digital™

Software Product Description

PRODUCT NAME: Purveyor™ Encrypt WebServer Version 1.2 for OpenVMS™ SPD 56.24.01

DESCRIPTION

Purveyor™ Encrypt WebServer V1.2 for OpenVMS™ from Process Software Corporation is one of three commercial HyperText Transport Protocol (HTTP) web servers in the OpenVMS Internet Product Suite. Purveyor Encrypt WebServer combines the reliability, security, and scalability of the OpenVMS platform with the graphical ease of use and functionality of World Wide Web technologies. Purveyor Encrypt lets you easily Web-enable your existing OpenVMS applications, develop an internal corporate intranet, or create a robust external web presence—all within a secure web environment. Using Secure Sockets Layer (SSL) encryption and authentication, Purveyor Encrypt ensures the security of access, traffic, and requests made to Web-enabled OpenVMS systems, which typically house mission-critical data. With Purveyor Encrypt WebServer, data is secure because of the following attributes:

— Privacy: all messages between client and server are encrypted.

— Authentication: server and sender are authenticated through public key/private key certificates.

— Reliability: message integrity is ensured during transit by means of message authentication code.

Purveyor Encrypt WebServer will also run without encryption services, thereby eliminating unnecessary network overhead if encryption is not required.

Purveyor Encrypt WebServer runs over DIGITAL TCP/IP Services for OpenVMS or other TCP/IP for OpenVMS implementations and can be configured to run in a clustered environment for high availability. It also includes the following other features:

- Virtual servers that allow more than one Web server to be configured.
- An integrated proxy server that requires no additional hardware or software.

Purveyor Encrypt provides the means to Web-enable existing OpenVMS applications within a secure web environment. This includes the power of the Web, such as hypertext links, Internet access, graphics, and multimedia.

Purveyor Encrypt for OpenVMS has been designed to take advantage of the OpenVMS architecture. Purveyor Encrypt fully supports load sharing across the multiple CPUs of a symmetric multiprocessing system for highly efficient system throughput. Additionally, Purveyor provides sophisticated support for clustering, including transparent operation on mixed-architecture OpenVMS Cluster. This allows you to have a primary Web server on one cluster system (either VAX or Alpha), with automatic, transparent failover to any other system in the cluster (either VAX or Alpha).

Flexible and Robust User Security

Purveyor Encrypt WebServer offers organizations a highly flexible and secure environment for managing access to all documents on the server, whether for an Internet or intranet application. Purveyor Encrypt supports the Secure Sockets Layer or SSL protocol, which provides advanced security features and has been widely adopted by major provideers of internet hardware and software.

SSL employs public key cryptographic technology from RSA Data Security, an established leader in computer data security, and works with various encryption algorithms. Purveyor Encrypt WebServer supports public

key encryption and delivers server authentication using signed digital certificates. A digital certificate is used to associate an identity with a server's public key. Digital signatures ensure the integrity and authenticity of information within a certificate. Purveyor Encrypt WebServer requires a signed digital certificate to operate securely; certification is an additional fee-based service. Pricing is available from your certification authority.

Purveyor Encrypt WebServer is available in both 40-bit and 128-bit encryption schemes. The difference between 128- and 40-bit encryption is, most notably, that the U.S. government restricts the export of 128-bit encryption but not the export of 40-bit encryption.

128-bit encryption provides significantly greater cryptographic protection than 40-bit encryption. It is now necessary to employ larger keys to counter the increasing computing power of potential criminals.

128 bits and 40 bits refer to the size of the key used to encrypt the message. 128-bit encryption is roughly 309,485,009,821,345,068,724,781,056 times stronger than 40-bit encryption. 40-bit encryption is not considered ''strong'' security in the cryptographic community. Even accounting for Moore's Law, which states that computing power doubles about every 18 months, 128-bit encryption represents a very strong method of encryption for the forseeable future.

Please note that this product is subject to export restrictions under the U.S. Department of Commerce's Export Administration Regulations (EAR) and cannot be transmitted in any form outside the United States or to a foreign national in the United States without a valid Department of Commerce export license.

In addition to encryption, Purveyor offers other administrative and management tools, such as access controls and proxy services.

Access Control

Secure your documents or server to only authorized visitors. Management is easily accomplished through the Remote Server Manager, by simply pointing and clicking. Access control lists do not need to be created. The server provides functionality to restrict access to individual HyperText Markup Language (HTML) pages based on IP address, user name, or both. This allows servers to be customized for access by groups, such as company employees or external users accessing specific information that may be restricted to authorized customers.

Purveyor Encrypt for OpenVMS supports multiple authorization databases for access control. In addition to Purveyor's built-in access control database, which provides for Web access control without the need to create OpenVMS accounts for each Web user, Purveyor has integrated support for the use of the OpenVMS SYSUAF.DAT file for authorization. Through the use of Purveyor's external authentication feature, you can substitute any external database, even integrate a relational database like Oracle® Rdb.

Proxy Services

Proxy server support is provided for HTTP, FTP, and Gopher protocols, providing LAN security by restricting Internet activities of LAN users. The proxy server also offers improved performance features by caching HTML pages to provide faster response to clients on the LAN. Purveyor Encrypt also provides proxy-to-proxy support for corporations with multiple proxy servers or firewalls.

Authentication

Purveyor Encrypt provides full access control to files and directories on the server. The secure server queries and verifies the integrity of digitally signed documents as it receives them. Authentication takes place by using agreed upon keys to generate and verify the message digest, which consists of summary information that is transmitted along with the message.

Key Management

Purveyor Encrypt allows management of multiple keys, stored locally and accessible through a user-specified password. System administrators can create private keys that specify a password, create certificates that may contain the public key and the encrypted private key, and sign certificates that specify the private key to use.

Application Interfaces

Process Software has codeveloped, with Microsoft Corporation, a new Internet Server Application Programming Interface (ISAPI), which provides a faster, higher-performance interface to back-end applications from the Web server. ISAPI provides a significant performance advantage over conventional CGI. ISAPI is supported by a number of Web server vendors allowing application developers to write for a single specification and to deliver on multiple platforms. Purveyor Encrypt WebServer for OpenVMS also supports the Common Gateway Interface (CGI). CGI programs can be DCL command procedures, applications written in any language, or a combination.

Supports Multiple Web Sites

Purveyor supports many logical Web sites on one server system (128 with the TCPware® TCP/IP for OpenVMS stack). It supports multiple ''virtual servers,'' in which a single Web server process responds to multiple TCP/IP addresses and host names. It can also run multiple copies of the Web server, with independent configuration databases, allowing totally independent operation.

Customized Logging

Purveyor Encrypt provides full transaction logging, including time, date, HTML page, and the IP address of the requester, plus capture of ‘‘referred URLs.’’ Users select information to log and report.

Server Management

Purveyor Encrypt allows users to manage administrative features of the Web server from a remote location on any browser. The user authentication feature ensures secure access.

Templates and Sample Home Pages

Sample HTML Web pages and forms help you get started using the server and its capabilities.

SOFTWARE PREREQUISITES

Purveyor Encrypt WebServer Version 1.2 for OpenVMS requires:

- OpenVMS Version 6.1 or later
- DECwindows ™ Motif ® Version 1.2-3 for OpenVMS or later (only if running a browser on OpenVMS to manage the server)
- DIGITAL TCP/IP Services for OpenVMS Version 3.3 or later or any TCP/IP product for OpenVMS that supports the Berkeley socket interface

HARDWARE REQUIREMENTS

Purveyor Encrypt WebServer has no specific hardware requirements. Any valid, supported configuration can support the server. The level of performance will vary depending upon the processor, memory, and system load.

ORDERING AND LICENSING INFORMATION

- Media: OpenVMS Internet Product Suite Media Kit (CD–ROM; Alpha and VAX):

  QA-5CNAA-H8 (International)

  QA-577AA-H8 (U.S. and Canada only)

- License: Purveyor Encrypt WebServer V1.2 for OpenVMS VAX or Alpha:

  QL-57HA9-AA (International)

  QL-57GA9-AA (U.S. and Canada only)

SOFTWARE WARRANTY

DIGITAL warrants its software products according to the terms of the DIGITAL license for each product. DIGITAL warrants that the software will substantially conform to the applicable Software Product Description or documentation accompanying the software unless provided "AS IS."

SOFTWARE PRODUCT SERVICE

Digital does not provide service for this software product. For information about software support, contact Process Software Corporation.
For calls from U.S. and Canada: 800-722-7770.

All other locations: 508-879-6994.

FOR MORE INFORMATION

For more information about OpenVMS Internet Product Suite, visit the OpenVMS home page at:

`http://www.openvms.digital.com`