美國國家標準技術局（NIST）更新電子簽章標準

美國國家標準技術局（National Institute of Standards and Technology, NIST）於近日（2013年7月）更新電子簽章的技術標準「FIPS (Federal Information Processing Standard) 186-4數位簽章標準」，並經商務部部長核可。NIST於1994年首次提出電子簽章標準，旨在提供工具可資促進數位時代的信賴性，後續也隨著技術進步與革新，而有多次修訂。此次修訂，主要是調合該標準，使之與NIST其他加密相關指引（如金鑰加密標準）一致，以避免將來可能產生的矛盾。

此次增訂，亦明列出三種可保護資料的簽章產製與確認技術：數位簽章演算法（Digital Signature Algorithm, DSA）、橢圓曲線簽章演算法（Elliptic Curve Digital Signature Algorithm, ECDSA）、以及RSA公眾金鑰演算法（Rivest-Shamir-Adleman Algorithm, RSA）。

其他修訂的部分，還包括語彙的明晰化，以及降低對於隨機號碼產生器的利用限制…等。

本文為「經濟部產業技術司科技專案成果」

相關連結

- NIST Approves FIPS 186-4, Digital Signature Standard
- NIST Releases Updates to Digital Signature Standard

張乃文
主任 編譯整理

上稿時間： 2013年07月

資料來源： http://www.nist.gov/itl/csd/fips-072313.cfm (last visited July 23, 2013)
http://cryptome.org/2013/07/nist-fips-186-4.htm (last visited July 23, 2013)

推薦文章