

HP Atalla Key Block

Data sheet



The Atalla Key Block is an extensible, secure, industry-standard foundation for cryptographic key management.

The Atalla Key Block is a new-generation key management solution from HP, designed from the ground up to provide unrivalled logical security for Triple DES and other advanced cryptographic keys. No matter what strength cryptographic algorithm is in use, secure key management is pivotal to its effectiveness. Customers deploying the Atalla Key Block are able to derive maximum value from their cryptographic schemes, overcome key security issues associated with mixed encryption environments, and enjoy extensible protection far into the future.

Designed for simplicity of use as well as security, the Atalla Key Block is supported by leading financial institutions, ISVs, and HP industry partners with an interest in the security of financial networks.

Raising the bar for cryptographic key protection

The heart of the Atalla Key Block is a variable-length, encrypted key field. This enables the key block to optimally secure keys of any length including single-length DES, two- and three-key Triple DES, public keys, and more. Shorter, weaker keys are provided the same protection as longer, stronger keys, thus eliminating a major vulnerability of mixed encryption environments where a broken single-length DES key can compromise overall system security.

The variable-length key field also enables the Atalla Key Block to secure future key types and key lengths. Customers can use the Atalla Key Block as the foundation for a safe and cost-effective migration, not only from single-length DES to Triple DES, but also from Triple DES to AES and beyond.

The result of more than three decades of cryptographic expertise, the Atalla Key Block has become the industry standard for cryptographic key management as defined by ANSI X9.24-2004, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques.

Features at a glance

- Enables true Triple DES security for ATM/EFT/POS networks
- Supports two- and three-key Triple DES, single-length DES, and public keys
- Protects mixed encryption environments
- Eases migration to future algorithms, key lengths, and key types
- Simple to implement and use

Compliance with all ASC X9.24 and X9.52 security requirements

The Atalla Key Block prevents an attacker from

- Changing any attribute of any key
- Changing any bits of any key
- Using part of a key as the entire key
- Rearranging any part of a key
- Substituting parts of a key into another key
- Identifying weaker keys

Secure, industry-leading architecture

The Atalla Key Block has the following attributes.

Variable-length, encrypted key field

- Protects key values
- Camouflages existence of shorter, weaker keys
- Keys can vary in length (8, 16, 24 bytes and longer)
- Pads shorter DES keys to three-key Triple DES length
- Triple DES encrypted

Clear header

- Controls key usage
- Common attributes for all key types (8 bytes fixed)

Message Authentication Code (MAC)

- Cryptographically binds key field to header using Triple DES
- Prevents tampering and maintains key integrity

Flexible and extensible

- Facilitates and secures mixed DES and Triple DES encryption environments
- Supports single-length DES, two- and three-key Triple DES, and public keys
- Supports easy deployment of new algorithms, key types, and key lengths
- Enables easy, cost-effective migration to more advanced future cryptographic mechanisms
- Provides ATM public key support for secure remote ATM key loading

Easy to use

- Simple to understand and manage without security background
- Attributes on byte boundaries
- Attributes represented by printable constants (ASCII letters or numbers)

Migration to the Atalla Key Block is made simple by firmware upgrades via the Atalla Ax100 CD-ROM.



Easily deployable

- Comprehensive migration guidelines and support provided by Atalla security products
- Runs on new-generation Atalla Ax100 NSP series
- Key conversion command that converts from Atalla variant key management scheme to Atalla Key Block
- GUI on Atalla Secure Configuration Assistant designed to make key loading and key transfer accurate and easy

Peak Triple DES processing performance for Atalla Ax100 NSPs with the Atalla Key Block

The new-generation Atalla Ax100 NSPs are the hardware complement to the Atalla Key Block, combining uncompromising security for sensitive data, high-performance processing, and fast host connectivity. Atalla Ax100 NSPs enable the Atalla Key Block to execute its functions within a 1U-high, rack-mountable, physically fortified form-factor, featuring

- Full FIPS 140-2 Level 3 certified protection
- Industry-leading Triple DES performance of up to 540 PIN translates per second

Together, the Atalla Key Block and Atalla Ax100 NSPs deliver the most secure implementation of Triple DES and other advanced encryption mechanisms in the industry.

HP Atalla Key Block

Ordering information

Product ID	Description
T16/AKBMIGRATE	<p>Atalla Key Block firmware upgrade for legacy Atalla NSPs</p> <p>The Atalla Key Block upgrade is offered at no premium to legacy Atalla NSP customers with a current maintenance contract. Migration must be started from legacy Atalla Release 2.9.</p> <p>All Atalla Ax100 NSPs ship with the Atalla Key Block.</p>

Specifications

Contents	Length
Clear header	8 bytes, fixed length
Comma (,)	1 byte, fixed length
Encrypted key field	Fixed 48 bytes for DES and Triple DES, but is designed to variable length to accommodate other cryptographic keys of greater lengths
Comma (,)	1 byte, fixed length
MAC	16 bytes, fixed length

© 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.

For more information, go to www.hp.com/go/atalla.

5982-5807EN, 06/2004

