SIMPLIFYING FIPS TO LOWER COMPLEXITY, COSTS, AND TIME TO MARKET

SUMMIT SUITE SECURITY SOLUTIONS

Building your own FIPS solution from scratch takes years of development with an incredibly steep learning curve. Focus on your core business and leverage our Summit Suite FIPS cryptographic modules on our products, skipping years of learning, testing, and development as well as the 18+ months required to validate a FIPS module.

We're one partner with every needed capability, providing the processing hardware, best-in-class Wi-Fi, and FIPS validation expertise under one roof. Don't sacrifice wireless and application performance for cryptographic excellence; get the best of all worlds with our Summit Suite FIPS.

Our FIPS modules are a regularly-updated, platform-based set of software that help you leverage our FIPS 140-2 Level 1 validations, with a software roadmap to FIPS 140-3 Level 1. They are validated versions of our Summit Linux BSPs. After receiving a FIPS-validated BSP, you can switch from a standard Summit Linux BSP to a FIPS-validated BSP in a matter of hours.

Our FIPS modules are custom to each product family and their respective Yocto or Buildroot Summit Linux board support package (BSP). They're built on our capabilities in maintaining long-term secure Linux BSPs and portions of the hardware acceleration inside application processors to balance the trade-offs between performance, maintainability, and functionality.

In addition, FIPS certificates expire after 5 years from initial certificate issuance. Before expiry, we will have an updated FIPS 140-3 validated BSP in place, allowing time for you to do an updated software integration, validation, and verification.

When you leverage a Summit Suite FIPS Cryptographic Module, you'll be able to claim validated cryptography for:

- **Wi-Fi Data-in-Transit –** validated hardware accelerated[1] Wi-Fi WPA2-Personal, WPA3-Personal[1], WPA2-Enterprise, and WPA3-Enterprise[1], WPA3-Enterprise CNSA/Suite B 192-bit mode[1]. Authentication methods supported are PSK, EAP-TLS, EAP-TTLS, and EAP-PEAP.
- **TLS Data-in-Transit –** validated Transport Layer Security (TLS) protocol 1.0, 1.1, and 1.2 for use with any internet transport protocols that can use the TLS APIs of OpenSSL.
- **Data-at-rest[1] –** validated hardware accelerated directory level encryption for storing sensitive files.
- **Algorithm available to build other solutions –** Create custom validated cryptographic solutions or port existing protocols to our OpenSSL userspace API.
- **Complete coverage for your product's life cycle -** We regularly update our FIPS cryptographic modules so you can support cryptographic operations for your device's full life cycle, such as:
  - Cryptographic code changes, required updated validation testing, and paperwork submissions for all new NIST guidance as the FIPS standards evolve to address new threats.
  - Non-cryptographic updates to address bug fixes and known CVEs to code that is required to be frozen as part of the FIPS validations. FIPS validations require portion of the BSP, e.g. OS kernel's cryptographic subsystem and userspace cryptographic library, to be frozen to verify validated code is properly installed and running on your device.

1: Hardware acceleration, data at rest and WPA3 support not available on the WB45NBT

Key Features

Encrypted WI-FI Data-in-transit

Hardware accelerated encryption with many WPA types and authentication types available, including WPA3-Enterprise CNSA/Suite B 192-bit mode[1]

Encrypted TLS Data-in-transit

Validated Transport Layer Security (TLS) for use with any internet transport protocols that can use the TLS APIs of OpenSSL

Encrypted data-at-rest

Validated hardware-accelerated directory-level encryption for storing sensitive files[1].

Algorithm available to build other solutions

Create custom validated cryptographic solutions or port existing protocols to our OpenSSL compatible userspace API.

Complete coverage for your product's lifecycle

Regular updates for critical CVEs, new validation testing, and evolving FIPS standards. We also proactively provide updated BSPs prior to 5 years expiration for you to integrate.

INDUSTRY-LEADING SUPPORT

Our Tier 2 and FAE support bring expert assistance, working with you and our engineering to reduce your time to market.

Application Areas

Infusion Systems

Patient Monitors

Surgical Instruments

Printers, Scanners, Test Equipment

Smart Hospital Beds

Interested in our Summit Suite?
Visit www.ezurio.com/summit-suite

FIPS Overview

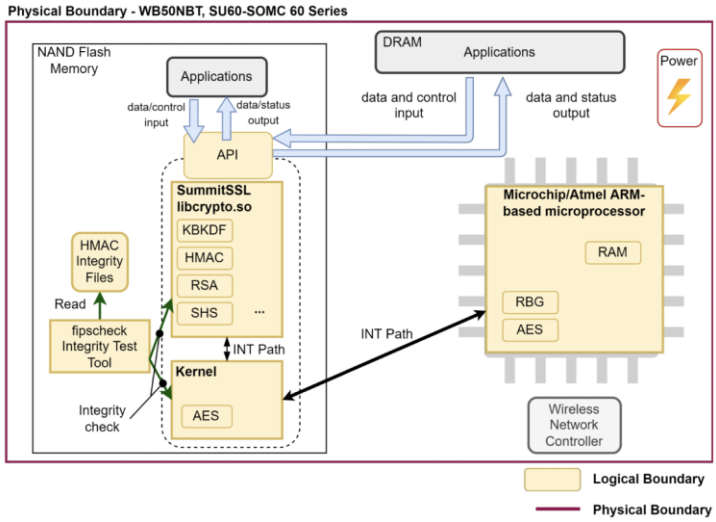
FIPS 140-2 and 140-3 (Federal Information Processing Standard 140-2 and 140-3) defines the U.S. federal government's standard for modules that protect sensitive but unclassified information through cryptography. Through a collaborative effort, NIST (National Institute of Standards and Technology) and Canada's CCCS (Canadian Centre for Cyber Security) created this standard to document cryptographic validation requirements. Adherence to this standard is required by all U.S. government agencies and as such it is also mandatory for any agency or organization that has operated for the U.S. government under contract.

In the healthcare system, all VA (Veterans Affairs) hospitals and the entire MHS (Military Health System) are required to use FIPS 140-2 or 140-3 validated encryption methods for all medical devices as well as for software that transmits data using any wireless technology. Considering that the VA alone is one of the largest medical device/ healthcare product customers, FIPS 140-2 or 140-3 is certainly a requirement for any device manufacturer who wants to do business with this organization.

It's more than just the U.S. federally operated healthcare facilities – the standards that make up FIPS are increasingly being adopted by OEMs everywhere, even for devices that don't operate in government facilities. The reason for this is simple: it's an existing set of standards, the work is already done, and the cryptographic modules and methods are commonplace even outside of FIPS. As an effective, pre-designed set of security policies, FIPS is becoming very commonplace, and many manufacturers are looking for ways to design it into their devices.

Summit Suite FIPS Cryptographic Modules are uniquely designed for each of our specific product families and their respective Yocto or Buildroot Summit Linux board support package (BSP). We leverage our expertise of maintaining a long-term secure Linux BSPs) and portions of the hardware acceleration inside the specific applications processors used in a product family to balance the trade-offs between performance, maintainability, and functionality. This eliminates the complex and often ambiguous design decisions your team would need to balance by using hardware from a vendor with no FIPS expertise and needing to find second partner to go forward with your FIPS validation.

This is augmented further by our expertise of our Wi-Fi radios used on our products. We can provide your device a best-in-class solution for Wi-Fi data-in-transit as we are experts in the Wi-Fi radio, applications processor, and FIPS. This allows your device to have the maximum performance possible for when enabling FIPS validated Wi-Fi cryptography.



Our optimized solution for the Summit 60, 60 Series SOM, IG60, and Summit SOM 8M Plus product familes minimized the validated logical boundary yet provided hardware acceleration by validating libcrypto.so in userspace, the cryptographic functions in the statically built Linux kernel, and the Advanced Encryption Standard (AES) encrypt/decrypt hardware and Deterministic Bit Generator hardware.

FIPS Cryptographic Modules Available

SOM Family	Cryptographic Module Names	FIPS Standard	Base Linux Kernel Version	Version of OpenSSL API	Link to CMVP Listing
60 Series SOM	Summit Linux FIPS Core Crypto Module	140-2 Level 1	4.19.x	1.0.2	Listing
WB50NBT	Summit Linux FIPS Core Crypto Module	140-2 Level 1	4.19.x	1.0.2	Listing
WB45NBT	Summit Linux FIPS Core Crypto Module	140-2 Level 1	4.19.x	1.0.2	Listing
IG60	Summit Linux FIPS Core Crypto Module	140-2 Level 1	4.19.x	1.0.2	Listing

Ordering Information

Part Number	Description
SAAS-SS-FIPS-WB45	One Year of FIPS Cryptographic Module Support on WB45NBT
SAAS-SS-FIPS-WB50	One Year of FIPS Cryptographic Module Support on WB50NBT
SAAS-SS-FIPS-SOM60	One Year of FIPS Cryptographic Module Support on 60 Series SOM
SAAS-SS-FIPS-IG60	One Year of FIPS Cryptographic Module Support on IG60 Summit Linux

Ezurio's products are subject to standard Terms & Conditions.