Cylink ATM Encryptor

FIPS 140-1 Security Policy

ECO, Date, and Revision History
Rev A, DO-025, 6/25/01, jvv
Rev B, DO-030, 1/20/02, RGB
Rev C, DO-032, 09/27/02, JVV

Contact: Rodney Bame				
Checked:	Released:			
Filename: New ATM Security Policy.doc				
Title:	**Cylink ATM Encryptor FIPS 140-1 Security Policy**			
.	Date: 09/26/02	Document Number: **005-076-003**	Rev: **C**	Sheet: **1 of 1**

CYLINK® Securing e-business

Table Of Contents

1 Introduction

This document describes the security policy of the Cylink ATM Encryptor as required and specified in the NIST FIPS-140-1 standard.
Under the standard, the ATM Encryptor system qualifies as a multi-chip stand-alone system and satisfies the FIPS 140-1 level 2 security requirements. The security policy includes:

- a list of all roles and cryptographic services provided by the system
- a list of all security relevant data items in the module
- a specification of user access in each of the roles to security relevant data items
- a description of physical security utilized by the system
- a list of security rules (physical or otherwise) imposed by the developer
- user/maintenance procedures that must be followed to maintain an ATM Encryptor system's FIPS 140-1 compliance at a particular security level
- for cases where the module can be operated in a non-FIPS approved mode, the conditions that must be maintained for FIPS 140-1 compliant operation

This document contains no known Cylink confidential material, and may be shared with users requiring FIPS 140-1 compliance.

2 Abbreviations & Definitions

ACL Access Control List, contains rules identifying called parties & calling parties and the type of connection allowed (Secure, Unsecure or None)

ATM Asynchronous Transfer Mode

CAM Certificate Authentication Message

CA Certificate Authority

CBC The cipher-block chaining mode of DES, as defined in FIPS PUB 81

CEM Certificate Exchange Message

Channel a single logical data connection/session established through a data network.

Crypto Certificate
a digital electronic certificate containing the public key of an ATM Encryptor. The Crypto certificate is created during the initialization process.

Crypto Passphrase Key
a 16 byte key created during initialization from the crypto passphrase string. It is used to create an authentication signature for the Crypto Certificate and to authenticate Crypto Certificates received from a far-end ATM Encryptor.

DES Data Encryption Standard, as defined in FIPS PUB 46-3.

ECB Electronic Code Book mode of DES

Manager Passphrase Key
a 56 bit key created during initialization from the manager passphrase string. It is used to provide authentication of an operator to enter the crypto officer role. In addition, it is used to encrypt session keys and SKUNKs stored on the internal disk. Associated with the key is a 64 bit initialization vector used in cases where the passphrase key is used with DES CBC encryption and a seed is required.

Path a collection of channels established through a data network that is treated as a single logical group.

Private network port
the ATM network port of the ATM Encryptor attached to the private, trusted network.

Public network port
the ATM network port of the ATM Encryptor attached to the public, untrusted network.

PVC Permanent Virtual Channel, a channel set up in an ATM network that once established remains in place until explicitly disabled.

PVP Permanent Virtual Path, a collection of channels set up in an ATM network that once established remains in place until explicitly disabled.

Session Key
a DES key used to encrypt/decrypt the ATM cell payloads of a designated channel.

SKC cell Session Key Changeover cell – the ATM cell used to cause the active and backup session keys to be interchanged for the channel designated in the header of the cell.

SKE cell Session Key Exchange cell – the ATM cell used to transmit an encrypted session key to a far-end system.

SKUNK Session Key Update eNcryption Key – A key, generated when a channel is established, that is distributed to a far-end ATM Encryptor for the purpose of encrypting session keys created by a key update event.

SVC Switched Virtual Connection, a connection set up in an ATM network that remains in place only as long as it is needed. It is automatically disabled following its use.

Software Integrity Signature
a digest computed over all executable files in a Cylink software release and encrypted with the Cylink Manufacturing CA private key. It is used on power up to authenticate the software on an ATM Encryptor.

3 References

Cylink Document # 005-076-002, Cylink ATM Encryptor FIPS 140-1 Supporting Documentation
FIPS 140-1 Security Requirements for Cryptographic Modules
Netscape Security Module 1 (FIPS DSA cert #14) - for performing the firmware integrity test

4 Roles and Services

4.1 Roles

The ATM Encryptor supports two roles:

1. A **Crypto Officer** role in which the system is initialized/reinitialized or managed. The Crypto Officer performs Initialization through which system parameters and management control are configured. During Initialization the Crypto Officer sets the Manager and Crypto passphrases. Access to Initialization is authenticated through secret password entry. Management commands may be entered to configure the ATM Encryptor system and enable secure channels or paths between the public and private network ports, as well as specify key values. The Crypto Officer specifically establishes PVCs and PVPs. SVCs are configured by enabling signaling support within the system and establishing an Access Control List (ACL). The ACL is the mechanism for specifying the rules for handling SVC requests.

   The Crypto Officer is authenticated by means of the system password and manager passphrase. Only a Crypto Officer has access to the user interface.

2. A **User** role in which data can be presented to the ATM Encryptor system on the private network port for encryption. The encrypted data is transmitted out of the public network port if it is in a channel that has been enabled. All data traffic being received on the private port is assumed to be from authenticated private users since, by virtue of their connection to the local private network, they are operating inside the secure, trusted local network. In the User role, only data encryption services are provided. No facilities are available in the User role to establish permanent channels, specify key values to be used in encryption, or otherwise control the operation of the ATM Encryptor system. If the user requests a switched connection, and the ACL allows the requested connection, the connection is enabled. In the User role, data can also be presented to the ATM Encryptor System on the public network port for decryption. If the data is in an enabled channel, the decrypted data is transmitted out of the private network port. Untrusted users can submit data to the ATM Encryptor system for decryption; however, only data that has been submitted on a channel previously enabled or allowed by the Crypto Officer will be processed.

   Since data encryption services are the only services available to the User Role, and since the encryptor is connected to the private network within the physical confines of the trusted environment, there is no direct authentication of the user role. When data is presented for encryption on the private port, it must be presented to a previously enabled channel. If it is not, the “request” is effectively blocked. The “request” for data encryption services is considered authorized since it comes from the trusted environment. Similarly, when data is presented for decryption on the public port, it must presented on an enabled channel. Any data presented to a disabled channel is blocked. Data presented to an enabled channel must be encrypted per the established connection to be authorized.

4.2 Security Relevant Data Items

The following table identifies the Security Relevant Data Items (SRDIs), for the ATM Encryptor, along with their general function. The data items are then mapped to the relevant roles and services in the following section. The Services table shows how the data items are used within the overall system.

Security Relevant Data Item	Instances / Definition	Purpose
Initialization Login Initialization login name Initialization password string Initialization password digest	Login required to initialize the crypto	Initialization
Manager Login Manager login name Manager password string Manager password digest	Login required to manage the crypto	Initialization Crypto officer commands
Crypto Passphrase Crypto passphrase Crypto passphrase key	Security parameter for crypto to crypto identification	Initialization Crypto officer commands
Manager Passphrase Manager passphrase Manager passphrase key	Security parameter for Crypto Officer identification	Initialization Crypto officer commands Key backup and restoration
Crypto Public/Private Key Pair	Crypto Identification	Initialization Key backup and restoration
Session Keys Session encryption key Session decryption key	Encrypt / Decrypt keys for secure communications	Encryption/Decryption
KK (One per connection)	System generated shared secret for subsequent SVC communications	Encryption/Decryption
SKUNK	Session Key Update eNcryption Key used to encrypt new Session Keys for distribution	Crypto officer commands Key backup and restoration
Encryption Configuration	Key length and cipher mode	Encryption/Decryption Crypto officer commands
Update Policy	Key update policy	Encryption/Decryption Crypto officer commands
Celotek Public Key	Validates the Software Integrity Signature	Test Functions
Cylink Manufacturing CA Public Key CA Public Key CA Public Key Hash value	Validates the crypto during initialization	Initialization Upgrade
Software Integrity Signature	Internal integrity signature Upgrade file integrity signature	Test Functions Upgrade

4.3 Services

The ATM Encryptor provides encryption services for users attached to the private network port and decryption services for users attached to the public network port. Lower level services are also provided supporting the basic functionality seen by the end user. The following table outlines the services provided by the ATM Encryptor, the roles in which the services are available, the security-relevant objects created or used in the performance of the service, and the form of access given to the objects in the specified role. The following forms of access are available:

- **Use** – The data item is used during the performance of the service. "Use" does not imply that the data item is observable by the operator.
- **Create** – The data item is created as part of performing the service. Creation of a data item can be either "direct" or "indirect". Direct creation allows the operator to directly change the setting of the data item to a desired value. Indirect creation allows the operator to simply control whether or not a data item is created, not what its value will be.
- **Transmit** – the data item is transmitted out of the ATM Encryptor on one of the network ports.
- **Receive** – The data item is received from outside the ATM Encryptor on one of the network ports.
- **Keyboard Entry** – The data item is entered into the system through a keyboard attached to the serial port or through a remote host connection.

- **Terminal Display** – The data item is output to a display attached to the serial port or through a remote host connection.
- **Modify** – The data item is modified in performing the service.

Security data items received/transmitted by the ATM Encryptor in encrypted form are *italicized*. Security data items received/transmitted by the ATM Encryptor that are protected from modification or substitution with a signature are identified in **bold**.

Cylink document # 005-076-002 should be consulted for additional detail about each of the security data items referred to in the following table. Only security relevant services and items are discussed in the following table.

Function/Service	Roles	Security Relevant Data Items	Access
Test functions			
Self-test (algorithm test, critical function test, power-up and conditional tests, software authentication).	Command initiated: Crypto officer role Power on initiated: Crypto officer role	Celotek Public Key Software Integrity Signature	Use Use
Encryption/Decryption			
ATM cell encryption	User role	ATM cells presented on the input private network port for encryption Session encryption key *encrypted ATM cell output on the public network port*	Receive/Use Use Indirect Creation/Transmit
ATM cell decryption	User role	*ATM cells, containing encrypted data payload, are presented at the input public network port* Session decryption key decrypted ATM cell output on the private network port	Receive/Use Use Indirect Creation/Transmit
Key Update			
Updated session key generation	Crypto officer role	Update key specified by crypto officer or randomly generated update key created by the system	Direct creation or Indirect creation
Updated session key transmission	Crypto officer role	Updated key and SKUNK of the channel to be updated *SKE cell, containing the encrypted updated key, output on the public network port* SKC cell to cause key changeover	Use Indirect creation/Transmit Indirect creation/Transmit
Updated session key reception	User role	*SKE cell received on public network port* SKUNK for the channel designated in the SKE cell New session decryption key placed in backup session key bank of the channel designated in the SKE cell SKC cell received causing key changeover	Receive and Use Use Indirect creation Receive and Use
Initialization			
Initialization Login	Crypto officer role	Terminal entry of the initialization login name Initialization password string Initialization password digest	Keyboard entry Keyboard entry Use

Creation of manager password digest	Crypto officer role	Terminal entry of the new Manager password string Manager password digest	Keyboard entry Indirect creation
Creation of initialization password digest	Crypto officer role	Terminal entry of the new Initialization password string Initialization password digest	Keyboard entry Indirect creation
Creation of crypto passphrase key	Crypto officer role	Terminal entry of the new crypto passphrase Crypto passphrase key	Keyboard entry Indirect creation
Creation of manager passphrase key	Crypto officer role	Terminal entry of the new manager passphrase Manager passphrase key and Initialization vector	Keyboard entry Indirect creation
Creation of public/private key pair	Crypto officer role	Crypto certificate containing public key Private key	Indirect creation Indirect creation
Key backup	Crypto officer role	Private key, Public key Manager passphrase key and initialization vector *Encrypted keys stored on disk*	Use Use Indirect creation
Key backup and restoration			
Session, updated session, SKUNK or KK key backup	Crypto officer role	New session and updated session keys, SKUNKs and KKs Manager passphrase key and initialization vector *Encrypted session encryption key*	Use Use Indirect creation
Key restoration	Crypto officer role	*Encrypted backup file containing, session and updated session keys, SKUNKs* and KKs crypto private key Manager passphrase key and initialization vector Session keys decrypted and placed in key memory	Use Use Use Indirect creation
Crypto officer commands			
Manager login	Crypto officer role	Terminal entry of the Manager login name, password string, and passphrase. Manager password digest Manager passphrase key	Keyboard entry Use Use
Specification of current key length and cipher mode	Crypto officer role	Terminal entry of the desired key length and/or cipher mode Internal key length and cipher mode state set to specified values	Keyboard entry Direct modification
Specification of current key update policy	Crypto officer role	Terminal entry of the desired key update policy Update policy state set to the specified setting	Keyboard entry Direct modification
Establishment of a permanent channel/path using manual keys	Crypto officer role	Terminal entry of the VPI,VCI and desired key value Session encryption and decryption keys	Keyboard entry Direct creation
Establishment of a permanent	Crypto officer role	Keyboard entry of desired unsecure	Keyboard entry

unsecure bypass channel/path		VPI/VCI Identity Session Key	 Direct creation
Establishment of a permanent channel/path using auto key exchange.	Crypto officer role	Keyboard entry of desired secure VPI/VCI New session encryption and decryption keys, SKUNK and KK generated	Keyboard entry Indirect creation
Disable a channel/path	Crypto officer role	Keyboard entry of VPI, VCI of channel/path to disable Session key SKUNK	Keyboard entry Modify (zeroize) Modify (zeroize)
Update of crypto passphrase key	Crypto officer role	Terminal entry of the current & new crypto passphrases Crypto passphrase key	Keyboard entry Indirect creation
Update of manager passphrase	Crypto officer role	Terminal entry of the new manager passphrase Manager passphrase key	Keyboard entry Indirect creation
Creation of SKUNK	Crypto officer role	System generated SKUNK	Indirect creation
Creation of KK	Crypto officer role	First automatic key exchange on an SVC between a pair of ATM Encryptors. System generated KK	Indirect creation
Creation and transmission of CEM message	Crypto officer role	Crypto certificate Nonce **CEM message output on system public network port**	Use Indirect creation/Use Indirect creation/Transmit
Reception/Verification of CEM message	User role	**signed crypto certificate containing the far-end public key and** nonce Crypto passphrase key	Receive/Use Use
Creation and transmission of CAM message	Crypto officer role	Far-end nonce Far-end public key Session encryption key SKUNK **signed CAM message** containing encrypted *nonce, session key, and SKUNK* output on public network port	Use Use Use Use Indirect creation/Transmit
Reception/verification of CAM message	User role	Far-end public key Crypto private key *session decryption key* *Far-end SKUNK*	Use Use Receive/install Receive/install
Show status	Crypto officer role	Terminal output displaying security status of each established channel/path. Terminal output also indicates error status	Terminal Display
Show configuration	Crypto officer role	Terminal output displaying current encryption configuration and update policy	Terminal Display
Display audit log	Crypto officer role	Terminal output displaying significant events recorded by the system	Terminal Display
Upgrade			
Software upgrade	Crypto officer	**Upgrade file received through Ethernet port** Software Integrity signature from the	Receive/Use Receive/Use

		upgrade file Cylink Manufacturing CA public key Software integrity signature	 Use Use
Verification of Cylink Manufacturing CA Public Key	Crypto officer	Cylink Manufacturing CA Public Key Cylink Manufacturing CA Public Key Hash value	Use Use

5 Physical Security Policy

The ATM Encryptor has been designed by Cylink to satisfy the Level 2 physical requirements of the FIPS 140-1 standard. The system is housed in an opaque, aluminum box with external connections provided for the private and public data network ports, as well as the console display/keyboard, Ethernet port, and status LEDs. The internal assemblies are attached to the chassis using screws. The chassis is surrounded by an external shell which is also attached using screws. A seal is provided over one of the screws attaching the shell to the chassis to provide evidence of tampering.

The individual responsible for maintaining the ATM Encryptor should periodically check the tamper evident seal to verify that the unit has not been opened. If the seal is broken, the unit is no longer FIPS 140-1 compliant. The tampered unit should be returned to Cylink for re-certification (following the required return procedures). Other units with which it exchanged keys and which have no evidence of tampering should be re-initialized. In re-initializing, the Initialization and Manager passwords should be changed, the crypto passphrase should be changed, and any manual key channels/paths should be re-established using new key values.

6 Initialization Policy

When an ATM Encryptor is shipped from the factory to a customer, encryption/decryption services between the public and private network ports are disabled until the system is initialized and channels between the two ports are established. In addition, access to the normal management functions (the manager login) is disabled until Initialization is completed. Finally, Initialization can only be performed through the serial port of the unit, restricting Initialization access to only those individuals with access to the system's console port.

During Initialization, the crypto officer must establish the passwords associated with the Initialization and Manager logins, the Manager passphrase, and the Crypto passphrase. During the Initialization process, the crypto officer can also enable the system to be managed from a remote host not attached to the local IP sub-net. To enable remote management, the IP address of a gateway and a remote management station must be specified as part of initialization. During a remote management session, IP packets will be sent to the specified gateway and routed to the designated remote host. If the gateway and remote host IP addresses are not specified during initialization, management of the unit can only be performed through a host attached to the same IP sub-net as the ATM Encryptor. Additionally, during Initialization Ethernet access to the ATM Encryptor can be disabled, restricting access to the crypto officer role to only those individuals with access to the system's console port.

To strictly maintain FIPS 140-1 compliance, the individual with responsibility for initialization of an ATM Encryptor should periodically assume the crypto officer role and login to the Initialization login to ensure that the Initialization password has not been changed.

7 Management Policy

The crypto officer of the ATM Encryptor is responsible for establishing connections between ATM Encryptors comprising a larger virtual private network. Access to the manager login is controlled by the entry of a password and passphrase, established during Initialization of the unit.

To ensure FIPS 140-1 compliance, the crypto officer must only utilize the ECB encryption mode for secure channels. Counter mode encryption is a DES-based stream cipher established by the ATM Forum (see ATM Forum document AF-SEC-0100.01). It is not recognized by the FIPS 140-1 standard as a compliant mode of operation.

To operate the ATM Encryptor in **FIPS mode**, the crypto officer uses the **`configure`** command to confirm, or set, the default Cipher Mode to **ECB**. Channels and paths are then enabled using the approved ECB encryption mode. Changing the default Cither Mode to **Counter Mode**, places the ATM Encryptor in a **non-FIPS mode**.

If a unit is to be returned to the factory for any reason, the unit should be zeroized prior to shipment.

As an added precaution, at the conclusion of a Manager session, the crypto officer should be sure to log out of the unit. This will prevent an unauthorized user from creating new secure connections to a private network or changing the keys associated with already established channels/paths. To ensure that sessions are logged out, an automatic time-out capability is provided. This automatically logs off a management session after a specified time period during which no commands have been entered. After logging out, the Crypto officer should also ensure that the display used during the session is cleared. In many windowing environments a large session buffer, capturing all terminal input and output created in a window, is maintained. Unauthorized individuals with access to the window buffer are capable of recreating a complete session, replete with key values if manual channels/paths are established.

In most cases, once an ATM Encryptor is deployed and data network connections established, no access to the system is required to maintain operation. Despite the minimal amount of activity required of the crypto officer, it is recommended that the crypto officer periodically check the status of all ATM Encryptors. The checks involved include:

- Checking the tamper evident seal on the unit to verify that it is intact.
- Checking the status LEDs to ensure that the unit is operating correctly.
- Logging on as the Manager to ensure that the Manager password and passphrase have not been modified.
- Checking the audit log for possible attempts to breach the system's security. Audit log checks would include:
  - ✓ Verifying that Manager access was not attempted with an incorrect password or passphrase.
  - ✓ Verifying that the private and public network ports were not disconnected inappropriately.
  - ✓ Checking the command log to ensure that connections through the CellCase unit were not added or changed.
  - ✓ Looking for instances where key updates were attempted and failed. Failed key updates could indicate an attack by an untrusted party on the public network port connection.

Finally, consideration should be given to the security required of the communication link between the crypto officer and the ATM Encryptor. The FIPS 140-1 standard does not provide guidance in specifying the way in which communications with the ATM Encryptor should be handled. As described in the Manager's manual (ATM Encryptor User's Guide, Cylink document: 82321-00N), the ATM Encryptor can be managed through the serial port, a local Ethernet connection or a remote Ethernet connection; each form of communication being successively less secure. In connecting an ATM Encryptor to a local network, it should be kept in mind that all Ethernet based communication between the crypto officer and the system is plaintext. As a result, all logins, passwords, commands etc., are passed to the system across the network in plaintext form. An unauthorized individual could eavesdrop on a session connection and obtain the passwords to the system. Obviously, managing an ATM Encryptor through the serial port is the most secure since serial port connections are local and are made directly between an ATM Encryptor and a terminal (display/keyboard). Managing an ATM Encryptor over a local Ethernet connection ensures that access to the data traffic traversing the link is limited to a select group of more trusted users. Managing an ATM Encryptor through a remote host connected via a gateway is the least secure method, making the management connection open to potentially untrusted users with access to the intervening data network fabric.

Appendix A. Cryptographic Algorithm Support

The following list identifies all cryptographic algorithms employed in the ATM Encryptor.

Encrypt / Decrypt:

- 3-DES-ECB
- 2-DES-ECB
- DES-ECB
- 3-DES-CM
- 2-DES-CM
- DES-CM
- DES-CBC

Digests / Key Exchange:

- SHA-1
- DH-1024

Additional Modules:

- Embodied in the firmware, the encryptor employs Netscape Security Module 1 (FIPS DSA cert #14) for performing the firmware integrity test
- Digital Signature Standard (FIPS 186)