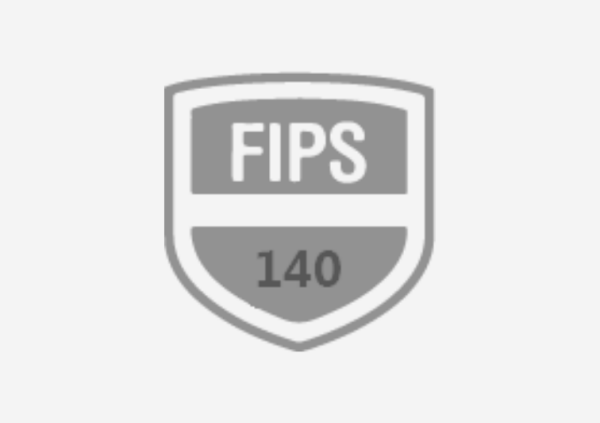
FIPS 140-3 Certification

FIPS 140-3 is a US and Canadian government co-sponsored security standard that specifies security requirements for cryptographic modules in hardware, software and firmware solutions. Crypto devices used by US and Canada Federal agencies to process Sensitive but Unclassified information must complete a FIPS 140-3 validation of their technology.



FIPS 140-3 (based on ISO 19790) is also widely accepted internationally as a benchmark certification for cryptographic implementations, providing a competitive edge and client trust on your product security features.

Thanks to our extensive experience, growing capacity and our custom automation tooling, we can speed up and optimize the entire validation process. Our qualified personnel and management team have collectively completed hundreds of successful FIPS 140 validations.

Reliable FIPS 140-3 Certification at your fingertips

Our FIPS 140 test validation lab has NVLAP (Lightship Security Inc. - Lab Code 600207) accreditation and is an approved lab under the Cryptographic Module Validation Program (CMVP). We have specialized capabilities, tools and testing expertise in HSMs, Open Source cryptographic libraries, network devices and a wide range of security solutions.

We develop the best validation strategy, according to your technical requirements and business goals.

- **Onsite or remote gap analysis workshops**: Get a grasp on the whole validation process and quickly identify all requirements to support your cryptographic module testing. Our workshops provide specific know-how on the Cryptographic Module Validation Program (CMVP) and specific FIPS 140-3 conformance requirements.
- **Algorithm validations (stand alone or to support module validation):** Test algorithm implementations to comply with the Cryptographic Validation Program (ACVP). A prerequisite for cryptographic module validation and an essential part of the process for approved cryptographic algorithms and their individual components.
- **Module boundary scoping and definition**: We help to define the appropriate scope of testing for the cryptographic boundary to optimize the validation lifecycle and to allow for the most flexibility for changes to the product that won't affect the underlying validated components.
- **Validation roadmap planning and FIPS 140-3 risk mitigation**: We engage early on in the validation process to foresee risks that need to be mitigated and to align with your development, and overall product certification strategy.
- **Documentation support and Project Management**: We can support our clients with the specific documentation requirements that are needed as part of the validation process. We also provide turn-key dedicated project management support throughout the process to ensure that all parties are aligned on status and progress.
- **Full validation services including re-validations and certificate maintenance**: Our experienced team can help with certificate re-validations and maintenance to ensure that our clients can maximize the lifespan of the certificate to support their business needs on an ongoing basis.