AOCE: How ASDSP Encrypts (10/93)

Article Created: 4 October 1993

TOPIC ---

This article describes how AppleTalk Secure Data Stream Protocol (ASDSP) Encrypts in Apple Open Collaborative Environment (AOCE).

DISCUSSION ---

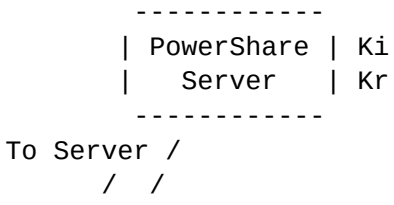
The authentication process in AOCE technology relies on a trusted authority, the PowerShare Catalog Server, to authenticate two parties to each other. Each entity on the network trusts the server to authenticate other entities on the network.

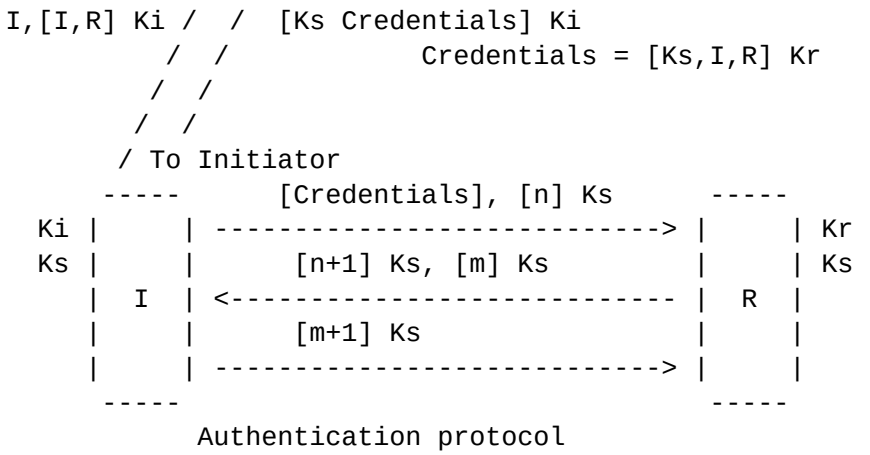
The PowerShare Catalog Server can provide these authentication services because everyone has a PowerShare account. The server converts the user's password into a key that is used to encrypt information.

A Walk Through the Protocol

Suppose "I", the Initiator, wants to talk to "R", the Recipient. There is also a PowerShare Catalog on the network. At the beginning of the process, the Initiator knows the Initiator's key, Ki, the Recipient knows the Recipient key, Kr, and the PowerShare Catalog knows both their keys.

The process begins with the Initiator sending a request to the PowerShare Catalog asking for a set of credentials to use in establishing a secure session with the Recipient. This request contains who the Initiator is and who the intended Recipient is, encrypted with the Initiator's key, Ki. The encrypted information is accompanied by a clear text statement of who the Initiator is so the catalog knows which key to use to decrypt the request. The PowerShare Catalog Servers serving that catalog folder are the only entities on the network, besides the Initiator, which can decrypt the credential request.





Authentication protocol

Once the PowerShare Catalog Server decrypts the credential request, the server sends the Initiator a set of credentials along with a session key, Ks. The session key will be used to encrypt communication between the Initiator and the Recipient. The packet returned by the PowerShare Catalog Server is encrypted with Ki, the Initiator's key. The only entity on the network that can decrypt this packet, besides the PowerShare Catalog Server, is the Initiator. Once the Initiator decrypts this packet, using Ki, the Initiator knows both its own key, Ki, and the session key, Ks.

The next step is for the Initiator to begin to send the Recipient the credentials package in order to authenticate the Initiator to the Recipient. The Initiator cannot decrypt the credentials package because the information in the credentials package is encrypted with Kr, the Recipient's key. The Initiator sends the credentials package to the Recipient who then decrypts it. The credentials package contains the session key, Ks, the Initiator's identity, and the Recipient's identity. The Recipient now has the session key.

The next portion of the authentication process is the challenge exchange. This is to prevent a wiretapper from capturing packets on the network and then replaying them later in order to establish a false session.

Along with the credentials package, the Initiator sends a random number, n, encrypted with the session key. Once the Recipient successfully decrypts the credentials and has the session key, the Recipient will be able to decrypt the random number n. The Recipient adds one to the random number n, encrypts the result with the session key, and sends it to the Initiator. At the same time, the Recipient picks its own random number, m, encrypts it with the session key, and sends it to the Initiator.

The Initiator decrypts the n+1 package sent by the Recipient and confirms that it is indeed the original random number n, +1. The Initiator then decrypts the Recipient's random number m, adds one to it, encrypts it with the session key, and returns it to the Recipient. The Recipient confirms that what it receives really is m+1.

At this point, a secure session has been established. The Initiator and Recipient can use the session key to encrypt data traveling between them using ASDSP.

What This Means

The session key can be valid for up to eight hours. After that period, a new key must be negotiated. The process of session key negotiation is transparent to the user. An application using ASDSP can specify the time period for which the session key will be used.

The Initiator and Recipient must have accounts in the same PowerShare Catalog, though not on the same server or in the same catalog folder.

Import/Export Restrictions

Apple has a license to export all AOCE technology from the United States. At this date, there is a problem with importing the technology into France. To address this issue, there will be two versions of AOCE software available: encrypted and encryption-free. The encryption-free version will be shipped in France and any other country where importing AOCE technology becomes an issue.

If both sides are using the software that allows encryption, the session is encrypted. Otherwise, the session is not encrypted.

Keywords: <None>

==========

This information is from the Apple Technical Information Library.

19960215 11:05:19.00

Tech Info Library Article Number: 13538