# X-Wall® MX+

FIPS 140-2 Level 3 HSM

- 6Gbps AES CBC Off-load Engine
- Digital Signature Generation, Verifying and Signing

Armed with digital signature generation, verifying and signing capabilities the *X-Wall® MX+*, among other features, is an in-progress FIPS 140-2 Level 3 certified single chip SATA Gen 3 cryptographic bridge capable of ensuring trusted and encrypted communications for all computing tiers. A standard end point computing device such as a SATA disk drive or SSD can also benefit from the additional in-line 6Gbps AES CBC/XTS 256-bit hardware disk encryption capability it provides.

The X-Wall® MX+ HSM (Hardware Security Module)
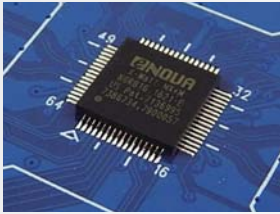
On top of the digital signature and in-line full disk encryption capabilities are FIPS certified Hash_DRBG, SHA256, HMAC (Hashed Message Authentication Code) and CMAC (Cryptographic Message Authentication Code) for either role based or identity based authentication. This means the entire authentication interfaces of the new *X-Wall® MX+* are protected (encrypted).

More, the *X-Wall® MX+* has built-in TCG Opal 2.0 capability to effectively transform any number of standard SATA disk drive or SSD to a TCG Opal 2.0 compliant drive. When working in conjunction with another built-in IEEE1667 firmware, the *X-Wall® MX+* can transform any number of standard SATA disk drive or SSD, regardless of its capacity, to eDrive, wherein Microsoft BitLocker can manage and configure, through the software interface of the IEEE1667 and Opal 2.0, as either a boot drive, a data drive or a portable drive using latest USB3.0/USB3.1 technology. The MBAM (Microsoft BitLocker Administration & Monitoring) takes advantage of the *X-Wall® MX+* transformed eDrive and provides enterprise-wise key management for fast deployment with low TCO (Total Cost of Ownership).

Important Applications

- **Microsoft Encrypted HDD (BitLocker managed eDrive):** The *X-Wall® MX+* automatically transforms any number of standard SATA drive (SSD included) into an eDrive to which Microsoft BitLocker manages and configures. Standard disk image cloning or data backup can be realized using the *X-Wall® MX+* transformed eDrive to significantly reduce corporate IT overhead for mass deployment.

- **Opal 2.0 Compliant Drive:** The *X-Wall® MX+* automatically transforms any number of standard SATA disk drive (and SSD) into an Opal 2.0 compliant drive.

- **FDE (Full Disk Encryption) or SED (Self Encrypting Device):** The *X-Wall® MX+* can be configured to perform in-line 6Gbps full disk encryption with AES CBC/XTS 256-bit strength protecting entire Data-at-Rest. This default solution is OS independent.

- **File Folder Encryption (FFE):** With add-on software components, the *X-Wall® MX+* can be configured to perform file/folder encryption, encrypting Data-in-Motion such that files stored in the Cloud storage remain MX+ hardware encrypted. Only the right secret key can successfully decrypt those encrypted files, solution that is OS dependent.

- **Trusted Communications/Relationship:** Armed with the built-in RSA 2048, HMAC, CMAC, AES ECB/XTS/CBC, SHA256, Hash_DRBG and TRNG, the *X-Wall® MX+* is able to generate signature, sign and verify each identity thus ensures layer of trusted communications among all computing tiers.

Performance

The *X-Wall® MX+* can be operated with SATA Gen 3, 2 and 1 compliant disk drive with a maximum cryptographic throughput at 6Gbps. There are no extra software driver to be loaded, eliminating entirely the memory and interrupt overheads thus freeing up the host CPU. The right chart is a typical benchmark result using latest SATA SSD which is configured as GPT-NTFS-4096bytes running under Windows 10 64-bit platform.