

X-Wall DX SPECIFICATION_APPROVAL SHEET
Rev. 1.2.2

Customer's Name: _____

Product SKU (Stock Keeping Unit):

X-Wall DX-128; X-Wall DX-128C; X-Wall DX-192C; X-Wall DX-256; X-Wall DX-256C

Product Description:

USB-to-USB real-time crypto processor with AES ECB or CBC strength up to 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

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

Table of Content	2
Introduction	3
<i>How does it work?</i>	5
<i>Applications</i>	6
<i>X-Wall DX features and benefits</i>	6
<i>Solution Provided</i>	7
<i>Ordering Codes</i>	7
X-Wall DX Pin Definitions	9
<i>Pin Assignment</i>	9
<i>Pin Definition and Description</i>	10
Electrical Characteristics	12
<i>Absolute Maximum Ratings</i>	12
<i>Power Consumption</i>	12
<i>DC Characteristics</i>	13
PCB Layout Guidelines	14
<i>Typical Application Schematics</i>	14
<i>Typical Bill of Materials (BOM)</i>	14
<i>PCB Trace Routing</i>	15
<i>PCB Parameters of Differential Signals</i>	16
X-Wall DX Interface for Key Loading	17
<i>AES Key Ordering Convention</i>	17
<i>X-Wall DX 2-wire Serial Interface Basic</i>	18
X-Wall DX Interface for firmware Update	20
<i>X-Wall DX SPI 4-wire Serial Interface Basic</i>	20
<i>SPI command codes supported by the X-Wall DX</i>	21
<i>SPI Flash by the X-Wall DX</i>	21
Power-On Sequence	22
<i>Hardware Packaging</i>	24
<i>Firmware Release</i>	24
<i>Hardware Version Control, Outline, and Dimension (LQFP Package) - Default</i>	24

Introduction

The patents protected¹ **X-Wall DX** 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 mode of operation up to 256-bit strength². 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 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.

The *X-Wall DX* solution provides two role-based authentications: Administrator and User. The Administrator role is capable of provisioning the storage device by deciding *Administrator PIN*, *User PIN*, *Failed Attempts*, *Write-Protect*, *Read-Only (CD-ROM) partition*, *Public Disk Partition*, *Cipher Disk Partition*, and *Secure Erase*. The User role can access the *Read-Only (CD-ROM) partition* and *Public Disk Partition* without presenting a User PIN. The *Cipher Disk Partition*, however, requires a correct *User PIN*. In particular, the *User PIN* authenticates the *Cipher Disk Partition* which would be invisible and inaccessible without the correct *User PIN* being presented. The *User PIN* can also be changed by either the Administrator role or the User role. More, the *Logout* feature, a means for brief recess which does not require the physical removal of the storage device when the User will be temporarily absent, is available to both Administrator and User roles. Those features are briefly described below:

Administrator PIN – the *Administrator PIN* provisions the storage device by deciding and changing the PIN for Administrator and User, the drive partitions of *Read-Only Partition*, *Public Disk Partition*, *Cipher Disk Partition*, *Failed Attempts*, and performing *Logout* and *Secure Erase*.

User PIN – the *User PIN* authenticates the *Cipher Disk Partition* for normal disk access. The *Cipher Disk Partition* is invisible and inaccessible without the *User PIN*. The User can change *User PIN* only after the successful login using the assigned User PIN by an Administrator; and the User can perform *Logout* for brief recess.

Cipher Disk Partition – It is the *X-Wall DX hardware* real-time encrypted logical partition with either AES ECB (Electronic Code Books) or CBC (Cipher Block Chaining) mode of operation up to 256-bit strength. The entire storage can be setup as the *Cipher Disk Partition* which is invisible and

¹ **US Patents: 7,136,995; 7,386,734; 7,900,057; Taiwan Patents: I330320; 179354; 190310; China Patents: 625110; Japan Patents: 306383; Korea Patents: 0445288; 0711190;**

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

inaccessible without a correct *User PIN* being presented. The *Cipher Disk Partition* is not visible and accessible using an *Administrator PIN* except that Administrator logs in using a *User PIN*. **The User PIN can still access the Cipher Disk Partition on the other host computer that equips with the same X-Wall DX crypto module without leaving any trace.**

Public Disk Partition – It is the *X-Wall DX* controlled logical partition that stores “public data” for sharing without presenting the *Administrator PIN* or the *User PIN*. As such, the *Public Disk Partition* presents itself as a normal disk drive for data access under the Operating System. The *Public Disk Partition* can be set to zero whereas the *Cipher Disk Partition* is set to maximum.

Read-Only Partition (CD-ROM) – It is the *X-Wall DX* controlled logical partition that stores all setup and login programs for portability. This Read-Only Partition (CD-ROM) is invisible when it leaves the *X-Wall DX* crypto module. Once the initialization has been done, the USB storage device can become portable to any other Windows (XP, Vista and 7) for operation without leaving any trace to that host computer.

Write Protect (Optional) – The *Write Protect* feature prevents any disk write to the *X-Wall DX* controlled storage device when it is enabled by an *Administrator PIN*. Once the *Write Protect* is enabled, the distributed USB storage devices can never be infected with any virus, worm and malware when they are leaving the corporate network security perimeter. This feature can be deployed as an add-on function to the existing Anti-Virus/Anti-Worm software for a complete secure mobile storage solution. This feature is also suitable for Forensic applications.

Failed Attempt – The *Administrator PIN* decides the numbers of *Failed Attempt* at provisioning stage. The number of the *Failed Attempt* can be from 1 to 15.

Secure Erase – The *Administrator PIN* decides when to erase the secret AES key and all Security Parameters settings at the provisioning stage. Upon execution of the *Secure Erase*, all data in the *Cipher Disk Partition* will become illegible as the actual secret AES key is zeroized. However, the *Secure Erase* does not erase the data in the *Public Disk Partition* which can still be normally accessed as long as the partition size of *Read-Only (CD-ROM)*, *Public Disk Partition* and *Cipher Disk Partition* are not adjusted.

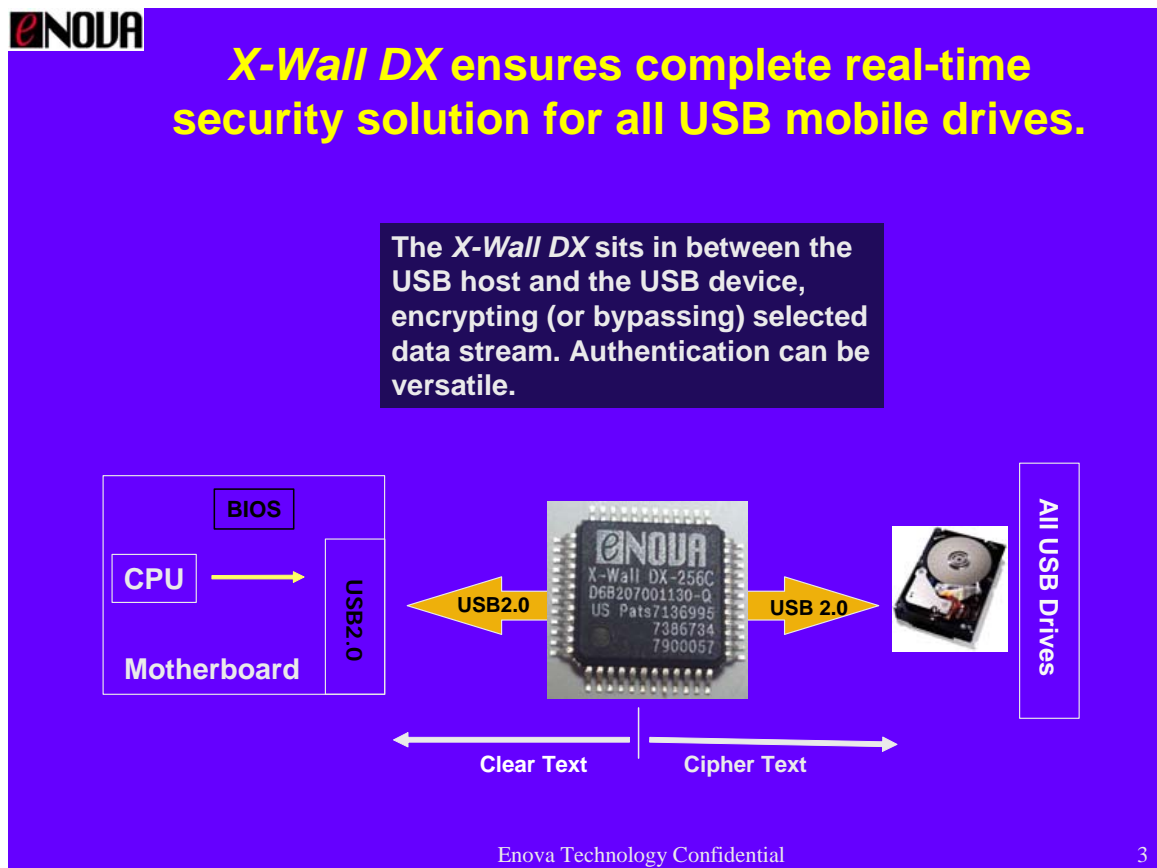
The *User PIN* can still access the *Cipher Disk Partition* on other host computers that equip with the same *X-Wall DX* crypto module without leaving any trace to those host computers. More, the “Write Protect” feature prevents virus, worms and malwares from being written into the storage device when the corporate network protection isn’t applicable. Additionally, the content of a CD or a DVD can be safeguarded as only the authorized role (be it a player station or a person) is able to “play back.” Duplication of the content is allowed but only in encrypted mode. Thus, the “Play Back” can only happen when the player station is authenticated. Consult Enova Technology (info@enovatech.com) for more details.

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) certifications³**.

The X-Wall DX equips complete USB2.0 MSC host and device protocol stacks thus can be embedded onto a motherboard USB host controller, a device USB controller, or as an independent adaptor as being elaborated in the following sections.

How does it work?



The X-Wall DX sits between a USB2.0 host and the USB2.0/1.1 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

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

produces no performance loss while all data-at-rest are hardware AES 256-bit encrypted. The Enova Secure Authentication (ESA) software responsible for authentication, is easy to use and requires no additional IT training. The X-Wall DX allows the creation of *Public Disk Partition* to which frequently shared data files are stored and *Cipher Disk Partition* to which all data contained within are real-time encrypted. The *Cipher Disk Partition* is not visible and inaccessible without a correct *User PIN*.

Applications

Integrated onto a host motherboard – The X-Wall DX is the ideal solution to be incorporated onto a standard USB2.0 and/or USB3.0 port of a host motherboard, making the USB port capable of encrypting every USB MSC storage device with U.S. Government certified hardware AES strength 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 MSC device – The X-Wall DX can be integrated onto the USB MSC storage drives include USB based disk drive, SSD and Flash. The USB MSC device that incorporates the X-Wall DX is capable of encrypting entire storage 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 onto their current USB based product lines, adding an unprecedented value to their current product offering.

Making an independent adapter – The X-Wall DX 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.

The Enova Secure Authentication Software (ESA) is also provided along with the hardware crypto-processor, the X-Wall DX as a total solution for fast time to market.

X-Wall DX features and benefits

Hardware Features	Key Benefits
<ul style="list-style-type: none"> ➤ Transparently encrypting all USB and UFD drives. 	Encrypting entire USB storage device including SSD, Disk Drive and Flash without performance degradation.
<ul style="list-style-type: none"> ➤ Compliance to USB 2.0/1.1 MSC bulk-only transport for cryptographic processing. ➤ Non-Mass Storage Class is passing through. 	Plug and play security solution for all UFD and USB mobile storage devices; Does not take up one specific USB port.

➤ 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 with 5 years warranty.	All in one cost saving solution securing all USB storage.
Authentication Features	Extras
➤ One time initialization and portable.	Leaves no trace over using on the other computer.
➤ One Administrator and one User account.	Administrator and User roles for different level of accessing control to the encrypted partition.
➤ Cipher Disk Partition is invisible and inaccessible without authentication.	Sensitive data can only be visible and accessed when the X-Wall DX is authenticated.
➤ Co-existing Cipher and Clear Text Partitions. ➤ Or 100% Cipher Text partition.	Administrator's discretion to determine partition split for classified (Cipher Disk)/unclassified (Public Disk) data.
➤ Optional Write-protect feature against unauthorized writes.	Optional Write-protect feature avoids Malware or Virus intrusion.
➤ Logout for brief recess.	For a short coffee break, there is no need to disconnect the drive as sensitive data is inaccessible after Logout.
➤ Windows XP & Windows 7 32/64-bit compliance.	Android and MAC OS to be supported in June, 2011.

Solution Provided

1. X-Wall DX-128, X-Wall DX-128C, X-Wall DX-192C, X-Wall DX-256 or X-Wall DX-256C crypto module;
2. Enova Secure Authentication software.

Ordering Codes

Stock Keeping Unit	Description	AES Mode of Operation⁴ (crypto mode)
X-Wall DX-128	USB Crypto Module with AES 128-bit strength	ECB
X-Wall DX-128C	USB Crypto Module with AES 128-bit strength	CBC
X-Wall DX-192C	USB Crypto Module with AES 192-bit strength	CBC
X-Wall DX-256	USB Crypto Module with AES 256-bit strength	ECB
X-Wall DX-256C	USB Crypto Module with AES 256-bit strength	CBC

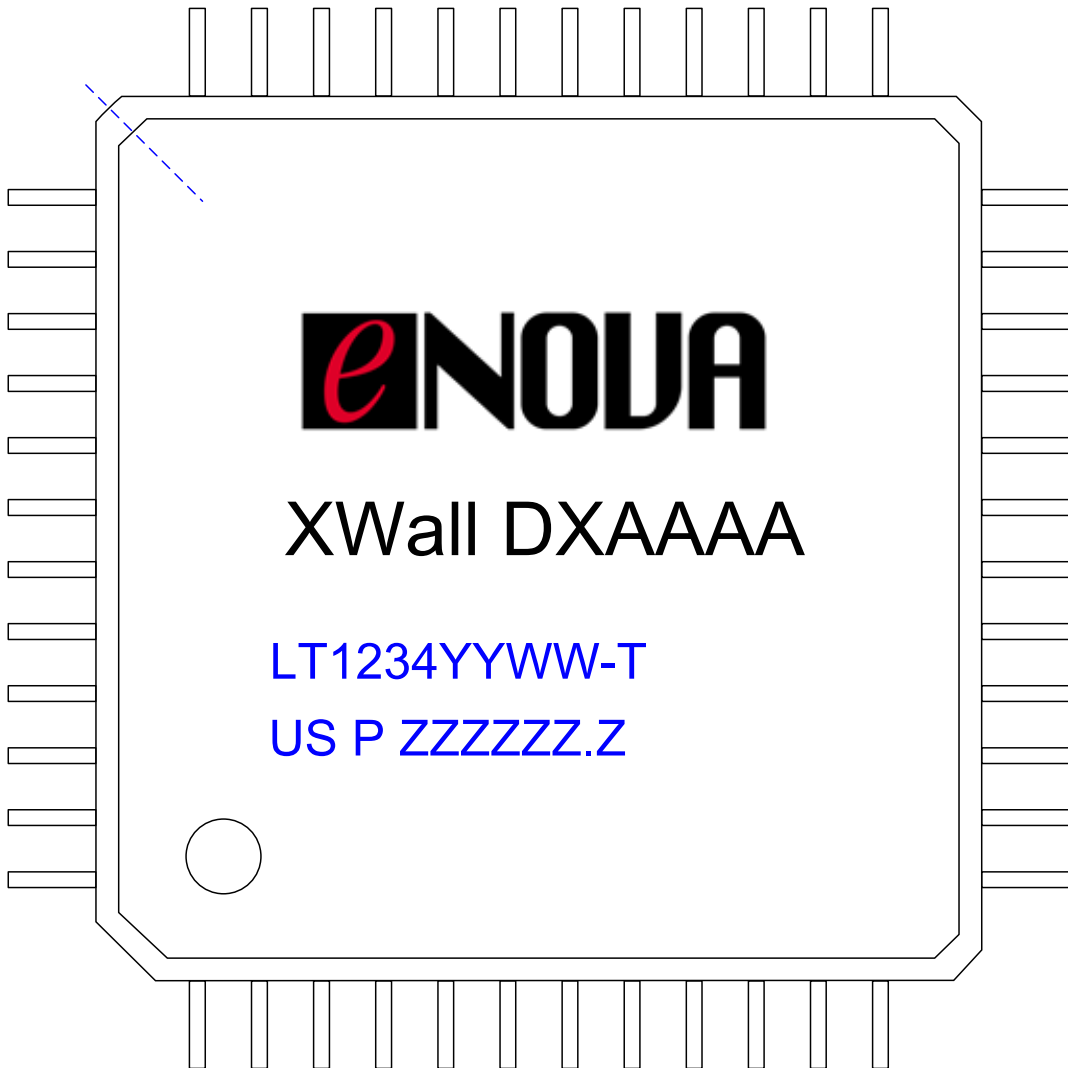
⁴ CBC stands for Cipher Block Chaining mode of operation where as ECB stands for Electronics Code Book mode of operation. The CBC mode is preferred for Government, Enterprise, and Military applications that demand highest attainable security level.



X-Wall DX Pin Definitions

Pin Assignment

All X-Wall DX 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 resistor 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-	
USBDRVRES	5	I/O	A	Connected to an external 8.2K Ohm resistor 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		O		Crystal/reference clock output	
Total	2				
FEATURE SETTING PINS					
NAME	PIN	DIR	TYPE	DESCRIPTION	
Total	1				
CONTROL AND INDICATE SIGNALS					
NAME	PIN	DIR	TYPE	DESCRIPTION	
SysRst	1	I	DU	Hardware master reset.	
				Programmable general purpose I/O pin.	
				Programmable general purpose I/O pin.	
GPIO_2	18	I/O	DU 8mA	Programmable general purpose I/O pins.	
GPIO_3	19				
GPIO_4	22				
GPIO_5	23				
GPIO_6	24	I/O	DU 8mA	Hardware trapped to enable/disable external firmware download. 1(default): Disable. 0: Enable.	
Total	10			Programmable general purpose I/O pin.	
SPI FLASH ROM INTERFACE					
NAME	PIN	DIR	TYPE	DESCRIPTION	
SCK	31	I	DD	SPI serial clock..	

MOSI	32	O	D 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
Total	2			
POWER GROUND				
NAME	PIN	DIR	TYPE	DESCRIPTION
VDD33	4 21 25 48		Power	3.3V digital power for I/O cells.
VSSPST	2 20 26 47		GND	3.3V digital ground for I/O cells.
VSS	3 15 27 46		GND	1.8V digital ground for core cells.
VDDAUSB	7 39		POWER	3.3V analog power for USB macro.
VSSAUSB	8 40		GND	3.3V analog ground for USB macro.
VSDLUSB	12 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 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 crypto module.

Absolute Maximum Ratings

Symbol	Parameter	Value		Unit
		Min	Max	
Ts	Storage Temperature	-55	+125	°C
Ta	Operating Temperature (Normal)	10	40	°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

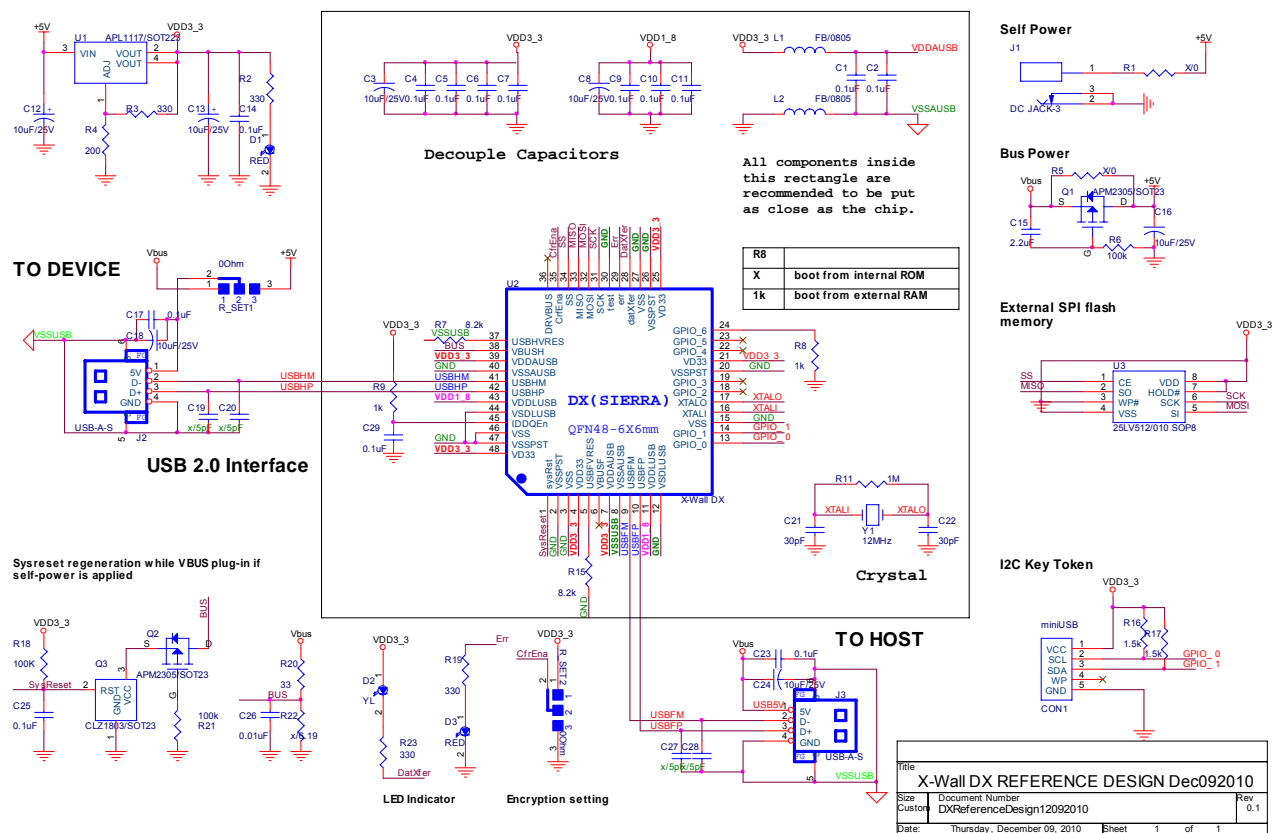
Operating Conditions: VDD33=AVDD33=3.3V ($\pm 9.09\%$),
VDD18=AVDD18=1.8V ($\pm 7.22\%$), GND=0V

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

PCB Layout Guidelines

Typical Application Schematics

A typical independent adapter design as shown below, the X-Wall DX is connected to two USB connectors, a Mini-USB key interface, a SPI flash, LED indicators and some control circuits. 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.



Typical Bill of Materials (BOM)

Item	Quantity	Reference	Part
1	1		Mini-USB
2	14		0.1uF
3	7		10uF/25V

4	1		2.2uF
5	4		5pF
6	2		30pF
7	1		0.01uF
8	2		RED LED
9	1		YELLOW LED
10	1		DC JACK-3
11	2		USB-A-S
12	2		FB/0805
13	2		APM2305/SOT23
14	1		CLZ1803/SOT23
15	2		0Ohm
16	2		X/0
17	4		330
18	1		200
19	3		100k
20	1		x/6.19k
21	2		1k
22	2		8.2k
23	1		1M
24	2		1.5k
25	1		3.3
26	1		X-Wall DX crypto module
27	1		APL1117/SOT223
28	1		25LV512/010 SOP8
29	1		12MHz

PCB Trace Routing

The routing of X-Wall DX 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 specifically.

USB Signal Layout

- ◆ The impedance of the USB differential pair should be 90 ohms. Please refer to the “PCB

parameter of differential signals⁵ 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 pair should be the same. The difference of 2 line traces should be restricted to below 150mils.
- ◆ 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 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 Interface for Key Loading

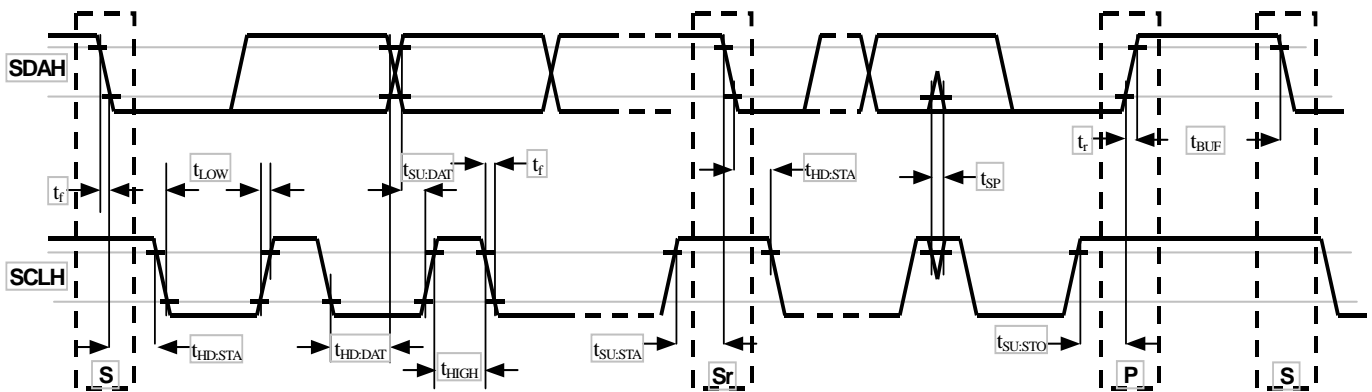
There are two methods to deliver *Secret Key* to *X-Wall DX*. The first method is for the *X-Wall DX crypto module* to read up to 32 data bytes AES secret key value through a 2-wire serial bus if a slave device exists after normal power on sequence. The data read through the 2-wire serial interface are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

The second method is for an application such as *Enova Secure Authentication (ESA)* software or an external micro controller to deliver the *AES Secret Key* via built-in API commands of the *X-Wall DX crypto module*. The delivery of the *AES Secret Key* under *ESA* is encrypted therefore no on-line snooping is possible. The API command sets are further explained in the “***X-Wall DX API Programming Guide.***”

AES Key Ordering Convention

X-Wall DX 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	$20+0.1C_b$	300	ns
Fall time for both SDA and SCL signals	t_f	$20+0.1C_b$	300	ns

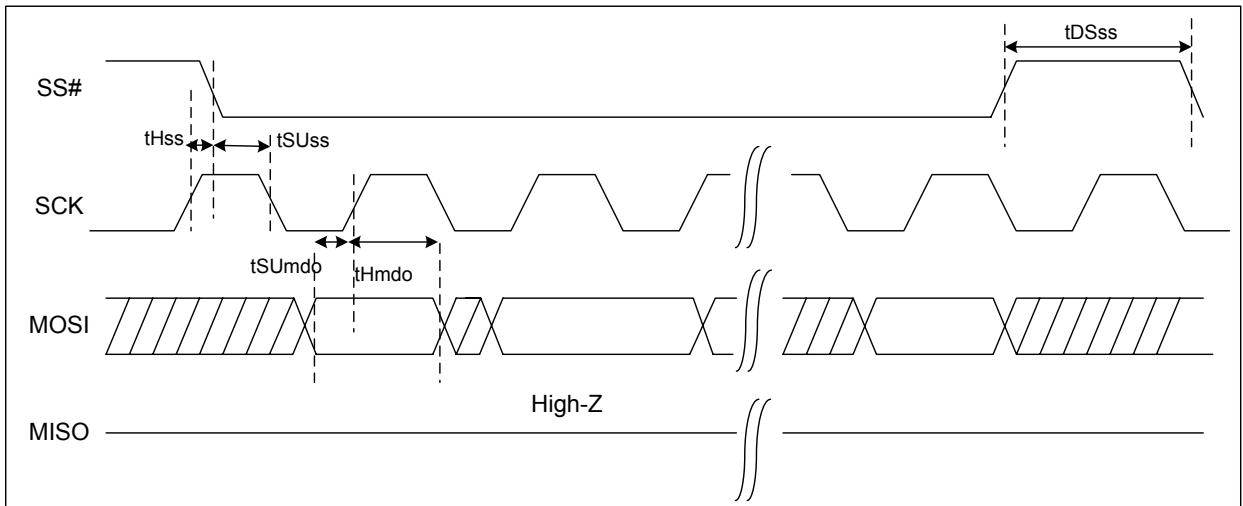
Setup time for STOP condition (P).	$t_{SU:STO}$	0.6	-	μs
Bus free time between a STOP and a START condition.	t_{BUF}	1.3	-	μs
Pulse width of spikes, which must be suppressed by the input filter.	t_{SP}	0	50	ns
C_b : total capacitance of one bus line if pf.				

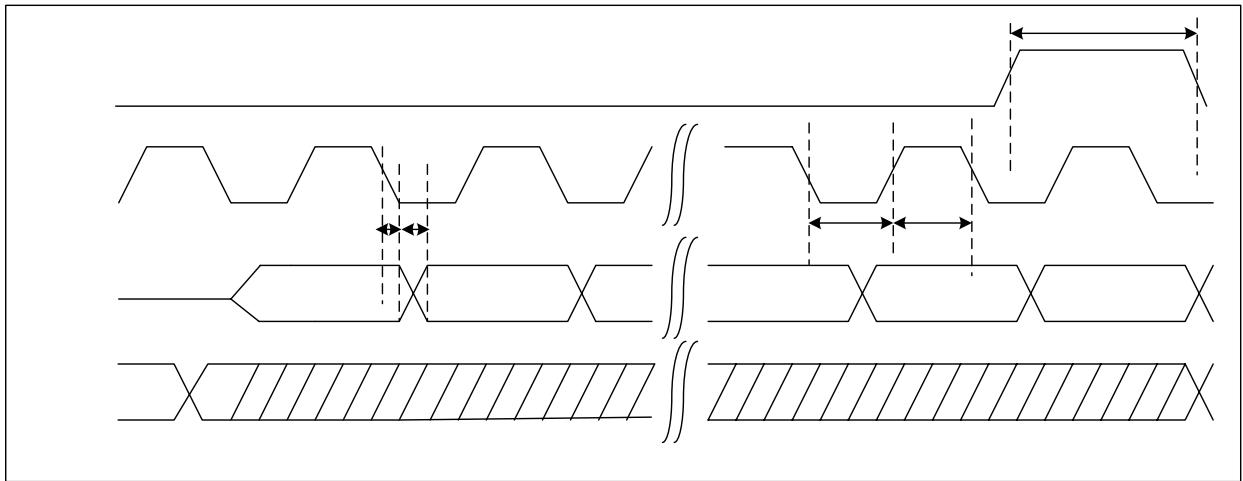
X-Wall DX Interface for firmware Update

X-Wall DX SPI 4-wire Serial 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 crypto module supports the *Serial Peripheral Interface* master compatible Mode 0 with default maximum speed of 15MHz. The X-Wall DX crypto module further supports basic READ/ERASE/PROGRAM SPI commands. Listed below is signal-timing specification of the X-Wall DX SPI interface:

X-Wall DX SPI master output timing





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

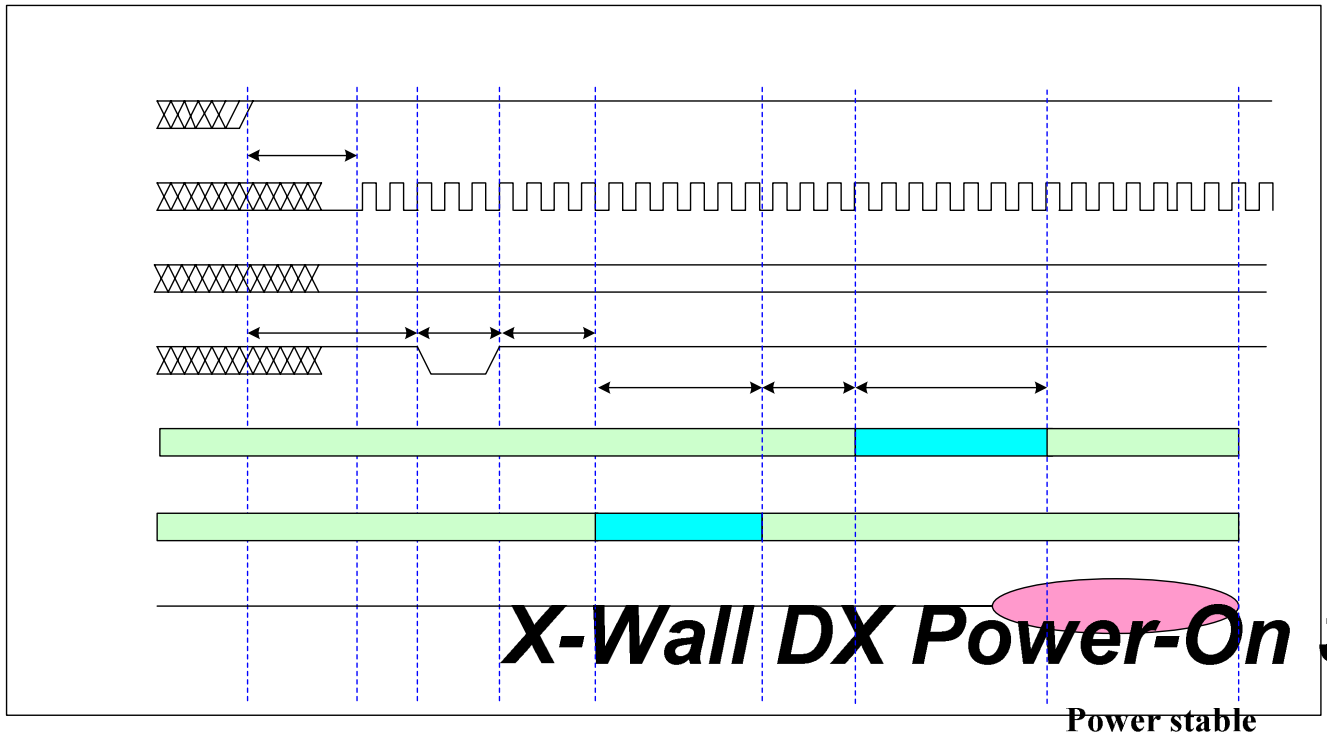
SPI command codes supported by the X-Wall DX

Command name	Command code
RDSR	09h
WREN	06h
WRDI	04h
READ	03h
PROGRAM	02h _i
ChipErase	C7h

SPI flash supported by the X-Wall DX

Those SPI Flash chips tested and supported by the X-Wall DX are MXIC MX25L2512C and Atmel AT25FS010. More devices can be added in the future after thorough testing.

Power-On Sequence



VDD18 & VDD33

tlckrdy

Name	Description	Value	Comment
tlckrdy	Power stable to internal clock stable CLK (1)	<0.5ms	Maximum 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 Config Signals (2)		
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 SysReset	~1.3ms	For Secret Key delivery

X-Wall DX 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. **All Enova X-Wall DX crypto modules comply with RoHS and Lead-free specification.**

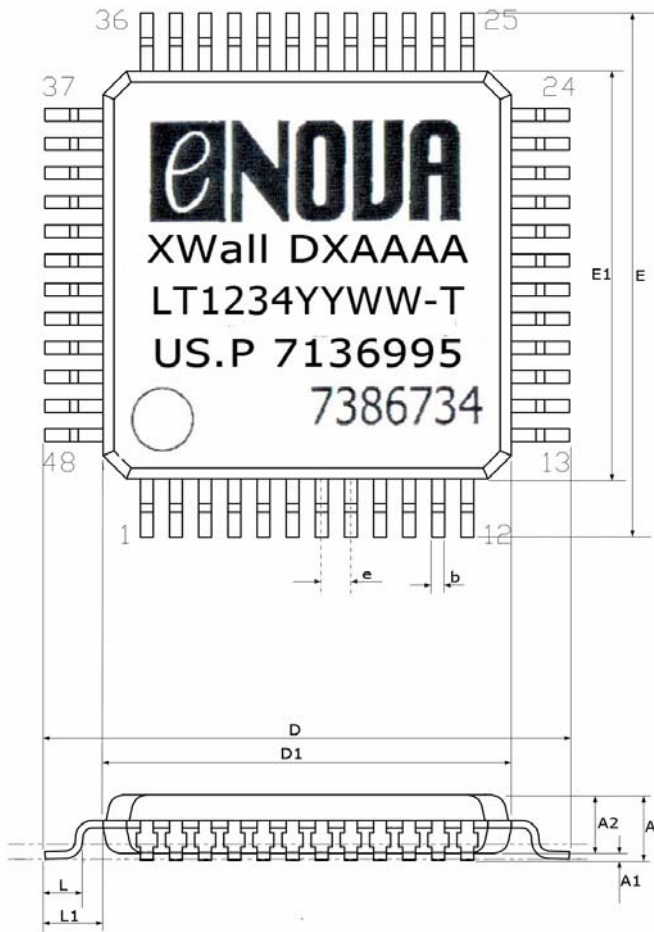
Features

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* 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:

- 128, AES ECB, 128-bit
- 128C, AES CBC 128-bit
- 192C, AES CBC 192-bit
- 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.