
# *X-Wall DX USB OTG SPECIFICATION_APPROVAL SHEET*
# *Rev. 1.5*

Customer's Name: _____

Product SKU (Stock Keeping Unit) & Product Description:

***X-Wall DX-256*** *– USB OTG real-time crypto module with AES ECB 256-bit;*

***X-Wall DX-256C*** *– USB OTG real-time crypto module with AES CBC 256-bit;*

Date of Approval: _____

Approved By: _____

## Revision History

| Rev No. | Description | Author | Rev. Date |
|---|---|---|---|
| 0.9 | Draft release | C.Y Chung & Butz Huang | 12/10/2010 |
| 1.0 | Initial Release | R. Wann | 1/25/2011 |
| 1.1 | Add functional description over ESA software | R. Wann | 1/27/2011 |
| 1.2 | Revising Product SKU, SPI Flash chip supported | R. Wann B. Huang | 2/8/2011 |
| 1.2.1 | Remove QFN Package availability; add approval sheet | R. Wann | 08/30/2011 |
| | Intentionally left blank | | |
| 1.2.2 | Minor Revision | R. Wann | 01/02/2012 |
| 1.3 | Change Operating Temperature to 0~70<br>Remove BOM. Add SPI flash supported | B. Huang | 03/28/2013 |
| 1.3.1 | Modify typical application schematics; Add alternative application schematics; Add flash controller & NAND flash support list; Modify SPI flash support list (Delete 512k); Change length matching from 150 mil to 20 mil; Modify page number in table of content; | B.Huang | 12/24/2013 |
| 1.4 | General Editing | R. Wann | 12/31/2013 |
| 1.5 | Adding Block Diagram; Significant Editing | R. Wann | 03/21/2014 |

***Asia Pacific***
***Enova Technology Corporation***
1st Floor, #11, Research & Development 2nd Rd.
Science-based Industrial Park, Hsin-Chu City
Taiwan 30076, Republic of China
P +886 3 577 2767 F +886 3 577 2770
www.enovatech.net; info@enovatech.net;

***North America***
***Enova Technology***
1918 Junction Avenue
San Jose, California 95131, USA
P +1 510 825 7900
http://www.enovatech.com
www.enovatech.com; info@enovatech.com

# Table of Content

# Introduction

The patents protected[1] ***X-Wall DX USB OTG*** is the *9th* generation of the *X-Wall* real-time hardware full disk encryption processor capable of encrypting all USB Mass storage class (MSC) devices at USB2.0 wire speed with NIST (National Institute of Standards and Technology) and CSE (Communication Security Establishment) certified hardware AES ECB and CBC up to 256-bit strength[2]. Entire data-at-rest including MBR (Master Boot Record) and Boot Sectors are hardware AES encrypted to attain the highest possible security level. The *X-Wall DX* is a ***USB OTG*** crypto module specifically engineered to secure all USB MSC storage devices including hard drive, SSD and Flash so that corporate assets and confidentiality are preserved. Non USB MSC devices are passing through.

There are three possible solutions using the new X-Wall DX USB OTG real-time crypto module: 1. Full Disk Encryptiion (FDE) to all connected USB MSC storage devices including DVD, CDR and Blue-Ray; 2. File/Folder Encryption (FFE) to any host detectable storage drives including cloud storages; and 3. FDE to the connected USB MSC devices + FFE to all host detectable storage devices.

The *X-Wall DX USB OTG* has equipped with complete USB2.0 host and device protocol stacks thus can be embedded onto a system motherboard, integrated onto a USB/Flash or USB/SATA bridge controller, or as an independent adaptor.

Enova Technology has dedicated research and development in hardware real-time full disk encryption technology since year 2000 and has brought up a variety of real-time crypto ASIC and system solutions including high speed interfaced IDE (ATA), SATA (Serial ATA), USB2.0/USB3.0, U.S. Government CAC/PIV based 2-factor authentication encrypted storage, SecureRAID 1U, SecureRAID Mini-Tower and SecureNAS T1. Please reference to Enova Technology website (www.enovatech.com) for comprehensive review. Additionally, the company's innovated *X-Wall MX*, the SATA-to-SATA real-time full disk encryption processor, has obtained ***FIPS 140-2 (US Federal Information Processing Standard) certifications***[3]***.***

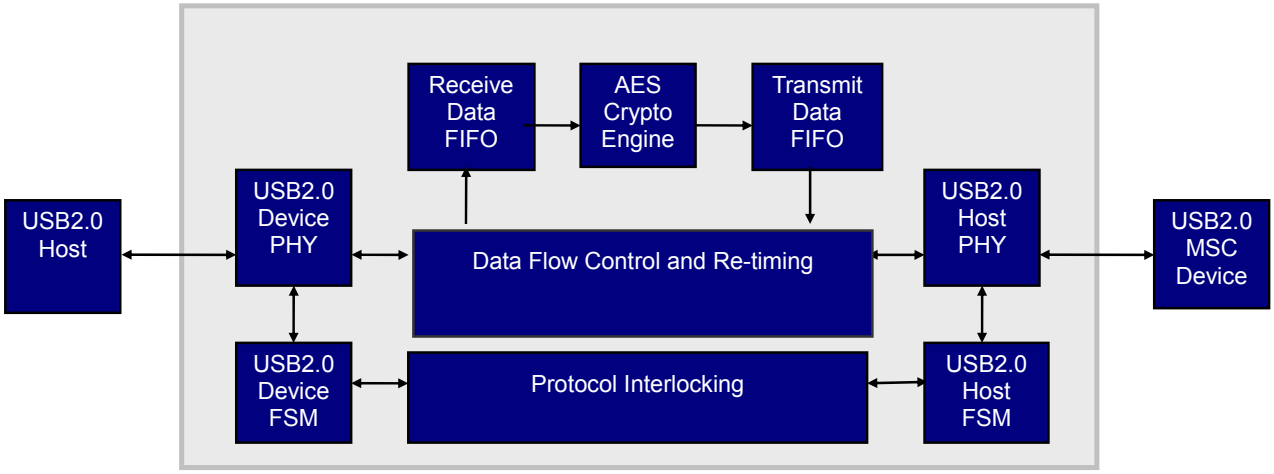
## *Functional Blocks*

---

1 **US Patents: 7,136,995; Taiwan Patents: I330320; 179354; 190310; PRC Patents: 625110; Japan Patents: 306383; Korea Patents: 0445288; 0711190;**

2 NIST & CSE hardware AES ECB and CBC implementation certificates #60 and #250 respectively.

3 ***FIPS 140-2 certification numbers 1471 and 1472 for the X-Wall MX-256 and X-Wall MX-256C crypto module respectively.***




**The** *X-Wall DX USB OTG* sits between the USB2.0/3.0 host and USB2.0/3.0 device, encrypting data before it is written to the storage and decrypting while it is read. The cryptographic operation is totally transparent to users thus produces no performance loss while all data-at-rest are hardware AES 256-bit encrypted. Enova provides customized API library SDK specifically targeting Linux, Windows and Macintosh operating systems.

## *Field Application Examples*

**Securing Short Range WiFi Traffics with Hardware AES 256-bit Encryption –** Typical WiFi traffic security today is provided via software AES 128-bit encryption. Changing it into an AES 256-bit software encryption may consume huge CPU bandwidth thus degrades other functional activities. By applying the *X-Wall DX USB OTG* on the transmitting and receiving end of the WiFi devices respecitively, traffics can be re-encapsulated using USB MSC protocols to take full advantages of the true hardware AES 256-bit encryption capability offered by the *X-Wall DX USB OTG*.

**Secure VoIP Channel with Hardware AES 256-bit Encryption –** Typical VoIP channel voice communication security is provided via software encryption. However, the software solution has its major draw back in terms of CPU bandwidth and non-real-time performance. Change to hardware AES 256-bit encryption frees up available CPU bandwidth and the real-time experience may be regained – all thanks to the **X-Wall DX USB OTG.**

**Integrated onto a host motherboard** – The *X-Wall DX USB OTG* is the ideal solution to be incorporated onto a standard USB2.0 and/or USB3.0 port of a host motherboard, making the dedicated USB port capable of encrypting every USB MSC storage device that completely safeguards your corporate assets and personal privacy. Non USB MSC devices such as USB mouse and USB printer are passing through unaffected.

**Integrated onto a USB/Flash device** – The *X-Wall DX USB OTG* can be integrated onto the USB/Flash drive, making the entire Flash drive real-time encrypted. The USB/Flash device that incorporates the *X-Wall DX USB OTG* is capable of encrypting entire media without user intervention. The easily lost USB Flash drive can then be safeguarded even when it is lost to the hostile hands. The peripherals manufacturers can also choose to integrate the *X-Wall DX USB OTG* onto their current USB based product lines, adding an unprecedented value to their current product offering.

**Making an independent adapter** – The *X-Wall DX USB OTG* is also a stand alone controller that can be tightly integrated as an adapter with two USB interfaces, capable of connecting to both a USB host and a USB MSC device. The independent adapter can then be a totally transportable solution, capable of working on every standard computer that has equipped with a USB2.0 and/or USB3.0 host controller.

## *X-Wall DX USB OTG features and benefits*

| Hardware Features | Key Benefits |
|---|---|
| ➢ USB OTG that transparently encrypting any number of USB based storage, including selective file/folder. | Encrypting entire USB drive, or only selective file/folder of any host detectable drives including cloud drives, without performance degradation. |
| ➢ Compliance to USB 2.0/1.1 MSC bulk-only transport for cryptographic processing.<br>➢ Compatible with USB3.0<br>➢ Non-Mass Storage Class is passing through. | Sound security solution for cloud computing, or use it to encrypt all UFD and USB mobile storage devices; |
| ➢ NIST (USA) & CSE (Canada) certified hardware AES ECB/CBC up to 256-bit. | Deployed the same FIPS 140-2 certified crypto module that ensures the highest level of attainable security level. |
| ➢ Small 48-pins QFP/QFN form factor | Small foot print makes adoption easy and fast. |
| ➢ Support Windows XP, 7 and 8 32/64-bit<br>➢ Support MAC OS 10.7 & 10.8<br>➢ Support Linux | Customized API library SDK for specific project development. |

## *Ordering Codes*

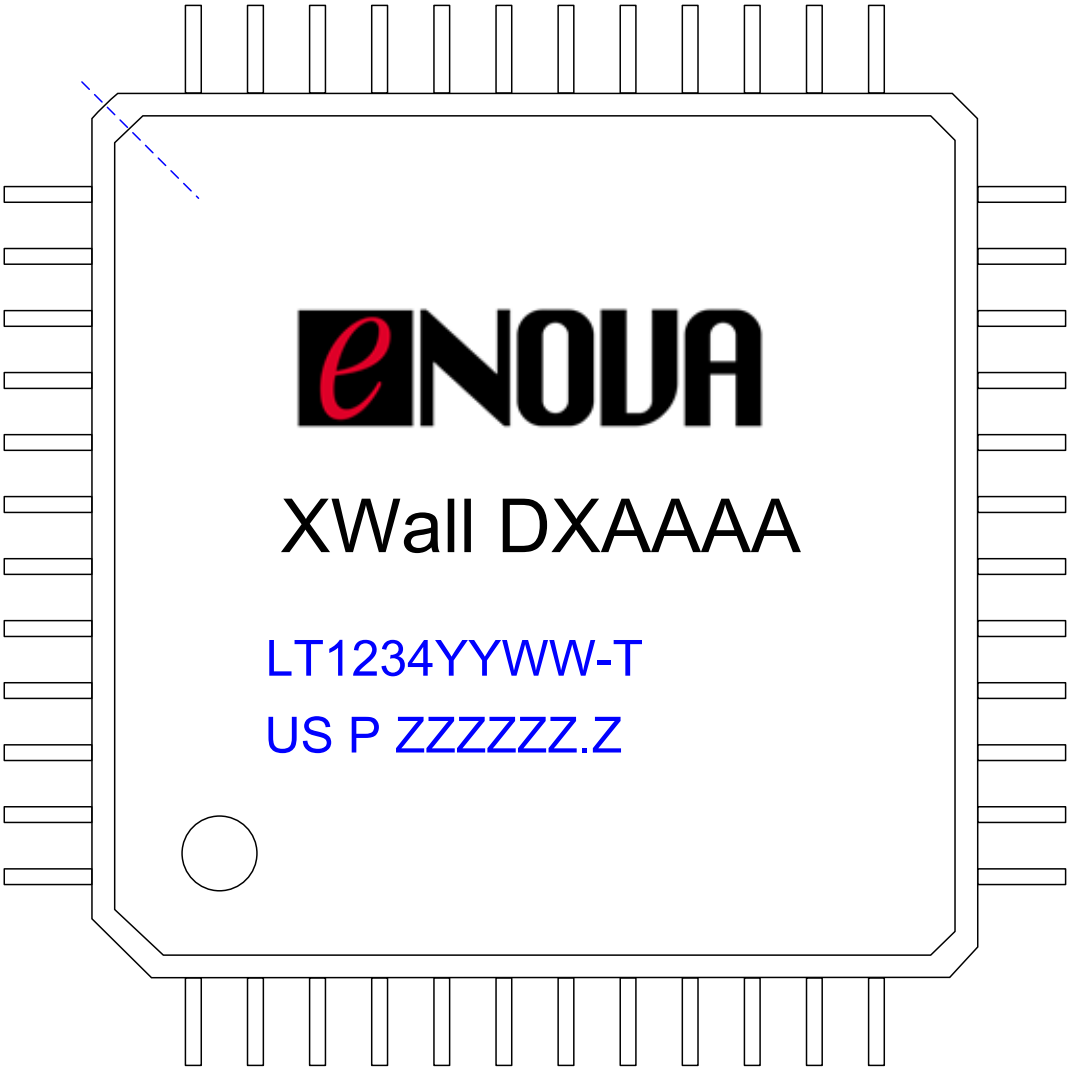
| Stock Keeping Unit | Description | AES Mode of Operation[4] (crypto mode) |
|---|---|---|
| X-Wall DX-256 | USB OTG Crypto Module with AES 256-bit strength | ECB |
| X-Wall DX-256C | USB OTG Crypto Module with AES 256-bit strength | CBC |

[4] CBC stands for Cipher Block Chaining mode of operation where as ECB stands for Electronics Code Book mode of operation. The CBC mode is preferred for Government, Enterprise, and Military applications that demand highest attainable security level.

# *X-Wall DX USB OTG* Pin Definitions

## *Pin Assignment*

All *X-Wall DX USB OTG* family ASIC shares the same pin assignment and pin definition as shown below.



## *Pin Definition and Description*

| **USB DOWNSTREAM INTERFACE WHEREBY *X-WALL DX* ACTS AS A HOST TO THE USB DEVICE** | | | | | |
|---|---|---|---|---|---|
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| USBHP | 42 | I/O | A | USB data pin data+ | Downstream connection to a USB device |
| USBHM | 41 | I/O | A | USB data pin data- | |
| USBHVRES | 37 | I/O | A | Connected to an external 8.2K Ohm resister for band-gap reference circuit. | |
| VBUSH | 38 | I | A | Connect to the VBUS pin on USB connector. | |
| Total | 4 | | | | |
| **USB UPSTREAM INTERFACE WHEREBY *X-WALL DX* ACTS AS A DEVICE TO THE USB HOST** | | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| USBFP | 10 | I/O | A | USB data pin data+ | Upstream connection to a USB Host |
| USBFM | 9 | I/O | A | USB data pin data- | |
| USBDVRES | 5 | I/O | A | Connected to an external 8.2K Ohm resister for band-gap reference circuit. | |
| VBUSF | 6 | I | A | Connect to the VBUS pin on USB connector. | |
| Total | 4 | | | | |
| **CLOCK AND PLL CONTROL PINS** | | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| XTALI | 16 | I | A | Crystal/reference clock input. | |
| XTALO | 17 | O | | Crystal/reference clock output | |
| Total | 2 | | | | |
| **FEATURE SETTING PINS** | | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| CfrEna | 36 | I | DU | Hardware trapped to enable/disable cryptographic operation.<br>1(default): Enable 0: Disable | |
| Total | 1 | | | | |
| **CONTROL AND INDICATE SIGNALS** | | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| SysRst | 1 | I | DU | Hardware master reset. | |
| Err | 29 | O | D 8mA | If the cryptographic mode is selected, an active HIGH at this pin indicates that errors are found during operation. | |
| DatXfer | 28 | O | D 8mA | Active LOW at this pin indicates that the *X-Wall DX* has detected data transfer activities at USB bus | |
| GPIO_0 | 13 | I/O | DU 8mA | 2-wire Serial clock. Pull high to 3.3V through 1.5K Ohm resistor. See also typical application schematics. | |
| | | | | Programmable general purpose I/O pin. | |
| GPIO_1 | 14 | I/O | DU 8mA | 2-wire Serial data. Pull high to 3.3V through 1.5K Ohm resistor. See also typical application schematics. | |
| | | | | Programmable general purpose I/O pin. | |
| GPIO_2<br>GPIO_3<br>GPIO_4<br>GPIO_5 | 18<br>19<br>22<br>23 | I/O | DU 8mA | Programmable general purpose I/O pins. | |
| GPIO_6 | 24 | I/O | DU 8mA | Hardware trapped to enable/disable external firmware download.<br>1(default): Disable. 0: Enable. | |
| | | | | Programmable general purpose I/O pin. | |
| Total | 10 | | | | |
| **SPI FLASH ROM INTERFACE** | | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** | |
| SCK | 31 | I | DD | SPI serial clock.. | |

| | | | | |
|---|---|---|---|---|
| MOSI | 32 | O | D<br>8mA | SPI master data output. |
| MISO | 33 | I | DD | SPI master data input. |
| SS | 34 | I | DU | SPI slave select. |
| Total | 4 | | | |
| **DEBUG INTERFACE** | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** |
| IDDQEn | 45 | I | DU | Hardware trapped to enable/disable IDDQ leakage test.<br>1(default): Disable. 0: Enable.<br>The pin is internally pull-high. During normal operation, the power-on voltage ramp up at this pin is served as an indication of a power cycle. |
| Test | 30 | I | DD | Hardware trapped for test mode selection:<br>Test / IDDQEn<br>Normal mode: 0 / 1<br>Reserved for testing purposes: 0 / 0, 1 / 0, 1 / 1 |
| Total | 2 | | | |
| **POWER GROUND** | | | | |
| **NAME** | **PIN** | **DIR** | **TYPE** | **DESCRIPTION** |
| VDD33 | 4<br>21<br>25<br>48 | | Power | 3.3V digital power for I/O cells. |
| VSSPST | 2<br>20<br>26<br>47 | | GND | 3.3V digital ground for I/O cells. |
| VSS | 3<br>15<br>27<br>46 | | GND | 1.8V digital ground for core cells. |
| VDDAUSB | 7<br>39 | | POWER | 3.3V analog power for USB macro. |
| VSSAUSB | 8<br>40 | | GND | 3.3V analog ground for USB macro. |
| VDDLUSB | 11<br>43 | | POWER | 1.8V digital power for USB macro. |
| VSDLUSB | 12<br>44 | | GND | 1.8V digital ground for USB macro. |
| Total | 20 | | | |

A: Analog  D: Digital  DU: Digital and internal pull-up  DD: Digital and internal pull down  8mA: drive strength

# Electrical Characteristics

This section contains electrical specifications for the *X-Wall DX USB OTG* crypto module. Please note, however, stressing conditions beyond the "Absolute Maximum Ratings" may cause permanent damage to the device. Operating beyond the "Maximum" condition is not recommended and extended exposure beyond the "Maximum" condition may adversely affect life and reliability of the *X-Wall DX USB OTG* crypto module.

## *Absolute Maximum Ratings*

| Symbol | Parameter | Value | | Unit |
|---|---|---|---|---|
| | | Min | Max | |
| Ts | Storage Temperature | -55 | +125 | °C |
| Ta | Operating Temperature (Normal) | 0 | +70 | °C |
| Ta' | Industrial Operating Temperature (upon special request) | -45 | +90 | °C |
| VDD33 | 3.3V Digital Supply Voltage | -0.5 | 3.6 | V |
| AVDD33 | 3.3V Analog Supply Voltage | -0.5 | 3.6 | V |
| VDD18 | 1.8V Digital Supply Voltage | -0.5 | 1.93 | V |
| AVDD18 | 1.8V Analog Supply Voltage | -0.5 | 1.93 | V |
| VIN_IO33 | Input Signal Voltage (Apply to 3.3V I/O pins) | -0.5 | 5 | V |
| VO_IO33 | Output Signal Voltage (Apply to 3.3V I/O pins) | -0.5 | VDD33 | V |

## *Power Consumption*

| Conditions | Power consumption (mA) |
|---|---|
| Idle with USB downstream linked (data transfer inactive) | 86 |
| Idle without USB downstream linked (no USB drive found connected) | 58 |
| Sleep | 52 |
| Data transfer active | 109 |

## *DC Characteristics*

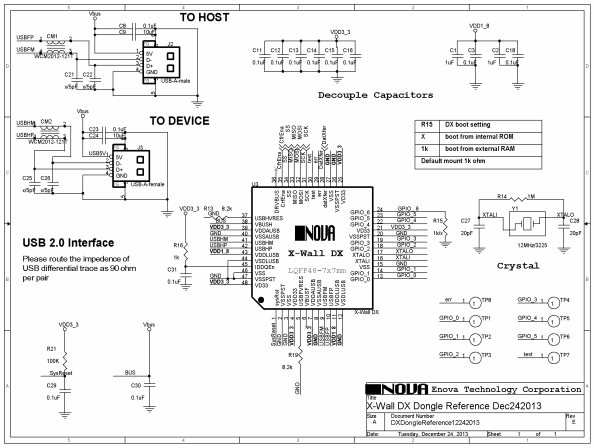
**Operating Conditions: VDD33=AVDD33=3.3V (±9.09%),**
**VDD18=AVDD18=1.8V (±7.22%), GND=0V**

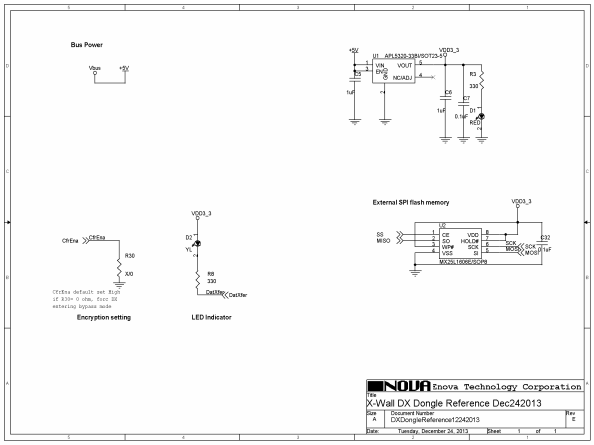
| Symbol | Parameter | Value | | Unit |
|---|---|---|---|---|
| | | Min | Max | |
| VDD33 | 3.3V Digital Supply Voltage | 3.0 | 3.6 | V |
| AVDD33 | 3.3V Analog Supply Voltage | 3.0 | 3.6 | V |
| VDD18 | 1.8V Digital Supply Voltage | 1.67 | 1.93 | V |
| AVDD18 | 1.8V Analog Supply Voltage | 1.67 | 1.93 | V |

# Reference Schematics

## *Typical Application Schematics (Pass-Thru Dongle version)*

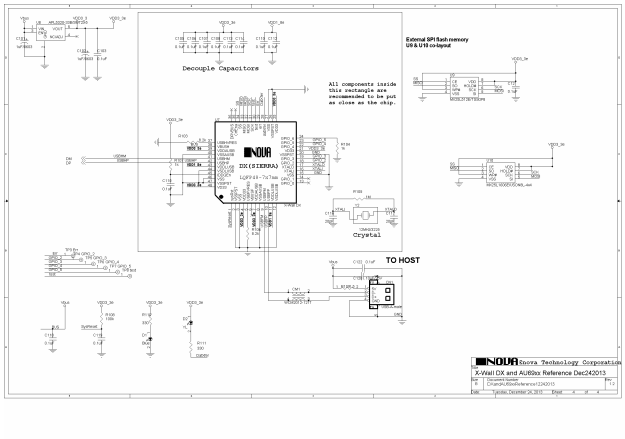
We will offer various schematics targeted for your specific requirement. A typical independent adapter design as shown below, the *X-Wall D*X is connected to two USB connectors (one male and one female connector), an SPI flash, LED indicators and some control circuits. This type of implementation can be applicable to perform FDE (Full Disk Encryption) to the connected USB MSC Storage Devices or perform FFE (File/Folder Encryption) to all host detectable storage devices including all cloud storages. For detailed circuit layout files and Bill of Materials, please contact your sales representatives. For special implementation such as customized SDK and software source codes, send your inquiries to info@enovatech.com.

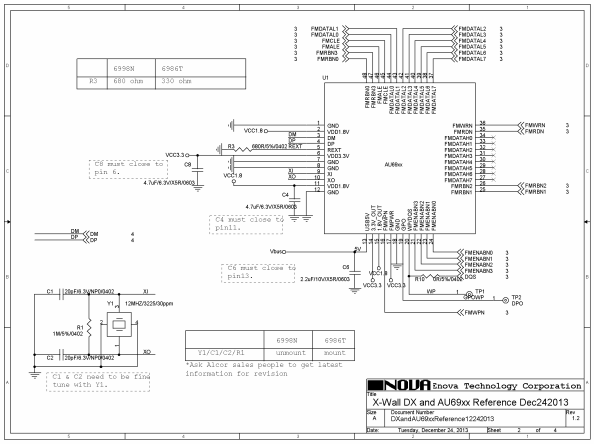


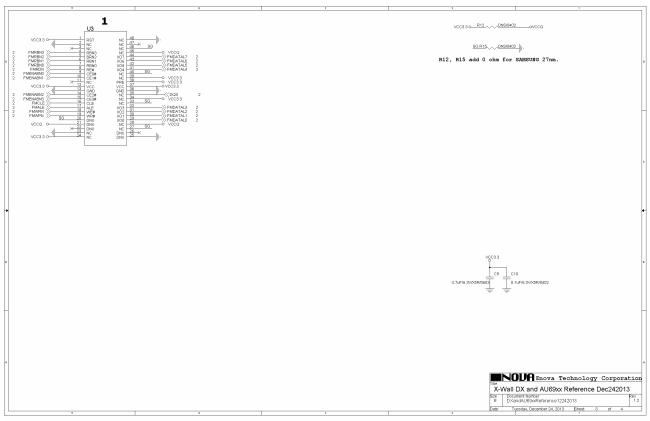




## *Alternative Application Schematics (Integrated USB/Flash module)*

Additional application such as integrated USB/Flash module is shown below. This application can provide stable performance and reliability for FFE (File/Folder Encryption) to all host detectable storage devices including cloud storages. For detailed circuit layout files and Bill of Materials, please contact your sales representatives. For special implementation such as customized SDK and software source codes, send your inquiries to info@enovatech.com.





### *Qualified Flash controller & NAND flash supported by the X-Wall DX USB OTG*

| Flash controller | NAND flash |
|---|---|
| AU6986T | Samsung K9F1G08U0D 128MB SLC |
| | Samsung K9WAG08U1D 2GB SLC |
| AU6998N | Samsung K9GBG08U0B 4GB MLC |
| | Sandisk SDTNQGAMA 8GB* MLC |

* More devices may be added in the future after going thorough qualification process.
* Sandisk SDTNQGAMA 8GB is conditionally approved (Criteria = Burn In 48 Hours).

## PCB Layout Guidelines

### *PCB Trace Routing*

The routing of *X-Wall DX USB OTG* signals requires careful attention. The following bullets are general guidelines for signal routing. Note, however, this guideline does not cover the entire horizon of a complete design other than dealing with *X-Wall DX USB OTG* specifically.

#### *USB Signal Layout*

.

- The impedance of the USB differential pair should be 90 ohms. Please refer to the "***PCB parameter of differential signals***" paragraph below to achieve aforementioned impedance value. You may want to consult with your PCB layout engineer to obtain the exact parameters.
- The trace length of the USB differential pairs should stay the same. The difference of 2 line traces should be restricted to below 20mils.
- Do not route USB traces underneath or near components that employ high clocking.
- The ground plane under the USB differential pair must be continuous. The VSSAUSB is the best

ground plane to be placed under USB signals.

***Power Trace Layout***

**The *X-Wall DX USB OTG* is engineered to take USB bus power to operate the connected USB MSC storage devices including hard disk therefore it's critical that the USB cable design meets at least AWG 20 (preferred to operate on USB MSC disk drive) or AWG 22 (marginal to operate on USB MSC Flash device).**

- If bus power traces which connect VBUS pin of USB connector to regulators or other essential connections are required for your PCB architecture, use traces which have width greater than 40mil.
- Follow the same rule to route all other main power traces on your PCB (For example, to the magnetic disk drive).
- The quality of USB cable influences the power supply, too. The Y-cable is suggested as a better alternative.

**PCB Parameters of Differential Signals**

(Assume 1oz cooper density)

| Type | Material (dielectric Constant) | PCB thickness | Dielectric thickness | Trace width | Trace spacing |
|---|---|---|---|---|---|
| 2-layer[5] | FR4 (4.2) | 1.6 mm | 57 mil | USB : 12mil | USB : 5mil |
| 4-layer | FR4 (4.2) | 1.6 mm | 4.3 mil | USB : 6mil | USB : 8mil |

[5] The layout engineer MUST follow this note precisely for a 2-layer PCB architecture which is not a standard micro strip transmission line structure. There is a definite requirement to the spacing between the differential trace and the nearby cooper plane of the same layer. For PCB parameters specified above, the defined spacing is 9mil for USB.

# *X-Wall DX USB OTG* Interface for Key Loading

There are two methods to deliver *Secret Key* to *X-Wall DX USB OTG*. The first method is for the *X-Wall DX USB OTG crypto module* to read up to 32 data bytes AES secret key value through a 2-wire serial bus if a slave device exists after normal power on sequence. The data read through the 2-wire serial interface are configured as *AES Secret Key*.

The second method is deliver the *AES Secret Key* via built-in API commands of the *X-Wall DX USB OTG* crypto module. The delivery of the *AES Secret Key* under *API* is encrypted therefore no on-line snooping is possible. The API command sets are further explained in the "***X-Wall DX USB OTG API Programming Guide.***"

The 2-wire serial interface is known as I²C compliance and is boot-trapped as a bus master by default. The *X-Wall DX*'s built-in micro controller will automatically generate bus master protocol seeking external slave EEPROM devices (7-bit device address 1010000b). If an external slave serial EEPROM device at bus address 1010000b is not found, *X-Wall DX* will not issue the next read protocol. And if the 2-wire bus master is so chosen, the only thing designers need to do is to provide external device (For example, an EEPROM) with the correct *AES Secret Key* content. The format listed below shows the content of an external 2K bits device (For example, the 24C02 EEPROM).

| | |
|---|---|
| **0x00h~ 0x1Fh** | 32 bytes of *AES Secret Key* with starting address = 0x00h |
| **0x20h~ 0xFFh** | Not application except the data byte at address 0x87h which is defined as the value of the Cryptographic Operation Register. This 0x87h address should be filled in 0x00h in general. |

## *AES Key Ordering Convention*

Through out this document, the *AES Secret Key* ordering will follow the convention stated in *FIPS-197*. That is, the least significant bit of a key sequence is the first input bit; the least significant byte is the first input byte, and so on. When denoting the key in symbols, the least significant bit is put to the left of the sequence. Therefore a 128-bit (16 bytes) AES Secret Key sequence can be denoted as

$Key_{128} = \{ b_0, b_1, b_3, \ldots, b_{127} \}$,

Or if it can be grouped in byte array or double word array as

$Key_{128} = \{ a_0, a_1, a_2, \ldots, a_{15} \}$,

and

$Key_{128}$ = { $w_0$, $w_1$, $w_2$, $w_3$ },

Where $a_n$ = { $b_{8n}$, $b_{8n+1}$,…, $b_{8n+7}$} and $w_n$ = { $a_{4n}$, $a_{4n+1}$, $a_{4n+2}$, $a_{4n+3}$}. For example, if

$Key_{128}$ = { *2b, 7e, 15, 16*, *28, ae, d2, a6,ab, f7, 15, 88, 09, cf, 4f, 3c* }, then

$w_0$ = { *2b, 7e, 15, 16* }

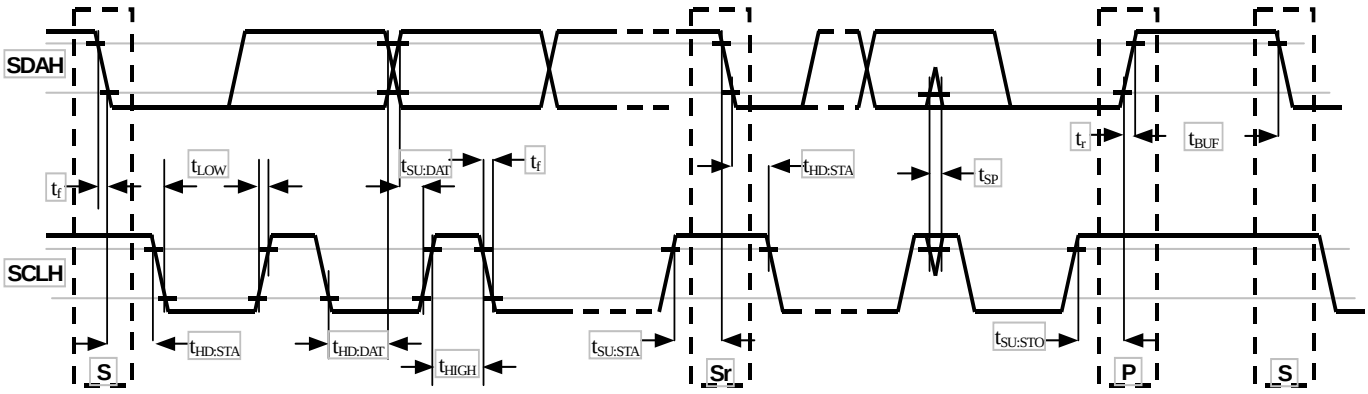
$w_1$ = { *28, ae, d2, a6* }

$w_2$ = { *ab, f7, 15, 88* }

$w_3$ = { *09, cf, 4f, 3c* }

## *X-Wall DX USB OTG 2-wire Serial Interface Basic*

The bus interface has two bus wires. The first one, namely SDAH, is used for transmitting and receiving serial bit data. The second one, namely SCLH, is used for transmitting (master mode) and receiving (slave mode) clock pulses. By combining those two signals the START, repeated START, and STOP conditions are created, which are then used for constructing entire bus protocol. Listed below is the signal-timing specification of SDAH and SCLH.




| PARAMETER | SYMBOL | MIN. | MAX. | UNIT |
|---|---|---|---|---|
| SCL clock frequency | $f_{SCL}$ | 0 | 400 | kHz |
| Hold time (repeated) START condition (**S**). After this period the first clock pulse is generated. | $t_{HD:STA}$ | 0.6 | - | µs |
| LOW period of the SCL clock | $t_{LOW}$ | 1.3 | - | µs |
| HIGH period of the SCL clock | $t_{HIGH}$ | 0.6 | - | µs |
| Set-up time for a repeated START condition (**Sr**) | $t_{SU:STA}$ | 0.6 | - | µs |
| Data hold time | $t_{HD:DAT}$ | 0 | 0.9 | µs |
| Data set-up time | $t_{SU:DAT}$ | 100 | - | ns |
| Rise time for both SDA and SCL signals | $t_r$ | 20+0.1$C_b$ | 300 | ns |
| Fall time for both SDA and SCL signals | $t_f$ | 20+0.1$C_b$ | 300 | ns |

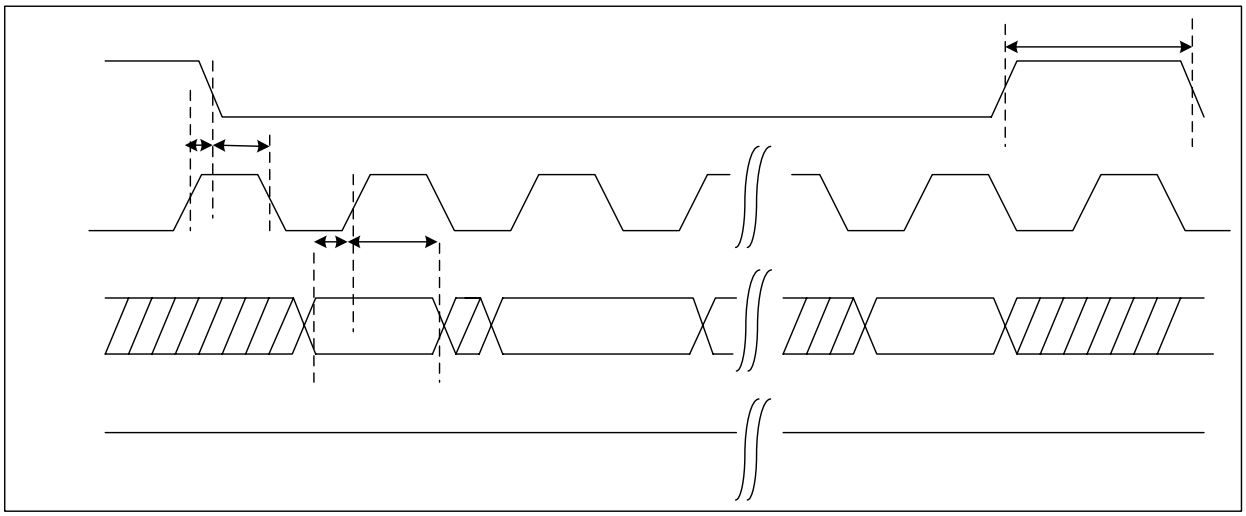
| | | | | |
|---|---|---|---|---|
| Setup time for STOP condition (**P**). | $t_{SU:STO}$ | 0.6 | - | μs |
| Bus free time between a STOP and a START condition. | $t_{BUF}$ | 1.3 | - | μs |
| Pulse width of spikes, which must be suppressed by the input filter. | $t_{SP}$ | 0 | 50 | ns |
| $C_b$: total capacitance of one bus line if pf. | | | | |

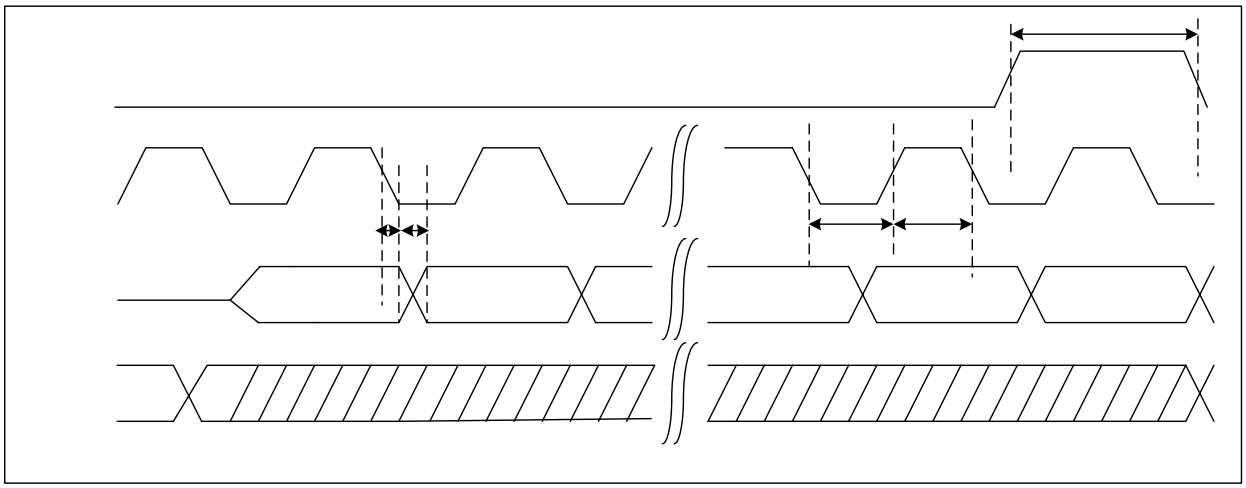
# *X-Wall DX USB OTG* Interface for firmware Update

*The X-Wall DX USB OTG* crypto module has a built-in single clock 8-bit micro-controller with 16K bytes hard-coded program ROM which contains firmware code that manages generic USB commands, Vendor Specific commands and security policy (SP). The *X-Wall DX USB OTG* crypto module can function correctly without any additional firmware update. *X-Wall DX USB OTG* also equips with a 12K bytes program RAM that dynamically loads customize firmware code from an external flash or EEROM into the program RAM through a 4-wire Serial Peripheral Interface (SPI). *The downloadable firmware code further extends the capability of the X-Wall DX USB OTG crypto module as more vender-specific tasks/functions may be added.* Additionally, the ROM code can be either replaced or reduced to meet specific design task. The boot-trapped value of pin24 (GPIO_6) is used to enable/disable this feature. For firmware update utilities and related information, please send your inquiries to Enova Technology at info@enovatech.com.

## *X-Wall DX USB OTG 4-wire SPI Interface Basic*

The bus interface has four bus wires which are clock output (*SCK*), serial master data output/slave data input (*MOSI*), serial master data input/slave data output (*MISO*) and slave select (*SS*). The *X-Wall DX USB OTG* crypto module supports the *Serial Peripheral Interface* master compatible Mode 0 with default maximum speed of 15MHz. The *X-Wall DX USB OTG* crypto module further supports basic READ/ERASE/PROGRAM SPI commands. Listed below is signal-timing specification of the *X-Wall DX USB OTG* SPI interface:





# X-Wall DX SPI master in

| PARAMETER | SYMBOL | MIN. | MAX. | UNIT |
|---|---|---|---|---|
| SCK clock frequency (configurable) | $f_{SCK}$ | 0.47 | 15 | MHz |
| SS deselect time | $t_{DSss}$ | 0.6 | - | ns |
| LOW period of the SCK clock | $t_{Hck}$ | 30 | - | ns |
| HIGH period of the SCK clock | $t_{Lck}$ | 30 | - | ns |
| Master data output setup time | $t_{SUmdo}$ | 4 | - | ns |
| Master data output Hold time | $t_{Hmdo}$ | 0 | 6 | ns |
| Clock low to slave data output valid | $t_{Vsdo}$ | | 30 | ns |
| Slave data output hold time | $t_{Hsdo}$ | 0 | | ns |
| Rise time for both SDA and SCL signals | $t_r$ | 20 | | ns |
| Fall time for both SDA and SCL signals | $t_f$ | 20 | | ns |

SS#

### *SPI command codes supported by the X-Wall DX USB OTG*

| Command name | Command code |
|---|---|
| RDSR | 05h |
| WREN | 06h |
| WRDI | 04h |
| READ | 03h |
| PROGRAM | 02h |
| ChipErase | C7h |

SCK

### *SPI flash supported by the X-Wall DX USB OTG*

| Vendor | P/N |
|---|---|
| MXIC | MX25L1606E |
| ESMT | F25L16PA |

MISO

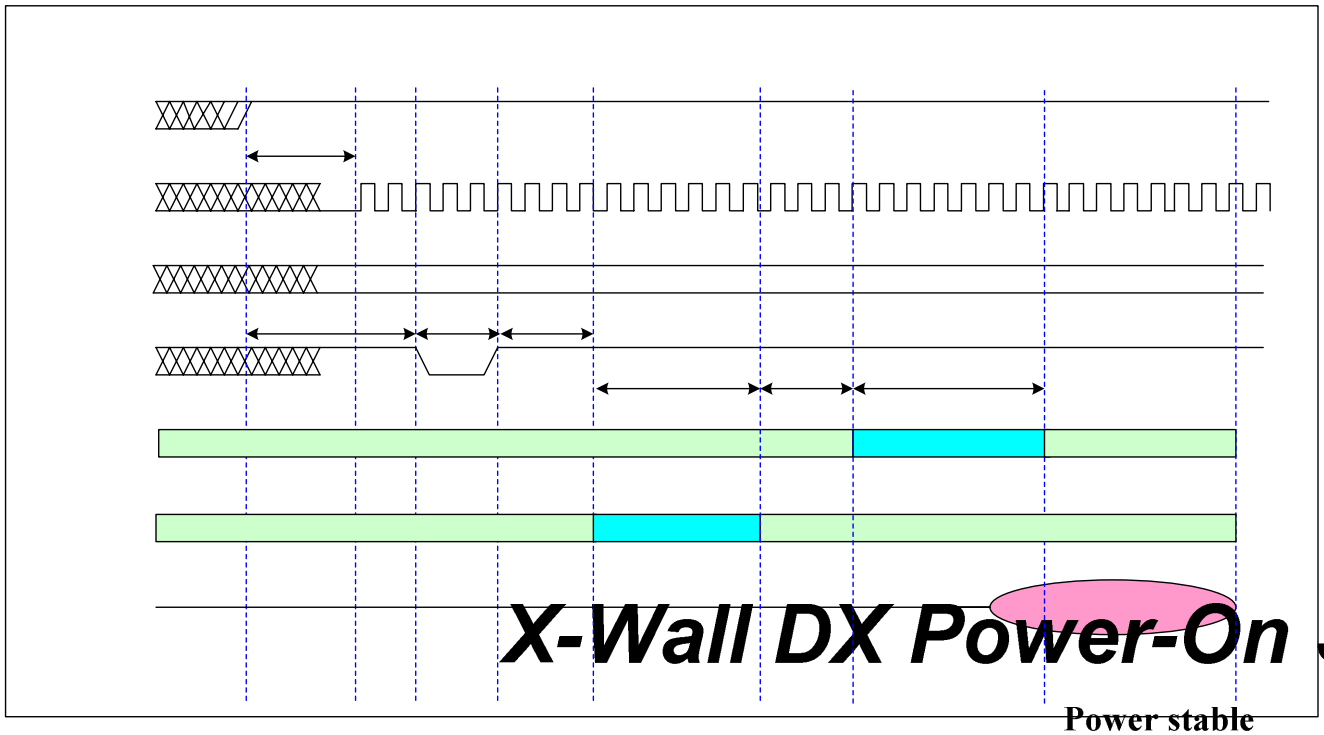
* More devices may be added in the future after thorough qualification process.

MOSI

Addr Out

## Power-On Sequence

After power on (the SysRst pin is negated LOW and released HIGH), the USB PHY module requires about 6μs for internal PLLs to become fully functional. At power on, the *X-Wall DX USB OTG* performs Power-On-Self-Test (POST) and searches an available external SPI flash device on the 4-wire SPI interface. If the SPI flash device exists and the load RAM code pin (Pin#24 GPIO_6) is enabled, *X-Wall DX USB OTG* starts loading the additional firmware code from the SPI interface. After which, the *X-Wall DX USB OTG* searches if an external *AES Secret Key* is available on the 2-wire Serial Interface (Pin#13 & 14 for GPIO_0 and GPIO_1 respectively). If the *AES Secret Key* exists, *X-Wall DX USB OTG* loads the *AES Secret Key* via the 2-wire serial interface and ends the power on sequence. After *X-Wall DX USB OTG* completes its normal power on sequence, it will wait for USB reset protocol then starts the required enumerations. Note that, if the *AES Secret Key* has been loaded and expanded, the *X-Wall DX OTG* is ready for cryptographic operations. If there is no *AES Secret Key* found, the *X-Wall DX USB OTG* crypto module stays in bypass mode which passes through every command and data it has received unmodified. Attempt to load the *Secret Key* via an external controller or a USB host adaptor using the *X-Wall DX USB OTG* built-in API command is feasible. However, be advised that the designers must ensure the *AES Secret Key* load sequence completes before any USB data transfer would occur for data corruption might happen if any USB data transfer occurs before the actual key load sequence is completed. Please reference below the typical *X-Wall DX USB OTG* Power-On Sequence.




| Name | Description | Value | Comment |
|---|---|---|---|
| tclkrdy | Power stable to internal clock stable | <0.5ms | Maxinum time for PLL to output stable clock |
| t0 | Power stable to SysRst valid (high) | >1ms | To ensure that SysRst is valid only after internal clock ready |
| t1 | Sysreset active low pulse | >1ms | Minimum reset time |
| t2 | Self test time | ~26ms | |
| t3 | SPI bus activity | ~17ms | *X-Wall DX* downloads the firmware code from the external flash device |
| t4 | Internal firmware runtime | ~17ms | |
| t5 | I2C bus activity | ~1.3ms | For Secret Key delivery |

## *X-Wall DX USB OTG* Configuration Management

### Hardware Packaging

QFP (Quad Flat Package) provides low profile 0.8mm body thickness, suitable for space concerned applications. Package size 7mm x 7mm (for QFP) lead frame-count 48 are offered for portable, lightweight and low profile applications. Optionally, we can offer QFN for smaller profile. Contact Enova Technology (info@enovatech.com) for information. **All Enova *X-Wall DX* crypto modules comply with RoHS and Lead-free specification.**

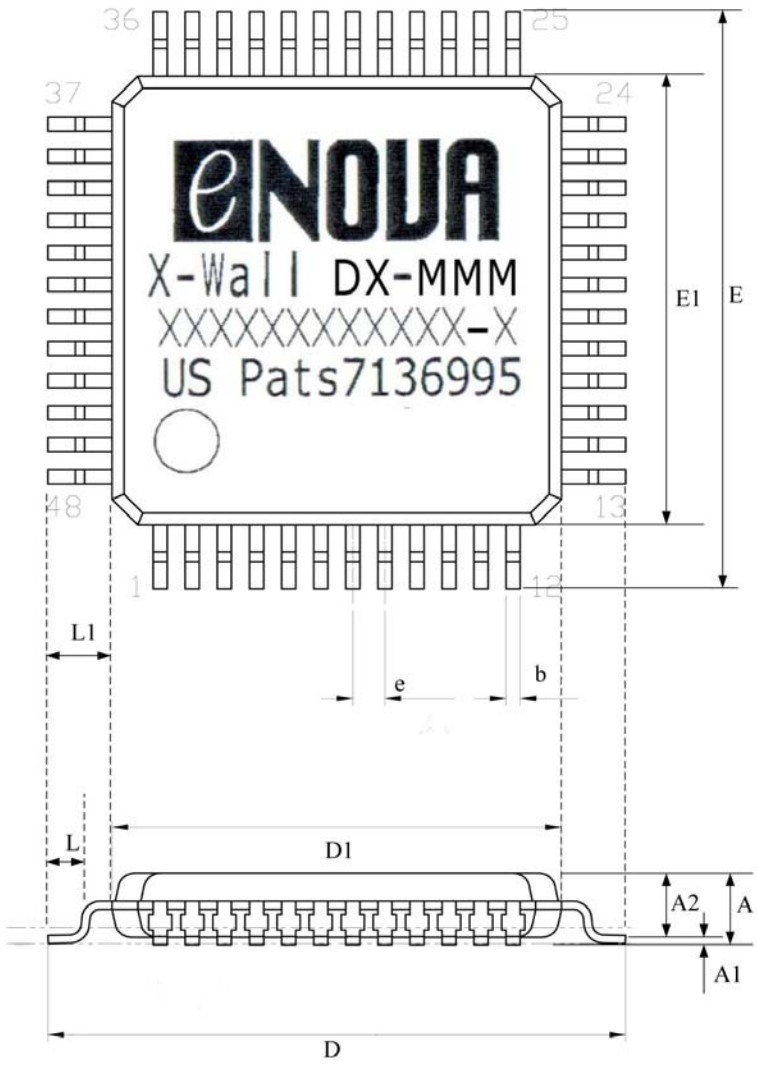
#### Features

1. 7mm x 7mm (for LQFP) body size with 48 lead frame-counts;
2. Copper lead-frame;
3. Low profile 0.8mm body thickness;
4. JEDEC MS-026/ACE standard outlines;

### Firmware Release

Hard coded version 2.0.1 released for ROM integration within the *X-Wall DX USB OTG* crypto module.

### Hardware Version Control, Outline, and Dimension (LQFP Package) - Default




| Symbol | Dimension [mm] | | |
|---|---|---|---|
| | MIN | NOR | MAX |
| A | | | 1.60 |
| A1 | 0.05 | 0.10 | 0.15 |
| A2 | 1.35 | 1.40 | 1.45 |
| b | 0.17 | 0.22 | 0.27 |
| D | 8.85 | 9.00 | 9.15 |
| D1 | 6.90 | 7.00 | 7.10 |
| E | 8.85 | 9.00 | 9.15 |
| E1 | 6.90 | 7.00 | 7.10 |
| e | 0.45 | 0.50 | 0.55 |
| L | 0.45 | 0.60 | 0.75 |
| L1 | 0.85 | 1.00 | 1.15 |

**X-Wall DX** top marking:

**Enova** – Trademark

**X-Wall DXAAAA**, trademark and product SKU where AAAA represents 3 to 4 digits as follows:

- 256C, AES CBC 256-bit
- 256, AES ECB 256-bit

**XXXXXXXXXXXX**

| 6 Lot No. | 4 date code | 2 version control|

6 digits for wafer lot number;

4 digits yyww (yy represents year and ww represents week) for manufacturing date code;

2 digits – version control for chip revision;

**US Patent No.**: granted US patents listing.