



Zymkey App Utils: Python

Generated by Doxygen 1.8.13

Contents

1	Intro	1
2	Hierarchical Index	5
2.1	Class Hierarchy	5
3	Class Index	7
3.1	Class List	7
4	File Index	9
4.1	File List	9
5	Class Documentation	11
5.1	zymkey.module.Zymkey Class Reference	11
5.1.1	Detailed Description	15
5.1.2	Member Function Documentation	15
5.1.2.1	clear_perimeter_detect_info()	15
5.1.2.2	create_ecdsa_public_key_file()	15
5.1.2.3	create_public_key_file()	15
5.1.2.4	create_random_file()	16
5.1.2.5	disable_public_key_export()	16
5.1.2.6	ecdh()	17
5.1.2.7	gen_ephemeral_key_pair()	17
5.1.2.8	gen_key_pair()	17
5.1.2.9	gen_wallet_child_key()	18
5.1.2.10	gen_wallet_master_seed()	18

5.1.2.11	get_accelerometer_data()	19
5.1.2.12	get_batt_volt()	19
5.1.2.13	get_cpu_temp()	20
5.1.2.14	get_current_binding_info()	20
5.1.2.15	get_ecdsa_public_key()	20
5.1.2.16	get_firmware_version()	21
5.1.2.17	get_perimeter_detect_info()	21
5.1.2.18	get_public_key()	21
5.1.2.19	get_random()	22
5.1.2.20	get_rtc_drift()	22
5.1.2.21	get_serial_number()	22
5.1.2.22	get_slot_alloc_list()	22
5.1.2.23	get_time()	23
5.1.2.24	get_wallet_key_slot()	23
5.1.2.25	get_wallet_node_addr()	24
5.1.2.26	invalidate_ephemeral_key()	24
5.1.2.27	led_flash()	24
5.1.2.28	lock()	25
5.1.2.29	lock_binding()	25
5.1.2.30	remove_key()	26
5.1.2.31	restore_wallet_master_seed_from_bip39_mnemonic()	26
5.1.2.32	set_digital_perimeter_delays()	26
5.1.2.33	set_digital_perimeter_lp_max_bits()	28
5.1.2.34	set_digital_perimeter_lp_period()	28
5.1.2.35	set_i2c_address()	28
5.1.2.36	set_perimeter_event_actions()	30
5.1.2.37	set_tap_sensitivity()	30
5.1.2.38	sign()	31
5.1.2.39	sign_digest()	31
5.1.2.40	store_foreign_public_key()	32
5.1.2.41	unlock()	32
5.1.2.42	verify()	33
5.1.2.43	verify_digest()	33
5.1.2.44	wait_for_perimeter_event()	34
5.1.2.45	wait_for_tap()	34
5.2	zymkey.module.Zymkey.ZymkeyAccelAxisData Class Reference	35

6 File Documentation	37
6.1 zymkey/module.py File Reference	37
6.1.1 Detailed Description	37
6.1.2 Variable Documentation	38
6.1.2.1 ENCRYPTION_KEYS	38
6.1.2.2 kdfFuncTypes	38
6.1.2.3 keyTypes	38
Index	39

Chapter 1

Intro

The Zymkey App Utils library provides an API which allows user space applications to incorporate Zymkey's cryptographic features, including:

- Generation of random numbers
- Locking and unlocking of data objects
- ECDSA signature generation and verification

In addition, the Zymkey App Utils library provides interfaces for administrative functions, such as:

- Control of the LED
- Setting the i2c address (i2c units only)
- Setting the tap detection sensitivity

A Note About Files

Some of the interfaces can take a filename as an argument. The following rules must be observed when using these interfaces:

- Absolute path names must be provided.
- For destination filenames, the permissions of the path (or existing file) must be set:
 - Write permissions for all.
 - Write permissions for common group: in this case, user `zymbit` must be added to the group that has permissions for the destination directory path and/or existing file.
 - Destination path must be fully owned by user and/or group `zymbit`.
- Similar rules exist for source filenames:
 - Read permissions for all.
 - Read permissions for common group: in this case, user `zymbit` must be added to the group that has permissions for the source directory path and/or existing file.
 - Source path must be fully owned by user and/or group `zymbit`.

Crypto Features

Random Number Generation

This feature is useful when the default host random number generator is suspected of having **cryptographic weakness**. It can also be used to supplement existing random number generation sources. Zymkey bases its random number generation on an internal TRNG (True Random Number Generator) and performs well under Fourmilab's `ent`.

Data Locker

Zymkey includes a feature, called Data Locking. This feature is essentially an AES encryption of the data block followed by an ECDSA signature trailer.

Data Locker Keys

In addition to a unique ECDSA private/public key pair, each Zymkey has two unique AES keys that are programmed at the factory.

ECDSA Operations

Each Zymkey comes out of the factory with a unique ECDSA private/public key pair. The private key is randomly programmed within hardware at the time of manufacture and never exported. In fact, Zymbit doesn't even know what the value of the private key is.

There are three ECDSA operations available:

- Generate signature: the Zymkey is capable of generating an ECDSA signature.
- Verification signature: the Zymkey is capable of verifying an ECDSA signature.
- Export the ECDSA public key and saving it to a file in PEM format. This operation is useful for generating a Certificate Signing Request (CSR).

Other Features

LED

The Zymkey has an LED which can be turned on, off or flashed at an interval.

i2c Address

For Zymkeys with an i2c interface, the base address can be changed to work around addressing conflicts. The default address is 0x30, but can be changed in the ranges 0x30 - 0x37 and 0x60 - 0x67.

Tap Sensitivity

The Zymkey has an accelerometer which can perform tap detection. The sensitivity of the tap detection is configurable.

Programming Language Support

Currently, C, C++ and Python are supported.

Binding

Before a Zymkey can be effectively used on a host computer, it must be "bound" to it. Binding is a process where a "fingerprint" is made which is composed of the host computer and its SD card serial numbers as well as the Zymkey serial number. If the host computer or SD card is changed from the time of binding, the Zymkey will refuse to accept commands.

To learn more about binding your zymkey, go to the Zymbit Community "Getting Started"page for your Zymkey model (e.g. [Getting Started with ZYMKEY](#))

Chapter 2

Hierarchical Index

2.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

object	
zymkey.module.Zymkey	11
zymkey.module.Zymkey.ZymkeyAccelAxisData	35

Chapter 3

Class Index

3.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

zymkey.module.Zymkey	
Return class for Zymkey.get_accelerometer_data	11
zymkey.module.Zymkey.ZymkeyAccelAxisData	35

Chapter 4

File Index

4.1 File List

Here is a list of all documented files with brief descriptions:

<code>zymkey/module.py</code>	
Python interface class to Zymkey Application Utilities Library	37

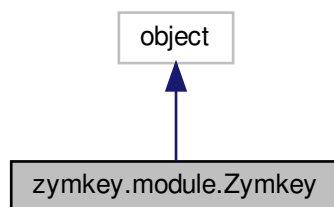
Chapter 5

Class Documentation

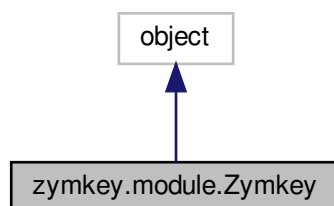
5.1 zymkey.module.Zymkey Class Reference

Return class for [Zymkey.get_accelerometer_data](#).

Inheritance diagram for zymkey.module.Zymkey:



Collaboration diagram for zymkey.module.Zymkey:



Classes

- class [ZymkeyAccelAxisData](#)

Public Member Functions

Zymkey Context

- def [__init__](#) (self)
The class initialization opens and stores an instance of a [Zymkey](#) context.
- def [__del__](#) (self)
The class destructor closes a [Zymkey](#) context.

LED Control

- def [led_on](#) (self)
Turn the LED on.
- def [led_off](#) (self)
Turn the LED off.
- def [led_flash](#) (self, on_ms, off_ms=0, num_flashes=0)
Flash the LED.

Random Number Generation

- def [get_random](#) (self, num_bytes)
Get some random bytes.
- def [create_random_file](#) (self, file_path, num_bytes)
Deposit random data in a file.

Lock Data

- def [lock](#) (self, src, dst=None, encryption_key=ZYMKEY_ENCRYPTION_KEY)
Lock up source (plaintext) data.

Unlock Data

- def [unlock](#) (self, src, dst=None, encryption_key=ZYMKEY_ENCRYPTION_KEY, raise_exception=True)
Unlock source (ciphertext) data.

ECDSA

- def [sign](#) (self, src, slot=0)
Generate a signature using the [Zymkey](#)'s ECDSA private key.
- def [sign_digest](#) (self, sha256, slot=0)
Generate a signature using the [Zymkey](#)'s ECDSA private key.
- def [verify](#) (self, src, sig, raise_exception=True, pubkey_slot=0, foreign=False)
Verify the given buffer against the given signature.
- def [verify_digest](#) (self, sha256, sig, raise_exception=True, pubkey_slot=0, foreign=False)
Verify a signature using the [Zymkey](#)'s ECDSA public key.

ECDH and KDF

- def [ecdh](#) (self, local_slot, peer_pubkey, kdf_func_type="none", salt=[], info=[], num_iterations=1, peer_↔
pubkey_slot_is_foreign=True, derived_key_size=32)

Derive a key or a pre-master secret from an ECDH operation (model >= HSM6).

Key Management

- def [create_ecdsa_public_key_file](#) (self, filename, slot=0)
[DEPRECATED] Use create_public_key_file.
- def [create_public_key_file](#) (self, filename, slot=0, foreign=False)
Create a file with the PEM-formatted public key.
- def [get_ecdsa_public_key](#) (self, slot=0)
[DEPRECATED] Use get_public_key.
- def [get_public_key](#) (self, slot=0, foreign=False)
Retrieves a public key as a binary bytearray.
- def [get_slot_alloc_list](#) (self, foreign=False)
Get a list of the allocated slots in the key store (model >= HSM6).
- def [store_foreign_public_key](#) (self, key_type, pubkey)
Stores a foreign public key on the Zymkey foreign keyring (model >= HSM6).
- def [disable_public_key_export](#) (self, slot=0, foreign=False)
Disables exporting of a public key at a given slot (model >= HSM6).
- def [gen_key_pair](#) (self, key_type)
Generates a new key pair (model >= HSM6).
- def [gen_ephemeral_key_pair](#) (self, key_type)
Generates a new ephemeral key pair (model >= HSM6).
- def [remove_key](#) (self, slot, foreign=False)
Remove a key at the designated slot (model >= HSM6).
- def [invalidate_ephemeral_key](#) (self, slot, foreign=False)
Invalidate the ephemeral key (model >= HSM6).

Digital Wallet (BIP 32/39/44)

- def [gen_wallet_master_seed](#) (self, key_type, master_gen_key, wallet_name, bip39=False)
Generates a new master seed for creating a new BIP32 wallet (model >= HSM6).
- def [gen_wallet_child_key](#) (self, parent_key_slot, index, hardened)
Generates a child key based on a parent key that is in a wallet (model >= HSM6).
- def [restore_wallet_master_seed_from_bip39_mnemonic](#) (self, key_type, master_gen_key, wallet_name, bip39_mnemonic)
Restore a wallet's master seed based on a BIP39 mnemonic string (model >= HSM6).
- def [get_wallet_node_addr](#) (self, slot)
Get a wallet node address from a key slot (model >= HSM6)
- def [get_wallet_key_slot](#) (self, node_addr, wallet_name=None, master_seed_slot=None)
Look up a wallet key slot number from a node address (model >= HSM6)

Administration

- def [set_i2c_address](#) (self, address)
Sets the i2c address of the Zymkey (i2c versions only)

Accelerometer

- def [set_tap_sensitivity](#) (self, axis='all', pct=50.0)
Sets the sensitivity of tap operations.
- def [wait_for_tap](#) (self, timeout_ms=-1)
Wait for tap event.
- def [get_accelerometer_data](#) (self)
Get current accelerometer data and tap info.

Time

- def [get_time](#) (self, precise=False)
Get current GMT time.

Binding Management

- def [lock_binding](#) (self)
Set soft binding lock.
- def [get_current_binding_info](#) (self)
Get current binding info.

Perimeter Breach

- def [set_perimeter_event_actions](#) (self, channel, action_notify=True, action_self_destruct=False)
Set perimeter breach action.
- def [set_digital_perimeter_lp_period](#) (self, lp_period)
Set the digital perimeter detect low power period (model >= HSM6).
- def [set_digital_perimeter_lp_max_bits](#) (self, max_num_bits)
Set the low power max number of bits (model >= HSM6).
- def [set_digital_perimeter_delays](#) (self, min_delay_ns, max_delay_ns)
Set the digital perimeter detect delays (model >= HSM6).
- def [wait_for_perimeter_event](#) (self, timeout_ms=-1)
Wait for a perimeter breach event to be detected.
- def [get_perimeter_detect_info](#) (self)
Get current perimeter detect info.
- def [clear_perimeter_detect_info](#) (self)
Clear perimeter detect info.

Module Info

- def [get_cpu_temp](#) (self)
Get current CPU temperature (model >= HSM6).
- def [get_rtc_drift](#) (self)
Get RTC drift (model >= HSM6).
- def [get_batt_volt](#) (self)
Get current battery voltage (model >= HSM6).

Model Information

Get [Zymkey](#) model number

This function gets the [Zymkey](#) model number.

Returns

The model number as a string.

- def [get_model_number](#) (self)
- def [get_firmware_version](#) (self)
Get [Zymkey](#) firmware version.
- def [get_serial_number](#) (self)
Get [Zymkey](#) serial number.

Static Public Attributes

- int **EPHEMERAL_KEY_SLOT** = -1
- **restype**
- **argtypes**
- **rettype**

5.1.1 Detailed Description

Return class for [Zymkey.get_accelerometer_data](#).

This class is the return type for [Zymkey.get_accelerometer_data](#). It contains the instantaneous reading of an axis along with the direction of force that caused the latest tap event. The [Zymkey](#) class definition

This class provides access to the [Zymkey](#) within Python

5.1.2 Member Function Documentation

5.1.2.1 clear_perimeter_detect_info()

```
def zymkey.module.Zymkey.clear_perimeter_detect_info (
    self )
```

Clear perimeter detect info.

This function clears all perimeter detect info and rearms all perimeter detect channels

5.1.2.2 create_ecdsa_public_key_file()

```
def zymkey.module.Zymkey.create_ecdsa_public_key_file (
    self,
    filename,
    slot = 0 )
```

[DEPRECATED] Use [create_public_key_file](#).

Create a file with the PEM-formatted ECDSA public key.

This method is useful for generating a Certificate Signing Request.

Parameters

<i>filename</i>	The absolute file path where the public key will be stored in PEM format.
<i>slot</i>	This parameter specifies the key slot for the public key.

5.1.2.3 create_public_key_file()

```
def zymkey.module.Zymkey.create_public_key_file (
    self,
    filename,
```

```
slot = 0,
foreign = False )
```

Create a file with the PEM-formatted public key.

This method is useful for generating a Certificate Signing Request.

Parameters

<i>filename</i>	The absolute file path where the public key will be stored in PEM format.
<i>slot</i>	This parameter specifies the key slot for the public key. Zymkey and HSM4 have slots 0, 1, and 2.
<i>slot_is_foreign</i>	If true, designates the pubkey slot to come from the foreign keystore (model \geq HSM6).

5.1.2.4 create_random_file()

```
def zymkey.module.Zymkey.create_random_file (
    self,
    file_path,
    num_bytes )
```

Deposit random data in a file.

Parameters

<i>file_path</i>	The absolute path name for the destination file
<i>num_bytes</i>	The number of random bytes to get

5.1.2.5 disable_public_key_export()

```
def zymkey.module.Zymkey.disable_public_key_export (
    self,
    slot = 0,
    foreign = False )
```

Disables exporting of a public key at a given slot (model \geq HSM6).

This method permanently disables exporting a public key from a given slot.

Parameters

<i>slot</i>	This parameter specifies the key slot for the public key.
<i>foreign</i>	If true, the slot refers to the foreign public keyring.

5.1.2.6 ecdh()

```
def zymkey.module.Zymkey.ecdh (
    self,
    local_slot,
    peer_pubkey,
    kdf_func_type = "none",
    salt = [],
    info = [],
    num_iterations = 1,
    peer_pubkey_slot_is_foreign = True,
    derived_key_size = 32 )
```

Derive a key or a pre-master secret from an ECDH operation (model >= HSM6).

Parameters

<i>local_slot</i>	This parameter specifies the local key slot to use.
<i>peer_pubkey</i>	
<i>kdf_func_type</i>	
<i>salt</i>	
<i>info</i>	

Returns

a byte array of the signature

5.1.2.7 gen_ephemeral_key_pair()

```
def zymkey.module.Zymkey.gen_ephemeral_key_pair (
    self,
    key_type )
```

Generates a new ephemeral key pair (model >= HSM6).

This method generates a new ephemeral key pair of the specified type, overwriting the previous ephemeral key pair.

Parameters

<i>key_type</i>	This parameter indicates the EC curve type that should be associated with the new key pair.
-----------------	---

5.1.2.8 gen_key_pair()

```
def zymkey.module.Zymkey.gen_key_pair (
    self,
    key_type )
```

Generates a new key pair (model \geq HSM6).

This method generates a new key pair of the specified type.

Parameters

<i>key_type</i>	This parameter indicates the EC curve type that should be associated with the new key pair.
-----------------	---

Returns

the slot allocated to the key or less than one for failure.

5.1.2.9 gen_wallet_child_key()

```
def zymkey.module.Zymkey.gen_wallet_child_key (
    self,
    parent_key_slot,
    index,
    hardened )
```

Generates a child key based on a parent key that is in a wallet (model \geq HSM6).

This method generates a child key based on a parent key that is in a wallet.

Parameters

<i>parent_key_slot</i>	This parameter specifies the parent key slot. This key must already be part of a wallet.
<i>index</i>	This parameter represents the index for the child key derivation which becomes part of the node address.
<i>hardened</i>	If true, the key is a hardened key.

Returns

the allocated slot on success

5.1.2.10 gen_wallet_master_seed()

```
def zymkey.module.Zymkey.gen_wallet_master_seed (
    self,
    key_type,
    master_gen_key,
    wallet_name,
    bip39 = False )
```

Generates a new master seed for creating a new BIP32 wallet (model \geq HSM6).

This method generates a new master seed for creating a new BIP32 wallet.

Parameters

<i>key_type</i>	This parameter indicates the EC curve type that should be associated with the new key pair.
<i>master_gen_key</i>	The master generator key (bytearray) used in the derivation of the child key.
<i>wallet_name</i>	The name of the wallet (string) that this master seed is attached to.
<i>bip39</i>	If true, generate the seed per BIP39 and return the mnemonic string.

Returns

a tuple with the slot and the BIP39 mnemonic if specified

5.1.2.11 get_accelerometer_data()

```
def zymkey.module.Zymkey.get_accelerometer_data (
    self )
```

Get current accelerometer data and tap info.

This function gets the most recent accelerometer data in units of g forces plus the tap direction per axis.

Parameters

<i>x</i>	(output) An array of accelerometer readings in units of g-force. array index 0 = x axis 1 = y axis 2 = z axis tap_dir (output) The directional information for the last tap event. A value of -1 indicates that the tap event was detected in a negative direction for the axis, +1 for a positive direction and 0 for stationary.
----------	---

5.1.2.12 get_batt_volt()

```
def zymkey.module.Zymkey.get_batt_volt (
    self )
```

Get current battery voltage (model >= HSM6).

This function gets the current battery voltage.

Returns

The battery voltage as a float

5.1.2.13 get_cpu_temp()

```
def zymkey.module.Zymkey.get_cpu_temp (
    self )
```

Get current CPU temperature (model >= HSM6).

This function gets the current HSM CPU temperature.

Returns

The CPU temperature in celsius as a float

5.1.2.14 get_current_binding_info()

```
def zymkey.module.Zymkey.get_current_binding_info (
    self )
```

Get current binding info.

This function gets the current binding lock state as well as the current binding state. This API is only valid for devices in the HSM family.

Parameters

<i>binding_is_locked</i>	(output) Binary value which expresses the current binding lock state. <i>is_bound</i> (output) Binary value which expresses the current bind state.
--------------------------	---

Returns

locked, is_bound AssertionError

5.1.2.15 get_ecdsa_public_key()

```
def zymkey.module.Zymkey.get_ecdsa_public_key (
    self,
    slot = 0 )
```

[DEPRECATED] Use get_public_key.

Retrieves the ECDSA public key as a binary bytearray.

This method is used to retrieve the public key in binary form.

Parameters

<i>slot</i>	This parameter specifies the key slot for the public key.
-------------	---

5.1.2.16 get_firmware_version()

```
def zymkey.module.Zymkey.get_firmware_version (
    self )
```

Get [Zymkey](#) firmware version.

This function gets the [Zymkey](#) firmware version.

Returns

The firmware version as a string.

5.1.2.17 get_perimeter_detect_info()

```
def zymkey.module.Zymkey.get_perimeter_detect_info (
    self )
```

Get current perimeter detect info.

This function gets the timestamp of the first perimeter detect event for the given channel. The index corresponds to the channel specified in `set_perimeter_event_actions`.

Returns

The array of timestamps for each channel for the first detected event in epoch seconds

5.1.2.18 get_public_key()

```
def zymkey.module.Zymkey.get_public_key (
    self,
    slot = 0,
    foreign = False )
```

Retrieves a public key as a binary bytearray.

This method is used to retrieve the public key in binary form.

Parameters

<i>slot</i>	This parameter specifies the key slot for the public key. Zymkey and HSM4 have slots 0, 1, and 2.
-------------	---

Returns

Bytearray of the public key

5.1.2.19 get_random()

```
def zymkey.module.Zymkey.get_random (
    self,
    num_bytes )
```

Get some random bytes.

Parameters

<i>num_bytes</i>	The number of random bytes to get
------------------	-----------------------------------

5.1.2.20 get_rtc_drift()

```
def zymkey.module.Zymkey.get_rtc_drift (
    self )
```

Get RTC drift (model >= HSM6).

This function gets the current RTC drift.

Returns

The RTC drift as a float

5.1.2.21 get_serial_number()

```
def zymkey.module.Zymkey.get_serial_number (
    self )
```

Get [Zymkey](#) serial number.

This function gets the [Zymkey](#) serial number.

Returns

The serial number as a string.

5.1.2.22 get_slot_alloc_list()

```
def zymkey.module.Zymkey.get_slot_alloc_list (
    self,
    foreign = False )
```

Get a list of the allocated slots in the key store (model >= HSM6).

This method gets a list of the allocated slots in the key store.

Parameters

<i>foreign</i>	If True, the allocation list of the foreign key store is returned
----------------	---

Returns

the allocation list and the maximum number of keys

5.1.2.23 get_time()

```
def zymkey.module.Zymkey.get_time (
    self,
    precise = False )
```

Get current GMT time.

This function is called to get the time directly from a [Zymkey](#)'s Real Time Clock (RTC)

Parameters

<i>precise</i>	If true, this API returns the time after the next second falls. This means that the caller could be blocked up to one second. If False, the API returns immediately with the current time reading.
----------------	--

Returns

The time in seconds from the epoch (Jan. 1, 1970)

5.1.2.24 get_wallet_key_slot()

```
def zymkey.module.Zymkey.get_wallet_key_slot (
    self,
    node_addr,
    wallet_name = None,
    master_seed_slot = None )
```

Look up a wallet key slot number from a node address (model >= HSM6)

This method gets a wallet key slot number from its node address and wallet name or master seed key slot. Either the wallet name or the master seed slot must be present.

Parameters

<i>node_addr</i>	The desired node address to look up
<i>wallet_name</i>	The name of the wallet that the node address belongs to. Either this parameter or master_seed_slot must be specified or this function will fail.
<i>master_seed_slot</i>	The master seed slot that the node address belongs to. Either this parameter or wallet_name must be specified or this function will fail.

Returns

the key slot.

5.1.2.25 get_wallet_node_addr()

```
def zymkey.module.Zymkey.get_wallet_node_addr (
    self,
    slot )
```

Get a wallet node address from a key slot (model \geq HSM6)

This method gets a wallet entry's node address from its key slot assignment. The wallet name and master seed slot are also returned.

Parameters

<i>slot</i>	The key slot assignment.
-------------	--------------------------

Returns

the node address, wallet name and master seed key slot.

5.1.2.26 invalidate_ephemeral_key()

```
def zymkey.module.Zymkey.invalidate_ephemeral_key (
    self,
    slot,
    foreign = False )
```

Invalidate the ephemeral key (model \geq HSM6).

This method invalidates the ephemeral key, effectively removing it from service until a new key is generated.

5.1.2.27 led_flash()

```
def zymkey.module.Zymkey.led_flash (
    self,
    on_ms,
    off_ms = 0,
    num_flashes = 0 )
```

Flash the LED.

Parameters

<i>on_ms</i>	The amount of time in milliseconds that the LED will be on for
<i>off_ms</i>	The amount of time in milliseconds that the LED will be off for. If this parameter is set to 0 (default), the off time is the same as the on time. Generated by Doxygen
<i>num_flashes</i>	The number of on/off cycles to execute. If this parameter is set to 0 (default), the LED flashes indefinitely.

5.1.2.28 lock()

```
def zymkey.module.Zymkey.lock (
    self,
    src,
    dst = None,
    encryption_key = ZYMKEY_ENCRYPTION_KEY )
```

Lock up source (plaintext) data.

This method encrypts and signs a block of data.

The zymkey has two keys that can be used for locking/unlocking operations, designated as 'shared' and 'one-way'.

1. The one-way key is meant to lock up data only on the local host computer. Data encrypted using this key cannot be exported and deciphered anywhere else.
2. The shared key is meant for publishing data to other sources that have the capability to generate the shared key, such as the Zymbit cloud server.

Parameters

<i>src</i>	The source (plaintext) data. If typed as a basestring, it is assumed to be an absolute file name path where the source file is located, otherwise it is assumed to contain binary data.
<i>dst</i>	The destination (ciphertext) data. If specified as a basestring, it is assumed to be an absolute file name path where the destination data is meant to be deposited. Otherwise, the locked data result is returned from the method call as a bytearray. The default is 'None', which means that the data will be returned to the caller as a bytearray.
<i>encryption_key</i>	Specifies which key will be used to lock the data up. A value of 'zymkey' (default) specifies that the Zymkey will use the one-way key. A value of 'cloud' specifies that the shared key is used. Specify 'cloud' for publishing data to some other source that is able to derive the shared key (e.g. Zymbit cloud) and 'zymkey' when the data is meant to reside exclusively within the host computer.

5.1.2.29 lock_binding()

```
def zymkey.module.Zymkey.lock_binding (
    self )
```

Set soft binding lock.

This function locks the binding for a specific HSM. This API is only valid for HSM series products. AssertionError

5.1.2.30 remove_key()

```
def zymkey.module.Zymkey.remove_key (
    self,
    slot,
    foreign = False )
```

Remove a key at the designated slot (model \geq HSM6).

This method removes a key at the designated slot in either the standard key store or the foreign public keyring.

Parameters

<i>slot</i>	This parameter specifies the key slot for the key.
<i>foreign</i>	If true, a public key in the foreign keyring will be deleted.

5.1.2.31 restore_wallet_master_seed_from_bip39_mnemonic()

```
def zymkey.module.Zymkey.restore_wallet_master_seed_from_bip39_mnemonic (
    self,
    key_type,
    master_gen_key,
    wallet_name,
    bip39_mnemonic )
```

Restore a wallet's master seed based on a BIP39 mnemonic string (model \geq HSM6).

This method restores a wallet's master seed based on a BIP39 mnemonic string and a master generator key. This method can be used in the process of wallet duplication.

Parameters

<i>key_type</i>	This parameter indicates the EC curve type that should be associated with the new key pair.
<i>master_gen_key</i>	The master generator key used in the derivation of the child key.
<i>bip39_mnemonic</i>	The BIP39 mnemonic string.

Returns

the allocated slot on success

5.1.2.32 set_digital_perimeter_delays()

```
def zymkey.module.Zymkey.set_digital_perimeter_delays (
    self,
    min_delay_ns,
    max_delay_ns )
```


Set the digital perimeter detect delays (model \geq HSM6).

This function sets the digital perimeter detect delay values.

Parameters

<i>min_delay_ns</i>	The minimum delay in nanoseconds
<i>max_delay_ns</i>	The maximum delay in nanoseconds

5.1.2.33 `set_digital_perimeter_lp_max_bits()`

```
def zymkey.module.Zymkey.set_digital_perimeter_lp_max_bits (
    self,
    max_num_bits )
```

Set the low power max number of bits (model \geq HSM6).

This function sets the digital perimeter detect low power max number of bits

Parameters

<i>max_num_bits</i>	The perimeter detect low power max number of bits
---------------------	---

5.1.2.34 `set_digital_perimeter_lp_period()`

```
def zymkey.module.Zymkey.set_digital_perimeter_lp_period (
    self,
    lp_period )
```

Set the digital perimeter detect low power period (model \geq HSM6).

This function sets the digital perimeter detect low power period (microseconds).

Parameters

<i>lp_period</i>	The perimeter detect low power period in microseconds.
------------------	--

5.1.2.35 `set_i2c_address()`

```
def zymkey.module.Zymkey.set_i2c_address (
    self,
    address )
```

Sets the i2c address of the [Zymkey](#) (i2c versions only)

This method should be called if the i2c address of the [Zymkey](#) is shared with another i2c device on the same i2c bus. The default i2c address for [Zymkey](#) units is 0x30. Currently, the address may be set in the ranges of 0x30 - 0x37 and 0x60 - 0x67.

After successful completion of this command, the [Zymkey](#) will reset itself.

Parameters

<i>address</i>	The i2c address that the Zymkey will set itself to.
----------------	---

5.1.2.36 `set_perimeter_event_actions()`

```
def zymkey.module.Zymkey.set_perimeter_event_actions (
    self,
    channel,
    action_notify = True,
    action_self_destruct = False )
```

Set perimeter breach action.

This function specifies the action to take when a perimeter breach event occurs. The possible actions are any combination of:

- Notify host
- [Zymkey](#) self-destruct

Parameters

<i>channel</i>	(input) The channel (0 or 1) that the action flags will be applied to
<i>action_notify</i>	(input) Set a perimeter breach to notify. (default = True)
<i>action_self_destruct</i>	(input) Set a perimeter breach to self destruct. (default = False)

5.1.2.37 `set_tap_sensitivity()`

```
def zymkey.module.Zymkey.set_tap_sensitivity (
    self,
    axis = 'all',
    pct = 50.0 )
```

Sets the sensitivity of tap operations.

This method permits setting the sensitivity of the tap detection feature. Each axis may be individually configured or all at once.

Parameters

<i>axis</i>	<p>The axis to configure. Valid values include:</p> <ol style="list-style-type: none"> 1. 'all': Configure all axes with the specified sensitivity value. 2. 'x' or 'X': Configure only the x-axis 3. 'y' or 'Y': Configure only the y-axis 4. 'z' or 'Z': Configure only the z-axis
<i>pct</i>	<p>The sensitivity expressed as percentage.</p> <ol style="list-style-type: none"> 1. 0% = Shut down: Tap detection should not occur along the axis. 2. 100% = Maximum sensitivity.

5.1.2.38 sign()

```
def zymkey.module.Zymkey.sign (
    self,
    src,
    slot = 0 )
```

Generate a signature using the [Zymkey](#)'s ECDSA private key.

Parameters

<i>src</i>	This parameter contains the digest of the data that will be used to generate the signature.
<i>slot</i>	This parameter specifies the key slot used for signing.

Returns

a byte array of the signature

5.1.2.39 sign_digest()

```
def zymkey.module.Zymkey.sign_digest (
    self,
    sha256,
    slot = 0 )
```

Generate a signature using the [Zymkey](#)'s ECDSA private key.

Parameters

<i>sha256</i>	A hashlib.sha256 instance.
<i>slot</i>	This parameter specifies the key slot used for signing.

5.1.2.40 store_foreign_public_key()

```
def zymkey.module.Zymkey.store_foreign_public_key (
    self,
    key_type,
    pubkey )
```

Stores a foreign public key on the [Zymkey](#) foreign keyring (model \geq HSM6).

This method stores a foreign public key onto the [Zymkey](#) foreign public keyring.

Parameters

<i>key_type</i>	This parameter indicates the EC curve type that should be associated with the public key
<i>pubkey</i>	The public key binary data

Returns

the slot allocated to the key or less than one for failure.

5.1.2.41 unlock()

```
def zymkey.module.Zymkey.unlock (
    self,
    src,
    dst = None,
    encryption_key = ZYMKEY_ENCRYPTION_KEY,
    raise_exception = True )
```

Unlock source (ciphertext) data.

This method verifies a locked object signature and decrypts the associated ciphertext data.

The zymkey has two keys that can be used for locking/unlocking operations, designated as shared and one-way.

1. The one-way key is meant to lock up data only on the local host computer. Data encrypted using this key cannot be exported and deciphered anywhere else.
2. The shared key is meant for publishing data to other sources that have the capability to generate the shared key, such as the Zymbit cloud server.

Parameters

<i>src</i>	The source (ciphertext) data. If typed as a basestring, it is assumed to be an absolute file name path where the source file is located, otherwise it is assumed to contain binary data.
------------	--

Parameters

<i>dst</i>	The destination (plaintext) data. If specified as a basestring, it is assumed to be an absolute file name path where the destination data is meant to be deposited. Otherwise, the locked data result is returned from the method call as a bytearray. The default is 'None', which means that the data will be returned to the caller as a bytearray.
<i>encryption_key</i>	Specifies which key will be used to unlock the source data. A value of 'zymkey' (default) specifies that the Zymkey will use the one-way key. A value of 'cloud' specifies that the shared key is used. Specify 'cloud' for publishing data to another source that has the shared key (e.g. Zymbit cloud) and 'zymkey' when the data is meant to reside exclusively withing the host computer.
<i>raise_exception</i>	Specifies if an exception should be raised if the locked object signature fails.

5.1.2.42 verify()

```
def zymkey.module.Zymkey.verify (
    self,
    src,
    sig,
    raise_exception = True,
    pubkey_slot = 0,
    foreign = False )
```

Verify the given buffer against the given signature.

The public key is not specified in the parameter list to ensure that the public key that matches the [Zymkey](#)'s ECDSA private key is used.

Parameters

<i>src</i>	The buffer to verify
<i>sig</i>	This parameter contains the signature to verify.
<i>raise_exception</i>	By default, when verification fails a VerificationError will be raised, unless this is set to False
<i>pubkey_slot</i>	The key slot to use to verify the signature against. Defaults to the first key slot.
<i>foreign</i>	If false, the normal key store is referenced. Otherwise, the foreign public key store is referenced.

Returns

True for a good verification or False for a bad verification when raise_exception is False

5.1.2.43 verify_digest()

```
def zymkey.module.Zymkey.verify_digest (
    self,
    sha256,
    sig,
```

```

        raise_exception = True,
        pubkey_slot = 0,
        foreign = False )

```

Verify a signature using the [Zymkey](#)'s ECDSA public key.

The public key is not specified in the parameter list to ensure that the public key that matches the [Zymkey](#)'s ECDSA private key is used.

Parameters

<i>sha256</i>	A hashlib.sha256 instance that will be used to generate the signature.
<i>sig</i>	This parameter contains the signature to verify.
<i>raise_exception</i>	By default, when verification fails a VerificationError will be raised, unless this is set to False
<i>pubkey_slot</i>	The key slot to use to verify the signature against. Defaults to the first key slot.
<i>foreign</i>	If false, the normal key store is referenced. Otherwise, the foreign public key store is referenced.

Returns

True for a good verification or False for a bad verification when raise_exception is False

5.1.2.44 wait_for_perimeter_event()

```

def zymkey.module.Zymkey.wait_for_perimeter_event (
    self,
    timeout_ms = -1 )

```

Wait for a perimeter breach event to be detected.

This function is called in order to wait for a perimeter breach event to occur. This function blocks the calling thread unless called with a timeout of zero.

Parameters

<i>timeout_ms</i>	(input) The maximum amount of time in milliseconds to wait for a perimeter breach event to arrive.
-------------------	--

5.1.2.45 wait_for_tap()

```

def zymkey.module.Zymkey.wait_for_tap (
    self,
    timeout_ms = -1 )

```

Wait for tap event.

Wait for a tap event to be detected

This function is called in order to wait for a tap event to occur. This function blocks the calling thread unless called with a timeout of zero.

Parameters

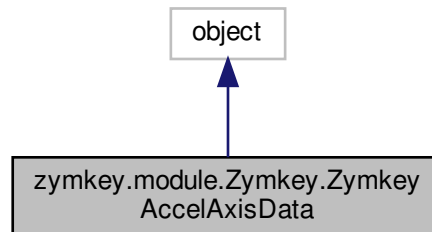
<i>timeout_ms</i>	(input) The maximum amount of time in milliseconds to wait for a tap event to arrive.
-------------------	---

The documentation for this class was generated from the following file:

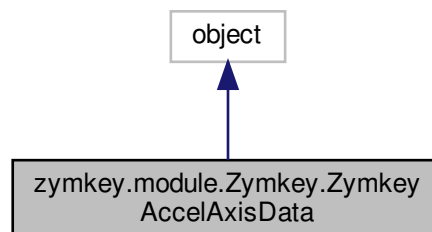
- [zymkey/module.py](#)

5.2 zymkey.module.Zymkey.ZymkeyAccelAxisData Class Reference

Inheritance diagram for zymkey.module.Zymkey.ZymkeyAccelAxisData:



Collaboration diagram for zymkey.module.Zymkey.ZymkeyAccelAxisData:



Public Member Functions

- `def __init__(self, g_force, tap_dir)`

Public Attributes

- **g_force**
- **tap_dir**

The documentation for this class was generated from the following file:

- zymkey/[module.py](#)

Chapter 6

File Documentation

6.1 zymkey/module.py File Reference

Python interface class to Zymkey Application Utilities Library.

Classes

- class [zymkey.module.Zymkey](#)
Return class for [Zymkey.get_accelerometer_data](#).
- class [zymkey.module.Zymkey.ZymkeyAccelAxisData](#)

Variables

- string **zymkey.module.CLOUD_ENCRYPTION_KEY** = 'cloud'
- string **zymkey.module.ZYMKEY_ENCRYPTION_KEY** = 'zymkey'
- tuple **zymkey.module.ENCRIPTION_KEYS**
- dictionary **zymkey.module.keyTypes**
- dictionary **zymkey.module.kdfFuncTypes**
- **zymkey.module.zkalib** = None
- list **zymkey.module.prefixes** = []

6.1.1 Detailed Description

Python interface class to Zymkey Application Utilities Library.

Author

Scott Miller

Version

1.0

Date

November 17, 2016

Copyright

Zymbit, Inc.

This file contains a Python class which interfaces to the the Zymkey Application Utilities library. This class facilitates writing user space applications which use Zymkey to perform cryptographic operations, such as:

1. Signing of payloads using ECDSA
2. Verification of payloads that were signed using Zymkey
3. Exporting the public key that matches Zymkey's private key
4. "Locking" and "unlocking" data objects
5. Generating random data Additionally, there are methods for changing the i2c address (i2c units only), setting tap sensitivity and controlling the LED.

6.1.2 Variable Documentation**6.1.2.1 ENCRYPTION_KEYS**

```
tuple zymkey.module.ENCRYPTION_KEYS
```

Initial value:

```
1 = (
2     CLOUD_ENCRYPTION_KEY,
3     ZYMKEY_ENCRYPTION_KEY
4 )
```

6.1.2.2 kdfFuncTypes

```
dictionary zymkey.module.kdfFuncTypes
```

Initial value:

```
1 = {
2     "none" : 0,
3     "rfc5869-sha256" : 1,
4     "rfc5869-sha512" : 2,
5     "pbkdf2-sha256" : 3,
6     "pbkdf2-sha512" : 4
7 }
```

6.1.2.3 keyTypes

```
dictionary zymkey.module.keyTypes
```

Initial value:

```
1 = {
2     "secp256r1" : 0,
3     "nistp256" : 0,
4     "secp256k1" : 1
5 }
```

Index

clear_perimeter_detect_info
 zymkey::module::Zymkey, [15](#)
create_ecdsa_public_key_file
 zymkey::module::Zymkey, [15](#)
create_public_key_file
 zymkey::module::Zymkey, [15](#)
create_random_file
 zymkey::module::Zymkey, [16](#)

disable_public_key_export
 zymkey::module::Zymkey, [16](#)

ENCRYPTION_KEYS
 module.py, [38](#)
ecdh
 zymkey::module::Zymkey, [16](#)

gen_ephemeral_key_pair
 zymkey::module::Zymkey, [17](#)
gen_key_pair
 zymkey::module::Zymkey, [17](#)
gen_wallet_child_key
 zymkey::module::Zymkey, [18](#)
gen_wallet_master_seed
 zymkey::module::Zymkey, [18](#)
get_accelerometer_data
 zymkey::module::Zymkey, [19](#)
get_batt_volt
 zymkey::module::Zymkey, [19](#)
get_cpu_temp
 zymkey::module::Zymkey, [19](#)
get_current_binding_info
 zymkey::module::Zymkey, [20](#)
get_ecdsa_public_key
 zymkey::module::Zymkey, [20](#)
get_firmware_version
 zymkey::module::Zymkey, [21](#)
get_perimeter_detect_info
 zymkey::module::Zymkey, [21](#)
get_public_key
 zymkey::module::Zymkey, [21](#)
get_random
 zymkey::module::Zymkey, [22](#)
get_rtc_drift
 zymkey::module::Zymkey, [22](#)
get_serial_number
 zymkey::module::Zymkey, [22](#)
get_slot_alloc_list
 zymkey::module::Zymkey, [22](#)
get_time
 zymkey::module::Zymkey, [23](#)
get_wallet_key_slot
 zymkey::module::Zymkey, [23](#)
get_wallet_node_addr
 zymkey::module::Zymkey, [24](#)

invalidate_ephemeral_key
 zymkey::module::Zymkey, [24](#)

kdfFuncTypes
 module.py, [38](#)
keyTypes
 module.py, [38](#)

led_flash
 zymkey::module::Zymkey, [24](#)
lock
 zymkey::module::Zymkey, [25](#)
lock_binding
 zymkey::module::Zymkey, [25](#)

module.py
 ENCRYPTION_KEYS, [38](#)
 kdfFuncTypes, [38](#)
 keyTypes, [38](#)

remove_key
 zymkey::module::Zymkey, [25](#)
restore_wallet_master_seed_from_bip39_mnemonic
 zymkey::module::Zymkey, [26](#)

set_digital_perimeter_delays
 zymkey::module::Zymkey, [26](#)
set_digital_perimeter_lp_max_bits
 zymkey::module::Zymkey, [28](#)
set_digital_perimeter_lp_period
 zymkey::module::Zymkey, [28](#)
set_i2c_address
 zymkey::module::Zymkey, [28](#)
set_perimeter_event_actions
 zymkey::module::Zymkey, [30](#)
set_tap_sensitivity
 zymkey::module::Zymkey, [30](#)
sign
 zymkey::module::Zymkey, [31](#)
sign_digest
 zymkey::module::Zymkey, [31](#)
store_foreign_public_key
 zymkey::module::Zymkey, [32](#)

unlock

- zymkey::module::Zymkey, 32
- verify
 - zymkey::module::Zymkey, 33
- verify_digest
 - zymkey::module::Zymkey, 33
- wait_for_perimeter_event
 - zymkey::module::Zymkey, 34
- wait_for_tap
 - zymkey::module::Zymkey, 34
- zymkey.module.Zymkey, 11
- zymkey.module.Zymkey.ZymkeyAccelAxisData, 35
- zymkey/module.py, 37
- zymkey::module::Zymkey
 - clear_perimeter_detect_info, 15
 - create_ecdsa_public_key_file, 15
 - create_public_key_file, 15
 - create_random_file, 16
 - disable_public_key_export, 16
 - ecdh, 16
 - gen_ephemeral_key_pair, 17
 - gen_key_pair, 17
 - gen_wallet_child_key, 18
 - gen_wallet_master_seed, 18
 - get_accelerometer_data, 19
 - get_batt_volt, 19
 - get_cpu_temp, 19
 - get_current_binding_info, 20
 - get_ecdsa_public_key, 20
 - get_firmware_version, 21
 - get_perimeter_detect_info, 21
 - get_public_key, 21
 - get_random, 22
 - get_rtc_drift, 22
 - get_serial_number, 22
 - get_slot_alloc_list, 22
 - get_time, 23
 - get_wallet_key_slot, 23
 - get_wallet_node_addr, 24
 - invalidate_ephemeral_key, 24
 - led_flash, 24
 - lock, 25
 - lock_binding, 25
 - remove_key, 25
 - restore_wallet_master_seed_from_bip39_
mnemonic, 26
 - set_digital_perimeter_delays, 26
 - set_digital_perimeter_lp_max_bits, 28
 - set_digital_perimeter_lp_period, 28
 - set_i2c_address, 28
 - set_perimeter_event_actions, 30
 - set_tap_sensitivity, 30
 - sign, 31
 - sign_digest, 31
 - store_foreign_public_key, 32
 - unlock, 32
 - verify, 33
 - verify_digest, 33
 - wait_for_perimeter_event, 34
 - wait_for_tap, 34