



The Atalla Secure Configuration Assistant-W (SCA-W) is a versatile tool that implements the well-regarded SCA-3 on an easy to manage application which runs on your company's managed Microsoft Windows computer.

## Product Highlights

The SCA-W enables security administrators to easily configure commands, define parameters, calculate cryptograms, and inject cryptographic keys into Atalla Hardware Security Modules (HSMs) in a trusted manner. Now, the easy-to-use GUI with natural event and decision flow is even more convenient to navigate on your own unrestricted screens thereby improving security administrator user experience and productivity.

The SCA-W is delivered on a FIPS 140-2 level 3 certified read-only USB storage media that conforms to best security practices, keeping it secure against corruptions and potential malware infections. The SCA-W package also includes the Atalla Secure Keypad (ASK) which works as a secure Key Loading Device (KLD). It implements the key loading and PIN related operations in a secure and compliant tamper responsive form factor.

A PC running the Atalla SCA-W can be directly or remotely connected to an Atalla HSM. Atalla Security Administrator smart cards perform individual user authentication and support multiple controls implementing M of N quorum control for Atalla HSM configuration. Atalla Backup Operator Smart Cards provide M of N quorum control for quickly replicating and restoring Atalla HSM configurations on new or restored HSM hardware.

The Atalla SCA-W along with Atalla Secure Keypad (ASK) implements remote management of Atalla HSMs in a unique one of its kind transactional model that allows Security Administrators to be geographically separate. Atalla HSMs along with the SCA-W are designed to be installed in a remote lights-out datacenter without any physical presence.



## Key Features

- Transaction based true remote management of Atalla HSMs
- Mandatory and role-based access control model
- Implements dual access and split knowledge
- Application based GUI saves time, enhances understanding, and facilitates entry accuracy.
- Proprietary Atalla smart cards support identity-based authentication, encrypted communication, and protected cryptographic key component storage.
- Atalla SCA-3 Backup Operator Smart Cards provide "L of M" quorum control for quick replication of configurations on both local and remote Atalla HSMs.
- Intuitive GUI interface enables security administrators to configure an Atalla HSM with minimal training.
- ASK implements an active tamper device for security critical data entry such as key components.
- FIPS 140-2 Level 3 compliant delivery and storage

## Physical and Logical Security

The Atalla SCA-W application is delivered on a FIPS 140-2 Level 3 certified read-only media, digitally signed to maintain integrity and security. Logical security features include digital code signing to prevent unauthorized software execution. The ASK is tamper reactive and has tamper-evident seals. Together, the Atalla HSM and Atalla SCA-W are leaders in meeting industry needs for end-to-end protected HSM Initialization and remote management with key loading.

## Smart Cards

Atalla 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-W uses public key cryptography to establish an encrypted channel with the Atalla HSM. All subsequent communication between these devices is encrypted. A cryptographic bond is formed between the smart cards and the Atalla HSM products they configure and manage.

## Cryptography Support

The Atalla SCA-W supports AES 128, 256-bit keys along with legacy single-length DES, 2-key and 3-key triple DES, public key cryptography Atalla Key Block key management, and legacy variant key management without storing any cryptographic material locally.



## Functionalities

### Flexible Management with Security Administrator and Backup Operator Cards

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

### Security Administrator Smart Cards

- Create Backup Operator Group
- Create and Store MFK Components
- Enable users to initialize Atalla HSMs
- Set Atalla SCA-W user policy
- Enable or disable Atalla HSM commands
- Calculate cryptogram

### Backup Operator Cards

- Provides flexibility in support of customer business needs
- Initialize an Atalla HSM to a predefined configuration set by security administrators only
- Can be distributed to local or remote operations staff
- Facilitate the operation of the Atalla HSM 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 HSM at remote locations or lights-out facilities



## Technical Specifications

### Physical Dimensions

#### USB Drive

- H x W x D:  
0.37 x 3.5 x 1 inches  
(0.94 x 8.89 x 25.4)
- Weight:  
1.3 oz (37.0 g)

#### Administrator Smart Card Jewel Kit with 3 Cards:

- H x W x D:  
0.37 x 3.5 x 2.37 inches  
(0.94 x 8.89 x 6.02 cm)
- Weight:  
1.3 oz (37.0 g)

#### Backup Operator Card 2 Jewel Kits, each with 5 Cards

- H x W x D:  
0.74 x 3.5 x 2.37 inches  
(1.88 x 8.89 x 6.02 cm)
- Weight:  
3.2 oz (90.9 g)

#### Atalla Secure Keypad (ASK)



- H x W x D:  
0.8 x 6.1 x 3.4 inches  
(2.0 x 15.5 x 8.6 cm)
- Weight:  
13.3 oz (378.0 g)

### ASK 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 ASK.  
All cryptographic operations occur within the smart cards FIPS 140-2 Level 3 certified SCA-W media.



### Application upgrade

- Application is user-upgradable with Atalla supplied software



### Operating System Compatibility

- Microsoft Windows 7 and Microsoft Windows 10





## EMEA

### Utimaco IS GmbH

📍 Germanusstraße 4  
52080 Aachen,  
Germany

☎ +49 241 1696 200

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

## Americas

### Utimaco Inc.

📍 900 E Hamilton Ave.,  
Suite 400  
Campbell, CA 95008,  
USA

☎ +1 844 UTIMACO

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

## APAC

### Utimaco IS Pte Limited

📍 50 Raffles Place,  
Level 19,  
Singapore Land Tower,  
Singapore 048623

☎ +65 6631 2758

✉ [hsm@utimaco.com](mailto:hsm@utimaco.com)

For more information about Utimaco HSM products, please visit:

[hsm.utimaco.com](https://hsm.utimaco.com)