Do You Need CAC for Secure Access?

Seamless, secure authentication for sensitive networks using CAC and SKVMs.

See reverse for use case graphics.

As part of a broader cybersecurity strategy, many government and military agencies, utility, healthcare, and financial organizations mandate using Common Criteria or NIAP-compliant Secure KVMs (SKVMs) at operator stations to isolate sensitive systems. The Common Criteria and NIAP certifications are internationally recognized standards that validate the security functionality of information technology products. Secure KVM switches physically isolate networks, ensuring that the most sensitive and mission-critical data is only accessible to those with tightly controlled permission. By meeting these standards, SKVMs ensure the highest level of data protection and secure communication in sensitive environments.

Many secure networks are enabled with a Common Access Card (CAC), also known as Personal Identity Verification (PIV) or Public Key Infrastructure (PKI) token, which is an encrypted smart card that provides rapid identification in the most secure environments. A CAC is inserted into a CAC reader for authentication. A PKI token is the principal form of access to the Department of Defense computer networks and systems. These smart cards offer two-factor authentication, ensuring that users not only possess the card but also know the associated credentials, providing a much higher level of security than traditional login methods.

Belkin offers US-manufactured and TAA-compliant SKVMs with and without a Dedicated Peripheral Port (DPP) to support a CAC reader. The DPP allows for streamlined user authentication processes by reducing the need for multiple CAC readers, improving both security and user efficiency in multi-classification environments. Belkin SKVMs with a CAC port include a unique front-panel mode, equipped with CAC freeze to allow a user to lock a CAC on a given channel while using another channel for keyboard, mouse, and video. The same capability is replicated on the Belkin SKVM Remote Control with Integrated Keyboard.

Belkin also offers SKVMs without a dedicated CAC port. Use cases and security protocols that require the DPP to be blocked and a CAC reader connected directly to each host, bypass the SKVM. In this case, if a user has access to four networks, a CAC reader is connected to each of the four networks, resulting in four CAC readers at the workstation.

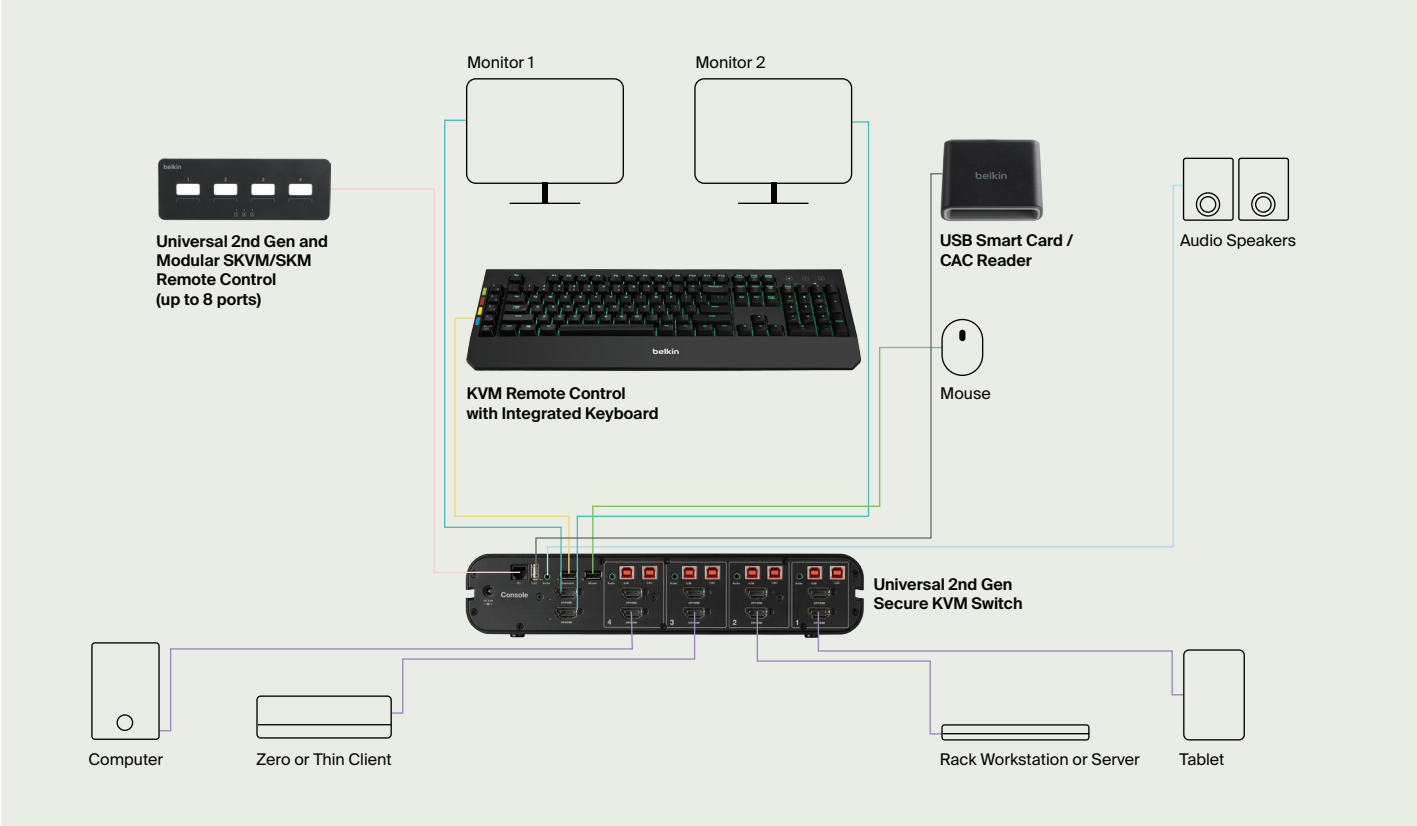
For organizations requiring maximum security and flexibility, SKVMs with DPP provide centralized CAC management across multiple networks. On the other hand, for environments with strict security protocols that mandate isolated access, SKVMs without DPP offer a more distributed solution by requiring a CAC reader for each network.

(continued on next page)

Use Case #1

CAC reader connected directly to the SKVM

SKVM includes a dedicated CAC. The dedicated CAC port is a shared resource, allowing a single reader to be shared across all connected systems for user authentication at the same level of classification.



Universal 2nd Gen Secure KVM Switch (up to 16 hosts)

F1DN204KVM-UN-4 (pictured)
F1DN104KVM-UN-4
F1DN208KVM-UN-4
F1DN108KVM-UN-4
F1DN202KVM-UN-4
F1DN102KVM-UN-4
F1DN116KVM-UN-4
F1DN216KVM-UN-4

KVM Remote Control with Integrated Keyboard

F1DN008KBD (pictured)

Universal 2nd Gen and Modular SKVM/SKM Remote Control (up to 8 ports)

F1DN-MOD-REM2
F1DN-MOD-REM4 (pictured)
F1DN-MOD-REM8

USB Smart Card / CAC Reader

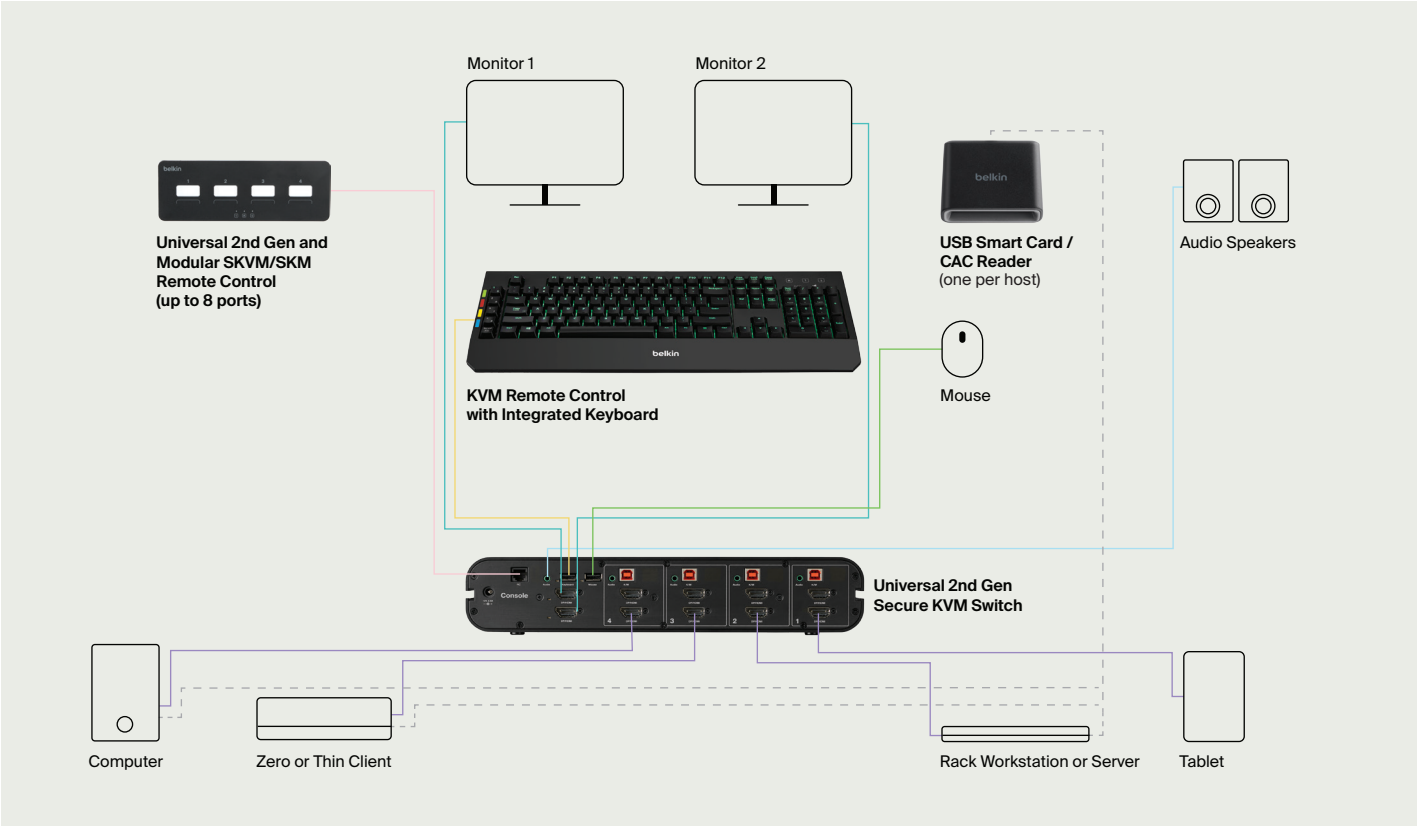
F1DN005U (pictured)
F1DN008U

(continued on next page)

Use Case #2

CAC reader is connected directly to the host, bypassing the SKVM

SKVM excludes a dedicated CAC port. CAC reader is connected directly to the host for user authentication.



Universal 2nd Gen Secure KVM Switch (up to 16 hosts)

F1DN204KVM-UNN-4 (pictured)
F1DN104KVM-UNN-4
F1DN208KVM-UNN-4
F1DN108KVM-UNN-4
F1DN202KVM-UNN-4
F1DN102KVM-UNN-4
F1DN116KVM-UNN-4
F1DN216KVM-UNN-4

KVM Remote Control with Integrated Keyboard

F1DN008KBD (pictured)

Universal 2nd Gen and Modular SKVM/SKM Remote Control (up to 8 ports)

F1DN-MOD-REM2
F1DN-MOD-REM4 (pictured)
F1DN-MOD-REM8

USB Smart Card / CAC Reader

F1DN005U (pictured)
F1DN008U

For more information, including data sheets on Belkin SKVMs with and without CAC ports, and CAC readers, visit our landing or resource page.

Belkin.com/cybersecurity | Belkin.com/cybersecurity/resources

Belkin International, Inc.
555 S Aviation Blvd, Suite 180
El Segundo, CA 90245-4852
USA
(310) 751-5757

Support
Secure SKVM/SKM Support
800-282-2355

Sales
FederalBusinessDivision@belkin.com

LinkedIn:

Learn more:

M121 1024REVA