EMERALD IP KVM PLATFORM

FIPS 140-3 LEVEL 1

Powered by Validated Cryptographic Technology

Featuring a FIPS 140-3 Level 1 Validated Cryptographic Module (CMVP Certificate #5002)

FIPS 140-3 VALIDATED CRYPTOGRAPHY FOR MISSION-CRITICAL ACCESS & CONTROL

Emerald IP KVM now incorporates a FIPS 140-3 Level 1 validated cryptographic module (CMVP Certificate #5002) to help protect data in transit across mission critical environments. By leveraging validated encryption technology, Emerald delivers enhanced security and confidence for government, defense, transportation, broadcast, and other control room applications where secure access and control are essential.

WHAT FIPS 140-3 VALIDATION MEANS

Incorporates a FIPS 140-3 Level 1 validated cryptographic module (CMVP Certificate #5002)

Uses AES 256 encryption and TLS 1.3 secure communications to protect KVM and management traffic

Employs validated cryptographic technology independently verified against U.S. government security standards

Includes cryptographic self-tests and key protection mechanismis to help maintain operational integrity

Delivers trusted encryption for government, defense, transportation, energy, and other mission-critical environments

Why this matters:
Federal, defense, and critical infrastructure organizations increasingly require trusted cryptographic protection to secure sensitive data and operations. By leveraging a FIPS 140-3 Level 1 validated cryptographic module (CMVP Certificate #5002), Emerald provides encryption based on technology that has been independently validated against the U.S. government's current cryptographic standard. For procurement teams, security architects, and compliance officers evaluating KVM infrastructure, this offers greater confidence than solutions that rely solely on vendor claims of being "FIPS capable" or "FIPS ready."

KEY PROOF POINTS

- ✓ Leverages a FIPS 140-3 Level 1 cryptographic module (CMVP Cert #5002
- ✓ Trusted encryption technology independently validated to U.S. government cryptographic standards
- ✓ AES 256 encryption secures all KVM and management communications
- ✓ TLS 1.3 secure session establishment and encrypted data transport

Emerald PE Transmitter uses FIPS 140–3 level 1 validated cryptography

VALIDATED PRODUCTS

PRODUCT	SKUS	VALIDATION LEVEL
Emerald SE Receivers Standard Edition KVM Receivers, single & dual-head	EMD2000SE-R EMD2002SE-R EMD2000SE-DP-R EMD2002SE-DP-R	FIPS 140-3 Level 1
Emerald PE Receivers Performance Edition KVM Receivers, single & dual-head	EMD2000PE-R-P EMD2002PE-R-P EMD2000PE-DP-R EMD2002PE-DP-R	FIPS 140-3 Level 1
Emerald 4K / 4K2 Receivers 4K KVM receivers	EMD4000R EMD4100R	FIPS 140-3 Level 1
Emerald SE Transmitters Standard Edition KVM Transmitters, single & dual-head	EMD2000SE-T-R2 EMD2000SE-DP-T EMD2002SE-DP-T	FIPS 140-3 Level 1
Emerald PE Transmitters Performance Edition KVM Transmitters, single & dual-head	EMD2000PE-T-R2 EMD2002PE-T-R2 EMD2002PE-T-P EMD2000PE-DP-T EMD2002PE-DP-T	FIPS 140-3 Level 1
Emerald 4K / 4K2 Transmitters 4K KVM transmitters	EMD4000T EMD4100T	FIPS 140-3 Level 1

***Independent testing covers FIPS 140-3 Security Level 1 across all 20 SKUs, evaluated under the same third-party lab engagement. Boxilla manager is not included in this testing scope.*

COMPLIANCE SCOPE

FRAMEWORK	REQUIREMENT	HOW EMERALD QUALIFIES
FISMA / FedRAMP	***Validated Cryptography***	FIPS 140-3 Level 1 Testing & Verification satisfies SC-13 control and federal encryption mandate
CMMC 2.0	***SC.3.177 Control***	Closes the cryptographic validation gap in Level 2 assessments, avoids 3-to-5 point scoring deduction
FBI CJIS	***Encryption Policy***	FIPS-validated AES-256 encryption meets CJIS security policy requirements for CJI data protection

Testing & Verification covers FIPS 140-3 Security Level 1. Also applicable to DFARS 252.204-7012, NIST 800-171, and IRS Publication 1075 requirements.

TARGET VERTICALS

Supported across 20 Emerald transmitter & receiver models

Government & Defense
Federal agencies, DoD, defense contractors handling CUI — FISMA, CMMC 2.0, and FedRAMP require validated encryption

Transportation & ATC
FAA NextGen modernization, airport operations, ATC facilities — critical infrastructure cybersecurity mandates

Public Safety & PSAP
911 call centers, EOCs, law enforcement dispatch — FBI CJIS policy requires FIPS-validated encryption for CJI access

Utilities & Media
NERC CIP OT/SCADA remote access, power grid NOCs, broadcast enterprise security policy requirements

FCC Part 15 | CE | RoHS 3 | FIPS 140-3 Level 1 | TAA Compliant

INDEPENDENTLY VALIDATED CRYPTOGRAPHY
FIPS 140-3 Validated Module

Emerald incorporates a FIPS 140-3 Level 1 validated cryptographic module (CMVP Certificate #5002), providing encryption technology independently validated to U.S. government cryptographic standards.

TRUSTED ENCRYPTION ASSURANCE
Beyond "FIPS Ready"

Unlike solutions that rely on self-attested security claims, Emerald leverages a cryptographic module that has been independently validated through the NIST Cryptographic Module Validation Program (CMVP).

PREPARE FOR FIPS 140-2 TRANSITION
Ready for Modern Security Requirements

With FIPS 140-2 validations approaching retirement, organizations evaluating secure KVM infrastructure can deploy Emerald with confidence using FIPS 140-3 validated cryptographic technology.

ENCRYPTION ACROSS EVERY SESSION
AES-256 + TLS 1.3 Protection

Emerald secures keyboard, video, mouse, audio, USB, and management communications using AES-256 encryption and TLS 1.3 secure communications, powered by a FIPS 140-3 Level 1 validated cryptographic module across 20 supported Emerald transmitter and receiver models.