Security AT Commands for Open AT Application Framework

Interface Guide

SIERRA WIRELESS

4112704
1.0
June 14, 2013

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where cellular modems are not advised without proper device certifications. These areas include environments where cellular radio can interfere such as explosive atmospheres, medical equipment, or any other equipment which may be susceptible to any form of radio interference. The Sierra Wireless modem can transmit signals that could interfere with this equipment. Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: *Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.*

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitations of Liability

This manual is provided "as is". Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Customer understands that Sierra Wireless is not providing cellular or GPS (including A-GPS) services. These services are provided by a third party and should be purchased directly by the Customer.

SPECIFIC DISCLAIMERS OF LIABILITY: CUSTOMER RECOGNIZES AND ACKNOWLEDGES SIERRA WIRELESS IS NOT RESPONSIBLE FOR AND SHALL NOT BE HELD LIABLE FOR ANY DEFECT OR DEFICIENCY OF ANY KIND OF CELLULAR OR GPS (INCLUDING A-GPS) SERVICES.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product includes technology licensed from QUALCOMM®.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Watcher® is a registered trademark of Netgear, Inc., used under license.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales Desk:	Phone:	1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	E-mail:	sales@sierrawireless.com
Post:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Technical Support:	support@sierrawireless.com	
RMA Support:	repairs@sierrawireless.com	
Fax:	1-604-231-1109	
Web:	www.sierrawireless.com	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases: www.sierrawireless.com

Document History

Version	Date	Updates
1.0	June 14, 2013	Creation

Contents

1. Introduction

The following subsections present introductory information regarding Security Library AT Commands.

1.1. Overview

This document provides Sierra Wireless customers with a description of the AT Commands for Security Services over AT commands.

This document mainly describes how to configure the security for of an HTTPS connection.

Note that the actual HTTP connections are handled as described in the ‘‘Internet Application AT Commands User Guide’’ [2].

For complete information about how to manage the files in the file system, refer to the different methods available in the Developer Studio Help.

1.2. Related Documents

[1] Open AT Application Framework AT Commands Interface Guide for Firmware

4111843

[2] Internet Application AT Commands User Guide

4111706

[3] Security Library for Open AT framework - Development Guide

4112704

1.3. Abbreviations and Glossary

Abbreviation	Definition
3DES	Triple DES.
AES	Advanced Encryption Standard.
API	Application Programming Interface.
DES	Data Encryption Standard.
DSA	Digital Signature Algorithm.
DSS	Digital Signature Standard.
HTTPS	HTTP over SSL.
MAC	Message Authentication Code.
MD5	Message Digest version 5.
OpenSSL	A free SSL toolkit. Please refer to http://www.openssl.org/ for more information.
RSA	The RSA algorithm. R, S, A are the first letter of the surnames of the three creators.
SHA1	Secure Hash Algorithm, version 1.
SHA2	Secure Hash Algorithm, version 2, is a collective name for SHA256, SHA384.
SHA256	Secure Hash Algorithm, version 2, with digest length of 256 bits.
SHA384	Secure Hash Algorithm, version 2, with digest length of 384 bits.

Abbreviation	Definition
SSL	Secure Socket Layer. See TLS.
TLS	Transport Layer Security. The successor to SSL version. Sometimes referred to as SSL when talking generally about TLS/SSL.

2. User Guide

This section provides the introduction and high level description of the Security Library features and AT command set.

2.1. Restriction of Use

The use of the Security AT software described in this document is strictly limited to the use in combination with the Sierra Wireless embedded modules. Please contact a Sierra Wireless representative in case of any questions or concerns.

2.2. Features

The Security AT command set extends the AirPrime embedded module command set to allow users to:

- Configure security settings for TLS/SSL connection used in HTTP(S).
- Release resources.

2.3. AT Command Sequence to Start Security Services

2.3.1. Example of AT command Start Sequence

The AT command sequence to type to set up an HTTPS connection is presented in this section.

Settings are not saved between reboots.

Note that the files referred to in the example below are already considered present in the file system. How they were put in the file system is out of the scope of this document.

2.3.1.1. Start Sequence

AT+WIPCFG=1	*//start IP stack*
OK	
AT+SSLINIT	*//Initialize the Security Library*
OK	
AT+SSLSET=1,"/dir/ca.pem"	*//Set the CA to a file already present in the file system.*
OK	
AT+SSLSET=0,"/dir/client-cert.pem"	*//Set the Client Certificate to a file already present in the file system.*
OK	

AT+SSLSET=2,"/dir/client-key.pem"	*// and the corresponding private key to the Client Certificate*
OK	
AT+SSLSET=3,"randomstring12345"	*// Provide a random string for crypto operations*
OK	
AT+SSLSET=9,3	*// Mandate TLS1.2*
OK	
AT+SSLSETOPTS	*// Sets the parameters previously provided.*
OK	
AT+WIPBR=1,6	*//open GPRS bearer*
OK	
AT+WIPBR=2,6,11,"APN name"	*//set APN name of GPRS bearer*
OK	
AT+WIPBR=2,6,0,"user name"	*//set user name*
OK	
AT+WIPBR=2,6,1,"passwd"	*//set password*
OK	
AT+WIPBR=4,6,0	*//start GPRS bearer*
OK	
AT+SSLBOOST=1	*//Boost the CPU and disables SW Watchdog.*
OK	
AT+WIPCREATE=5,1, "https://www.siteaddress.com",81, "username","password","header name","header value"	*//connect to remote HTTP proxy server port 81 //with authentication and some header fields*
OK	
+WIPREADY: 5,1	*//connection and authentication are successful*
AT+WIPFILE=5,1,1,"https:// www.siteaddress.com:4433"	*// Get the webpage. Please give it some time.*
[UART Switch to Data mode and displays Webpage]	
+WIPFILE: 5,1,1,200,"ok"	
OK	
AT+SSLBOOST=0	*//disable the CPU and re-enable SW Watchdog.*
OK	
at+wipclose=5,1	*//close the channel.*
OK	

3. Security Services States

This section provides information of the Security Services states, their transitions and allowed AT commands for each state.

3.1. State Machine

Below is a diagram of states and transitions of the Security Services application. Please refer to SSLSTATE for how to get the current state.

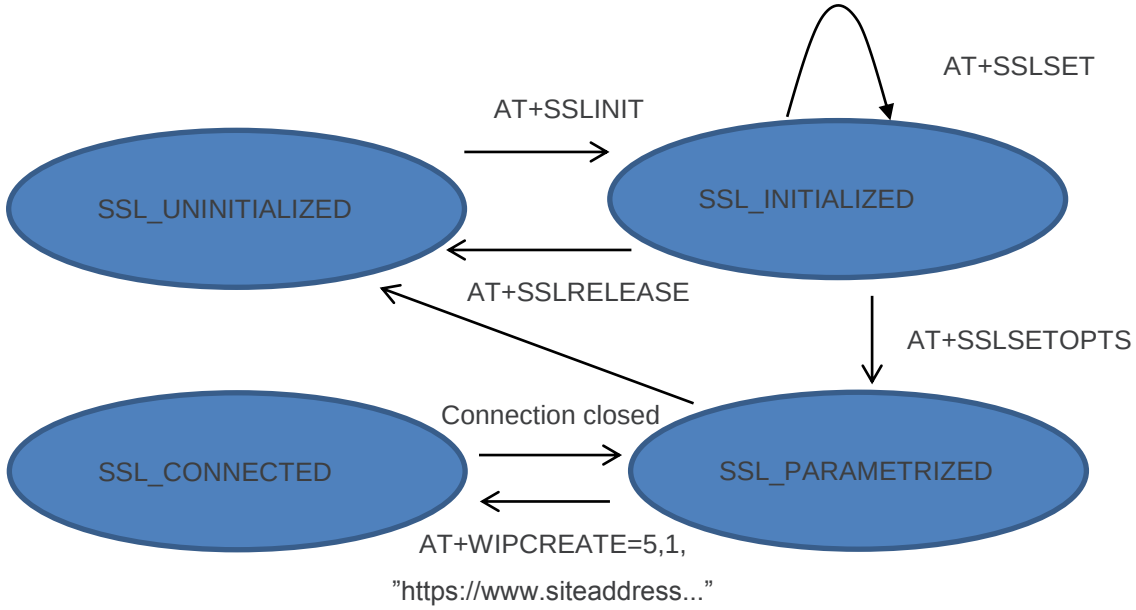

Figure 1. Security Services state diagram

Note that the AT+WIPCREATE is a feature of the Internet Application AT Commands User Guide[2]. The actual SSL connection is handled internally by the Internet Library which handles the HTTP protocol, hence the transition to connected mode is triggered by the Internet Application AT commands when connecting to HTTPS website.

3.2. AT Commands Calls Requirements

The following table shows the prerequisites when using the Security AT commands.

‘X’ means the AT Command is authorized in the corresponding state.

‘-’ means the AT Command is NOT authorized in the corresponding state.

Table 1: Security AT Commands Prerequisites

Function	SSL_UNINITIALIZED	SSL_INITIALIZED	SSL_PARAMETRIZED	SSL_CONNECTED
AT+SSLSTATE	X	X	X	X
AT+SSLINIT	X	-	-	-
AT+SSLSET	-	X	-	-
AT+SSLSETOPTS	-	X	-	-
AT+SSLBOOST	X	X	X	X
AT+SSLRELEASE	-	X	X	-
AT+SSLVERSION	X	X	X	X

4. AT Command Syntax

This section describes the general AT command format and the default value for their parameters.

4.1. Command Line

Commands always start by the standard prefix “AT+SSL” and end with the <CR> character. Optional parameters are shown in brackets [ ].

Example:

AT+SSLcmd=<Param1>[,<Param2>] <CR><LF>

<Param2> is optional.

4.2. Information Responses and Result Codes

Responses start and end with <CR><LF>.

- If command syntax is incorrect, the "ERROR" string is returned.
- If command syntax is correct but transmitted with wrong parameters, the "+SSL ERROR: <Err>" string is returned with adequate error codes. Please refer to Security AT commands error codes description for more details about error code values.
- If the command line has been executed successfully, an "OK" string is returned.

Command	Response
AT+SSLCMD=param	<CR><LF><text><CR><LF>

In the following examples <CR> and <CR><LF> are intentionally omitted.

5. AT Commands Reference

The following AT commands allow the control of Security Services for basic operation.

5.1. Command +SSLINIT

5.1.1. Description

This AT command initializes the Security Library. This command must always be called as the first command. All values are set to default, as explained in subsection 5.2.3.

Please refer to the State Machine and AT Commands Calls Requirements for more information about call state and transition mode.

5.1.2. Syntax

Action command

AT+SSLINIT

OK

Read command

AT+SSLINIT?

OK

Test command

AT+SSLINIT=?

OK

5.1.3. Parameters and Defined Values

There are no parameters for this AT command.

5.1.4. Examples

Command	Responses
AT+SSLINIT *Note: Initializes the Security Library.*	OK

5.2. Command +SSLSET

5.2.1. Description

This AT command configures the parameters for TLS/SSL connection before opening the connection. If a parameter is not explicitly set, the default value will be used. Please note that the default values are set to a recommended value.

Please refer to the State Machine and AT Commands Calls Requirements for more information about call state and transition mode.

5.2.2. Syntax

For <*option*> values 0, 1 and 2.

Action command

AT+SSLSET=<option>,<optionvalue>[,<password>]

OK

For all other <*option*> values

Action command

AT+SSLSET=<option>,<optionvalue>

OK

Read command

AT+SSLSET?

```
+SSLSET: <option>,<optionvalue>
[+SSLSET: <option>,<optionvalue>]
OK
```

Test command

AT+SSLSET=?

```
+SSLSET: <option>,(range for <optionvalue>)
OK
```

5.2.3. Parameters and Defined Values

<option>			**<optionvalue>**	***Default Value***
This parameter specifies the option to set.			Corresponding optionvalue type and range	The value per default
0	SSL_COPT_CERT	Set the modules local Certificate (local public key). The local Certificate file name with path is given as a string in *optionvalue*. The file must already be present in the file system. If the directory is protected with a password, then this must be provided in the <password> variable.	string	-
1	SSL_COPT_CERT_AUTHORITY	Set the Certificate Authority (CA). The CA file name with path is given as a string in *optionvalue*. The file must already be present in the file system. If the directory is protected with a password, then this must be provided in the <password> variable.	string	-
2	SSL_COPT_PRIVATE_KEY	Set the modules local Private Key. The file name with path is given as a string in *optionvalue*. The file must already be present in the file system. If the directory is protected with a password, then this must be provided in the <password> variable.	string	-
3	SSL_COPT_SEED	The random seed used for the randomness of the system.	string	-
4	SSL_COPT_VERIFY	If the CA presented by the server should be checked or not.	0: *do not check* 1: *check*	1
5	SSL_COPT_KEY	The version of authentication allowed.	0: *all* 1: *RSA* 2: *Ephemeral ECDH*	0

<option>			**<optionvalue>**	***Default Value***
6	SSL_COPT_AUTHENTICATION	The version of authentication allowed.	0: *all (except NULL)* 1: *RSA* 2: *DSS* 3: *NULL*	0
7	SSL_COPT_ENCRYPTION	The version of encryption allowed.	0: *all* (except NULL) 1: *DES* 2: *3DES* 3: *RC2* 4: *RC4* 5: *AES* 6: *NULL*	0
8	SSL_COPT_MAC	The version of MAC allowed.	0: *all* 1: *MD5* 2: *SHA1* 3: *SHA2*	0
9	SSL_COPT_VERSION	The version of SSL/TLS allowed.	0: *all* 1: *SSL3.0* 2: *TLS1.0* 3: *TLS1.2*	0
10	SSL_COPT_SESSION_MODE	SSL Session ID automatic usage. When possible the underlying security framework will try to reuse session, thus speeding up the session connection.	0: *Off* 1: *On.*	1

<password>	**Type**	***Default Value***
The password needed to access the directory containing the file.	string	-

5.2.4. Examples

Command	**Responses**
AT+SSLSET=0,"/dir/client-cert.pem" *Note: Set the path to the Client Certificate file that is already present in the file system.*	OK

Command	Responses
AT+SSLSET=1,"/dir/ca.pem" *Note: Set the path to the CA file that is already present in the file system.*	OK
AT+SSLSET=2,"/dir/client-key.pem" *Note: Set the path to the Client Private Key that is already present in the file system..*	OK
AT+SSLSET=3,"randomstring123456789" *Note: Provide a random string for crypto operations.*	OK
AT+SSLSET=4,1 *Note: Verify the server certificates against the local CA.*	OK
AT+SSLSET=5,0 *Note: allow all keys.*	OK
AT+SSLSET=6,1 *Note: allow only RSA authentication.*	OK
AT+SSLSET=7,5 *Note: allow only AES authentication.*	OK
AT+SSLSET=8,3 *Note: allow only SHA2 as MAC algorithm.*	OK
AT+SSLSET=9,3 *Note: allow only TLS1.2.*	OK
AT+SSLSET=10,1 *Note:HTTPS Session auto reuse set on.*	OK

5.3. Command +SSLSETOPTS

5.3.1. Description

This AT command sets all parameters previously provided via AT+SSLSET. If the command is successfully called in state SSL_INITLIALIZED, the state changes to SSL_PARAMETRIZED.

Please refer to the State Machine and AT Commands Calls Requirements for more information about call state and transition mode.

5.3.2. Syntax

Action command

AT+SSLSETOPTS

OK

Read command

AT+SSLSETOPTS?

OK

Test command

AT+SSLSETOPTS=?

OK

5.3.3. Parameters and Defined Values

There are no parameters for this AT command.

5.4. Command +SSLRELEASE

5.4.1. Description

This AT command closes the library and frees the associated resources. After this is called all settings previously set will be reset to default values. State will be SSL_UNINITIALIZED after this command is successfully called.

Please refer to the State Machine and AT Commands Calls Requirements for more information about call state and transition mode.

5.4.2. Syntax

Action command

AT+SSLRELEASE
OK

Read command

AT+SSLRELEASE?

OK

Test command

AT+SSLRELEASE=?
OK

5.4.3. Parameters and Defined Values

There are no parameters for this AT command.

5.4.4. Examples

Command	Responses
AT+SSLRELEASE	OK *Note: Frees all resources and resets all parameters.*

5.5. Command +SSLSTATE

5.5.1. Description

This AT command will return the state refer to in the State Machine.

5.5.2. Syntax

Action command

AT+SSLSTATE
+SSLSTATE: <state>
OK

Read command

AT+SSLSTATE?
OK

Test command

AT+SSLSTATE=?
OK

5.5.3. Parameters and Defined Values

<state>:

0	SSL_UNINITIALIZED
1	SSL_INITIALIZED
2	SSL_CONNECTED
3	SSL_PARAMETRIZED

5.5.4. Examples

Command	Responses
AT+SSLSTATE	0 OK

5.6. Command +SSLBOOST

5.6.1. Description

This AT command boosts the system to give extra calculation power during the SSL connection.

More specifically, it takes control of the Varispeed service, boosts the CPU speed, and then disables the Software watchdog.

5.6.2. Syntax

Action command

AT+SSLBOOST=<option>

OK

Read command

AT+SSLBOOST?
+SSLBOOST: <option>
OK

Test command

AT+SSLBOOST=?
+SSLBOOST: (range for <option>)

OK

5.6.3. Parameters and Defined Values

<state>:

0	Disable boost mode. This is the default value at startup. Reset CPU Varispeed speed to normal. Relase control of the Varispeed service. Re-enable the Software watchdog.
1	Enable boost mode. Takes control of the Varispeed service. Enables CPU Varispeed speed to high. Disables the Software watchdog for 120 seconds.

5.6.4. Examples

Command	Responses
AT+SSLBOOST=0	OK *Note: Disables SSL BOOST.*
AT+SSLBOOST=1	OK *Note: Enables SSL BOOST.*

5.7. Command +SSLVERSION

5.7.1. Description

This AT command displays the underlying versions of different system.

5.7.2. Syntax

Action command

AT+SSLVERSION=<option>
+SSLVERSION: (version string)

OK

Read command

AT+SSLVERSION?
OK

Test command

AT+SSLVERSION=?
+SSLVERSION: (range for <option>)
OK

5.7.3. Parameters and Defined Values

<option>:

0	The Security Library version.
1	The underlying OpenSSL version..
2	The highest possible SSL version capability of the current compilation of the Security library.

5.7.4. Examples

Command	Responses
AT+SSLVERSION=1	+SSLVERSION: OpenSSL 1.0.1c 10 May 2012 OK

6. Asynchronous Events

There are no asynchronous events from the Security Services events.
Please note that the HTTP(S) connection is handled via the Internet Application AT please refer to the [2] Internet Application AT Commands User Guide.

7. Security AT Commands Error Codes

The following error codes could be returned from Security AT commands.

Table 2: Security AT commands error codes

Error Code	Error name	Description
901	Invalid option	Not correct number of parameters.
902	Invalid option value	Bad parameter value..
903	Bad state	Calling an AT command when the Security Library is in a bad state. Please see table in chapter 0.
904	Not enough memory	Running out of free memory.
905	File not present	File specified is not present in the file system.
906	File access problem	File is present but there was an error while accessing it. Bad password will result in this error.
907	Unknown Error	The reason for this error is unknown.
908	Bad CA	The content of the CA file was read but not accepted.
909	Bad Client Cert	The content of the Client Cert file was read but not accepted.
910	Bad Client Key	The content of the Client Key file was read but not accepted.

Index

SIERRA
WIRELESS