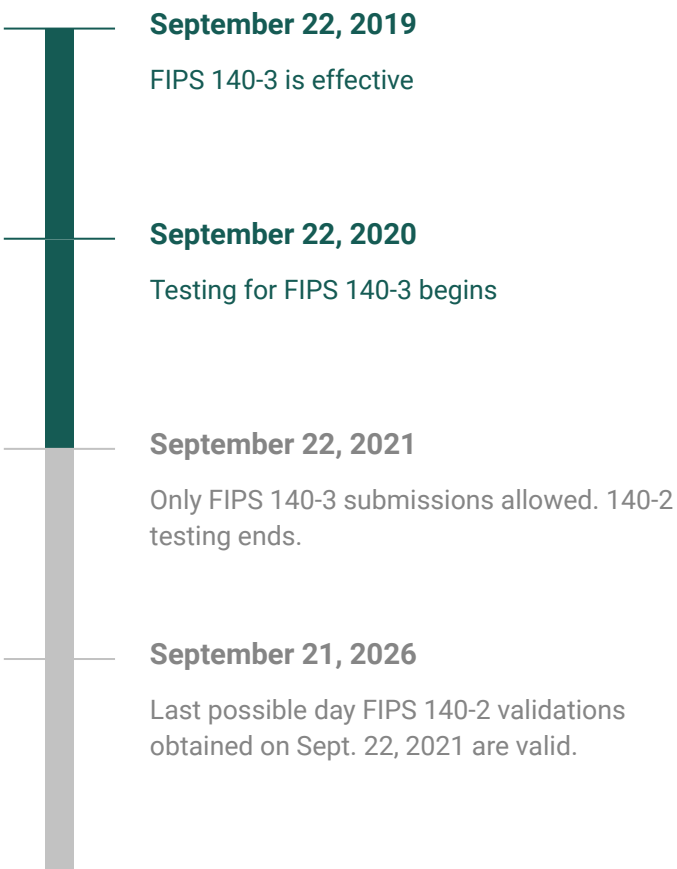

# FIPS 140-3

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL

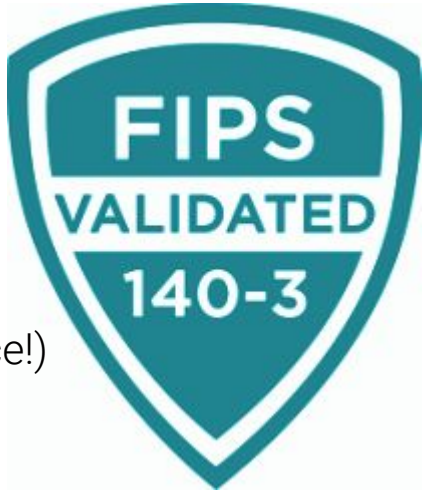
# What is FIPS 140-3?

- Federal Information Processing Standard Publication (FIPS PUB 140-3)
- Standard for cryptographic modules
- US Government Computer Security Standard
- wolfSSL is First to Market; Currently on “In Process” list



# Benefits of FIPS 140-3

- Modules validated under FIPS 140-3 are accepted by federal agencies
- Modernizes the standard (International!)
- Easier to stay up-to-date with the latest wolfSSL Releases
- Stricter requirements and standards (More assurance!)
- Hybrid modules and higher validation levels now possible
- Conditional Algorithm Self-Testing (Boot times and sub-set performance!)



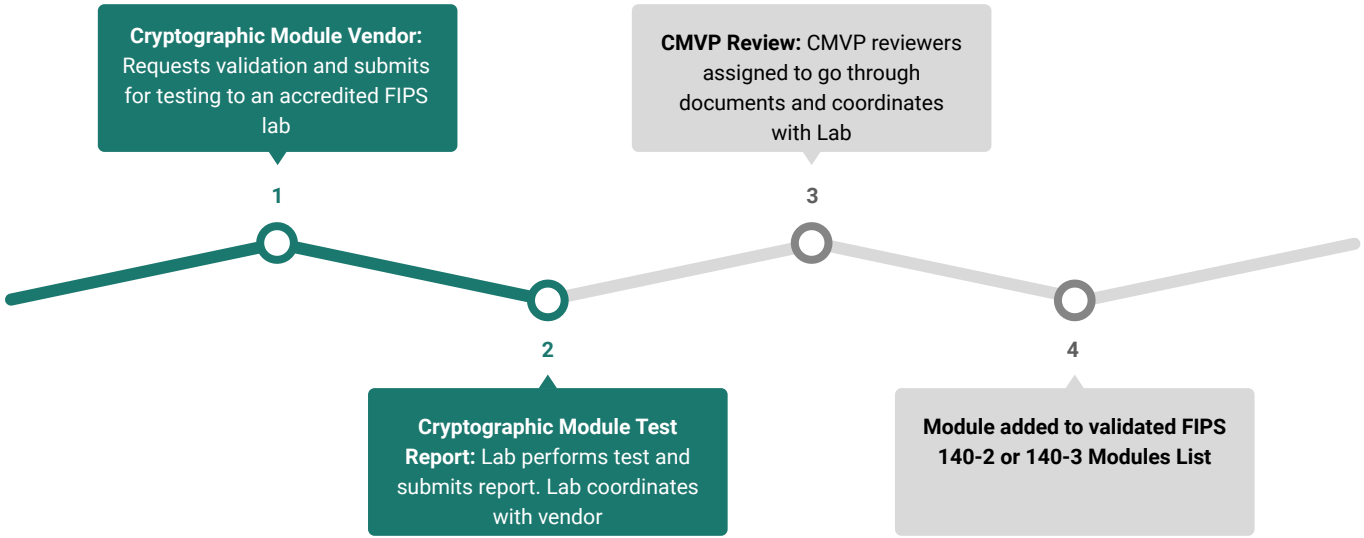
# Who/What is NIST

- National Institute of Standards and Technology
- Implements practical cybersecurity and privacy
- Application of standards and best practices
- Goal: Facilitate U.S. adoption of cybersecurity capabilities

# Cryptographic Module Validation Program

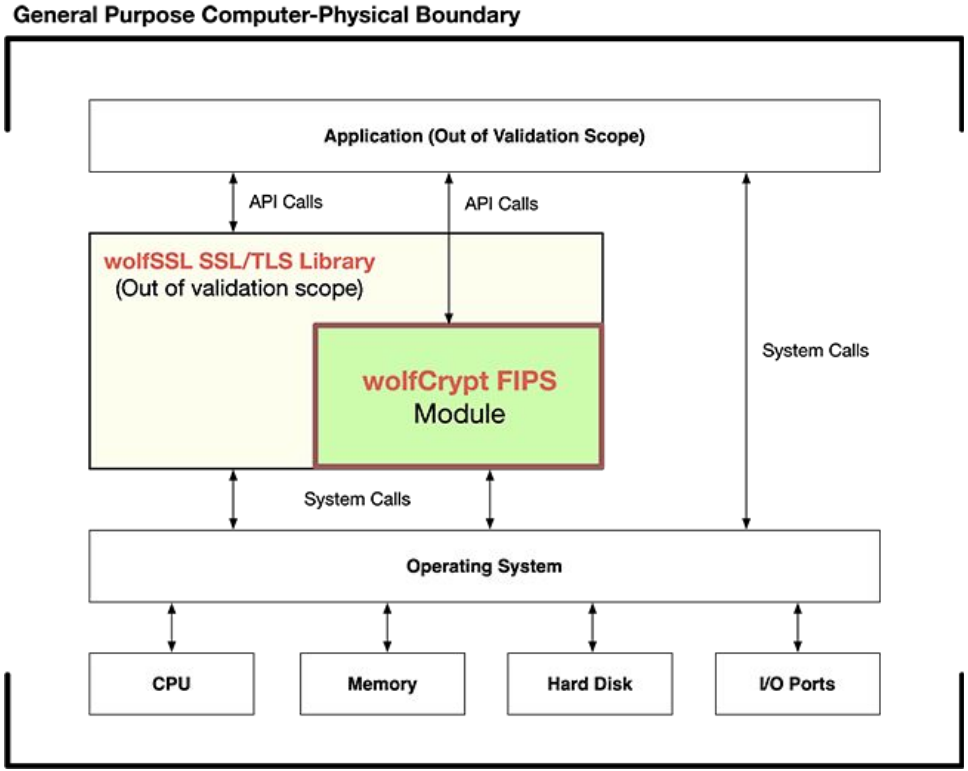
- Established by NIST and CSEC
- Promotes use of validated cryptographic modules
- Security metrics
- CST Labs
  - Verify if module meets cryptographic and security requirements
  - Each lab submission validated by CMVP

# Validation Process



# wolfCrypt

- Lightweight crypto library
- Portable with numerous supported ciphers including Suite B
- Version of wolfCrypt has been FIPS validated
- Used in billions of connections
- Update new versions of wolfSSL while maintaining FIPS validated code boundary



# wolfSSL FIPS 140-3 Certificate


– A merging of the FIPS + ISO Standard
– CAST (formerly CAVP, now ACVP) Testing has been Streamlined to only test the algos actually being used.
– wolfSSL has added the TLS v1.3 and TLS v1.2 KDFs in the wolfCrypt FIPS Boundary
– wolfSSL has added the SSH KDF in the wolfCrypt FIPS Boundary
– Added testing for RSA 4096-bit
– Added testing of ECDSA and SHA-3
– wolfSSL removed testing of insecure algorithms: example Triple DES

# What an OE is

What defines an OE:

- Chipset (Intel® CoreTM i7-7820 @2.9GHz x 4 with AES-NI)
- OS (Windows 10 Enterprise)
- Crypto Module (wolfCrypt v4.2.0)

When you might hear the term:

- Speaking with potential FIPS customers
- Speaking with wolfSSL support staff

Deciding which OE is right for you:

- Customer/Market Driven
- Desktop (doesn't exclude server)
- Laptop (doesn't exclude server)
- Server (doesn't exclude laptop or desktop)
- Embedded (thanks to our in-house proprietary "ACVP agent harness", wolfSSL is one of the only legitimate vendors doing validations for a software module running on Embedded RTOS' like OpenRTOS/FreeRTOS, ThreadX, etc. )

# Steps for adding an OE

## Steps to add an OE: (3 phases, typically takes 2.5-3 months from start to finish)

**Phase 1: 2-3 weeks** (we typically start 2 weeks AFTER receipt of all hardware/software from the customer so this might read 4-5 weeks given the 2 week start delay)

- Customer sends wolfSSL Hardware, Software and accessories (cords etc.) such that wolfSSL engineer can build, ***flash****, and run helloworld.c on target
- wolfCrypt and ***wolfSSL SSL/TLS Layer**** ported to target
- Detailed documentation of any changes made during porting (Later reviewed by the FIPS lab). Copy filed at wolfSSL for any future potential audits of the OE
- Agent Harness (or ACVP harness) ported to target
- Set of “Known Vectors” processed on the target
- Vector Request Paperwork filled out for target and sent to the lab (Copy placed on file with wolfSSL)
- DEMO vectors requested from lab and processed (First Vector Request Form signature required to proceed after vectors pass)
- PRODUCTION vectors requested from lab and processed (Second Vector Request Form signature required to proceed to op testing)
- Port Operational Test Application in place of ACVP harness in prep for phase 2 once all vectors are reported as passing
- MILESTONE 1: ACVP algorithms certificates issued

**Phase 2: 2-3 weeks**

- Create Remote Testing guide for Lab personnel and schedule a date for operational testing (copy placed on file with wolfSSL)
- Operational testing and code review with the lab (fill out and sign evidence paperwork, preserve a copy on file at wolfSSL)
    - Lab reviews any code changes made in porting for “security relevance”
    - Changes deemed security relevant rejected and must be re-done or must go through whole new FIPS validation (new certificate)
    - Fill out vendor affirmation evidence form of compliance with IG G.17 on remote testing (copy placed on file with wolfSSL)
- Send signed copy of vendor affirmation form to accredited FIPS Lab for inclusion in evidence file to be submitted to the CMVP
- Security Policy Updated with “Tested Configuration” and new algorithm certificates
- MILESTONE 2: Accredited FIPS lab submits all evidence of testing to the CMVP for review

**Phase 3: 3-6 weeks** (Much of the time in this phase depends on the CMVP turn-around times and negotiations on ***ambiguity**** of OE listing and tested configuration)

- wolfSSL engineer writes detailed User Guide for OE to be included in FIPS release bundles for that OE
- Internal PRs' with porting changes, Security Policy updates, User Guide and Automation ***Scripts**** to assist customer with the build process and ensuring compliance
- Release Cycle Updated to include the new OE and customer information for distribution
- MILESTONE 3: CMVP validation issued, wolfCrypt FIPS certificate updated with new OE

* if applicable ** To be covered in more detail, NOTE: No intent to hide this, this is so maintenance and security updates at the OS level can still be accepted.

# Solutions that benefit from FIPS module

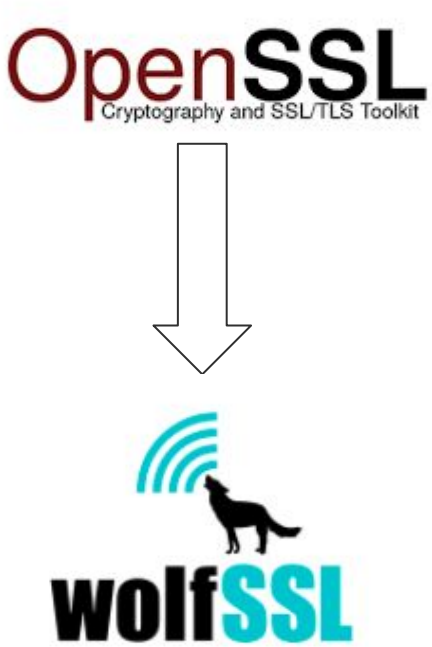
- wolfSSL
- wolfSSH
- wolfMQTT
- wolfBoot
- wolfSSL JNI (JSSE provider)
- wolfCrypt JNI (JCE provider)
- Other Language Wrappers (Python, C#, etc.)

**Third Party:**

- Nginx
- WPA Supplicant
- StrongSwan
- OpenSSH
- Apache
- Stunnel
- Lighttpd (Lighty)
- and the largest third party benefitter of all...

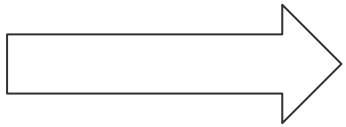
# OpenSSL (wolfCrypt as an engine)

- OpenSSL Engine API allows to replace OpenSSL crypto with third-party crypto.
- Connect wolfCrypt FIPS
- Install FIPS ***system wide*** without changing current applications
- Continue using OpenSSL at the SSL/TLS level and plug-in wolfCrypt FIPS validated crypto underneath
- wolfCrypt FIPS becomes a drop in replacement for OpenSSL crypto

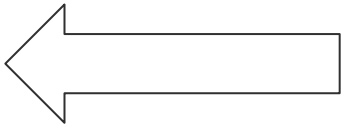


# Lastly: Current wolfCrypt FIPS 140-3 status

- One of the first in the world to be on the FIPS 140-3 in process list
- Proprietary ACVP test rig (developed in-house by wolfSSL engineers) has been used to complete all algorithm testing needed for 140-3 validation.
- All testing evidence and documentation for the module are now with our FIPS lab



We expect to be **out of the lab and into NIST in the next couple of months**.



We expect to have the **first FIPS 140-3 cryptographic library certificate by September**, depending on Government schedules.

- In house test rig supports algorithm testing on backend systems such as Linux, Windows, mac OS and also on embedded iot devices
- The engineers involved in the process will also be providing your support.


## Thanks!

Questions?

**info@wolfssl.com**
www.wolfssl.com

Bozeman, MT : Seattle, WA : Portland, OR : Rescue, CA : Tokyo, JP : Brisbane, AU : Mobile, AL