ATEN
Simply Better Connections

Make the Strategic Choice to Beat Cybersecurity Threats

Secure KVM Switches with NIAP PSD PP v4.0 / PSS PP v3.0 Compliance for Secure Desktop Workstations in All Industries

CONTENTS

1. Cyber Threats Evolve as Interconnectivity Reigns

Cybersecurity is on everyone’s mind these days and with good reason: the economy’s shift to hybrid and remote work has created increasingly interconnected and collaborative infrastructures and these present significant opportunities for cyber criminals. While there were a number of high-profile breaches in 2021, such as Solar Winds and Colonial Pipeline, according to Forbes[1], it is perhaps most concerning that critical infrastructure, power grids, and supply chain security weaknesses were targeted and exploited by adversaries at much higher rates than in the past. This does not bode well for 2022.

It’s an ever-evolving threat that many organizations are unprepared to face, especially governments. However it’s in their best interest to establish robust cybersecurity measures, because in addition to the risk to incentives for innovation and investment, cybercrime is estimated to cost the world US$10.5 trillion annually by 2025. According to researchers at Cybersecurity Ventures[2], this represents the greatest transfer of economic wealth in history, and is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.

Hackers, from independent ones to terrorists and those working for foreign governments, are responsible for ransomware, distributed denial of service, and stealing of classified information, while most cybersecurity providers specialize in specific verticals, forcing customers to secure their data using a patchwork of different providers. This is already an uneven playing field, and cyber attacks are constant evolving. Welcome to the future of business warfare, fought safely from behind a keyboard.

[1] https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=562d389a6b61
[2] https://cybersecurityventures.com/cybersecurity-almanac-2022/

2. How Secure KVM Switches Can Help

It has long been understood that government agencies, while aware of the need to be more adaptive, still struggle with basic cybersecurity measures, from reusing older passwords on management accounts, to devices exposed to the public Internet. Internet of Things (IoT) devices are especially poorly managed, and thus exposed, often undetected by agencies. Simply put, out-dated protocols and a non-tech-savvy workforce have been leaving the door wide open for hackers, terrorists, and other cyber criminals. The good news is that all of these problems are relatively simple to solve. The key is to be proactive instead of reactive. Replacing legacy technology that has long since been figured out by hackers is one of the first things government agencies can do. But what about the next level of protection?

Physical & Digital Protection

Secure KVMs are a robust solution that can meet these cyber threats head-on. Security-reinforced KVM switches provide the means to consolidate multiple workstations of various security classification levels with a single keyboard, monitor, and mouse, also known as a KVM console. With hardware and software-based security features built into the units, military, intelligence, and federal agency installations can rest assured that their data is being protected on both physical and digital levels. And these are not just solutions for government organizations. Other applications can also reap the benefits.

For example, healthcare providers often need to switch between private patient data and non-sensitive information platforms for things like general insurance. And in the finance sector, the need for network separation between classified and non-classified computers is increasing as banks consolidate in multiple markets and extend their presence across borders. Secure KVM Switches provide a level of physical security right at the user console station to isolate networks and prevent any information from getting into the wrong hands. They are the desktop's last line of defense against internal threat actors.

> "Cybersecurity attacks are increasing each year. With this in mind, the government requires reassurance that if a peripheral sharing switch or KVM is compromised, no usable data can be stolen from the device. PSS certified products are required to ensure that data leakage will not occur when switching between ports or classified to unclassified computers. Our new PSD PP v4.0 Secure KVM Switch series limits the connection of devices at the desktop level, ensuring secure remote authentication and access that meet U.S. government and military mandates."
> Aaron Johnson, KVM Product Manager,
> **ATEN Technology, Inc., USA**

3. NIAP introduces PSD PP v4.0

When it comes to Secure KVM Switches, the National Information Assurance Partnership (NIAP) is the regulatory body responsible for the implementation of Common Criteria testing and certification, in partnership with the National Institute of Standards and Technology (NIST). NIAP serves as the U.S. representative in the 31 member nations of the Common Criteria Recognition Arrangement (CCRA). The purpose of this arrangement is ensure evaluation of IT products and protection profiles are performed to high and consistent standards and contributes significantly to confidence in the security of certified products. Since 2015, PSS PP v3.0 (Protection Profile for Peripheral Sharing Switch) has been the go-to certification for Secure KVM Switches for the international market.

But times changes and cybersecurity threats evolve. In 2020, NIAP introduced PSD PP v4.0 (Protection Profile for Peripheral Sharing Device) to reflect necessary updates to security requirements that were considered prudent by the US government. Constant re-evaluation and improvement is fundamental to staying ahead of cyber terrorism and crime, and this latest Protection Profile takes aim at many of the newer types of threat actors that have come to light in the last few years. Many of the current vulnerabilities are a direct the result of the global workplace hurtling towards improved efficiency and collaboration as a response to the COVID-19 crisis, and hackers took advantage of the resulting vulnerabilities and gaps in security by businesses. This is also why many agencies remain still unprepared.

NIAP for Trusted Secure KVM Certification

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product performance to international standards. The program, known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS), was implemented to help consumers and government agencies select commercial off-the-shelf IT products that meet their security requirements.

4. The ATEN Secure KVM Solution

ATEN has expanded its enterprise KVM solutions with the launch of a new series of Secure KVM switches. ATEN Secure KVM Switches are compliant with Common Criteria and NIAP Protection Profile (PSD PP v4.0, PSS PP v3.0) and specifically designed to enforce stringent desktop security by keeping sensitive assets isolated while providing advanced user data protection and flexible administrative security management features. They are suitable for deployment in any industry that needs to handle sensitive, confidential, or proprietary information, or implement multi-level security on separate networks, such as government and military agencies, healthcare providers, banking & finance institutions, and more.

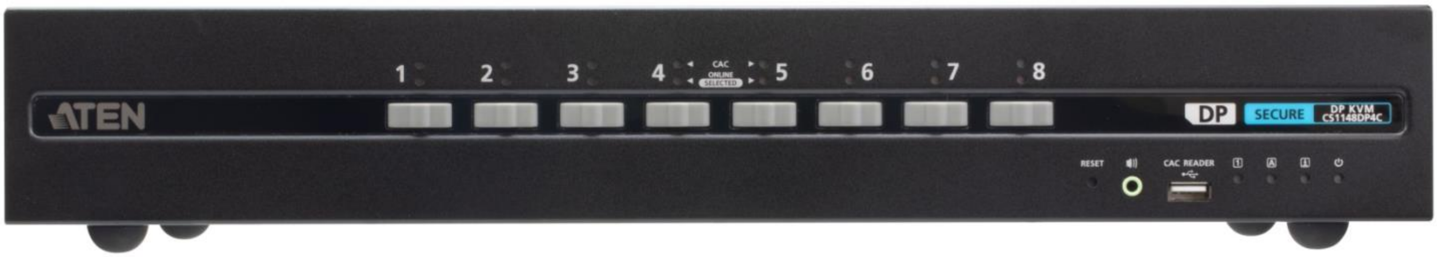
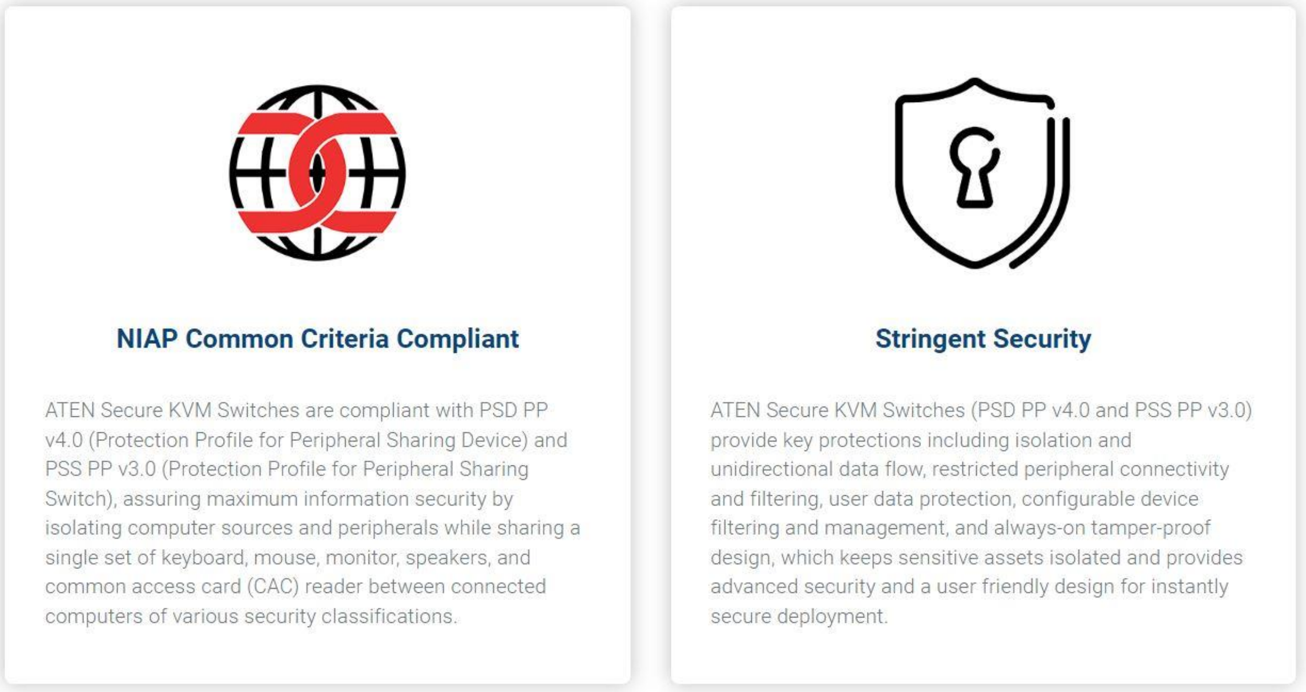


Fig 1: ATEN PSD PP v4.0 Secure KVM Switches control and isolate data flow between the console devices and connected computers.



NIAP Common Criteria Compliant

ATEN Secure KVM Switches are compliant with PSD PP v4.0 (Protection Profile for Peripheral Sharing Device) and PSS PP v3.0 (Protection Profile for Peripheral Sharing Switch), assuring maximum information security by isolating computer sources and peripherals while sharing a single set of keyboard, mouse, monitor, speakers, and common access card (CAC) reader between connected computers of various security classifications.

Stringent Security

ATEN Secure KVM Switches (PSD PP v4.0 and PSS PP v3.0) provide key protections including isolation and unidirectional data flow, restricted peripheral connectivity and filtering, user data protection, configurable device filtering and management, and always-on tamper-proof design, which keeps sensitive assets isolated and provides advanced security and a user friendly design for instantly secure deployment.

5. Key Protections from ATEN for Instantly Secure Deployment

The Secure KVM Series from ATEN meets all key security requirements. They are designed to keep sensitive assets isolated while providing advanced security and a user friendly design for instantly secure deployment.

Multi-Layer Security

- **Always-on chassis intrusion detection –** renders the ATEN Secure KVM Switch Series inoperable when physical tampering is detected
- **Tamper-evident labels –** provides visual indication of any attempt to access the ATEN Secure KVM Switch's internal components
- **Non-reprogrammable firmware –** prevents reprogramming the ATEN Secure KVM Switch's firmware
- **Restricted peripheral connectivity –** non-authorized HIDs (Human Interface Devices), video, or authentication device connections are rejected
- **Secure Port Switching –** Port selection via pushbuttons / Remote Port Selector (RPS) to enhance security (PSD PP v4.0 models only)
- **Clear LED Indications –** LED indications for peripheral filtering and KVM security status
- **Rugged metal enclosure**
- **Strict audio filtration –** protects against audio leakage (PSD PP v4.0 models only)

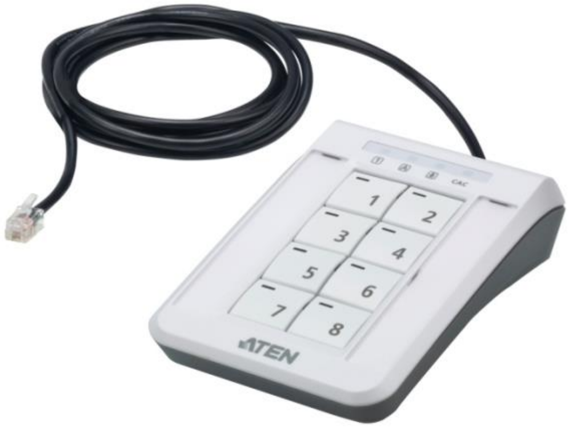


Fig 2: Thanks to its compact size, the ATEN PP4.0 Secure KVM Remote Port Selector (RPS) can be placed line-of-sight on the desktop, enabling instant switching across multiple PCs and optimizing productivity while eliminating cable clutter.

Data Channel Isolation and Unidirectional Data Flow

- True data path isolation – data cannot be transferred between computers
- The ATEN Secure KVM Switches control and isolate data flow between console devices and connected computers
- Unidirectional data flow between console devices and the selected computer is ensured
- Supports analog audio (speakers only)

User Data Protection

The keyboard/mouse data of ATEN Secure KVM Switches is automatically deleted after transmission and automatically purged when the KVM port focus is switched.

Security Management

- Supports administrative configuration of CAC Port filtering to accept or reject specific USB authentication devices (PSD PP v4.0 CAC models and PPS PP v3.0 models only)
- Supports administrative configuration of keyboard/mouse ports filtering to reject specific USB HID devices (PSD PP v4.0 models only)
- Provides administrative functions for authorized administrators to audit KVM log data
- The CAC function can be enabled/disabled by port (PSD PP v4.0 CAC models and PPS PP v3.0 models only)

Superior Video Quality

- **4K Image Quality**
  Supports image resolution up to 3840 x 2160 @60 Hz (with PSD PP v4.0 models) and 3840 x 2160 @30 Hz (with PSS PP v3.0 models)
- **Dual Display**
  Video outputs can be displayed on two monitors seamlessly.
- **ATEN Video DynaSync™**
  Exclusive ATEN technology eliminates boot-up display problems and optimizes resolutions when switching among different sources

6. PSS PP v3.0 versus PSD PP v4.0. What’s the Difference?

As previously mentioned, the main provisions of the latest PSD PP v4.0 profile reflect necessary updates to security requirements that are considered prudent by the US government and are the result of contact re-evaluation and improvements since 2015. For example, new video interfaces are allowed and video interface-specific protocols have been incorporated into the testing procedure, and there is stricter testing for audio filtration.

While PSD PP v4.0 models meet the very latest NIAP requirements for certification to U.S government standards, it is important to note that certified PSS PP v3.0 models still meet all the relevant requirements of their classification for the lifetime of the device, and remain an excellent and fully secure choice for many applications with less stringent concerns than government agencies.

Specifically for ATEN’s Secure KVM Switches, see the following table for the main differences between ATEN’s PSD PP v4.0 and PSS PP v3.0 models:

	PSD PP v4.0	PSS PP v3.0
Secure Port Selection	Pushbutton, Remote Port Selector (RPS)	Pushbutton
Strict Audio Filtration	✓	×
Configurable Device Filtration on Keyboard/Mouse Ports	✓	×
Non-CAC Model Available	✓	×
LED Indication for Unauthorized USB HID Connection	✓	×
4K UDH Video Quality	Up to 3840 x 2160 @60 Hz	Up to 3840 x 2160 @30 Hz

7. Case Study: ATEN Secure KVM Solutions in Action

Multi-Layered Cybersecurity Protection at the Desktop for Government Agency

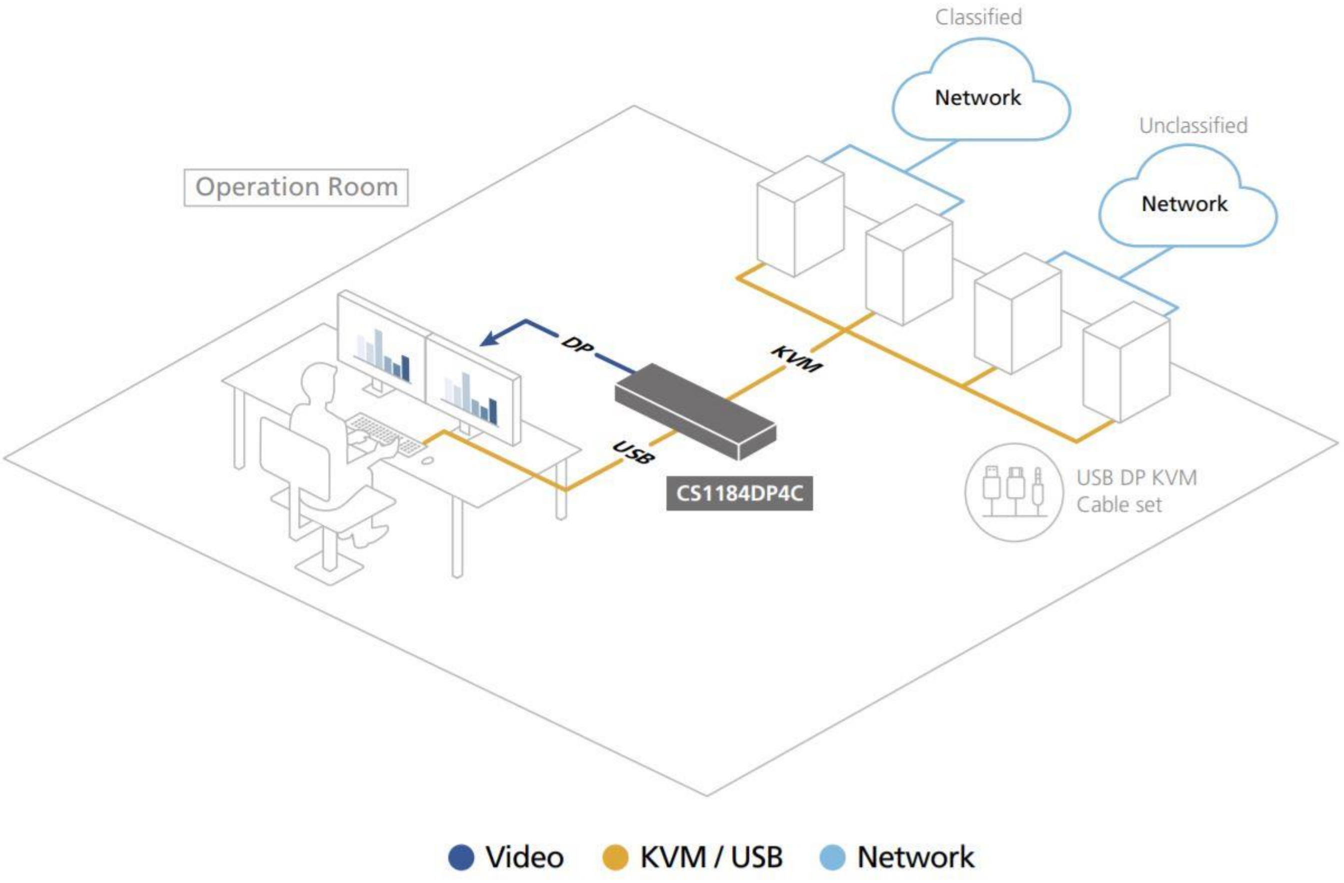
A large state-owned office building that houses various government branches was looking to shield their attack surface from threat actors and establish robust cybersecurity measures by consolidating multiple workstations of various security classification levels with a mix of single- and dual-monitor setups. While the desktop functionalities required were similar to a regular desktop KVM switch, the new solution needed to help guard against potential cyber attacks on the national infrastructure, such as power grids, by being completely unexploitable. It was therefore imperative that the solution provided true network separation between classified and non-classified data channels and complied with the latest international protection protocols.

Challenges:

- Minimize security threats by ensuring data integrity between user desktops accessing secure and unsecure networks
- Required channel isolation so that data cannot be transferred between computers
- Provide hardware and software-based security features
- Compliant with PSD PP v4.0 (Protection Profile for Peripheral Sharing Switch) security requirements

The ATEN Solution

The ATEN solution allows the government office to enforce stringent, multi-level security at the desktop by keeping sensitive assets isolated on separate networks while providing advanced user data protection and flexible security management features. With strict audio filtration, configurable device filtration on keyboard/mouse ports, chassis intrusion detection, and tamper-proof hardware coupled with layers of software security, the ATEN solution mitigates the vulnerabilities of a variety of cyber attacks on government IT infrastructure. ATEN Secure KVM Switches provide military-class security with multi-layered protection on both the physical and digital levels to combat data leakage across internal ports as well as to external networks.



8. Making the Right Secure KVM Choice with ATEN

For government & military agencies, healthcare providers, banking & finance institutions, and more, looking for true network separation between classified and non-classified, and compliance with the latest international protection protocols, ATEN Secure KVM Switches provide an ideal solution. With protection on both the physical and user operation levels to combat data leakage across internal ports as well as to external networks, which can mitigate the vulnerabilities of a variety of cyber attacks, ATEN Secure KVM Switches are the strategic choice for security-conscious desktop applications across all industries.

ATEN PSD PP v4.0 Secure KVM Switches

		2-Port		4-Port		8-Port	
	CAC	**Single Head**	**Dual Head**	**Single Head**	**Dual Head**	**Single Head**	**Dual Head**
DisplayPort	✓	CS1182DP4C	CS1142DP4C	CS1184DP4C	CS1144DP4C	CS1188DP4C	CS1148DP4C
	×	CS1182DP4	CS1142DP4	CS1184DP4	CS1144DP4	CS1188DP4	CS1148DP4
HDMI	✓	CS1182H4C	CS1142H4C	CS1184H4C	CS1144H4C	N/A	N/A
	×	CS1182H4	CS1142H4	CS1184H4	CS1144H4	N/A	N/A
DVI	✓	CS1182D4C	CS1142D4C	CS1184D4C	CS1144D4C	CS1188D4C	CS1148D4C
	×	CS1182D4	CS1142D4	CS1184D4	CS1144D4	CS1188D4	CS1148D4

ATEN PSS PP v3.0 Secure KVM Switches

		2-Port		4-Port		8-Port	
	CAC	**Single Head**	**Dual Head**	**Single Head**	**Dual Head**	**Single Head**	**Dual Head**
DisplayPort	✓	CS1182DP	CS1142DP	CS1184DP	CS1144DP	CS1188DP	CS1148DP
HDMI	✓	CS1182H	CS1142H	CS1184H	CS1144H	CS1188H	CS1148H
DVI	✓	CS1182D	CS1142D	CS1184D	CS1144D	CS1188D	CS1148D

For more information about ATEN's PSD PP v4.0 / PSS PP v3.0 Secure KVM Switches, please visit https://www.aten.com/global/en/products/kvm/secure-kvm-switches/