An Overview of FIPS 140-2

What is FIPS 140-2?

A NIST computer security standard used to approve cryptographic modules. Cryptographic modules are any combination of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signature, authentication techniques and random number generation to improve security of cryptographic keys.

Why is the State of California requiring this standard?

The California State Administrative Manual (SAM), section 5300.5, states: "California has adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as minimum information security control requirements to support implementation and compliance with the Federal Information Processing Standards (FIPS). Each state entity shall use the FIPS and NIST SP 800-53 in the planning, development, implementation, and maintenance of their information security programs."

What are the different levels of FIPS 140-2?

Federal Information Processing Standard Processing Standard (FIPS) 140-2

F5 offers virtual editions (VEs), full-box FIPS platforms, integrated hardware security module (HSM) PCI cards, and external (network HSM) FIPS solutions to meet the most rigorous compliance requirements and architectures.

For customers who only require a FIPS 140-2 Level 1 solution, the F5 FIPS BIG-IP VE incorporates a NIST-validated, software-based, cryptographic module for x86 platforms.

F5 full-box FIPS platforms provide device-level validation at FIPS 140-2 Level 2, including the application of tamper evident stickers.

F5 also offers a select set of BIG-IP platforms, which include an HSM that supports a FIPS 140-2 Level 2 implementation for RSA cryptographic key generation, use, and protection. Keys generated on, or imported into, a BIG-IP integrated HSM are not extractable in plain-text format. BIG-IP hardware devices with integrated HSMs come with a sealed epoxy cover that, if removed, will render the card useless and the keys inaccessible. For additional protection, several platforms support a FIPS 140-2 Level 3 implementation of the internal HSM. This security rating means that the internal HSM card includes tamper-resistance, which recognizes physical access attempts, cryptographic module manipulation, and/or tampering, and will destroy the keys and render the card useless.

FIPS Integration Support in the Public Cloud

- AWS CloudHSM – With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. BIG-IP v14.1.0 and AWS versions 1.0.18 and 1.1.0.

- Equinix SmartKey – HSM-grade security in an easy-to-use cloud service with built-in encryption and tokenization, and FIPS 140-2 Level 3 certification. BIG-IP v14.1.0 and SmartKey client version 2.9.804.

Which organizations require FIPS 140-2 compliance?

FIPS 140-2 validation is mandatory for use in federal government departments that collect, store, transfer, share and disseminate sensitive but unclassified information. This applies to all federal agencies as well as their contractors and service providers, including networking and cloud service providers. FIPS 140-2 has become the de-facto standard for encryption beyond the federal government and is recognized as an important security standard outside the United States. This standard is used extensively in many state and local government agencies as well as non-governmental industries, particularly manufacturing, healthcare, and financial services, or wherever there are federal regulations governing data security. Regulations in such industries may require FIPS 140-2 compliance.

Anyone deploying systems into a U.S. federal SBU environment – and this includes cloud services – are required to comply with FIPS 140-2 certification. In other words, the encryption associated with the computer systems, solutions and services used by federal government agencies must meet the minimum standards specified in FIPS PUB 140-2. This has a huge impact on the IT procurement process, as the only solution vendors that can be considered (without obtaining a variance) are those that have had their products validated as being FIPS 140-2 compliant.

How easy is FIPS to implement?

F5 makes FIPS compliance simple with their FIPS System that includes a Full-Box FIPS add-on license and tamper evidence seals that are applied directly onto an appliance.

Additional Resources

A continuously updated resource for customer

CLICK HERE