X-Wall MX Dongle Board Quick Guide
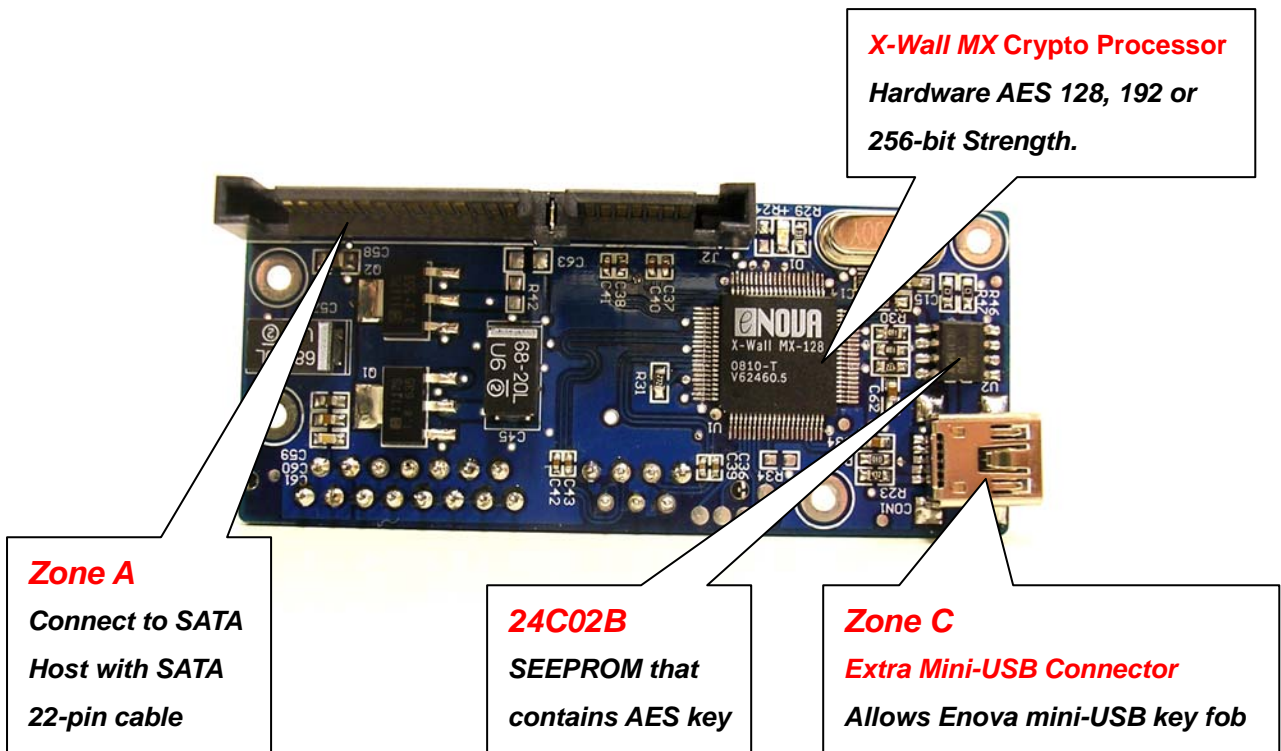
X-Wall MX Crypto Processor
Hardware AES 128, 192 or 256-bit Strength.

Zone A
Connect to SATA Host with SATA 22-pin cable

24C02B
SEEPROM that contains AES key

Zone C
Extra Mini-USB Connector
Allows Enova mini-USB key fob

Figure 1. The front view of the MX dongle board

Zone B
Connect to SATA disk drive

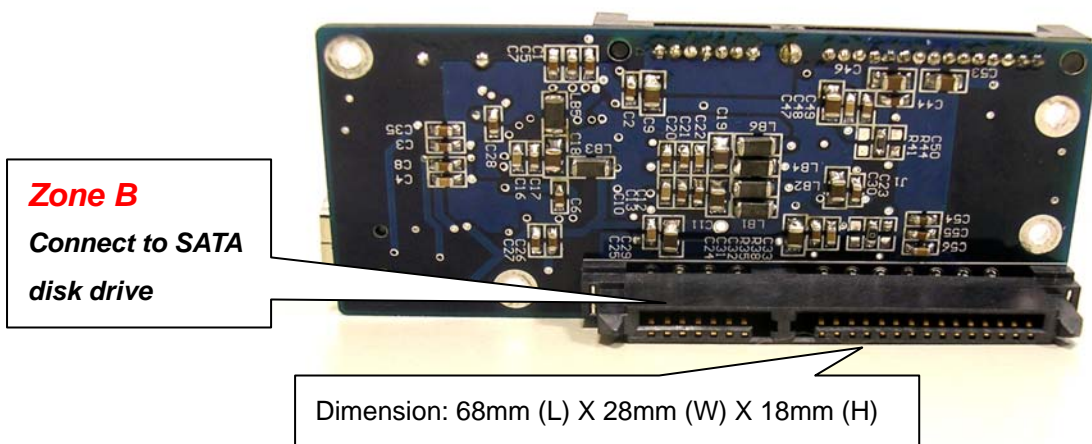Dimension: 68mm (L) X 28mm (W) X 18mm (H)

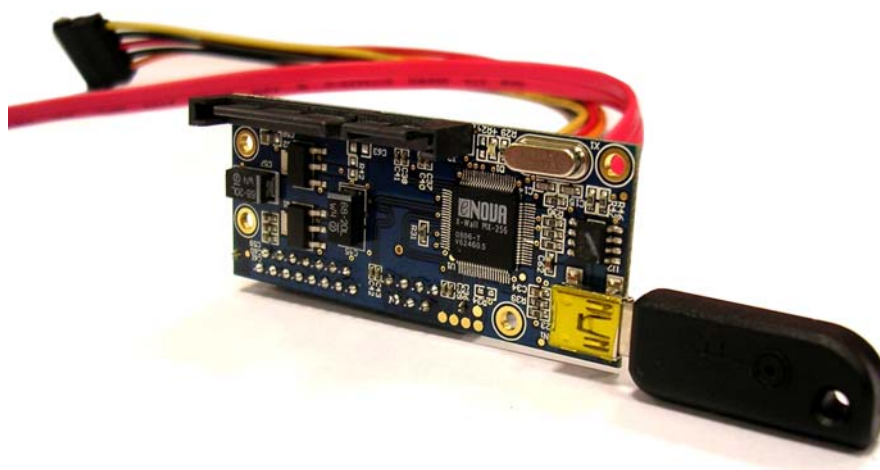Figure 2. The back view of the MX dongle board. The measured length is in mm.

Figure 3.   The MX dongle board is affixed with a standard SATA 22-pin cable to the host and an Enova mini-USB type key fob to the socket in Zone C.

Quick Installation

Zone	Description
A	SATA A channel – Connect to motherboard SATA host using standard SATA 22-Pin cable.
B	SATA B channel – Connect to SATA disk drive via direct insertion.
C	Socket for key fob insert. The AES secret key code is written to the on-board EEPROM. Or, it can be done with the external key fob. If your board comes with an external key fob, it will not have an on-board EEPROM.

1. Connect the A connector (SATA channel A as illustrated in Figure 1) to your motherboard or controller SATA host via a standard SATA 22-Pin cable.
2. Connect the B connector (SATA channel B as illustrated in Figure 1) to your SATA hard disk via direct insertion.
3. The dongle board is default at Crypto Mode, which means the key code is affixed to the dongle board as a form of key fob. If key fob is not applied, the MX dongle board acts as a pure ByPass mode, which read/write data blocks in clear text. If the key fob is applied, the MX dongle board enters into Crypto mode for regular cryptographic operations.
4. For development purpose, the AES key is affixed to the key fob. To alter AES key and later on the development stage to deliver the AES key, remove the key fob.
5. Power up your System.
6. Partition and Format this new *X-Wall MX* controlled disk drive with key fob ON and load OS and/or other applications software just like what you had performed with a regular unencrypted disk drive. The *X-Wall MX* automatically and transparently encrypts when you write and decrypts when you read.