Office of Information Technology Standard

Security: Encryption

Definition(s):

Encryption is the translation of data into a secret code (cipher text) that is only readable by the intended recipient. To read or decrypt an encrypted file, the recipient must have access to a secret key, certificate or password. Decryption is the conversion of cipher text into plain text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption. Asymmetric encryption utilizes two keys (one for encryption and one for decryption) and symmetric encryption uses only one key.
This standard identifies the minimum acceptable technical features of encryption for use by state agencies.

This standard addresses the following areas:

- Encryption of files over the internet via Internet Browser.
- Encryption of files in internal transit.
- Encryption of files in storage.
- Hashing Functions.
- Encryption of files through VPN.

Rationale:
Encryption ensures the authenticity, integrity, confidentiality, and reliability of digital transactions. Currently, encryption schemes offer the best method for protecting the confidentiality of data in transit and data at rest. Its purpose is to ensure privacy of data even if the access to the encrypted data is gained.

Approved Standards:

- Internet Browser: SSL 3.0 minimum for the browser over the Internet.
- Transit: SSH 2.0 for transport of files on an internal network (i.e., FTP, RCP, RSH, telnet, logins)
- Storage: AES would be minimum for files in storage (block encryption) for intel servers and mainframe.
- Hashing Functions: SHA-1 utilizing MD5 algorithm
- Remote access: IPSec with minimum 3DES encryption

- Email: Secure Multi-Purpose Internet Mail Extensions (S/MIME) version 3

The minimum acceptable key length for any symmetric encryption shall be set as 128 bits.

Applicability:
Applications and systems that require the use of encryption technologies due to the security sensitive nature of data must ensure the encryption technology utilized is consistent with the requirements of this standard.

Justification:
Encryption can enable the highest level of security for sensitive data, protecting its contents even when other security methods have been compromised. The most secure environment is when files are decrypted in operating memory of the end-workstation, just before being passed to the end-application.

Encryption is used in many different processes involving security of accessed, transported and stored data. There are many different standards, which apply to the different pieces of these processes. Products have to be selected that meet the required standards that will ensure the particular security goals desired. No single vendor or single product addresses all areas or meet desired standards in every areas of encryption security. Interoperability with other application software, operating systems and security systems will require analysis for appropriate product selection.

Guidelines/Technical Considerations:

- All newly purchased products must comply with the OIT approved standard for encryption.
- Encryption can be resource intensive, care must be applied to balance proper security with data sensitivity.
- Readily available public methods of encryption such as Pretty Good Privacy (PGP) are acceptable forms of encryption.
- Administration of a file encryption system basically consists of two tasks: initial deployment and management of encryption keys. A system should be self-enforcing not requiring user input.

Review Cycle:
As required.

Timeline:
Issued: October 7, 2004

Transition:
Not applicable