Raritan
A brand of legrand

SOLUTIONS BRIEF

Remote Access and Control of SIPRNet Servers

The DoD Chief Information Officer Oct. 14, 2011 memo "DoD SIPRNet Public Key Infrastructure Cryptographic Logon and Public Key Enablement of SIPRNET Applications and Web Servers" mandates SIPRNET token authentication by mid-2013.

For effective intelligence work, secret and classified information often needs to be shared among government agencies, increasing the risk to national security if distributed in an unsecure manner. With the expansion of military and intelligence operations, the labor intensive nature of counterterrorism work, and new mandates for clearance and secrecy, greater effort is now required to ensure that government security standards are always met.

The Challenge

Remotely accessing and controlling a "secure network" can be quite daunting. The government data center or lab environment includes both internal and external networks such as the Internet, intranets, extranets, and demilitarized zones (DMZs). Centralized, secure remote access can improve the speed in which critical information is shared by minutes, hours and even days.

The Government Mandate

To ensure the secure transmission of classified and secret information, the U.S. Government has mandated that beginning in April, 2013 all access to military, intelligence, and other agency classified systems will require the use of a limited-access computer network Secret Internet Protocol Router Network (SIPRNet) token. This token will contain individual PKI certificates used for network logon, Web site authentication and secure e-mail.

Similar to the use of a common access card (CAC) for entry to non-classified systems, the SIPRNet token is a hardware token, cryptographically bound to the user's identity. The SIPRNet token doesn't have a picture, name, grade or service component listed.

Challenges

- Increase security of secret networks to address internal/external threats
- Provide secure, remote KVM access and control of SIPRNet classified systems
- Meet DoD mandates, including DoD schedule

Benefits

- Avoid travel to data center, computer room or lab
- Centralized, high speed access to multiple systems
- The Paragon SIPRNet solution has been tested in multiple environments
- Raritan's Paragon solutions have been supporting federal, state and local government/military customers for over 15 years

The Raritan Solution

Building upon the industry's first and most widely deployed CAC KVM solution, Raritan's Paragon II solution is an enterprise-class, Cat5 analog KVM solution that gives government IT professionals the power to securely access and control servers and other network devices.

Paragon II Provides:

- High speed, secure, out-of-band, BIOS-level remote access and control, including remote power control
- Non-blocked access for up to 64 simultaneous users, controlling more than 10,000 servers
- Support for SIPRNet hardware tokens and 90meter middleware
- Security tested in multiple SIPRNet test environments
- Consolidated view of all Paragon connected devices

Raritan's Paragon II Solution Includes:

Paragon UMT
Paragon II Cat5 Matrix Stacking Switch

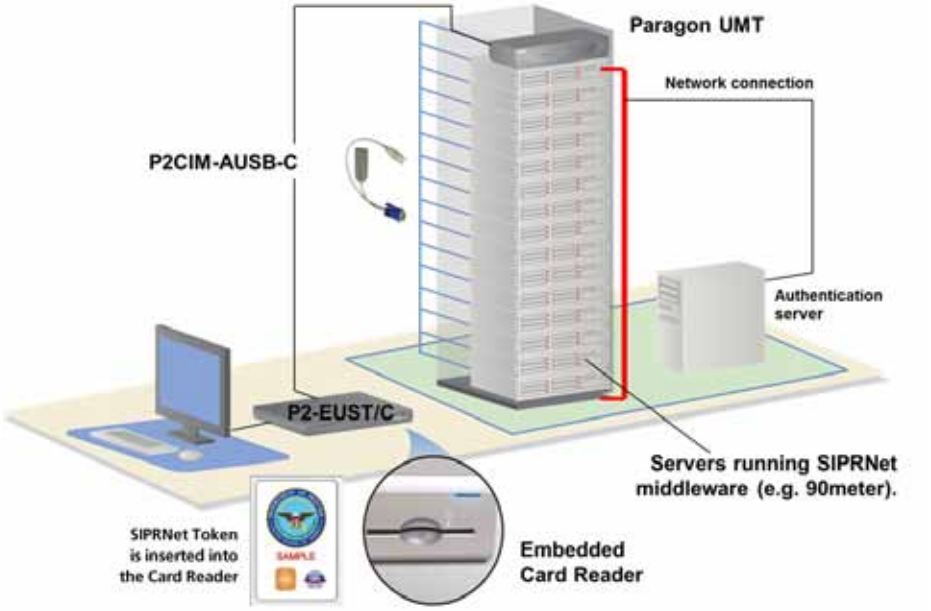
User Station (P2-EUST/C)

- Integrated Card Reader
- Support for SIPRNet cards

Paragon II Release 4.8.3 Software

CIM (P2CIM-AUSB-C) Firmware
CIM Firmware updated to support 90meter middleware

Raritan's Paragon II, centralized remote access and control including support for DoD-mandated SIPRNet token access to classified systems



Ready to find out more? Contact Raritan today.
Call 1.800.724.8090 or visit www.raritan.com

Raritan®
A brand of legrand®