Digital Signature

08/15/2024 03:45:09

FAQ Article Print

Category:	RRZE: Glossary	**Votes:**	0
State:	public (all)	**Result:**	0.00 %
Language:	en	**Last update:**	15:22:15 - 06/25/2010

Keywords

Identity, Security

Symptom (public)

Problem (public)

Solution (public)

An electronic signature that can be used to authenticate the identity of the sender of an electronic message or the signer of a digital document, and to ensure that the original content of the message or document that has been sent is unchanged. Not to be confused with a digital certificate.

A cryptographically calculated value is derived from the message and the private key associated with the digital certificate. The public key in the digital certificate can be used to verify that the calculated value corresponds with the message, proving that the digital signature was created by the person in possession of the private key associated with the digital certificate, and that the message has not been changed.

Digital signatures can be susceptible to a "birthday attack" so called because the probability of two or more people in a small sample having the same birthday appears to defy intuition (as do most coincidences). It is applicable to coincidences in languages and alphabetic cyphers. As an example, for a 64-bit hash there are approximately 1.9 x 1019 different results, but it would take 'only' approximately 5.1 x 109 attempts to generate a match. To create a "birthday attack", you first prepare a document where a number of things can be changed without changing the meaning, such as inserting commas, empty lines, replacing synonyms, etc., and then you create a large number of variations of the document and apply the hash function to all these variations until a version of the original and a version of the fraudulent document are found to have the same hash value. After the recipient has signed the original document, the issuer takes the signature and attaches it to the fraudulent document, thus "proving" that he signed the fraudulent document. To avoid this attack, the output length of the hash function used for a signature scheme should be large enough so that the birthday attack becomes computationally infeasible, i.e. about twice as large as is needed to prevent an ordinary brute force attack. It is also recommended that a recipient always cosmetically modify any document presented for signing; however this may not solve the problem, because the issuer may then suspect the signer of attempting to use a birthday attack.

Source: "http://identityaccessman.blogspot.com/2006/08/identity-dictionary.html"