CERTIFAX 3000
Security Policy

Document # 001

Author Neil Witchlow

Revision $Revision: 1.14 $

Last Updated $Date: 1999/07/29 16:43:51 $

Certicom Corporation
103-200 Matheson Blvd. West
Mississuaga, Ontario
L5R 3L7

Creation Date: December 1, 1997
Last Update: July 29, 1999

TABLE OF CONTENTS

MODIFICATION HISTORY

Rev.	Date	Changes
0	19980109	Initial draft. Replaces earlier document by K. Smith.
2	19980127	Revised after internal review.
3	19980427	Correction of errata
4	19980525	Correction of errata
5	19980915	Correction of errata
6	19981102	Correction of errata
7b	19990208	Correction of errata, FS1000 information
9	19990302	Correction of errata, FAXBUFF
1.10		Moved document into MKS Si (new revision numbering)
1.11		Corrections for FIPS 140-1 Certification
1.12		Removed ECDSA signature on firmware
1.13		Final corrections for FIPS 140-1 Certification
1.14	19990729	Final corrections

RECENT CHANGES

- New “encryption-free” functionality
- Only one system report can be printed at a time
- Modem settings per domain, specified by CO.
- Revised SRDI matrix to accommodate FS1000 and FAXBUFF functionality

TERMS AND DEFINITIONS

CF3000	Certicom's second generation fax encryptor
CO	Crypto-Officer; the local "administrator" for the CF3000 unit
CSM	PC application for managing CF3000 units
FS1000	Certicom's first generation fax encryptor
FSM	Certification Authority for FS1000 networks
ID	Identification
LCD	Liquid Crystal Display
PSTN	Public Switched Telephone Network
DTMF	Dual-Tone Multi-Frequency tones used in "tone dialing"

1 INTRODUCTION

This document describes the Security Policy for the CertiFax 3000 (CF3000) fax encryptor, as part of the submission for this product towards FIPS-140 certification. The CF3000 is implemented as a multi-chip stand-alone cryptographic module per the definition of FIPS 140-1. The physical cryptographic boundary of the CF3000 is defined by the CF3000's case.

1.1 CF3000 Description

The CertiFax 3000 fax encryptor allows for secure transmission and reception of faxes between any two Group III facsimile devices equipped with the unit. The CF3000 module is inserted between the facsimile device and its telephone network, and operates transparently to the attached fax device, at data rates between 2400 and 14400 bps.

Beginning each communication session, the CF3000 executes a public-key X.509 certificate based key negotiation protocol using the Elliptic Curve Cryptosystem (ECC). Both the private and public keys are generated by the module itself and the private key *never* leaves the module under any circumstances. A secure communication path is established between the calling module and answering module before any critical data is transmitted. Symmetric key encryption is used for data transfer.

The module implements the following algorithms:

- Elliptic Curve Digital Signature Algorithm (ECDSA – ANSI X9.62)
- Elliptic Curve Key Agreement Protocol (MQV2 – ANSI X9.63)
- Secure Hash Algorithm (SHA-1 – FIPS 180-1)
- Data Encryption Standard (DES – ANSI X3.92-1981)
- Triple DES (TDES – ANSI X9.52-1998)
- FIPS-approved random number generator (FIPS 186)

The CF3000 conforms to FIPS 140-1 Level 3 physical security. The enclosure is tamper resistant, preventing any critical security parameters from being extracted. Physical probing of the module interior will leave clear evidence of tampering. If the module is opened, tamper response circuitry will erase all critical data.

Up to 99 secure "domains" (user groups) are supported, where each domain holds its own X.509 certificate, certified by a Certification Authority (CA). Two modules may communicate within a domain only if they both hold a valid certificate for that domain. Thus, each module can participate in up to 99 secure networks. In addition, the CF3000 supports a "CLEAR" domain for communicating with unsecured faxes, and a "PUBLIC" domain for secure but unauthenticated communication with CF3000 units outside the

customer's network. A FAXBUFF domain is available for use in jurisdictions that prohibit the use of encryption. This domain uses clear, unauthenticated transmission, but enhance confidentiality by storing the fax in a mailbox at the receiving end.

An optional mailbox feature stores an incoming fax within the unit until the intended recipient authorizes printing to the attached fax device. The receiving device can be configured to store all incoming faxes that are not addressed to specific mailboxes in a general "domain" mailbox.

The CF3000 supports a number of configuration options that allow it to be tailored to the customer's requirement. Most of these options involve a trade-off between convenience and security. The module will qualify for FIPS 140-1 Level 3 compliance only when specific options are configured. These are documented later.

The unit provides an operator interface using text menus, via a 2x16-character LCD display, and a numeric keypad with menu navigation keys.

The CF3000 can be administered via this interface, or with suitable configuration, from a PC-based application known as the CertiFax Security Manager (CSM). The CSM can connect to the unit directly via the serial port, or remotely via a dial-up connection to the telco port. The CSM provides a Certification Authority that permits the customer to define domains, and a centralized administration point for the customer's network of CF3000 units.

The FS1000 is Certicom's first generation fax encryptor. It uses a certificate-based encryption scheme that is different from that of the CF3000. The installed base of FS1000 units includes a small number of customers that have large FS1000 networks. These customers need a way of migrating to the CF3000 without wholesale replacement of existing units.

A specially equipped model (the CF3102) is capable of inter-operating with a network of FS1000 units. This model contains an alternative daughter-board that has the hardware needed to participate in the FS1000 secure protocols.

A CF3102 is designed to participate simultaneously in both a (new) CF3000 network, and an (existing) FS1000 network. Operationally, it offers complete CF3000-oriented functionality when exchanging faxes with CF3000 units, and appears to be a fully functional FS1000 when exchanging faxes with an FS1000 unit. Administratively, it takes its configuration instructions from the CSM, but will co-operate with an FSM for the purposes of installing, removing or re-certifying FS1000 "groups" (i.e. domains.)

The CF3102 is the only CERTIFAX 3000 product that operates in this non-FIPS mode. Physically the CF3102 looks no different from any other CF3000 model. The only way to distinguish between them is to view the model number on the display by using the System Info command on the keypad.

Specially-equipped models (denoted by a '1' in the tens position) are intended for use in jurisdictions that prohibit encryption. These models do not contain the DES chip used for

encryption. Such models support only the CLEAR and FAXBUFF domains. These models can exchange faxes with each other, and with regular CertiFax units, using the FAXBUFF domain, which can be installed on a regular unit by the CSM.

1.2 CF3000 Operation

The CF3000 acts as an invisible buffer between the fax device and the telephone network. The telephone network line plugs into the Telco port of the unit, and the fax device into the Fax port. This ensures that all outgoing or incoming calls are routed through the CF3000 unit.

The unit operates in one of four general modes: Send, Receive, Configure or Test. To send a fax, the user provides authentication, identifies the target domain and optionally a mailbox, and then uses the fax device to dial the call to the receiving fax. Depending on the security settings, some or all of these parameters can be built into the dialing sequence output by the fax device. Once the call is placed, the sending CF3000 isolates its fax device from the receiving one while it establishes a secure session with the receiving CF3000. Fax information is then relayed from the sending fax device to the receiving CF3000, via the sending CF3000. The receiving CF3000 either relays the fax transmission to the receiving fax device, or stores it in a mailbox for later pickup.

The unit will receive incoming fax calls without operator action. The incoming fax is relayed through to the attached fax device, or stored in a mailbox for later retrieval.

The CF3000 unit will periodically run diagnostic checks when idle. It will also test its telco and fax ports to ensure that it is connected to the network and/or fax device.

The unit can be administered locally by the crypto-officer, using either the keypad/menu interface, or the CSM attached to the local serial port. If so configured, it will also accept incoming calls from the CSM over the telco port. The unit does not originate calls to the CSM.

2 SECURITY POLICY

2.1 Security Level

~~In many areas, the CF3000 design meets the requirements for the highest FIPS security rating, namely FIPS PUB 140-1 Level 4. However, its physical design and software implementation result in an overall rating of Level 3.~~ Table 1 shows the highest security level attainable by this design, for each of the eleven sections of the FIPS requirement.

FIPS Requirement Section	Level
Cryptographic Module	3
Module Interfaces	3
Roles and Services	3
Finite State Machine	3
Physical Security	3
Software	3
Operating System Security	N/A
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self-Tests	4

Table 1: FIPS 140-1 Security Level Specification for the CF3000

2.2 Roles and Services

The CF3000 supports the following roles and services:

2.2.1 Crypto-Officer Role ("Administrator")

The Crypto-Officer is responsible for initializing the CF3000 unit, and configuring it. Configuration includes security settings, system settings, access control. Configuration can be delegated to the CSM.

2.2.1.1 Crypto Officer Services

The following services can be invoked by the Crypto-Officer, after providing proper authentication:

CO Authentication	Providing identity and password, in order to secure access to the other services listed in this table. Inputs: CO ID and PIN Outputs: Access to desired function.
Initialize Module	A step in the installation process, where the CO is prompted to enter the new CO password, and specify whether a CSM is to be used. Inputs: Fax receiving device attached to Fax port, Network attached to Telco port, New PIN for CO 1, New PIN re-entered for verification, Selection re enabling CSM Access. Outputs: Initialized local database.
Initiate CSM Serial Port Access	Instruct the unit to await connection to a CSM via the serial port. Inputs: CO Authentication, CSM performing "Connect Request" attached to the serial port. Outputs: CSM session over serial port.

Initiate FSM Serial Port Access	Instruct the unit to await connection to a FSM via the serial port. (CF3102 only) Inputs: CO Authentication, FSM performing "Connect Request" attached to the serial port. Outputs: FSM session over serial port.
Print Log	Print recent log entries to the attached fax device. Inputs: CO Authentication, Fax receiving device attached to Fax port. Outputs: Logs delivered to fax device.
Print Reports	Print one of several system reports to the attached fax device. Inputs: CO Authentication, Fax receiving device attached to Fax port. Outputs: Reports delivered to fax device.
Zeroize Unit	Destroy the database key, rendering stored data unusable. Inputs: CO Authentication. Outputs: Destruction of database key.
Reset Defaults	Return all configuration settings to the "factory" defaults. Inputs: CO Authentication. Outputs: Updated database settings.

In addition, the CO may also invoke the following services described elsewhere:

Module Configuration Services (see page 10.)

2.2.2 CSM Role

The CSM is an optional accessory that lets a customer (a) create and install private domains and (b) manage a network of CF3000 units using a graphical user interface. The CSM can be connected via a cable attached directly to the CSM serial port, or via a dial-up connection over the telephone port.

2.2.2.1 CSM Services

The following services can be invoked by the CSM:

Initial Certification	Establish the relationship between the unit and a specific CSM. No other CSM will be given access to the unit. Inputs: CO Authentication, CSM performing "Initial Certification Request" attached to the serial/Telco port. Outputs: CSM relationship established.
Establish Local or Remote Session	Establish a secure and authenticated session over the indicated connection (serial port or dialup) as a pre-requisite to accessing the other services in this table. Inputs: Case 1: CO Authentication, Indication of serial port for CSM Connection, "CSM Connection Request" on serial port. or Case 2: Incoming call from CSM on Telco port Outputs: Secure CSM session established.
Install/Re-certify Domains	Install a new domain on the unit, or re-certify an existing domain. Inputs: Authenticated CSM session, Domain install/re-certify request. Outputs: Updated local database.
Remove Domain	Remove a domain from the unit. Inputs: Authenticated CSM session, Domain removal request Outputs: Updated local database.

Create/Delete COs	Create new COs, or delete them from the unit. Inputs: Authenticated CSM session, CO create/remove request Outputs: Updated local database.
Replace Firmware	Download updated/upgraded firmware to the unit. Inputs: Authenticated CSM session, Firmware replacement request. Outputs: Updated local firmware. **Note: This service is not a FIPS 140-1 approved mode.**
Extract Logs	Transfer log file entries to CSM for archival purposes. Inputs: Authenticated CSM session, Extract Logs request. Outputs: Updated log pointers, logs transmitted.
Enable/Disable FS1000	Enable/disable FS1000 Interoperability (CF3102 only.) Inputs: Authenticated CSM session, Enable FS1000 request. Outputs: Updated local database.
FS1000 User Permissions	Enable/disable FS1000 groups access for individual users. (Only if FS1000 interoperability is enabled.) Inputs: Authenticated CSM session, FS1000 User Permissions request. Outputs: Updated local database.

In addition, the CSM may also invoke the following services described elsewhere:

Module Configuration (see page 10.)

2.2.2.2 Module Configuration Services

The following services can be invoked by both the Crypto-Officer and the CSM:

Enable/Disable Domain	Enable or disable a specific domain. Inputs: Authenticated CO/CSM session, Domain enable/disable request. Outputs: Updated local database.
Create/Remove/Change User	Create or remove user, or change ID, PIN, Name, Domain Permissions, and/or Mailbox attributes Inputs: Authenticated CO/CSM session, User create/remove/change request. Outputs: Updated local database.
Enable/Disable CO	Enable or disable another CO. Inputs: Authenticated CO/CSM session, CO disable request. Outputs: Updated local database.
Change Security Settings	Change configuration options that affect security features. Inputs: Authenticated CO/CSM session, Security setting change request. Outputs: Updated local settings.
Change System Settings	Change configuration options that affect other system features. Inputs: Authenticated CO/CSM session, System setting change request. Outputs: Updated local settings.
Change Log Settings	Change configuration options that affect the Log feature. Inputs: Authenticated CO/CSM session, Log setting change request. Outputs: Updated local settings.

Enable/Disable CSM Access:	Disallow or allow remote CSM access. Inputs: Authenticated CO/CSM session, CSM Access disable request. Outputs: Updated local settings.
Change Admin PIN:	Change the CO password. Inputs: Case 1: CO Authentication, New CO PIN (twice) or Case 2: Authenticated CO session, Change Co PIN request. Outputs: Updated local database.
Un-initialize Module	Permanently remove all content, keys, etc. and return all settings to the original “out-of-box” values. Inputs: Authenticated CO/CSM session, Uninitialize module request. Outputs: Cleared settings and database.
Disable Unit	Enable or disable access to end-user services. Inputs: Authenticated CO/CSM session, Disable unit request. Outputs: Updated local settings.
Modem Settings	Display and/or alter modem settings. Inputs: CO Authentication Selected domain. Outputs: Information displayed on LCD, and/or revised modem settings

2.2.3 FSM Role

The FSM is the certification authority for the first generation fax encryptor (FS1000.) The CF3102 supports interworking with established FS1000 networks. The FSM is the certification authority for the FS1000 network. The FSM connects to the CF3102 via a cable attached directly to the CSM serial port.

2.2.3.1 FSM Services

The following services can be invoked by the FSM:

Establish Local Session	Establish a secure and authenticated session over the indicated connection (serial port or dialup) as a pre-requisite to accessing the other services in this table. Inputs: CO Authentication, Indication of serial port for FSM Connection, "FSM Connection Request" on serial port. Outputs: Secure FSM session established.
Install/Re-certify FS1000 Groups	Install a new FS1000 group on the unit, or re-certify an existing group. Inputs: Authenticated FSM session, Group install/re-certify request. Outputs: Updated local database.
Remove Group	Remove an FS1000 group from the unit. Inputs: Authenticated FSM session, Group removal request Outputs: Updated local database.
Enable/Disable Group	Enable or disable a specific FS1000 group on the unit. Inputs: Authenticated FSM session, Group enable/disable request Outputs: Updated local database.

2.2.4 User Role

The operator in the user role is using the CF3000 primarily to send clear or secure fax messages. (No end-user action is required to receive faxes.) There are other related services, such as printing a received fax from a mailbox.

2.2.4.1 User Services

The following services are available from the user role:

User Authentication	Providing user identity and/or password (as per Access Level settings) in order to access to the other services listed in this table. Inputs: UserID, User PIN Outputs: Access to all other user services
Clear Send	Send a non-encrypted fax to a destination outside of the customer network. Inputs: Authenticated user, Domain 0 (Clear) Incoming fax call on Fax port Outputs: Outgoing fax call on Telco port
Mailbox Send	Send a secure fax to a specific user mailbox at another destination within the customer network. Inputs: Authenticated user, Any secure domain[1], Target mailbox number, Incoming fax call on Fax port Outputs: Outgoing fax call on Telco port

[1] Excludes FS1000 groups, which do not support mailboxing.

Domain Send	Send a secure fax to another destination within the customer network. (The fax may or may not be mailboxed according to settings at the receiving end.) This may involve the FS1000 protocol, if so configured by the CSM. Inputs: Authenticated user, Any secure domain, Incoming fax call on Fax port Outputs: Outgoing fax call on Telco port
Print User Mailbox	Print messages being held in a user mailbox. Requires ID and PIN, regardless of Access Level setting. Inputs: Authenticated user. Outputs: Outgoing call on Fax port, to print messages.
Print Domain Mailbox	Print messages being held in a domain mailbox. Inputs: Authenticated user, Any secure domain (for which user has permission). Outputs: Outgoing call on Fax port, to print messages.
Emergency Zeroize	Voluntarily destroy the database key, rendering all stored information useless. (This is independent of the similar function available to the CO.) Inputs: Authenticated user. Outputs: Disabled unit.
Change User PIN	Change the password associated with a specific user. Requires ID and PIN, regardless of Access Level setting. Inputs: Authenticated user, New PIN, New PIN again for verification purposes. Outputs: Updated PIN.

2.2.5 Services Not Requiring a Role

The following services are available to all users without requiring a specific role.

Reset Print/Connect Alarm	Reset an alarm raised by failure of a print function or connect audit function. Inputs: ESC key Outputs: Cancelled alarm
Run Tests	A set of tests to be individually selected and executed, with results noted on display and in log file. Inputs: Selected test (or ALL tests) Outputs: Test results displayed on LCD
System Info	A sequence of displays showing hardware/firmware identification and memory configuration. Inputs: None Outputs: Information displayed on LCD
Display Last Error	Display the last error code to be detected, if any. Inputs: None Outputs: Information displayed on LCD
Check Connections	Initiate connection audit. Inputs: None Outputs: Information displayed on LCD

2.3 Security-Relevant Data Items

The following list explains each security-related data item used or affected by the above services.

SRDI	Description
X.509	An X.509 domain certificate that contains the domain information, Digital Signature Algorithm Identifier, and CA Digital Signature of the domain information. Also used for FS1000 group certificates.
DomPrivKey	The private key of the domain.
DomPubKey	The public key of the domain.
SessionKey	The symmetric session key that is derived for secure communication.
RandomSeed	The seed used for random number generation.
DatabaseKey	The key used to encrypt all stored information, including settings and the session keys used to encrypt stored messages.
MfrPubKey	Certicom public key used to verify signature on firmware image.
OperPIN	The PIN (user or administrator) entered by the operator during authentication.
OperInfo	The information pertaining to a particular operator (CO vs. user, display name, PIN, permitted domains, mailbox indicator)
DomPerms	Domain Permissions for the current user. Includes FS1000 group permission.
DomInfo	Domain information: display name, enabled indicator.
CLRSend	Setting indicates if bypass is permitted on send operation
CLRReceive	Setting indicates if bypass is permitted on receive operation.
FS1000 Enable	Setting indicates if FS1000 functionality (of a CF3102) is to be enabled.
FS1000 Inverse	The inverse (in the ring) of the group private key, used for computing fast signatures that are needed in the FS1000 transport protocol.

2.3.1 Configuration Settings

These settings control the operation of the CF3000. A special indication is used for items that must have a specific setting in order to qualify for the overall FIPS 140-1 Level 3 approval. These configuration settings can only be set/modified by an authenticated CO or CSM.

Item	Description	Level-3
Access Level	How much authentication (0=none, 1=PIN only, or 2=ID+PIN) is required for access to end-user functions. **N.B. Must be '2' for FIPS 140-1, Level 3 operation.**	**2**
Dialstring Authentication	Boolean. True permits authentication information may be entered via number dialed by fax device. **N.B. Must be false for FIPS 140-1, Level 3 operation.**	**false**
Authentication Timeout	For send operations, the maximum length of time system will wait after keypad operations are complete before fax call is dialed by the fax device.	any
Allow Clear Send	Boolean. If false, the unit cannot be used to send unsecured faxes. (i.e. the CLEAR domain will not be available for SEND operations.)	any
Allow Clear Receive	Boolean. If false, the unit cannot be used to receive unsecured faxes. (i.e. the CLEAR domain will not be available for RECEIVE operations.)	any
Default Domain	The domain which will be used if the operator does not explicitly choose one. It is also the initial offering when the operator is presented with a list of domains.	any
End-User Zeroize	Boolean. If true, an "emergency zeroize" function is available to end-users.	any
Secure Banner	Boolean. If true, a security notice is appended at the end of each printed fax document.	any

Alpha Security Indicator	Boolean. If false the security notice that appears in the header strip will contain only numeric digits	any
Auto Print Log	Boolean. If true, the log will automatically be printed to the attached fax device when approximately one-page's worth has accumulated.	any
Log Archiving	Boolean. If true, the log data will not qualify for being overwritten until it has been collected by the CSM.	any
Buzzer	Boolean. If true, the buzzer will be sounded (a single beep) upon successful transmission of a fax.	any
Auto Print Test Page	Boolean. If true, the power-on test sequence includes printing a test page to the attached fax device.	any
Local Administration Allowed	Boolean, settable only from the CSM. If false, the local administrator is not permitted to change any system settings.	any
Language	Determines the language to be used in text produced by the system. One of French or English.	any
Diagnostic Period	Minutes of inactivity after which diagnostic test suite is executed. Zero indicates feature is disabled. **N.B. Must be > 0 for FIPS 140-1, Level 3 operation.**	**non-zero**
Connection Audit Period	Minutes of inactivity after which connection audit test suite is executed. Zero indicates feature is disabled.	any
Admin Session Timeout	Number of seconds of inactivity after which crypto-officer session is terminated.	any
FS1000 Interoperability Enabled	Boolean, settable only from the CSM, for selected models. If true, unit will be capable of accepting group certificates from an FSM, and exchanging faxes using the FS1000 protocol. (This mode is only available with the CF3102 model number.)	**any**

3 SECURITY RULES

This section documents the security rules enforced by CF3000 to implement the security requirements of FIPS 140-1. Note that in many cases, the design meets the requirements for Level 4 approval, but the overall target is Level 3 because of physical design and operating system choices.

Each rule has a unique mnemonic identifier enclosed in square brackets, and the rule itself appears in italic font. The value in parentheses is the ID of the transition that implements this rule, according to the accompanying Finite State Machine description. Some rules may be accompanied by additional information in plain font. Rules have been grouped into headings for review purposes.

3.1 Operation

[OP-POWERUP1] The unit performs diagnostic tests on power up. During these tests, the modems are held in reset to inhibit data output. If a fault is detected, the unit enters an error state, holds the modems in reset to prevent data output, and remains inoperative. (A18) The tests performed include:

- A "known answer" cryptographic algorithm test for each of encryption, decryption, and signing/verifying.
- Verification of the CRC of the firmware image.
- A test of critical hardware such as the DES chip, and the real-time clock.
- Statistical random number generator tests specified by FIPS 140-1.

[OP-CONDTEST1] Each of the tests performed on power up can also be invoked on demand. Modem control during testing and error state are as described above. (D9)

[OP-CONDTEST2] In addition, the following tests can be performed on demand. Modem control during testing and error state are as described above. (D9)

- A pairwise consistency test for public and private keys
- A test of other hardware components including the LCD display, keypad keys, buzzer and lamp.
- A test of telephony interface functions (Modem Response, Loopback, Relays, DTMF Detection, Loop Current)
- A test of module memory (RAM, D/B Flash, M/B Flash, Firmware)

[OP-TESTPAGE] The unit can be configured to print a test page to the attached fax device on successful completion of the power-up tests. (A31)

[OP-DIAG] The unit will periodically perform diagnostic checks after a configurable period of inactivity, to ensure that the unit remains in operable condition. (A6)

[OP-CONNECT] The unit will periodically check that it is connected to a fax device and network, after a configurable period of inactivity, to ensure that the unit remains in operable condition and in service. (A6)

[OP-SINGLE] The unit is engaged in at most one activity at any one point in time. (General assertion). After power-up, the system enters the idle state. Activity will be generated in response to one of operator input, internal timer or incoming call detection events. Once the unit is engaged in some activity, events not involved with that activity are ignored.

[OP-IDLE] After each activity, the unit returns to the idle state. (A3 et al.)

[OP-MENU] When idle, use of any of the keypad keys will launch the Menu activity, preventing the unit from responding to other inputs or requests. (A14) The operator can navigate a set of menus, potentially launching another activity.

[OP-COMMANDS] As an alternative to navigating a menu tree, the operator can use a shortcut to directly launch selected activity. (D0) This implicitly terminates the current activity, if there is one.

[OP-PROMPT1] Input prompts require the operator to take some action. The prompt is displayed until input is given, or the task times out. (D25) The time-out duration may vary from task to task.

[OP-PROMPT2] Transient prompts are used to display information that does not require user reaction. (Assertion) A transient prompt normally lasts 3000 milliseconds, and is then followed by another transient prompt or input prompt. However, transient prompts may also be used to report real-time changes in status, in which case the prompt may be replaced whenever the underlying status changes.

3.2 Domains

[DOMAIN-1] Two units can exchange secure faxes only if they share a domain (a certificate given by a common certification authority, or use the PUBLIC domain.) (E8,[]) Domains are identified internally by a 16-character domain name, and are designated by the operator using a two-digit code. Each unit can currently support up to 99 customer-defined domains.

[DOMAIN-00] Domain code 00 is reserved for the CLEAR (bypass) domain. (CSM.)

[DOMAIN-99] Domain code 99 is initially used for the PUBLIC domain shipped with the unit. However, the customer may remove this domain and reassign the code 99 to a customer-defined domain. (CSM)

[DOMAIN-CSM] The CertiFax Security Manager (CSM) is used to create customer-defined domains, and install these domains on selected CF3000 units. (CSM)

[DOMAIN-ENABLE] The CO can enable or disable any user-accessible[2] domain that is installed on the unit. However, only the CSM can install new domains on the unit. (P4,P12,E17)

3.3 Mailboxes

[MAILBOX-FEATURE] The unit can optionally be equipped with mailbox capability, in one of several capacities. (Assertion)

[MAILBOX-NOTIFICATION] When a new message is stored in a (user or domain) mailbox, a notice is printed to the attached fax device. (A23) The notice identifies the mailbox, date, time, and total number of pages waiting (which includes earlier unprinted faxes.)

[MAILBOX-USER] Each user ID can be selectively given a User Mailbox. (P6) This means that users at other locations can send secure faxes addressed to this specific user ID.

[MAILBOX-DOMAIN] Each user-accessible[3] domain (other than CLEAR) can be selectively given a Domain Mailbox. (P4) When a domain is granted a mailbox, all incoming faxes using this domain (excluding those addressed to a User Mailbox) are stored in the domain mailbox. A notification page is generated. Any user who is authorized to send using this domain can authorize the printing from the domain mailbox. Establishing a domain mailbox is strictly a local decision, and does not require the knowledge or cooperation of the sender.

[MAILBOX-USER-DOMAIN] If an incoming message is addressed to a particular user mailbox, but that user does not have permission to use the domain selected by the sender, the transmission will be disallowed. (E13,E14)

[MAILBOX-OVERFLOW] The unit will stop accepting new messages into mailboxes when the storage capacity is exhausted. (E13,E14) The unit will display a status message to this effect.

[MAILBOX-DELETION] Deleting the user or domain from the unit will delete the associated mailbox, together with any messages stored in the mailbox. (P4,P6)

---

[2] This term was chosen to exclude the CSM domain that authenticates and secures CSM access.

[3] This term was chosen to exclude the CSM domain that authenticates and secures CSM access.

3.4 Send

[SEND-AUTH] In order to send a fax, the user must be authenticated to the specified Access Level. The authentication can be entered via the keypad. If permitted by configuration rules, the authentication information can alternatively be entered via the dialstring. (F16,F2,F3)

[SEND-DOMAIN] In order to send a secure fax, the user must accept the default domain, or specify a domain via the keypad or dialstring. (F3)

[SEND-DOMAIN-PERMS] In order to send a secure fax, the user must have permission to use the selected or implied domain. (F3)

[SEND-MAILBOX] A (secure) fax may optionally be sent to a specific user mailbox at the receiving site, by inclusion of a "mailbox" parameter. The validity of this parameter cannot be determined until the transmission is attempted. The receiver will terminate the transmission if the requested user does not exist, is disabled, does not have mailbox capability, or does not have permission to use the domain selected by the sender. (E13,E14)

[SEND-PARMS-CONFLICT] If a send parameter is entered via the keypad interface, the dialstring must not include parameters. (F16)

[SEND-DIALSTRING-EXTRANEOUS] The send operation will fail if the dialstring contains extraneous parameter information. (F16)

[SEND-CLEAR] In order to send a fax to a non-secure device, the user will need to select the CLEAR domain. The CO determines if this domain is available. (F2,P4)

[SEND-DOMAIN-DEFAULT1] There is a default domain specified for the unit. The keypad interface will normally offer this domain as the default domain. This domain will be used if the user does not explicitly select a domain (P20,F2,F3)

[SEND-DOMAIN-DEFAULT2] The keypad interface will offer the user the default domain specified for the unit, unless this domain is not valid for the user, in which case the interface offers the lowest numbered valid domain. (I2,J2)

[SEND-AUTHTIMEOUT] After entering authentication information and send parameters, the unit will wait for a configurable time for the attached fax device to dial the actual call. The send operation is terminated if the call does not begin within this period. (K6,J4)

3.5 Print Mailbox

[PRINT-DOMAIN] In order to print the contents of a domain mailbox, the user must be authenticated to the specified Access Level. The interface will only offer the user those domains which (a) have mailboxes (b) have pages waiting and (c) for which the user has permissions. (L2,L4)

[PRINT-USER] In order to print the contents of their personal mailbox, the user must provide ID and PIN, independent of the setting of Access Level. (M2)

[PRINT-OPERATION] Printing a mailbox will cause all waiting pages to be printed, oldest first. Each document is deleted from storage as the local unit acknowledges receipt. (M3,L5)

[PRINT-RECOVERY] Standard fax protocol allows the unit to re-transmit any page that is not properly received by the fax device. If this is unsuccessful, the unit sounds an alarm, and the operator will have a choice of Retry Printing (from start of current document), Purge Document or Cancel Printing. (L5,M3) Cancel Printing is assumed if no input is forthcoming.

3.6 Zeroize

[ZEROIZE] If so configured via the CO, the user may voluntarily zeroize the unit. The user must authenticated to the level specified by Access Level. (N2) Independent of this setting, there is a CO function to zeroize the unit.

3.7 Installation

[FIRST-USE] Initialization is performed on first power-up, after startup tests, and includes: update the random seed, install the PUBLIC domain; prompt for administrator PIN, prompt for initial setting of CSM Access (enable or disable.) (A16)

[INITIAL-CERT1] Initial certification establishes control of a unit by a specific CSM. Only the CSM that performs the Initial Certification of the unit may administer the unit. (E6)

[INITIAL-CERT2] Initial certification must be initiated by the local CO. It can occur via a dialup connection or by direct connection to the serial port. The certification session itself is encrypted using the PUBLIC domain installed during initialization) but is not authenticated. (P10) All subsequent contact between the CSM and the unit is encrypted and authenticated using keys exchanged during the initial certification session.

3.8 General Administration

[LOCAL-CONTROL1] The CSM cannot assume control over a unit without an explicit action at the unit by the CO. (P10) The unit must be placed into “Initial Cert” for the initial CSM contact.

[LOCAL-CONTROL2] The CO retains the ability to disable CSM access if and only if the CO has not been disabled by the CSM (see [CSM-CONTROL1]). (P20) This action is appropriate if the CSM is believed to have been compromised.

[CSM-CONTROL1] The CSM can disable any or all CO-s, thus taking exclusive control over a unit if and only if the CSM has not been disabled by the CO (see [LOCAL-CONTROL2]). (E17)

[ADMIN-AUTH] The CO must provide both ID and PIN to gain access to local administration functions. (P2) Access is via the Configure menu.

[ADMIN-EXIT] The CO session will continue until the Configuration menu is exited, or an inactivity timer expires. (P1)

[ADMIN-REPORTS] The CO can print one of several reports to the attached fax device. These include a system status report, a mailbox status report, a list of available user mailboxes, and a list of available domains. (P24)

[ADMIN-ZEROIZE] The CO can voluntarily zeroize the unit, rendering any stored contents useless. The unit will require re-manufacture before it can be used again. (P14) Some customers will prefer to do this prior to returning the unit to Certicom for service.

[ADMIN-RESET] The CO can reset all system settings to the factory default. (P22)

[ADMIN-UNINITIALIZE] The CO can voluntarily un-initialize the unit. This action will permanently remove all content, keys, etc. and return all settings to the original "out-of-box" values. (P16) The process takes about one minute to complete. It is appropriate if the unit is to be taken out of service, possibly in preparation for re-deployment in another location or network. Note that for the CF3102, the MOBIUS group is permanently removed. The only way to restore this group is to return the unit for re-manufacture.

[ADMIN-MAINTENANCE] The CO can initiate any of several diagnostic tests. (D9) These include various Crypto, Telephony, Memory and Interface tests.

[ADMIN-DISABLEUNIT] The CO can temporarily disable a unit, preventing it from providing any service to the user role. (P20) Administration functions and CSM access remain available.

3.9 Audit Trail

[LOG] All important events and transactions are recorded in a log file, which can be printed via the attached fax device, and/or collected by the CSM. (Assertion.)

[LOG-AUTO-PRINT] The CO can arrange to have the log automatically printed to the attached fax device. (P20) Printing occurs when a page's worth of activity has occurred. This provides a continuous hard-copy local record of activity.

[LOG-PRINT] The CO can print the most recent log entries on demand. (P18) This does not affect Auto Printing.

[LOG-ARCHIVE] The CO can specify that all log files are to be kept until collected by the CSM for archiving purposes. (P20) This ensures that a continuous soft-copy record is kept at the CSM.

[LOG-OVERFLOW] The unit will not overwrite a log entry until it has been collected by the CSM (if Archiving is enabled.) (Assertion.) If the buffer becomes full, the unit will stop accepting new transactions. This ensures the record of activity provided by Auto-Printing and/or Archiving is complete and continuous.

3.10 User Administration

[USER-OPTIONAL] Users need only be defined if (a) the Access Level is 2, or (b) an individual requires a personal mailbox. (Assertion.)

[USER-UNIQUEID] A user is identified by a 1-8 digit number that is unique across units. The number 0 is not a valid ID. (P6,CSM)

[USER-NAME] A user has a 16-character text name. (P6,CSM) This consists of upper-case ASCII characters, plus selected special characters (space, hyphen apostrophe.)

[USER-PIN] A user has a numeric PIN (3-8 digits). This PIN is never displayed or printed. To guard against undetected access to the user account, the CO may change the PIN but may not determine its current value. (P26,CSM)

[USER-ENABLED] The CO may disable a user ID, preventing the user from taking any action that requires user authentication. (P6)

[USER-MAILBOX] If the unit supports mailboxing, the CO may grant/revoke the user the ability to have messages stored in a mailbox. (P6,CSM) Revoking this privilege prevents the reception of new message into the mailbox, but does not affect the ability to print messages that are already received.

[USER-DOMAINS] The user must be given explicit permission to use each domain. (P6,CSM) A newly created user does not have permission to use any domains. A newly installed domain is initially disabled for all users.

3.11 CO Administration

[CO-ID] Each CO is identified by a 1-8 digit number that is unique for the unit only. The number 0 is not a valid CO ID. (CSM)

[CO-NAME] A CO has a 16-character text name. (P8,CSM) This consists of upper-case ASCII characters, plus selected special characters (space, hyphen apostrophe.)

[CO-PIN] A CO has a numeric PIN (3-8 digits). This PIN is never displayed or printed. To guard against undetected access to the unit, the CSM may change the PIN but may not determine its current value. (P28,CSM)

[CO-DEFAULT] As shipped from the factory, the unit has a single CO with ID "1" and name "ADMIN1". (Assertion.)

[CO-PIN-INITIALIZE] The CO is forced to change the PIN for CO "1" as part of the initialization process. (H0) This guards against an attack using the default CO PIN.

[CO-ENABLED] The CO may disable any other CO, but not him/herself. (P8)

[CO-MULTIPLE] A unit can support up to 8 CO-s. (CSM) Additional CO-s are defined using the CSM. Only the CSM can create or delete CO-s.

[CO-LAST] The CSM is not permitted to delete the last CO of a unit. (CSM)

3.12 Security Settings

[SECURITY-ACCESS-LEVEL] The CO determines the level of authentication required for the user role. (P20) Level 2 requires both ID and PIN; Level 1 is PIN only and Level 0 requires no authentication. When the Access Level is 1, the CO specifies the (single) PIN to be used by the user role. **N.B. This setting must be "2" to qualify for FIPS 140-1 Level 3.**

[SECURITY-DIALSTRING] The CO determines if authentication information (ID and/or PIN) may be entered via the digits dialed by the attached fax device. (P20) **N.B. This setting must be false to qualify for FIPS 140-1 Level 3.**

[SECURITY-AUTH-TIMEOUT] The CO determines how long the unit waits after completion of keypad input before the fax device must place the call. (P20) The value is in the range of 1-999 seconds, default 90 seconds.

[SECURITY-ALLOW-CLEAR-SEND] The CO determines if end-users are permitted to send unencrypted faxes to devices that are not equipped with CF3000 units. (P20)

[SECURITY-ALLOW-CLEAR-RECEIVE] The CO determines if end-users are permitted to receive unencrypted faxes from devices that are not equipped with CF3000 units. (P20)

[SECURITY-DEFAULT-DOMAIN] The CO can specify the default domain to be used for Send operations, to be used in the absence of operator input. (P20)

[SECURITY-USER-ZEROIZE] The CO determines if emergency zeroization is available to the user role. (Zeroization is always available to the CO role.) (P20)

[SECURITY-SECURE-BANNER] The CO determines whether secure faxes are to have the original calling station ID replaced with a security indication. (P20) Actual display of this calling station ID is up to the attached fax device. Some units display this information on an LCD and/or in the transmission log; many print it together with date-time and page number on the "header strip" that appears at the top of each printed page.

[SECURITY-DIAGNOSTIC-PERIOD] The CO determines how frequently an idle unit will perform self-diagnostic tests. (P20) The default is 60 minutes, but may be any value between 0-9999 where 0 implies "do not test." **N.B. This setting must be set to a non-zero value to qualify for FIPS 140-1 Level 3.**

[SECURITY-CONNECTAUDIT-PERIOD] The CO determines how frequently an idle unit will perform a connection audit. (P20) The default is 60 minutes, but may be any value between 0-9999 where 0 implies "do not test."

[SECURITY-ADMIN-TIMEOUT] The CO determines the number of seconds of inactivity which will cause the CO session to terminate. (P20) The range is 1-999 seconds, with a default of 90.

3.13 System Settings

[SETTING-OTHER] Other settings control: Auto-Printing of Log, Trace Information in Log, Print Test Page on Startup, Prompt Language, Use of Alphanumeric Text in Security Indicator. (P20)

[SETTING-LOG-ARCHIVE] The CSM determines whether log entries should be kept until collected by the CSM. (P20)

3.14 FS1000 Interoperability

[FS1000-ENABLING] Only selected models (CF3100-series) have the hardware needed to interoperate with FS1000 units. This capability is not expressed until it is specifically enabled. (E2,F25) Only the CSM can enable this capability. (E17) The capability can be enabled only if it is permitted by the license file provided by Certicom. (CSM)

[FS1000-RESERVED-CODES] For CF3100-series units, domain codes 90-94 are reserved, and may not be used for private domains. This is true even if FS1000 Interoperability is disabled. (F4) These codes will be used by end-users to designate groups 0-4 for Secure Send operations:

Group 0 – Domain 90
Group 1 – Domain 91
Group 2 – Domain 92
Group 3 – Domain 93
Group 4 – Domain 94

[FS1000-INIT-CERT] Certification for the FS1000 communications is performed by the Fax Secrets Manager (FSM) through the serial interface of the CF3102. The local administrator must first place the unit into FSM connection mode before the serial interface is used by the CF3102. (P30)

[FS1000-RECERT] Once an FSM has installed an FS1000 certificate (using the serial port) it can subsequently delete, re-certify or disable the certificate using either the serial

port, or by calling the CF3102. (P30,E31) The exchange is encrypted using the existing certificate. **N.B. This function is not yet implemented.**

[FS1000-FSM-ACCESS] The local administrator can prevent the unit from accepting a call from any FSM by disabling FSM access. (E31) This does not disable access by the CSM. ***N.B. This function is not yet implemented.***

[FS1000-SEND] To send a fax to an FS1000 Destination, the CF3102 user simply selects the appropriate domain code for the destination. If the domain code selected by the user corresponds to one of the FS1000 groups, the unit will initiate the FS1000 send protocol for the transmission. (*F25*) The user need not "do" anything special, and may indeed be unaware of any special treatment being accorded this transmission. Note that even though the FS1000 protocol is used for the actual transmission, the CF3102 continues to offer CF3000-level functionality, such as dialstring validation, that is not available to FS1000 users.

[FS1000-USER-PERMS] When configured for Access Level 2, the user must have explicit permission in order to send using an FS1000 group. (F3) Users have a single enable/disable status which, when enabled, allows access to any FS1000 group that is available on the unit. The User indicates the selection by using the domain code that corresponds to the group.

[FS1000-RECEIVE] No user action is necessary to receive a fax from an FS1000-equipped location. When the FS1000 send attempt is detected the CF3100 engages the FS1000 receive protocol. (E35) Once the group is authenticated, fax reception proceeds. (E22,E27)

[FS1000-PROTOCOL] The Fax Secrets protocol implements Certicom proprietary encryption algorithms. The signature scheme is El Gamal like, and the key exchange is Diffie-Hellman like. (Assertion) These protocols and the stream cipher are described in the CF3000 Functional Specification, and in full detail in "Response to CSE - Annex A of A282-6,R2/376-93" by Ashok Vadekar (1994).

3.15 Encryption-Free CertiFax

[FAXBUFF-MODELS] Several models will be prepared without DES encryption hardware, and with a special firmware compilation which omits all encryption functionality. (Assertion) Such models are suitable for deployment is jurisdictions that prohibit encryption.

[FAXBUFF-INITIALIZATION] On manufacturing power-up, an encryption-free model will detect the absence of encryption hardware, and prepare for encryption-free operation. (Assertion) This action creates and installs a FAXBUFF domain as domain code 98, with mailboxing enabled by default. An encryption-free CertiFax supports only the CLEAR and FAXBUFF domains – the PUBLIC domain is not installed in these units.

[FAXBUFF-INTERWORK] A CSM can install the FAXBUFF domain on a regular CertiFax model, in any non-reserved domain code. (E17)

[FAXBUFF-CERTIFICATE] When sending or receiving using the FAXBUFF domain, the unit does not attempt to authenticate the certificate received from the other unit. (E36,F33) This action is unnecessary, because the certificate is self-created; also, the required cryptographic functions are not available.

[FAXBUFF-TRANSMISSION] Actual transmission using the FAXBUFF domain occurs in the clear. (E37,F34)

[FAXBUFF-INTERLOCK] Two encryption-capable CertiFax units will be prevented from transmitting a fax using the FAXBUFF domain. (E12,F12) The tags contained in the certificate from the other unit will allow a regular CertiFax to determine if it is dealing with another regular CertiFax unit. If this is the case, the transmission is terminated.

[FAXBUFF-CSM] An encryption-free CertiFax cannot be administered by a CSM. It does not support the cryptography needed to secure this connection. (E17) CSM-related functions may still appear in the menu structure, but these will not be effective.

4 SERVICE/ROLE VS. SRDI

The table shown on the following pages serves two purposes:

1. It shows the role or roles in which a particular service is available.

2. It shows which Security-Relevant Data Items (SRDIs) are used and/or altered by each service.

The table is explained as follows:

- The rows of the table are each of the services offered by the CF3000, grouped into one of several categories. These are CO, CSM, Module Configuration, User and Unauthenticated User services. Services are listed by name in the major column labeled "Service". A description of each service can be found in section 2.2.

- The next set of columns, grouped under the label "Roles", identify each of the four roles provided by the CF3000. An "X" in one of these columns indicates that the particular service is available under the role. Roles are also described in section 2.2.

- The final set of columns, grouped under the label "SRDI-s", identify each of the security-related data items provided by the CF3000. A symbol in one of these cells indicates that the particular SRDI is accessed by the service. The nature of the access is one of:

R for "Read"	the value of the item is used by not changed by the service.
W for "Write"	the SRDI is changed by the service
M for "Modify"	some portion of the SRDI is changed by the service. (This is similar to "W" but is used for SRDIs that are "collections" rather than single items.)

- Recent changes are shown in *italics.*

Service Category/Name	Role					SRDI Identifier														
	User	No Role Req'd	CO	CSM	*FSM*	X.509	DomPrivKey	DomPubKey	SessionKey	RandomSeed	DatabaseKey	MfrPubKey	OperPIN	OperInfo	DomPerms	DomInfo	ClrSend	ClrReceive	*FS1000 Enable*	*FS1000 Inverse*
CO																				
CO Authentication			X								R		R	R						
Initialize Module			X			W	W	W			W		W	W	W	W	W	W	*W*	*W*
Initiate CSM Serial Port Access			X				R	R												
Initiate FSM Serial Port Access			*X*																	
Print Log			X																	
Print Reports			X											*R*		*R*	*R*	*R*		
Zeroize Unit			X							W	W									
Reset Defaults			X										R	W	*W*	W	W	W		
CSM																				
Initial Certification				X		W	W	W			R					M				
Establish Local/Remote Session				X		R	R	R	W		R					R				
Install/Re-certify Domain				X		W	W	W			R					M				
Remove Domain				X												M				
Create/Delete COs				X							R			M						
Replace Firmware (Not a FIPS 140-1 approved mode)				X								R								
Extract Logs				X																
Enable/Disable FS1000 ability				*X*							*R*								*W*	
FS1000 User Permissions				*X*							*R*				*M*					
Module Configuration																				
Enable/Disable Domain			X	X												M				
Create/Remove/Change User			X	X							R			M	*M*					
Disable CO			X	X										M						
Change Security Settings			X	X																
Change System Settings			X	X																
Change Log Settings			X	X																
Disable CSM Access			X	X																
Change CO PIN			X	X							R			M						
Un-initialize Module			X	X		W	W	W			W		W	W	W	W	W	W	*W*	*W*
Disable Unit			X	X																
Modem Settings			*X*	*X*												*M*				
FSM																				
Establish Session					*X*	*R*	*R*	*R*	*W*		*R*					*R*				
Install/Re-certify FS1000 Group					*X*	*W*	*W*	*W*			*R*					*M*				*W*
Remove FS1000 Group					*X*											*M*				
Enable/Disable FS1000 Group					*X*											*M*				

Table 2 SRDI Matrix Part 1

Service Category/Name	Role					SRDI Identifier														
	User	No Role Req'd	CO	CSM	*FSM*	X.509	DomPrivKey	DomPubKey	SessionKey	RandomSeed	DatabaseKey	MfrPubKey	OperPIN	OperInfo	DomPerms	DomInfo	ClrSend	ClrReceive	*FS1000 Enable*	*FS1000 Inverse*
User																				
User Authentication	X										R		R	R						
Clear Send	X																R			
Mailbox Send	X					R	R	R	*R*		R				R	R				
Domain Send	X					R	R	R	*R*		R				R	R				
Print User Mailbox	X										*R*									
Print Domain Mailbox	X										*R*				R	R				
Emergency Zeroize	X									W	W									
Change User PIN	X												*M*	*R*						
Services Not Requiring a Role																				
Reset Print/Connect Alarm		X																		
Run Tests		X		X																
System Info		X		X																
Display Last Error		X		X																
Check Connections		X		X																

Table 3 SRDI Matrix Part 2

5 END OF DOCUMENT