Raritan
A brand of legrand

Best Practices When Enabling Smart Card Authentication in a KVM System

A White Paper from Raritan

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 abrogates much 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 the 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 benefits of enabling smart cards specifically in an out-of-band ("analog") KVM system; and does not address an in-band ("networked," "digital") KVM-over-IP system. Additionally, this paper is concerned with 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. Finally, note that for simplicity, the term "smart card" is used throughout this document. However, the same principles apply to other types of smart media, such as USB smart sticks and fingerprint readers.

Introduction

The use of integrated PKI and smart card authentication infrastructure for strengthening user identification credentials is growing worldwide. Global revenues in the corporate smart card security market (both physical and logical) are expected to grow at a compound annual growth rate of 9.8% during the forecast period 2005-2010[1]. And the estimated worldwide shipment of smart cards for use in corporate security was 15 million units in 2006, estimated to grow to 20 million units in 2007[2]. 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 non-trivial costs in a large organization. Smart cards provide a form

1. Frost and Sullivan, World Corporate Security (Physical and Logical Access Control) Smart Cards Market, October 19, 2006

2. www.EuroSmart.com, Smart Card Shipment Global Sales 2006, Smart Card Shipment Global Forecast 2007

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.

A pioneer in the adoption of smart card infrastructure is the United States Department of Defense (DoD), who has 3.8 million smart card users as a result of its Common Access Card (CAC) program[3], an initiative motivated by HSPD-12. This presidential mandate hopes 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 by the end of 2007.

Global Smart Card Shipments By Sector (2006)

Sector	Memory (Millions of Units)	Microprocessor
Telecom	480	2040
Financial Services/ Retail/Loyalty	30	410
Government/Healthcare	250	90
Transportation	140	20
Pay TV		65
Corporate Security	15	15
Others	10	15
Total	925	2655
Aggregate Total	3580	

Source: www.EuroSmart.com

Global Smart Card Shipments By Sector (2007 Forecast)

Sector	Memory (Millions of Units)	Microprocessor
Telecom	440	2400
Financial Services/ Retail/Loyalty	30	490
Government/Healthcare	350	140
Transportation	160	30
Pay TV		70
Corporate Security	20	20
Others	10	15
Total	1010	3165
Aggregate Total	3580	

Source: www.EuroSmart.com

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 be in tune 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 thresholds are met. In the next section, we explore the practical implications of these requirements.

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

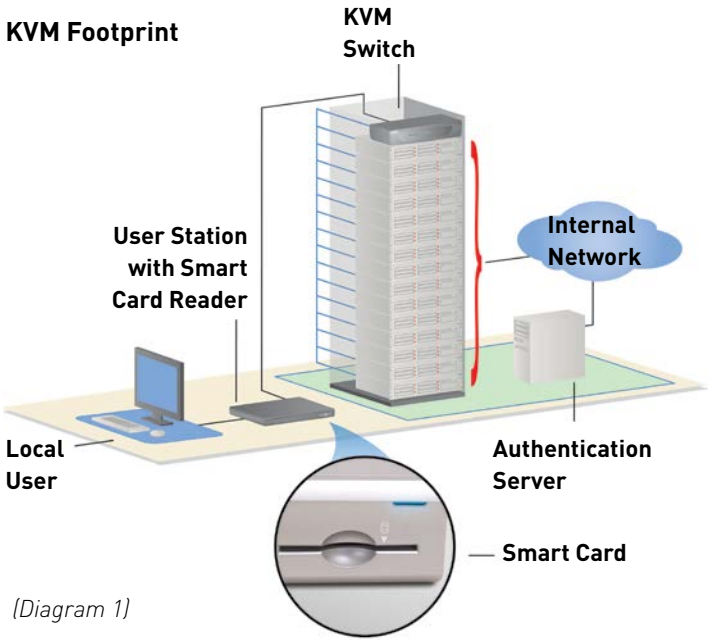
Components of a Smart Card-Enabled KVM Solution

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

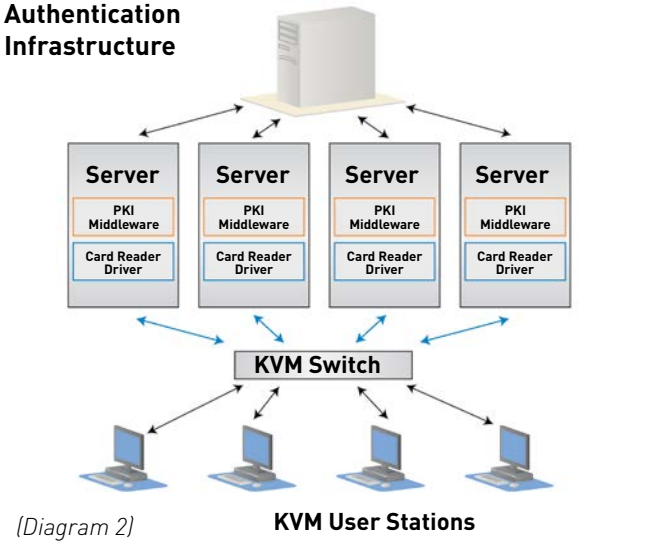
- Small dongles that attach to each server's I/O interfaces and emulate a keyboard, mouse, VGA monitor, and smart card reader. Servers then behave as if these peripherals were physically attached to their I/O ports. *(See Diagram 1)*
- Central, matrix KVM switch(es). Each dongle is connected to the KVM 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 compliments them with low-level device interfaces and APIs.

The components mentioned in Diagram 1 are part of the KVM footprint. 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 support 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. *(See Diagram 2.)*



(Diagram 1)



(Diagram 2)

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 smart card reader should be transparent to host computers.

Smart card readers, the middleware the readers interface with, and the authentication server that stores and manages user credentials each strictly follow industry specifications. For example, readers and server middleware utilize PC/SC as the communication protocol between them, and support x.509 certificates if their respective vendors choose to employ them. 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 an entire bank of servers, while only requiring a single smart card reader per user access point.

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 an analog KVM system provides a direct out-of-band connection between users and the servers to do so. No other infrastructure should be necessary besides what is already deployed for the servers themselves. The reader should interface with the target server exactly as if directly connected to one of its I/O ports. Specifically, in an analog/out-of-band KVM system, the card reader should not require connectivity to the authentication server or be on the network.

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 card reader utilized within a KVM system could open security holes 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:

- The KVM system should automate loss of authentication to a server when the user switches away from a particular KVM channel. 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 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.

- If configured as such within the server's smart card behavior settings, the card reader (and thus the KVM system) should support the automatic loss of authentication to the server upon removal of the card.
- Because the analog KVM system is out of band, unwarranted sniffing of the card's data via the corporate network is eliminated.

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 in to "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 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 integrate seamlessly 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 operates 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, a brand of Legrand, is a trusted provider of rack power distribution units, branch circuit monitors, transfer switches, environmental sensors, KVM-over-IP switches, serial console servers, and A/V solutions for data centers and IT professionals. Established in 1985 and based in Somerset, N.J., Raritan has offices worldwide serving customers in 76 countries. In more than 50,000 locations, Raritan's award-winning hardware solutions help small, midsize, enterprise, and colocation data centers to increase efficiency, improve reliability, and raise productivity. And provide IT departments with secure, reliable remote access tools needed to manage mission-critical environments. For more information, visit us at Raritan.eu.