FIPS 140-2 Security Policy

FibeAir® 1500P™ Secure Basic Indoor Unit

Ceragon Networks Ltd.
24 Raoul Wallenberg St.
Tel-Aviv 69719
Israel

May 25, 2006

Revision Version 4.0

FIPS 140-2 Security Policy

FibeAir 1500P™ Secure Basic Indoor Unit

1. Introduction

The following document describes the security policy for "FibeAir 1500P™ Secure Basic Indoor Unit" product and has been created as part of the process of submitting this product to the FIPS 140-2 validation for security level 2. The security policy involves a specification of the security rules under which a cryptographic module shall operate.

FibeAir 1500P™ Secure Basic Indoor Unit's cryptographic module operation is based on encryption/decryption processes using symmetric block cipher (AES algorithm) and the asymmetric key establishment technique (Diffie-Hellman Key Establishment). The AES standard was implemented using a hardware AES core. The system provides FIPS-validated operator authentication, secure key storage and management, and performs secure authentication for all firmware and software files downloaded to the cryptographic module.

The user controls the cryptographic module either via Ceragon's Network Element Management application (CeraView) installed directly to the host computer or via craft terminal menus.

1.1 Purpose

This document covers the secure operation of FibeAir 1500P™ Secure Basic Indoor Unit including the initialization, roles, and responsibilities of operating the product in a secure, FIPS-compliant manner.

1.2 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
CO	Crypto-officer
BER	Bit Error Ratio
CRC	Cyclic Redundancy Check
DEA	Data Encryption Algorithm
DH	Diffie-Hellman key establishment protocol
DSS	Digitally Signed Signature
EOW	Engineering Order Wire
FE	Fast Ethernet
FPGA	Field-Programmable Gate Array
ID	Identification Number
IDC/IDU	Indoor Controller/Unit
IF	Intermediate Frequency Cable

KAT	Known Answer Test
KEP	Key Exchange Protocol
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal
MUX	Multiplexing Unit
ODU	Outdoor Unit
PDH	Plesiochronous Digital Hierarchy
PRNG	Pseudo Random Number Generator
RF	Radio Frequency
RS232	Serial Interface Data communication Standard
Rx	Receive Direction
SRDI	Security Relevant Data Item
SD Card	Secure Digital Card
T1	PDH Standard Protocol
Tx	Transmit Direction
WSC	Wayside Channel

1.3 Product Overview and Physical Interfaces

The FibeAir 1500P™ Secure Basic Indoor Unit product is part of Ceragon's FibeAir1500P® product family of broadband wireless systems. It was developed to provide a FIPS compliant secure operating mode using special hardware, software, and state-of-the-art technology.

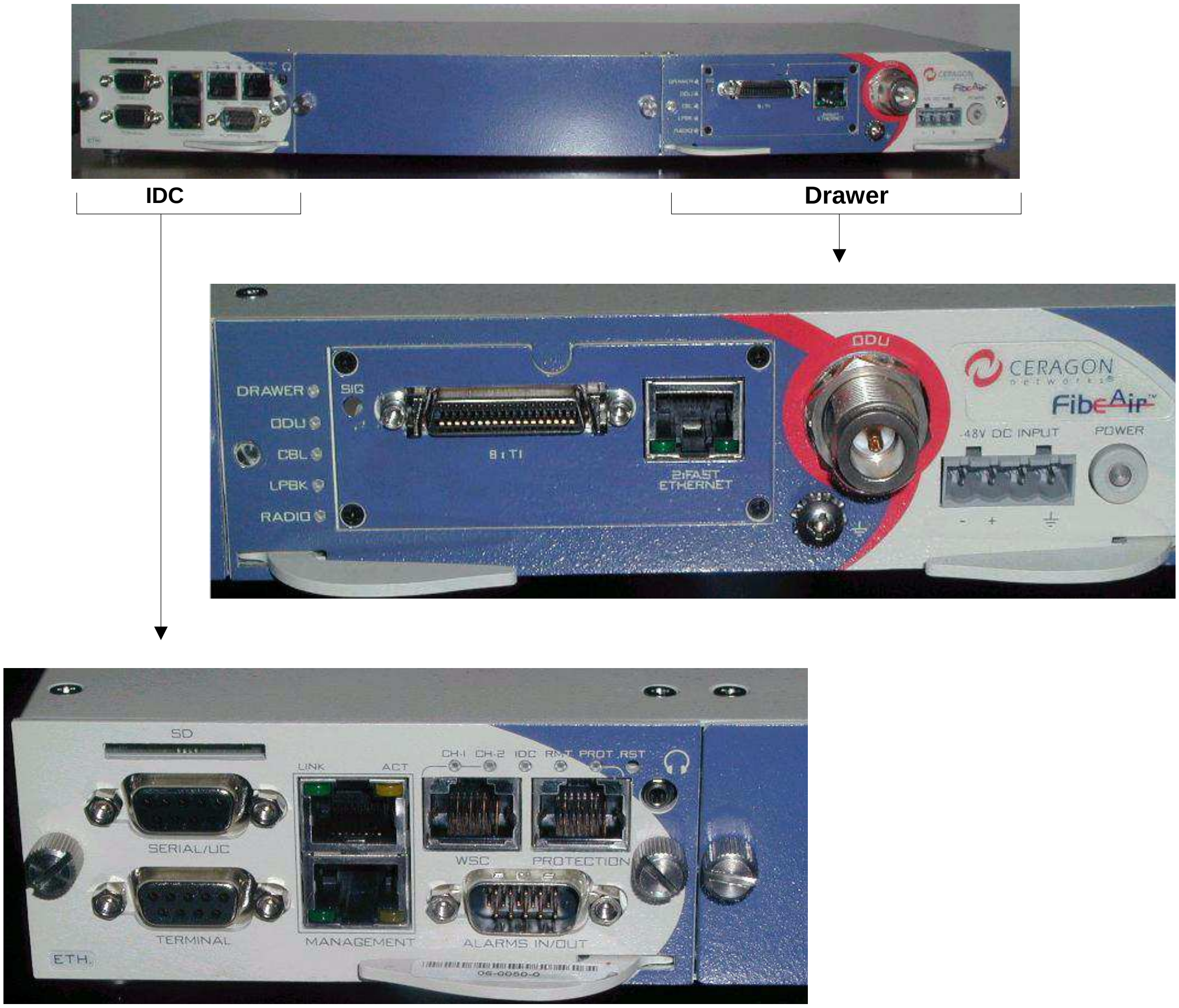


Figure 1. FibeAir 1500P^{TM} Secure Basic Indoor Unit's Physical Interface Ports

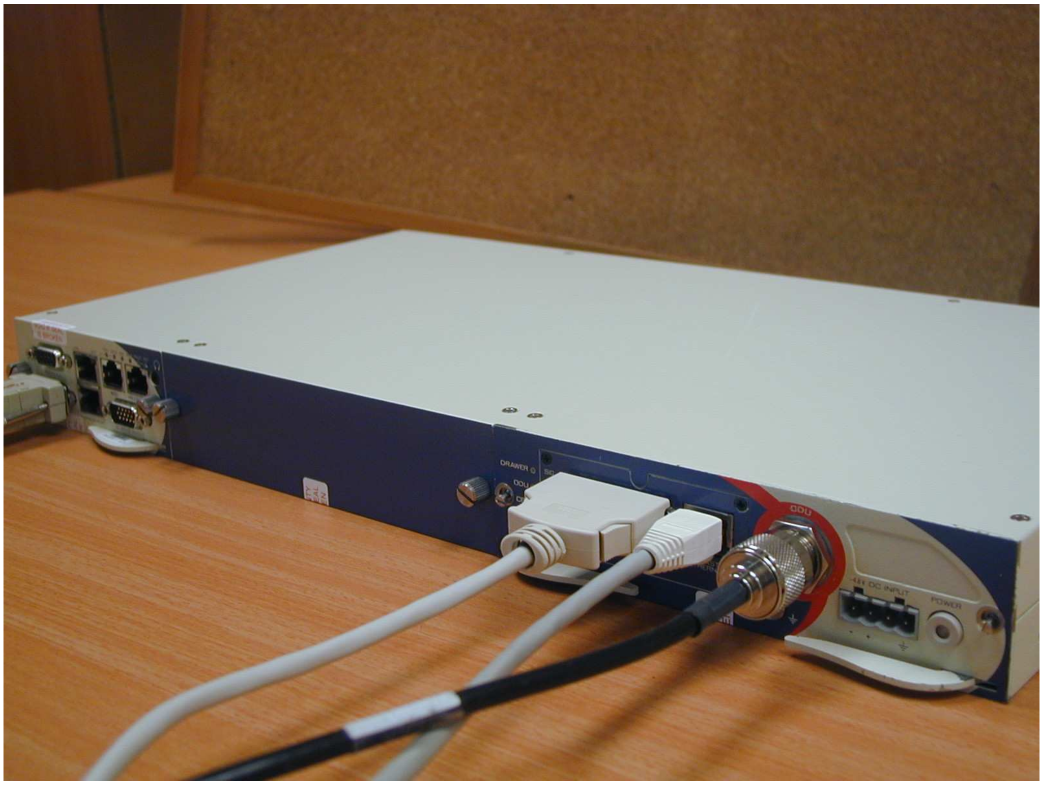


Figure 2. FibeAir 1500P™ Secure Basic Indoor Unit with Interface Ports Connected: Radio, Fast Ethernet and 8xT1;

The following table presents the FibeAir 1500P™ Secure Basic Indoor Unit's physical interface ports.

Interface name	Interface type	Description
Power Receptacle	Power	Receptacle for 45-70 VDC power connector
Radio IF connector	Data I/O	Used for communication between IDU and ODU via the IF cable.
RJ45 Fast Ethernet communication port	Data I/O	Fast Ethernet 10/100 Mbps interface for the data that is sent to the radio in encrypted form.
8xT1 connector	Data I/O	T1 interface connector provides access for eight T1 ports. Data is sent to the radio in encrypted form.
RJ45 Management Network Port (x2)	Control input, Status output	Provides 10 Mbps network port for the device management interface.
RS232 Management Serial Port	Control input, Status output	Provides terminal access to the module's command line interface.
Serial Line Internet Protocol Port (SLIP)	Control input, Status output	Provides device management interface over serial line.
RS232 Communication	Control input,	Used for external alarms input/output.

Serial Port	Status output	
RJ45 Protection Port	None	Since this is N/A for FIPS
RJ45 Wayside Channel Port	Data I/O	64 Kbps used for Wayside Channel communication.
Engineering Order Wire Port	Data I/O	64 Kbps interface for the data sent to the radio in encrypted form.

The following table presents the FibeAir 1500P™ Secure Basic Indoor Unit's LED indicators.

Please note that the LEDs do not provide a unique identifier to the State or Problem, but rather provide the operator with an indication that they should check the current alarm/alarm log for further details.

LED location	LED name	Color/ Description
Drawer	POWER	Green LED indicates that the device is powered on. Gray LED indicates that the device is powered off. During normal operation, the LED is green.
Drawer	SIG	Indicates the T1 traffic status. During normal operation, the LED is green or gray (if no T1 port is enabled). Red LED indicates about: • LOS on T1 port • Excessive BER (EXBER) on T1 port Yellow LED indicates about: • Unexpected signal on T1 port • Signal degraded on T1 port Gray LED indicates that no T1 port is enabled.
Drawer	DRAWER	Shows the status of cryptographic module and other system alarm indications. During normal operation, the LED is green. For cryptographic "Module Show Status" see the table in the chapter 2.2 Services. Other system alarm indications: Red LED indicates about: • Radio Link ID mismatch • Drawer internal power failure Yellow LED indicates about: • Hardware configuration problem • Drawer temperature out of range
Drawer	ODU	Indicates the status of connected ODU. During normal operation is green. Red LED indicates about: • ODU power failure • No signal from ODU

		Yellow LED indicates about: • Transmit or receive level out of range • ODU temperature out of range • Transmit is muted • Drawer – ODU communication failure
Drawer	CBL	Red LED indicates about any communication problems between IDU and ODU. During normal operation, the LED is green.
Drawer	LPBK	Indicates system loopbacks. During normal operation, the LED is gray. Red LED indicates about: • ODU internal loopback • Drawer internal loopback • External or internal loopback on T1 port
Drawer	RADIO	Indicates a problem in the radio interface. During normal operation, the LED is green. Red LED indicates about: • LOF in the radio interface • EXBER in the radio interface Yellow LED indicates that signal is degraded in the radio interface.
IDC	IDC	Shows the status of cryptographic module and other system alarm indications. During normal operation, the LED is green. For cryptographic "Module Show Status" see the table in the chapter 2.2 Services. Other system alarm indications: Red LED indicates about remote communication failure. Yellow LED indicates about IDC hardware problems.
IDC	CH1	Indicates the WSC traffic status. During normal operation, the LED is green or gray (if WSC port is disabled). Red LED indicates about LOC on WSC port. Yellow LED indicates about WSC loopback.
IDC	RMT	Red LED indicates about remote communication failure. During normal operation, the LED is green.

2. Roles, Services, and Authentication

The FibeAir 1500P™ Secure Basic Indoor Unit provides five different roles and a set of services particular to each of the roles. The system will authenticate an operator's identity by verifying his PIN and will then implicitly assign him one of the roles: Monitor, User, Maintenance, or Crypto-officer depending on the password.

2.1 Roles

The roles of the cryptographic module are: Crypto-officer, Maintenance, User and Monitor.

User Role

This role performs the general security services in both encrypted and non-encrypted working mode: general system management (except cryptographic operations), PDH/FE ports configuration and management for transmitting and receiving data, radio resource configuration and management, alarms, performance monitoring, download/upload SW/FW and configuration files. The user role is not allowed to activate the maintenance and Crypto-officer role operations.

Monitor Role

This role permits monitoring of the configurations and status of the FibeAir 1500P™ Secure Basic Indoor Unit. The access policy of this role is read-only for all general security services and configurations in both encrypted and non-encrypted working mode that are accessed by the user role.

Maintenance Role

Authorized for all the operations related to the User role. In addition, it is authorized to perform operations related to the maintenance (loop-backs, clear disk configuration, etc). The maintenance role is not allowed to activate the Crypto officer role operations.

Crypto-officer Role

This role performs the cryptographic initialization and management operations and has all maintenance and user role permissions. The Crypto-officer controls the encryption menu: setting and changing PIN values for all other roles and enabling or disabling encryption mode.

Unauthenticated Role

This role performs FibeAir 1500P™ Secure Basic Indoor Unit management via IP connection by special Ceragon's application (Ceraview).

Authorized for Ceraview application users for some operations, related to Monitor, User and Maintenance roles.

2.2 Services

The following table provides brief descriptions of all the security services supported by the module.

Service name	Service description
Authentication	Each role (monitor, user, maintenance and crypto-officer) must be authenticated by the relevant PIN.
Module self-tests and initialization (during IDC SW reset, IDC/Drawer HW reset, button reset)	At power up (cold or warm) resets all CSPs stored in RAM, clears information about authenticated operators, performs power-up self-tests, and if successful, branches to DH key

<table>
<tr><td></td><td>establishment. After the secret key has been successfully established the module enters its Ready state. This is also the service used to recover from the Error state (if the Drawer/IDC module enters the self-test error state or initial key exchange protocol error state, the FibeAir 1500P™ Secure Basic Indoor Unit is not initialized, and the only way to resume normal operation is to reset or power-on the drawer).</td></tr>
<tr><td>Module Show Status</td><td>Displays indication of module state (Uninitialized, Ready or Error) and the module mode via craft terminal or management application. The module status can be displayed via the current alarm/alarm log via the CeraView application. The state is also indicated via the LEDs on the drawer and IDC front panels:
<table>
<tr><th>State</th><th>Problem</th><th colspan="2">LED</th></tr>
<tr><td></td><td>Power-up self-tests</td><td>IDC</td><td>Drawer</td></tr>
<tr><td>Uninitialized</td><td>SW AES KAT</td><td>Green</td><td>Red</td></tr>
<tr><td>Uninitialized</td><td>SW DSS KAT</td><td>Red</td><td>Green</td></tr>
<tr><td>Uninitialized</td><td>HW AES KAT</td><td>Green</td><td>Red</td></tr>
<tr><td>Uninitialized</td><td>PRNG KAT</td><td>Red</td><td>Green</td></tr>
<tr><td>Uninitialized</td><td>Seed and Seed Key Check</td><td>Red</td><td>Green</td></tr>
<tr><td>Uninitialized</td><td>SW/FW Integrity</td><td>Red</td><td>Green</td></tr>
<tr><td>Uninitialized</td><td>Bypass</td><td>Green</td><td>Red</td></tr>
<tr><td>Uninitialized</td><td>Continuous PRNG</td><td>Red</td><td>Green</td></tr>
<tr><td>Error</td><td>Crypto-officer password validation</td><td>Yellow</td><td>Green</td></tr>
<tr><td></td><td>Conditional self-tests</td><td></td><td></td></tr>
<tr><td>Error</td><td>Seed and Seed Key Check</td><td>Yellow</td><td>Green</td></tr>
<tr><td>Error</td><td>Continuous PRNG</td><td>Yellow</td><td>Green</td></tr>
<tr><td>Error</td><td>Digital Signature Verification</td><td>Yellow</td><td>Green</td></tr>
<tr><td>Uninitialized</td><td>Key Establishment</td><td>Green</td><td>Yellow</td></tr>
<tr><td>Error</td><td>Encryption validation or loss of sync problem</td><td>Green</td><td>Red</td></tr>
<tr><td>Error</td><td>Session key exchange</td><td>Green</td><td>Yellow</td></tr>
<tr><td>Ready</td><td>Change encryption mode off/on (on next reset)</td><td>Green</td><td>Yellow</td></tr>
</table></td></tr>
<tr><td>Radio Resource management</td><td>Display and configure radio parameters including transmitter power, receiver sensitivity and RF channel and frequency. This service does not use a cryptographic algorithm.</td></tr>
<tr><td>Transmit PDH/FE data</td><td>The PDH/FE data from the input interfaces (one FE port, eight T1 ports, WSC, EOW) is multiplexed into proprietary frame and encrypted before sending to the radio.</td></tr>
<tr><td>Receive PDH/FE data</td><td>Received from the radio, PDH/FE data is decrypted and after demultiplexing is sent to the relevant output interface</td></tr>
</table>

	(FE/T1/ WSC/ EOW)
Download FW/SW files	All downloaded SW and FW files are authenticated by digital signature verification key (they must be properly signed by Ceragon).
Configuration changes that request a reinitialization (IP number, in-band, set default configuration).	FibeAir 1500P™ Secure Basic Indoor Unit has the several configuration parameters that can have effect only after HW or SW reset to the IDC or the drawer. During the reset the CSPs and SRDIs are recreated automatically – see Access Control Policy table.
Maintenance related operations	The service is used for HW and SW diagnostics, internal and external traffic loop-backs (the data is encrypted by randomly generated HW session key value stored to FPGA registers when entering the role) and returning to factory defaults.
Zeroize CSP	This service is performed in the following scenarios: - zeroize all CSPs stored in RAM and EEPROM including resetting the passwords to their default values when entering/exiting the maintenance role; - zeroize all PRNG CSPs stored in RAM during IDC SW reset;
Set/Change PIN	Only CO has the authority to set and change authentication PINs. When entering/exiting the maintenance role all PINs are reset to their default values, so each time CO should renew PIN per role.
Set encryption mode	Set encryption mode on/off is authorized only to the CO. The IDU will be initialized in the new working mode after HW reset only.

2.3 Services by Role Policy

The following table lists all the security services and indicates whether an operator in each role can perform that service.

Service name	Monitor	User	Mainten.	Crypto-officer	Unauthent.
Authentication	Yes	Yes	Yes	Yes	No
Module self-tests and initialization (during IDC SW reset, IDC/Drawer HW reset, button reset)	Automatic during power up (button reset only)	Automatic during power up	Automatic during power up	Automatic during power up (including change encryption mode)	Automatic during power up
Module Show Status	Yes	Yes	Yes	Yes	Yes
Radio Resource management	Display only	Yes	Yes	Yes	Yes
Transmit PDH/FE data	Yes	Yes	Yes	Yes	Yes
Receive PDH/FE data	Yes	Yes	Yes	Yes	Yes
Download FW/SW files	No	Yes	Yes	Yes	Yes

Configuration changes that require a reinitialization (IP address, in-band, set default configuration).	No	Yes	Yes	Yes	Yes
Maintenance related operations	No	No	Yes	Yes	Partially
Zeroize CSP	No	No	When entering/exiting the role	No	No
Set/Change PIN	No	No	No	Yes	No
Set encryption mode	No	No	No	Yes	No

2.4 Authentication Mechanisms and Strength

When initialised to operate in FIPS level 2 mode, the FibeAir 1500P™ Secure Basic Indoor Unit supports PIN authentication and role-based authentication. The system enforces a minimum PIN length and maximum number attempts per minute to ensure a secure authentication mechanism.

Operator Authentication

All operator role passwords have at least six alphanumeric characters, which are case sensitive. In this case, the authentication mechanism is much stronger than FIPS 140-2 level 2 requirements for a single attempt.

To achieve the FIPS 140-2 level 2 multiple attempt requirement, the FibeAir 1500P™ Secure Basic Indoor Unit limits the maximum of attempts per minute. The craft terminal access using serial RS-232 communication (19200 bit/sec baud rate) complies with this requirement. The 19200 bit/sec baud rate equates to approximately 400 authentications per second, which is less than the ~9466 authentications per second required to violate the requirement.

Firmware and Software Authentication

The FibeAir 1500P™ Secure Basic Indoor Unit authenticates firmware and software downloads by using an Approved authentication technique. The system only allows downloading digitally signed (by Ceragon) firmware and software files. Each file should have a special digital signature, which is verified by RSA Digital Signature Verification Key as part of the download process. Download of unauthorized files will fail, with a suitable alarm indication. The system will continue working with previously downloaded and verified files without any traffic disruption or any other changes.

3. Secure Operation and Security Rules

In order to operate the FibeAir 1500P™ Secure Basic Indoor Unit product securely, the operator should be aware of security rules enforced by the cryptographic module and should adhere to the physical security rules and secure operation rules required.

The Crypto-officer must know how to configure the system to encryption mode. Once FibeAir 1500P™ Secure Basic Indoor Unit is setup to operate in encryption mode, all secure processes are executed automatically at power-up. The embedded software initiates self-tests, secret key establishment and session key exchange with the remote side of the radio link.

3.1 Security Rules

The security rules enforced by the FibeAir 1500P™ Secure Basic Indoor Unit include both the security rules that Ceragon Networks has imposed and the security rules that result from the security requirements of FIPS 140-2.

Ceragon Security Rules

The following are Ceragon's Security Rules:

1. The default initialization mode of FibeAir 1500P™ Secure Basic Indoor Unit shall be encryption enable mode. The alternative mode is bypass mode (encryption disable mode).
2. The FibeAir 1500P™ Secure Basic Indoor Unit shall perform encryption mode changing as part of power-up initialization.
3. The FibeAir 1500P™ Secure Basic Indoor Unit shall perform the special Crypto-officer PIN test during power-up. The Crypto-officer PIN value should be different from its default value, otherwise a suitable alarm indicates this error.
4. The FibeAir 1500P™ Secure Basic Indoor Unit shall perform session key exchange at 7.5-minute intervals. These key exchanges are not required by security level 2 and should be considered as continuous pseudo random generator tests from FIPS 140-2 point of view. It also increases the security of the system.
5. The FibeAir 1500P™ Secure Basic Indoor Unit shall never output the Diffie-Hellman secret key or HW session keys.
6. The FibeAir 1500P™ Secure Basic Indoor Unit shall use a random generated value for seed key derivation (used for further PRNG ANSI X.931 Appendix A section A.2.4 implementation).
7. During the IDC SW reset, the FibeAir 1500P™ Secure Basic Indoor Unit shall zeroize the PRNG related CSPs. The secret and HW keys that were used previously, are kept safe.
8. During either the IDC or the drawer HW reset, the FibeAir 1500P™ Secure Basic Indoor Unit shall zeroize all CSPs, excluding authentication PINs.

FIPS 140-2 Security Rules

The following are security rules that stem from the requirements of FIPS PUB 140-2. The module enforces these requirements when initialized in FIPS level 2 mode:

1. When initialized to operate in level 2 mode, the FibeAir 1500P™ Secure Basic Indoor Unit only supports FIPS-approved cryptographic algorithms.
2. The FibeAir 1500P™ Secure Basic Indoor Unit shall employ the FIPS-approved pseudo random number generator specified in ANSI X.931 Appendix A section A.2.4 whenever generating keys.
3. The FibeAir 1500P™ Secure Basic Indoor Unit shall provide role-based authentication of operators by verifying the operator's PIN.
4. When initialized to operate in FIPS level 2 mode, the FibeAir 1500P™ Secure Basic Indoor Unit shall only allow internal generation of cryptographic keys.

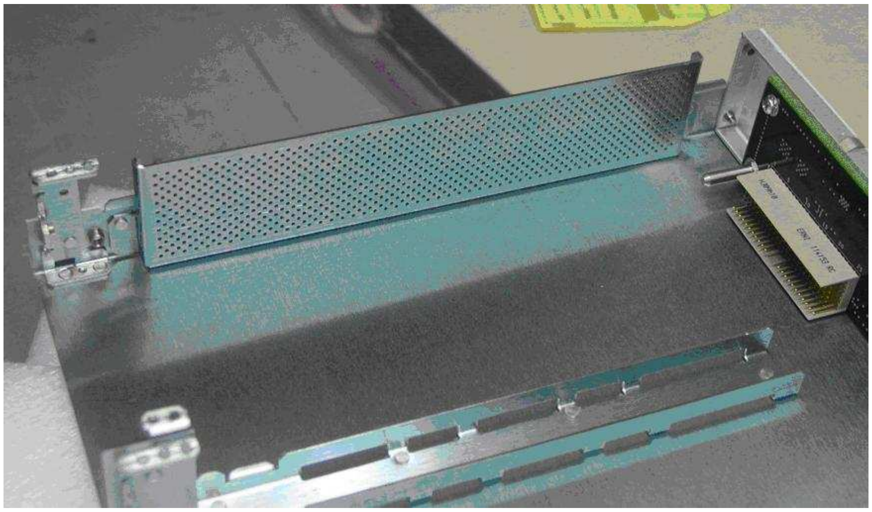
The FibeAir 1500P™ Secure Basic Indoor Unit shall not allow input of cryptographic keys in both plaintext or chipper form.

5. When initialized to operate in FIPS level 2 mode, the FibeAir 1500P™ Secure Basic Indoor Unit shall only allow password authentication of operators. The FibeAir 1500P™ Secure Basic Indoor Unit shall not allow entry of plaintext PINs for authentication.
6. The FibeAir 1500P™ Secure Basic Indoor Unit shall provide the Crypto-officer the capability to zeroize the plaintext CSPs contained within the system. See for reference the CSPs and SRDIs table.
7. The FibeAir 1500P™ Secure Basic Indoor Unit shall allow loading and running of only digitally signed files added by Ceragon firmware and software.
8. The FibeAir 1500P™ Secure Basic Indoor Unit shall perform self-tests and known-answer tests of all cryptographic components during power-up. If upon any failure, the unit becomes non-functional: FE ports are shut down, AIS is sent to the line (T1 ports) and radio directions, no signal in EOW.
9. The FibeAir 1500P™ Secure Basic Indoor Unit shall validate the on-board firmware and software files using 32-bit CRC checksum algorithm.
10. The FibeAir 1500P™ Secure Basic Indoor Unit shall perform conditional self-tests. See for reference Self-tests chapter.
11. The FibeAir 1500P™ Secure Basic Indoor Unit shall zeroize all CSPs (including authentication PINs) when entering or exiting the maintenance role.

3.2 Physical Security Rules

The physical security of the cryptographic module is designed to meet requirements of FIPS 140-2 level 2. The physical boundary of the module is the same as the physical boundary of the FibeAir 1500P™ Secure Basic Indoor Unit: the hard metal enclosure with airflow mesh holes.

In order eliminate visibility to underlying circuitry, the IDU enclosure is opaque. The mechanical baffling plates must be used and installed in order to comply with the FIPS mode of operation. This baffling installation is performed at the vendor's (Ceragon) facilities, and the module will come with this baffling pre-installed. These plates with special ventilation holes (on the IDU chassis) close the view of the inner components via the airflow mesh holes, see the figures below.



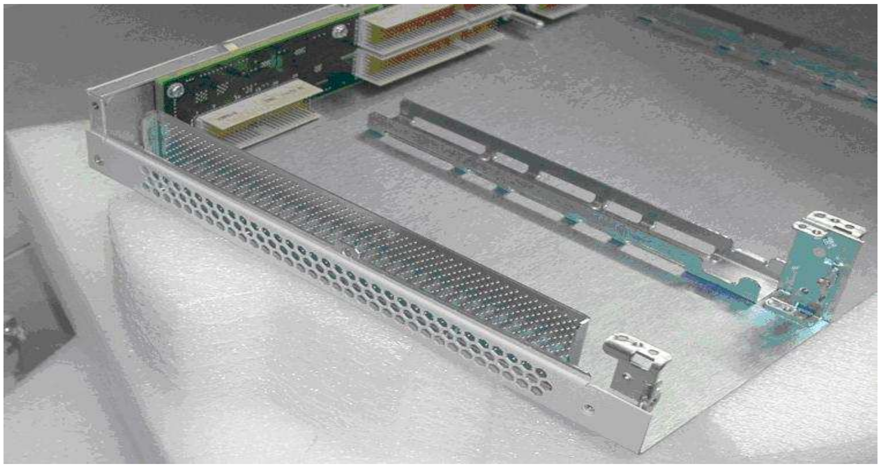
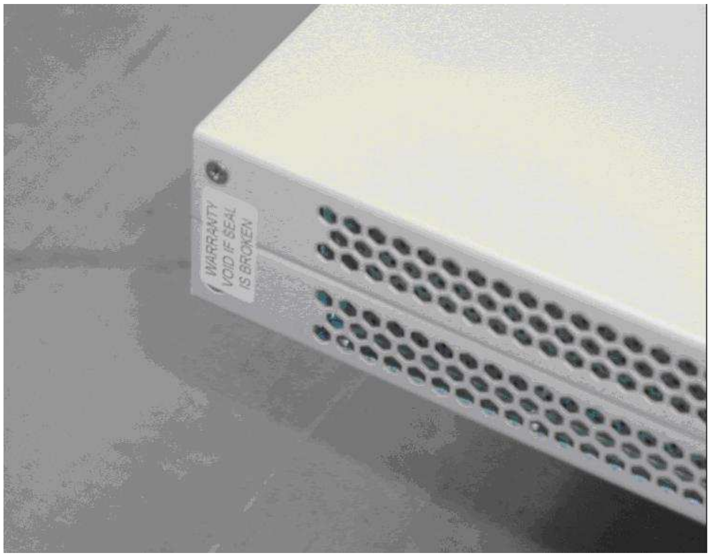


Figure 3. FibeAir 1500P^{TM} Secure Basic Indoor Unit's Baffling Plates

The eight tamper evident stickers are placed on the IDC and drawer screws, bottom and front panels, for detection of tamper to the chassis, and the attempt of IDC/drawer removal. For sticker placements see the figure 2 and the figures below.



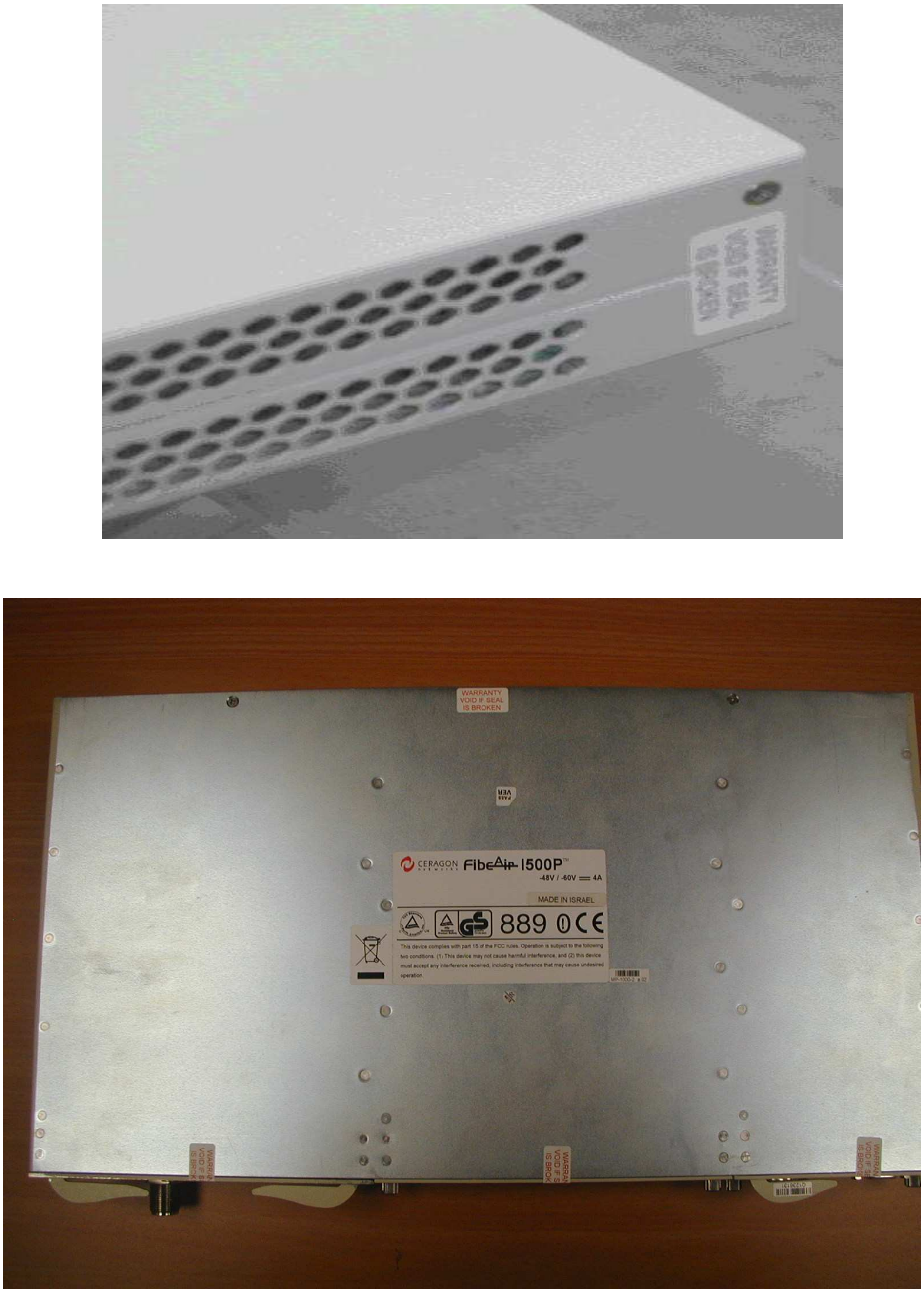


Figure 4. FibeAir 1500P^{TM} Secure Basic Indoor Unit's Sticker Placements

All maintenance operations that request chassis disassembling or IDC/drawer removal must be carried out at Ceragon's facility. After the maintenance operation is completed, new stickers will be placed.

The recommended inspection process is provided in the following table:

Physical security mechanism	Recommended frequency of inspection	Inspection details
Tamper evident stickers	Once per month	Examine stickers for signs of removal, replacement or tearing. The stickers location: 2 stickers are placed on each side of the chassis on the seam (right and left side); 3 stickers on the bottom side front of the chassis and wrap around the corner; 1 sticker on the bottom side rear of the chassis on the middle screw; 1 sticker on the front panel of the drawer that locks the front panel; 1 sticker on the front panel of the IDC that closes the open slot on the upper left hand side.
Hard opaque production grade enclosure	Once per month	Examine enclosure for signs of any new openings that might have been cut into the device

3.3 Multi-Chip Standalone

The FibeAir 1500P™ Secure Basic Indoor Unit module is being validated as a "multi-chip standalone" cryptographic module. The physical boundary of the FibeAir 1500P™ Secure Basic Indoor Unit cryptographic module is the same as the physical boundary of the device.

3.4 Secure Operation Initialization Rules

The FibeAir 1500P™ Secure Basic Indoor Unit provides the following FIPS-approved cryptographic algorithms:

Algorithm Type	Key Sizes/Modes	FIPS-approved/Certificate
Signature Algorithms		
RSA (ANSI X9.31)	1024-bit modulus	Yes (Certificate #141)
Symmetric Algorithms		
Firmware AES	256-bit key ECB	Yes (Certificate #396)
HW AES	256-bit key, OFB 128 bit	Yes (Certificate #395)
Asymmetric Algorithms		
Diffie-Hellman Key Establishment	Secret key 256-bit size (derived from 1024 bits)	Allowed for use in a FIPS-approved mode (Annex D)
Hashing Algorithms		
SHA-1	Byte-oriented	Yes (Certificate #467)
RNG Algorithms		

PRNG ANSI X.931 standard	Seed 128 bit, Seed key 256 bits, 128-bit random output	Yes (Certificate #192)
CRC Algorithms		
CRC 32		Yes

The following applications are used in the FibeAir 1500P™ Secure Basic Indoor Unit access, control and management:

1. Craft terminal application (according to comm. port connected). This application is used by all roles (except Unauthenticated role) with the relevant access permissions.
2. The appropriate version of Ceragon's management application (CeraView) depending on OS of the host (Windows or Unix) is meant for the Unauthenticated role only. This application should be installed using the installation CD.

The FibeAir 1500P™ Secure Basic Indoor Unit supports both FIPS-approved (encryption enabled) and non-approved (encryption disabled) operation modes. The default mode is encryption enabled. While operating in this mode, the Crypto-officer should complete the following initialization rules to ensure FIPS level 2 compliance:

1. Power up the FibeAir 1500P™ Secure Basic Indoor Unit
2. Establish the RS232 connection to the IDU via the serial port.
3. Open a terminal application (according to comm. port connected).
4. When the system enters the Un-initialized State (because of the Crypto-officer PIN is in the default sate), the operator should authenticate to the system using the default Crypto-officer PIN.
5. Upon entering the Uninitialized Crypto-officer state, the operator should go through the terminal menus: Configuration/IDC/Advanced/Passwords and change all PINs (per role) from their default values: [six to eight case sensitive, alphanumeric characters]. A Crypto-officer should avoid setting the same PIN values for different roles.
6. Save and exit the Crypto-officer role.
7. Power reset the system.
8. When the same operations are completed for the remote IDU of radio link, enter the system using a user PIN that previously had been changed from its default value, and configure all RF parameters (frequencies, channel, transmit and receive levels and others).

The current status of operating mode (encryption enabled or disabled) can be determined by each role performing the following steps:

Via craft terminal:

1. Establish the RS232 connection to the IDU via the serial port.
2. Open a terminal application (according the comm. port connected).
3. Login with the relevant PIN to the terminal menu.
4. Go through the terminal menus: Configuration/Right Drawer/Advanced/General/Encryption Configuration.

5. There are two fields to check for encryption status: "Encryption mode" and "Current encryption mode".
    - "Encryption mode" field indicates the last value set.
    - "Current encryption mode" field indicates the actual working mode.

    For example, if "Encryption mode" field value is enabled and "Current encryption mode" field value is disabled, the system will switch the mode to enable (last value that was set) only after power reset.
6. Check the status of encryption: Encryption mode and Current encryption mode values.

Via management application:

1. The appropriate version of Ceragon's management application (Ceraview) should be installed on the host.
2. Establish an Ethernet connection to the IDU via the management port.
3. Open CeraView application according to the IDU IP address.
4. Login with Ceraview application user's PIN.
5. The status can be checked either by clicking on the "AES" inscription on the drawer's application picture or via application pull-down menu: File/AES/Right.

4. Definition of SRDIs Modes of Access

This section specifies the FibeAir 1500P™ Secure Basic Indoor Unit's Security Relevant Data Items as well as the access control policy enforced by the system.

4.1 Cryptographic Keys Management, CSPs and SRDIs

While operating in a level 2 FIPS-compliant manner, the FibeAir 1500P™ Secure Basic Indoor Unit contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
Seed Key	This is a 256-bit length random value automatically generated during power-up, stored to RAM. Used for PRNG ANSI X.931 algorithm (Appendix A section A.2.4) implementation. Zeroized* when entering/exiting the maintenance role.
Seed Value	This is a 128-bit random value, stored to RAM. Used for PRNG ANSI X.931 algorithm (Appendix A section A.2.4) implementation. Zeroized after use – after PRNG initiation.
Prime	This number has a length of 1024 bits and is stored to RAM. The prime number is needed for the DH algorithm (for each DH key exchange initialized process). Zeroized after use –

	after creating the secret key. See also Annex A, section 9.2
D-H Private Key	The private key is PRNG (ANSI X.931 Appendix A section A.2.4) 512-bit length output and used for the secret key creation. Is stored to RAM and zeroized after use – after creating the secret key. See also Annex A, section 9.3
Tx D-H Public Key	The public key is a calculated shared value, which is transmitted to the remote side of the radio link and used for a secret key creation during the Diffie-Hellman establishment. Stored to RAM and zeroized after use – after creating the secret key.
Rx D-H Public Key	The public key is a calculated shared value, which is received from the remote side of the radio link and used for a secret key creation during the Diffie-Hellman establishment. Stored to RAM and zeroized after use – after creating the secret key.
Tx D-H Secret key	This 256-bit length value is a result of a key establishment protocol (calculated value), which is stored in plaintext in the hardware. Secret key will encrypt the HW session key before sending to the remote side of the radio link - this encryption will be done by SW AES core. Zeroized when entering/exiting the maintenance role.
Rx D-H Secret key	This 256-bit length value is a result of a key establishment protocol (calculated value), which is stored in plaintext in the hardware. Secret key will decrypt the HW session key after receiving from the remote side of the radio link - this decryption will be done by SW AES core. Zeroized when entering/exiting the maintenance role.
Tx HW Session key	This is a PRNG (ANSI X.931 Appendix A section A.2.4) 256-bit length output used for encryption of the data to be transmitted. Stored in RAM and loaded in the local FPGA registers in plaintext form. In addition, this value is sent in encrypted form (encrypted with a secret key) to the remote side of radio link. Zeroized after use – after sending to remote side and loading to local MUX FPGA, or when entering/exiting the maintenance role.
Rx HW Session key	This is a PRNG (ANSI X.931 Appendix A section A.2.4) 256-bit length output used for decryption of the data to be received. Stored in RAM and loaded in the local FPGA registers in plaintext form. This value is received in decrypted form (decrypted with a secret key) from the remote side of radio link. Zeroized after use – after receiving from the remote side and loading to local MUX FPGA, or when entering/exiting the maintenance role.
RSA Digital Signature Verification Key	The public key for the verification process will be configuration value stored in plaintext in the hardware. This key is used for verification of application/firmware files that will be downloaded to the IDU.
Crypto-officer PIN	At least 6 characters, case sensitive, alphanumeric string of

	the Crypto-officer. Stored in plaintext in the hardware. Zeroized to the default value when entering/exiting the maintenance role. The Crypto-officer PIN will be checked for deviating from its default value upon each power up (a suitable alarm will be initiated if the value is not the default)
Maintenance PIN	At least 6 characters, case sensitive, alphanumeric string of the Maintenance operator. Stored in plaintext in the hardware. Zeroized to the default value when entering/exiting the maintenance role.
User PIN	At least 6 characters, case sensitive, alphanumeric string of the User. Stored in plaintext in the hardware. Zeroized to the default value when entering/exiting the maintenance role.
Monitor PIN	At least 6 characters, case sensitive, alphanumeric string of the Monitor user. Stored in plaintext in the hardware. Zeroized to the default value when entering/exiting the maintenance role.

* Zeroization means loading a randomly generated number value.

4.2 Clear CSPs

The purpose of the CSP clearing is to zeroize (set to 0 or regenerate) the secured elements according to the FIPS-140-2 level 2 requirements. The following elements are zeroized:

CSP	Location	When is cleared	Who does it
Seed Key	RAM	Cleared when entering/exiting the maintenance role.	Maintenance user
Seed Value	RAM	Cleared after PRNG initiation.	SW, after PRNG initiation
Prime	RAM	Cleared after creating the secret key.	SW, after creating the secret key.
D-H Private Key	RAM	Cleared after creating the secret key.	SW, after creating the secret key.
Tx D-H Public Key	RAM	Cleared after creating the secret key.	SW, after creating the secret key.
Rx D-H Public Key	RAM	Cleared after creating the secret key.	SW, after creating the secret key.
Tx D-H Secret key	HW registers	Cleared when entering/exiting the maintenance role.	Maintenance user
Rx D-H Secret key	HW registers	Cleared when entering/exiting the maintenance role.	Maintenance user
Tx HW Session key	RAM, MUX FPGA	Cleared after sending to remote side and loading to local MUX FPGA, or when entering/exiting the maintenance role.	SW, after loading to local MUX FPGA or by maintenance user
Rx HW Session key	RAM, MUX FPGA	Cleared after receiving from the remote side and loading to local	SW, after loading to local MUX FPGA or by

		MUX FPGA, or when entering/exiting the maintenance role.	maintenance user
RSA Digital Signature Verification Key	HW registers	This key is used for verification of application/firmware files that will be downloaded to the IDU.	Is updated by manufacturer when another pair of RSA digital signature keys (sign/verification) is generated.
Crypto-officer PIN	HW registers	Cleared to the default value when entering/exiting the maintenance role. Can be set by CO.	Crypto-officer, maintenance user
Maintenance PIN	HW registers	Cleared to the default value when entering/exiting the maintenance role. Can be set by CO.	Crypto-officer, maintenance user
User PIN	HW registers	Cleared to the default value when entering/exiting the maintenance role. Can be set by CO.	Crypto-officer, maintenance user
Monitor PIN	HW registers	Cleared to the default value when entering/exiting the maintenance role. Can be set by CO.	Crypto-officer, maintenance user

4.3 Access Control Policy

FibeAir 1500P™ Secure Basic Indoor Unit allows controlled access to the SRDIs contained within it. The following table defines the access that an operator or application has to each SDRI while operating the IDU in a given role performing a specific service (command). The permissions are categorized as a set of four separate permissions: automatically created after reset (a), zeroize (d - automatically deleted or set default value), write (w), use (u). If no permission is listed, an operator outside the IDU has no access to the SRDI.

FibeAir 1500P™ Secure Basic Indoor Unit **SRDI/Role/Service Access Policy**	Security Relevant Data Item	Seed Key	Seed Value	Prime	D-H Private Key	Tx D-H Public Key	Rx D-H Public Key	Tx D-H Secret key	Rx D-H Secret key	Tx HW Session key	Rx HW Session key	RSA Digital Signature Verification Key	Crypto-officer PIN	Maintenance PIN	User PIN	Monitor PIN
Role/Service																
Monitor																
Authentication (via PIN)																u
Module Show Status																
Radio resource management																
Transmit PDH/FE data (encrypted)								u		u						
Receive PDH/FE data (encrypted)									u		u					
Button reset		a	a	a	a	a	a	a	a	a	a					
User role																
Authentication (via PIN)															u	
Module Show Status																
Radio resource management																
Transmit PDH/FE data (encrypted)								u		u						
Receive PDH/FE data (encrypted)									u		u					
IDC/Drawer HW reset, button reset		a	a	a	a	a	a	a	a	a	a					
IDC SW reset		a	a	a												
Download FW/SW files												u				
Change IP address (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Change In-band Configuration (requests HW reset)		a	a	a	a	a	a	a	a	a	a					

Maintenance role																
FibeAir 1500P™ Secure Basic Indoor Unit **SRDI/Role/Service Access Policy**	Security Relevant Data Item	**Seed Key**	**Seed Value**	**Prime**	**D-H Private Key**	**Tx D-H Public Key**	**Rx D-H Public Key**	**Tx D-H Secret key**	**Rx D-H Secret key**	**Tx HW Session key**	**Rx HW Session key**	**RSA Digital Signature Verification Key**	**Crypto-officer PIN**	**Maintenance PIN**	**User PIN**	**Monitor PIN**
Authentication (via PIN)		d	d	d	d	d	d	d	d	d	d		d	u d	d	d
Module Show Status																
Radio resource management																
Transmit PDH/FE data (encrypted)								u		u						
Receive PDH/FE data (encrypted)									u		u					
IDC/Drawer HW reset, button reset		a	a	a	a	a	a	a	a	a	a					
IDC SW reset		a	a	a												
Download FW/SW files												u				
Change IP address (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Change In-band Configuration (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Maintenance related operations.		a	a	a	a	a	a	a	a	a	a					
Zeroize CSP (when entering/exiting the role)		d	d	d	d	d	d	d	d	d*	d*		d	u d	d	d
Crypto-officer Role																
Set/Change PIN													u w	w	w	w
Module Show Status																
Radio resource management																
Set encryption mode (requests HW reset)		a	a	a	a	a	a	a	a	a	a					

Transmit PDH/FE data (encrypted)								u		u						

FibeAir 1500P^{TM} Secure Basic Indoor Unit **SRDI/Role/Service Access Policy**	**Security Relevant Data Item**	**Seed Key**	**Seed Value**	**Prime**	**D-H Private Key**	**Tx D-H Public Key**	**Rx D-H Public Key**	**Tx D-H Secret key**	**Rx D-H Secret key**	**Tx HW Session key**	**Rx HW Session key**	**RSA Digital Signature Verification Key**	**Crypto-officer PIN**	**Maintenance PIN**	**User PIN**	**Monitor PIN**
Receive PDH/FE data (encrypted)									u		u					
IDC/Drawer HW reset, button reset		a	a	a	a	a	a	a	a	a	a					
IDC SW reset		a	a	a												
Download FW/SW files												u				
Change IP address (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Change In-band Configuration (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Maintenance related operations		a	a	a	a	a	a	a	a	a	a					
Unauthenticated Role																
Authentication (optional)																
Module Show Status																
Radio resource management																
Transmit PDH/FE data (encrypted)								u		u						
Receive PDH/FE data (encrypted)									u		u					
IDC/Drawer HW reset, button reset		a	a	a	a	a	a	a	a	a	a					
IDC SW reset		a	a	a												
Download FW/SW files												u				
Change IP address (requests HW reset)		a	a	a	a	a	a	a	a	a	a					
Maintenance related operations.		a	a	a	a	a	a	a	a	a	a					

FibeAir 1500P™ Secure Basic Indoor Unit **SRDI/Role/Service Access Policy**	**Security Relevant Data Item**	**Seed Key**	**Seed Value**	**Prime**	**D-H Private Key**	**Tx D-H Public Key**	**Rx D-H Public Key**	**Tx D-H Secret key**	**Rx D-H Secret key**	**Tx HW Session key**	**Rx HW Session key**	**RSA Digital Signature Verification Key**	**Crypto-officer PIN**	**Maintenance PIN**	**User PIN**	**Monitor PIN**
Change In-band Configuration (requests HW reset)		a	a	a	a	a	a	a	a	a	a					

* Zeroization means loading a randomly generated number value.

5. Operational Environment

The module operates in a *limited operational environment*. The module only supports the loading of digitally signed code using RSA. Any loading of invalidated code invalidates the FIPS 140-2 validation. Given the limited operational environment, the requirements of FIPS-140-2 section 4.6.1 (Operating system requirements) do not apply.

6. Electromagnetic Interference and Compatibility

For security level 2 the cryptographic module shall conform to EMI/EMC requirements, specified by 47 Code of Federal Regulations, part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e. for business use). The FibeAir 1500P™ Secure Basic Indoor Unit has been tested and certificated to FCC Part 15: 2002 Class B, where the test conditions are more demanding than for Class A, therefore the FibeAir 1500P™ Secure Basic Indoor Unit complies to the standard FIPS 140-2. The device is labeled in accordance with FCC regulations.

7. Self-tests

This section describes the Power-up Self-tests and the Conditional Self-tests supported by the module.

7.1 Power-Up Tests

The following tests have to be completed during the FibeAir 1500P™ Secure Basic Indoor Unit power-up:

Test name
Software AES KAT
Software Digital Signature KAT
Seed and Seed Key Check
Hardware AES KAT
Approved PRNG KAT
Software/firmware files integrity test
Hardware Bypass self-test
Crypto-officer password validation

In case of any test (except Crypto-officer password validation) failing the system enters the Error state, no cryptographic operation is performed and all data output is inhibited: FE ports are shut down, AIS is sent to the line (T1 ports) and radio directions, no signal in EOW. The module zeroizes all critical security parameters stored in RAM and clears all remembered authentication results. The only way to resume the module initialization is via HW reset of the drawer upon re-initiation of power-up self-tests.

The Crypto-officer password should be different from its default value, otherwise a suitable alarm indicates this error (see chapter 3.1 Security Rules and the table in chapter 2.2 Services).

7.2 Conditional Tests

The following table lists the conditional self-tests that are performed by the module.

Test Name
Software/Firmware Digital Signature verification
Hardware Bypass self-test
Seed and Seed Key Check
Continuous PRNG self-test

Software/Firmware Digital Signature verification and Hardware Bypass self-tests are executed as user command requests for SW/FW download and switching the encryption mode. Continuous PRNG self-tests are performed internally.

As a conditional self-test, Seed and Seed Key Check is executed when reseeding the FIPS-approved PRNG in case of entering/exiting the maintenance role.

Encryption mode enabling and disabling requires a drawer power reset, so that conditional Hardware Bypass self-tests are always a part of the relevant power-up self-test.

During the tests triggered by the encryption mode switch, only the AIS and idle FE packets are sent to the radio direction.

8. Mitigation of Other Attacks

This Section is not applicable.

9. Annex A: Key specification

9.1 Seed Key and Seed Value

The seed key K (256 bit) is generated at power up or by CSPs clearing. It is used to generate a new seed value V (128 bit) during power up, CSPs clearing or whenever a new random number generated is required.

9.2 Prime

The Prime is generated and checked for primality each time in the following manner:

1. Generate random number according to the *Generate128bitRandom* algorithm which is based on X9.31 standard.
2. Test if this value is prime, using Miller-Rabin Probabilistic Primality Test technique.
3. If the number is prime then return it, otherwise go to step 1.

9.3 Diffie-Hellman Private Key generation

The private key of the D-H is generated using the *Generate128bitRandom* algorithm which is based on the X9.31 standard.