Tech Info Library

AOCE: DigiSign What It Does (12/94)

Revised: 12/9/94
Security: Everyone

AOCE: DigiSign What It Does (12/94)

===

Article Created: 04 October 1993
Article Reviewed/Updated: 09 December 1994

TOPIC ---

DigiSign is Apple’s implementation of digital signature technology. It is a way of electronically signing data. With a digital signature attached, a user can verify the signature to detect whether or not the data has been altered since the signature was attached. Signature verification also checks the validity of the signature itself, providing positive identification of who signed the data.

DISCUSSION --

DigiSign has two goals:

- To provide a mechanism by which a user can detect whether or not a document has been altered since the time it was signed

- To positively identify the signer

Signing a document does not in any way encrypt data or prevent it from being altered. While the process of signing something does use encryption in the signature process, it is not possible to use DigiSign or Apple’s digital signature manager to encrypt data.

Signing a document does not prevent someone else from reading or altering the document. The data is not encrypted, just as it was before the signature was attached. Anyone can read it and anyone can make changes.

The process of verifying a signature detects whether or not changes have been made although it is not possible to discover what the changes were.

How to Sign Something

The process of signing something begins with the data to be signed. The digital signature manager creates a 16 byte digest. The digest is a highly sophisticated checksum of the data. It is nearly impossible for two sets of data that differ in any way to produce the same digest.

This diagram ilustrates the signing process:

```
   -----------------------------
  |                             |
  |            -----            |
  |    Data   |     |           |
  |    to be  |     |           |
  |    signed |     |           |
  |            -----            |         -----
  |              |              |        |     | Data
  |              |              |------> |     |
  |            -----            |        |     |
  |    Digest |     |           |         -----
  |            -----            |      --------------------------
  |              |    --------  |     |  -----                   |
  |              | <-| Signer | |     | |-/-/-| Encrypted digest |
  |              |    --------  |     |  -----                   |
  |            -----            |     |  -----                   |
  | Encrypted |-/-/-|           |     | |     | Public key       |
  | digest     -----            |     |  -----  Certificate      |
  |                             |      --------------------------
   -----------------------------
```

The signer file uses a private key from the signer file to encrypt the digest. The data itself is not encrypted. Only the digest of the data is encrypted.

The resulting encrypted digest and a public key certificate are appended to the data file as a signature resource. The original data remains unchanged and unprotected from anyone reading the data or making changes to it. The only thing that is changed about the file is the addition of the signature resource.

How to Verify Something

The process of verifying a signature begins with calculating a new digest of the original data. Next, the public key is retrieved from the public key certificate in the digital signature attached to the document. The public key is used to decrypt the encrypted version of the digest.

The two digests are then compared. If they match, the signature verifies. If they do not match, then something has been changed on the original document so that the digests are different.

This diagram illustrates the verification process:

```
             Original Data
                 -----              Digest
                |     |             -----
                |     |----------> |     |------> = ?
                |     |             -----
                |     |
                 -----
              Public Key            Digest
                 -----              -----
                |     |----------> |     |------> = ?
                 -----    Apply     -----
                 -----   Public Key
  Public key  ->|     |
  Certificate    -----
```

The process of signature verification also verifies all signatures in the attached public key certificate. This is to ensure that the signature itself is valid and has not been altered.

Finder Signing

Third party applications will integrate digital signature technology into their products. For example, Shana Corporation will incorporate digital signature technology into their Informed Manager product to enable electronic authorization of forms.

PowerTalk users can sign entire files from the Finder by dragging a file to be signed onto a Signer file. Files signed from the Finder have a signature resource attached to them. The document is also locked. However, the file locking is not secure. In order to unlock the document, the user need only select the document, choose Get Info from the File menu and then uncheck the Locked check box. The purpose of locking the file is to prevent casual changes to the document, not to secure the file against any possible changes.

If the name of the file changes, the signature still verifies. The reason for this is that the document itself has not changed, only the name of the document.

- Validating a Signature

  A file signed from the Finder has a new icon in the Get Info window for the file the Verification button. Click this button and a DigiSign dialog box appears.

  To verify the signature, click the Verify button in the DigiSign dialog box. The signature is checked for validity. If the signature is verified a successful signature dialog box is displayed.

  If the signature fails to verify, a dialog displays stating, “The signature of ‘Document Name’ could not be verified. Either the file has been modified since it was signed or the signature itself has been altered”.

- Removing a Digital Signature

  To remove a digital signature from a document signed in the Finder, click the Remove button instead of the Verify button in the preceding process.

Article Change History:

09 Dec 1994 - Added keyword, reformatted, made numerous technical changes.

Support Information Services

Copyright 1993-94, Apple Computer, Inc.

Tech Info Library Article Number:13561