3e Technologies International, Inc.

FIPS 140-2

Non-Proprietary Security Policy

3e-030-2 Security Server Cryptographic Core (Version 3.0)

January 2007

Table of contents

1. INTRODUCTION 2

1.1. PURPOSE 2
1.2. DEFINITION 2
1.3. SCOPE 3

2. ROLES, SERVICES, AND AUTHENTICATION 4

2.1. ROLES AND SERVICES 4
2.1.1. Services 4
2.1.2. Roles 4
2.2. AUTHENTICATION MECHANISMS AND STRENGTH 6

3. SECURE OPERATION AND SECURITY RULES 6

3.1. SECURITY RULES 6
3.2. FIPS MODE OF OPERATION 7
3.3. FIPS POLICY 7
3.4. SECURE OPERATION INITIALIZATION 8
3.4.1. Installing the 3e-030-2 Security Server 8
3.4.2. Configuring the 3e-030-2 Security Server 8
3.4.3. Verifying the Status 10

4. PHYSICAL SECURITY 10

5. SECURITY RELEVANT DATA ITEMS 11

5.1. CRYPTOGRAPHIC ALGORITHMS 11
5.2. SELF-TESTS 11
5.2.1. Power-up Self-tests 11
5.2.2. Conditional Self-tests 12
5.2.3. Critical Functions tests 12
5.3. CRYPTOGRAPHIC KEYS, CSPS AND SRDIS 12
5.4. ACCESS CONTROL POLICY 13

6. MITIGATION OF OTHER ATTACKS 15

GLOSSARY OF TERMS

AP	Access Point
CO	Cryptographic Officer
DH	Diffie Hellman
IP	Internet Protocol
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HTTPS	Secure Hyper Text Transport Protocol
LAN	Local Area Network
MAC	Medium Access Control
PRNG	Pseudo Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRDI	Security Relevant Data Item
SSID	Service Set Identifier
TLS	Transport Layer Security
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1. Introduction

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's 3e-030-2 Security Server Cryptographic Core (Version 3.0), hereafter known as the Security Server. This software is intended to run on Microsoft Windows based computers. This software was created to communicate with the 3eTI Family of Wireless Gateways and Crypto Clients which are 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 3e-030-2 Security Server Cryptographic Core meets the Level 1 FIPS 140-2 requirements.

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 Security Server Cryptographic Core is a software program that runs as a Windows service. It authenticates wireless users when they log onto the network, and distributes dynamic session keys for the user. The Security Server operates in one of two modes, FIPS mode or non-FIPS mode. The cryptographic boundary of the Security Server is defined as in Figure 1. 3e-030-2 Security Server is software running on a computer within a Windows Operating Environment. The module can be run on Windows 2000 Server or Windows 2003 Server. *The Operating System must be configured to run single-user mode (See Section 3)*. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product.

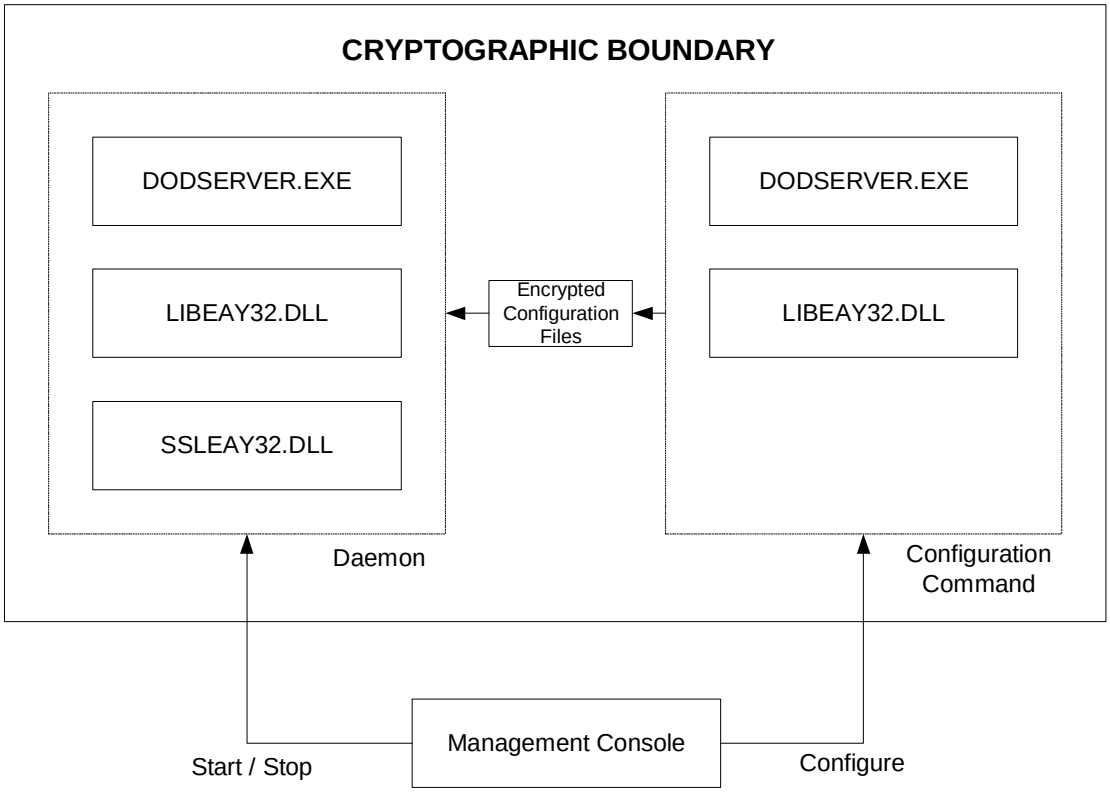


Figure 1 Cryptographic Boundary

3e-030-2 Security Server provides the following major services:

- The Security Server software provides authentication service for wireless users. The Security Server verifies user's digital certificate against a chain of certificate issuers and their corresponding Certificate Revocation List. The Security Server grants user access to the wireless network only upon successful authentication.

- The Security Server software provides dynamic session key exchange for wireless communication. It reduces the security threat for unauthorized users to break the cryptographic key for the wireless network. This is based on the EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) authentication protocols.

1.3. Scope

This document will cover the secure operation of the 3e-030-2 Security Server, including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and describe the Security Relevant Data Items (SRDIs).

2. Roles, Services, and Authentication

The 3e-030-2 Security Server supports four separate roles. The set of services available to each role is defined in this section. The 3e-030-2 Security Server authenticates an operator's role by verifying his PIN.

2.1. Roles and Services

2.1.1. Services

The 3e-030-2 Security Server provides the following major services:

- Wireless client authentication
- Send encrypted wireless session key to Gateway (Access Point)
- The 3e-030-2 allows authorized roles to control server configuration settings, change Crypto Officer Password, and change Crypto Officer Login credentials. The 3e-030-2 services include starting and stopping crypto functions, wireless client authentication (mutual between Client and 3e-030-2), and wireless session key exchange.
- DODSERVER.EXE is a windows service. Its main functionality is to perform EAP-TLS authentication of the 802.11 wireless client. It reads the configuration files at start up time and performe the integrity check and algorithm test. After that the service application will listen on UDP port (1812 defaul) and perform EAP-TLS authentication.
- AESMAIN.EXE is a console application with fixed interface: check user name & password, read/write key-server configuration file, read/write key-wrapper configuration file and change the user password. The file written by Aesmain.exe is AES encrypted.
- The managment console (Out of Cryptographic boundary) is a UI to facilitate the user of the whole application to input and configure the dodserver.exe. It uses the aesmain.exe behind scene to generate the configuration files and controls the start/stop of the dodserver.exe.

2.1.2. Roles

The 3e-030-2 Security Server supports the following authorized roles for operators:

Crypto Officer Role: The Crypto Officer role performs all security functions provided by the 3e-030-2 Security Server. This role performs cryptographic initialization and management functions (e.g., server initialization, configuring operation mode, and modifying server configuration). The Crypto Officer must operate within the Security Rules specified in Sections 3.1 and 3.2. Only one Crypto Officer is defined in the 3e-030-2 Security Server. The Crypto Officer authenticates to the 3e-030-2 Security Server using a password.

Administrator Role: This role performs general 3e-030-2 Security Server operations, including wireless user authentication and dynamic wireless session key exchange. The Administrator Role does not have privilege to modify server configuration settings. The Administrator authenticates to the 3e-030-2 Security Server using a password. Only a single Administrator Role exists.

The follow table outlines the functionalities that are provided by each role:

Role	**Authorized Services**
Crypto Officer Role and Administrator Role	Starting and stopping Security Server
Crypto Officer Role and Administrator Role	Wireless user authentication
Crypto Officer Role and Administrator Role	Send AES encrypted wireless session key to Gateway
Crypto Officer Role only	Server initialization
Crypto Officer Role only	Modifying server configurations

Wireless Client Role (User role): This role is assumed by the wireless client workstation that communicates wirelessly with the wireless Gateway.

The only service available to the Wireless Client role is for the Security Server to authenticate the wireless client, using wireless client's public key certificate. Once authenticated, the wireless client may start to send and receive packets to and from the Gateway.

Gateway Role: This role is assumed by the FIPS 140-2 validated 3eTI Wireless Gateway to communicate wirelessly with the wireless client. The wireless Gateway acts as an access point providing a communication link from the wireless Crypto Client to the wired uplink LAN and the wireless LAN. The wireless Gateway authenticates to the Security Server using a shared secret, using the HMAC SHA1 algorithm. Details of the 3eTI Gateway device are contained in the 3e-DMG security policy.

The Security Server and 3e-WAP / Gateway perform following services:

- The EAP-TLS authentication from 3e-SS through the 3e-WAP / Gateway to the 3e-010F Crypto Client
- Process dynamic key exchange after a successful authentication
- Perform a DH key exchange with the 3e-WAP / Gateway to negotiate an AES key
- Send Gateway Client Shared Secret key to the 3e-WAP / Gateway encrypted with the AES key negotiated using a DH key exchange

2.2. Authentication Mechanisms and Strength

The difference between a Crypto Officer and Administrator is as follows: The Administrator (In the management console application) can NOT, while the Crypto Officer CAN:

1. Set up the security server (configuring server side certificate, set private key password and all other field under the setup screen)
2. View Logs
3. Configure log settings and alarm settings.
4. Change password other than Admin itself.

The following table summarizes the four roles and the type of authentication supported for each role:

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	User ID and password
Administrator	Role-based	User ID and password
Wireless Client	Role-based	Digital Signature
Gateway	Role-based	HMAC SHA1 (Shared secret)

The following table identifies the strength of authentication for each authentication mechanism supported:

Authentication Mechanism	Strength of Mechanism
User ID and password	Minimum 8 characters => 1 / (94^8) = 1.64E-16
HMAC SHA-1 shared secret	Minimum 10 characters => 1/ (94^10) = 1.86E-20
Digital signature	80-bit, 1024-bit modulus

Please note that although the strength of authentication requirements are identified, the module was only tested for Level 1 compliance.

3. Secure Operation and Security Rules

3.1. Security Rules

The following security rules must be followed by the operator in order to ensure secure operation:

1. The Crypto Officer operator will not violate trust by sharing his/her password associated with the Crypto Officer with any other operator or entity.

2. The Crypto Officer will not share any key, or SRDI used by the 3e-030-2 Security Server with any other operator or entity.

3. The Crypto Officer should change the default password when configuring the 3e-030-2 Security Server for the first time. The default password should not be used.

4. The Crypto Officer will monitor the application log using "View Log" program provided by 3e-030-2 Security Server Management Console. The Crypto Officer will monitor the log for self-test errors.

3.2. FIPS mode of operation

The following steps must be performed to install and initialize the module for operating in a FIPS 140-2 compliant manner:

1. The operating system must be configured to prevent remote login and access to the workstation as a server. The operating system must be configured to run in single-user mode. For Windows 2000 Server or Windows 2003 Server, this can be done by disabling the Server and RunAsService services using the Control Panel Services program.

2. The paging file (Virtual memory) must be configured to reside on a local drive on the workstation, not a network drive.

3. The Crypto Officer initiates the 3e-030-2 Security Server into FIPS mode by selecting "FIPS 140-2 Mode" checkbox and "Apply" button, using the "Security Server" panel from 3e-030-2 Security Server Management Console.

3.3. FIPS Policy

The following policies must always be followed in order to achieve a FIPS 140-2 mode of operation:

1. The cryptographic module must only be used by one human operator at a time, and must not be actively shared among operators at any time.

2. None of the files belonging to the module that are installed on the machine should be moved from their original location.

3. The 3e-030-2 Security Server User (end-user of the server computer) must not be given Windows Administrative privileges on the workstation. This will prevent the Administrator from modifying any registry key values, or uninstalling the 3e-030-2 Security Server software using the Control Panel Add/Remove Programs applet.

4. The 3e-030-2 Security Server Crypto Officer must have Administrative privileges on the computer on which the module is run. This will allow the CO to install and uninstall the software if needed.

3.4. Secure Operation Initialization

3.4.1. Installing the 3e-030-2 Security Server

Note: It is recommended that the operator close all open Windows programs before beginning the installation wizard.

Insert the 3e-030-2 Security Server Installation CD in the CD-ROM drive. The CD should automatically play and display a menu that will allow the operator to start the installation process using a typical installation program.

Note: If the computer has AUTOPLAY set off, from "My Computer", locate the CD-ROM drive symbol and double-click to open its window. Locate the "autoplay.exe" file and double click to bring up the menu. Or, find the "DoDPKI-setup-2.4.1F.exe" file and double click to begin the installation process.

The installation wizard guides the operator through the installation process.

First, the Welcome screen will display. Click "Next" to continue.

The operator needs to read and accept the terms of the 3eTI license agreement before the installation can continue.

On the next screen, the operator can select the software components to install. After selecting the components to be installed, click "Next" to continue.

On the next screen, the operator can confirm the default Destination Folder, or select an alternate folder to install the software. Click "Install" and the wizard will begin to install the software.

Once the installation wizard says the installation is complete, click "Finish".

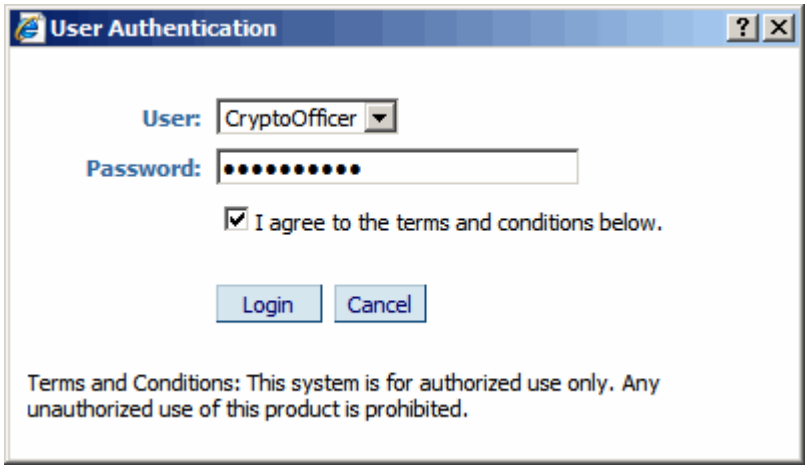
The operator should now configure the 3e-030-2 Security Server. Until the Security Server has been configured properly, the server software will not be able to start working.

3.4.2. Configuring the 3e-030-2 Security Server

Note: The management console (Out of Cryptographic boundary) is a UI to facilitate the user of the whole application to input and configure the dodserver.exe. It uses the aesmain.exe behind scene to generate the configuration files and controls the start/stop of the dodserver.exe. Fields entered through the GUI are fed directly to the aesmain.exe component.

The operator opens the management console by double click "3eTI Security System Management" icon from the computer desktop, or click the "3eTI Security System Management." icon from the quick launch bar.

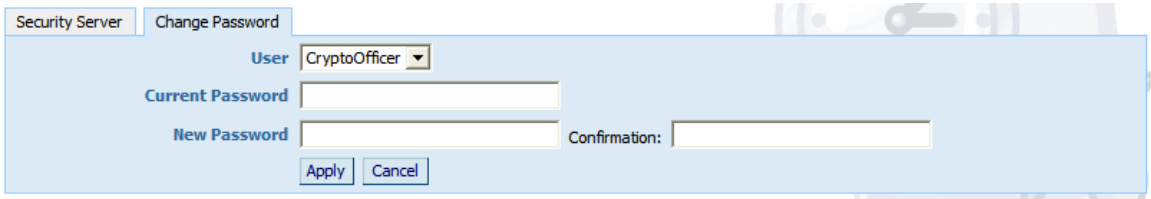
The management console requires user authentication. Only Crypto Officer can access the configuration utility to initialize and modify server configurations.



Type in the correct password for Crypto Officer, and click "Apply". Once the password is successfully authenticated, the operator assumes Crypto Officer Role, and can access the server configurations.

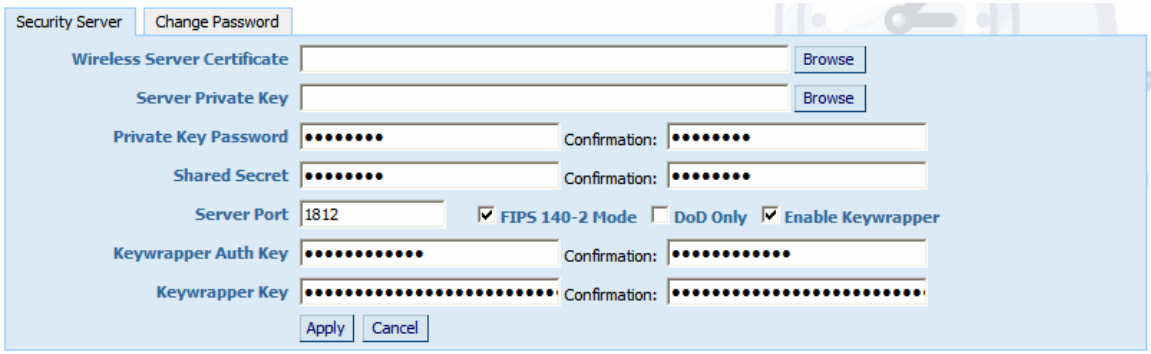
From the management console, click "Setup" button.

To change the password for the Crypto Officer, open the tab of "Change Password".



Type the correct "Current Password", "New Password" and "Confirmation" of the New Password, and click "Apply" to change the password. The password length must be at least 8 characters.

To configure the Security Server, open the tab of "Security Server".



Configure the Security Server parameters as follows:

- In "Wireless Server Certificate" field, specify the file location of the X509 certificate for the server.

- In “Server Private Key” field, specify the file location of the private key that corresponds to the server certificate.
- In “Private Key Password” and “Confirmation” fields, input the secret used to protect the server private key file.
- In the “Shared Secret” and “Confirmation” fields, input the secret shared between the Security Server and the Gateway (AP). This is the secret that the AP authenticates to the Security Server.
- In “Server Port”, specify the port number that the Security Server is running on.
- Check “FIPS 140-2 Mode” box to have the Security Server run in FIPS 140-2 compliant mode.
- Check “DOD Only” box if the Security Server should only accept DOD compliant certificates.
- Check “Enable Keywrapper” box if the key wrapper protocol should be enabled. If key wrapper is enabled, the following values need to be provided:
    - In “Keywrapper Auth Key” and “Confirmation” fields, input the key wrapper authentication key. The key needs to be at least 6 characters.
    - In “Keywrapper Key” and “Confirmation” fields, input the key wrapper key. The key needs to be 32 hexadecimal characters.

Once the Crypto Officer establishes the specific parameters for the Security Server, the Crypto Officer must click “Apply” to save all parameters.

After Security Server configurations are applied, the operator starts the Security Server by clicking the “Start Service” button from the management console front.

3.4.3. Verifying the Status

Security Server status can be viewed and verified from the management console.

- The “Security Server” label on the management console front indicates whether the Security Server is running or not running.
- The “Setup” tab from the management console displays detailed Security Server status.
- View Security Server log file by using management console “View Log” button.

4. Physical Security

The 3e-030-2 Security Server is software that has been tested on the Windows 2000 Server or Windows 2003 Server. It can be run on other Windows Operating Systems but was not

tested on these platforms. The module itself does not provide any physical security mechanisms.

5. Security Relevant Data Items

This section specifies the 3e-030-2 Security Server's Security Relevant Data Items (SRDIs) as well as the access control policy enforced by the 3e-030-2 Security Server.

5.1. Cryptographic Algorithms

The 3e-030-2 Security Server provides the following FIPS-approved cryptographic algorithms:

- AES (ECB mode; 256-bit key size) Certificate #415, #428
- SHA-1 Certificate #484
- HMAC-SHA1 Certificate #189
- FIPS 186-2 (Appendix 3.1, 3.3) PRNG Certificate #210
- RSA Sign/Verify Certificate #153

The 3e-030-2 Security Server also supports the following non-FIPS cryptographic algorithms:

- Diffie Hellman (1024-bit modulus)
- RSA decrypt (PKCS#1) for key un-wrapping.
- MD5 for EAP-TLS
- CRNGT for non-Approved PRNG

5.2. Self-tests

5.2.1. Power-up Self-tests

- AES ECB - encrypt/decrypt KAT
- SHA-1 KAT
- HMAC-SHA-1 KAT
- FIPS 186-2 (Appendix 3.1, 3.3) KAT
- RSA KAT
- Software Integrity Test

5.2.2. Conditional Self-tests

- CRNGT for Approved PRNG
- CRNGT for non-Approved PRNG

5.2.3. Critical Functions tests

- DH pair wise consistency test (power-up)

5.3. Cryptographic Keys, CSPs and SRDIs

The 3e-030-2 Security Server contains the following security relevant data items:

Type	ID	Storage Location	Form	Zeroizable	Zeroization Mechanism	Function
Plaintext Keys						
HMAC-SHA-1 key 128 bit	"Software Integrity Check Key"	Hard Disk/RAM	Plaintext (inaccessible, hard-coded)	N/A	N/A	Calculate system file HMAC; hashing Crypto Officer password
AES ECB Static 256 bit	"System Configuration AES Key"	Hard Disk/RAM	Plaintext (inaccessible, hard-coded)	N/A	N/A	Protect system configuration files
TLS Session Key	"TLS Session Key"	RAM	Plaintext (inaccessible)	Y	Zeroized immediately after session ends	For encrypting certain EAP-TLS traffic between Server and Client
Gateway Client Shared Secret	"Gateway Client Shared Secret"	RAM	Plaintext (inaccessible)	Y	Zeroized immediately after use	Shared secret between Server and AP to negotiate a session key between AP and Client
Diffie-Hellman Private Exponent, 1024-bit	"diffie-hellman prime"	RAM	Plaintext	Y	Zeroized immediately after use	Used for Diffie-Hellman algorithm to exchange secret
Encrypted Keys: These keys are stored encrypted in the module and as such do not require zeroization.						

AES Key 128 bit	"AES Key Wrapper Key"	Hard Disk/RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	To encrypt GW Client shared secret in RADIUS key wrapper mode
DKE Key Encryption Key	"DKE Key Encryption Key"	Hard Disk/RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	To encrypt GW Client shared secret in DKE mode
Other						
HMAC-SHA-1 secret(1)	"Key Wrapper EAP message authenticator secret"	Hard Disk/RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	Generate and verify EAP message MAC
HMAC-SHA-1 secret (2)	"DKE EAP message authenticator secret"	Hard Disk/RAM	Encrypted AES using "System Configuration AES Key"	N/A	N/A	Generate and verify EAP message MAC
Crypto Officer Password	"Crypto Officer Password"	Hard Disk/RAM	HMAC hashed using "Software Integrity Check Key"	N/A	N/A	CO password
RSA Certificate	"Server Certificate"	Hard Disk	Plaintext (inaccessible)	N/A	N/A	RSA certificate for authentication
RSA Private Key	"Server Private Key"	Hard Disk	Plaintext	N/A	N/A	RSA private key for authentication

5.4. Access Control Policy

The 3e-030-2 Security Server 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-030-2 SRDI Roles and Services Access Policy	Security Relevant Data Item	HMAC-SHA-1 key 128 bit SW Integrity	HMAC-SHA-1 key 128 bit Authentication	AES Static 256 bit	TLS Session Key	Diffie-Hellman Session Key	AES Key 128 bit	DKE Key Encryption Key	HMAC-SHA-1 secret (1)	HMAC-SHA-1 secret (2)	Crypto Officer Password	RSA Certificate	RSA Private Key
Role/Service													
Crypto Officer Role													
Server Configuration Settings				E			W		W	W		R/E	R/E
Change Crypto Officer Password		E									W		
Crypto Officer Login		E									E		
Starting and Stopping Service		E		E									
Wireless Client Authentication												R	E
Wireless Session Key Exchange					R	E	E		E	E			
Administrator Role													
Server Configuration Settings													
Change Crypto Officer Password													
Crypto Officer Login													
Starting and Stopping Service		E		E									
Wireless Client Authentication												R	E
Wireless Session Key Exchange					R	E	E		E	E			
Wireless Client Role													
Wireless Client Authentication												R	
Gateway Role													

Wireless Session Key Exchange			E		R		E	E	E	E			

6. Mitigation of Other Attacks

The module does not provide mitigation against any commonly known attacks.