



Best Practices When Enabling Smart Card Authentication in a KVM System

By Marissa Waddell, Derek Finch

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 touch-points provides. IT managers thus face a difficult decision: greater security or greater convenience.

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.

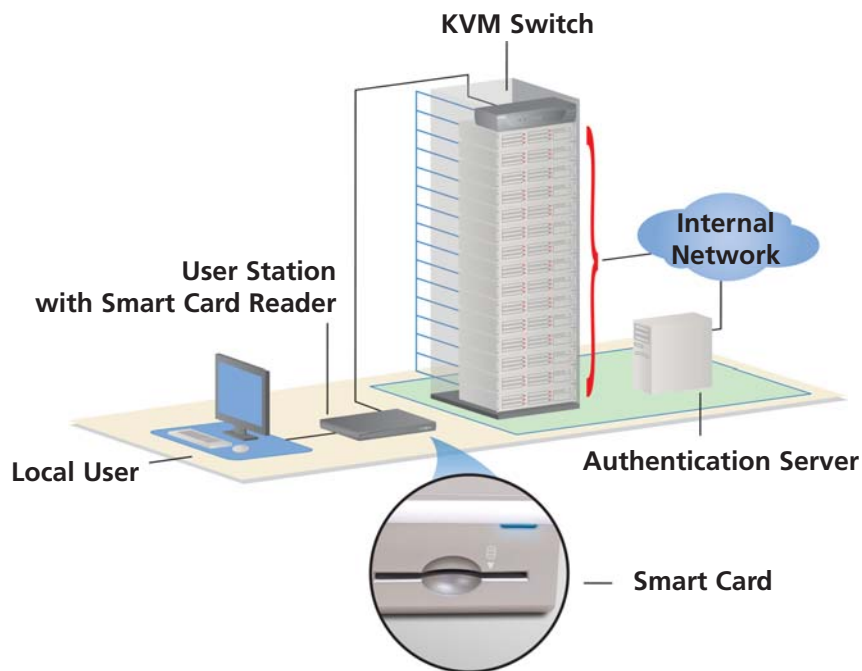
(Note that this white paper provides perspective on the benefits of enabling smart cards in an out-of-band ("analog") KVM system; and does not address an in-band ("networked", "digital") KVM-over-IP system.



Components of a Smart Card-Enabled KVM Solution

An analog KVM system with smart card support will include 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.
- ▶ Central, matrix KVM switch(es). Each dongle is connected to the KVM switch using standard Cat5/6 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 cables, 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 integrated or connected to each user station. 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 above 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) 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.

Solution Best Practices

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. As a result, today's smart card readers are essentially "plug-and-play", and this should hold true in a KVM solution.

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 user cards to the server, and an analog KVM system provides a direct out-of-band connection between users and the servers to do so. No additional infrastructure should be necessary.

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.

The solution should not store or cache smart card data, requiring a physical card to be present for any server access purposes.

A card reader utilized within a KVM system could open security holes if it performs data caching of any kind. Instead, the KVM system 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 at that discrete moment. 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.
- ▶ If 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 be left in the reader. 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.
- ▶ Because the analog KVM system is out of band, unwarranted sniffing of the card's data via the corporate network is eliminated.

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. Another 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.

Conclusion

Enabling users to employ smart cards to access servers should not be a daunting task, but in a data center it can be difficult to deploy without a KVM solution that integrates smart card capabilities. At the same time, implementing a seamless KVM solution with smart card features should not compromise security in any way. An ideal solution, therefore, supports the use of smart cards and integrates a card reader 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, while server administrators can adhere to security policies without losing the convenience and efficiency that a centralized KVM solution provides.

For additional information about this article, contact:

Marissa Waddell is a product marketing manager at Raritan, Inc. Marissa has twelve years of sales and product marketing experience in the IT industry. Email: marissa.waddell@raritan.com

Derek Finch is a product manager at Raritan, Inc. For over 15 years, Derek has introduced and managed an array of products and services at Raritan, Lucent, Telesciences and Fiberlink. Key areas of focus have included KVM, VPNs and billing mediation. Email: derek.finch@raritan.com

About Raritan

Raritan is a leading provider of management solutions that simplify IT operations. Based on KVM (Keyboard, Video, and Mouse) switches, serial console servers, management software, power management and remote connectivity, our secure solutions drive data center and branch office efficiency and productivity in more than 50,000 locations around the world. Raritan, Inc. is the thought leader in improving data center security and provides integrated smart card access in its Paragon II platform. Raritan has partnered with SCM Microsystems Inc., an industry leader in smart card readers and interface technology, to develop Paragon II's smart card reader solution.

Raritan's Paragon II KVM Smart Card Reader solution is ideal for government, financial and other organizations that want an additional layer of security provided by smart card user authentication for accessing IT resources. For more information, please visit www.raritan.info.

