# *3e Technologies International, Inc.*
# FIPS 140-2
# Non-Proprietary Security Policy

# 3e-010F-A-2 Cryptomodule and 3e-010F-C-2 Cryptomodule

April 2006

Document Version 1.1

# TABLE OF CONTENTS

# 1. Introduction

## 1.1 Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International 3e-010F-A-2 Cryptomodule and 3e-010F-C-2 Cryptomodule (Software Versions: 3e-010F-A-2 Version 2.0 Build 18 and 3e-010F-C-2 Version 2.0 Build 15) for Windows, hereafter known as the Crypto Clients. The target of FIPS 140-2 validation is a WLAN client comprised of either the 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software. The difference between the clients is in the drivers related to the supported hardware. The 3e-010F-C-2 supports Intel PRO/Wireless 2200BG and 2915ABG cards, and the 3e-010F-A-2 supports WLAN cards based on the Atheros AR5001X+ and AR5002X chipsets. Other than the drivers needed to work with the specific cards, the clients are functionally identical. The 3e-010F-C-2 or 3e-010F-A-2 Crypto Client Software supports Windows 2000 and Windows XP (Home and Professional). The Crypto Client provides standard 802.11a/b/g wireless access along with enhanced protection through a variety of cryptographic features, providing a high level of security for wireless environments. If encryption is desired for the WLAN, different encryption can be employed depending on the mode selected. In FIPS 140-2 mode (highly secure), encryption can be set for None, Static AES, Static TDES, Dynamic Key Exchange and WPA2 Enterprise and Personal (AES-CCMP). In non-FIPS mode, you can select None, Static AES, Static TDES, Dynamic Key Exchange, Static WEP, WPA-Enterprise and Personal (TKIP or AES-CCMP) and WPA2-Enterprise and Personal (TKIP or AES CCMP). The Configuration Utility provides an intuitive user interface to configure, manage and use various features. The administrator can configure up to 10 separate profiles. Each profile consists of various wireless configuration parameters like:

Security Mode (FIPS or non-FIPS mode)
SSID
Card type (802.11a/b/g)
Wireless authentication type
Encryption (AES, TDES, DKE, AES-CCMP) and related keys or certificate.
Power level
Transmit rate.

The user interface also provides a Site Survey tool. The FIPS 140-2 mandated Self test suite can also be invoked from the GUI. The Radio state can also be controlled.

The following security modules have been implemented in the Crypto Client:

AES (128/192/256 bit)
TDES (192 bit)
AES-CCMP
TKIP
WEP
802.1x/EAP-TLS for authentication
WPA

WPA2/802.11i

The Crypto Clients use an approved RNG as per FIPS 186-2 appendix 3.1 for generation of random data used during EAP-TLS and WPA2 session key negotiation.

This software is intended to run on Windows Based Client devices such as laptop computers, PDAs, Network Capable Application Processors(NCAP), other embedded devices running the Windows. This software was created to communicate with Wireless APs which support encryption such as the 3e-525A-3 Wireless Access Point designed and manufactured by 3eTI. This policy was created to satisfy the requirements of FIPS 140-2 Level 1. This document defines 3eTI's security policy and explains how Crypto Client software meets the requirements outlined in the FIPS 140-2 standard.

The cryptographic module security policy consists of a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard. Please refer to FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules* available on the NIST website at http://csrc.nist.gov/cryptval/.

## 1.2 Definition

The Crypto Client is a set of software components and utilities. The Crypto Client operates in one of four modes, Bypass, AES Encryption, TDES Encryption, and AES-CCM Encryption/Integrity. The cryptographic boundary of the Crypto Client is defined as in Figure 1. Crypto Client is software running on a device within a Windows Operating Environment. All software components listed outside the Cryptographic Boundary are excluded from the security requirements.

The Crypto Client has three main components: (a) WinSupp Service, (b) Management Subsystem – User Interface, and (c) Driver. Refer to Figure 1.

3e-010F-A-2 includes the files:

CcsAthCfg.exe
AepAthLib32.dll
AepAthSsl32.dll
CcsAthCrypt.dll
WAthSupp.exe
CcsAthN51.sys

3e-010F-C-2 include the files:

CcsCx2Cfg.exe
AepCx2Lib32.dll
AepCx2Ssl32.dll
CcsCx2Crypt.dll
WCx2Supp.exe

CcxCx2N50.sys/CcsCx2N51.sys

The Crypto-Client contains logical interfaces to transfer data, control, and status through the cryptographic boundary. Refer to Figure 1 with interfaces lettered in red.

A. Logical interface to launch GUI by double clicking the GUI System Tray icon or selecting "Crypto Client Utility" from the System Tray menu.

B. Logical interface from Microsoft Network Device Interface Specification (NDIS 5.0 for Windows 2000 and 5.2 for XP, to the Crypto Client DRIVER. NDIS is a common specification described in Microsoft literature.

C. Logical interface from RawEther API to the Crypto Client WINSUPP and DRIVER.

D. Logical interfaces from Crypto Client WINSUPP to the event log and from the Crypto Client GUI to the event log. The logical interface involves opening the event log file and appending to it.

E. Logical interface from the WLAN-Card to the Crypto Client DRIVER.

F1. Logical interface from the Windows Registry to the Crypto Client DRIVER.

F2. Logical interface from the Windows Registry to the Crypto Client WINSUPP.

F3. Logical interface from the Windows Registry to the Crypto Client GUI.

## 1.3 Scope

This cryptographic module security policy will cover a fair amount of detail about the architecture and rules of operation. This policy will describe access privileges to various types of data by various operators, in various roles performing various services. This shall be accomplished by specifying the security policy in terms of roles, services, and cryptographic keys and CSPs. The following individual policies are described in detail:

- an identification and authentication (I&A) policy,
- an access control policy,
- a physical security policy

FIPS 140-2 Level 1 does not require a specific security policy for mitigation of other attacks except those for which testable requirements are not defined in the standard.

**Identification and Authentication Policy**

This cryptographic module security policy specifies an identification and authentication policy, all roles (e.g., user/administrator and crypto officer) along with associated type of authentication (e.g., role-based etc) and the authentication data required of each role or operator (e.g., password) and the corresponding strength of the authentication mechanism.

**Access Control Policy**
This cryptographic module security policy specifies an access control policy. This specification covers details related to identification the cryptographic keys and CSPs that the operator has access to while performing a service, and the types of access the operator has to the parameters.

The security policy also specifies:

- All roles supported by a cryptographic module,
- All services provided by a cryptographic module,
- All cryptographic keys and CSPs employed by the cryptographic module, including
  - secret, private, and public cryptographic keys (both plaintext and encrypted),
  - authentication data such as passwords or PINs, and
  - other security-relevant information (e.g., audited events and audit data),
- For each role, the services an operator is authorized to perform within that role,
- For each service within each role, the type(s) of access to the cryptographic keys and CSPs.

**Physical Security Policy**
The Crypto Client Driver Subsystem consists of a WLAN Microsoft NDIS Miniport driver which is based on different versions of NDIS specification depending which operating system it is executed on.

For 3e-010F-A-2, both Windows 2000 and Windows XP use NDIS 5.

For 3e-010F-C-2, Windows 2000 uses NDIS 5 while Windows XP uses NDIS 5.1.

The Crypto Client meets all FIPS 140-1 level 1 physical requirements. A conceptual diagram of the Crypto Client is included in Figure 1.

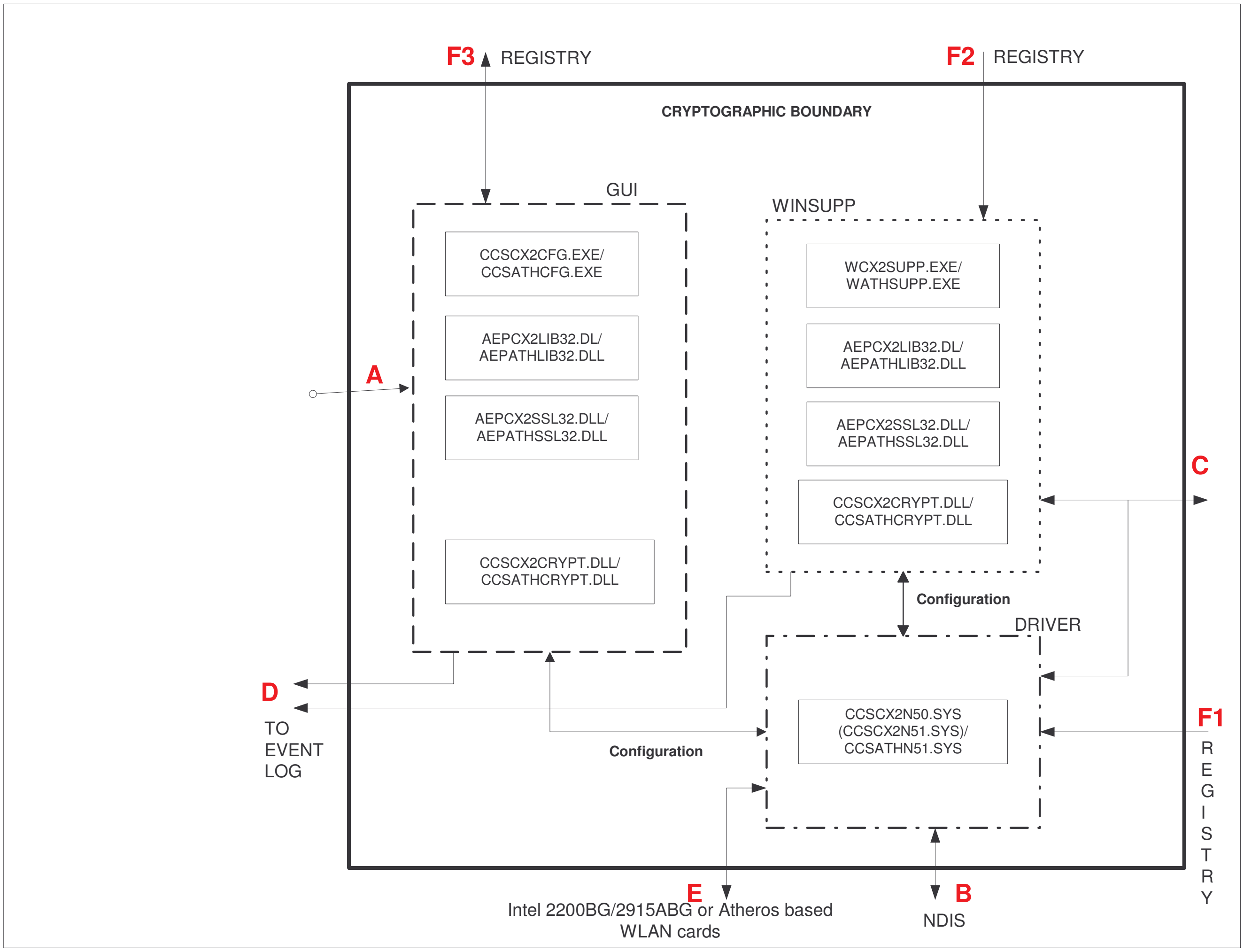


*FIGURE 1 – Crypto Client Subsystem Architecture*

# 2. Roles, Services, and Authentication

## 2.1 Roles

The 3eTI Security Solution supports the following authorized roles for operators:

*Crypto Officer Role*: This role performs cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions). This role exists on the Crypto Client.

*Administrator Role*: This role performs general security services, including cryptographic operations and other approved security functions such a viewing CSP status but without modification privileges.  This role is assumed by the client workstation or device that uses static or dynamic key AES or TDES encryption to communicate wirelessly with the Gateway AP. The Administrator Role is authenticated using username and password. The client authentication is assumed by the correct knowledge of the static key, or for dynamic key encryption, EAP-TLS authentication is performed. This role exists in the Crypto Client.

*Security Server Role*: This role is assumed by the authentication server, which is a self-contained workstation connected to the Wireless Gateway over the Ethernet Uplink WAN port. The security server is employed for authentication and key management activities. This role does not exist on the Crypto Client.

*Gateway User Role*: This role is assumed by the FIPS 140-2 validated 3eTI wireless gateway. The wireless gateway acts as an access point providing a communication link from the wireless Crypto Client to the wired uplink LAN. Details of the 3eTI gateway device are contained in the 3e-DMG security policy. Crypto Client(s) operate in an infrastructure network mode, so every Crypto Client must communicate directly with a gateway device acting in the Gateway User Role. This role is external to the Crypto Client.

## 2.2 Services

The 3eTI Crypto Client provides the following three major services:

### 2.2.1 Crypto Client Windows Service – WinSupp

The Crypto-Client has a Windows service which functions as a Windows Supplicant. Its primary functionality is to provide 802.1x/EAP-TLS authentication with the 3e-Access System (3e-AS). This service meets the following requirements:

- FIPS 140-2 Level 1
- 802.1x/EAP-TLS for authentication
- WPA
- WPA2/802.11i
- Log every attempt to authenticate and the results of authentication.
- Log service starting and stopping

The service is configured to auto-start along with the Windows operating system. It uses RawEther NDIS protocol driver and APIs (3rd party commercially available software) to filter out received 802.1x packets from the Crypto Client NDIS miniport driver for authentication. It uses OpenSSL library to provide EAP-TLS functionality.

### 2.2.2 Crypto Client Management Subsystem

The Crypto Client Management Subsystem consists of a system tray Configuration Utility which provides an intuitive user interface to configure, manage, and use various features.

The Configuration Utility provides two User roles – CryptoOfficer and Admin.

- CryptoOfficer has full access to change any configuration including Cryptographic keys and certificates.
- Admin has limited access to view status of the current connection.

The CryptoOfficer can configure up to 10 location profiles which can allow a user to connect to different WLANs. Each location profile consists of various wireless configuration parameters like:

- Security Mode (FIPS or non-FIPS mode)
- SSID
- Card type (802.11a/b/g)
- Wireless authentication type
- Encryption (AES, TDES, DKE, AES-CCMP) and related keys or certificates.
- Power level
- Transmit rate.

It also provides a Site Survey tool. The FIPS 140-2 mandated Self test suite can also be invoked from this utility. The Radio state can also be controlled.

### 2.2.3 Crypto Client Driver Subsystem

The Crypto Client Driver Subsystem consists of a WLAN Microsoft NDIS Miniport driver which is based on different versions of NDIS specification depending which operating system it is executed on.

> For 3e-010F-A-2, both Windows 2000 and Windows XP use NDIS 5.
>
> For 3e-010F-C-2, Windows 2000 uses NDIS 5 while Windows XP uses NDIS 5.1.

The NDIS driver supports standard 802.11a/b/g features along with the following security features:

- AES
- TDES
- Dynamic Key Exchange (3eTI proprietary and works with 3e Access Systems only)
- WEP
- TKIP
- AES-CCM
- WPA
- WPA2/802.11i

# 3. Cryptographic Design Overview

## *3.1. Software Subsystems and Interfaces*

### 3.1.1. Crypto Client software features summary

- Wireless (802.11a/b/g) interface
  - AES/TDES
  - Open system authentication
  - Seamless roaming (within the same subnet)
  - *Radio on/off*
  - *Lower radio power*
- Dynamic Key Exchange
- Logging to Windows Event Log
- Software upgrade
- Factory default

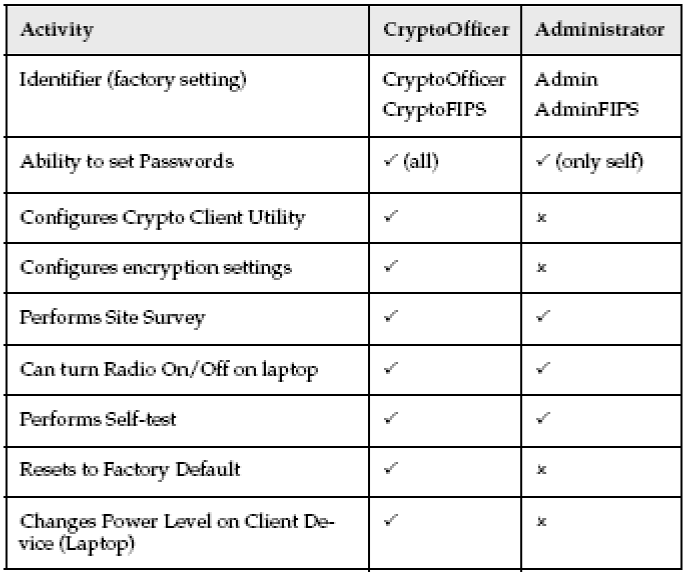
The following cryptographic modules have been implemented in 3eTI Crypto Client:

- AES for wireless (802.11b)
- TDES for wireless (802.11b)
- SHA-1 for POST
- EAP-TLS for authentication

3e-010F-C-2 supports Intel PRO/Wireless 2200BG and 2915ABG cards, while 3e-010F-A-2 supports WLAN cards based on the Atheros AR5001X+, AR5002G and AR5002X chipsets. These cards support standard 802.11 a/b/g implementations to provide the physical communication with the 3e-AS.

**Encryption Utility Configuration**

The CryptoOfficer must now configure the encryption utility to allow the user access to the WLAN. Until the utility has been configured to allow access to the 3e AP, you will not be able to access the WLAN from the particular wireless device you are configuring. There are two types of roles on the secure system: CryptoOfficer and Administrator. The following chart shows the different permissions in respect to the Crypto Client Utility.



| Activity | CryptoOfficer | Administrator |
|---|---|---|
| Identifier (factory setting) | CryptoOfficer<br>CryptoFIPS | Admin<br>AdminFIPS |
| Ability to set Passwords | ✓ (all) | ✓ (only self) |
| Configures Crypto Client Utility | ✓ | × |
| Configures encryption settings | ✓ | × |
| Performs Site Survey | ✓ | ✓ |
| Can turn Radio On/Off on laptop | ✓ | ✓ |
| Performs Self-test | ✓ | ✓ |
| Resets to Factory Default | ✓ | × |
| Changes Power Level on Client Device (Laptop) | ✓ | × |

## 3.2. Roles, Services, and Authentication

### 3.2.1. Security Policy Checklist Tables

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| Crypto Officer | Role-Based | Role id and password |
| Administrator | Role-Based | Role id and password |

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| Userid and password | Minimum 6 characters => 72^6 = 1.39E11 |
| Static Key (TDES or AES) | TDES (192-bits) or AES (128, 192, or 256-bits) |
| CA signature | 128-bit |
| AES CCM Passphrase | Minimum 8 characters => 72^8 = 7.22E14 |
| EAP-TLS | CA signature => 128-bit |

| Role | Authorized Services |
|---|---|
| Administrator or Crypto Officer | TX Power Mode Setting |
| Administrator or Crypto Officer | Launch GUI Self Test |
| Crypto Officer Only | Profile Name Creation |
| Crypto Officer Only | SSID Setting |
| Crypto Officer Only | Restore Crypto Client to factory defaults |
| Crypto Officer Only | Modify encryption keys |
| Crypto Officer Only | Set MAC address filters |
| Crypto Officer Only | View system processes |
| Crypto Officer Only | Perform standard services |
| Crypto Officer Only | Set Transmit Rate |
| Crypto Officer Only | Encryption Type Selection:<br>- None/Bypass<br>- AES (128-bit, 192-bit, 256-bit)<br>- TDES<br>- AES-CCM |
| Crypto Officer Only | Dynamic Key Exchange<br>- Certificate<br>- Key<br>- Certificate Authority<br>- Password<br>- Status |

## 3.3. Cryptographic Key Management

The following is a list of all cryptographic keys and key components used within the module, including zeroization information:

| Type | ID | Storage Location | Form | Zeroizable |
|---|---|---|---|---|
| AES CCM Passphrase 8 to 63 bytes | "AES CCM Passphrase" | Registry | Encrypted AES using "system config AES key" | Y |
| AES Static 128,192, or 256 bit | "static AES key" | Registry | Encrypted AES using "system config AES key" | Y |
| TDES Static 192 bit | "static TDES key" | Registry | Encrypted AES using "system config AES key" | Y |
| AES Dynamic Broadcast 128,192, or 256 bit | "dynamic broadcast AES key" | RAM | Plaintext (inaccessible) | Y |
| TDES Dynamic Broadcast 192 bit | "dynamic broadcast TDES key" | RAM | Plaintext (inaccessible) | Y |
| AES Dynamic Unicast 128,192, or 256 bit | "dynamic unicast AES key" | RAM | Plaintext (inaccessible) | Y |
| TDES Dynamic Unicast 192 bit | "dynamic unicast TDES key" | RAM | Plaintext (inaccessible) | Y |
| AES Static 128 bit | "system config AES key" | Hard coded in source (CCSCONTROL.CPL, CCSDRIVER.SYS, WINSUPP.EXE) | Plaintext, used to encrypt the real static Aes/TDES keys (inaccessible, hard-coded) and passwords | Y |
| HMAC SHA-1 Key | "firmware integrity check and certificate integrity key" | Hard coded in source (CCSCONTROL.CPL, WINSUPP.EXE) | Plaintext (inaccessible, hard-coded) | Y |
| RSA Public Key | "EAP/TLS RSA certificate" | Key File | Plaintext (inaccessible) | Y |
| RSA Private Key | "EAP/TLS RSA private key" | Key File | Plaintext (inaccessible) | Y |
| CryptoOfficer Password | "CO password" | Registry | Encrypted using "system config AES key" | Y |
| Admin Password | "Admin password" | Registry | Encrypted using "system config AES key" | Y |
| Certificate Authority (CA) public key certificate | "CA public key" | Key File | Plaintext | Y |
| AES-CCM Dynamic Groupcast 128 bit | "dynamic groupcast AES-CCM key" | RAM | Plaintext (inaccessible) | Y |
| AES-CCM Unicast 128 bit | "dynamic unicast AES-CCM key" | RAM | Plaintext (inaccessible) | Y |
| AES Static 128 bit | "AP communication AES key" | Hard coded in source (WINSUPP) | Plaintext, used to encrypt/decrypt special communication with AP, example: Power management. (inaccessible, hard-coded) and passwords | Y |
| EAP-TLS Pre-Master Key 48-byte | "dynamic session pre-master key" | RAM | Plaintext (inaccessible) | Y |

**Zeroization Mechanism:** Key Zeroization is performed by writing an all five pattern "55555…" into the Key Data Field being zeroized exactly one time, followed by writing an all A pattern "AAAAA…" into the Key Data Field being zeroized exactly one time, followed by writing an all five pattern "55555…" into the Key Data Field being zeroized exactly one time, followed by writing an all zero pattern “00000…” into the Key Data Field being zeroized exactly one time.

The above mechanism is applicable for keys/CSPs stored in the Registry and the RAM. The hard coded keys are zeroized by deleting the module and formatting the hard drive. The keys that are stored on hard drive in a key file are zeroized by deleting those files and formatting the hard drive.

### 3.3.1. Authentication: EAP-TLS Authentication

The authentication process follows the standard of EAP-TLS protocol. Please refer to RFC-2716 for the details. Here is a short summary of the protocol.

1. When the AP starts the dynamic key service, it listens at the wireless LAN interface.
2. Client sends a EAP-START message to the AP to start the authentication process.
3. AP sends back a EAP-ID request packet to the client.
4. Client replies with its ID.
5. AP forwards the ID packet to the Security Server.
6. Security server sends back EAP-TLS-START message.
7. Client and Server exchanges certificates according to the TLS protocol and authenticate each other. AP just simply passes the network traffic between the client and the server.
8. Once the TLS authentication succeeds, the AP will enter into post-authentication state. If the TLS authentication fails, the AP simply sends a reject message to the client to reject its access to the wireless service.

Note: No encryption is involved so far in the AP. All the encryptions(if any) are done either by the server or the client.

Note: For TLS key transport (RSA encryption/decryption) and signature based authentication, the user should load RSA keys that have modulo sizes in the range of 1024 bits to 4096 bits. With these RSA keys, the key establishment methodology provides between 80 and 150 bits of encryption strength.

## 3.4. Access Control Policy

The Crypto Client maintains and enforces the access control policy for each SRDI stored within the module. These access control policies cannot be changed or modified by any role within the module. The permissions are categorized as a set of three separate permissions: read ( R ), write ( W ), and execute ( E ). If no permission is listed, then the operator cannot access the SRDI. The following table defines the access that an operator has to each SRDI and through which services.

| **3e-010F-A-2 & 3e-010F-C-2 SRDI Roles & Services Access Policy** | **CO – System Configuration** | **CO – Wireless Configuration** | **CO – Service Settings** | **CO – User Management** | **CO – Monitoring / Reporting** | **CO – System Administration** | **AD – System Configuration** | **AD – Wireless Configuration** | **AD – Service Settings** | **AD – User Management** | **AD – Monitoring / Reporting** | **AD – System Administration** | **User Role – Sending Data** | **AS Role – Provides Authentication** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AES CCM Passphrase 8 to 63 bytes | W | | | | | | | | | | | | | |
| AES Static 128, 192, or 256 bit | W | | | | | | | | | | | | | |
| TDES Static 192 bit | W | | | | | | | | | | | | | |
| AES Dynamic Broadcast 128,192, or 256 bit | | | | | | | | | | | | | E | |
| TDES Dynamic Broadcast 192 bit | | | | | | | | | | | | | E | |
| AES Dynamic Unicast 128,192, or 256 bit | | | | | | | | | | | | | E | |
| TDES Dynamic Unicast 192 bit | | | | | | | | | | | | | E | |
| AES Static 128 bit | W | | | | | | | | | | | | | |
| HMAC SHA-1 Key | W | | | | | | | | | | | | E | |
| RSA Public Key | | | | | | | | | | | | | | W |
| RSA Private Key | E | E | E | E | E | E | E | E | E | E | E | E | | W |
| CryptoOfficer Password | W | | | | | | | | | | | | | |
| Admin Password | W | | | | | | | | | | | | | |
| Certificate Authority (CA) public key certificate | | | | | | | | | | | | | | E |
| AES-CCM Dynamic Groupcast 128 bit | | | | | | | | | | | | | E | |
| AES-CCM Unicast 128 bit | | | | | | | | | | | | | E | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AES Static 128 bit | | | | | | | | | | | | | E | |
| EAP-TLS Pre-Master Key 48 byte | | | | | | | | | | | | | | E |