zymbit

ZYMBIT **HSM6**

HARDWARE SECURITY MODULE FOR EMBEDDED APPLICATIONS

Key Features

- Multifactor device identity and authentication
- Data encryption and signing engine
- Key generation and secure storage
- Physical tamper detection sensors
- Secure element as root of trust

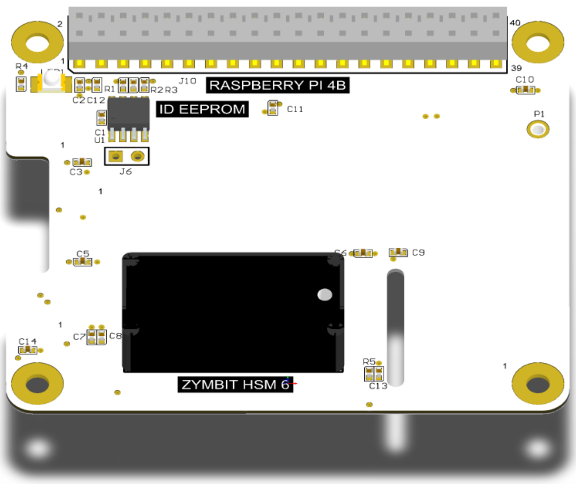
Applications

- Cyberphysical security of single board computers
- Secure device registration with AWS IoT
- Independent key management & sovereignty
- Embedded blockchain wallets

Easy To Integrate Module

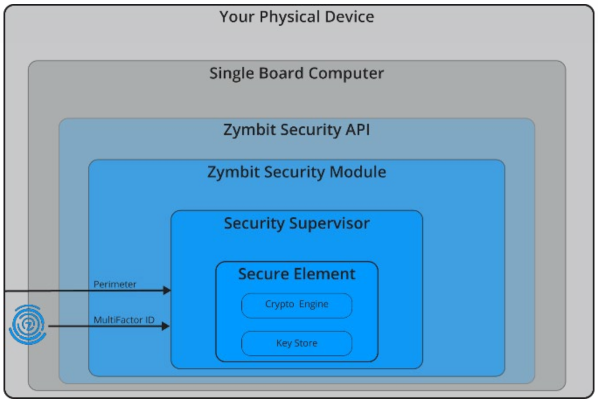
HSM6 is a ‘snap in’ security module designed for easy integration within a secure manufacturing environment. All connections are through a single, 30 pin connector that is hidden underneath the module. No soldering is required, which simplifies provisioning and supply chain management.

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 Raspbian distributions. Support for other Linux distributions is optionally available.



Hard To Penetrate

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

Multifactor Device ID and Authentication

HSM 6 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

HSM 6 provides a cryptographic engine featuring some of the strongest commercially available 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

HSM 6 generates and stores key pairs in tamper resistant silicon to support a variety of secure services:

- 32 key slots, pre-defined and user available
- Cryptographic primatives
  - 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)
- Private keys never exposed outside of silicon
- Keys destruction available, user selectable

Physical Tamper Detection

HSM 6 monitors the physical environment for symptoms of physical tampering:

- Power quality monitor detects anomolies 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

Real Time Clock

HSM 6 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

HSM 6 provides multiple layers of hardware security:

- Hard to penetrate dual secure-processor architecture
- Secure microcontroller supervises device multifactor identity / authentication and physical security.
- Secure microcontroller isolates secure element from host
- Secure elements from Microchip - ATECC608
- Hardware based cryptoengine and keystore

Ultra-Low Power Operation

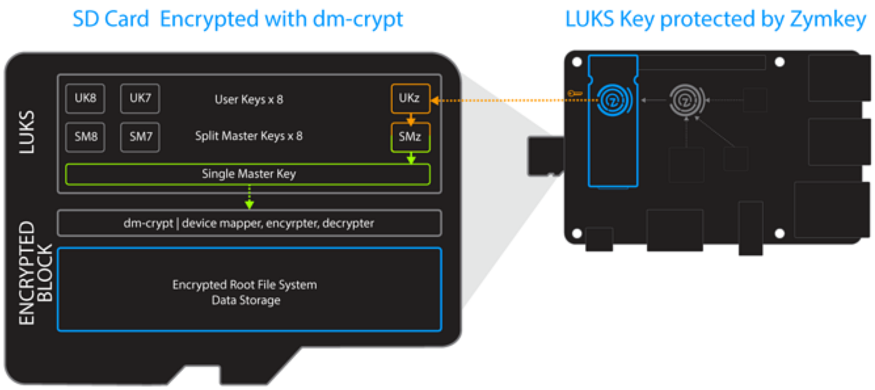
HSM 6 delivers long term autonomous security from a battery:

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

APPLICATIONS

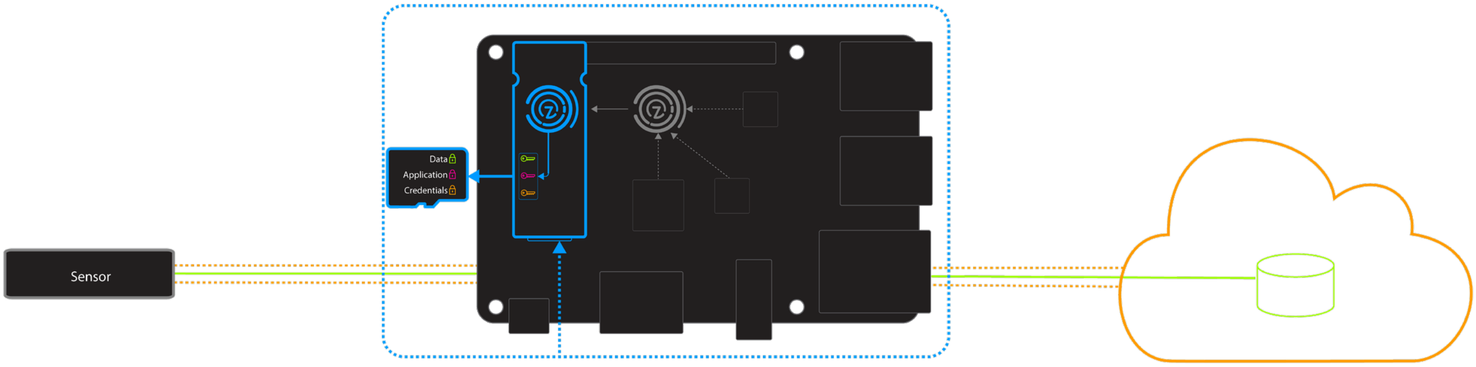
Protect Digital Assets with SD Card Encryption

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. Zymkey integrates seamlessly with dm-crypt & LUKS open standards. Learn how > https://community.zymbit.com/t/150


SD Card Encrypted with dm-crypt
LUKS Key protected by Zymkey
LUKS
UK8
UK7
User Keys x 8
UKz
SM8
SM7
Split Master Keys x 8
SMz
Single Master Key
dm-crypt | device mapper, encyrpter, decrypter
ENCRYPTED BLOCK
Encrypted Root File System
Data Storage

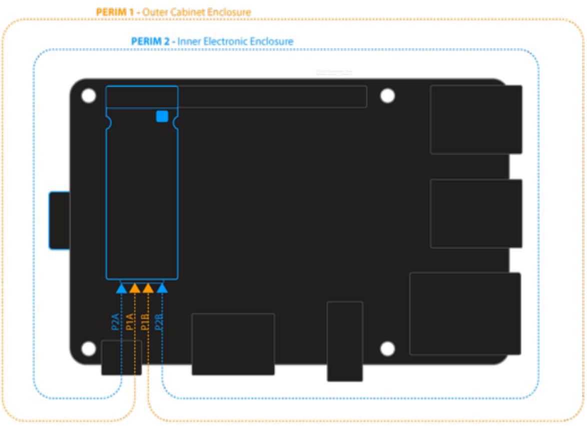
Secure Credentials for Cloud Service Connections

Zymkey delivers device-based security features that are easy to integrate with AWS IoT, MS Azure and PKCS11 frameworks, and other general connection services that require TLS with client-side identity and authentication.   Learn how > https://community.zymbit.com/t/354

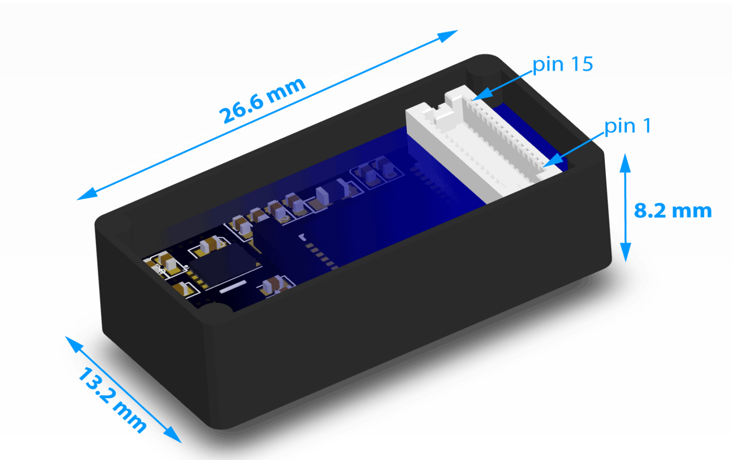


Physically Secured Enclosure with Tamper Detection

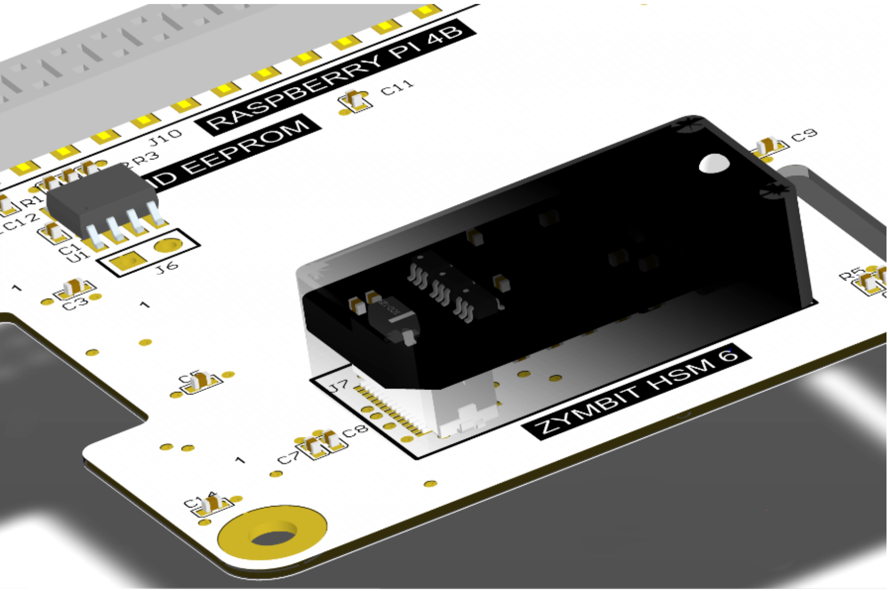
Zymkey provides multiple layers of physical tamper detection that protect unattended devices from threats in the real world. Learn how > https://community.zymbit.com/t/using-perimeter-detect/204

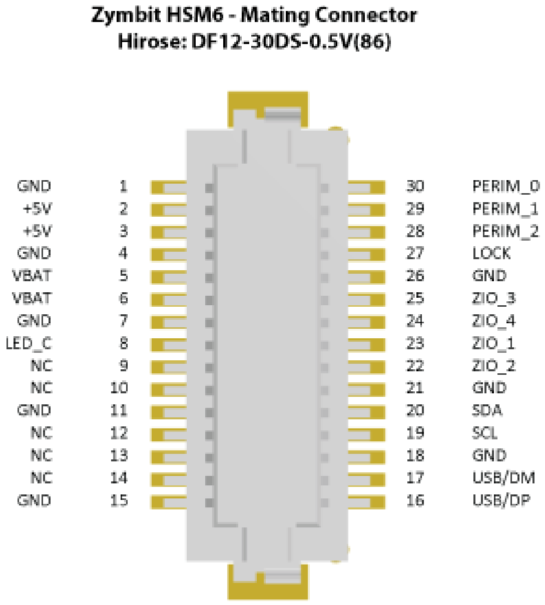

PERIM 1 - Outer Cabinet Enclosure
PERIM 2 - Inner Electronic Enclosure
P2A
P1A
P1B
P2B

MECHANICAL /ELECTRICAL



Mating Connector
Hirose DF12-30DS-0.5V(86)





Zymbit HSM6 - Mating Connector
Hirose: DF12-30DS-0.5V(86)

GND	1	30	PERIM_0
+5V	2	29	PERIM_1
+5V	3	28	PERIM_2
GND	4	27	LOCK
VBAT	5	26	GND
VBAT	6	25	ZIO_3
GND	7	24	ZIO_4
LED_C	8	23	ZIO_1
NC	9	22	ZIO_2
NC	10	21	GND
GND	11	20	SDA
NC	12	19	SCL
NC	13	18	GND
NC	14	17	USB/DM
GND	15	16	USB/DP

DOCUMENTATION

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

- Getting Started
- Software APIs
- Applications
- Compliance Documentation

For more information, visit **www.zymbit.com/HSM**

Copyright © 2019 Zymbit Corporation. All rights reserved. ZYMBIT, the ZYMBIT logo and Zymkey are trademarks and/or registered trademarks of ZYMBIT Corporation. All other company and product names are trademarks or registered trademarks of the respective owners with which they are associated. Features, pricing, availability, and specifications are all subject to change without notice.

zymbit