

HP Atalla WebSafe functionality

Data sheet



Key features and benefits

- Supports public and symmetric key cryptography
- Industry-leading physical security
- Plug-and-play fast host connectivity
- Superior flexibility and ease of use
- Scales to handle increasing traffic requirements
- Space-saving, state-of-the-art, rack-mountable platform
- Easy firmware upgrades via the Atalla A8100 CD-ROM

Atalla WebSafe functionality secures mission-critical Internet transactions on the Atalla A8100 network security processor, the market's most secure, low-cost cryptographic hardware.

HP Atalla WebSafe functionality supports both the symmetric and public key cryptography required to secure today's e-commerce applications. It is also the most secure bridge between the Internet and the PIN-based financial interchange network of banks, switches, and other financial institutions. It provides the dedicated hardware encryption processing capability that can handle millions of secure transactions for the global bank payment network every day. WebSafe functionality, a set of Internet commands for the HP Atalla A8100 network security processor (NSP), is physically secure and has received Federal Information Processing Standard (FIPS) 140-2 Level 3 certification from the U.S. National Institute of Standards and Technology (NIST).

The cycle-intensive cryptographic operations are handled by the Atalla A8100 NSP rather than your general-purpose servers, which eliminates bottlenecks and lowers hardware costs. WebSafe functionality for the Atalla A8100 NSP is configured and managed by the Atalla Secure Configuration Assistant (SCA). The Atalla SCA is a handheld device with an easy-to-use graphical user interface that ensures accuracy while maintaining security. The SCA Remote Management application allows WebSafe functionality to be securely managed from anywhere in the network. WebSafe functionality provides a direct bridge between the Internet and the bank payment network security protocols, resulting in faster processing and more efficient management.

The only end-to-end security solution for Internet commerce

Atalla WebSafe functionality is the most secure RSA-to-DES translation device available today. It is the first hardware-based functionality designed to move today's point-to-point Internet security into a full end-to-end security system. The best of both private and public security methods are combined into a single security processor that supports both secret and private keys, such as DES and two-key and three-key Triple DES, and public keys, such as RSA. Those organizations facing compliance with privacy mandates such as the Gramm-Leach Blighly Act (GLBA) or the Health Insurance Portability and Accountability Act (HIPAA) may also find the WebSafe functionality of benefit in protecting customer and employee records.

From its hardened, rack-mountable, 1U perimeter to its state-of-the-art tamper-resistant architecture to its secure remote key loading, the Atalla A8100 NSP has reset the bar for physical and logical security, flexibility, and ease of use. Its also interoperates transparently with non Atalla hardware security modules. As the optimal platform for the WebSafe functionality, the Atalla A8100 NSP enables customers to derive the full security value of both symmetric and public key encryption.

The new-generation Atalla A8100 NSP incorporates more than three decades of standards-based cryptographic expertise coupled with the latest open systems technologies from HP—making the Atalla A8100 NSP the safest, and easiest to use, security processor solution to secure your Internet or e-commerce networks.

Atalla hardware-based encryption: Stronger than any software solution

Data security on a public network, such as the Internet, needs to be even more stringent and sophisticated than that on a private network. Software-based solutions are always vulnerable to attack, but with the Atalla hardware-based solution, all cryptographic processing takes place within the safety of a physically and logically secure shell. This “hardware-encapsulated envelope” safeguards algorithms and keys against unauthorized access, disclosure, alteration, duplication, and substitution.

An Atalla hardware-based encryption solution ensures the security that Internet commerce requires. Software-based security products decrypt sensitive data in unsecured memory, displaying keys and other sensitive data in readable form, which makes the data vulnerable to cyber-pirate attacks.

Atalla NSP hardware, on the other hand, performs all cryptographic processing within a physically secure shell. Any tampering automatically triggers measures that “zeroize” data such as passwords and keys. Keys and other sensitive data never appear in cleartext form, and thus remain safe from attacks by hackers and even from insiders within the organization. The Atalla A8100 NSP hardware along with WebSafe functionality is the most sophisticated security available today.

The fastest, most cost-effective processing

To stay ahead of the hacker community, cryptographic 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 security processor like the Atalla A8100 NSP with WebSafe functionality. It delivers faster processing than software-based solutions can achieve, while freeing the host processor to handle business applications.



Easy migration from earlier Atalla products

WebSafe functionality for the A8100 NSP is a superset of the previous Atalla WebSafe2 and SignMaster products. Migrating from those products to the new WebSafe functionality on the A8100 NSP is very simple. Users of the Websafe2 Internet security processor (ISP) must only configure the A8100 NSP to have the same IP address and Master File Key as the WebSafe2 ISP and the switch units. Users of the Load Balancer to communicate to a Websafe2/PCI card must configure the Load Balancer to match the IP address of the WebSafe functionality on the A8100 NSP. No programming modifications are necessary. Finally, users of theWebSafe2/PCI card that use DeviceControl() functions to communicate with the card need to replace the communications routines with simple TCP/IP socket calls.

Physical security

- FIPS 140-2 Level 3 certification for physical security plus active zeroization
- Rack-mountable (1U), physically fortified form factor
- Double-locking bezel with Medeco locks
- Penetration protection (protective grid)
- Out-of-range temperature and voltage detection
- Low battery voltage protection
- Data security and key management implemented within a secure hardware perimeter for protection against manipulation

Logical security

- Advanced security architecture that prevents retrieval of sensitive data in cleartext form
- Automated and manual key management options
- Encrypted, convenient configuration, management, and key loading via the Atalla Secure Configuration Assistant (no cleartext passing of keys or key components)

Fast host connectivity

- Autosensing 10/100/1000Base-T Ethernet interface for point-to-point TCP/IP
- Integrated high-performance TCP/IP stack and communications processor
- Asynchronous connection suitable for lower transaction workloads

Flexibility and extensibility

- Broad application support
- Easy command set customization
- Seamless interoperability with non Atalla environments
- Command set compatibility with previous WebSafe2 and SignMaster Internet security processors

Easy to use and manage

- Encrypted, convenient key loading via the Atalla Secure Configuration Assistant
- Fast, convenient release upgrades via CD-ROM
- No need to replace firmware components (for example, EPROM) when upgrading

Public key support

- RSA key management (key generation, distribution, storage, and usage)
- RSA digital signatures (PKCS1-v1_5)
- DSA digital signatures
- RSA digital envelopes (PKCS1-v1_5)
- Diffie-Hellman Key Exchange (PKCS-3)

DES support

- Data encryption/decryption, ANSI X3.92, ANS X9.52 (TCBC), and FIPS Publication 46
- DES key management (key generation, distribution, storage usage, and destruction)
- Message Authentication Code (MAC), ANSI X9.9
- Retail key management, ANSI X9.24–1998

SSL, PEM, and S/MIME support

- Digital signatures
- Key management
- Encryption/decryption algorithms
- Diffie-Hellman
- RC2 and RC4
- SHA-1, MD5, and MD2 hashing algorithms

Global support

HP provides worldwide support and services to ensure a secure business environment.

Technical specifications

Atalla A8100 network security processor

Physical dimensions

Height	4.34 cm (1.71 in)
Width	48.64 cm (19.15 in)
Depth	68.45 cm (26.95 in)
Weight	12.3 kg (27 lb)

Controls	Power on/off switch
-----------------	---------------------

Electrical

Dual input voltage, autosensing	100–120 V AC at 3 A, 50–60 Hz; 200–240 V AC at 1.5 A, 50–60 Hz
Power consumption	120 V AC at 1.8 A, average; 3.25 A maximum at power on

Operating environment

Temperature	10°–35° C
Relative humidity	10%–85% at 35° C noncondensing

Certification/compliance

Safety	ULC, CE, TUV approved
Emissions	FCC, C-Tick, Gost

Connectivity

Communications	Ethernet running TCP/IP
Connection	10/100/1000Base-T (RJ45) autosensing Asynchronous connection

Ordering information

Product ID	Product description
T16/A8100	Atalla WebSafe functionality Atalla WebSafe functionality is offered at no charge to Atalla 8100 NSP customers with a current maintenance contract. All Atalla A8100 NSPs ship with WebSafe functionality.
T16/AN015	Atalla Secure Configuration Assistant, 110 V, with three security administrator cards
T16/AN016	Atalla Secure Configuration Assistant, 220 V, with three security administrator cards

HP Atalla WebSafe functionality

For more information

HP Financial Services provides innovative financing and financial asset management programs to help you cost-effectively acquire, manage, and ultimately retire your HP solutions. For more information on these services, contact your HP sales representative or visit www.hp.com/go/hpfinancialservices.

HP Customer Support provides a broad spectrum of services to commercial and enterprise customers with performance and availability services, such as proactive mission-critical services, and services ranging from deployment to support management of the entire IT infrastructure, including HP and multivendor environments. For more information on these services, contact your HP sales representative or visit www.hp.com/hps/support.

© 2004 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 herein.

To learn more, visit www.hp.com/go/atalla.

5982-8130EN, 08/2004

