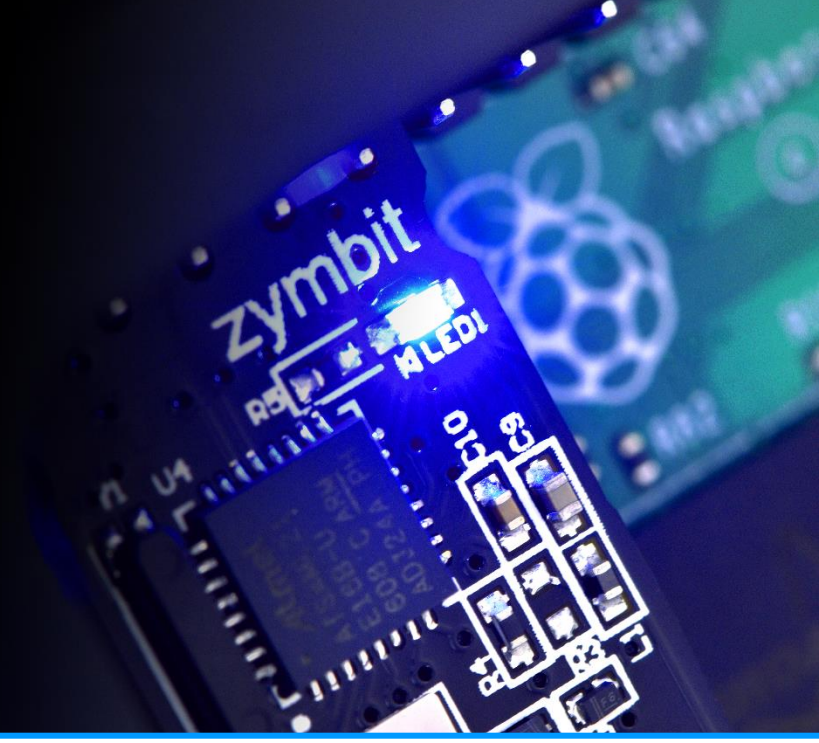
zymbit



ZYMKEY 4i

HARDWARE SECURITY MODULE FOR RASPBERRY PI

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

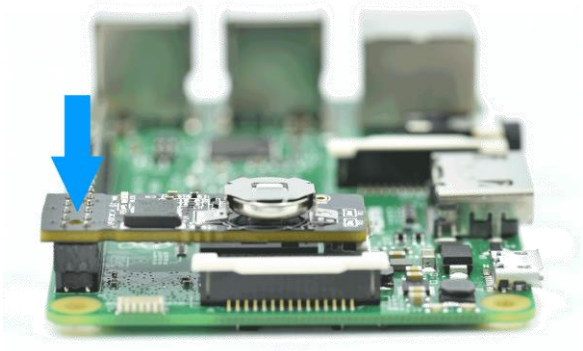
Applications

- SD card file system encryption for protection of IP, data and credentials
- Secure device registration with AWS IoT
- Autonomous security for unattended IoT devices, no cloud dependence

Easy To Integrate Module

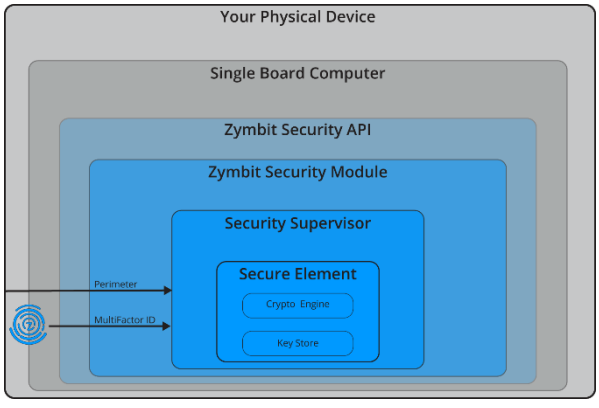
Zymkey plugs directly onto the GPIO header of a Raspberry Pi making it quick and easy to install, even late in the design cycle.

Software APIs are available in Python, C and C++. Example code and online documentation provide a simple low-risk way to integrate Zymkey security into your application running on standard Raspbian distributions. Support for other Linux distributions is optionally available.



Hard To Penetrate

Zymkey 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

ZYMKEY 4i 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

ZYMKEY 4i 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
- Integrates with TLS client-side certificates
- TRNG - true random number generator, suitable seed for FIPS PUB 140-2, 140-3 DRNG.

Key Security Generation & Storage

ZYMKEY 4i generates and stores key pairs in tamper resistant silicon to support a variety of secure services:

- Multiple key slots, pre-defined and user available
- Private keys never exposed outside of silicon
- Keys destruction available, user selectable

Physical Tamper Detection

ZYMKEY 4i 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

ZYMKEY 4i includes a battery-backed real time clock to support off grid applications:

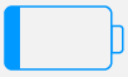
- 18-36 month operation, application dependent
- RTC clock service, available to client applications
- RTC/UTC anamoly alerts available with zymbit security services
- 20ppm accuracy (standard). Optional 5ppm accuracy (OEM feature, MOQ apply)

Secure Element Hardware Root of Trust

ZYMKEY 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, ATECC508
- Hardware based cryptoengine and keystore

Ultra-Low Power Operation



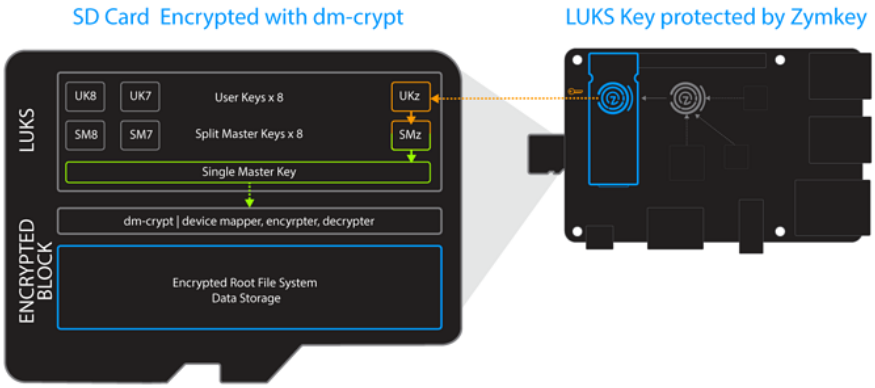
ZYMKEY delivers long term autonomous security from a battery:

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

APPLICATIONS

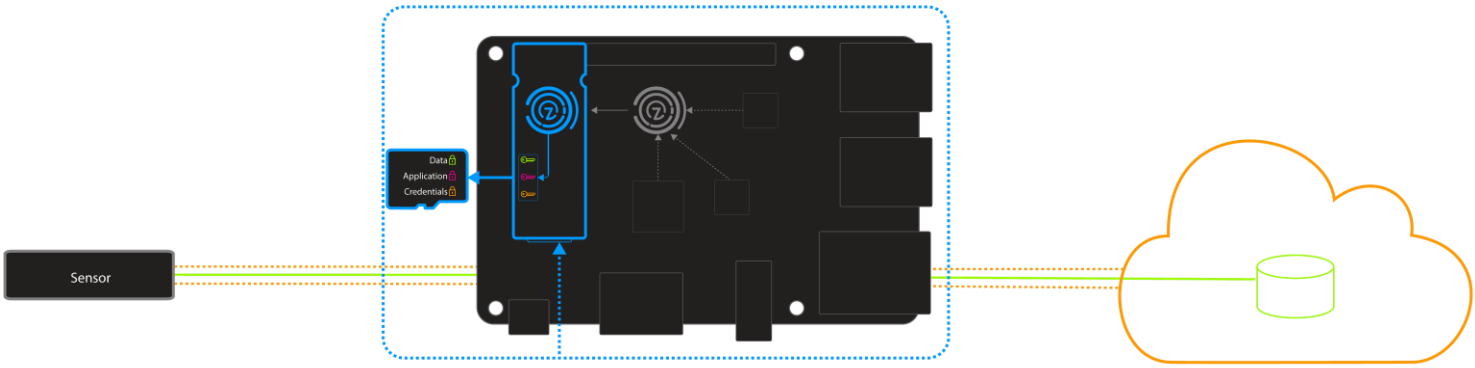
SD Card Encryption

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



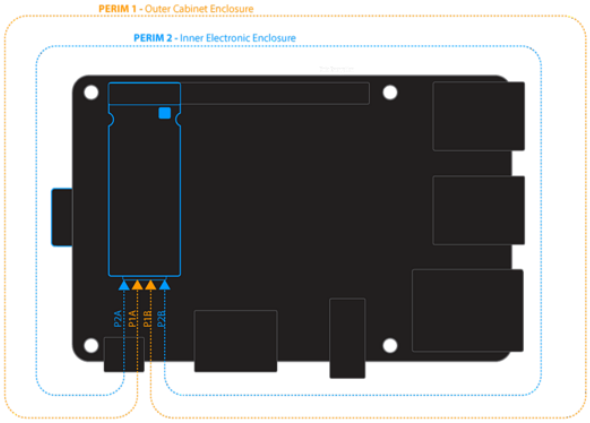
AWS IoT Integration – TLS, JITR

Zymkey delivers device-based security features that are easy to integrate with Amazon Web Services IoT, just in time certificate registration (JITR) services. Learn how > https://community.zymbit.com/t/354

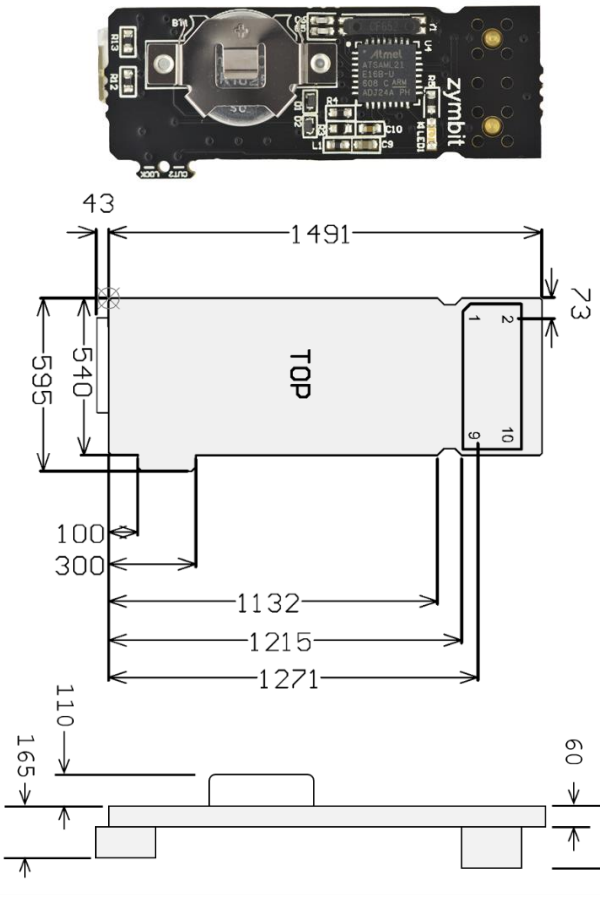


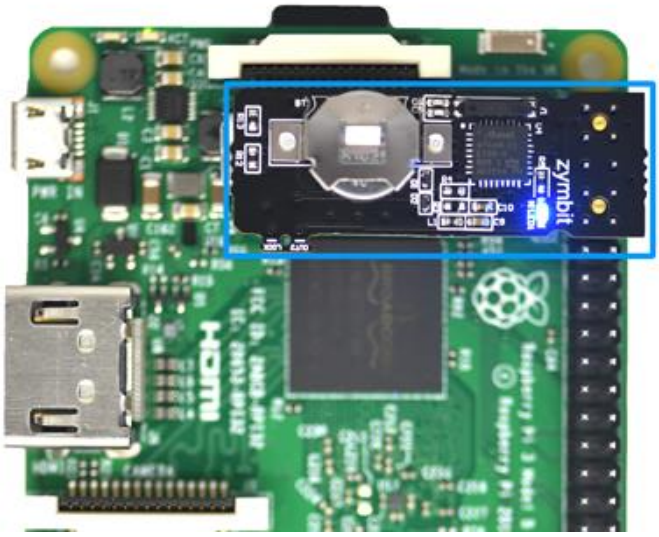
Secure Enclosure with Tamper Detection

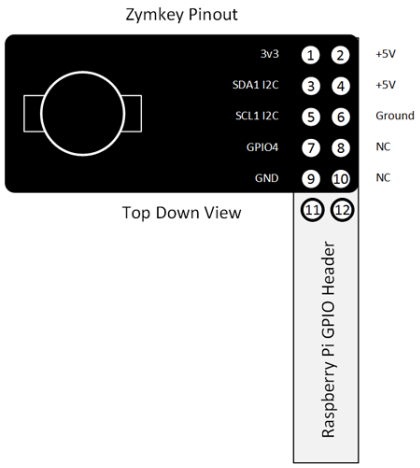
Zymkey provides multiple layers of physical tamper detection that protect unattended devices from threats in the real world. Learn how > https://community.zymbit.com/t/using-perimeter-detect/204



MECHANICAL / ELECTRICAL







DOCUMENTATION

Zymkey is designed to be easy to integrate. 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
- CAD Footprint and mechanical Files

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

zymbit