SerialSpillway: Security, compliance & standards

What SerialSpillway's cryptography is validated against, which operating environments that covers, and how the product aligns with the frameworks an auditor is likely to ask about, including where that alignment stops.

At a glance

- **Unidirectional by physics, not by policy.** The sender drives an optical transmitter; the receiving end carries only an optical receiver. There is no emitter at the receiving end, so a return path does not exist to be enabled. The fiber also gives galvanic isolation.
- **No network stack on the data path.** Transfer rides a raw serial link: no TCP/IP, no listening port, and no routable attack surface between the two zones.
- **FIPS 140-3 validated cryptography.** All cryptographic operations run through the OpenSSL FIPS Provider 3.1.2, a validated module (NIST CMVP certificate #4985), operated in approved mode.
- **Encrypted administration channel.** TLS 1.3 only, pinned to the single ciphersuite TLS_AES_256_GCM_SHA384, external PSK with an ECDHE key share for forward secrecy. TLS 1.2 and below are not compiled into the accepted configuration.
- **Configuration encrypted at rest.** AES-256-GCM authenticated encryption, under a per-instance key the engine mints on the device at first start.
- **Signed licensing.** ECDSA P-256 with SHA-256, validated through the same FIPS crypto boundary as everything else.
- **Framework alignment, documented and self-attested.** IEC 62443 zone-and-conduit, NERC CIP, NIST SP 800-53 (SC-7 boundary protection), NIST SP 800-82, CMMC, NRC RG 5.71, TSA security directives, and EU NIS2 / UK NCSC CAF / Australia SOCI.

> Every claim above is set out in full, with the evidence behind it and the limits on it, in the sections that follow.

FIPS 140-3 validated cryptography

Embedded validated module: OpenSSL FIPS Provider 3.1.2, NIST CMVP certificate #4985, operated in approved mode. The module is validated; the product has not undergone its own CMVP validation. Read with **Operating environments** below.

SerialSpillway uses **FIPS 140-3 validated cryptography**: an embedded validated module, the **OpenSSL FIPS Provider 3.1.2**, **NIST CMVP certificate #4985**, operated in approved mode. All cryptographic operations in the product are performed through that module.

The precise distinction, because it matters to an auditor: the module is validated. SerialSpillway as a product has not undergone its own CMVP validation, and this page does not claim that it has.

How the module is integrated

- **Strict, fail-closed loading.** The module is explicitly loaded at service start and its integrity self-test must pass. If it is missing, damaged, or tampered with, the service enters a crypto_error posture: the data path and all cryptographic functions are disabled, and the management channel drops to a plaintext read-only diagnostic mode, where status and logs remain visible and every connection is logged with a warning. **There is no silent fallback to non-validated cryptography, anywhere.**
- **A single cryptographic boundary.** One internal module is the sole gateway to OpenSSL. No other code path touches a cryptographic primitive, which is what keeps the approved-algorithm boundary auditable.

Operating environments: tested vs. ported

SerialSpillway ships on **ported** environments, not CMVP-tested ones. That does not weaken the approved-algorithm claim, but a regime requiring the **tested** configuration specifically is **not** satisfied by a ported one.

A CMVP certificate validates a module **as tested on specific operating environments**, each named on the certificate. Certificate #4985's tested environments are Ubuntu Linux 22.04.1 Server, Debian 11.5, FreeBSD 13.1 and Windows 10 Pro on Intel x86-64, plus macOS 11.5.2 on Apple M1 and on Intel, each listed twice, once with and once without processor algorithm acceleration.

SerialSpillway runs the module on the environments below. How far each sits from a tested one differs, so they are stated separately rather than averaged:

Shipped environment	Relationship to the certificate's tested environments
Windows, x86-64	**Same OS family and architecture as a tested environment** (Windows 10 Pro, Intel x86-64).
Linux, x86-64 (glibc 2.35+)	**Same OS family and architecture as two tested environments** (Ubuntu 22.04.1 Server and Debian 11.5, Intel x86-64).
Linux, aarch64 (glibc 2.36+, including 64-bit Raspberry Pi OS)	Tested OS family (Debian), but **no Linux/ARM64 combination appears on the certificate**. The nearest tested ARM64 environment is macOS on Apple M1.

What this does not change

The approved-algorithm claim is unaffected. Which algorithms the module implements, and that SerialSpillway operates it in approved mode with no fallback to non-validated cryptography, are properties of the module's behavior, not of the host it runs on. That holds identically on every environment above.

What it does change: one word

These environments are **ported**, not **tested**. The CMVP's rules for this are in the FIPS 140-3 CMVP Management Manual, Section 7.9, Vendor or User Affirmation of Modules. Certificate #4985 is an overall Level 1 module, and for a Level 1 operating environment Section 7.9.2 provides that a software module “will remain compliant with the FIPS 140-3 validation on any general-purpose platform/processor that supports the specified operating system listed on the validation entry, or another compatible operating system.”

Where the module is built from source, the same section permits it on two conditions, **both of which are met**: the source is unmodified upstream, verified by GPG signature against OpenSSL's published signing keys, with no SerialSpillway code inside the module boundary, and the module's own Security Policy supplies the build method followed.

> **Whose affirmation this is: ours, as the integrator.** Certificate #4985 lists **no** vendor-affirmed operating environments, and a vendor affirmation in the CMVP sense is something only the module's own vendor can file. Nothing on this page should be read as an OpenSSL affirmation, or as an extension of the certificate.

What the CMVP itself says about ported environments, quoted rather than paraphrased: the CMVP “makes no statement as to the correct operation of the module or the security strengths of the generated keys” when a module is ported to an environment not listed on its certificate. That is the CMVP's position on every ported deployment, this one included.

What was done instead, since the CMVP does not speak to it

The assurance on these environments is ours to demonstrate, so:

- The module's integrity check and power-on self-tests pass on every shipped platform, and failure is fail-closed (data path disabled, cause logged) rather than a silent fallback to unvalidated code.
- **On aarch64, the platform furthest from a tested environment and so the one carrying the most of our own evidence, both sides of the certificate's processor-acceleration split are green from the single shipped artifact.** It is built on a processor without the ARMv8 cryptographic extensions, then self-tested on a board without them, on a board with them, and a third time on that board with those code paths forced off, so neither dispatch path is inferred from the other.
- **Cross-architecture operation is measured, not assumed.** File transfer between x86-64 and aarch64 hosts has been verified in both directions with a byte-exact accounting ledger, zero corrupt or discarded packets, and output files bit-identical to their originals.

> **The limit of this position, stated plainly.** A procurement or accreditation regime that requires the **tested** configuration specifically, the exact operating environment named on the certificate, is **not** satisfied by a ported one. Customers subject to one should raise it with us before purchase.

Approved algorithms in use

TLS 1.3 only on the management channel, AES-256-GCM at rest and for config sync, ECDSA P-256 for licensing. No legacy protocol versions and no negotiable downgrade.

Function	Algorithm
Management channel	TLS 1.3 only, single ciphersuite TLS_AES_256_GCM_SHA384, external PSK with psk_dhe_ke. A P-256 ECDHE key share provides forward secrecy
Configuration at rest	AES-256-GCM authenticated encryption
Config sync over the serial link	AES-256-GCM authenticated encryption under a pairing key
License signing	ECDSA P-256 with SHA-256
Hashing / key derivation	SHA-256, HKDF-SHA256 (RFC 5869)

No legacy protocol versions and no negotiable downgrade. TLS 1.2 and below are not compiled into the accepted configuration, and the ciphersuite list is pinned to exactly one AEAD suite.

IEC 62443 alignment

Documented design alignment, self-attested. No third-party IEC 62443 certification of the product has been performed. Covers 4-2 component requirements and 3-3 system requirements.

> **Documented design alignment, self-attested.** No third-party IEC 62443 certification of the product has been performed. Formal certification is tracked but not held.

SerialSpillway is designed against the component-level requirements of **IEC 62443-4-2** and supports system-level claims under **IEC 62443-3-3**.

IEC 62443-4-2: component requirements

Requirement	How SerialSpillway meets it
CR 1.2: Software process identification & authentication	Every management connection must complete a TLS 1.3 PSK handshake proving possession of a per-instance key held in an OS-permission-locked directory. A process that cannot read the key cannot authenticate.
CR 2.8: Auditable events	Every successful management handshake is logged with client process ID and process path; every configuration change is logged as a change event with old and new values. **Roadmap: RFC 5424 syslog forwarding to SIEMs is in active development and is not shipped.**
CR 3.1: Communication integrity	Management traffic uses TLS 1.3 AEAD. Config sync over the serial link uses AES-256-GCM authenticated encryption. A tampered or mis-keyed push is rejected with a logged warning, never applied. File transfer payloads carry CRC32 packet and whole-file verification with automatic discard of corrupt packets.
CR 4.1: Confidentiality in transit	The management channel is TLS 1.3 encrypted; config-sync pushes are AES-256-GCM encrypted.
CR 4.2: Confidentiality at rest	The service configuration is stored encrypted (AES-256-GCM) under a per-instance key minted by the engine on first boot. Plaintext configuration files are rejected as tampering once the instance is initialised.

IEC 62443-3-3: system requirements

Requirement	How SerialSpillway supports it
SR 3.1 / SR 3.4: Communication & software integrity	System-level equivalents of CR 3.1 above; cryptography is provided by a FIPS 140-3 validated module, satisfying the “use of cryptography in accordance with applicable standards” clause.
SR 5.x: Restricted data flow / zone segmentation	The core function: optically enforced unidirectional data flow between zones (transmitter, fiber, receiver, with no emitter on the receive side), and no software-defined reverse path to misconfigure.
SR 6.1: Audit log accessibility	Local structured logs with OS-permission gating: administrators only on Windows, a dedicated group on Linux. **Roadmap: a direct SIEM feed is in active development and is not shipped.**

NERC CIP alignment

Documented design alignment, self-attested. No third-party certification against NERC CIP has been performed. Covers CIP-005, CIP-007 and CIP-010.

> **Documented design alignment, self-attested.** No third-party certification of the product has been performed against NERC CIP.

- **CIP-005: Electronic Security Perimeter.** NERC CIP explicitly recognizes unidirectional gateways as an acceptable ESP control. SerialSpillway's optically isolated one-way link is precisely that control.

- **CIP-005-6 R2: Interactive Remote Access.** The local management leg is itself TLS-encrypted and authenticated, so a remote management path is encrypted end to end with no plaintext gap on the box.
- **CIP-007-6 R4 / R5: Security Event Monitoring and Access Control logging.** Management-channel authentication events and configuration changes are logged with actor identification: process ID and process path. **Roadmap: RFC 5424 syslog forwarding to SIEMs is in active development and is not shipped.**
- **CIP-010-4 R1: Configuration Change Management.** The baseline configuration is protected against unauthorized modification: it is stored AES-256-GCM sealed, writable only through the authenticated management channel, and every change produces a logged change record. On-disk tampering fails authentication and is rejected visibly: the service enters a flagged error state rather than loading altered settings.

Additional framework alignment

Documented design alignment, self-attested. No certification pursued at this stage. Covers NIST SP 800-82 and 800-53, CMMC, NRC RG 5.71, TSA directives, and NIS2 / NCSC CAF / SOCI.

> **Documented design alignment, self-attested.** No certification has been pursued against any of the following at this stage.

- **NIST SP 800-82** (OT/ICS security guide): unidirectional gateways are a recognized boundary-protection control; SerialSpillway's architecture and terminology map directly.
- **NIST SP 800-53** supports the AC (access control), AU (audit), SC (system and communications protection: SC-7 boundary protection, SC-8 transmission confidentiality and integrity, SC-28 protection of information at rest) and CM (configuration management) control families.
- **CMMC**: one-way transfer out of, or into, a CUI enclave maps to several Level 2 controls; audit logging supports AU.L2-3.3.1 and AU.L2-3.3.2.
- **NRC RG 5.71** (nuclear): explicitly names unidirectional gateways as an acceptable control for data flowing out of higher-security levels.
- **TSA Security Directives** (pipeline): supports the mandated OT/IT segmentation controls.
- **EU NIS2, UK NCSC CAF, Australia SOCI**: the same segmentation and boundary-protection value proposition for international critical infrastructure operators.

Defense in depth

On-device key generation, per-instance isolation, two-layer management access control, first-trust pairing with tamper-evident lockout, and fail-visible behavior throughout.

Details that distinguish the engineering, beyond the headline claims:

- **Keys are minted on-device and never leave it.** Each instance's keys are generated by the engine itself on first start and stored in a directory locked to the service identity: tight ACLs on Windows, owner and group permissions on Linux. Installers never loosen those permissions.
- **Per-instance isolation.** Every service instance has its own keys, its own sealed configuration, its own management endpoint and its own log files. A compromise or misconfiguration of one instance does not bleed into another.
- **Two-layer management access control.** Before TLS is even attempted, the operating system gates the transport: the Windows named pipe admits administrators only, and the Linux socket requires membership of a dedicated service group. The TLS PSK handshake is the second, cryptographic layer.
- **First-trust pairing with tamper-evident lockout.** Config sync between sender and receiver uses a supervised one-time pairing, or fully out-of-band key carriage by removable media for strict sites. A receiver that has ever held a key **rejects** a different key with a security warning, and a key that disappears puts the receiver into a loud held state requiring a deliberate operator reset. A missing key is treated as possible tampering, not as an invitation to

re-trust.

- **Every failure is visible.** Key mismatch becomes a logged rejection with the old settings kept. Config tamper becomes a flagged error state with defaults loaded. Module failure becomes a read-only diagnostic mode with warnings on every connection. Nothing degrades silently.
- **License integrity.** Licenses are ECDSA P-256 signed files bound to the hardware serial numbers of the adapter pair, validated through the same cryptographic boundary as everything else.
- **Transfer reliability on a one-way link.** Because a diode cannot acknowledge, SerialSpillway ships configurable redundant transmission with automatic receiver-side deduplication, plus CRC32 packet and file verification: availability and integrity engineering that acknowledges the physics of unidirectional transfer.
- **Upgrade-safe key handling.** Reinstalls rotate the management key automatically, preserve the configuration key, and prompt before touching any file that would destroy operator state. The validated module's artifact set is always replaced as a matched unit, so its integrity check remains valid.

SerialSpillway incorporates the OpenSSL FIPS Provider, a FIPS 140-3 validated cryptographic module (NIST CMVP certificate #4985), operated in approved mode. The module is used as validated, without source modification; the operating environments SerialSpillway ships on are ported rather than CMVP-tested configurations, which does not affect the approved-algorithm claim. Statements regarding IEC 62443, NERC CIP, NIST, CMMC, and other frameworks describe design alignment intended to support customers' own compliance programs; they do not constitute third-party certification of the product. Compliance obligations rest with the deploying organization; consult the referenced standards and your auditors for applicability.