WINC3400 Software

Release Notes

VERSION :	**1.4.6**
DATE :	**14 AUG, 2024**

Abstract

This document presents an overview of the WINC3400 firmware release version 1.4.6, and corresponding driver.

1 **Introduction** 3

1.1 Highlights of the release 3

1.2 Firmware readiness 3

2 **Release summary** 4

2.1 Auditing information 4

2.2 Version information 4

2.3 Released components 5

2.4 Release Comparison 6

3 **Test Information** 9

3.1 Internal testing 9

4 **Known Issues** 11

5 **Fixes and Enhancements** 14

5.1 Issues Fixed 14

5.2 Enhancements 16

6 **Appendix A – TLS Root certificates** 17

6.1 TLS root certificates 17

1 Introduction

This document describes the WINC3400 version 1.4.6 firmware release package. This is a release containing Wi-Fi functionality with basic BLE support including an on-chip provisioning profile and custom BLE profiles using the Atmel BLE API and BluSDK.

The release package contains all the necessary components (binaries and tools) required to make use of the latest features including tools, and firmware binaries.

1.1 Highlights of the release

- Added EAPOL v3 support for WPA Enterprise connections.
- Fixed connection parameter saving code to ensure it doesn’t make unnecessary flash writes
- Correctly parse and handle the “critical” field of x.509 certificate extensions
- Check CA Basic Constraint in TLS certificate chain
- Improvements and bugfixes to the BLE API
- BLE MAC address generation code no longer requires WiFi MAC to be even

1.2 Firmware readiness

Microchip Technology Inc. considers version 1.4.6 firmware to be suitable for production release.

2 Release summary

2.1 Auditing information

Master Development Ticket	:	`https://jira.microchip.com/projects/W3400/versions/81112`

Wi-Fi:

Release Repository Branch	:	/chn-vm-svnrepo01.microchip.com/repo/wsg/Wifi_M2M/branches/rel_3400_1.4.6
Subversion Revision	:	**20669**

BLE:

Release Repository Branch	:	`/svn/Bluetooth/branches/ATWILC3400_BT_BLE_API`
Subversion Revision	:	**r7655**

BLE API:

Release Repository Branch	:	`/svn/Bluetooth/branches/ATWILC3400_BLE_API`
D21 Subversion Revision	:	**r7664**
SAM4 Subversion Revision	:	**r7664**

2.2 Version information

WINC Firmware version	:	1.4.6
Host Driver version	:	1.3.2
Host Interface Level	:	1.6

RF version: 1.0

2.3 Released components

The release contains documentation, sources and binaries.

2.3.1 Documentation overview

The Application manuals, Release notes and Software API guides can be found in the `doc/` folder of the release package.

Release Notes:

This document

Software APIs:

WINC3400_IoT_SW_APIs.chm

WINC3400_BLE_APIs.chm

2.3.2 Binaries and programming scripts

The main 3400 firmware binary is in the `firmware` directory and named `m2m_image_3400.bin`. This can be flashed to a WINC device using, for example, a serial bridge application available from ASF.

An OTA image is provided in the `ota_firmware` directory named `m2m_ota_3400.bin`.

2.3.3 Sources

Source code for the host driver can be found under the `src/host_drv` directory.

Source code for the tools, including crypto_lib, can be found under the `src/Tools` directory.

2.4 Release Comparison

Features in 1.4.4	**Changes in 1.4.6**
Wi-Fi STA	
• IEEE 802.11 b/g/n. • OPEN (WEP protocol is deprecated, attempts to configure it will result in error). • WPA Personal Security (WPA/WPA2), including protection against key re-installation attacks (KRACK) and countermeasures for ‘Fragattack’ vulnerabilities. • WPA Enterprise Security (WPA/WPA2) supporting: EAP-TTLSv0/MS-Chapv2.0 EAP-PEAPv0/MS-Chapv2.0 EAP-PEAPv1/MS-Chapv2.0 EAP-TLS EAP-PEAPv0/TLS EAP-PEAPv1/TLS • Simple Roaming Support	• Added EAPOLv3 support to WPA Enterprise Security. • Fixed code that saves connection info to WINC flash upon successful connection to ensure it doesn’t perform unnecessary flash writes
Wi-Fi Hotspot	
• Only ONE associated station is supported. After a connection is established with a station, further connections are rejected. • OPEN security mode • The device cannot work as a station in this mode (STA/AP Concurrency is not supported). • Includes countermeasures for ‘Fragattack’ vulnerabilities.	No change
WPS	
The WINC3400 supports the WPS protocol v2.0 for PBC (Push button configuration) and PIN methods.	No change
TCP/IP Stack	
The WINC3400 has a TCP/IP Stack running in firmware. It supports TCP and UDP full socket operations (client/server). The maximum number of supported sockets is currently configured as: • 7 TCP sockets (client or server). • 4 UDP sockets (client or server). • 1 RAW socket	No change

Transport Layer Security	
• The WINC3400 supports TLS v1.2, 1.1 and 1.0. • Client mode only. • Mutual authentication. • Integration with ATECC508 (ECDSA and ECDHE support). • Multi-scream TLS RX operation with 16KB record size • Supported cipher suites are: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128 _CBC_SHA256 (requires ATECC508) TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (requires ECC508) TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (requires ATECC508)	• The “critical” field of x.509 certificate extensions is now correctly handled • Ensure Basic Constraint is checked in server certificate chain
Networking Protocols	
• DHCPv4 (client/server) • DNS Resolver • SNTP	No change
Power saving Modes	
• The WINC3400 supports these powersave modes: ○ M2M_NO_PS ○ M2M_PS_DEEP_AUTOMATIC • BLE powersave is always active	No change
Device Over-The-Air (OTA) upgrade	
• The WINC3400 has built-in OTA upgrade. • Firmware is backwards compatible with driver 1.0.8 and later. • Driver is backwards compatible with firmware 1.2.0 and later (though the functionality will be limited by the firmware version in use).	No change
Wi-Fi credentials provisioning via built-in HTTP server	
The WINC3400 has built-in HTTP provisioning using AP mode (Open only - WEP support has been removed).	No change

WLAN MAC only mode (TCP/IP Bypass, or Ethernet Mode)	
Allow WINC3400 to operate in WLAN MAC only mode and let the host send/receive Ethernet frames.	No change
ATE Test Mode	
Embedded ATE test mode for production line testing driven from the host MCU.	No change
Miscellaneous features	
	No change
BLE functionality	
BLE 4.0 functional stack	BLE API improvements/fixes (see 5.1 for more details)

3 Test Information

This section summarizes the tests conducted for this release

3.1 Internal testing

Please refer to ticket W3400-820 for full details.

Testing was performed against the release candidate 1.4.6 against the following configuration(s):

H/W Version	:	WINC3400 XPRO module
Host MCU	:	ATSAMD21-XPRO

For Elliptic Curve cryptography support verification, a CRYPTOAUTH XPLAINED PRO board (containing an ECC508A chip) was inserted into the EXT2 socket on the ATSAMD21-XPRO board.

Testing was performed in both open air and shielded environments.

The following testing has been performed:

1. General functionality including:
    1. HTTP Provisioning
    2. BLE API verification
    3. Station Mode
    4. AP Mode
    5. IP (TCP and UDP client and server)
    6. HTTP POST/GET
    7. WPS (PIN and PushButton methods)
    8. Over-The-Air (OTA) update functionality and robustness (with and without TLS)

2. TLS functionality including:
    1. All supported TLS ciphersuites
    2. SNI Client Hello extension
    3. Server certificate name validation
    4. Client authentication
    5. Amazon AWS IoT environment with client authentication and ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. MQTT connection, publishing and subscribing all succeed.
3. Performance under interference
4. Wi-Fi AP interoperability testing
5. Regression and longevity tests
6. TCP/IP stack robustness testing
    a. Using an internal implementation of IPerf.
    b. Verification of multi socket functionality

Known issues are declared in Section 4

4 Known Issues

Jira	Severity	Description
W3400-605	Medium	Prolonged heavy IP traffic load can result in the SPI becoming unusable between the WINC3400 and the host. Observed with SAMD21 host and WINC powersave disabled. Could potentially occur with other host platforms, but not yet observed. Recommended workaround: On SAMD21 host, the frequency of the issue can be minimized by using M2M_PS_DEEP_AUTOMATIC when transferring IP traffic. The issue could be detected by checking the return value of an API such as m2m_get_system_time(). A negative return value indicates that the SPI is unusable. If this occurs, reset the system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-621	Medium	The AP initiated group rekey process sometimes fails when the WINC is processing a high volume of receive traffic. Recommended workaround: Reconnect the Wi-Fi connection to the AP if a disconnection occurs due to this issue
W3400-102	Medium	During HTTP provisioning, if applications are running on the device being used to provision the WINC3400, they will not be able to access the internet during provisioning. Furthermore, if they attempt to do so, then the WINC3400 can become flooded with DNS requests and crash. This applies to HTTP provisioning only; BLE provisioning is unaffected. Also, this only applies if powersave is enabled. Recommended workarounds: (1) Use M2M_NO_PS when WINC3400 is in HTTP provisioning mode. (2) Close other internet applications (browsers, skype etc) before HTTP provisioning. If crash occurs, reset system via system_reset(). Alternatively, m2m_wifi_reinit() can be used to reset just the WINC. In this case, the different driver modules also need to be initialized (m2m_ota_init(), m2m_ssl_init(), socketInit()).
W3400-40	Medium	The WINC3400 occasionally fails to proceed with 4-way handshake in STA mode, when using 11N WPA2. It does not send M2 after receiving M1. Recommended workaround: Retry the Wi-Fi connection.
W3400-293	Medium	1% of Enterprise conversations fail due to the WINC3400 not sending an EAP response. The response is prepared and ready to send but does not appear on the air. After 10 seconds the firmware times-out the connection attempt and the application is notified of the failure to connect.

		Recommended workaround: Configure the authentication server to retry EAP requests (with interval < 10 seconds). The application should retry the connection request when it is notified of the failure.
W3400-298	Medium	70% of Enterprise connection requests fail with a TP Link Archer D2 access point (TPLink-AC750-D2). The access point does not forward the initial EAP Identity Response to the authentication server. The issue is bypassed by PMKSA caching (WPA2 only), so reconnection attempts will succeed. Recommended workaround: The application should retry the connection request when it is notified of the failure.
W3400-708	Medium	When the WINC3400 is operating in M2M_PS_DEEP_AUTOMATIC powersave mode, and is receiving two concurrent TLS streams, one of which consists of 16KB record sizes, the other has record sizes smaller than 16KB, the WINC3400 can occasionally leak memory buffers when the streams are closed. If sockets in this configuration are opened and closed repeatedly, eventually it will not be possible to open any further TLS sockets, and a restart of the WINC3400 will be needed to restore TLS functionality. Recommended workaround: The leak can be avoided by disabling powersave when receiving two concurrent TLS streams in this configuration.
W3400-461	Low	Sometimes the WINC3400 fails to see ARP responses sent from certain APs at 11Mbps. Recommended workaround: None. The ARP exchange will be retried several times and the response will eventually get through to the WINC3400.
W3400-60	Low	During BLE provisioning, the AP list is not cleaned up at the start of each scan request. As a result, the AP scan list can sometimes display duplicate or old scan entries. Recommended workaround: Only use one scan request during BLE provisioning.
W3400-59	Low	APIs at_ble_tx_power_get() and at_ble_max_PA_gain_get() return default values which do not correspond to the actual gain settings. Recommended workaround: None. Do not use these APIs.
W3400-30	Low	If the TLS server certificate chain contains RSA certificates with keys longer than 2048 bits, the WINC takes several seconds to process it. A Wi-Fi group rekey occurring during this time can cause the TLS handshake to fail. Recommended workaround: Retry opening the secure connection.

W3400-64	Low	at_ble_tx_power_set() needs special handling. Return values 0 and 1 should both be interpreted as successful operation. Refer to WINC3400_BLE_APIs.chm for more detail. Recommended workaround: Process the return value with care, according to the API documentation.
W3400-240	Low	After writing new firmware to the WINC3400, the first Wi-Fi connect attempt in STA mode takes an extra 5 seconds. Recommended workaround: Allow longer for the Wi-Fi connection to complete.
W3400-451	Low	When running in AP mode, the WINC3400 DHCP Server sometimes takes 5 to 10 seconds to assign an IP address. Recommended workaround: Allow longer for DHCP to complete.
W3400-838	Low	When performing intensive crypto operations, the WINC3400 can become unresponsive to host interactions for up to 5 seconds. Specifically, when performing PBKDF2 passphrase to PMK hashing during WPA/WPA2 WiFi connects, or TLS certificate verification using 4096-bit RSA keys, the WINC3400 can take up to 5 seconds to perform the necessary calculations. During this time, it does not service it’s event queues, so any host interactions, and expected responses can be delayed. Recommended workaround: Host code should be written to expect a delay in responses from the WINC3400 of up to 5 seconds in the rare cases that it is busy performing the scenarios described above.

5 Fixes and Enhancements

These are the fixes and enhancements since the previous released version (1.4.4)

5.1 Issues Fixed

Jira ID	Description
W3400-788	**When powersave is enabled, WINC3400 sometimes misses broadcast ARP frames shortly after a new WiFi connection** An internal scheduling problem caused the WINC3400 to sometimes not wake up for beacons on time for a short period after connection, missing broadcast frames Fixed: The scheduling issue has been resolved
W3400-803	**New WiFi connections disallowed after a failed Default Connect** When a Default Connection fails (m2m_wifi_default_connect()), in some instances the WINC3400 will refuse all new connection attempts. Fixed: Ensure new WiFi connections can be attempted after a default connect failure
W3400-816	**Inappropriate casting in m2m_ssl_retrieve_cert()** The casting of variable pu16Curve was leading to corruption of the upper two bytes. Fixed: Code adjusted to resolve casting issue
W3400-819	**Connection parameter info in flash is updated on every re-connection** The Connection Parameter information should only be updated in flash if the connection parameters have changed. However, WINC3400 was updating parts of the Connection Parameter info when there had been no changes, resulting in unnecessary flash writes. Fixed: Code refactored to only write to flash when necessary (e.g. connection parameters (such as SSID, passphrase) are changed)
W3400-823	**Correctly parse and handle the Critical Field of x.509 certificate extensions** The x.509 v3 SAN extension (see rfc5280) includes a boolean designating whether the extension in a certificate is designated as either critical or non-critical. WINC3400 does not parse this extension correctly in this or other x.509 extensions. Fixed: Code adjusted to ensure X.509 extensions are correctly processed
W3400-824	**BLE API improvements/fixes** • Improved handle validation in BLE API; functions will return with error if the presented handle is invalid • Fixed AT_BLE_INDICATION_CONFIRMED structure, no longer returns random data • AT_BLE_NOTIFICATION_CONFIRMED now includes a data structure to allow the application to determine the service or characteristic associated with the message.

W3400-832	**If the BLE API times out when waiting for a response back from the WINC3400, no more BLE API calls can be successfully made.** The error path for a timeout when waiting for a BLE response failed to give a semaphore that was taken at the start of the transaction, resulting in failure of all subsequent BLE API messages over the host interface. Fixed: Fix the error path to ensure the semaphore is given.

5.2 Enhancements

W3400-813	**TLS stack does not check CA Basic Constraint in the server certificate chain** As per RFC 5280 section 4.2.19, a TLS client should check the CA Basic Constraint in certificates in the received server certificate chain. This field should be set in all certificates except the end entity server certificate. The WINC3400 was not checking this field in the certificate chain. Fixed: Implement checking of this field in the WINC3400 TLS stack
W3400-822	**WINC3400 doesn’t support EAPOLv3 messages that can be used in the WPA Enterprise handshake.** Messages of type EAPOLv3 would be ignored, resulting in failed connections. Fixed: Correctly handle EAPOLv3 messages
W3400-828	**Remove dependency for WiFi MAC address to be even when generating BLE MAC address** When generating the BLE MAC address, the WiFi MAC address was required to be even, otherwise the generation would fail and a default MAC address would be used for BLE. Fixed: Generate the BLE MAC address from the WiFi MAC address even if the WiFi MAC address is even
W3400-838	**BLE API calls can timeout when the WINC is performing intense crypto operations** When verifying TLS certificates using 4096-bit RSA keys or performing PBKDF2 passphrase to PMK hashing for WPA/WPA2 WiFi connections, the WINC3400 will not respond to host interactions for up to 5 seconds. Some host BLE API messages will wait for a response – the timeout value of 4 seconds for this response was too low, so the BLE driver code would give up too early and the eventual response would be lost. Fixed: Increase the timeout to 6 seconds to allow for the scenarios described above.
W3400-836	**BLE API calls can timeout when the WINC is processing TLS certificate chains of 4096-bit RSA certificates** When verifying chains of multiple 4096-bit RSA certificates, the WINC3400 can fail to respond to BLE API calls within the 6 second timeout. Fixed: Allow the WINC do more processing between each certificate, reducing the maximum time taken to handle a BLE API message whilst processing 4096-bit RSA chains to around 4 seconds.

6 Appendix A – TLS Root certificates

The WINC3400 1.4.6 module comes with a preselected selection of TLS root certificates that will allow a TLS connection to be established with a range of internet TLS servers out of the box.

These preselected certificates are described in 6.1

6.1 TLS root certificates

Issuer	Filename	Expiry	Public Key	Signature Alg.	Notes
Amazon Root CA 1	AmazonRootCA1.cer	17 January 2038 01:00:00	RSA (2048 bits)	SHA256RSA	AWS Cloud
Baltimore CyberTrust Root	BaltimoreCyber-TrustRoot.cer	13 May 2025 00:59:00	RSA (2048 bits)	SHA1RSA	Azure Cloud
DigiCert High Assurance EV Root CA	DigiCert.cer	10 November 2031 01:00:00	RSA (2048 bits)	SHA1RSA	
DigiCert High Assurance EV Root CA	DigiCertSHA2.cer	22 October 2028 13:00:00	RSA (2048 bits)	SHA256RSA	
Entrust Root Certification Authority	EnTrust.cer	27 November 2026 21:53:42	RSA (2048 bits)	SHA1RSA	
GlobalSign Root CA	GlobalSignRoot.cer	28 January 2028 13:00:00	RSA (2048 bits)	SHA1RSA	
Internet Security Research Group Root X1	isrgrootx1.cer	04 June 2035 12:04:38	RSA (4096 bits)	SHA256RSA	LetsEncrypt
QuoVadis Root CA 2	QuoVadis_Root.cer	24 November 2031 19:23:33	RSA (4096 bits)	SHA1RSA	
VeriSign Class 3 Primary Certification Authority	VeriSign.cer	17 July 2036 00:59:59	RSA (2048 bits)	SHA1RSA	

Terms and Definitions

Term	Definition
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BLE	Bluetooth Low Energy
BSS	Basic Service Set
CBC	Cyclic Block Chaining
DHE	Diffie-Hellman Ephemeral
DNS	Domain Name Server
DTIM	Directed Traffic Indication Map
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read Only Memory
ESD	Electrostatic Discharge
ESS	Extended Service Set (infrastructure network)
GAP	Generic Access Profile
HTTP	Hypertext Transfer Protocol
IBSS	Independent BSS (ad-hoc network)
IEEE	Institute of Electronic and Electrical Engineers
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NDIS	Network Driver Interface Specification
OTA	Over The Air update
PCI	Peripheral Component Interconnect
PMK	Pair-wise Master Key
PSK	Pre-shared Key
RSA	Rivest-Shamir-Adleman (public key cryptosystem)
RSN	Robust Security Network
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
SSID	Service Set Identifier
RSSI	Receive Strength Signal Indicator
TIM	Traffic Indication Map
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WINC	Wireless Network Controller
WLAN	Wireless Local Area Network
WMM™	Wi-Fi Multimedia
WMM-PS™	Wi-Fi Multimedia Power Save
WPA™	Wi-Fi Protected Access
WPA2™	Wi-Fi Protected Access 2 (same as IEEE 802.11i)