



SIM800系列_SSL_应用文档_V1.01



手册名称	SIM800 系列_SSL_应用文档
版本	1.01
日期	2014-06-30
状态	发布
文档控制号	SIM800 系列_SSL_应用文档_V1.01

一般事项

SIMCom把本手册作为一项对客户的服务，编排紧扣客户需求，章节清晰、叙述简要，力求客户阅读后，可以通过AT命令轻松使用模块，加快开发应用和工程计划的进度。

SIMCom不承担对相关附加信息的任何独立试验，包含可能属于客户的任何信息。而且，对一个包含SIMCom模块、较大型的电子系统而言，客户或客户的系统集成商肩负其系统验证的责任。

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。手册中信息修改，恕不另行通知。

版权

本手册包含芯讯通无线科技（上海）有限公司的专利技术信息。除非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本手册内容的部分或全部，并不得以任何形式传播，犯规者可被追究支付赔偿金。对专利或者实用新型或者外观设计的版权所有，SIMCom保留一切权利。

版权所有© 芯讯通无线科技（上海）有限公司2014年

目录

1. SSL 功能.....	5
1.1. SSL介绍.....	5
1.2. HTTPS 介绍.....	5
1.3. FTPS 介绍.....	5
1.4. EMAIL 加密传输 介绍.....	6
1.5. SSL AT命令使用	6
2. AT 命令.....	7
2.1. AT+EMAILSSL 设置邮件使用SSL功能.....	7
2.2. AT+HTTPSSL 设置HTTP使用SSL功能.....	8
2.3. AT+FTPSSL 设置FTP使用SSL功能.....	8
2.4. AT+CIPSSL 设置TCP使用SSL功能.....	9
2.5. AT+SSLSETCERT 导入SSL证书	9
2.6. AT+SSLOPT SSL选项设置	10
3. 应用实例	11
3.1. EMAIL使用普通端口加密发送邮件	11
3.2. EMAIL使用加密端口发送邮件	11
3.3. EMAIL使用普通端口加密接收邮件	12
3.4. EMAIL使用加密端口接收邮件	14
3.5. HTTPS GET方法.....	15
3.6. 使用FTPS的Implicit模式下载数据	16
3.7. 使用FTPS的Explicit模式下载数据	17
3.8. TCP建立一个SSL加密的客户端链接.....	18
3.9. 多链路模式下TCP建立SSL加密的客户端链接.....	18
3.10. 导入SSL证书.....	19
附录.....	21
A. 参考文档.....	21
B. 术语和缩写.....	21

版本历史

日期	版本	修改点描述	作者
2013-10-18	1.00	第一版	张平
2014-06-30	1.01	章节适用范围，修改部分项目	张平
		章节 2.4，增加 SSL 加密的 TCP 连接描述	刘涵君
		章节 2.5，增加 SSL 导入证书描述	刘涵君
		章节 2.6，增加 SSL 选项设置	张平
		章节 3.8、3.9、3.10，增加应用实例	张平

适用范围

本手册描述了 SSL 相关 AT 命令操作方法和应用实例。本手册适用于 SIM800, SIM800-WB64, SIM800H（不带蓝牙功能）和 SIM800G。

1. SSL 功能

1.1. SSL介绍

安全套接层（Secure Sockets Layer, SSL），一种安全协议，是网景公司（Netscape）在推出Web浏览器首版的同时提出的，目的是为网络通信提供安全及数据完整性。SSL在传输层对网络连接进行加密。

SSL采用公开密钥技术，保证两个应用间通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。它在服务器和客户机两端可同时被支持，目前已成为互联网上保密通讯的工业标准。现行Web浏览器亦普遍将HTTP和SSL相结合，从而实现安全通信。此协议和其继任者是TLS（Transport Layer Security, TLS）。

TLS利用密钥算法在互联网上提供端点身份认证与通讯保密，其基础是公钥基础设施（public key infrastructure, PKI）。不过在实现的典型例子中，只有网络服务者被可靠身份验证，而其客户端则不一定。这是因为公钥基础设施普遍商业运营，电子签名证书通常需要付费购买。协议的设计在某种程度上能够使主从式架构应用程序通讯本身预防窃听、干扰（Tampering）、和消息伪造。

SIM800 系列模块目前支持 SSL2.0, SSL3.0, TLS1.0

1.2. HTTPS 介绍

HTTPS 是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。即 HTTP 下加入 SSL 层，HTTPS 的安全基础是 SSL，因此加密的详细内容请看 SSL。

它是一个URI scheme(抽象标识符体系), 句法类同http:体系。用于安全的HTTP数据传输。HTTPS:URL表明它使用了HTTP, 但HTTPS存在不同于HTTP的默认端口及一个加密/身份验证层（在HTTP与TCP之间）。这个系统的最初研发由网景公司进行，提供了身份验证与加密通讯方法，现在它被广泛用于万维网上安全敏感的通讯，例如交易支付方面。

1.3. FTPS 介绍

一种多传输协议，相当于加密版的FTP。当你在FTP服务器上收发文件的时候，你面临两个风险。第一个风险是在上载文件的时候为文件加密。第二个风险是，这些文件在你等待接收方下载的时候将停留在FTP服务器上，这时你如何保证这些文件的安全。你的第二个选择(创建一个支持SSL的FTP服务器)能够让你的主机使用一个FTPS连接上载这些文件。这包括使用一个在FTP协议下面的SSL层加密控制和数据通道。一种替代FTPS的协议是安全文件传输协议(SFTP)。这个协议使用SSH文件传输协议加密从客户机到服务器的FTP连接。

FTPS是在安全套接层使用标准的FTP协议和指令的一种增强型FTP协议，为FTP协议和数据通道增加了SSL安全功能。FTPS也称作“FTP-SSL”和“FTP-over-SSL”。SSL是一个在客

户机和具有SSL功能的服务器之间的安全连接中对数据进行加密和解密的协议。

1.4. EMAIL 加密传输 介绍

对于接收邮件，我们提供了 SSL 加密的 POP3 协议被称为 POP3S。使用特殊的端口，默认为：995。对于发送邮件，我们采用 HTTPS 方式通讯，默认端口是：465。也支持使用普通端口，通过 STARTTLS（SMTP）和 STLS（POP3）来启用加密传输。

1.5. SSL AT命令使用

在标准模块上使用 SSL 功能，我们提供了一套 AT 命令来支持 SSL 操作，包括 HTTP，EMAIL 和 FTP 功能。

2. AT 命令

SIM800 系列模块提供加密链接的 AT 命令如下：

命令	描述
AT+EMAILSSL	设置 EMAIL 使用 SSL 功能
AT+HTTPSSL	设置 HTTP 使用 SSL 功能
AT+FTPSSL	设置 FTP 使用 SSL 功能
AT+CIPSSL	设置 TCPIP 使用 SSL 功能
AT+SSLSETCERT	导入 SSL 证书
AT+SSLOPT	SSL 选项设置

2.1. AT+EMAILSSL 设置邮件使用SSL功能

AT+EMAILSSL 设置邮件使用 SSL 功能	
测试命令 AT+EMAILSSL=?	<p>响应</p> <p>+EMAILSSL: (list of supported <n>s)</p> <p>OK</p> <p>参数</p> <p>见设置命令</p>
查询命令 AT+EMAILSSL?	<p>响应</p> <p>+ EMAILSSL: <n></p> <p>OK</p> <p>参数</p> <p>见设置命令</p>
设置命令 AT+EMAILSSL=<n>	<p>响应</p> <p>OK</p> <p>参数</p> <p><n> 0 不要加密传输 1 使用加密端口进行加密传输 2 使用普通端口进行加密传输</p>
参考	<p>备注:</p> <p>如果 SSL 通道建立失败或者通讯错误，发送邮件的时候会返回错误码：</p> <p>+SMTPSEND: <code></p> <p>登录 POP3 服务器的时候会返回错误码：</p> <p>+POP3IN: <code></p> <p><code> 71 SSL 建立通道失败 72 SSL 通讯警告错误</p>

2.2. AT+HTTPSSL 设置HTTP使用SSL功能

AT+HTTPSSL 设置 HTTP 使用 SSL 功能	
测试命令 AT+HTTPSSL=?	响应 +HTTPSSL: (0-1)
	OK 参数 见设置命令
查询命令 AT+HTTPSSL?	响应 + HTTPSSL: <n>
	OK 参数 见设置命令
设置命令 AT+HTTPSSL=<n>	响应 OK
	参数 <n> 0 关闭SSL功能 1 打开 SSL 功能
参考	备注: HTTPACTION 失败时会返回错误码: +HTTPACTION: <code> <code> 605 SSL 建立通道失败 606 SSL 通讯警告错误

2.3. AT+FTPSSL 设置FTP使用SSL功能

AT+FTPSSL 设置 FTP 使用 SSL 功能	
测试命令 AT+FTPSSL=?	响应 +FTPSSL: (0-2)
	OK 参数 见设置命令
查询命令 AT+FTPSSL?	响应 + FTPSSL: <n>
	OK 参数 见设置命令
设置命令 AT+FTPSSL=<n>	响应 OK

	<p>参数</p> <p><n> <u>0</u> 关闭SSL功能</p> <p> 1 使用 FTPS 的 Implicit 模式</p> <p> 2 使用 FTPS 的 Explicit 模式</p>
参考	<p>备注:</p> <p>FTP 操作失败时会返回错误码, 以 FTPGET 为例:</p> <p>+FTPGET: <code></p> <p><code> 80 SSL 建立通道失败</p> <p> 81 SSL 通讯警告错误</p> <p> 82 FTP 协商扩展验证错误</p> <p> 83 FTP 协商保护缓冲区错误</p> <p> 84 FTP 协商保护级别错误</p>

2.4. AT+CIPSSL 设置TCP使用SSL功能

AT+CIPSSL 设置 TCP 使用 SSL 功能

测试命令 AT+CIPSSL=?	<p>响应</p> <p>+CIPSSL: (0-1)</p> <p>OK</p> <p>参数</p> <p>见设置命令</p>
查询命令 AT+CIPSSL?	<p>响应</p> <p>+ CIPSSL: <n></p> <p>OK</p> <p>参数</p> <p>见设置命令</p>
设置命令 AT+CIPSSL=<n>	<p>响应</p> <p>OK</p> <p>参数</p> <p><n> <u>0</u> 关闭SSL功能</p> <p> 1 打开 SSL 功能</p>
参考	<p>备注:</p> <p>打开 SSL 功能后, 模块会在 TCP 连接建立后自动进行 SSL 验证。</p> <p>当前仅支持作为 SSL Client 应用</p>

2.5. AT+SSLSETCERT 导入SSL证书

AT+SSLSETCERT 导入 SSL 证书

测试命令 AT+SSLSETCERT=?	<p>响应</p> <p>+SSLSETCERT: 参数<file>的最大长度,参数<password>的最大长度</p>
--------------------------------	--

	OK
设置命令 AT+SSLSETCERT =<file>[,<password >]	响应 OK 如果导入成功 +SSLSETCERT: 0 如果导入失败 +SSLSETCERT: 1
	参数 <file> 待导入的文件。文件名(含路径)最多输入 100 个字符 <password> 导入文件需要的密码，最多 32 个字符
参考	备注： <ul style="list-style-type: none"> ● 只能导入一个证书。如果导入多次，模块只保留最后一次导入的证书。 ● 支持导入".crt"或".cer"证书文件

2.6. AT+SSLOPT SSL选项设置

AT+SSLOPT SSL 选项设置	
测试命令 AT+SSLOPT=?	响应 +SSLOPT: (参数<opt>的范围),(参数<enable>的范围) OK 参数 见设置命令
查询命令 AT+SSLOPT?	响应 +SSLOPT: 0,<enable> +SSLOPT: 1,<enable> OK 参数 见设置命令
设置命令 AT+SSLOPT=<opt >,<enable>	响应 OK 参数 <opt> 0 忽略无效证书功能 1 客户端认证功能 <enable> 0 功能关闭 1 功能开启
参考	备注： 客户端认证功能目前没有实现

3. 应用实例

下面的表格提供一些 SSL 功能的使用方法。

如下表格“语法”列中黑色文字是输入给模块的AT命令，蓝色文字是模块返回值。

3.1. EMAIL使用普通端口加密发送邮件

语法	说明
AT+SAPBR=3,1,"APN","CMNET" OK	配置承载场景 1
AT+SAPBR=1,1 OK	激活承载场景 1
AT+EMAILCID=1 OK	配置 EMAIL 使用承载场景 1
AT+EMAILTO=30 OK	设置 EMAIL 超时时间
AT+EMAILSSL=2 OK	设置 EMAIL 使用普通端口进行加密传输
AT+SMTPSRV="SMTP.GMAIL.COM" OK	设置 SMTP 服务器地址，端口省略，表示使用默认端口：25
AT+SMTPAUTH=1,"account","password" OK	设置用户名和密码
AT+SMTPFROM="account@GMAIL.COM","account" OK	设置发送方地址和名字
AT+SMTPSUB="Test" OK	设置邮件主题
AT+SMTPRCPT=0,0,"john@sim.com","john" OK	设置接收方(To:)
AT+SMTPBODY=19 DOWNLOAD This is a new Email OK	设置邮件正文
AT+SMTPSEND OK +SMTPSEND: 1	发送邮件

3.2. EMAIL使用加密端口发送邮件

语法	说明
----	----

AT+SAPBR=3,1,"APN","CMNET" OK	配置承载场景 1
AT+SAPBR=1,1 OK	激活承载场景 1
AT+EMAILCID=1 OK	配置 EMAIL 使用承载场景 1
AT+EMAILTO=30 OK	设置 EMAIL 超时时间
AT+EMAILSSL=1 OK	设置 EMAIL 使用加密端口进行加密传输
AT+SMTPSRV="SMTP.GMAIL.COM" OK	设置 SMTP 服务器地址，端口省略，表示使用默认端口：465
AT+SMTPAUTH=1,"account","password" OK	设置用户名和密码
AT+SMTPFROM="account@GMAIL.COM","account" OK	设置发送方地址和名字
AT+SMTPSUB="Test" OK	设置邮件主题
AT+SMTPRCPT=0,0,"john@sim.com","john" OK	设置接收方(To:)
AT+SMTPBODY=19 DOWNLOAD This is a new Email OK	设置邮件正文
AT+SMTPSEND OK +SMTPSEND: 1	发送邮件

3.3. EMAIL使用普通端口加密接收邮件

语法	说明
AT+SAPBR=3,1,"APN","CMNET" OK	配置承载场景 1
AT+SAPBR=1,1 OK	激活承载场景 1
AT+EMAILCID=1 OK	配置 EMAIL 使用承载场景 1
AT+EMAILTO=30 OK	设置 EMAIL 超时时间

AT+EMAILSSL=2 OK	设置 EMAIL 使用加密端口进行加密传输
AT+POP3SRV="mail.sim.com","john","123456" OK	设置 POP3 服务器地址，账户，密码，端口不设置，默认为 110
AT+POP3IN OK +POP3IN: 1	登录 POP3 服务器
AT+POP3NUM OK +POP3NUM: 1,2,11124	得到邮件总数和总的大小
AT+POP3LIST=1 OK +POP3LIST: 1,1,5556	得到第一封邮件的大小
AT+POP3CMD=4,1 OK +POP3CMD: 1	读取第一封邮件
AT+POP3READ=1460 +POP3READ: 1,1460 ... OK AT+POP3READ=1460 +POP3READ: 1,1460 ... OK	读取该邮件内容
AT+POP3READ=1460 +POP3READ: 2,1183 ... OK	该邮件内容已经读完
AT+POP3OUT OK +POP3OUT: 1	退出 POP3 服务器

3.4. EMAIL使用加密端口接收邮件

语法	说明
AT+SAPBR=3,1,"APN","CMNET" OK	配置承载场景 1
AT+SAPBR=1,1 OK	激活承载场景 1
AT+EMAILCID=1 OK	配置 EMAIL 使用承载场景 1
AT+EMAILTO=30 OK	设置 EMAIL 超时时间
AT+EMAILSSL=1 OK	设置 EMAIL 使用加密端口进行加密传输
AT+POP3SRV="mail.sim.com","john","123456" OK	设置 POP3 服务器地址，账户，密码，端口不设置，默认为 995
AT+POP3IN OK +POP3IN: 1	登录 POP3 服务器
AT+POP3NUM OK +POP3NUM: 1,2,11124	得到邮件总数和总的大小
AT+POP3LIST=1 OK +POP3LIST: 1,1,5556	得到第一封邮件的大小
AT+POP3CMD=4,1 OK +POP3CMD: 1	读取第一封邮件
AT+POP3READ=1460 +POP3READ: 1,1460 ... OK AT+POP3READ=1460 +POP3READ: 1,1460 ... OK	读取该邮件内容
AT+POP3READ=1460	该邮件内容已经读完

+POP3READ: 2,1183 ... OK	
AT+POP3OUT OK +POP3OUT: 1	退出 POP3 服务器

3.5. HTTPS GET方法

从 HTTPS 服务器下载数据。

语法	说明
AT+HTTPIPINIT OK	初始化 HTTP 服务
AT+HTTTPARA="CID",1 OK AT+HTTTPARA="URL","www.gmail.com" OK AT+HTTTPARA="REDIR",1 OK	设置 HTTP 会话参数
AT+HTTSSL=1 OK	打开 HTTPS 功能
AT+HTTTPACTION=0 OK +HTTTPACTION: 0,200,84200	GET 会话开始 GET 成功
AT+HTTTPREAD +HTTTPREAD: 84200 OK	读取 HTTP 服务器的数据 向 UART 口输出数据
AT+HTTPTERM OK	结束 HTTP 服务

3.6. 使用FTPS的Implicit模式下载数据

以 Implicit 模式从 FTP 服务器下载数据。

语法	说明
AT+FTPCID=1 OK AT+FTPSERV="116.228.221.52" OK AT+FTPUN="sim.cs1" OK AT+FTPPW="*****" OK AT+FTPGETNAME="1K.txt" OK AT+FTPGETPATH="/"	设置 FTP 会话参数
AT+FTPSSL=1 OK	打开 FTPS 的 Implicit 模式
AT+FTPGET=1 OK +FTPGET: 1,1	打开 FTP GET 会话 数据可读
AT+FTPGET=2,1024 +FTPGET: 2,50 012345678901234567890123456789012345678901 23456789 OK	请求读取1024字节，但当前仅50字节可读
AT+FTPGET=2,1024 +FTPGET: 2,0 OK +FTPGET: 1,1	再次请求读取1024字节。 当前没有数据可读，但会话尚未结束 如果模块收到了数据，但用户没有输入“AT+FTPGET:2, <reqlength>”来读取数据，“+FTPGET:1,1”会在一定时间后再次显示
AT+FTPGET=2,1024 +FTPGET: 2,1024 012345678901234567890123456789012345678901 234567890.....1234 OK +FTPGET:1,0	请求读取1024字节数据 当前有 1024 字节数据可读 数据传输结束，FTP 服务器连接关闭

3.7. 使用FTPS的Explicit模式下载数据

以 Explicit 模式从 FTP 服务器下载数据。

语法	说明
AT+FTPCID=1 OK AT+FTPSERV="116.228.221.52" OK AT+FTPUN="sim.cs1" OK AT+FTPPW="*****" OK AT+FTPGETNAME="1K.txt" OK AT+FTPGETPATH="/"	设置 FTP 会话参数
AT+FTPSSL=2 OK	打开 FTPS 的 Explicit 模式
AT+FTPGET=1 OK +FTPGET: 1,1	打开 FTP GET 会话 数据可读
AT+FTPGET=2,1024 +FTPGET: 2,50 012345678901234567890123456789012345678901 23456789 OK	请求读取1024字节，但当前仅50字节可读
AT+FTPGET=2,1024 +FTPGET: 2,0 OK +FTPGET: 1,1	再次请求读取1024字节。 当前没有数据可读，但会话尚未结束 如果模块收到了数据，但用户没有输入“AT+FTPGET:2, <reqlength>”来读取数据，“+FTPGET:1,1”会在一定时间后再次显示
AT+FTPGET=2,1024 +FTPGET: 2,1024 012345678901234567890123456789012345678901 234567890.....1234 OK +FTPGET:1,0	请求读取1024字节数据 当前有 1024 字节数据可读 数据传输结束，FTP 服务器连接关闭

3.8. TCP建立一个SSL加密的客户端链接

AT+CGATT? +CGATT: 1 OK	检查 GPRS 附着状态
AT+CSTT="CMNET" OK	开始任务，设置 APN。 默认 APN 是 “CMNET”，没有用户名和密码。可以查询当地 GSM 运营商来获得 APN
AT+CIICR OK	建立无线链路 (GPRS 或者 CSD)
AT+CIFSR 10.78.245.128	获得本地 IP 地址
AT+CIPSSL=1 OK	打开 SSL 功能
AT+CIPSTART="TCP","116.228.221.51","8500" OK CONNECT OK	建立 TCP 链接 TCP 链接成功建立。SSL 验证完成
AT+CIPSEND > hello TCP serve SEND OK hello SIM800 CLOSED	发送数据到远端服务，CTRL+Z (0x1a) 发送。 用户必须要等到 “>”后才输入数据，然后用 CTRL+Z 发送。用户可以用命令 “AT+CIPSPRT” 来设置是否在字符串 “AT+CIPSEND”后显示提示符 “>”。 数据已经发送出去并且被远端服务器成功接收 收到远端服务器发来数据 远端服务器关闭了链接

3.9. 多链路模式下TCP建立SSL加密的客户端链接

仅在设置 SSL 功能打开后，建立的 TCP 连接才是 SSL 加密的 TCP 连接。在 SSL 打开前已经建立的 TCP 连接不会进行 SSL 验证。

语法	说明
AT+CGATT? +CGATT: 1 OK	检查 GPRS 附着状态
AT+CIPMUX=1 OK	设置多链路模式
AT+CSTT="CMNET" OK	开始任务，设置 APN

AT+CIICR OK	建立无线链路(GPRS 或者 CSD)
AT+CIFSR 10.78.245.128	获得本地 IP 地址
AT+CIPSTART=0, "TCP", "116.228.221.51", "8500" OK 0, CONNECT OK	在第 0 路建立 TCP 链接
AT+CIPSSL=1 OK	打开 SSL 功能。此时第 0 路的 TCP 连接仍保持为普通连接，而不会进行 SSL 连接。
AT+CIPSTART=1, "TCP", "116.228.221.51", "9600" OK 1, CONNECT OK	在第1路建立TCP链接。SSL验证完成。
AT+CIPSEND=0 > TCP test 0, SEND OK	第0路发送数据
AT+CIPSEND=1 > TCP Over SSL test 1, SEND OK +RECEIVE,0,17: SIM800 TCP test +RECEIVE,1,26: SIM800 TCP Over SSL test 0, CLOSED	第1路发送数据 第0路收到数据，长度是17 第1路收到数据，长度是26 第0路链接被远端关闭
AT+CIPSTATUS OK STATE: IP PROCESSING C: 0,0,"TCP","116.228.221.51","8500","CLOSED " C: 1,0,"TCP","116.228.221.51","9600","CONNECTED " C: 2,,"","","","INITIAL " C: 3,,"","","","INITIAL " C: 4,,"","","","INITIAL " C: 5,,"","","","INITIAL "	查询当前链接状态

3.10. 导入SSL证书

Grammar	Description
AT+FSCREATE=C:\USER\HENRY_SSL.CRT OK	在文件系统上建立证书文件.
AT+FSWRITE=C:\USER\HENRY_SSL.CRT,0,1196,10 > OK	证书内容写入刚才创建的文件中
AT+SSLSETCERT="C:\USER\HENRY_SSL.CRT","**** ****" OK	导入证书文件
+SSLSETCERT: 0	导入成功

附录

A. 参考文档

编号	文档名称	说明
[1]	SIM800 Series AT Command Manual	

B. 术语和缩写

术语	描述
URC	主动上报命令
TE	终端设备
TA	终端适配器
DTE	数据终端设备或简单地说是在嵌入式系统上运行的应用
DCE	数据通信设备 DCE 或传真（传真调制解调器，传真卡）
ME	移动设备
MS	基站
SSL	安全套接层
TLS	安全传输层协议

联系我们:

芯讯通无线科技（上海）有限公司

地址：上海市金钟路 633 号晨讯科技大楼 A 楼

邮编：200335

电话：+86 21 3252 3300

传真：+86 21 3252 3020

网址：www.sim.com/wm

SIMCOM CONFIDENTIAL FILE