

The Technology Authority for Government

GCNLAB

 Raritan®

# Uncommon smart-card control

## Raritan's new KVM switch balances security and convenience with a CAC reader

BY MICHELLE S. HAASE  
GCN CONTRIBUTING WRITER

**MAKERS OF INFORMATION** technology equipment often walk a fine line between security and convenience. If you make a product extremely secure, users might not be willing to jump through the hoops required to use it. But if you make it too convenient, security suffers — something especially unacceptable in the federal government.

Raritan has struck an excellent balance with its new Paragon II Smart Card Reader Solution, an analog keyboard-video-mouse with an integrated smart-card reader. The reader supports the Defense Department's Common Access Card and is the first smart-card reader for a KVM switch. Homeland Security Presidential Directive 12 mandates that DOD use CACs for access to federally controlled computer systems and facilities. The department has several million CACs in circulation at a given time.

The analog format increases security by allowing Paragon II to remain completely off the network. The reader provides the card data to the target server through the Paragon analog pathway.

The card reader authenticates users against a third-party external authentication platform before allowing access to servers, and the solution does not store or cache data on the card. It also requires new authentication from

the card when switching from one server to another, although users may leave the card in the reader.

When used with personal identification numbers — the typical configuration — the solution meets the new federal requirement for two-factor authentication.

Video is another important component of KVM switches, given the increased use of graphics and video-intensive computer programs. The problem with video is that its quality degrades as the distance between the computer and the switch increases.

The Paragon II system consists of a user station with an integrated smart-card reader from SCM Microsystems, one or more stackable switches and a Computer Interface Module for each connected server that requires smart-card or CAC authentication.

The switches are available in several models that allow different numbers of users and connected servers. We reviewed the P2-UMT832, which supports as many as eight users and 32 servers. The user station can be connected to stacked Paragon II switches and tiered switches. By stacking the switches, administra-

tors can use Paragon II to manage thousands of servers.

Our test configuration included the user station with smart-card reader, one switch and ActivClient middleware from ActivIdentity that emulated the authentication experience. Setup is plug-and-play with the exception of installing a smart-card driver on every server that requires a smart card to access it. We set up our test configuration in just a few minutes using the clear, step-by-step quick setup guide that included diagrams.

We connected two test computers to the Paragon II system. Hitting the Scroll Lock key twice in rapid succession brings up the Paragon On-Screen User Interface, a DOS-like list of connected servers that lets you select one to view by highlighting it and pressing the Enter key. When you insert a smart card into the slot, the LED on the user station flashes green while the station is reading the card data and glows

solid green when the data-reading process is finished.

We left the card in the slot when we switched between the computers. We had to enter a personal identification number each time we accessed a different computer, but the smart-card authentication was automatic as long as the card was still in the reader. It took the system about 13 seconds to read the card data and simulate authentication, and we could not switch to a different server during the data exchange process.

When you switch from one server to another, you lose your authentication to the server you're leaving. Once you install the user station, the entire Paragon II system enters private mode, which means that only one connected user at a time can access a server. This protects the data on the smart card and prevents unauthorized access. And when you're using a smart card, the scan function — which tells the system to scan through every system available to you at that point — is disabled.

The Paragon II Smart Card Reader Solution fills an important security gap in government data centers by requiring smart-card authentication for access to servers. The system is convenient and easy to use. ■

Raritan, (800) 724-8090,  
[www.raritan.com](http://www.raritan.com).



### GCNLAB TEST

#### RARITAN PARAGON II SMART CARD READER SOLUTION

**PROS:** VERY SECURE,  
SIMPLE TO USE.

**CONS:** A BIT EXPENSIVE,  
VIDEO QUALITY DEGRADES  
OVER DISTANCE.

#### PERFORMANCE: A

#### FEATURES: A

#### VALUE: B+

**PRICE:** \$1,185 for the  
P2-EUST/C user station,  
\$170 for each  
P2CIM-AUSB-C  
Computer Interface  
Module and \$6,000 for  
the P2-UMT832 switch.