Part Number: ZYMKEY 4i
Description: HARDWARE SECURITY MODULE, RASPBERRY Pi

SCOPE

This Getting Started Guide applies to **Zymkey 4i products only.**

Zymkey 4i replaces 3i and 2i products.

Refer to Zymkey 3i 59 and Zymkey 2i 11 Getting Started Guides if you are using these products.

If you would like to upgrade your application from 3i or 2i products Contact Zymbit 31 for assistance.

Zymkey 4i is backward compatible with Zymkey 3i.

Zymkey 4i

Zymkey 4i is version four of Zymkey, designed to interface to an I2C bus. It's interfac complies to the Raspberry Pi GPIO header, but it can also be used with other I2C configurations.

In this Getting Started guide we describe how to install your Zymkey 4i to a Raspberry Pi running Rasbian Stretch.

If you are using Arch or other mainstream Linux distributions, Contact Zymbit to learn how to integrate Zymkey into your application.

Zymkey 4i Feature Upgrades

Based upon customer demand we have created two versions of Zymkey 4i.

Standard: that integrates physical security features.
Lite: that offers crypto-only services, at a lower cost.

Features	Zymkey 4i	Zymkey 4i Lite	Zymkey 3i
Crypto authentication engine	●	●	●
Key Store	● x3	● x3	● x1
TRNG	●	●	●
I2C interface	●	●	●
Real Time Clock	●		○
Tamper detect - perimeter	●		○
Tamper detect - accelerometer	●		○
OEM custom features	○	○	
event response policy			
I/O pin mapping			
perimeter detect connectorization			
packaging			
other, customer specific			

● standard feature
○ OEM option feature

HARDWARE & CONNECTORS
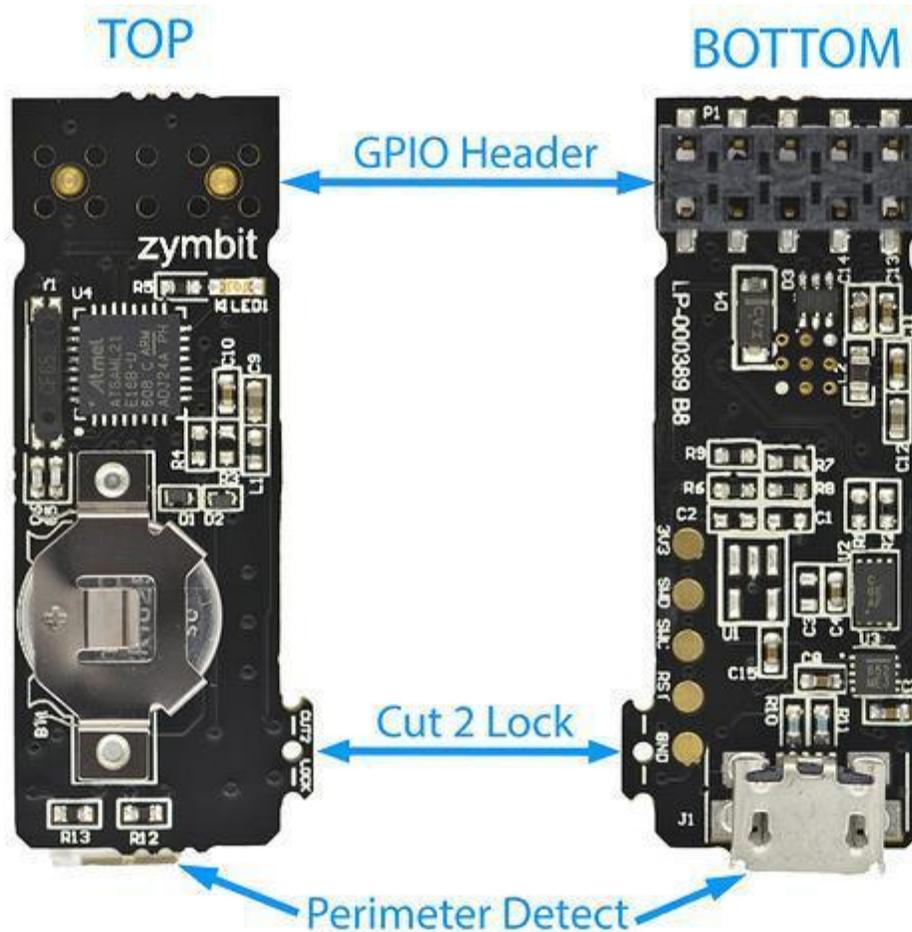
BATTERY INSTALLATION

If your Zymkey 4i shipped without a battery, then you should install it now. The battery is a 3V CR1025.
and used to support the Real Time Clock (RTC) and tamper detect features. Details on how the RTC is set to NTP can be found here. 44

(If you ordered Zymkey 4i lite, these devices do not require a battery).

**IMPORTANT:** Note the correct polarity with +ve facing upwards !!
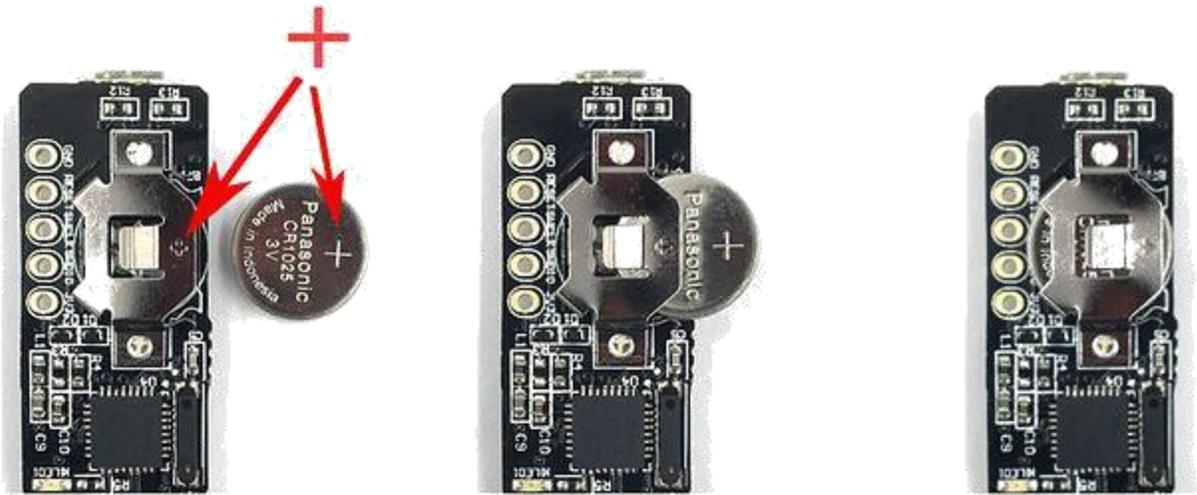
HARDWARE INSTALLATION

Power down your Raspberry Pi first !

IMPORTANT: Installing your hardware correctly is important to avoid destroying your Pi or Zymkey. Be sure to follow the images below to ensure the first 10 GPIO pins are correctly aligned with the Zymkey header. Note: the coin cell battery should be facing up.
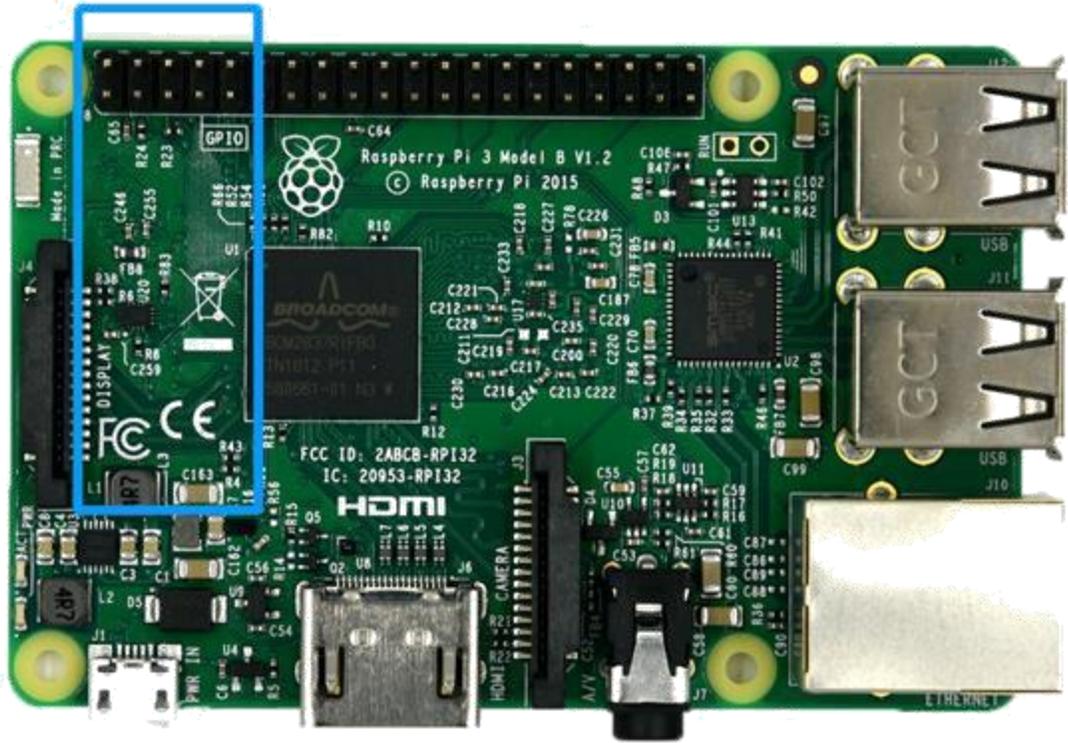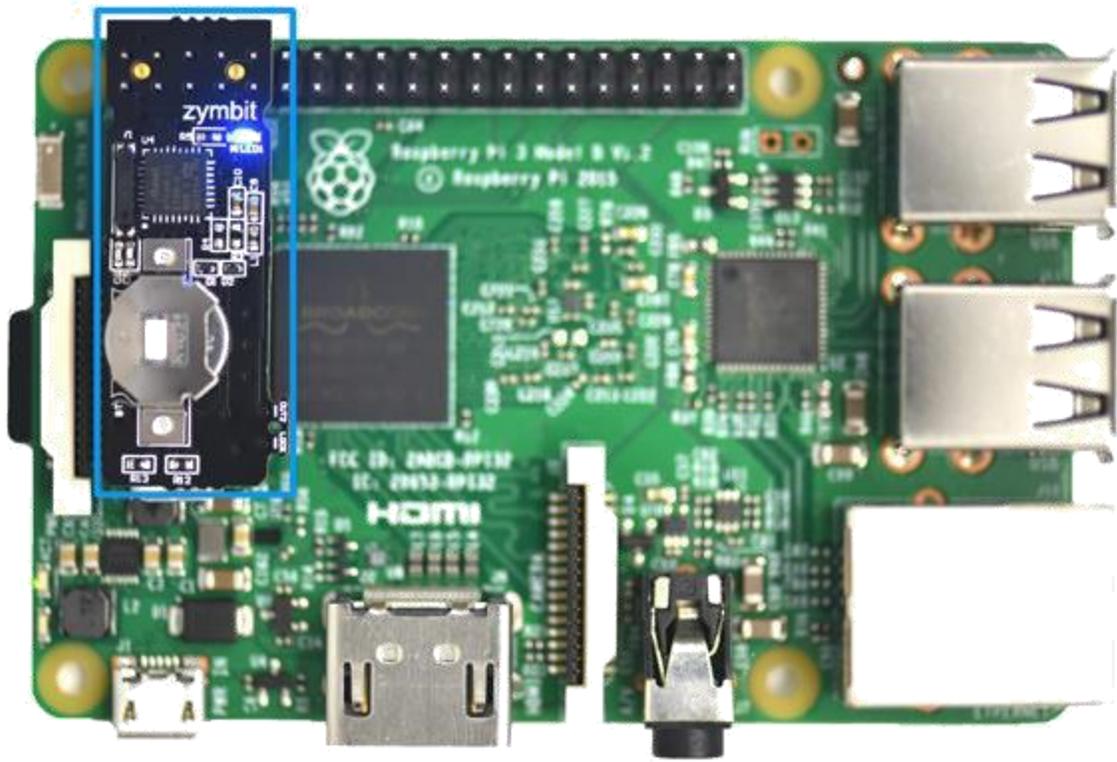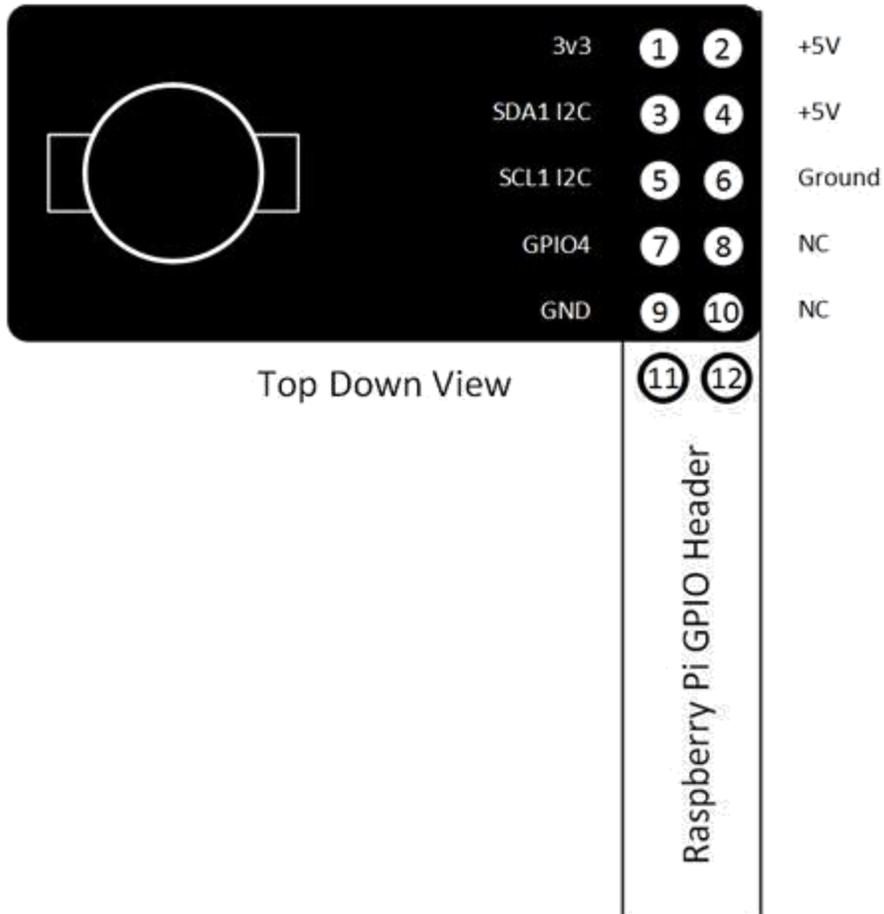
Fit the Zymkey 4i with battery facing upwards. Be sure the black connector is properly aligned with the first 10 GPIO pins and that pressed firmly down onto the header. If missaligned, this could cause damage to the Zymkey and/or your Raspberry Pi. Your Zymkey should fit relatively snug and maintain a tight interference fit around the pins.

Zymkey occupies 10 pins on the GPIO header. It can also be used with Pi Plate devices attached, or other i2c devices attached. See options later for correct address range and use of IO pins.

Zymkey Pinout

3v3	① ②	+5V
SDA1 I2C	③ ④	+5V
SCL1 I2C	⑤ ⑥	Ground
GPIO4	⑦ ⑧	NC
GND	⑨ ⑩	NC
	⑪ ⑫	

Top Down View

Raspberry Pi GPIO Header

Option: The default configuration uses GPIO4. This can be reconfigured to use another GPIO. Contact Zymbit for more details.
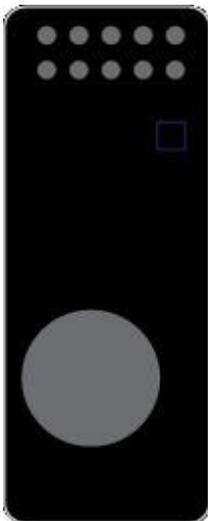
Option: Using Zymkey with another Pi Plate fitted.
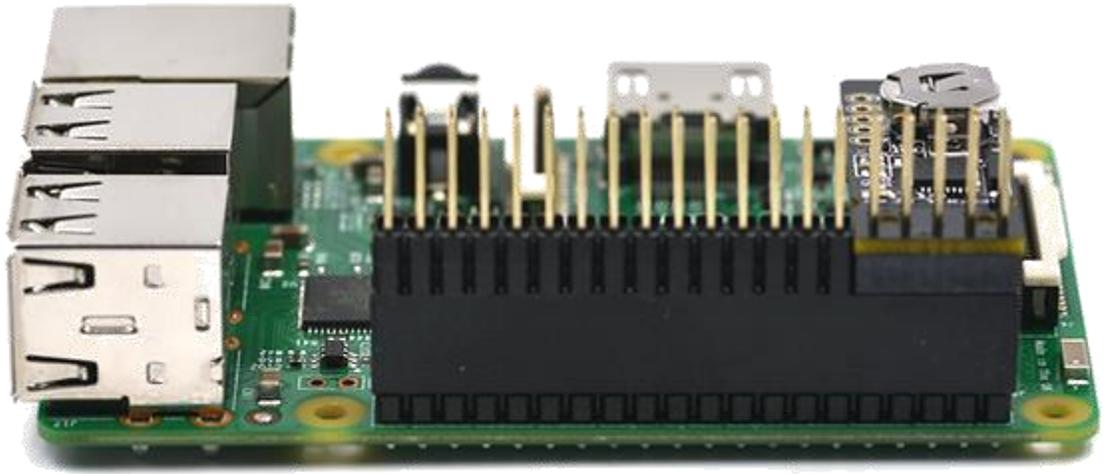
Power On, Confirm Operation

Finally, power up the pi and you will see a blue led blinking rapidly and consistently (5 blinks per second)

Zymkey operational, but not configured

(If the blue LED blinks erratically, or not at all, then there is an installation error and you should check your connections.)

Configure the I2C Bus:

Here we are going to configure the state of the I2C bus   to   "ON".

1. Log in to your pi and run `sudo raspi-config`
2. Select Interfacing Options -> I2C ->
   Would you like the ARM I2C interface to be enabled ? select (Yes), enter, enter
3. Arrow Right to Finish

Your I2C bus is now configured and ready to talk to the Zymkey. Next install the Zymkey interface software (ZKIFC) onto your Pi.

SOFTWARE PACKAGE INSTALLATION & API

For a bare raspbian system, first login to your pi.

NOTE: Your Zymkey will require a number of packages to be installed from the Raspberry Pi and Zymbit apt repositories. The following setup script will be installing a number of files and software packages on your system:

- Zymbit .service files located in the /etc/systemd/system directory
- pip

Download and install the necessary Zymbit services onto your Pi.
`curl -G https://s3.amazonaws.com/zk-sw-repo/install_zk_sw.sh | sudo bash`
(grab a cup of coffee because this will take between 4 and 20 minutes).

Binding, Device ID and Authentication.

Good security begins with assigning each device a unique and unalterable identity (Device ID), that is used to authenticate subsequent interactions with the device.

Zymkey generates a unique Device ID by measuring certain attributes of the specific host Raspberry Pi (Measurement), and then combining that Measurement with the unique ID of a specific Zymkey. The combination process uses a cryptographic function and this process is generally termed "binding".   On   completion   of   a   binding   procb**e**ss,"bound"then Zymkeytothe isPi .said   t

Zymkey can be operated in two modes - Developer and Production mode.

Developer Mode (temporary binding)

Once the software installation has finished, reboot your pi. After the reboot has completed, the pi will perform an operation that will temporarily bind the Zymkey to your pi. Once the Zymkey is bound to

the pi, the Zymkey's blue LED - shouldonceevery blink3secondsslowly-toindicate that the binding is complete.

At this point, the binding is temporary and the Zymkey can be moved to another Pi and the binding process repeated.

Zymkey operational, temporary binding to host (developer mode)
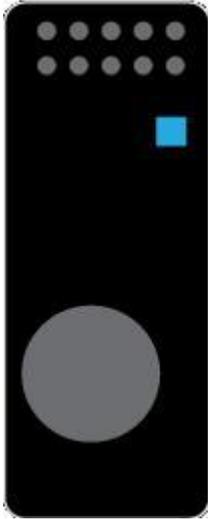
Production Mode (permanently locked binding)

When you have completed all your development work and you are ready to deploy into the field you should permanently bind your Zymkey to a 'specific' Pi. This will lo Mode.

IMPORTANT : this binding is permanent and cannot be reversed !

WARNING : Once you have locked your zymkey into production mode , we cannot gaurantee its operation if you subsequently upgrade your Linux distribution. Contact Zymbit for more information. 31

Your specific Zymkey will be locked to the specific host Pi and it is impossible to move or bind your Zymkey to another Pi. There are no factory resets, masterkeys or other forms of recovery.

(If you are not ready for permanent binding then leave it in developer mode, but beware this makes it easier for a bad actor to replace the host with a rogue hardware.)

Manual Cut-2-Lock

IMPORTANT: first power down your Pi and Zymkey. Removing the Cut-2-Lock tab can be done in situ, or by removing the Zymkey from the Pi.

Cut using sharp diagonal cutter pliers