CellCase FIPS 140-1 Security Policy

ECO, Date, and Revision History	Contact: Pervaze Akhtar		CELOTEK
Rev A Released [date], R-98-[ ], [Initials]	Checked:	Released: Apr. 19, 2000	
	Filename: RevisedSecurity Policy.doc		
	Title: **CellCase FIPS-140 Security Policy**		

Date:	Document Number:	Rev:	Sheet:
Aug. 21, 2000		**D**	**1 of** 9

Table Of Contents

1 Introduction

This document describes the security policy of the Celotek CellCase as required and specified in the NIST FIPS-140-1 standard. Under the standard, the CellCase 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 a CellCase 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 Celotek confidential material, and may be shared with users requiring FIPS 140-1 compliance.

2 Abbreviations & Definitions

ATM Asynchronous Transfer Mode

CAM Certificate Authentication Message

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 a CellCase system. The Crypto certificate is created during the initialization process.

Crypto Passphrase Key
a 20 byte key created during initialization from the crypto passphrase string (by performing an SHA-1 hash on the passphrase string) and used to create an authentication signature for the Crypto Certificate and to authenticate Crypto Certificates received from a far-end CellCase system.

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

ECB Electronic Code Book

Manager ID Key
a 56 bit DES key created during initialization from randomly generated bytes and used to encrypt session keys and SKUNKs stored on the internal disk.

Manager Passphrase Key
a 20 byte key created during initialization from the manager passphrase string (by performing an SHA-1 hash on the passphrase string) and used to provide authentication of an operator to enter the crypto officer role.

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 CellCase system attached to the private, trusted network.

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

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 update key to a far-end system.

SKUNK Session Key Update eNcryption Key – A key, generated when a channel is established, that is exchanged with a far-end CellCase system for the purpose of encrypting session keys created during an update event.

Software Integrity Signature

a digest computed over all executable files in a Celotek software release and encrypted with Celotek's private key. It is used on power up to authenticate the validated software resident on a CellCase system.

3 Roles and Services

The CellCase system supports two roles:

- A User role in which data can be presented to the CellCase system on the private network port for encryption. The encrypted data is transmitted out of the public network port. In this user role, only data encryption services are provided. No facilities are available to establish new channels, specify key values to be used in encryption, or otherwise control the operation of the CellCase system. In the user role data can also be presented to the CellCase System on the public network port for decryption. The decrypted data is transmitted out of the private network port. The user is also able to submit key exchange requests to the CellCase system. The session key exchange requests are authenticated by the CellCase system prior to use of the key values for decryption. If not received from a trusted CellCase system, the key exchange will be aborted. Finally, a user can submit SKE and SKC cells to perform a session key update. SKE and SKC cells are not authenticated by the CellCase system. Without the knowledge of the SKUNK, an unauthenticated user submitting an SKE cell is incapable of knowing what key value will actually be installed.
- A Crypto Officer role in which commands may be entered to configure the CellCase system and enable secure channels or paths between the public and private network ports, as well as specify key values. Access to the crypto officer role is controlled using a secret password and passphrase login procedure. The crypto officer also performs initialization through which system parameters and access control are configured. During initialization the crypto officer can set the Manager and crypto passphrases, controlling access to the system. Access to initialization is authenticated through secret password entry.

The CellCase System 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 CellCase system, 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 CellCase system on one of the network ports.
- Receive – The data item is received from outside the CellCase system.
- 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 CellCase system in encrypted form are *italicized*. Security data items received/transmitted by the CellCase system that are protected from modification or substitution with a signature are identified in **bold**.

Celotek 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	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	*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			
Update 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
Update key Transmission	Crypto officer role	Update key and SKUNK of the channel to be updated. *SKE cell, containing the encrypted update key, output on the public network port.* SKC cell to cause key changeover	Use Indirect creation/Transmit Indirect creation/Transmit
Update key Reception	User	*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 signature	Keyboard entry Indirect creation
Creation of initialization password digest	Crypto officer role	Terminal entry of the new Initialization password string Initialization password signature	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	Keyboard entry Indirect creation

		Initialization vector.	
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 ID key *Encrypted keys stored on disk*.	Use Use Indirect creation
Key backup and restoration			
Session, update, or SKUNK key backup	Crypto officer role	New session or update key Manager ID key *Encrypted session encryption key*	Use Use Indirect creation
Key restoration	Crypto officer role	*Encrypted backup file containing, session keys, SKUNKs*, crypto private key. Manager ID key. 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 signature. 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 channel/path using manual keys	Crypto officer role	Terminal entry of the VPI,VCI and desired key value Session key	Keyboard entry Direct creation
Establishment of an unsecure bypass channel/path	Crypto officer role	Keyboard entry of desired unsecure VPI/VCI . Identity Session Key	Keyboard entry Direct creation
Establishment of a channel/path using auto key exchange.	Crypto officer role	Keyboard entry of desired secure VPI/VCI. New session encryption and decryption keys 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 key	Crypto officer role	Terminal entry of the new manager passphrase	Keyboard entry

		Manager passphrase key	Indirect creation
Creation of SKUNK	Crypto officer role	System generated SKUNK.	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	Crypto officer 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* *decryption key 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 upgrade file Celotek public key. Software integrity signature	Receive/Use Receive/Use Use Indirect modification
Verification of Celotek Public Key	Crypto officer	Celotek Public Key Celotek Public Key Hash value	Use Use

4 Physical Security Policy

The CellCase system has been designed by Celotek to satisfy the Level 2 physical requirements of the FIPS 140-1 standard. The system is housed in an opaque, steel box with external connections provided for the private and public data network ports, as well as the console display/keyboard, Ethernet ports, and status LEDs. The top lid and baseboard sub-assembly are attached to the case using screws. A seal is provided between the top lid and case to provide evidence of tampering. A similar tamper evident seal is used between the baseboard sub-assembly and case.

The individual responsible for maintaining the CellCase system should periodically check the two tamper evident seals to verify that the unit has not been opened. If the seals are broken, the unit and others with which it exchanges keys are no longer FIPS 140-1 compliant. The tampered unit should be returned to Celotek 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.

5 Initialization Policy

When a CellCase system 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 access to Initialization to only those individuals with access to the system's console terminal.

In Initialization, the crypto officer must establish the passwords associated with the Initialization and Manager logins, the Manager passphrase, and the Crypto passphrase. In the Initialization process, the crypto officer can 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 remote host attached to the same IP sub-net as the CellCase system. Additionally, during Initialization telnet access to the CellCase can be disabled, restricting access to the Manager login to the serial port and limiting access to the crypto officer role to only those individuals with access to the system's console terminal.

It is recommended that in order to maintain strict security, the individual with responsibility for initialization of a CellCase system should periodically assume the crypto officer role and login to the Initialization login to ensure that the Initialization password has not been changed.

6 Management Policy

The crypto officer of the CellCase system is responsible for establishing connections between CellCase systems 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 56 bit, 112 bit, and 168 bit 3DES ECB encryption modes for secure channels. The counter mode encryption supported by CellCase is a DES-based stream cipher established by the ATM Forum (see draft ATM Forum document BTD-Security-01.01). It is not recognized by the FIPS 140-1 standard as a compliant mode of operation.

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 is maintained, capturing all terminal input and output created in a window. 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 a CellCase system 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 CellCase systems. The checks involved include:

- Checking the tamper evident seals on the unit to verify that they are 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 substituted or 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 exchanges were attempted and failed. Failed key exchanges 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 CellCase system. The FIPS 140-1 standard does not provide guidance in specifying the way in which communications with the CellCase system should be handled. As described in the Manager's manual (CellCase ATM Cryptographic System Manager's Guide, Celotek Doc. #800-001-016), the CellCase system 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 a CellCase unit to a local network, it should be kept in mind that all Ethernet based communication between the Crypto officer and system is plaintext. As a result, all logins, passwords, commands etc., are entered and passed to the system, across the network, in plaintext form. An unauthorized individual could easily eavesdrop on a session connection and obtain the passwords to the system. Obviously, managing a CellCase system through the serial port is the most secure since serial port connections are local and are made directly between a CellCase system and a terminal (display/keyboard). Managing a CellCase system 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 a CellCase system through a remote host connected to a CellCase system through a gateway is the least secure method, making the management connection open to trusted, and potentially untrusted users, with access to the intervening data network fabric.