



HPE Atalla Secure Configuration Assistant-3



HPE Secure Configuration Assistant-3 with Atalla Secure Keypad

HPE Security - Data Security is a trusted security vendor, with 35+ years of experience in data protection, security, and cryptographic performance. Hewlett Packard Enterprise payment and data security solutions meet the highest government and financial industry standards—including National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology (HITECH) for Economic and Clinical Health Act—protect sensitive data, and prevent fraud. HPE Secure Key Manager (ESKM) and Atalla Network Security Processor (NSP) provide robust security, high performance, and transparency while ensuring comprehensive, end-to-end network security.

Security and regulatory requirements dictate that at least two trusted individuals participate in all key entry operations and approve all security-related changes. All too often, this requirement results in carefully trained users standing in the data center, typing in cryptographic key components, and navigating elaborate, non-intuitive menu trees in an attempt to configure the HSM correctly. With more data centers moving to lights-out operation and strict control of physical access to the data center, such a manual and error-prone approach is unacceptable to most Hewlett Packard Enterprise customers.

The HPE Atalla Secure Configuration Assistant-3 (SCA-3) is a versatile tablet-based tool that implements the well-regarded SCA-2 on an easy-to-read tablet platform. The SCA-3 still enables security administrators to easily configure commands, define parameters, calculate cryptograms, and inject cryptographic keys into HPE Atalla Network Security Processors (NSPs) in a trusted manner. Now, an easy-to-use GUI with natural event and decision flow is even more convenient to navigate on wider tablet screens thereby improving security administrator user experience and productivity.

The Atalla SCA-3 can be directly or remotely connected to an Atalla NSP. Atalla SCA-3 security administrator smart cards perform individual user authentication and support multiple controls for Atalla NSP configuration. Atalla SCA-3 shareholder cards provide “L of M” quorum control for quickly replicating and restoring Atalla NSP configurations on new or restored NSP hardware.

Features and benefits

Features at a glance

- Tablet-based GUI saves time, enhances understanding, and facilitates entry accuracy.
- SCA-3 is fully backward compatible with SCA-2 based smart cards, as well as older Atalla Ax150 and Ax160 NSP devices.
- Custom Atalla SCA-3 smart cards support identity-based authentication, encrypted communication, and protected cryptographic key component storage.
- Atalla SCA-3 shareholder cards provide “L of M” quorum control for quick replication of configurations on both local and remote Atalla NSPs.
- Intuitive GUI interface enables security administrators to configure an Atalla NSP with minimal training.
- Atalla Secure Keypad (ASK) provides a tamper reactive device for security critical data entry such as key components.

The Atalla SCA-3 is based on a security-enhanced tablet, presenting an easy-to-use GUI that saves time and reduces risk of data entry errors. The Federal Information Processing Standard (FIPS) 140-2 level 3 evaluated Atalla SCA-3 smart card performs all cryptographic functions and stores security-relevant data (for example, key components) to provide customer data security.

Physical and logical security

The Atalla SCA-3 tablet is manufactured with tamper-evident seals. Logical security features include digital code signing to prevent unauthorized software execution. The ASK is tamper reactive and has tamper-evident seals. The custom Atalla SCA-3 smart card has been certified to FIPS 140-2 level 3 requirements. Together, the Atalla NSP and Atalla SCA-3 tablet are leaders in meeting industry needs for end-to-end protected key initialization.

Smart cards

Atalla SCA-3 smart cards are personalized to individual cardholders, such as security administrators, IT managers, or executives. An organization defines its own security policy by setting the minimum number of cardholders required to approve each type of security action. Atalla SCA-3 uses public key cryptography to establish an encrypted channel with the Atalla NSP. All subsequent communication between these devices is symmetrically encrypted. Security associations are formed between the SCA-3 smart cards and the Atalla NSP products they configure and manage.

Technical specifications

Physical SCA-3 tablet dimensions (with expansion jacket attached)	26.99 cm x 1.78 cm x 20.32 cm (10.63 in. x 0.7 in. x 8 in.); weight (with smart card reader): 1.07 kg (2.34 lb)
Physical security administrator smart card jewel kit dimension (with 3 cards)	8.89 cm x 0.94 cm x 6.02 cm (3.5 in. x 0.37 in. x 2.37 in.); weight: 37 grams (1.3 oz.)
Physical share smart card jewel kit dimension (2 kits, each with 5 cards)	8.89 cm x 1.88 cm x 6.02 cm (3.5 in. x 0.74 in. x 2.37 in.); weight: 90.9 grams (3.2 oz.)
Physical ASK dimensions	15.5 cm x 8.6 cm x 2.0 cm (6.1 in. x 3.4 in. x 0.8 in.) weight: 378 grams (13.3 oz.)
Processor	Intel® Atom processor (1.8 GHz BFM)
Graphics	Intel graphics media accelerator (533 MHz)
Memory	2 GB
Internal storage	32 GB
Standard features	Docking station with AC adapter power and charger, USB smart card reader, serial adapter cable, USB to serial interface cable, and serial null-modem cable.
Touch-screen display	10.1 in. diagonal, 1280 x 800 WXGA, LED backlit, red-green-blue (RGB) stripe, 0.1695 x 0.1695 pixel pitch
Input method	Touch-sensitive display
Easy access buttons	Power button, home button
Notification systems	Audible feedback
Power supply	10 watt AC adapter, internal 2 cell (25 Wh) polymer battery, and recharging supplied through AC adapter
Operating environment	Temperature: 0°C to 35°C (32°F to 95°F); relative humidity: 10% to 90%
Security	Tamper seals on the back of the device. All cryptographic operations occur within the smart cards.
Application upgrade	Application is user-upgradable with HPE Atalla security products supplied software

ORDERING INFORMATION

C8Z33AA	HPE Atalla Secure Configuration Assistant-3 (SCA-3) appliance
C8Z34AA	HPE Atalla SCA-3 Enh SW package of ten shareholder smart cards
C8Z35AA	HPE Atalla SCA-3 Enh SW package of three security administrator smart cards
AJ543A	HPE Atalla SCA-2 package of three security administrator smart cards
AJ542A	HPE Atalla SCA-2 package of ten shareholder smart cards

Important Note: C8Z34AA and C8Z35AA smart cards will **only work** with the Atalla Secure Configuration Assistant-3. They can be used to initialize and configure the Atalla Ax160 Network Security Processor models that are running Enhanced Software (version 2.0 or higher).

HPE ESP Global Services take a holistic approach to building and operating cyber security and response solutions and capabilities that support the cyber threat management and regulatory compliance needs of the world's largest enterprises. We use a combination of operational expertise—yours and ours—and proven methodologies to deliver fast, effective results and demonstrate ROI. Our proven, use-case driven solutions combine market-leading technology together with sustainable business and technical process executed by trained and organized people.

Learn more about HPE ESP Global Services at hpe.com/software/esp

Flexible management with security administrator and share smart cards

Atalla SCA-3 uses two types of custom smart cards to inject keys, enforce an organization's security policy, and manage Atalla NSP products.

Security administrator smart cards

- Enable users to initialize Atalla NSPs
- Set Atalla SCA-3 user policy
- Enable or disable Atalla NSP commands
- Calculate cryptogram

Share smart cards

- Provides flexibility in support of customer business needs
- Initialize an Atalla NSP to a predefined configuration set by security administrators only
- Can be distributed to local or remote operations staff
- Facilitate the operation of the Atalla NSP at remote locations or lights-out facilities
- Enables a subset of a security administrator sanctioned group (L of M) to bring up or restore an NSP at remote locations or lights-out facilities

Key strengths

The Atalla SCA-3 supports single-length Data Encryption Standards (DES), 2-key and 3-key triple DES, AES, public key cryptography, Atalla Key Block key management, and older variant key management.

About Hewlett Packard Enterprise Security

Hewlett Packard Enterprise is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HPE Security ArcSight, HPE Security Fortify, and HPE Security - Data Security the HPE Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at hpe.com/software/DataSecurity or hpe.com/software/esp



Sign up for updates

★ Rate this document