

HP Atalla NSP Enhanced software



Enhanced software for HP Atalla Ax160 Network Security Processors



NSP Enhanced software features at a glance

- Optional support for multiple MFKs
- SSL/TLS secure connectivity support
- New PIN and key component printing commands
- Whitelist client restriction
- Automated health diagnostic checks
- NSP CPU performance monitoring
- Enhanced remote manageability
- Stronger SCA key sizes (2048-bit RSA keys)
- Secure clock adjustment

Overview

The HP Atalla NSP Enhanced software offering is a software-only release loaded with features that enhance the HP NSP Enhanced software hardware security module (HSM) portfolio. This offering continues to reap the benefits of your Ax160 NSP enterprise class hardware security module and Federal Information Processing Standard (FIPS) 140-2 Level 3 security while taking advantage of increased security and usability features—including Secure Sockets Layer (SSL) and Transport Layer Security (TLS) secure connectivity, whitelist access control, and optional multiple Master File Key (MFK) capability.

NSP Enhanced software incorporates more than 35 years of standards-based cryptographic expertise from Atalla. This makes the NSP Enhanced software an additional enhancement to complement your Ax160 NSPs and will provide your organization additional feature options for your ATM/EFT/POS payment processing environment.

Wide ranging HSM interoperability

HP Atalla NSPs also interoperate transparently with non-Atalla hardware security modules. As an efficient platform for the industry-standard Atalla Key Block, the Atalla NSP Enhanced software package derives the full security value of two- and three-key triple DES and public key encryption—alone or in a mixed encryption environment—while providing you a cost-effective migration path to even stronger future algorithms.

Powerful features for demanding environments

The NSP Enhanced software package enables clients to make trusted SSL/TLS secure connections with the Atalla NSP, thereby preserving privacy and integrity of the command and response interactions. Further, the NSP can now limit the range of IP addresses it will accept connections from—better protecting the NSP from potential “insider” attack.

Automated health diagnostic checks can now be run facilitating an important PCI HSM requirement; while administrators directly monitor NSP CPU utilization to ensure the NSP HSM use is not going to max out—potentially crippling a transaction processing capabilities.

PIN and key component printing is now possible by simply connecting your printer to the Ax160 NSP second NIC and enabling printing commands with your Secure Configuration Device (SCA) device. The NSP time can also be set through the SCA to the local geographic region where the NSP resides. New remote manageability commands have also been added to help you more securely manage the files on the NSP Universal Serial Bus (USB) flash memory device. The security of the SCA and NSP hardware security module communication has also been enhanced with the use of a large 2048-bit RSA key.

Finally, a multiple MFK capability now exists. For an additional enablement charge (and only on the HP Atalla A10160 NSP platform), you can now create up to 10 MFKs. Each MFK will have its own:

- Security association
- Pending Master File Key (PMFK)
- NSP security policy (i.e., command and option configuration)
- ASCII, management, status, and printing ports
- VNSP log file (contains all VNSP-specific log messages)

Features

Logical security

- Industry-standard Atalla Key Block key management technology
- Advanced security architecture that prevents retrieval of PINs, Keys, and other sensitive data in clear text form
- Automated and manual key management options
- Encrypted, convenient configuration, management, and key loading via HP Atalla Secure Configuration Assistant (no clear text passing of keys or key components)
- Remote ATM key initialization and rekeying via the optional Atalla Remote Key feature
- PCI Security Standards Council PIN Transaction Security (PTS) approved hardware

Flexibility and extensibility

- Broad application support (ATM/EFT/POS, stored value, loyalty cards, corporate funds, EMV cards, transfer)
- Customer-defined security policies
- Easy command set customization
- Seamless interoperability with non-Atalla environments and hardware security modules
- Remote rekey support for NCR, Diebold, Wincor Nixdorf, and other ATM vendor devices
- Command set compatibility with earlier models of Atalla NSPs

Easy to use and manage

- Encrypted, convenient key loading via the Atalla Secure Configuration Assistant
- Simple-to-use GUI for key loading and configuration
- Fast, convenient secure software upgrades
- No need to replace when upgrading (for example, EPROM)

Standards support

Cryptographic support

- Data encryption algorithm (DEA) standard (ANSI X3.92-1987, ISO 10126-2), DES, and two- and three-key triple DES
- Banking procedures for message encipherment, general principles (ISO 10126-2)
- PIN management and security, parts 1 and 2 (ANSI X9.8, ISO 9564-1 and 2)
- Message authentication (ISO 9797-1, ANSI X9.9-1987, ISO 9807)
- MasterCard CVC, Visa CVV, and American Express CSC
- MasterCard CVC3, Visa dCVV, and Discover dCVV
- Unique key per transaction (ANSI X9.24-2004)
- EMV-based smart card support

PIN verification methods

- IBM 3624
- Visa PVV
- Atalla Bi-Level DES
- Diebold
- NCR

PIN block formats

- ISO 9564
- PIN pad
- IBM 3624 ATM PIN format
- IBM 4731 PIN block
- IBM encrypting PIN pad
- Unisys (Burroughs)
- Diebold
- Docutel/Olivetti

Key management standards

- ANSI X9.24 parts 1 and 2
- ANSI X9.52
- Triple DES—derived unique key per transaction

Resources

Learn more about **HP Enterprise Security products, services, and solutions**
hp.com/go/atalla

Contacts

Worldwide sales assistance
hpatallaglobalsales@hp.com

Sales orders
atallaorders@hp.com

Worldwide technical support

Atalla Support
Atalla.support@hp.com
U.S. only: +1-800-500-7858
Outside U.S.: +1-916-414-0216

HP Atalla and HP Security

About HP Atalla and HP Security Voltage

HP Atalla and HP Security Voltage drive leadership in data-centric security and encryption solutions. With over 80 patents and 51 years of expertise, we protect the world's largest brands and neutralize breach impact by securing sensitive data at rest, in use, and in motion. Our solutions provide advanced encryption, tokenization, and key management that protects sensitive data across enterprise applications, data processing IT, cloud, payment ecosystems, mission-critical transactions, storage, and Big Data platforms. HP Atalla and HP Security Voltage solve one of the industry's biggest challenges: simplifying the protection of sensitive data in even the most complex use cases.

About HP Security

HP enables organizations to take a proactive approach to security, disrupting the lifecycle of an attack through prevention and real-time threat detection. With market-leading products, services, and innovative research, HP Enterprise Security enables organizations to integrate information correlation, application analysis, and network-level defense. Additional information about HP Enterprise Security can be found at hp.com/go/esp.

Table 1. Ordering guide

Part numbers	Description
C8Z36AAE	NSP Enhanced Software for NSP Ax160 AKB
C8Z37AAE	NSP Enhanced Software for NSP Ax160 Variant

Learn more at
hp.com/go/atalla

Sign up for updates
hp.com/go/getupdated



Share with colleagues



Rate this document

