Enova *Mt. Vista* 抗量子單晶片與解決方案

主題	內容
為何需要抗量子(Quantum Resistant)？	• 與密碼學相關的量子電腦(CRQC[1])的學術和產業研究持續進展促使美國國家安全局(NSA)要求所有國家安全系統(National Security System)立即逐步導入抗量子 CNSA[2] Suite 2.0。 • NSA 優先將「軟體與韌體程式碼簽署」類別作為 QR 遷移的實用例，並指定 NIST SP800-208 標準為基於雜湊函數的數位簽章方案(HBS[3])如 XMSS[4]和 LMS DSA。 • 從 2025 起，QR 為軟體/韌體程式碼數位簽章的預設和首選，並於 2030 完成遷移。
什麼是 XMSS/LMS 抗量子數位簽章演算法(DSA)？	• 它們是「有狀態」的 HBS，意味著簽章私密金鑰(Private Key)隨著使用時間而改變。 • QR DSA 僅執行簽章功能，除非有額外協定如 TLS[5]或 IPSec 的協助，否則不會加密資料。Enova ***Mt. Vista*** 使用 QR DSA 及 AES 256-bit 引擎加密保護軟體與韌體程式碼並簽章。 • 與 FIPS 203[7]和 204[8]不同，HBS 雜湊函數演算法經過產業常期驗證，已知能抵抗 CRQC、暴力破解和旁路攻擊。
NIST SP800-208 標準是什麼？	• 引介 XMSS/LMS HBS 有狀態數位簽章演算法。 • 要求硬體密碼模組提供 FIPS 140-2/140-3 Level 3 或更高的實體安全性，以保護私密種子(SEEDs)與狀態(STATES)。 • 要求使用經核准的內建式真亂數產生器的「熵」。
Enova *Mt. Vista* 單晶片提供哪些加密技術？	• 通過 FIPS 140-2 Level 3 驗證的單晶片，提供 Level 3 的實體安全性。 • 晶片獲得美國前十大主要國防承包商的信任和部署。 • 提供符合 NIST SP800-208 標準的 HBS DSA。 • 為靜態資料(DAR)和傳輸中資料(DIT)提供硬體 AES 256 位元保護，包括雲端資料備份。 • 低尺寸、重量和功率 SWaP，成本效益高且易於部署[9]。
對於簽署授權方和依賴方來說，部署有多容易？	• 簽署授權方(Signing Authority)可以是 ***Mt. Vista*** 晶片、模組或轉接器，在標準的 Windows/Linux 個人電腦上運行。 • 依賴方(Relying Party)可以是遠端設備上的 ***Mt. Vista*** 晶片、模組或轉接器。
聯絡方式	• www.enovatech.com ｜ P: +886 3 577 2767 ｜電子郵件：contact@enovatech.net

定義：

1. **CRQC (Cryptographically Relevant Quantum Computer)**是為 Shor 演算法量身打造的量子電腦，這種電腦可能迅速破解廣泛部署的公開金鑰密碼學 PKC (Public Key Cryptography)系統（如 RSA、DSA、ECC 和 ECCDH）所使用的因數分解和對數運算等數學難題。
2. **CNSA (Commercial National Security Algorithms) Suite 2.0** 是美國國家安全局最新頒布的抗量子演算法。
3. **HBS (Hash-based Digital Signature Algorithm)**是基於雜湊函數的抗量子數位簽章演算法。
4. **XMSS (eXtended Merkle Signature Scheme)**和 **LMS (Leighton-Micali Signature)**是基於有狀態雜湊函數的抗量子數位簽章。
5. **TLS (Transport Layer Security)**是一種網路傳輸層協定，基於 ECCDH 或 RSA 金鑰交換協定協商一個工作階段金鑰(Session Key)用於加密兩個通訊方之間的資料。TLS 需要對其部署的 PKC 系統進行 QR 遷移；IPSec 採取 VPN 的機器驗證標頭(Machine Authentication Header)，然後應用網際網路金鑰交換協定(Internet Key Exchange)用來建立一個秘密金鑰加密兩個通訊方之間的所有流量。請注意，沒有 IPSec 功能的 VPN 不能加密資料。
6. **AES 256 位元加密**是抗量子演算法。Enova *Mt. Vista* 晶片內建了一個優化的硬體 AES 引擎。
7. **FIPS 203** 是模組格基金鑰封裝機制標準(ML-KEM)。舊稱為 Kyber。
8. **FIPS 204** 是模組格基數位簽章演算法(ML-DSA)。舊稱為 Dilithium。
9. **ENOVA *Mt. Vista* QR 單晶片**：在撰寫本文時已投入生產。