NIST: SP 800-89: Recommendation for Obtaining Assurances for Digital Signature Applications

return to the NIST Standards

Table 1: Data sheet for Recommendation for Obtaining Assurances for Digital Signature Applications

Title	Recommendation for Obtaining Assurances for Digital Signature Applications
Acronym	
Version	
Series	SP
Document Number	800-89
Release Date	November 2006
Download	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf

Note: The following is an excerpt from the official NIST catalog. It is provided here as a connivence and is not authoritative. Refer to the original document as the authoritative reference.

Introduction

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). Each signatory has a public and private key and is the owner of that key pair. The private key is used by the owner to generate a digital signature; the public key is used in the signature verification process.

Entities participating in the generation or verification of digital signatures depend on the authenticity of the process. This Recommendation specifies methods for obtaining the assurances necessary for valid digital signatures: assurance of domain parameter validity, assurance of public key validity, assurance that the key pair owner actually possesses the private key, and assurance of the identity of the key pair owner.

Federal Information Processing Standard (FIPS) 186-3 allows three techniques for the generation of digital signatures: the Digital Signature Algorithm (DSA), RSA [1)], and the Elliptic Curve Digital Signature Algorithm (ECDSA). For DSA and ECDSA, assurance of the validity of the domain parameters must be obtained (see Section 4). RSA has no domain parameters. Domain parameters may be generated by anyone, and assurance of domain parameter validity `shall` be obtained prior to performing any other process associated with digital signatures, including the generation of

digital signature key pairs and the generation and verification of digital signatures.

Digital signature keys may be generated by the intended signatory, cooperatively generated by the intended signatory and a Trusted Third Party (TTP), or generated entirely by a TTP and provided to the intended signatory. For all digital signature algorithms, each party associated with the digital signature process `shall` have assurance of the validity of the public keys (see Section 5) and assurance that the key pair owner actually possesses the private key used for generating the digital signature (see Section 6). In addition, assurance of the claimed signatory's identity is required by all verifiers, including any TTPs involved in the process (see Section 7).

All methods that are used to provide assurance assume the security and reliability of any routines involved in the process. Obtaining assurances normally requires explicit actions by someone. However, once the appropriate assurances are obtained, the explicitly obtained assurance can be leveraged as assurance for subsequent messages. Note that it may be appropriate to renew this assurance periodically.

1)

An algorithm developed by Rivest, Shamir and Adelman.