RETIRED: Retired products sold prior to the November 1, 2015 separation of Hewlett-Packard Company into Hewlett Packard Enterprise Company and HP Inc. may have older product names and model numbers that differ from current models.

Models

The proven solution for Internet commerce—powerful hardware-based security at a reduced size and cost

Product highlights

- Adds a dedicated cryptographic coprocessor to your server, offloading cycle-intensive cryptographic tasks
- Supports public and symmetric key cryptography
- Takes full advantage of the PCI bus system resources for fast, high-performance security processing
- Manages and protects cryptographic keys using specialized, secure hardware
- Provides powerful hardware security features at an affordable price
- Plugs directly into your Windows NT Server or UNIX system based server Available for use worldwide

Fast, offloaded encryption processing for PEM and EDI applications

Now you can provide the strong security and fast processing that Internet commerce requires, without adding costly server capacity. WebSafe2/PCI Internet Security Processor (ISP) adds a dedicated hardware encryption engine on a low-cost, easy-to-use PCI board. Now you can add Atalla security directly to your Windows NT® 4.0 Server or UNIX® system–based server, and provide speedy, secure key management, encryption/decryption, and certificate management (using DES, RSA, and DSS) in a very cost-effective manner.

Because cycle-intensive cryptographic operations are handled by the harware engine rather than your server, transactions can be processed more quickly, and your server is freed to handle business applications. A dedicated encryption engine keeps keys physically and logically secure, while providing a full range of flexible management options.

Strong security. Fast processing. Proven solutions. Compaq delivers the power of Atalla hardware security to you.

The most sophisticated security available

Data security on a public network, such as the Internet, needs to be even more stringent and sophisticated than what you'd use on a private network. That's why Compaq designed and built WebSafe2/PCI ISP.

Software-based solutions are always vulnerable to attack. But with a hardware-based approach, all cryptographic processing takes place within the safety of a physically secure shell. Encryption keys are generated, disseminated, controlled and maintained by the hardware system; they never appear in cleartext form and cannot be altered at any point on the network.

The fastest, most cost-effective processing

Key lengths continue to grow, as do the number of cryptographic operations required for each transaction sent over the Internet. This exponential growth imposes an enormous burden on server CPU cycles. The most cost-effective solution is to offload the security processing to a hardware-based system like WebSafe2 ISP. It delivers faster processing than software-based solutions can achieve, while freeing the host processor to handle business applications.

RETIRED: Retired products sold prior to the November 1, 2015 separation of Hewlett-Packard Company into Hewlett Packard Enterprise Company and HP Inc. may have older product names and model numbers that differ from current models.

Technical Specifications

Public key support

- RSA key management (key generation, distribution, storage, and usage)
- RSA public key cryptography
- Public Key Cryptography Standards (PKCS)
- Digital signatures
- Digital envelopes

DES support

- PIN security, ANSI X9.8 (PIN block only)
- Data encryption/decryption, ANSI X3.92, and FIPS Publication 46
- DES key management (key generation, distribution, storage usage, and destruction)
- Message Authentication Code (MAC), ANSI X9.9

SSL, PEM, and S/MIME support

- Digital signatures
- Key management
- Encryption/decryption algorithms

Standard ISP features

Cryptographic functions

Supported algorithms

- RSA, DSA, DES, MD5, SHA-1, Diffie-Hellman, RC2 and RC4

Supported key lengths

- 256 to 2048 user selectable for public key operations
- 40 to 128 for symmetric key operations

ISP security features

Physical security

- Compliance with FIPS 140-1 level 3 requirements

Logical security

- The security architecture precludes unauthorized retrieval of sensitive data in its clear text form anywhere in the network.
- The RSA algorithms and key management are embedded to protect against unauthorized access or modification.

Secure initialization

- Hardware is initialized with cryptographic keys using Atalla's Secure Configuration Terminal (SCT).

Secure key management

- This additional layer of security provides hierarchical support for varied key types to restrict how individual keys are used.

Specifications

Physical dimensions	Length	6.875 in/17.73 cm
	Width	3.525 in/9.09 cm
	Height (primary side)	0.570 in/14.48 mm
	Height (back side)	0.105 in/2.67 mm
Certification/compliance	Safety	UL, CSA, TUV
Export	Some functionality may not be available or is restricted on export versions.	

© Copyright 2003 Hewlett-Packard Development Company, L.P.

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained.