zymbit

ZYMBIT **HSM6**

HARDWARE WALLET FOR EMBEDDED LINUX COMPUTERS

Key Features

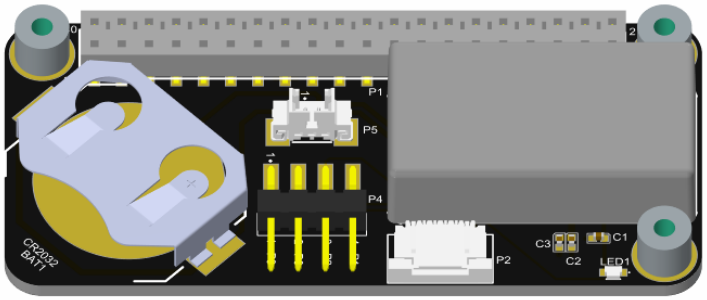
- BIP 32/39/44 HD wallet
- 654 private/public keys
- ED25519, X25519, KOBLITZ P-256 (secp256k1).
- Multifactor device identity & authentication
- Physical tamper detection sensors
- Temperature & battery monitoring with last gasp

Applications

- Blockchain edge devices
- Embedded hardware wallets
- On premise key management & sovereignty
- Secure device registration with AWS IoT
- Cyberphysical security of single board computers

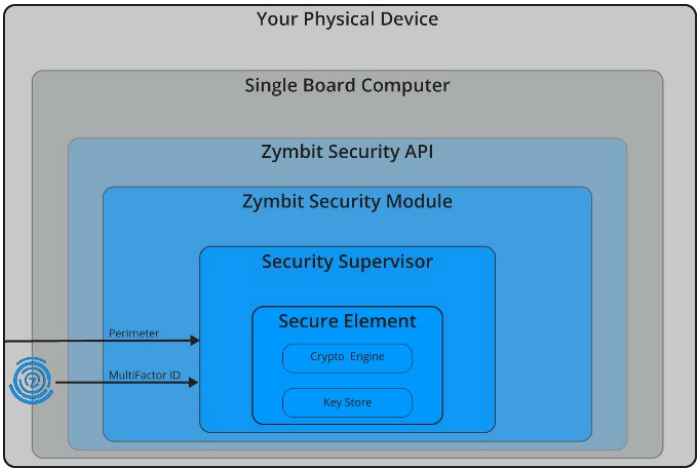
Easy To Integrate Module

HSM6 is a secure hardware wallet designed to support blockchain and crypto applications running on single board computers. HSM6 is packaged in a secure encapsulated module with hidden 30 pin connector that simplifies integration with custom OEM boards and manufacturing workflows. Software APIs are available in Python, C, and C++. Example code and online documentation provide a simple low-risk way to integrate Zymbit security features into your application running on standard Raspberry Pi OS and Ubuntu.



Tough to Infiltrate

HSM6 delivers multiple layers of security to protect against cyber and physical threats. A secure element (SE) with micro-grid protected silicon stores the most sensitive resources. A security supervisor isolates the SE from the host computer and provides additional functions of multi-factor identity/authentication for devices, and multi-sensor physical security.



SPECIFICATIONS

BIP 32/39/44 HD Wallet

HSM6 with BIP 32/39/44 Hierarchical Deterministic Wallets feature:

- Create master seeds and derive child keys
- Ability to recover master seeds
- Ability to index wallet nodes with ZYMKEY key slots

Multifactor Device ID and Authentication

HSM6 enables remote attestation of host device hardware configuration:

- Unique ID token created using multiple device specific measurements
- Cryptographically derived ID token never exposed
- Custom input factors available to OEMs
- ID tokens bound to host permanently for production, or temporarily for development
- Changes in host configuration trigger local hardware & API responses, policy dependent

Data Integrity Encryption & Signing

HSM6's cryptographic engine utilizes strong cipher functions to encrypt, sign and authenticate data:

- Strong cipher suite includes ECDSA, ECDH, AES-256, SHA256
- AES-256 encrypt/decrypt data service
- Integration with TLS client certificate, PKCS11
- TRNG - true random number generator, suitable seed for FIPS PUB 140-2, 140-3 DRNG.

Key Security Generation & Storage

HSM6 generates and stores key pairs in tamper resistant silicon to support a variety of secure services:

- 14 key slots, factory-defined, user available
- 512 empty key pair slots, user available
- 128 foreign public key slots, user defined
- Cryptographic primitives
  - ED25519, X25519
  - ECC KOBLITZ P-256 (secp256k1), ECC NIST P-256 (secp256r1)
  - ECDSA (FIPS186-3), ECDH (FIPS SP800-56A)
  - AES-256 (FIPS 197), TRNG (NIST SP800-22)

Physical Tamper Detection

HSM6 monitors the physical environment for symptoms of physical tampering:

- Power quality monitor detects anomalies like brown-out events
- Optional accelerometer detects shock and orientation change events
- Optional perimeter integrity circuits detect breaks in user defined wire loops/mesh
- Event reporting and response according to pre-defined policies
- Temperature & battery monitoring with 'last gasp' key protection

Real Time Clock

HSM6 includes a battery-backed real time clock to support off grid applications:

- 2-10 years operation, dependent upon external battery size.
- RTC clock service, available to client applications
- RTC/UTC anamoly alerts available with Zymbit security services
- 20ppm accuracy (standard). Optional 5ppm accuracy (OEM feature, MOQ apply)

Secure Element Hardware Root of Trust

HSM6 provides multiple layers of hardware security:

- Hard to penetrate dual secure-processor architecture
- Secure microcontroller isolates secure element from host
- Secure elements from Microchip - ATECC608
- Hardware based cryptoengine and keystore

Ultra-Low Power Operation

HSM6 delivers long term autonomous security from a battery:

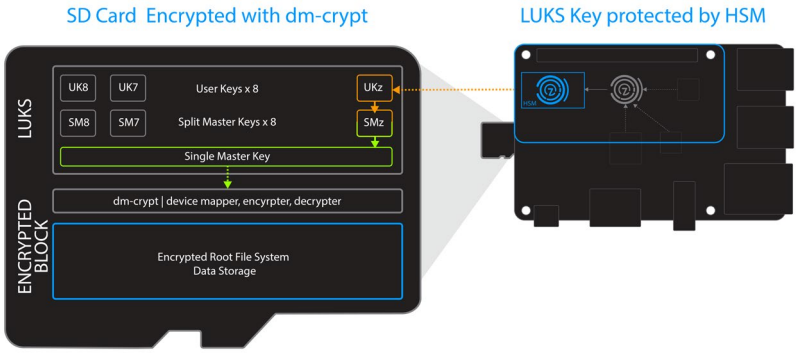
- ARM Cortex-M0 microcontroller
- Years of secure operation from a coin cell - optional larger battery
- Secure operation autonomous from host

APPLICATIONS

Protect Digital Assets with SD Card Encryption

There are many reasons to encrypt the Root File System (RFS) on the Raspberry Pi, from keeping Wi-Fi credentials private to protecting proprietary software and sensitive data from cloning. HSM6 integrates seamlessly with dm-crypt & LUKS open standards.

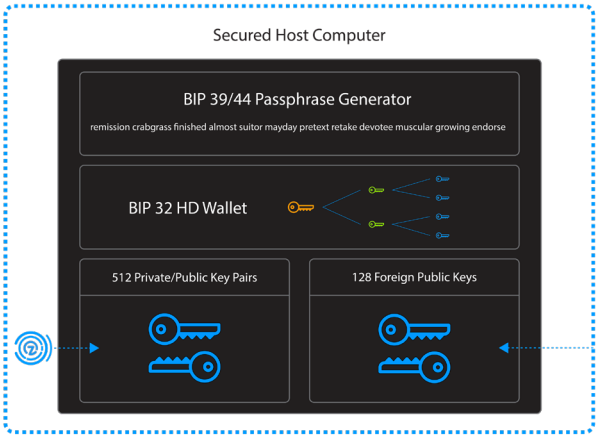
Learn how > https://docs.zymbit.com/tutorials/encrypt-rfs/hsm6/



HSM6 and Digital Wallet

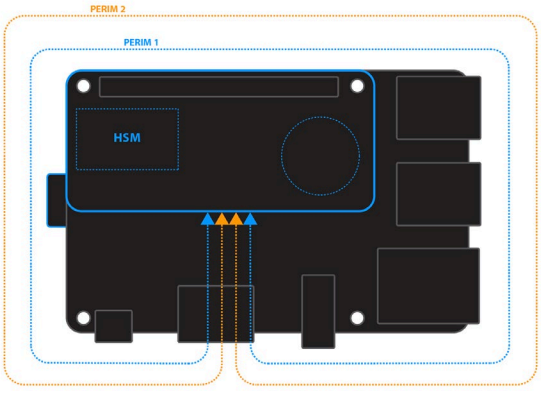
The digital wallet provided by the HSM6 is a BIP32/39/44 HD wallet, or Hierarchical Deterministic wallet. An HD wallet derives all new addresses/keys from a master seed, thus creating a hierarchical wallet structure.

Learn how > https://docs.zymbit.com/tutorials/digital-wallet/



Physically Secured Enclosure with Tamper Detection

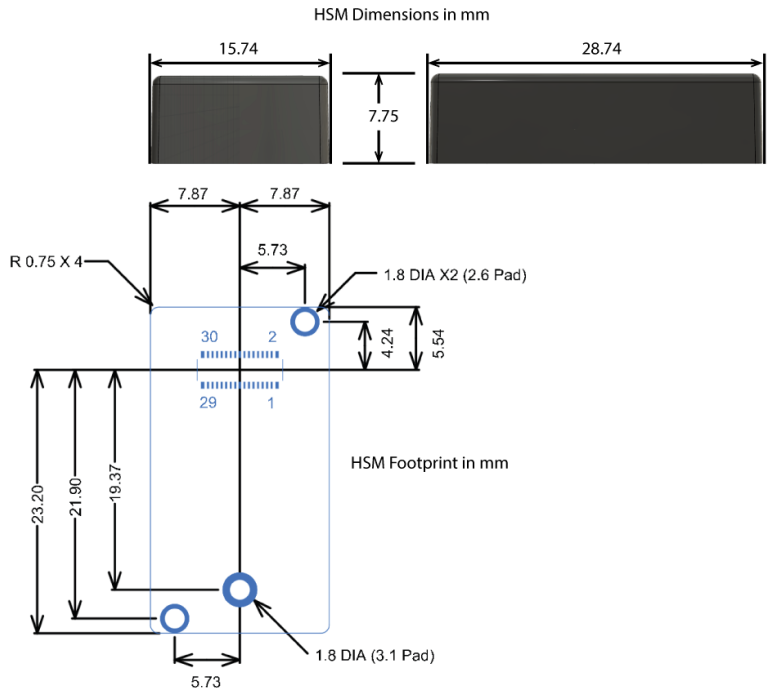
HSM6 provides multiple layers of physical tamper detection that protect unattended devices from threats in the real world. Learn how > https://docs.zymbit.com/tutorials/perimeter-detect/hsm6/



MECHANICAL / ELECTRICAL

Dimensions & Footprint

Get CAD files > https://docs.zymbit.com/reference/cad/

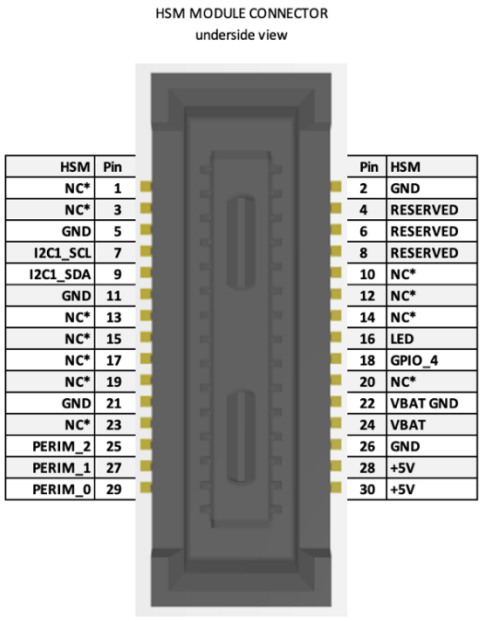


HSM4 Connector

Hirose Header DF40HC(3.5)-30DS-0.4V(51)

Mating Connector

Hirose Receptacle DF40C-30DP-0.4V(51)



HSM	Pin	Pin	HSM
NC*	1	2	GND
NC*	3	4	RESERVED
GND	5	6	RESERVED
I2C1_SCL	7	8	RESERVED
I2C1_SDA	9	10	NC*
GND	11	12	NC*
NC*	13	14	NC*
NC*	15	16	LED
NC*	17	18	GPIO_4
NC*	19	20	NC*
GND	21	22	VBAT GND
NC*	23	24	VBAT
PERIM_2	25	26	GND
PERIM_1	27	28	+5V
PERIM_0	29	30	+5V

*NC = No Connect (Do NOT Connect); Pin reserved for future Zymbit use

OTHER ZYMBIT SECURITY MODULES

HSM6 is a secure hardware wallet designed to support blockchain and crypto applications running on single board computers. It shares the same modular packaging as HSM4, and is code compatible with ZYMKEY4 and HSM4.
For a full list of features for ZYMKEY4, HSM4, and HSM6 visit www.zymbit.com/security-modules

ELECTROMECHANICAL SPECIFICATIONS	**ZYMKEY**4	**HSM**4	**HSM**6
Mechanical format	RPi GPIO	Module	Module
Connectors	2	1	1
I2C	●	●	●
SPI			○
USB			○
Lock function (enter production mode)	Lock Tab	via API	via API
ACCESSORIES	**ZYMKEY**4	**HSM**4	**HSM**6
Developer Kit		●	●
HAT for RPi	●	●	●
Application Reference Designs		●	●
OTHER FEATURES & HIGHLIGHTS	**ZYMKEY**4	**HSM**4	**HSM**6
Backup battery – (for RTC and perimeter breach during loss of power)	Internal	External	External
Backup battery monitoring			●
"Last gasp" feature and user policies			●
Perimeter breach detection circuits - standard	2	2	
Perimeter breach detection - enhanced			2
Unique key slots, user available	3	3	654
Digital wallet			●

● = standard feature
○ = OEM feature

DOCUMENTATION

HSM6 is designed to be easy to integrate into embedded applications. For full and detailed information on how to integrate HSM6 in your application, visit https://docs.zymbit.com/

- API Documentation
- Getting Started Guides
- FAQ & Troubleshooting
- Reference Materials
- Tutorials & How-To Guides

For more information, visit https://zymbit.com/hsm6/

PRODUCT BRIEF 26050911 F1 SEPT 2021