

# ZYMBIT HSM4

## HARDWARE SECURITY MODULE FOR EMBEDDED APPLICATIONS

### Key Features

- Measured device identity and authentication
- ECDSA signing/ verification engine
- Key generation and secure storage
- Physical tamper detection sensors
- Secure element as root of trust

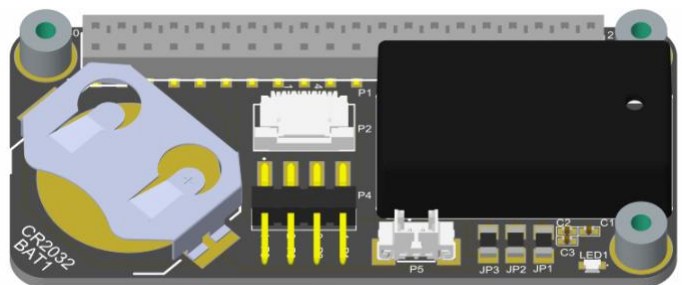
### Applications

- Cyberphysical security for single board computers
- Secure device registration with AWS IoT
- Independent key management & sovereignty
- Secure node in distributed fintech and identity

### Easy To Integrate Module

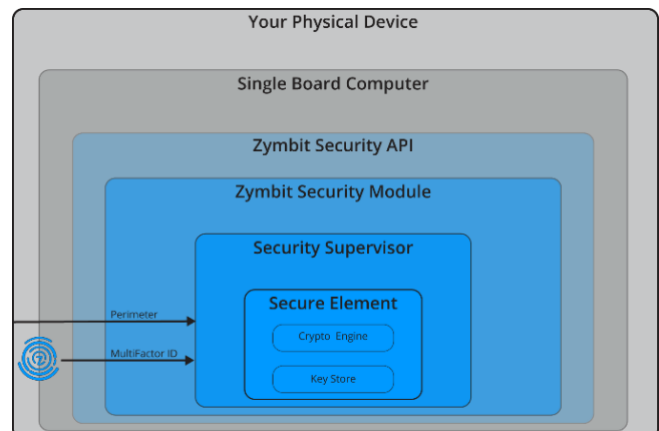
HSM4 is a 'snap in' security module designed for easy integration within a secure manufacturing environment. All connections are through a single, 30 pin connector that is hidden underneath the module. No soldering is required, which simplifies installation, provisioning and supply chain management.

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 and Ubuntu.



### Defense in Depth

HSM4 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.





## Multifactor Device ID and Authentication



HSM4 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



HSM4 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



HSM4 generates and stores key pairs in tamper resistant silicon to support a variety of secure services:

- Multiple key slots, pre-defined and user available
- Cryptographic primitives
  - ECC NIST P-256 (secp256r1), ECDSA (FIPS186-3)
  - AES-256 (FIPS 197), TRNG (NIST SP800-22)
- Private keys never exposed outside of silicon
- Keys destruction available, user selectable

## Physical Tamper Detection



HSM4 monitors the physical environment for symptoms of physical tampering:

- Two perimeter integrity circuits detect breaks in user defined wire loops/mesh
- Power quality monitor detects anomalies like brown-out events
- Three axis accelerometer detects shock and orientation change events
- Event reporting and response according to pre-defined policies

## Real Time Clock



HSM4 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 anomaly alerts available with zybit security services
- 20ppm accuracy (standard). Optional 5ppm accuracy (OEM feature, MOQ apply)

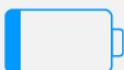
## Secure Element Hardware Root of Trust



HSM4 provides multiple layers of hardware security:

- Hard to penetrate dual secure-processor architecture
- Secure microcontroller supervises device multifactor authentication and physical security.
- Secure microcontroller isolates secure element from host
- Secure elements from Microchip - ATECC508
- Hardware based cryptoengine and keystore

## Ultra-Low Power Operation



HSM4 delivers long term autonomous security from a battery:

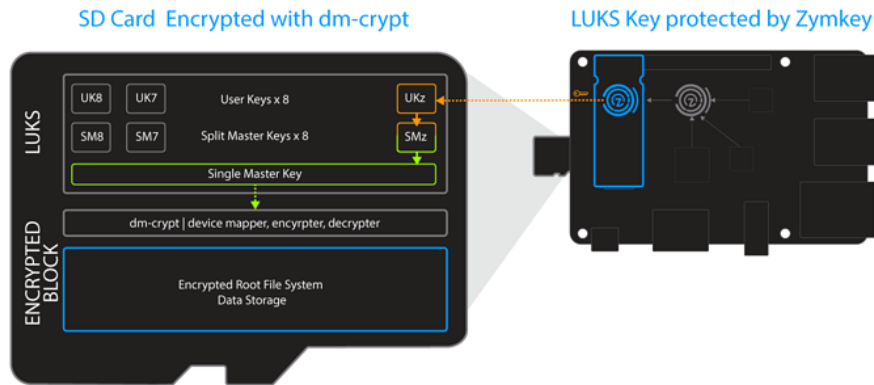
- ARM Cortex-M0 microcontroller
- Years of secure operation from an external CR2032 coin cell, or larger
- Secure operation autonomous from host



## Protect Digital Assets with SD Card Encryption

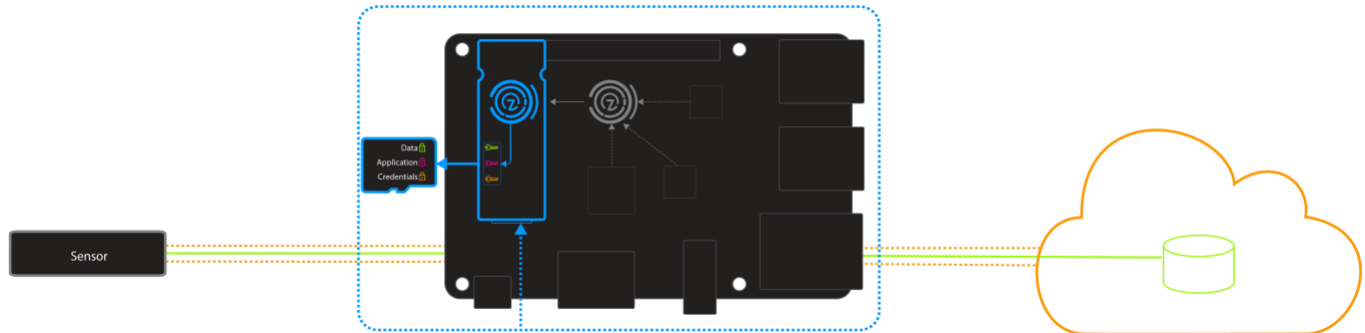
There are many reasons to encrypt the Root File System (RFS) on the Raspberry Pi or other Single Board Computer, from keeping Wi-Fi credentials private to protecting proprietary software and sensitive data from cloning. HSM4 integrates seamlessly with dm-crypt & LUKS open standards.

Learn how > <https://community.zymbit.com/t/150>



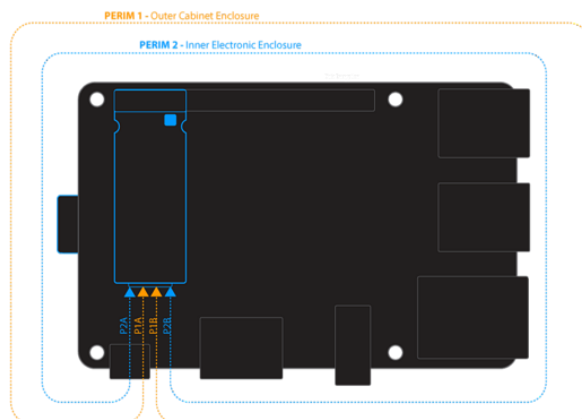
## Secure Credentials for Cloud Service Connections

HSM4 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>



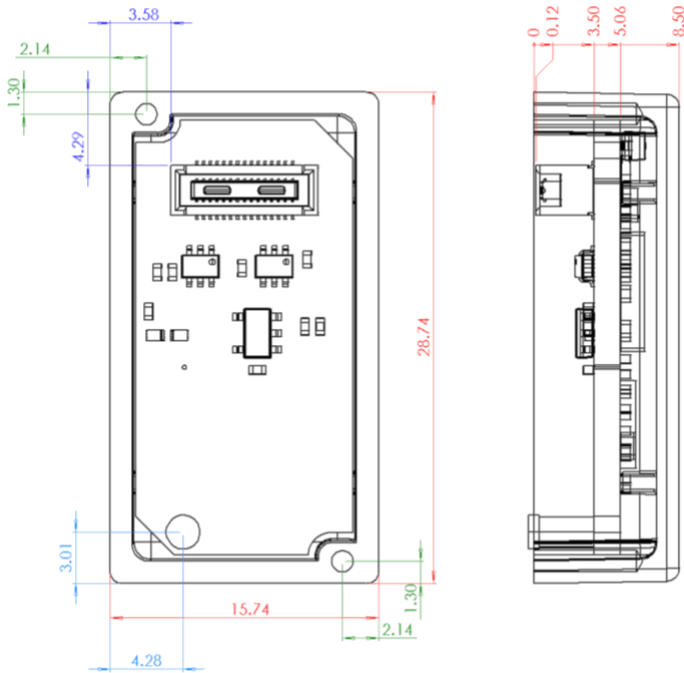
## Physically Secured Enclosure with Tamper Detection

HSM4 provides multiple layers of physical tamper detection that protect unattended devices from threats in the real world. Learn how > <https://community.zymbit.com/t/204>





## Dimensions (mm) Underside view of HSM



## HSM Underside



## HSM Connector

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

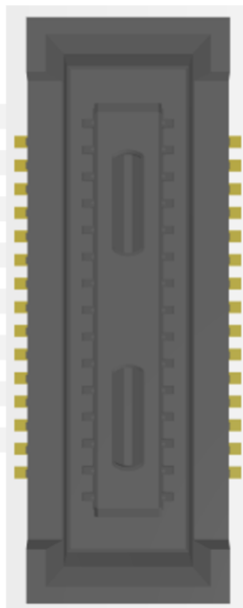
## Mating Connector

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

HSM4, HSM6 MODULE CONNECTOR  
underside view

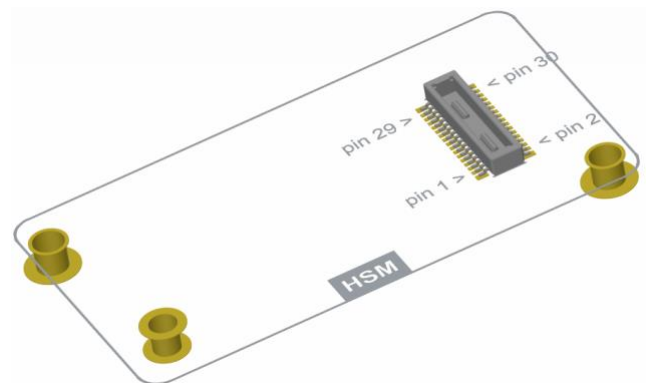
Module

HSM6	HSM4	Pin
USB/DP	NC	1
USB/DM	NC	3
GND	GND	5
I2C1_SCL	I2C1_SCL	7
I2C1_SDA	I2C1_SDA	9
GND	GND	11
ZIO_2	NC	13
ZIO_1	NC	15
ZIO_4	NC	17
ZIO_3	NC	19
GND	GND	21
ZIO_5	NC	23
PERIM_2	PERIM_2	25
PERIM_1	PERIM_1	27
PERIM_0	PERIM_0	29



Rev C2

Pin	HSM4	HSM6
2	GND	GND
4	RESERVED	RESERVED
6	RESERVED	RESERVED
8	RESERVED	RESERVED
10	NC	NC
12	NC	PI_RUN
14	NC	NC
16	LED	LED
18	GPIO_4	GPIO_4
20	NC	NC
22	GND	GND
24	VBAT	VBAT
26	GND	GND
28	+5V	+5V
30	+5V	+5V



**Note:** The four larger corner pads of the mating connector are mounting pads. Only the middle 30 pins are used.

## OTHER ZYMBIT SECURITY MODULES

HSM4 is designed to have all the features of ZYMKEY4, in Zymbit’s Hardware Security Module (HSM) format. The smaller dimensions of both HSM4 and HSM6, as well as the new form, single connector, and external battery are designed for embedded and OEM applications. HSM4 is code compatible with ZYMKEY4.

For a full list of features for ZYMKEY4, HSM4, and HSM6 visit [www.zybit.com/security-modules](http://www.zybit.com/security-modules)

ELECTROMECHANICAL SPECIFICATIONS	ZYMKEY4	HSM4	HSM6
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	ZYMKEY4	HSM4	HSM6
Developer Kit	●	●	●
HAT for RPi		●	●
Application Reference Kits		●	●
OTHER FEATURES & HIGHLIGHTS	ZYMKEY4	HSM4	HSM6
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	700
Digital wallet			●

## DOCUMENTATION

HSM4 is designed to be easy to integrate into embedded applications. For full and detailed information on how to integrate HSM4 in your application, visit <https://community.zybit.com/>

- Getting Started
- Software APIs
- Applications
- Compliance Documentation
- CAD Footprint and Mechanical Files

For more information, visit [www.zybit.com/HSM](http://www.zybit.com/HSM)

Copyright © 2020 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.

