Device Name	**Device Part Numbers and Revision Ranges**
Zymkey 4i	Z044-01-000-F1
HSM4	Z240-01-000-D1
HSM6	Z260-01-000-A1

Manufacturer: Zymbit

Volatile Memory

Type	Size	User Accessible/ System Accessible	Battery Backup?	Purpose	Tamper Event Cleared?[1]	Method of Clearing[2]
(Zymkey 4i, HSM4)						
SRAM	16 kbytes	Yes/Yes	Yes	RAM	Partially	Remove backup battery, cycle power
(HSM6)						
SRAM	32 kbytes	Yes/Yes	Yes	RAM	Partially	Remove backup battery, cycle power
(Zymkey 4i, HSM4, HSM6)						
SRAM	ATECC	Yes/Yes	No	RAM	Access Keys Cleared	Cycle power

Non-Volatile Memory

Type	Size	User Accessible/ System Accessible	Battery Backup?	Purpose	Tamper Event Cleared?[1]	Method of Clearing[2]
(Zymkey 4i, HSM4)						
Flash	128 kbytes	No/Yes		Firmware	No	Physical destruction
Flash	(part of 128 kbytes)	Yes/Yes		Secrets	Access Keys Cleared	Tamper event, or physical destruction of unit
(HSM6)						
Flash	256 kbytes	No/Yes		Firmware	No	Physical destruction
Flash	(part of 256 kbytes)	Yes/Yes		Secrets	Access Keys Cleared	Tamper event, or physical destruction of unit
EEPROM	128 kbytes	Yes/Yes		Secrets	Access Keys Cleared	Tamper event, or physical destruction of unit
(Zymkey 4i, HSM4, HSM6)						
Non-volatile	ATECC	Yes/Yes		Secure Element	Access Keys Cleared	Tamper event, or physical destruction of unit

[1] Please refer to Zymbit documentation on how to configure tamper events to delete keys and how to place the unit in production mode. Tamper events that are set to delete keys will render units unusable forever and will most likely prevent any data recovery from the device or the system that was using it.
[2] Physical destruction of unit requires destruction of silicon dies in order to remove all traces of data.

Add-on and Connected Devices

Zymbit I/O boards, development kits, and Secure Edge nodes contain expansion connectors (such as M.2, SIM, USB, microSD). Zymbit modules are typically used with host devices, which are often equipped with expansion slots and connectors (such as microSD, USB, etc.) Therefore, thus created combination devices may have expansion connectors that are populated with add-on devices that may contain volatile and/or non-volatile memory. Please refer to add-on device documentation for the respective statements of volatility. Please contact Zymbit for additional details if your device has add-on devices installed by Zymbit.

If data on an add-on device is properly encrypted using secrets properly stored only in Zymbit hardware, then access to said data will be effectively terminated following a properly configured and triggered tamper event. However, add-on storage that is either unencrypted or encrypted using other methods may be unaffected by tamper events and may thus retain data. Please refer to documentation for more details.

Terms and Definitions

User Accessible: The user, by the use of the API, can directly or indirectly write or modify the contents of the memory during normal operation. This includes transmission and storage of sequences of values from user calls, such as keys or data, to a storage location. This includes both encrypted and unencrypted data.

System Accessible: Firmware or software running on the device has access to this data.

Tamper Event: Tamper event occur when a certain pre-configured trigger is detected. When configured properly, and when triggered with sufficient available power or backup power, tamper event will cause all access keys to be erased. This has similar effect to erasing the storage areas, as the data can no longer be deciphered. However, encrypted data may remain, and may be recoverable even if overwritten. Please refer to documentation on how to configure tamper events, event conditions, and how to place units in production mode so that tamper events are active. Tamper events may not be available on preview or beta units. Please contact Zymbit for further details if you have a customized build unit. Data loss may occur.

Physical Destruction: Physical destruction of units in such a manner that also destroys silicon dies is the only method to completely remove all traces of data.

Cycle Power: Remove all power from the unit, wait 5 seconds, reapply power. Rebooting the unit is not sufficient.

Volatile Memory: Volatile memory requires power to maintain the stored information. When all power is removed from this memory, its contents are lost.

Non-Volatile Memory: Non-volatile memory will retain its contents when power is removed. This type of memory typically contains firmware, user data, secret, etc.