Tech Info Library

## AOCE: Public Key Cryptography (10/93)

Article Created: 4 October 1993

TOPIC -----------------------------------------------------------

This article describes Public Key Cryptography in Apple Open Collaborative Environment (AOCE).

DISCUSSION ------------------------------------------------------

While the process of signing something does use encryption, the data itself is never encrypted.  If digital signatures could be used to encrypt data, Apple would not be able to export the technology.  However, digital signatures does use encryption to create the signature.

The type of encryption used by digital signatures is called public key cryptography.  This is different from the usual private key encryption.

To encrypt something using private key encryption, a private key is used to encrypt the original data and create ciphertext.  The same private key is used to decrypt the ciphertext and reproduce the original data.  The challenge with private key technology is how to communicate the private key in such a way that it does not become compromised.

```
           Data                      Data
           -----                     ------
          |     |                   |      |
          |     |                   |      |
          |     |                   |      |
          |     |                   |      |
           -----                     ------
                 \                 /
                  \               /
    -------------  \             /  -------------
   | Private Key |  \           /  | Private Key |
    -------------    \         /    -------------
                      \       /
                        -----
                       |- - -|
                       | - - |
                       |- - -|
                       | - - |
                        -----
                      Ciphertext
```

Private key cryptography

DigiSign uses something called public key encryption. With public key encryption, a private key is still used to encrypt the original data into ciphertext. This private key remains private, protected by the entity which does the original encryption. Public key technology uses a second public key to decrypt the data. This second key is called a public key because it can be widely distributed. Since both keys are necessary to complete an encrypt/decrypt cycle, only one key need be kept secret.

```
           Data                      Data
           -----                     ------
          |     |                   |      |
          |     |                   |      |
          |     |                   |      |
          |     |                   |      |
           -----                     ------
                 \                 /
                  \               /
    -------------  \             /  ------------
   | Private Key |  \           /  | Public Key |
    -------------    \         /    ------------
                      \       /
                        -----
                       |- - -|
                       | - - |
                       |- - -|
                       | - - |
                        -----
                      Ciphertext
```

Public key cryptography

RSA

Apple has licensed digital signature technology from RSA Data Security, Inc. The RSA system has been in use for quite some time. It is the emerging commercial standard of public key encryption systems. By using a standard, Apple ensures that as commercial products using digital signature technology become available on other platforms, Apple will be compatible.

Keywords: <None>

=================================================================

This information is from the Apple Technical Information Library.

19960215 11:05:19.00

Tech Info Library Article Number: 13553