and contractors worldwide by requiring extensive implementation of smart cards in the DoD, including extensive smart card-based authentication to information systems.

Practical Challenges Raised During Physical Implementation

Within organizations that have deployed smart cards for server access, administrators face a unique challenge. **In a data center setting, attaching individual smart card readers (or keyboards with integrated readers) to each and every server is impractical. A traditional KVM switch does not help this problem.** Directly-attached smart card readers require users to be physically located at the server when authenticating, essentially defeating the purpose of a KVM switch – and resulting in a big step backwards in efficiency and productivity.

Thus, a large number of organizations are now beginning to implement convenient smart card authentication infrastructure in their data centers by enabling the technology through a new generation of KVM switching solutions. These new KVM solutions do not simply integrate card readers as an additional peripheral at the KVM workstation. They also adapt their core functionality to support with secure smart card use.

When seeking a smart card-enabled KVM system, choose not only a solution that fulfills the basic requirement of supporting PKI authentication to multiple servers from a single location, but also one that makes the necessary KVM feature adjustments to enable seamless use of the reader. Finally, it should adhere to industry standards to ensure that security needs are met. In the next section, we explore the practical implications of these requirements.

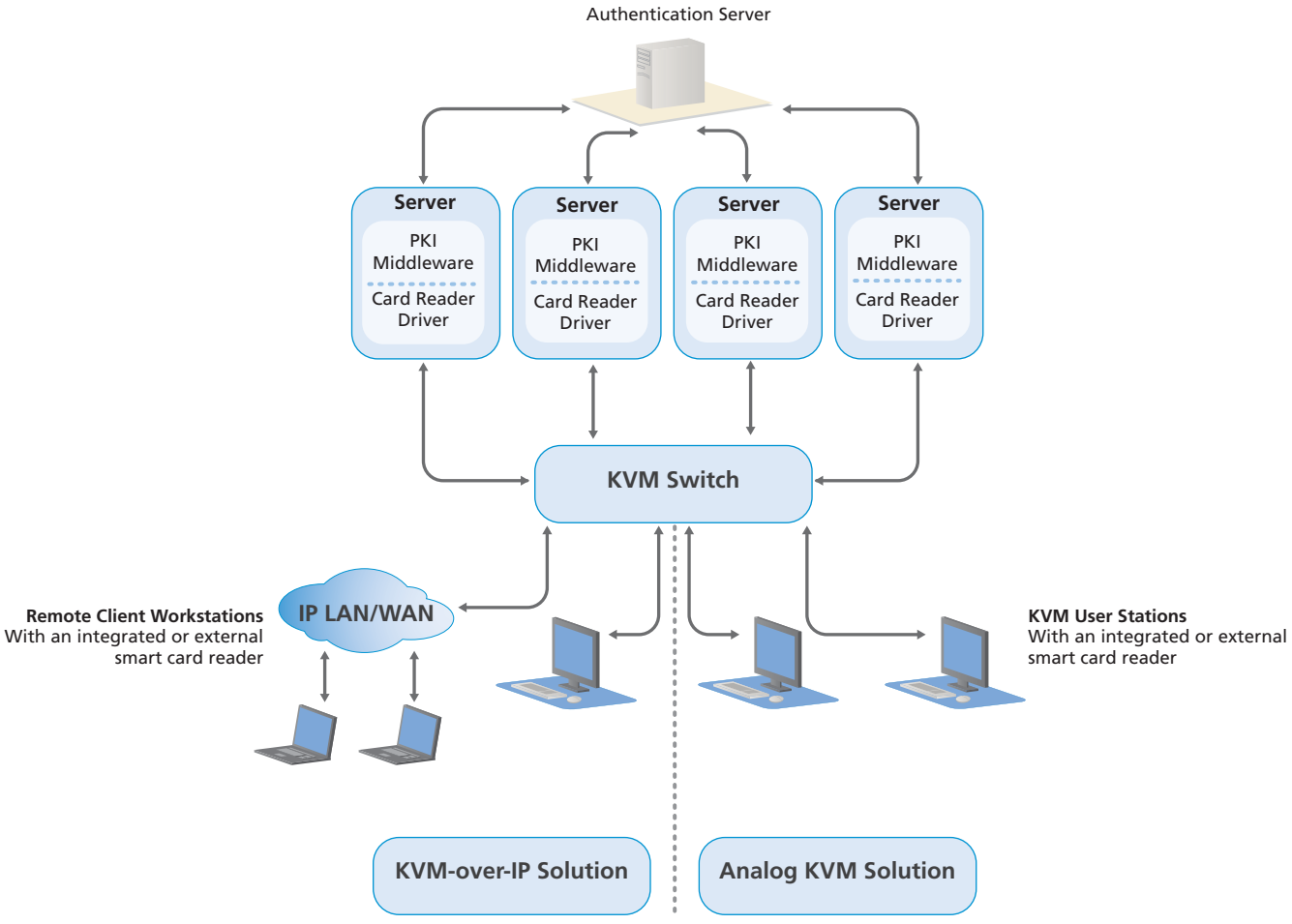
[1]Smart Card Alliance: Smart Card Alliance Annual Government Conference Opens with Strong Department of Defense Network Security Case Study, April 12, 2007

Components of a Smart Card-Enabled KVM Solution

To implement smart card authentication, an authentication server, middleware and driver must be installed on target servers to communicate with smart card readers. Also a KVM infrastructure must be in place. (See Diagram 1)

On the server side, special middleware deployed on each target server communicates with the card reader and the authentication infrastructure that's in place. The middleware is essentially a "go-between" that utilizes various specifications (such as PC/SC and x.509) and supports PKI certificates – enabling the use of smart cards for a wide variety of desktop, network security and productivity applications.

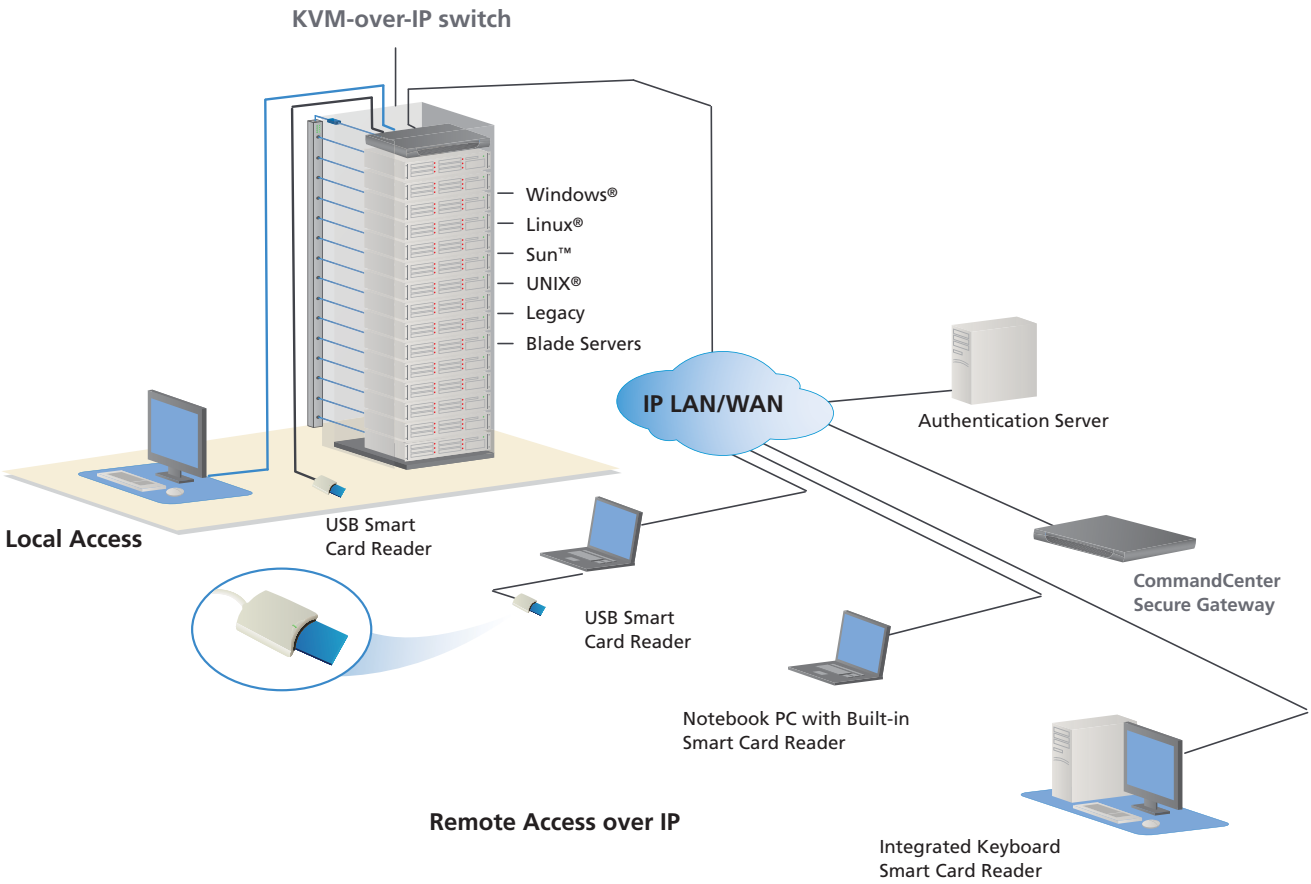
Additionally, a driver compatible with the card reader must be running on each target server. Compatible drivers are typically provided as a standard component of the server's operating system. Reader manufacturers also provide drivers as a download on their respective web sites.



(Diagram 1)

KVM-over-IP Solution

- Small dongles, called CIMs, attach to each server's I/O interfaces and emulate a keyboard, mouse, VGA monitor and smart card reader. Servers then behave as if these peripherals are directly attached to their I/O ports. (See Diagram 2)
- Digital (KVM-over-IP) switch(es). Each dongle is connected to the KVM switch using standard Cat5 or Cat6 cables. The digital KVM switches then provide users secure, anytime/anywhere BIOS-level access.
- For larger deployments, the Centralized Management System provides centralized access across multiple digital KVM switches, giving the user a single IP address to access hundreds or thousands of servers.
- Remote client software is used by the end user to connect to the remote servers over the IP LAN/WAN infrastructure, through the digital KVM switch. Smart card readers can be integrated in the user's workstation or plugged in via the USB port.
- Analog access in the data center is provided via the local port of the digital KVM switch. In this case, the smart card reader is connected through a USB port of the KVM switch itself. Be sure that the reader meets the ISO 7816, USB CCID and PC/SC standards.

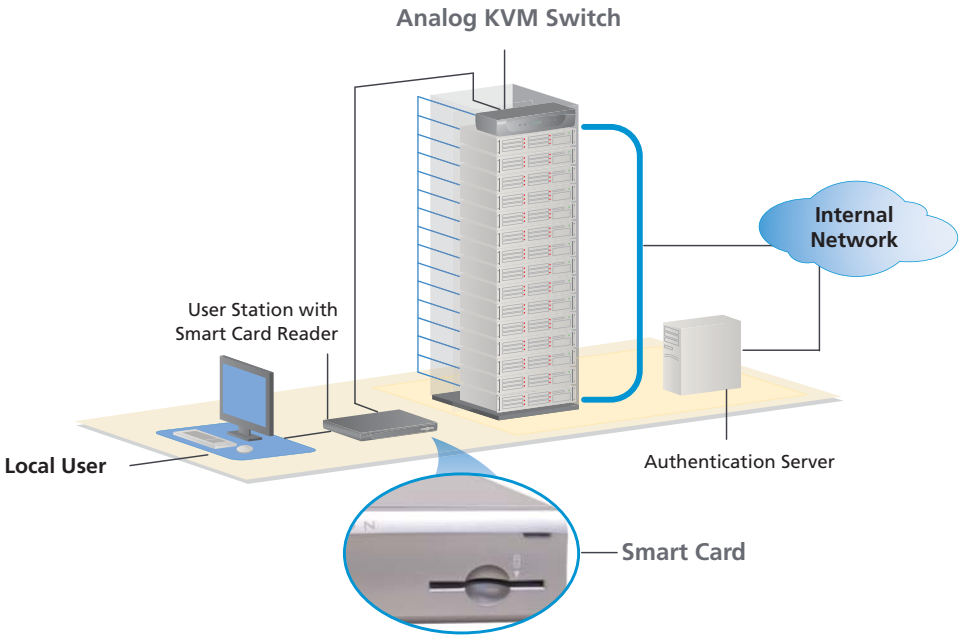


(Diagram 2)

Analog KVM Solution

An analog KVM solution that enables smart card authentication consists of the following components:

- Small dongles that attach to each server's I/O interfaces and emulate a keyboard, mouse, VGA monitor and smart card reader. Servers then behave as if these peripherals were physically attached to their I/O ports. (See Diagram 3)
- Central, matrix KVM switch(es). Each dongle is connected to the KVM switch using standard Cat5 or Cat6 cables. The matrix KVM switch infrastructure provides a single, logical system allowing multiple users to switch between hundreds of servers.
- User access workstation (user station). Each station is connected to the KVM switch with a Cat5/6 cable, and thus has access to all connected servers. These user stations provide a straightforward system-authentication and server-selection interface for each operator.
- A smart card reader, integrated or connected to each user station via USB. Note that USB "smart sticks" are also becoming more and more popular. A KVM platform that supports external readers should also support USB smart sticks. Be sure that the reader meets the PC/SC specification, which builds upon existing industry smart card standards and complements them with low-level device interfaces and APIs.



(Diagram 3)

Solution Best Practices

To deploy a truly secure solution, while maintaining optimal convenience and efficiency, IT managers should be sure to seek the following attributes:

1. **The integration with the smart card reader should be transparent to host computers.**
   Smart card readers, their middleware and the authentication server that manages user credentials each strictly follow industry specifications. For example, reader and server middleware utilize PC/SC as a communication protocol, and generally support x.509 certificates. As a result, today's smart card readers are essentially "plug-and-play."

   The goal of a smart card-enabled KVM switching solution is to provide the exact same "plug-and-play" reader capabilities to racks and rows of servers, while only requiring a single smart card reader per user.

2. **The smart card reader should not add complexity to the KVM solution.**
   Adding smart card capabilities to your KVM solution should be inherently simple. The primary purpose of a smart card reader is to quickly provide information stored on a user's card to the server, and a KVM system provides a direct out-of-band connection between users and the servers to do so. No other infrastructure should be necessary. The reader, although it may be located in the next room or the next continent, should interface with the target server exactly as if directly connected to one of its I/O ports.

3. **The solution should protect security by providing read-only access to card data.**
   Generally speaking, a smart card is simply a specialized form of digital media: data can be both read from the card as well as written to the card. But for the purposes of user authentication, only data reads are appropriate. Thus, to maximize security, a KVM system should only allow read-only access to the smart card, and disable data writes.

4. **The solution must not store or cache smart card data.**
   A KVM system could be a major security risk if it performs data caching of any kind. It's critical that the KVM system does not store or cache the card data. It should only transmit data to a single server at a time upon request, and only from a card that is physically present in the reader. By implication, the following behavior should occur:

   - If configured to do so, the card reader (and thus the KVM system) should support the automatic loss of authentication to the server upon removal of the card. To the middleware, switching away from a server should essentially be considered the same behavior as removing the smart card. And because the card data is not being stored or cached, users will automatically be required to reauthenticate when switching between servers. As a result, the card can conveniently remain in the reader during the user's session. The PKI middleware will "ask" for the card information again. Because there is no storage of the card information and reauthentication is required when navigating from server to server, the solution is very secure. This helps guard against unauthorized access by other KVM users who may connect to the same channel. In fact, if a user returns to a previously-accessed server, authentication should again be required.
   - Because the analog KVM system is out of band, unwarranted sniffing of the card's data via the corporate network is eliminated.
   - Digital KVM systems employ 128 and 256-bit encryption, which ensures that smart card data is secure.

5. **The solution should automatically enter "private mode."**
   A common feature of most KVM platforms is to allow multiple users to simultaneously access a particular server. When smart cards are in use, the solution should automatically enter into "private mode," allowing only one user at a time to access servers connected to the KVM switch.

6. **The solution should adapt its core features for a favorable user experience.**
   Some standard KVM features will need to be modified or disabled to avoid interference with the functionality of the card reader. For example, many KVM systems provide a scan feature, which automatically searches for the next available channel. Use of automatic scan with a card reader is inconvenient and the system should deactivate this feature whenever a smart card is in use.

Summary

When implementing a KVM-over-IP or an analog KVM solution, enabling users to employ smart cards for the purpose of accessing servers should not be a daunting task. But it can be especially difficult to deploy if the KVM platform does not seamlessly integrate such support. At the same time, implementing an efficient KVM system with smart card features should not compromise security in any way. An ideal solution, therefore, supports the use of smart cards and integrates card readers that operate exactly as if directly connected to the target servers. As a result, it should deliver the same inherent security features. When these attributes are met, security officers will be pleased by the broader deployment of highly-secure smart card capabilities in the data center, NOC and other facilities – while server administrators can adhere to security policies without losing the convenience and efficiency that a centralized KVM solution provides.

About Raritan

Raritan is a leading provider of secure IT infrastructure management solutions. We offer IT and facility directors, managers and administrators the control they need to increase power management efficiency, improve data center productivity and enhance branch office operations. In over 50,000 locations worldwide, our integrated in-band and out-of-band products help companies monitor and manage their energy, servers and other IT devices. Our intelligent PDUs, combined with energy management software and environmental sensors, offer remote power control and monitoring at the rack and device level, empowering data center owners with information to improve uptime and capacity planning, while efficiently utilizing energy to save power and money. And our access solutions, including KVM, serial and centralized management devices, offer unprecedented control of servers to maintain mission-critical environments.

Raritan's OEM division provides embedded hardware and firmware for server and client management, including intelligent power management, KVM over IP, IPMI and other industry standards-based management applications.