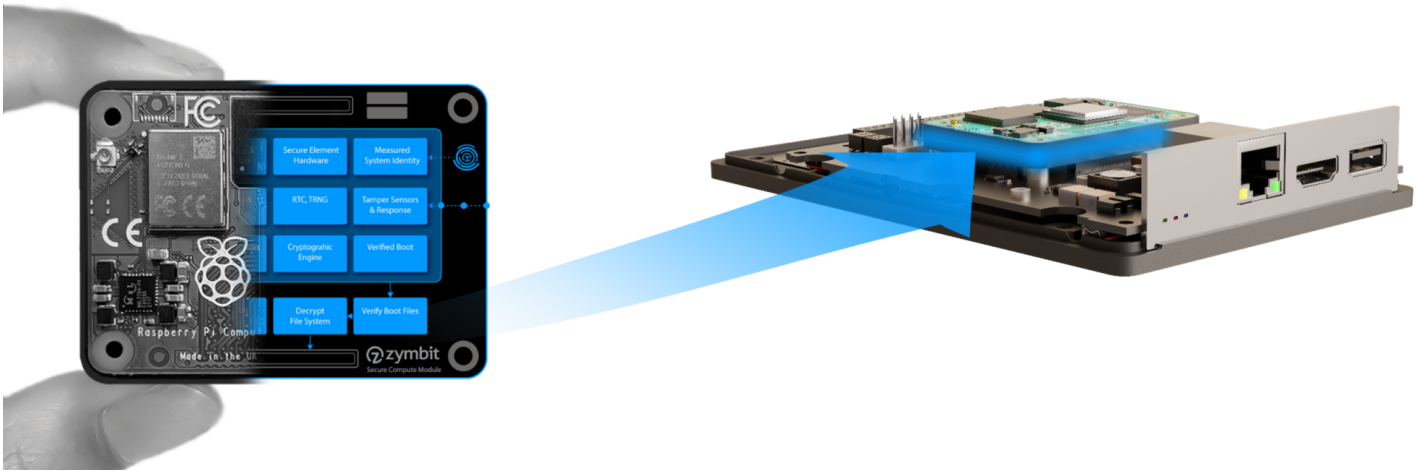
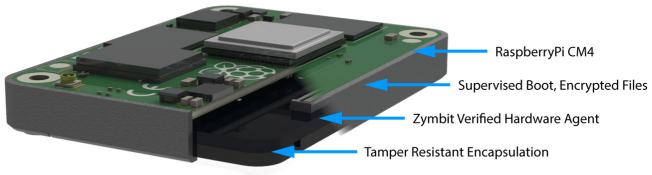
Secure Compute Module

The hardened Raspberry Pi compute module for zero-trust environments.

BUY NOW



Open for developers. Hardened for life on the edge.



Enjoy all the freedoms of the Raspberry Pi developer ecosystem with the protection of Zymbit verified hardware and tools.

- Raspberry Pi CM4 compute
- Secure boot
- Encrypted file system
- Hardware cryptographic engine
- Fully encapsulated, tamper resilient
- Standard and custom images

BUY NOW

Overview

Specifications

Documentation

Overview

Hardware secured compute for critical applications

RASPBERRY PI CM4

SECURE BOOT

ENCRYPTED FILE SYSTEM

KEY STORAGE & GENERATION

DATA ENCRYPTION & SIGNING

REAL TIME CLOCK

MEASURED SYSTEM IDENTITY

ENCAPSULATED MODULE

PHYSICAL TAMPER SENSORS

CRYPTOGRAPHIC ENGINE

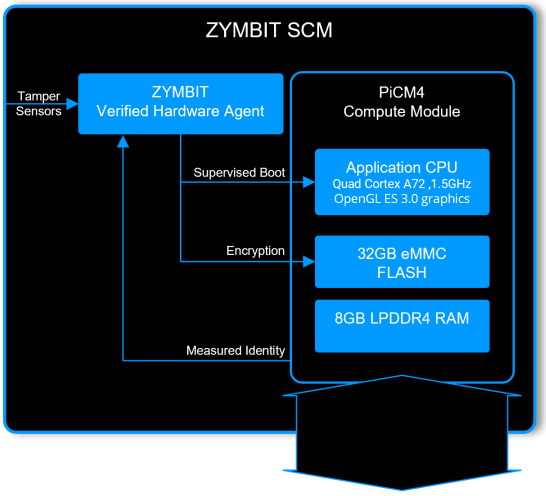
HD HARDWARE WALLET

SHAMIRS SECRET SHARING

ULTRA LOW POWER

BATTERY MONITOR, LAST GASP

QUAD CORE CORTEX-A72



Zymbit Verified Hardware

Each SCM includes a PiCM4 compute module that is protected by a Zymbit Verified Hardware Agent. The agent runs autonomously from the CPU and provides independent verification of boot, file system access and overall system integrity.

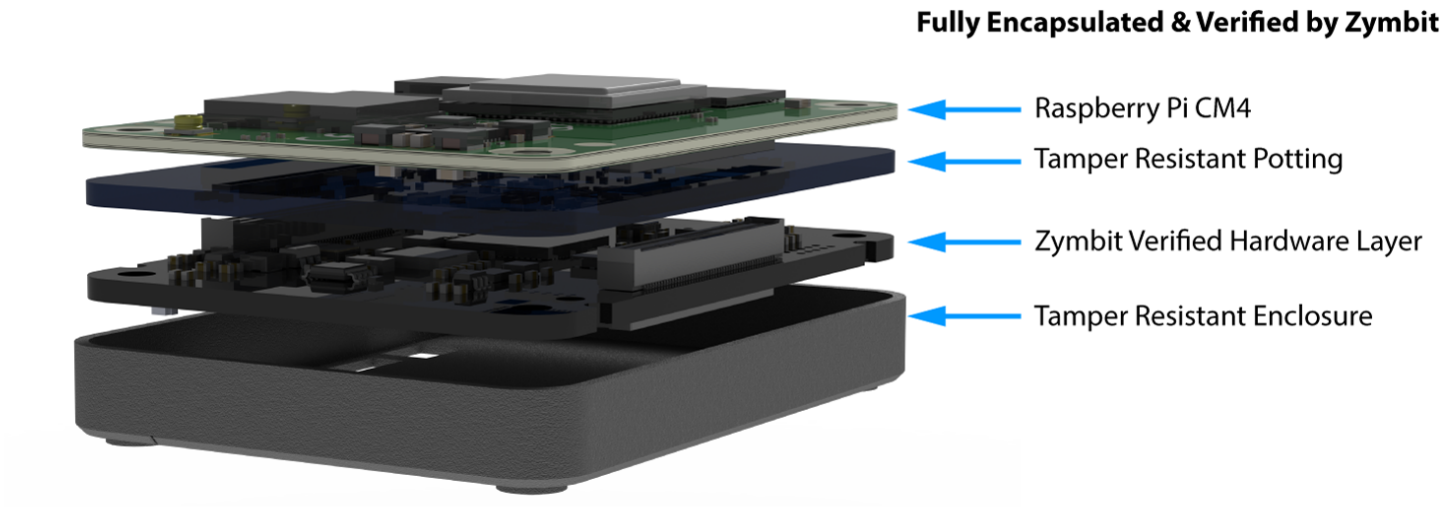
Verified Highlights

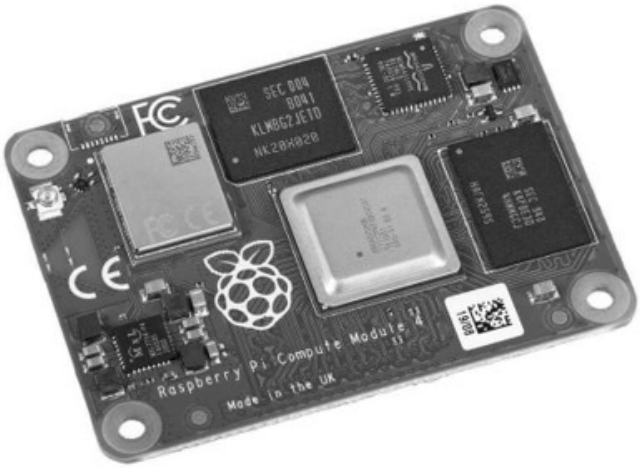
- Secure boot on raspberry pi
- Measured system identity
- File system encryption
- Physical tamper sensors

Secure encapsulated hardware stack

The SCM hardware is fully assembled and encapsulated by Zymbit, ready for provisioning and customer applications.

- Reduced attack surface, increased security
- All connections hidden
- External battery, under module option
- Internal last-gasp destruction mode





Full spec compute module

SCM includes the powerful PiCM4 Linux compute modules.

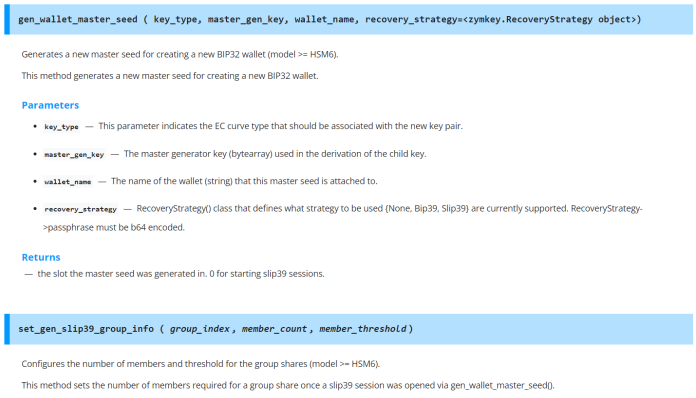
- Broadcom BCM2711 quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz
- H.265 (HEVC) (up to 4Kp60 decode), H.264 (up to 1080p60 decode, 1080p30 encode)
- OpenGL ES 3.1, Vulkan 1.0
- Up to 8GB LPDDR4-3200 SDRAM
- Up to 32GB eMMC Flash memory

FULL SPEC

Python, C, C++ APIs

As developers ourselves, we try to build APIs that allow you to benefit from the power of cryptography, without needing to understand the underlying math. Zymbit wallet functions are designed to provide access to powerful features like generating a wallet master seed, child keys and managing wallet recovery from mnemonic phrases and shared secrets.

LEARN MORE



`gen_wallet_master_seed ( key_type, master_gen_key, wallet_name, recovery_strategy=<zymkey.RecoveryStrategy object>)`

Generates a new master seed for creating a new BIP32 wallet (model >= HSM6).

This method generates a new master seed for creating a new BIP32 wallet.

Parameters

- `key_type` — This parameter indicates the EC curve type that should be associated with the new key pair.
- `master_gen_key` — The master generator key (bytearray) used in the derivation of the child key.
- `wallet_name` — The name of the wallet (string) that this master seed is attached to.
- `recovery_strategy` — RecoveryStrategy() class that defines what strategy to be used (None, Bip39, Slip39) are currently supported. RecoveryStrategy->passphrase must be b64 encoded.

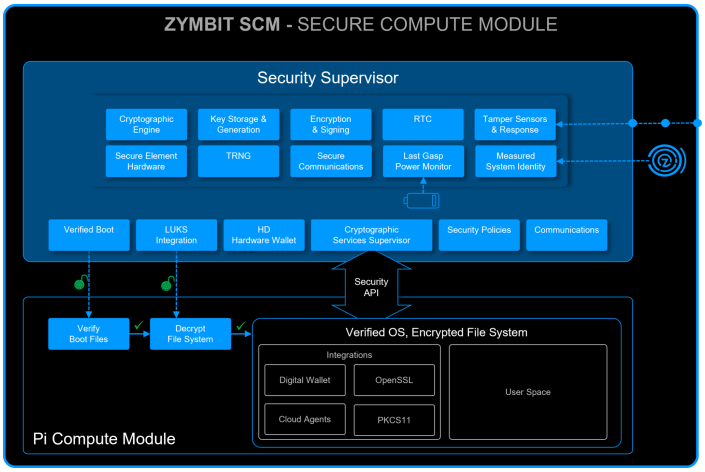
Returns

— the slot the master seed was generated in. 0 for starting slip39 sessions.

`set_gen_slip39_group_info ( group_index , member_count , member_threshold )`

Configures the number of members and threshold for the group shares (model >= HSM6).

This method sets the number of members required for a group share once a slip39 session was opened via gen_wallet_master_seed().



Cryptographic Engine & Services

The Secure Compute Module provides a wide choice of cryptographic services and types that are easily accessed through the Zymbit API.

Services

- Key generation and storage
- Encryption, signing and hash functions
- True random number generator (TRNG)

Cypher Suite

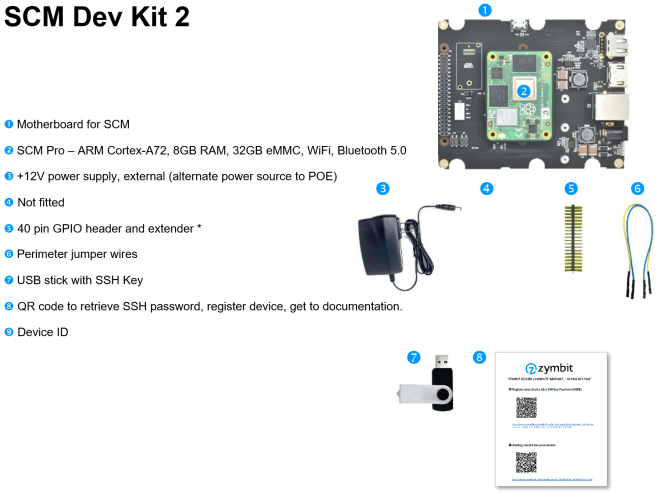
- ECC KOBLITZ P-256 (secp256k1)
- ED25519, X25519
- ECDH (FIPS SP800-56A)
- TRNG (NIST SP800-22)
- ECC NIST P-256 (secp256r1)
- ECDSA (FIPS186-3)
- AES-256 (FIPS 197)

Developer tools

Dev Kit

- Zymbit Secure Compute Module (Integrated Pi CM4
- Motherboard for SCM
- Perimeter Detect breakout cable
- External battery breakout
- 12V power supply
- USB drive with SSH keys necessary for SSH login

SCM Dev Kit 2

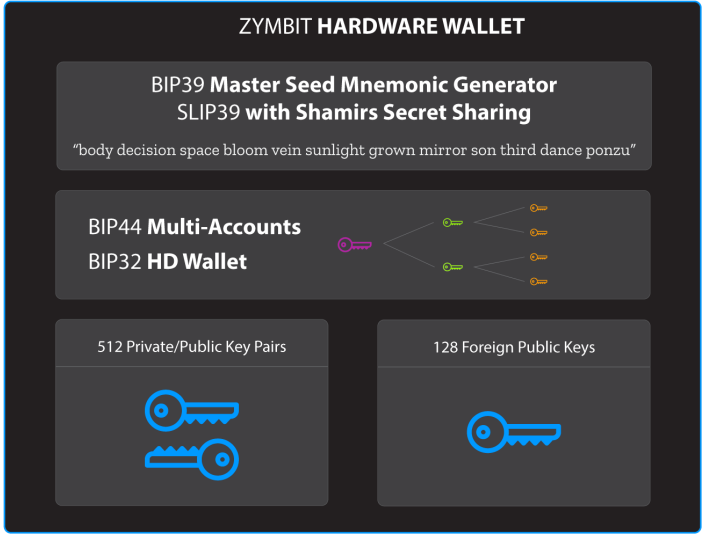


BUY NOW

Optional HD Hardware Wallet

A Hierarchical Deterministic (HD) wallet is a reliable and secure way to manage hundreds of keys, embedded in a single device.

HD wallets use proven de-facto standard algorithms developed for blockchain and crypto applications. Zymbit's HSM6 product implements standard protocols – BIP32/39/44 and SLIP39 – in a compact, easy to integrate module that's programmable through secure APIs.

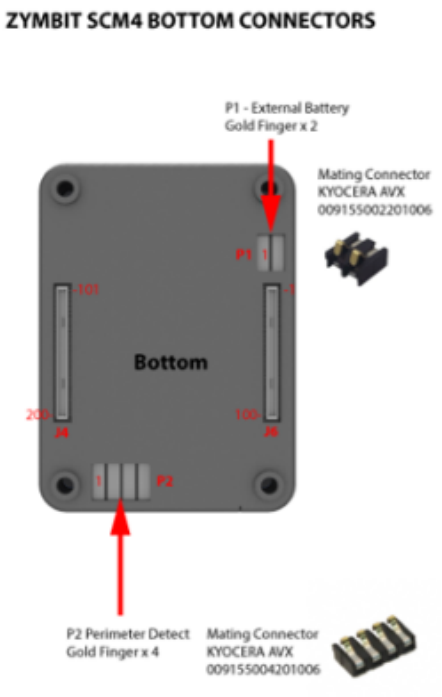


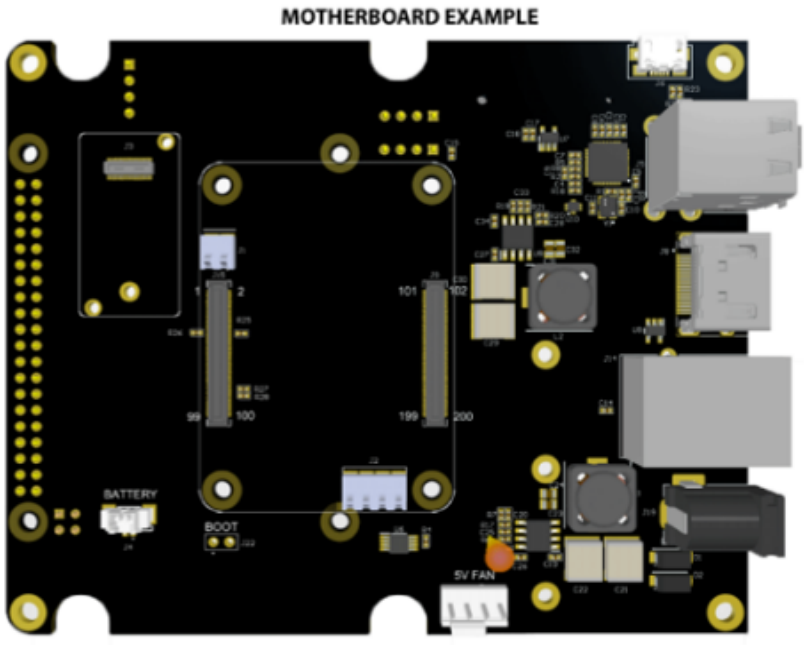
Tutorials on using HD wallet:

- Send Web3 Ethereum transactions
- Wallet recovery with SLIP39 Shamir's secret sharing
- Read-only oversight wallet

LEARN MORE

Footprint compatible with CM4





Ready to embed into your custom design

- PCB footprint, schematic symbol, 3D models
- Altium Designer & CircuitStudio
- KiCAD
- Mechanical drawings
- CAD documents >

Pre-configured the way you want

To simplify your life, the SCM can be shipped with a choice of pre-configured OS, application software and security policies that align with your product development stage.

Develop

- Optimized for maximum development flexibility
- Standard OS builds & tools
- Partially encrypted file system
- Relaxed security policies, open ports

Secure

- Defined security policies enabled
- Optimized OS build
- Fully encrypted file system
- Supervised boot configured
- Finalize configuration with Security Sanitization Guide and Scripts.

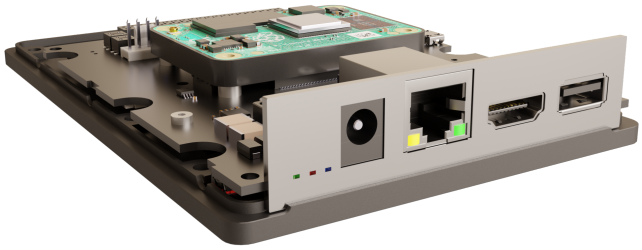
Deploy

- Customer-specific configurations loaded, tested, deployed.
- Standard zymbit curated configurations available.

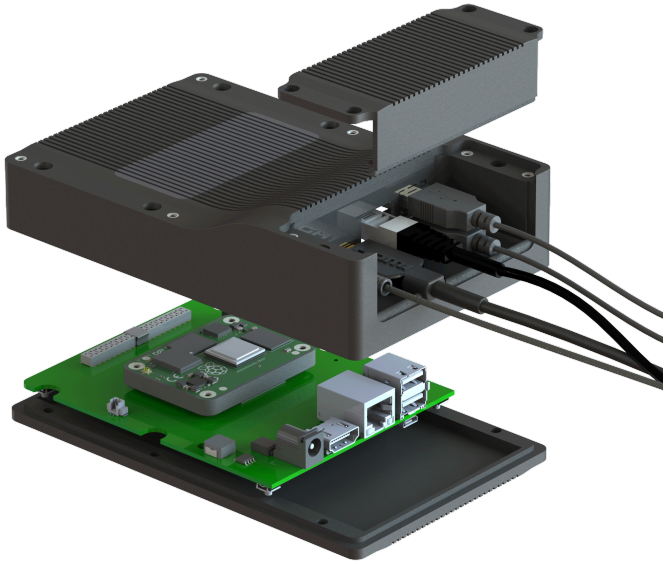
Need a complete secure edge node?

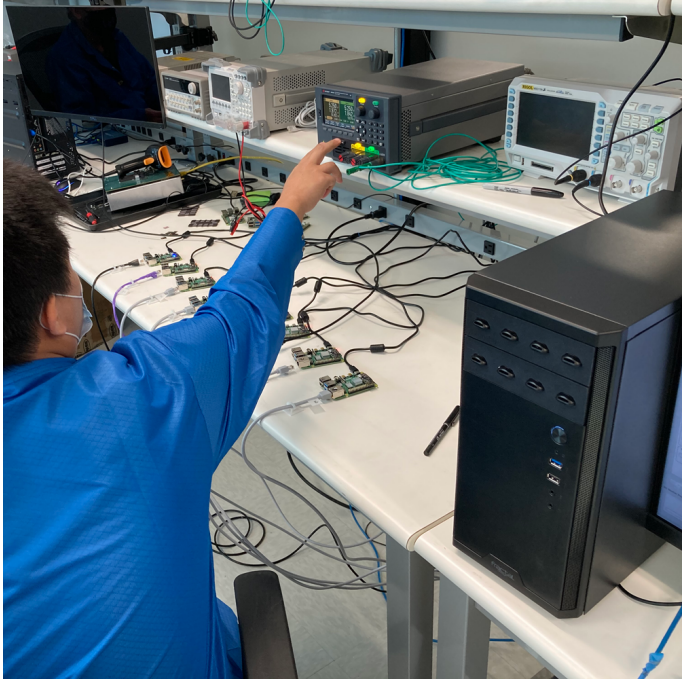
Add SCM to your choice of motherboard, enclosure and power source

- Pre-assembled, encrypted and sanitized computes.
- Pre-loaded with your choice of OS and image.
- Standard enclosure options.
- Choice of power sources.
- OEM white label and custom features available.



SECURE EDGE NODES >





Manufacturing tools and support

Zymbit manufacturing tools and services help you transition your SCM based design to volume manufacturing quickly and securely.

LEARN MORE

Specifications

Security Highlights	Secure boot on Raspberry Pi File system encryption Key generation, storage and management in secure hardware Cryptographic engine
Compute resources	Broadcom BCM2711 quad-core Cortex-A72 (ARM v8) 64-bit SoC @ 1.5GHz H.265 (HEVC) (up to 4Kp60 decode), H.264 (up to 1080p60 decode, 1080p30 encode) OpenGL ES 3.1, Vulkan 1.0 Up to 8GB LPDDR4-3200 SDRAM Up to 32GB eMMC Flash memory
Compute interfaces	Gigabit Ethernet, IEEE 1588 precision time protocol 2.4 GHz and 5.0 GHz IEEE 802.11ac wireless

	Bluetooth 5.0, BLE 28 x user GPIO configurable for SPI, I2C, UART, ADC, DAC, PWM, I2S 2 x HDMI 2.0 ports (up to 4kp60 supported) 1 x MIPI DSI Serial Display 1 x MIPI CSI-2 Serial Camera 1 x PCIe 1-lane Host, Gen 2 (5Gbps) 1 x USB 2.0 port (highspeed)
Private / public key pairs	512
Foreign public keys	128
Wallet Functions	BIP 32 – hierarchical deterministic wallet BIP 39 – master seed mnemonic generator SLIP 39 – with shamir's secret sharing BIP 44 – mulit-account support
Cryptographic Services	ECC KOBLITZ P-256 (secp256k1) ED25519, X25519 ECDH (FIPS SP800-56A) TRNG (NIST SP800-22) ECC NIST P-256 (secp256r1) ECDSA (FIPS186-3) AES-256 (FIPS 197)
Tamper Sensors	2 x Perimeter breach detection circuits Accelerometer shock & orientation sensor Main power monitor Battery power monitor battery removal monitor
Software API	Python, C++, C
Physical Format	Encapsulated module
Dimensions	57.2 x 42.5x 9.5 mm 2.25 x 1.67 x 0.37 Inches
Connectors	Module main connectors: 2x Hirose Header DF40C-100DP-0.4V Mating main connectors: 2x Hirose Receptacle DF40C-100DS-0.4V, 1.5mm clearance Mating main connectors, extended** : 2x Hirose Receptacle DF40HC(3.0)-100DS-0.4V, 3.0 mm clearance Mating external battery connector: 1x KYOCERA AVX 009155002201006 Mating perimeter, LED connector: 1x KYOCERA AVX 009155004201006

	*** required if CR2412 battery fitted under module*
Production mode lock	Software API command
Measured system identity & authentication	Standard factors include RPI host, Zymbit HSM, eMMC memory
Data encryption & signing applications.	Encrypt root file system with dm-crypt, with LUKS key manager hook Encrypt data blobs with “zblock” function Encrypt data in flight with OpenSSL integration
Real time clock	36-60 months operation with external CR2032, application dependent, 5ppm accuracy.
Backup battery	Used for RTC and perimeter circuits Under-module battery connector pads, to any 3V source on motherboard Optional under module battery holder, for CR2412 coin cell * ** requires motherboard connector height 3.0mm*
Backup battery monitor	Yes
Last Gasp battery removal detection	Yes
OEM Custom features	Contact Zymbit
Example Cipher Suites	AWS-IOT | TLS_ECDHE_ECDSA_AES256_SHA MS-AZURE | TLS_ECDHE_ECDSA_AES_128_GCM_SHA256_P256
Accessories & related products	Developer Kit
Warranty	18 months

Documentation

Using Product >

- Getting started
- Software APIs – python, C, C++
- Tutorials
- FAQ & troubleshooting

Conformity Documents >

- EU Declaration of Conformity
- FCC Declaration of Conformity
- RoHS/Reach Declaration of Conformity
- California Prop 65 Declaration of

CAD Files >

- Mechanical dimensions
- Step model

Manufacturing Tools >

- Secure high speed encryption appliance
- Programming and provisioning

Need help choosing product?

Explore and choose the best Zymbit product for your application. If you have questions or need something custom then were ready to help.

I'M READY TO BUY

Zymbit products are available from major distributors around the world, or directly from our webstore.

Buy now >

I HAVE QUESTIONS

If you need help with your application, or want to discuss a custom solution then contact us today.

Contact support >

EXPLORE PRODUCT

120 Cremona Drive, Goleta,

California, 93117, USA

+1 (805) 481 4570

PRODUCTS

- Secure Compute Module
- Secure Edge Node
- ZYMKEY4
- HSM4
- HSM6
- Product Overview
- Engineered Solutions
- Manufacturing Tools