COCOON DATA SECURE OBJECTS INCORPORATING SECURE ENVELOPES

PROTECT

Product Description

Secure Objects incorporating Secure Envelopes is an encryption-based, access control system for protecting the confidentiality of electronic files.

The product is comprised of a client application (Secure Envelopes) and an enterprise server (Secure Objects Enterprise Server) that encompasses three back-end web based applications and three front-end web console applications.

The product uses a client-server model, with encryption performed on the Client, and access control, key management and logging being the responsibility of the corresponding Server.

Evaluation Scope

The scope of the DSD Cryptographic Evaluation included the following functionality:

a. Encryption of data

b. Authentication

Common Criteria Certification – Summary

The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

DSD Findings and Recommendations

A DSD Cryptographic Evaluation (DCE) of the product was performed in addition to the Common Criteria evaluation.

As the product has successfully completed a DCE, it can be used to downgrade the requirements for PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Information Security Manual (ISM).

Client devices used to process, store or communicate classified data must be treated as per the physical storage and handling requirements for that classification.

Where Client devices are connected to a network of a lower security classification, agencies must consult the Gateway Security chapter of the ISM.

The strength of the authentication process between Client and Server is heavily reliant on the strength of the Client's PIN. This means that the PIN must be suitably secure in order to prevent an attacker compromising the authentication process. PINs are randomly generated on the Server. Administrators must ensure the Server is configured such that PINs are at least 10 characters in length.

Where the product is used to downgrade the requirements for data in transit of a higher classification to those of a lower classification, PINs must be treated as per the physical storage and handling requirements for the higher classification. For example, if the product is used to downgrade the requirements for PROTECTED data in transit to those of UNCLASSIFIED, PINs must be treated as per the requirements for PROTECTED data, and therefore must not be delivered to Clients via public network infrastructure. It is the Administrator's responsibility to securely deliver the PIN to the Client.

The Administrator must configure the maximum number of authentication attempts before the Client is locked out to 10 or less attempts.

The strength of the HTTPS connection between Client and Server is in part reliant on the strength the Server's Private Key. This means that the Server's Private Key must be suitably secure in order to prevent an attacker spoofing the identity of the Server. Administrators must use a PKI product or Hardware Security Module that has completed a DCE to generate the Server's Private Key. Client software must be configured to only accept the Server certificate.

Recommendations given in this consumer guide take precedence over those in the ISM where there is a conflict.

Point of contact

For further information regarding the certification, cryptographic evaluation or compliance with the Information Security Manual (ISM), please email assist@dsd.gov.au or phone 1300 CYBER1 (1300 292 371).

Date of this Consumer Guide

This Consumer Guide was issued by DSD during March 2012.