Security Policy
A-Key

Version 1.0.0

Authenex, Inc.

February 3, 2006

TABLE OF CONTENTS

1. Module Overview

The Authenex A-Key is a multi-chip standalone cryptographic module, encased in a hard, opaque potting material (HW P/N AKEY2T0-01, Version 2.0.0; FW Version 3.6.0). This device is designed primarily to perform identity-based authentication and cryptographic data processing. The device provides a USB interface for data input, data output, control input, and status output. The cryptographic boundary is defined as the outer perimeter of the A-Key enclosure. The picture below depicts the USB interface, as well as the cryptographic boundary.

Figure 1 – Image of the Cryptographic Module

2. Security Level

The Authenex A-Key cryptographic module meets the overall security requirements for a FIPS 140-2 Level 3 cryptographic module.

Table 1 - Module Security Level Specification

FIPS 140-2 Security Requirement Areas	Level
1. Cryptographic Module Specification	3
2. Module Ports and Interfaces	3
3. Roles, Services and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self-Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved Mode of Operation

The Authenex A-Key only supports a FIPS mode of operation; therefore, the cryptographic module can only operate in an Approved mode. The "Show Status" service may be invoked to view the firmware version of the module, which will allow the operator to identify FIPS Approved versions. The cryptographic module only supports FIPS Approved and allowable algorithms, as follows:

- RSA Sign/Verify with 1024-bit and 2048-bit keys for digital signature generation and verification
- DRNG, implemented according to ANSI X9.31, for the generation of RSA keys
- SHA-1, for hashing
- AES with 128 and 256 bit keys, for encryption
- RSA Encrypt/Decrypt with 1024-bit and 2048-bit keys (key wrapping, key establishment methodology provides 80 to 112 bits of encryption strength)

Non-FIPS Mode of Operation

The Authenex A-Key does not support a non-FIPS mode of operation.

4. Ports and Interfaces

The Authenex A-Key supports data input, data output, control input, and status output interfaces. In addition, the module supports a power interface, through which it receives power from an external source. The following is a description of the physical ports provided by the A-Key, and the logical interfaces that are associated with them:

USB port: data input, data output, status output, control input, and power input

5. Identification and Authentication Policy

Assumption of Roles

The cryptographic module shall support two distinct operator identities: User and Cryptographic-Officer. The cryptographic module shall enforce the separation of roles using identity based operator authentication. The operator must prove knowledge of a shared secret and enter a password to log-in; passwords are encrypted by the Authenex AES Key upon entry. The password is an alphanumeric string of five to 63 characters randomly chosen from a set of 94 printable and human readable characters. Upon correct authentication, the role is selected based on the authentication data of the operator.

If the User fails to authenticate to the module after 50 consecutive attempts, the module will zeroize all CSPs except the Authenex AES Key. At the end of a session, the operator must log-out. If the CO fails to authenticate to the module after 10 consecutive attempts, the module will zeroize all contents of the internal flash memory and all CSP locations in non-volatile memory.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Knowledge of a 128-bit shared secret and password
Cryptographic-Officer	Identity-based operator authentication	Knowledge of a 128-bit shared secret and password

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and password	The probability that a random attempt will succeed or a false acceptance will occur is 1/[(94^63) x (2^128)], which is less than 1/1,000,000. The probability of successfully authenticating to the User within one minute through random attempts is 50/[(94^63) x (2^128)], which is less than 1/100,000. The probability of successfully authenticating to the CO within one minute through random attempts is 10/[(94^63) x (2^128)], which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide all of the normal operational services.	• Signature Generation: Generate a digital signature using one of the RSA private keys stored within the module. • Signature Verification: Verify a digital signature using one of the RSA public keys stored within the module. • Key Generation: Generate an RSA key pair in accordance with ANSI X9.31. • Key Unwrap: RSA decrypt a key that has been received. • Key Wrap: RSA encrypt a key for key transport.

	• Import RSA Key Pair: Import an AES encrypted RSA key pair from the Host. • Export RSA Public Key: Export a RSA public key to the Host. • Data Storage: Store user data in internal flash. Data is entered into the module AES encrypted. • AES Encrypt/Decrypt: Encrypt/decrypt data using one of the AES keys stored within the module. • Import AES Keys: Import an encrypted AES key from the Host; all keys are imported encrypted by the Authenex AES Key. • Setup User Password: Update the User password (password is entered in an encrypted form). • Zeroize CSPs: Zeroize all CSPs contained within the module in volatile and non-volatile memory.
Cryptographic-Officer: This role shall provide only the service necessary to decommission a device.	• Setup CO Password: Update the CO password (password is entered in an encrypted form). • Reset Token: Zeroizes all CSPs, with the exception of the Authenex AES Key and AES data processing keys. • Zeroize FLASH: Zeroizes all of FLASH memory.

Unauthenticated Services:

The A-Key supports the following unauthenticated services:

- Show status: This service provides the current status of the cryptographic module.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2.
- Log-out: This service logs out the current operator.
- Log-in: This service allows an operator to authenticate to the A-Key.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- **RSA Private Keys**: These are RSA keys used to create digital signatures or unwrap keys.
- **AES Data Processing Keys**: These are AES keys used to encrypt/decrypt data.

- **Authenex AES Key**: This is an AES key used to protect CSPs during transport, and may also be used to protect data.
- **User Password**: This CSP is used to authenticate the User identity.
- **CO Password**: This CSP is used to authenticate the CO identity.
- **RNG Seed Key**: This CSP is used to seed the internal ANSI X9.31 RNG.

Definition of Public Keys

The following are the public keys contained in the module:

- **RSA Public Keys**: These are used to verify digital signatures.

Definition of CSPs; Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Generate**: This operation generates a random value that will be used to create a key pair.
- **Use**: This operation accesses the CSP for usage.
- **Modify**: This operation modifies the CSP.
- **Destroy**: This operation actively erases the CSP.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
	X	Signature Generation	Use RSA private keys
	X	Signature Verification	Use RSA public keys
	X	Key Generation	Generate RSA private and public keys
	X	Key Unwrap	Use RSA private keys
	X	Key Wrap	Use RSA public keys
	X	Import RSA Key Pair	Use Authenex AES Key
	X	Export RSA Public Key	N/A
	X	Data Storage	Use Authenex AES Key
	X	AES Encrypt/Decrypt	Use AES data processing keys
	X	Import AES Keys	Use Authenex AES Key
	X	Setup User Password	Modify User password
	X	Zeroize CSPs	Destroy all CSPs, except Authenex AES Key
X		Setup CO Password	Modify CO password
X		Reset Token	Destroy RSA private keys, destroy User and CO passwords
X		Zeroize FLASH	Destroy all CSPs
		Show Status	None
		Self-Tests	None
		Log-out	None
		Log-in	Use User password, CO password

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable, because the Authenex A-key cryptographic module does not contain a modifiable operational environment. The module does not support the external loading of code.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules imposed upon the cryptographic module to ensure that it meets FIPS 140-2 Level 3 security requirements.

1. The cryptographic module shall provide two distinct operator roles: The User role and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. If the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall not support multiple concurrent operators.
5. The cryptographic module shall not support a maintenance role or a bypass capability.
6. The cryptographic module shall not support manual key entry.
7. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests:
        1. Cryptographic algorithm tests:
            a. AES Known Answer Test
            b. SHA-1 Known Answer Test
            c. RSA Known Answer Test (Sign/Verify and Encrypt/Decrypt)
            d. RNG Known Answer Test
        2. Software Integrity Test
            a. 16-bit CRC
        3. Critical Functions Tests: N/A
    B. Conditional Self-Tests:
        1. RSA Pairwise Consistency Test (Sign/Verify and Encrypt/Decrypt)
        2. Continuous RNG Test
8. The operator shall be able to command the module to perform the power up self-tests by power cycling the module.
9. Data output shall be inhibited during self-tests, zeroization, and error states.
10. Status information shall not contain CSPs or sensitive data that, if misused, could lead to a compromise of the module.

9. Physical Security Policy

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production grade components.
- Multiple chip circuitry enclosure encapsulated in a hard, opaque potting material; attempts at removal or penetration of this material leave significant tamper evidence.

Operator Required Actions

The operator is required to periodically inspect the module for evidence of tamper.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard potting material encapsulation	Once a month	Inspect the module's enclosure for evidence of a tamper attempt.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

11. Definitions and Acronyms

AES Advanced Encryption Standard

CO Crypto-Officer

CSP Critical Security Parameter

RNG Random Number Generator

RSA Rivest Shamir Adelman

SHA Secure Hash Algorithm

USB Universal Serial Bus