Tech Info Library

AOCE: Certificate Sets Part Of The Digital Signature (10/93)

Revised: 9/30/93
Security: Everyone

AOCE: Certificate Sets Part Of The Digital Signature (10/93)

==========

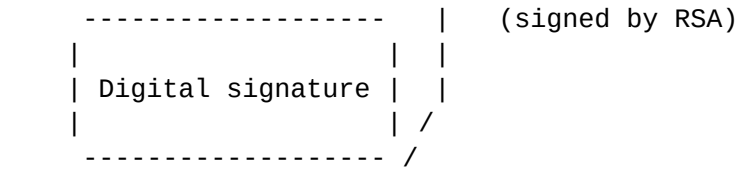
Article Created: 4 October 1993

TOPIC --

The certificate set is part of what is attached to data that has been signed. The public key certificate contains the signer's public key, signed by the issuing organization.

DISCUSSION --

A certificate set contains a complete chain of signed certificates. In this example, Joe's public key certificate is signed by Apple. The digital signature portion of Joe's signed certificate consists of a digest of Joe's public key certificate signed by Apple. That means the digest is encrypted with Apple's private key. The encrypted digest is decrypted by using Apple's public key which is the next certificate in the chain. Apple's signed certificate follows Joe's certificate. Apple's signed certificate is constructed in the same way: a public key certificate containing Apple's public key and various other identifying information followed by an encrypted digest of the public key certificate signed by RSA.



Certificate Set

There is no certificate for RSA because everyone knows RSA's public key. RSA's public key is installed into a user's Macintosh with AOCE.

To validate something signed by Joe, Apple's public key is taken from Joe's certificate set and used to decrypt the digest of Joe's public key certificate. The decrypted digest is then compared with a new digest of Joe's public key. In turn, Apple's signature is verified by using RSA's public key to decrypt the digest of Apple's public key certificate and then the digests are compared. Finally, Joe's public key is applied to the encrypted digest of the data being signed. The result is compared with a newly calculated digest of the data. If they match, the signature is validated.

If any of the above steps fails the signature will not verify.

Tech Info Library Article Number:13535