NIST proposes update to digital signature standard

April 18 2012

The National Institute of Standards and Technology (NIST) has announced proposed changes to a standard that specifies how to implement digital signatures, which can be used to ensure the integrity of electronic documents, such as wills and contracts, as well as the identity of the signer.

These proposed changes to the Federal Information Processing Standard (FIPS) 186-3, known as the Digital Signature Standard, were posted for public comment on April 10, 2012. First published in 1994 and revised several times since then, the standard provides a means of guaranteeing authenticity in the digital world by means of operations based on complex math that are all but impossible to "forge". Updates to the standard are still necessary as technology changes.

The proposed revisions provide clarification on how to implement the digital signature algorithms approved in the standard: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adelman algorithm (RSA). Included in the proposed revision is allowing the use of additional, approved random number generators, which are used to generate the cryptographic keys used for the generation and verification of digital signatures.

More information: The comment period on the proposal is open until May 25, 2012. Both FIPS 186-3 and a separate four-page document outlining the proposed changes are available at

csrc.nist.gov/publications/PubsDrafts.html . Electronic comments may be sent to: fips_186-3_change_notice@nist.gov , with "186-3 Change Notice" in the subject line.

Provided by National Institute of Standards and Technology