


Cheat Sheet

Enova *Mt. Vista* Quantum-Resistant Single Chip and Solution

Why Quantum-Resistant (QR)?	<ul style="list-style-type: none"> The continuous advancement of academic and industrial research of CRQC¹ has prompted the NSA (National Security Agency) to require all National Security Systems to immediately phase in Quantum Resistant CNSA² Suite 2.0. NSA has identified and prioritized the use case of “Software and Firmware Code Signing” for QR mitigation and specified NIST SP800-208 standard for HBS³ (hash-based signature) schemes like XMSS⁴ and LMS DSA (Digital Signature Algorithm). QR is default and preferred starting 2025 for specifically the Software/Firmware Code Signing which shall be completely mitigated by 2030.
What is XMSS/LMS Quantum-Resistant Digital Signature Algorithm (DSA)?	<ul style="list-style-type: none"> They’re “Stateful” HBS, meaning the signing Secret Key changes over time. The QR DSA performs signature only and does NOT encrypt data, unless with the help from additional protocols such as TLS or IPsec⁵. Enova recommends AES 256-bit⁶ encryption to make it whole – encrypt & sign. Unlike FIPS 203⁷ and 204⁸, the hash algorithms of the HBS are industrial proven and are known to resist CRQC, brute-force, and side channel attacks.
What is the NIST SP800-208 standard?	<ul style="list-style-type: none"> Introduces the XMSS/LMS HBS stateful digital signature algorithms. Requires a hardware crypto module that provides FIPS 140-2/140-3 Level 3 or higher physical security where the private SEEDs are secured. Requires to use the ENTROPY of an APPROVED embedded random bit generator.
 Enova’s <i>Mt. Vista</i> single chip provides QR, DAR, and DIT encryption technologies.	<ul style="list-style-type: none"> FIPS 140-2 Level 3 validated single chip that provides Level 3 physical security. Chips are trusted and deployed by top 10 US prime defense contractors. Provides HBS DSA that meets the NIST SP800-208 standard. Provides hardware AES 256-bit protection to data-at-rest (DAR) and data-in-transit (DIT), including data backups to cloud. Low SWaP (Size, Weight, and Power), cost effective, and easy to deploy⁹.
Easy to deploy – for both <i>Signing Authority</i> and <i>Relying Party</i> .	<ul style="list-style-type: none"> Signing Authority – can be the <i>Mt. Vista</i> chip or module or adaptor, running on a standard Windows/Linux laptop. Relying Party – can be the <i>Mt. Vista</i> chip or module or adaptor on a remote device.
Contacts	<ul style="list-style-type: none"> www.enovatech.com Robert Wann rwann@enovatech.com M +1 510 789 8434

¹ CRQC (Cryptographically Relevant Quantum Computer) means quantum computer tailored to Shor’s Algorithm that could break the conjectured mathematical difficulties of factoring and logarithms used by the widely deployed PKC (Public Key Cryptography) systems like RSA, ECC and ECCDH.

² CNSA (Commercial National Security Algorithms) Suite 2.0 is the latest NSA mandated quantum resistant algorithms.

³ HBS - Hash-based Digital Signature Algorithms (DSA).

⁴ XMSS (eXtended Merkle Signature Scheme) and LMS (Leighton-Micali Signature) are stateful hash-based signature.

⁵ TLS (Transport Layer Security) – a transport layer protocol that negotiates, based on ECCDH or RSA, a session key used to encrypt data between two communicating parties. The TLS requires QR mitigation for its deployed PKC systems; IPsec assumes VPN’s machine authentication header then applies internet key exchange to establish a secret key to encrypt all traffics between the two parties. Note that a VPN without IPsec capability does not encrypt data.

⁶ AES 256-bit encryption is quantum resistant. Enova’s *Mt. Vista* chip has built an optimized hardware AES engine.

⁷ FIPS 203 – Module Lattice-based Key Encapsulation Mechanism Standard (ML-KEM). Previously known as Kyber.

⁸ FIPS 204 – Module Lattice-based Digital Signature Algorithm (ML-DSA). Previously known as Dilithium.

⁹ The ENOVA *Mt. Vista* QR single chip is in production as this is written.