Software Product Description

PRODUCT NAME: Encryption for OpenVMS, Version 1.6 **SPD 26.74.06**

Note: This Software Product Description describes the Encryption for OpenVMS Version 1.6 software for Integrity, Alpha and VAX computer families. Except where explicitly noted, the features described in this SPD apply equally to OpenVMS Integrity, Alpha and VAX systems. Encryption Version 1.6 on Integrity and Alpha systems running OpenVMS V8.2 and later does not require a specific license, as this product is now covered under the OpenVMS operating system license. An Encryption license is required for all Alpha and VAX systems running versions of OpenVMS prior to Version 8.2.

PRODUCT SUMMARY

Encryption for OpenVMS is a layered product that enhances the confidentiality and integrity of information stored on OpenVMS systems. The rapid growth of business transactions over the Internet combined with more system administration functions being outsourced, heighten the need for stronger protection of your data. Encryption for OpenVMS provides the ability for your information to transfer safely through unknown hands and channels without disclosing its contents. Encryption for OpenVMS also provides a mechanism to detect if your information has been altered from its original form.

STANDARDS

Encryption for OpenVMS is a software implementation of the Data Encryption Standard (DES) algorithm, from the United States Government. Details on the DES cryptographic algorithm are found in the Federal Information Processing standard 46 (FIPS PUB 46-2).

DESCRIPTION

Encryption is a process that transforms data into an unreadable form called cipher. Decryption transforms the cipher back into its original (readable) form. Encryption for OpenVMS assures that the data you decrypt is the same as your original data through synchronization processes that utilizes variables known as keys. Once encrypted, data can only be decrypted with the appropriate key. Thus, encryption can protect sensitive data by limiting access to only individuals who have access to the appropriate keys.

Data authentication is a two-step process that verifies the authenticity of data, that is, that the data has not been altered. The first step is to calculate code that is directly dependent on the data. Encryption for OpenVMS supports the use of encrypted manipulation detection codes (MDCs) and cryptographic message authentication codes (MACs). MDCs are generated by algebraic functions that accept the data as input. Examples of such functions include cyclic redundancy checks. Encryption for OpenVMS uses CRC-16 to calculate MDCs. MACs are generated by cryptographic functions that take the data as input. Encryption for OpenVMS uses the DES algorithm to generate MACs. The second step is to recalculate the code as needed. If the calculated code is identical to the original code, there is assurance that the original data has not been altered.

Encryption for OpenVMS provides these features.

A DCL interface from which users can:

- Encrypt and decrypt complete files
- Generate and verify MACs on complete files

- Access the Encryption for OpenVMS help library

An Application Program Interface allowing programs to:

- Encrypt and decrypt complete files or specific data elements
- Generate and verify MACs on complete files or specific data elements

An interface to the OpenVMS Backup utility that allows users to maintain encrypted backup save sets.

File Encryption

Encryption for OpenVMS provides a Digital Command Language (DCL) interface to specify encryption keys and to control the encryption and decryption of disk-resident files. The entire contents of files are encrypted along with separately stored file attribute information such as record structure, original creation date, and original file name. These attributes are then restored at decryption time along with original file contents. Encryption for OpenVMS supports several options during the encryption and decryption process including: automatic deletion of the input file upon successful encryption and data compression of the input file before encryption.

File Authentication

The same Encryption for OpenVMS DCL interface is used to control the generation and verification of MACs for disk-resident files. Only the data portion of files are processed for MACs. File attribute information, which can normally change during authorized file operations, is not processed. The files themselves remain unencrypted and the MACs are stored in a separate data base.

For files that are encrypted, authentication checks are done automatically by Encryption for OpenVMS during the decryption processes. An MDC is calculated and is encrypted along with the other file attribute information. When the file is decrypted, the MDC is recalculated and compared with the decrypted MDC.

Key Specification and Storage

Key values for the encryption and authentication algorithms may be specified as either sixteen hexadecimal digits or by a more easily remembered and manipulated phrase of words and numerals. The alphanumeric phrase format is scanned and packed into a form required by the selected algorithm. In Encryption for OpenVMS Version 1.6, all keys are stored, themselves encrypted, in the OpenVMS logical name tables.

Application Program Interface

Encryption for OpenVMS provides a set of callable routines that allows users to integrate its encryption/decryption and authentication functions in application programs. The Encryption for OpenVMS library of callable routines adheres to the OpenVMS Calling Standard and the modular design established in the *Guide to Creating OpenVMS Modular Procedures.* Entry points are provided to permit the specification and deletion of keys, encryption/decryption of complete files, encryption/decryption of user-specified data elements, and generation of MACs for user-specified data elements.

For example, the data-encryption facility permits a user application to manage a data file containing employee information with the salary data field encrypted. Almost all functions possible by the DCL command interface are provided by the application interface. The binary kit includes a complete PASCAL example of an encrypting utility to serve as a model of how such an application might be written.

Backup Utility

The online OpenVMS Backup utility incorporates an interface to Encryption for OpenVMS to permit the encryption of backup save sets. Restoration or listing of the contents of an encrypted backup save set is not permitted without respecification of the encryption key and algorithm parameters used when the save set was encrypted and created. When key and algorithm parameters are stored or transmitted separately from the resulting backup media, access to the backed up data may be more carefully controlled. This enhances the security of backup tapes and disks when stored or transported off the customer's premises.

DES Algorithm and Modes

The DES algorithm may be applied in several modes to the processing of data. Encryption for OpenVMS Version 1.6 supports: Electronic Code Book mode (ECB), Cipher Block Chain mode (CBC), Cipher Feedback mode (CFB), and Message Authentication Code mode (MAC). CFB mode is limited to 8-bit character feedback only. The MAC mode uses the CBC mode for processing.

INSTALLATION

Only experienced customers should attempt installation of this product, Compaq recommends that all other customers purchase Compaq's Installation Services. These services provide for installation of the software product by an experienced Compaq Software Specialist.

HARDWARE REQUIREMENTS

To install Encryption for OpenVMS Version 1.6 an additional 2000 free blocks of disk space is required.

SOFTWARE REQUIREMENTS

Encryption for OpenVMS runs on the following versions of OpenVMS.

OpenVMS Integrity

OpenVMS Integrity Version 8.2-1
OpenVMS Integrity Version 8.2

OpenVMS Alpha

OpenVMS Alpha Version 8.2
OpenVMS Alpha Version 7.3-2

OpenVMS VAX

OpenVMS VAX Version 7.3

ORDERING INFORMATION

Encryption for OpenVMS Integrity and Alpha

For Versions 8.2 and 8.2-1 on Integrity and Version 8.2 on Alpha, the software license is covered by the OpenVMS operating system license.

Encryption for OpenVMS Alpha Version 7.3-2

Software License: QL-597A*-**
Software Documentation: BR-081AA-GZ
Software Product Services: QT-597A*-*

Encryption for OpenVMS VAX Version 7.3

Software License: QL-081A*-**
Software Documentation: BR-081AA-GZ
Software Product Services: QT-081A*-**

Note: * Denotes variant fields. For additional information on available licenses, services and media, refer to the appropriate price book.

SOFTWARE WARRANTY

As with any security product, Encryption for OpenVMS should be considered part of an overall security plan. Customers are encouraged to follow industry recognized security practices and not rely on any single security product to provide complete protection.

DISTRIBUTION MEDIA

For Integrity servers, this product is distributed as part of the OpenVMS Layered Product Library. For Alpha and VAX systems, this product is distributed as part of the Software Product Libraries.

The software documentation is also available as part of the OpenVMS Online Documentation Libraries on CD–ROM.

DOCUMENTATION

Encryption for OpenVMS documentation includes:

- *Encryption for OpenVMS Installation and Reference Manual* — Details the basic encryption user commands, documents the application programming interface, and provides the installation instructions.