3e Technologies International, Inc.
Non-Proprietary Security Policy
FIPS 140-2 for
3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3, and 3e-525Ve-4
AirGuard™ Wireless Access Points

Security Policy Version 3.3

December 8, 2010

1. Introduction

This document describes the non-proprietary cryptographic module security policy for 3e Technologies International's wireless product variations, the 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP,3e-525V-3 and 3e-525Ve-4 Wireless Access Points that support the IEEE 802.11a/b/g Wi-Fi standards for wireless LAN communications, and the IEEE 802.11i standard for wireless LAN security. They are multiple-chip standalone cryptographic modules, compliant with all requirements of FIPS 140-2. This document defines security policy and explains how the product variations meet the FIPS 140-2 security requirements.

In the FIPS mode of operation, the modules secure all wireless communications with Wi-Fi Protected Access 2 (WPA2). WPA2 is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. The modules use the following cryptographic algorithm implementations:

- AES
- AES-CCM
- SHA-1
- HMAC SHA-1
- FIPS 186 Random Number Generator
- RSA
- Triple-DES

This document details the security policy for 3e-525A-3, 3e-525A-3EP, 3e-525A-3MP, 3e-525V-3 and 3e-525Ve-4 cryptographic modules. 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.

The table below summarizes the evaluated platforms

Table 1: Evaluated Platforms

Model	Firmware Version	Hardware Revision
3e-525A-3	4.4	2.0 (A) and 2.1
3e-525A-3EP	4.4	2.1
3e-525A-3MP	4.4	2.0 (A) and 2.1
3e-525V-3	4.4	2.0 (A) and 2.1
3e-525Ve-4	4.4	2.0 (A) and 2.1

All cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-2. The table below summarizes the subcategory specifications

Table 2: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.1. Cryptographic Module

The five variants of the 3eTI 525 AirGuard Wireless Access Point module (the module) are devices, which consist of electronic hardware, embedded software and strong metal case. The modules share the identical CPU and motherboard, with identical firmware. They differ in non-cryptographic related aspects such as the power options (DC versus POE among A-3 family modules) or the video input interfaces (V3 and V4 modules). Yet all modules provide the same cryptographic services.

The physical cryptographic boundary of the 525A series and 525V series product variants is defined to be the entire enclosure of the module. While the 3e-525-A-3 family AP's logical boundary is the same as the physical one, the V-3/Ve-4's logic boundary excludes the security non-relevant circuitry which is the video components included inside the physical boundary.

525A metal case

3e-525V

2. Module Ports & Interfaces

The modules have the following physical ports:

- 10/100 Mbps Ethernet (Qty. 2): Control In, Data In/Out, Power In
- External RF Antenna (Qty. 3): Control In, Data In/Out
- LEDs: Status Out
- Video Input (525-“V” models only, 1-2). Video signal input
- Camera PTZ (525-“V” models only, 0-1) Control to camera, In/Out

The cryptographic module provides the following logical interfaces with mapping to physical ports as summarized in the table below:

Table 3: Logical Interfaces and Physical Ports Mapping

FIPS Logical Interface	Module interface
Data input	Local antennae (2)
	Bridging antenna (if enabled)
	Ethernet 10/100 Mbps WAN port
	Video (525-"V" models only)
Data output	Local antennae (2)
	Bridging antenna (if enabled)
	WAN port
	Camera PTZ (525-"V" models only)
Control input	Ethernet 10/100 Mbps LAN port, WAN port Bridging antenna
Status output	LEDs: • Power • WAN • WLAN 1 • WLAN 2 • WLAN SS • FIPS/MODE

The management interface of the Cryptographic Module (CM) uses HTTPS protocol. During the HTTPS session setup, the Cryptographic Module enforces mutual authentication between the web client and CM by requesting and validating the web client's certificate. The Cryptographic Officer must configure the CM with proper root certificate and OCSP server address to facilitate this mutual authentication between the web client and the CM.

3. Roles, Services and Authentication

The 525A and 525V series product variants support user identity based operator authentication. There are total of three roles supported by the modules. Two of which are operator roles and the other role is wireless user. Any operator user can belong to one of the operator roles. The operator user authenticates to the cryptographic module by using username and password and assumes his role upon successful authentication.

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

Table 4: Roles and User Identify Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based	Crypto officers present unique usernames and passwords to log in to the module over HTTPS session
Administrator	Identity-based	Administrator present unique usernames and passwords to log into the module over HTTPS session
Wireless User	Identity-based	Wireless client user authenticate to the RADIUS server using certificate. Then client prove its possession of the 256 bit PMK by performing 802.11i defined 4-way handshake protocol. Each wireless client user is uniquely identified by its MAC address

Passwords for all Users and Crypto Officers shall be configured to be 8 or more characters, including both numbers and letters and special characters. Following this guidance will result in a password space of 2.8 trillion possible passwords. The module halts (introduces a delay) for a second after each unsuccessful authentication attempt by CO or Admin. The highest rate of authentication attempts to the module is one attempt per second. This translates to 60 attempts per minute. Therefore the probability for successful brute force multiple attempts to compromise the module's authentication mechanism during a one-minute period is 60/ (94^8), or less than (9.84E-15).

In addition, wireless user connections are authenticated by means of a 256 bit Pre-shared Key (PSK). The PSK is either manually input by Crypto Officer through the HTTPS channel or received from RADIUS server as part of the RADIUS_ACCEPT message that is protected with AES key wrap in the format of 64 bytes of hex number. An attacker would have a 1 in 2^{256} change of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2.

Beside, the set of services available to each user depends on the role that the user belongs to. The services available to each role are defined in the following section.

3.1.1. Crypto Officer and Administrator Role Services

Crypto Officer Role: The Crypto officer (CO) role performs all security .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 other CO and Administrator users and can define up to ten users in CO category. The Crypto officer uses a secure web-based HTTPS connection to configure the 525A and 525V series products and authenticates to the module using a username and password.

Administrator Role: This role performs in general the module's configuration such as defining the WLAN, LAN settings, and viewing system log messages for auditing purposes. No CO security functions are available to the Administrator.

The Administrator must use a secure web-based HTTPS connection to configure the module and authenticates to the module using a username and password. Up to 5 operators in the Administrator role can be defined. All Administrators have the same set of services available. The Crypto Officer is responsible for managing (creating, deleting) Administrator users.

The table below summarizes the Crypto Officer and Administrator services that each role has access to using HTTPS web GUI.

Table 5 Roles and Services

Categories	Features	Operators							
		Crypto Officer				Administrator			
		Show[1]	Set[2]	Add[3]	Delete[4]	Show[5]	Set[6]	Add[7]	Delete[8]
System Configuration									
• Operating Mode	AP / Bridging Mode – FIPS AP / Bridging Mode – Non-FIPS	X	X X			X X	X X		
Wireless Access Point									
• Security	AES (128-/192-256-bit) FIPS 802.11i	X X	X X						
Wireless Bridge									
• Encryption	AES (128-/192-256-bit) AES_CCMP	X X	X X		 X				
Service Settings									
• SNMP agent	Enable/ Disable Community settings Secure User Configuration System Information	X X X X	X X X X			X X X X	X X X X		
User Management									
• List All Users		X		X	X	X			
• Add New User			X						
• User Password Policy	Enable/Disable Policy setting	X X	X X						
Monitoring/Reports									
• System Log	Date/Time/Message	X			X	X			X
• Web Access Log		X			X	X			X
Auditing									
• Log		X				X			
• Report Query		X				X			

[1] *The operator can view this setting*
[2] *The operator can change this setting*
[3] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*
[4] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*
[5] *The operator can view this setting*
[6] *The operator can change this setting*
[7] *The operator can add a required input. For example: Adding an entry to the MAC address filtering table*
[8] *The operator can delete a particular entry. For example: Deleting an entry from the MAC address filtering table*

Categories	Features	Operators							
		Crypto Officer				Administrator			
		Show[1]	Set[2]	Add[3]	Delete[4]	Show[5]	Set[6]	Add[7]	Delete[8]
• Configuration	Enable/Disable Selectable items	X X	X X						
System Administration									
• System Upgrade	Firmware Upgrade Local Configuration Upgrade Remote Configuration Upgrade	X X X	X X X						
• Self Tests	Perform Cryptographic algorithm KAT, key error detection test, software integrity check	X	X						
• Factory Defaults		X							
• Remote Logging	Enable/Disable Settings	X X	X X			X X	X X		
• Reboot		X	X			X			
• Default Reset			X				X		

3.1.2. User Role Services

Wireless User Role: This role is assumed by the wireless client workstation or another wireless access point. The user authenticates to the module by presenting the 128/256 bit encryption key. The encryption key is either established during the 802.11i EAP-TLS session or manually input into the user and module. The encryption key is unique per wireless user if the user uses 802.11i EAP-TLS authentication method. The encryption key is the same for wireless users if they use 802.11i PSK authentication method. Each wireless user is uniquely identified by its own MAC address.

The User role has the ability to send data to and through the module. All data is sent in the form of 802.11i wireless packets. All wireless communication is encrypted using or AES encryption (based upon the module configuration). The module will perform encryption and decryption services on behalf of the user.

The following table summarizes the keys and services the wireless user has access to:

Table 6: Services and keys accessible to the wireless user

Services	Keys	Read key	Write key	Delete Key
AES_CCM	128 bit Unicast Key	Yes	No	No
AES_ECB (static key)	128, 192, 256 bit key	Yes	No	No

3.2. Cryptographic Algorithms

The 525A and 525V series product variants support the following FIPS-approved cryptographic algorithms:

- AES (ECB mode; 128, 192, 256-bit keysizes), cert#1021(Cryptolib Kernel Module), cert #1022 (OpenSSL), and #1023 (Hardware Cryto-engine)
- AES CCM (128-bit keysize), cert #1023
- Triple-DES (CBC mode, KO 1,2), cert. #783
- SHA-1, cert #976 and #977
- HMAC-SHA1, cert #571 and #572
- FIPS 186-2 (Appendix 3.1 and 3.1) PRNG, cert#583
- RSA Cert #490

The 525A and 525V series product variants also support the following non-FIPS cryptographic algorithms:

- RSA decrypt (PKCS#1 using a 1024-bit modulus) allowed in FIPS mode for key un-wrapping. This key establishment method provides 80-bits of security.
- 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)

3.3. Cryptographic Keys Management

Cryptographic keys are stored in encrypted form in flash for long term storage and in plaintext form in SDRAM (for active keys). The plaintext keys in SDRAM are zeroized as soon as they are no longer used by the module. All keys are input into the module in encrypted form via HTTPS session. The PMK is input from the Radius server encrypted with the AES key wrap protocol or manually input via HTTPS session in encrypted form. RSA public keys are output in plaintext in the form of X.509 certificates.

The table below summarizes the Keys and CSPs in the cryptographic module

Table 6: Keys & CSPs

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	Hash value in flash (PKCS#5)	Zeroized at factory default	Used to authenticate CO and Admin role operators
Configuration file passphrase	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext in RAM. It is put into temporary memory/auto variable/stack.	Zeroized after it is used.	Used for downloaded configuration file message authentication
Firmware integrity check key	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext in flash	Zeroized at factory default.	Used for firmware load message authentication
RNG Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Non-Approved RNG seed	20-byte value	512 bytes from system interrupt numbers hashed by HMAC SHA-1	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG	Used as Seed for non-Approved RNG which provides seed key for FIPS PRNG.
FIPS 186-2 seed key	Symmetric	RNG	Not output	Plaintext in RAM	Zeroized every time a new random number is generated using the FIPS PRNG	Used to initialize FIPS PRNG
3eTI Static Protocol Keys/CSPs						
Key/CSP	**Type**	**Generation/ Input**	**Output**	**Storage**	**Zeroization**	**Use**
Static key	1. AES ECB (e/d; 128,192,256)	Input encrypted (using TLS session key)	Not output	Encrypted text in flash	Zeroized when encryption mode is changed Zeroized when reset to factory default settings.	Used to encrypt unicast, and broadcast/ multitcast traffic in support of static mode
IEEE 802.11i Protocol PSK Keys/CSPs						

Key/CSP	Type	Generation/ Input	Output	Storage	Zeroization	Use
802.11i PMK	64 bytes Hex number	Input manually by CO through encrypted (using TLS session key) Or input from RADIUS server with ASE Key Wrap	Not output	Plaintext in flash	Zeroized when local authentication mode changed Zeroized when reset to factory default settings.	Used to authenticate wireless client user in 802.11i PSK mode
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
GMK	AES (key derivation; 256)	Not input (RNG)	Not output	Plaintext in RAM	Zeroized when local authentication mode changed When re-key period expires	802.11i GMK
GTK	AES CCM (e/d; 128)	Not input (derived from GMK)	Output encrypted (using KEK)	Plaintext in RAM	Zeroized when local authentication mode changed When re-key period expires	802.11i GTK
Backend password	HMAC key (ASCII string)	Input encrypted (using TLS session key)	Not output	Plaintext	Zeroized when authentication mode is changed Zeroized when reset to factory default settings.	Authenticate messages between module and security server in support of 802.11i EAP-TLS
AES Key Wrap key	AES ECB key (d;128)	Input encrypted (using TLS session key)	Not output	Plaintext	Zeroized when mode changes Zeroized when reset to factory settings.	Decrypt TLS master secret returned to 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) AES CCMP (128)	Input encrypted (using TLS session key)	Not output	Plaintext	Zeroized when bridge encryption mode is changed Zeroized when reset to factory settings.	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), same private key for all manufactured modules	Not output	Plaintext in flash	Zeroized at firmware upgrade time	Used to support CO and Admin HTTPS interfaces.
HTTPS TLS Pre-Master Secret	Shared secret	No input	No output	Plaintext in RAM	Zeroized when TLS session ends	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created. The module enforeces the TLS cipher and will use either AES or Triple-DES only.
HTTPS TLS Encryption Key	AES-CBC or Triple-DES-CBC Key	No	No	Plaintext in RAM	Zeorized when TLS session ends	AES or Triple-DES key used to encrypt HTTPS data.
HTTPS TLS Integrity Key	HMAC-SHA1 Key	No	No	Plaintext in RAM	Zeorized when TLS session ends	HMAC-SHA-1 key used for HTTPS integrity

						protection.

3.4. Self-Tests

The module performs the following 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 (Kernel Software)
AES ECB - encrypt/decrypt KAT

Kernel Crypto Coprocessor Power-on Self Tests (Hardware)
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

3.5. Conditional self-tests:

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.

3.6. Secure Operation of the AirGuard Wireless Access Point

The following 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 525A and 525V product variants. No operator will violate trust by sharing his/her password associated with the user-id with any other operator or entity.
2. The Crypto Officer will not share any key, or SRDI used by the 525A and 525V product variants with any other operator or entity.
3. The operators will explicitly logoff by closing all secure browser sessions established with the 525A and 525V product variants.
4. The Crypto officer is responsible for inspecting the tamper evident seals on a daily basis. A compromised tape reveals message "OPENED" with visible red dots. Other signs of tamper include wrinkles, tears and marks on or around the label.
5. The Crypto Officer should change the default password when configuring the 525A and 525V product variants for the first time. The default password should not be used.
6. 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. Under 802.11i PSK mode, the Crypto Officer must set up MAC filtering to identify the wireless users.

3.6.1. Applying Tamper-Evident Seals (All Models)

The following section contains detailed instructions for the Crypto Officer to check and install the tamper evident seals to the 525A and 525V product variants enclosure, in order to provide physical security for FIPS 140-2 level 2 requirements.

The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. The Crypto Officer is responsible for: securing and having control at all times of any unused seals.

A security seal is added from the back plate to the antenna plate. A second security seal is added from the front of the unit to the antenna plate, taking care not to cover the L.E.D.

Materials:

525A and 525V product variants product variants – Quantity: 1
Seal, Tape, Tamper-evident – Quantity: 4, part number: 90000522-001
Isopropyl Alcohol Swab
3M Adhesive Remover (citrus or petroleum based solvent)

Installation – Tamper-evident tape

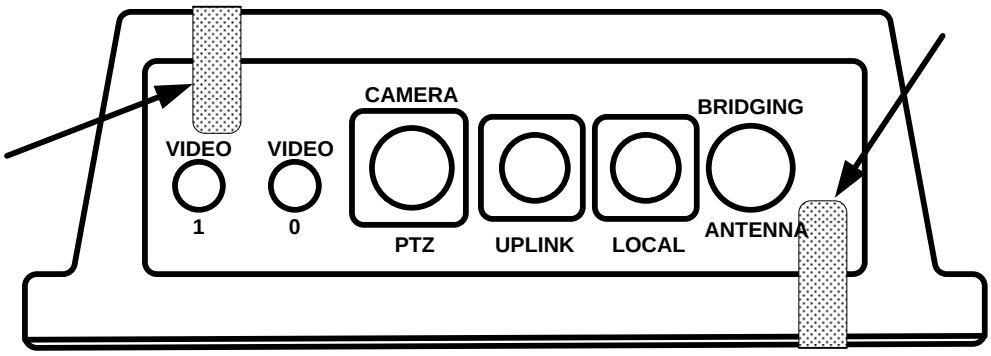
1. Locate on 525A and 525V product variants the placement locations of tamper-evident tape seals
2. Thoroughly clean the area where tamper-evident tape seal is to be applied with isopropyl alcohol swab. Area must be clean of all oils and foreign matter (dirt, grime, etc.)
3. Record tracking number from tamper-evident tape seal.
4. Apply seal to locations on the 525A and 525V product variants as shown in the figure below. It is important to ensure that the seal has equal contact area with both top and bottom housings.
5. After application of seals to the 525A and 525V product variants, apply pressure to verify that adequate adhesion has taken place.

The photos below show the physical interface of the 3e-525A enclosure with tamper evident seals.

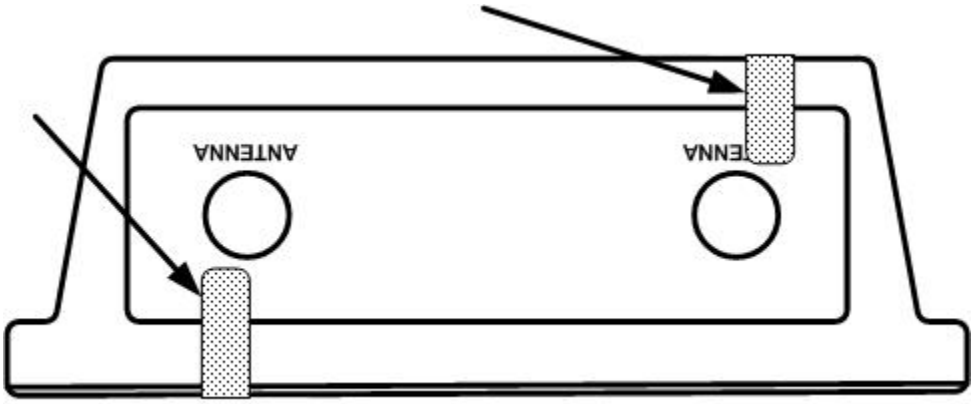
3e-525A Side One

3e-525A Side Two

The figures below show the physical interface of the 3e-525V enclosure with tamper evident seals.



3e-525V Side One



3e-525V Side Two

3.6.2. Checking for Tamper Evidence

Tamper-evident seals should be checked for letters from the word “OPENED” left behind by seal residue when the seal is removed.

Tamper-evident seals should also be checked for nicks and scratches that make the metal case visible through the nicked or scratched seal.

Glossary

AP	Access Point
CO	Cryptographic Officer
DH	Diffie Hellman
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