3e Technologies International, Inc.
FIPS 140-2
Non-Proprietary Security Policy
Level 2 Validation

3e-523-F2 & 3e-523-3
Secure Multi-function
Wireless Data Points

HW Versions 1.0, 1.1, 1.2, 2.0
FW Versions 4.3.2

Security Policy
Version 5.6

December 2009

Copyright ©2009 by 3e Technologies International.
This document may freely be reproduced and distributed in its entirety.

GLOSSARY OF TERMS **3**

1. INTRODUCTION **4**

1.1. PURPOSE 4
1.2. DEFINITION 5
1.3. PORTS AND INTERFACES 5
1.4. SCOPE 6

2. ROLES, SERVICES, AND AUTHENTICATION **6**

2.1.1. Roles & Services *6*
2.1.2. Authentication Mechanisms and Strength *10*

3. SECURE OPERATION AND SECURITY RULES **11**

3.1. SECURITY RULES 11
3.2. PHYSICAL SECURITY TAMPER EVIDENCE 13
3.2.1. 3E-523-F2 13
3.2.2. 3E-523-3 14

4. SECURITY RELEVANT DATA ITEMS **15**

4.1. CRYPTOGRAPHIC ALGORITHMS 15
4.2 SELF-TESTS 16
4.3 BYPASS MODE 17
4.4 CRYPTOGRAPHIC KEYS AND SRDIS 17

Glossary of terms

AP	Access Point
CO	Cryptographic Officer
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
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
NAT	Network Address Translation
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

The definition of the cryptographic boundaries is as follows: The 3e-523-F2 cryptographic boundary includes the Level 2 enclosure of the product and everything inside it. The 3e-523-3 cryptographic boundary includes the Level 2 enclosure of the product and everything inside it.

1.1. Purpose

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless universal products, the *3e-523-F2 & 3e-523-3 Secure Multi-function Wireless Data Points (3e-523-F2 & 3e-523-3)* (Hardware Versions: HW V1.0, V1.1, V1.2 (3e-523-F2) V2.0 (3e-523-3); Firmware Versions: 4.3.2). This policy was created to satisfy the requirements of FIPS 140-2 Level 2. This document defines 3eTI's security policy and explains how the 3e-523-F2 and the 3e-523-3 meet the FIPS 140-2 security requirements.

The figure below shows the 3e-523-F2.

Figure 1 – 3e-523-F2

The figure below shows the 523-3.

Figure 2 – 3e-523-3

The 3e-523-3 basically contains the same printed circuit board as a 3e-523-F2, but the PCB is housed in a weatherproof, ruggedized enclosure. The firmware is the same between the 3e-523-F2 and the 3e-523-3.

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/groups/STM/index.html.

1.2. Definition

The 3e-523-F2 and the 3e-523-3 are devices which consist of electronic hardware, embedded software and an enclosure. For purposes of FIPS 140-2, the module is considered to be a multi-chip standalone product. The 3e-523-F2 is physically bound by the mechanical enclosure, which is protected by tamper evident tape.

1.3. Ports and Interfaces

The module provides one RJ45 Ethernet port and two RF antenna ports that connect to the same radio card inside the module.

Ethernet port is meant to be plugged into a secure IT environment. Data packets coming in and going out of Ethernet port are in plaintext.

Data packets coming in and going out of RF antenna ports are encrypted by AES/3DES/AES-CCM depending on configuration.
For 523-F2

a. Status output: Ethernet port pins and LED pins
b. Data output: Ethernet port pins and serial port pins and RF on antenna ports
c. Data input: Ethernet port pins and serial port pins and RF on antenna ports
d. Control input: Ethernet port pins and RF on antenna ports

For 523-3

a. Status output: Ethernet port and LED
b. Data output: Ethernet port and serial port and RF on antenna ports
c. Data input: Ethernet port and serial port and RF on antenna ports
d. Control input: Ethernet port and RF on antenna ports

1.4. Scope

This document covers the secure operation of the 3e-523-F2 and 3e-523-3, including the initialization, roles and responsibilities of operating the product in a secure, FIPS-compliant manner, and a description of the Security Relevant Data Items (SRDIs). The term “product” in this document is used if both the 3e-523-F2 and the 3e-523-3 apply.

2. Roles, Services, and Authentication

The product software supports three separate roles. The set of services available to each role is defined in this section. The product authenticates an operator’s role by verifying his/her PIN or access to a shared secret.

2.1.1. Roles & Services

The product supports the following authorized roles for operators:

Crypto Officer Role: The Crypto officer (CO) role performs all security functions provided by the product. This role performs cryptographic initialization and management functions (e.g., module initialization, input/output of cryptographic keys and SRDIs, audit functions and user management). The Crypto officer is also responsible for managing the Administrator users. The Crypto Officer authenticates to the product using a username and password. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

Administrator Role: This role performs general product configuration. No CO security functions are available to the Administrator. The Administrator can also reboot the

product if deemed necessary. The Administrator authenticates to the product using a username and password. All Administrators are identical; i.e., they have the same set of services available.

Device Role: The purpose of the device role is to describe other devices as they interact with this Cryptographic Module, including:

- Other Access Points (connecting in Bridge mode)
- WLAN Client
- Security Server

The Device Role has access to the following services:

For Device Role (WLAN client)

- Apply Wireless Access Point Security on Data Packet
  - No Encryption
  - Triple-DES
  - AES
  - 802.11i AES-CCM

For Device Role (AP)

- Apply Wireless Bridge Encryption on Data Packet
  - No Encryption
  - Triple-DES
  - AES
- Communicate with Security Server for Authentication and Key Setting
  - AES KeyWrap

The following table outlines the security-relevant cryptographic functionalities that are provided by the "operator" roles (Crypto Officer and Administrator):

Table 1 – Operator Role Functionalities

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset
System Configuration													
Wireless Access Point													
• Security	No Encryption(Bypass)	X	X				X						X
	*Dynamic Key Exchange**	X	X			X	X						X
	Triple-DES	X	X			X	X						X
	AES (128-/192-256-bit)	X	X			X	X						X
	802.11i (AES-CCM)	X	X				X						X
Wireless Bridge													
• Encryption	No Encryption(Bypass)	X	X				X						X
	Triple-DES	X	X		X	X	X						X
	AES (128-/192-256-bit)	X	X		X	X	X						X
Monitoring / Reports													
• System Status	Security Mode	X						X					
	Current Encryption Mode	X						X					
	Bridging encryption mode	X						X					
	Network Access Logs	X						X					
System Administration													

Categories	Features	Operator Roles											
		CryptoOfficer						Administrator					
		Show[1]	Set[2]	Add[3]	Delete[4]	Zeroize[5]	Default Reset[6]	Show[7]	Set[8]	Add[9]	Delete[10]	Zeroize[11]	Default Reset
• Factory Defaults		X	X										
• Reboot (perform self-test)		X	X					X	X				
• Operating Mode	Enable/Disable FIPS mode Select wireless operating mode among AP, bridge, AP&bridge, client modes	X	X				X	X					X
• Firmware Upgrade	Upgrade firmware and bootloader if bootloader is included in upgrade package. Note: Only the FIPS-validated firmware version (4.3.2) can be loaded to the module. Otherwise, the module is not operating in FIPS mode.	X	X										
• Password	Change password for Crypto Officer		X				X						
	Change password for Administrator		X	X	X		X		X				
	Change password policy for Crypto Officer		X				X						
	Change password policy for Administrator		X				X						

[1] *The operator can view this setting*
[2] *The operator can change this setting*
[3] *The operator can add a required input.*
[4] *The operator can delete a particular entry*
[5] *The operator can zeroize these keys.*
[6] *The operator can reset this setting to its factory default value.*
[7] *The operator can view this setting*
[8] *The operator can change this setting*
[9] *The operator can add a required input.*
[10] *The operator can delete a particular entry.*
[11] *The operator can zeroize these keys.*

The following table outlines the security-relevant cryptographic functionalities that are provided to the Device Role:

Table 2 – Device Role Functionalities

Categories	Features	Device Role					
		Show	Apply	Add	Delete	Zeroize	Default Reset
System Configuration							
Wireless Access Point							
• Security	No Encryption		X				X
	*Dynamic Key Exchange**		X			X	X
	Triple-DES		X			X	X
	AES (128-/192-256-bit)		X			X	X
	802.11i (AES-CCM)		X			X	X
Wireless Bridge							
• Encryption	No Encryption		X			X	X
	Triple-DES		X		X	X	X
	AES (128-/192-256-bit)		X		X	X	X

**The proprietary Dynamic Key Exchange (DKE) mode of operation uses Diffie-Hellman which is no longer approved by FIPS. DKE is provided for backward compatibility.*

2.1.2. Authentication Mechanisms and Strength

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

Table 3 – Authentication versus Roles

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	Userid and password
Administrator	Role-based	Userid and password
Device		
Wireless client	static key or 802.11i authentication between wireless client and Device	The possession of PTK
AP		The possession of the static key
Radius Server	802.1x EAP protocol between security server and	Key Wrapper key and authentication key

	Device	

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

Table 4 – Strength of Authentication

Authentication Mechanism	Strength of Mechanism
Userid and password	Minimum 8 characters => 94^8 = 6.096E15
PSK	128 bits => 2^128 = 3.40E38
Digital certificates	Private keys in certificates => 128 bits => 2^128 = 3.40E38
Shared secret	128 bits => 2^128 = 3.40E38
Bridging static key	128 bits => 2^128 = 3.40E38

3. Secure Operation and Security Rules

By factory default, the device is put in FIPS mode with NO security setting, and the radio is turned off.

In order to operate the product securely, each operator shall be aware of the security rules enforced by the module and shall adhere to the physical security rules and secure operation rules detailed in this section.

Note: The proprietary Dynamic Key Exchange (DKE) mode of operation uses Diffie-Hellman which is no longer approved by FIPS. DKE is provided for backward compatibility.

3.1. Security Rules

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

1. Every operator (Crypto Officer or Administrator) has a user-id on the product. No operator shall violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer shall not share any key, or SRDI used by the product with any other operator or entity.
3. The Crypto Officer shall not share any MAC address filtering information used by the product with any other operator or entity.
4. The operators shall explicitly logoff by closing all secure browser sessions established with the product.

5. The Crypto officer is responsible for inspecting the tamper evident seals. A compromised tape reveals message “OPENED” with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
6. The Crypto Officer shall change the default password when configuring the product for the first time. The default password shall not be used.
7. The Crypto Officer shall login to make sure encryption is applied in the device.
8. The Crypto Officer shall login to make sure the device is in FIPS mode by logging in the Web UI and checking “Security Mode” in the page header. This header is available on every web GUI page.
9. The Crypto Officer shall not use DKE in the web GUI configuration.
10. The Crypto Officer shall not use an ASCII passphrase for the 802.11i PSK (Pre-Shared Key with Passphrase). Instead, the Crypto Officer must use either direct 802.11i PSK key input (Pre-Shared Key with Master Key) or EAP-TLS (802.1x) methods.

3.2. Physical Security Tamper Evidence

The difference between the 523-F2 and the 523-3 is that the 523-F2 is intended to be placed into a larger enclosure. The 523-3 has its own weatherproof enclosure and is a stand-alone unit. Functionally, the two modules operate identically. The material used to cover both modules is production grade and opaque within the visible spectrum.

3.2.1. 3e-523-F2

The physical security provided is intended to provide FIPS 140-2 Level 2 physical security (i.e. tamper evidence). The tamper evidence tape is applied at the factory. Crypto Officer should check the integrity of the tape.

The picture below shows the physical interface side of 3e-523-F2 enclosure with tamper-evident seals.

Figure 3 – 3e-523-F2 with tamper seals

3.2.2. 3e-523-3

The physical security provided is intended to provide FIPS 140-2 Level 2 physical security (i.e. tamper evidence).

The figures below show the physical interface sides of 3e-523-3 enclosure with tamper-evident seals.

Figure 4 – 3e-523-3 Physical Interface Side 1

Figure 5 – 3e-523-3 Physical Interface Side 2

4. Security Relevant Data Items

This section specifies the product's Security Relevant Data Items (SRDIs) as well as the product-enforced access control policy.

4.1. Cryptographic Algorithms

The product supports the following FIPS-approved cryptographic algorithms. The algorithms are listed below, along with their corresponding CAVP certificate numbers.

3e Technologies International Inc. 3eTI CryptoLib (User Space Library) Algorithm Implementation 1.0 (RNG only)
RNG: #583

3e Technologies International Inc. 3eTI OpenSSL Algorithm Implementation 0.9.7-beta3
TDES: #783
AES; #1022
SHS: #976
RSA: #490
HMAC: #571

3e Technologies International Inc. 3eTI CryptoLib (Kernel Module) Algorithm Implementation 1.0
TDES: #782
AES; #1021
SHS: #975
HMAC: #570

The product also supports the following **non-Approved but FIPS allowed** cryptographic algorithms:

- RSA (key wrapping, key establishment methodology provides 80 bits of encryption strength)
- MD5 hashing in HTTPS over TLS
- AES (Cert. #1021, key wrapping)
- Non-Approved RNG

The product also supports the following **non-Approved FIPS** cryptographic algorithms:

- RC4 (used in WEP/WPA)
- MD5 hashing (used in MS-CHAP for PPPoE and SNMP agent)
- DES CBC (non-compliant) (used in SNMP v3)
- AES CFB (non-compliant) (used in SNMP v3)
- Diffie-Hellman for Dynamic Key Exchange (DKE). DKE is provided in FIPS mode for backward compatibility and should not be used in FIPS mode.

4.2 Self-tests

POST (Power on Self Tests) is performed on each boot. A command to reboot the device is considered on-demand self test. Both "Crypto Officer" and "Administrator" roles can send reboot command from web GUI.

4.2.1 Power-on Self-tests

OpenSSL Power-on Self Tests

AES ECB - encrypt/decrypt KAT
Triple-DES CBC – encrypt/decrypt KAT
RSA KAT
SHA-1 KAT
HMAC-SHA-1 KAT

Crypto-1.0 User Library Power-on Self Tests

FIPS 186-2 (Appendix 3.1, 3.3) RNG KAT

Kernel Crypto Module Power-on Self Tests

Triple-DES ECB - encrypt/decrypt KAT
AES ECB - encrypt/decrypt KAT
AES CCM KAT
SHA-1 KAT
HMAC-SHA-1 KAT

Software Integrity Power-on Self Tests

SHA-1 Integrity Test for firmware
SHA-1 Integrity Test for bootloader

If any of the Power-on Self-tests fail, the system halts. The operator can attempt to power cycle the module to clear the error condition. Once the error condition has been cleared, the Crypto Officer or Administrator can view the logs to determine the type of failure.

4.2.2 Conditional Self-tests

Whenever the module is configured by the Crypto-Officer to use an encryption algorithm and specific key, an exclusive bypass self test is performed on the configuration change before the modification takes effect. If this self test fails, the system halts.

Whenever a firmware package is uploaded through HTTPS over TLS secure channel, the package integrity check is performed before the firmware can be

updated. The firmware package is wrapped in 3eTI proprietary format and HMAC-SHA1 hashed for integrity check.

Whenever a random number is generated (both FIPS 186-2 Approved and non-Approved), a Continuous Random Number Generator test is performed to ensure the random number is not repeating.

4.2.3 Firmware Integrity Check by bootloader

After device is powered on, the first thing done by bootloader is to check firmware integrity. If the integrity is broken, firmware won't boot. Firmware integrity is also performed at POST (Power On Self Test) during firmware boot up. The bootloader integrity is done at POST, too.

4.3 Bypass mode

When "no encryption" option is selected for wireless security, the device is in exclusive bypass mode. Data packets are in plaintext. User with Crypto Officer role can login the device to check whether it's in bypass mode. The AP bypass information is in "Wireless Access Point"→"Security" page. The bridge bypass information is in "Wireless Bridge"→"Encryption" page.

When wireless security is switched from bypass mode, a conditional self test is performed in the backend to make sure the encryption algorithm is working as configured.

4.4 Cryptographic Keys and SRDIs

The module contains the following security relevant data items:

Table 5 - SRDIs

Non-Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Operator passwords	ASCII string	Input encrypted (using TLS session key)	Not output	Plaintext	Zeroized when reset to factory settings.	Used to authenticate CO and Admin role operators
Configuration file passphrase	HMAC key (ASCII string)	Input encrypted (using TLS session key) by Crypto Officer	Not output	Plaintext in RAM.	Zeroized when a configuration file is uploaded after it is used.	Used for downloaded configuration file message authentication

Firmware load key	HMAC key (ASCII string)	Embedded in firmware at compile time. Firmware upgrade is through encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used for firmware load message authentication
SNMP packet authentication keys, username	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	Zeroized when reset to factory settings.	Use for SNMP message authentication
system config AES key (256 bit)	AES key (HEX string)	Harcoded in FLASH	Not output	Plaintext in FLASH	Zeroized when firmware is upgraded.	Used to encrypt the configuration file
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
FIPS 186-2 PRNG Seed Key	20-byte value	RNG Seed	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used to initialize FIPS PRNG
RNG Seed	20-byte value	512 bytes from system interrupt numbers hashed by HMAC-SHA1		Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG after it is used.	Used as seed for Non-approved RNG which provides the seed key for the FIPS 186-2 PRNG.
3eTI Static Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
AP / Client Static key	1. AES ECB (e/d; 128,192,256) 2. TDES (Triple-DES 192)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	N/A	Used to encrypt unicast, and broadcast/ multitcast traffic in support of static mode
IEEE 802.11i Protocol Keys/CSPs (Common to PSK and EAP-TLS)						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
PMK	Typed in directly as a Hex string	Typed in directly as a Hex string. Input	Not output	If 802.11i PSK, then plaintext in flash	Zeroized when local antennae Approved	802.11i PMK

	If 802.11i EAP-TLS, then secret key (TLS master secret)	encrypted using the TLS session key. If 802.11i EAP-TLS, then not input, instead derived (TLS master secret resulting from successful User EAP-TLS authentication)		For both 802.11i PSK and EAP-TLS, plaintext in RAM	encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. If 802.11i PSK, zeroized when reset to factory settings.	
PTK	AES (key derivation; 256)	Not input (derived from PMK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i PTK
KCK	HMAC key (128 bits from PTK)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KCK
KEK	AES ECB(e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i KEK
TK	AES CCM (e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
TK (copy in driver)	AES CCM (e/d; 128)	Not input (derived from PTK)	Not output	Plaintext in RAM	When 802.11i session ends.	802.11i TK
GMK	AES (key derivation; 256)	Not input (RNG)	Not output	Plaintext in RAM	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to	802.11i GMK

					802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. When re-key period expires	
GTK	AES CCM (e/d; 128)	Not input (derived from GMK)	Output encrypted (using KEK)	Plaintext in RAM	Zeroized when local antennae Approved encrypting mode either reconfigured or changed from IEEE 802.11i mode to any other local antennae Approved encrypting mode (including from 802.11i PSK to 802.11i EAP-TLS, and 802.11i EAP-TLS to 802.11i PSK), to bypass mode. When re-key period expires	802.11i GTK

3eTI Security Server Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Security Server password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	N/A	Authenticate module to Security Server in support of 802.11i EAP-TLS authentication
Backend password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	N/A	Authenticate messages between module and security server in support of 802.11i EAP-TLS
Backend key	AES ECB key (d;128)	Input encrypted (using TLS	Not output	Ciphertext in flash, encrypted	N/A	Decrypt TLS master secret returned to

		session key)		with "system config AES key"		module by Security Server after successful User authentication in support of 802.11i EAP-TLS
3eTI Bridging Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Bridging static key	AES ECB (e/d; 128,192,256) TDES (Triple-DES 192)	Input encrypted (using TLS session key)	Not output	Ciphertext in flash, encrypted with "system config AES key"	N/A	Used to encrypt bridged traffic between two modules
RFC 2818 HTTPS Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
RSA private key	RSA (1024) (key wrapping; key establishment methodology provides 80-bits of encryption strength)	Not input (installed at factory)	Not output	Plaintext in flash	Zeroized when firmware is upgraded.	Used to support CO and Admin HTTPS interfaces.
TLS session key for encryption	Triple-DES (192)	Not input, derived using TLS protocol	Not output	Plaintext in RAM	Zeroized when a page of the web GUI is served after it is used.	Used to protect HTTPS session.

The following is a table of cryptographic keys and key material that are unique to the product when it is operating in wireless Client mode:

Table 6 – SRDIs in Client Mode

Type	ID	Storage Location	Form	Zeroization
Certificate Authority (CA) public key certificate	"CA public key"	FLASH	Plaintext (inaccessible)	Zeroized when a new certificate is uploaded
Client public key certificate	Wpaclt.der	FLASH	Plaintext	Zeroized when a new certificate is uploaded
Client private key RSA 1024	Wpaclt.pem	FLASH	Plaintext	Zeroized when a new certificate is uploaded