


Cheat Sheet Enova FIPS140-2 Level 2 & 3 Validated Single Chip Crypto Modules	
Inventor of the Full Disk Encryption (FDE) Technology in 2000.	<ul style="list-style-type: none"> ○ ENOVA invented the FDE technology and was awarded 16+ patents world-wide. ○ FDE automatically encrypts whole drive at the interface speed (aka on-the-fly encryption), starting at the Boot Sector (sector 0) and up to the maximum LBA¹. ○ The disk drive interface can be ATA/SATA, PCIe, USB, or others. ○ NIST validated AES XTS/CBC 256-bit² hardware real-time engine.
Why the Full Disk Encryption Technology?	<ul style="list-style-type: none"> ○ It protects data confidentiality and integrity³ of the attached disk drive from the boot sector up to the maximum LBA including operating system and applications. ○ <i>It protects the sensitive data of a misplaced, mishandled, captured, lost, or stolen disk drive of a vehicle from being dissected</i>, as the data remains encrypted via cryptographic erasing of the secret key and keying materials.
What is the SED (Self-Encrypting Drive) and TCG OPAL drive?	<ul style="list-style-type: none"> ○ The SED is a derivative of the FDE technology, where the on-the-fly encryption is done via drive's internal disk controller. ○ The TCG OPAL drive has built on top the FDE technology layer, an OPAL software protocol capable of performing role-based authentication. ○ The secret key for both SED and TCG OPAL disk drive is generated by the internal disk controller, which likely presents significant security vulnerabilities of how the secret key is generated, stored, disseminated, destroyed, and recovered.
 What's the FIPS Validation and How Significant It Is?	<ul style="list-style-type: none"> ○ FIPS 140-2⁴ evaluates and verifies the security implementation of a clearly defined boundary of a target crypto module through the rigid processes of CAVP⁵ and CMVP⁶ with increased level of functionality and assurance from level 1 to 4⁷. ○ The ENOVA X-Wall MX+ family chips are awarded FIPS level 2⁸ and level 3⁹ (for both FDE & TCG OPAL functions) validations with a performance fine-tuned AES 256-bit engine that encrypts data-at-rest and data-in-transit, including cloud backups.
Additional Benefits of Using ENOVA FIPS Validated Single Chips	<ul style="list-style-type: none"> ○ Low SWaP (Size 7x7mm, Weight, and Power), cost effective, and easy to deploy¹⁰. ○ Safeguards all standard SATA disk drive. ○ Serves as a hardware root of trust with a CMVP validated TRNG (True Random Number Generator) protected within a Level 3 physical security boundary. ○ Pre-boot authentication and ENOVA SafeBoot that <i>monitors and safeguards the boot process and the authenticity of software applications</i>.
Contacts	<ul style="list-style-type: none"> ○ www.enovatech.com Robert Wann rwann@enovatech.com M +1 510 789 8434

¹ **LBA** (Logical Block Addressing) is a sector addressing mode of a disk drive with either 512- or 4,096-bytes length.

² AES 256-bit encryption is quantum-resistant. Back in year 2000, the encryption algorithms were DES and TDES.

³ Confidentiality and Integrity are key roles in modern **CIA** (Confidentiality, Integrity, Availability) security objectives.

⁴ FIPS 140-2 (Federal Information Processing Standard) is migrating to FIPS 140-3 starting year 2024.

⁵ **CAVP** (Cryptographic Algorithms Validation Program) evaluates and validates all NIST published crypto algorithms, a prerequisite to the CMVP process that leads to a final FIPS certification. **Some algorithms would choose to stop here.**

⁶ **CMVP** (Cryptographic Modules Validation Program) evaluates and validates a target crypto module *with a defined cryptographic boundary*. A successful CMVP process leads to a final FIPS certification.

⁷ Software crypto module can only be validated at level 1; hardware module can be validated at level 2 and higher.

⁸ FIPS Level 2 focused on role-based authentication, security policy, system & communications protection, and configuration management. See <https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3675>.

⁹ FIPS Level 3 adds identity-based authentication and tamper resistant capabilities on top of those of a Level 2.

¹⁰ ENOVA chips operated a continuous burst of SATA Gen 3 AES encryption at approximately 0.6W power consumption.