

# USR-C322 SSL Client 通信说明

V1.0



## 1、SSL 通信说明

首先检查您模块的版本号，如果版本低于 V2.1.10，则需要升级固件才能支持此功能。

SSLSocket 通信是对 SOCKET 通信的拓展, 支持 TCP Client 模式。

SSL 通信是在 Socket 通信的基础上添加了一层安全性保护，提供了更高的安全性，包括身份验证、数据加密以及完整性验证。

其中身份验证用于数字证书的发放和应用。

数据加密可以防止消息传递过程中被别人监听而造成的损失，即使第三方监听到传递的消息，但是由于没有正确的密钥，其仍然无法得到正确的消息。

完整性验证以防止消息在传递过程中被别人修改。

加密类型支持：

- ◆ SSLV3
- ◆ TLSV1
- ◆ TLSV1\_1
- ◆ TLSV1\_2
- ◆ SSLv3\_TLSV1\_2
- ◆ DLSV1

加密算法支持：

- |                                      |              |
|--------------------------------------|--------------|
| ◆ SSL_RSA_WITH_RC4_128_SHA           | 对应网页 SSL_SHA |
| ◆ SSL_RSA_WITH_RC4_128_MD5           | 对应网页 SSL_MD5 |
| ◆ TLS_RSA_WITH_AES_256_CBC_SHA       | 对应网页 TLS     |
| ◆ TLS_DHE_RSA_WITH_AES_256_CBC_SHA   | 对应网页 TLS_DHE |
| ◆ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | 对应网页 TLS_256 |
| ◆ TLS_ECDHE_RSA_WITH_RC4_128_SHA     | 对应网页 TLS_128 |
| ◆ SECURE_DEFAULT                     | 对应网页 DEFAULT |

支持加密证书设置（[加密证书烧写方法参考无线升级软件说明](#)）只有 UART1 支持此模式。

## 2、使用例程

本例程连接到支付宝：<https://www.alipay.com/>

### 1) 查看网站证书加密类型和加密方式

使用 IE 11 浏览器，地址栏输入 <https://www.alipay.com/>，回车，如图 1，可以看到地址栏前端有“https”。

点击“查看”-->“安全报告”，弹出如图 2，点击“查看证书”，弹出如图 3 窗口。

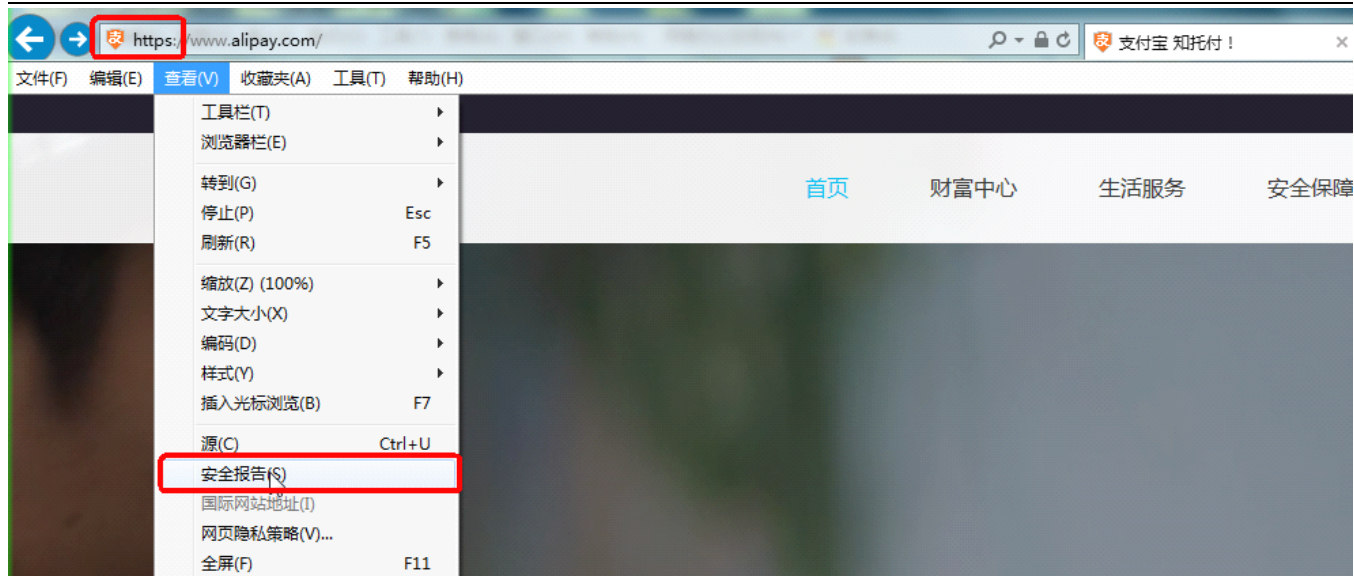


图 1



图 2

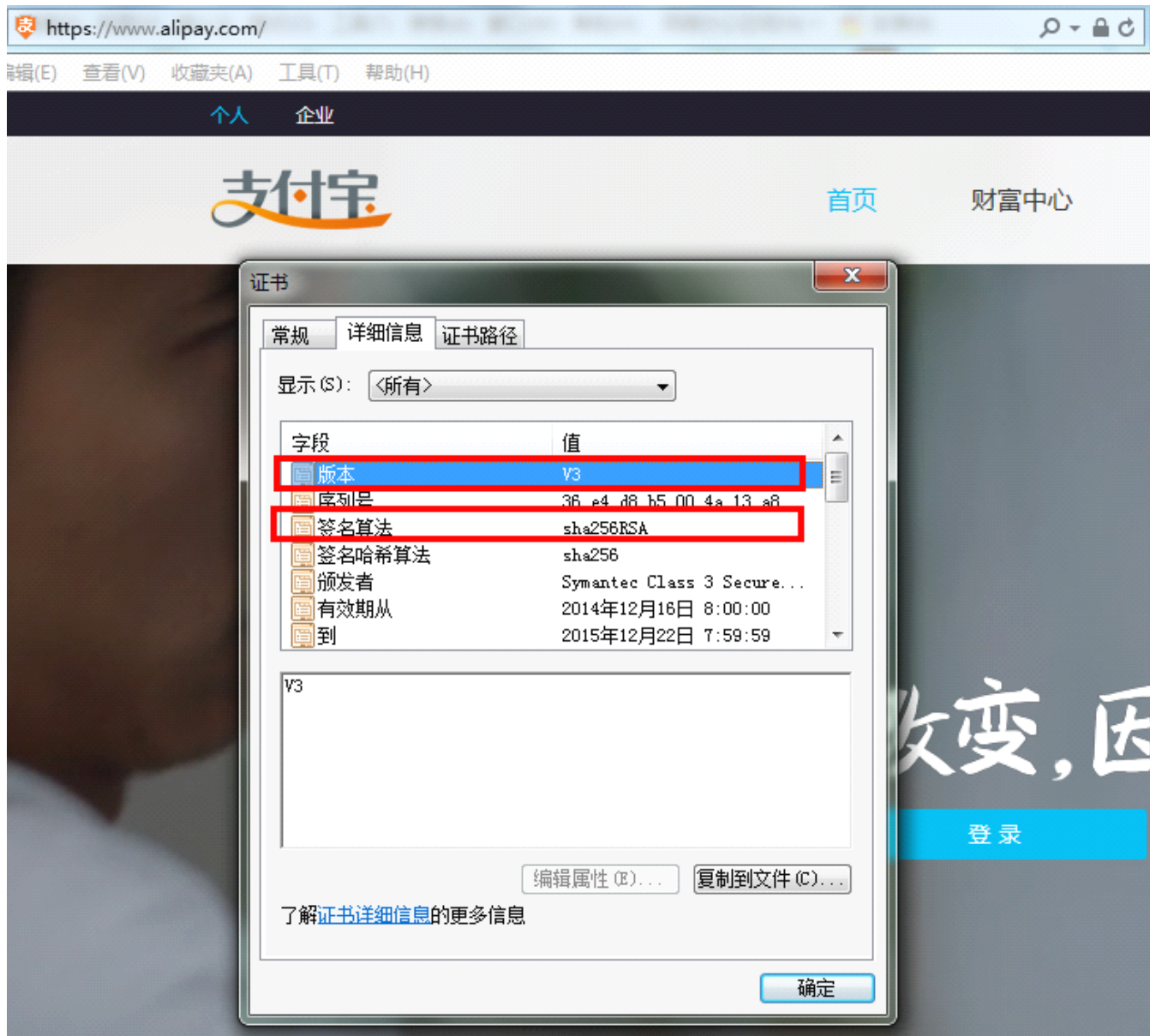


图 3

- ◆ 在图 3 证书信息页面,可以看见证书版本“V3”(即 SSLV3)。
- ◆ 在图 3 证书信息页面,可以看见签名算法“sha256RSA”(即 SSL\_RSA\_WITH\_RC4\_128\_SHA)。

## 2) 配置模块 SSL 参数

### ① 通过网页配置:

选择模块串口 1 Socket 模式为 SSL Socket  
 SSL Socket 端口 443  
 SSL 服务器地址 [www.alipay.com](https://www.alipay.com/)  
 加密类型 SSLV3  
 加密算法 SSL\_SHA

证书名称 NONE （不验证服务器发送来的证书，如果验证服务器发送的证书，则在此输入服务器证书名称，服务器证书烧写方法参见“[USR-C322 无线升级使用说明](#)”）

[中文](#) | [English](#)



**>> 串口1参数设置**  
**>> Socket参数设置**

**Socket连接设置**

socket 模式

**SSL Socket 功能**

SSL Socket 端口

SSL 服务器地址

加密类型

加密算法

证书名称

图 4

② 通过串口 AT 命令配置

AT+SSLSECM=SSLV3\r

AT+SSLMASK=SSL\_SHA\r

3) 串口发送数据获取服务器数据

串口发送：

GET <https://www.alipay.com/>\r\n

User-Agent: Mozilla/4.0 \r\n

Host: [www.alipay.com](http://www.alipay.com)\r\n

串口接收：

数据如下图 5: [www.alipay.com](http://www.alipay.com) 的主页数据



```
0-> <!DOCTYPE html> <html> <head> <meta charset="gb2312"> <meta http-equiv="X-UA-Compatible" content="IE=edge" /> <title>支付宝 知托付! </title> <meta name
<script type="text/javascript">
window.location.href = 'https://www.alipay.com/x/kill-ie.htm';
</script>
<![endif--> <link href="https://a.alipayobjects.com" rel="dns-prefetch" /> <link href="https://app.alipay.com" rel="dns-prefetch" /> <link href="https://my.alipay
ler)for(var b=arguments.callee.caller,e=[],h=0;b.arguments.callee.caller;){b=b.arguments.callee.caller;e.push("at "+q(b));if(b.caller
METHODS.length;i<1;i++){method=METHODS[i];if('function'!=typeof win.monitor[method]){win.monitor[method]=function(){}}}(window).</scrip
METHODS[i];var isString=typeof("String")===0||var isRegExp=typeof("RegExp");var whitelist=[];whitelist.push('https
8->(isString(rule)&&url.indexOf(rule)===0)||var isRegExp(rule)&&rule.test(url))return "anonymous";
alog','easing','events','iframe-uploader','iframe-shim','messenger','overlay','popup','position','select','switchable','tip','validator','widget'];var util={};ut
) { return id; } // arale 开头88 if (root === 'arale') { // 处理 arale/handlebars 的情况 if (contains(GALLERY_MODULES, name)) { return i
ht.base-1.8.js,tracker-all/2.1.0/index.js,alipay/smartracker/2.0.0/smartracker.js"></script> <script> window.Tracker && Tracker.start && Tracker.start();
@font-face {
font-family: 'alipayhome';
src: url('https://at.alicdn.com/t/font_1426748170_7530262.eot'); /* IE9*/
src: url('https://at.alicdn.com/t/font_1426748170_7530262.eot?#iefix') format('embedded-opentype'), /* IE6-IE8 */
url('https://at.alicdn.com/t/font_1426748170_7530262.woff') format('woff'), /* chrome、firefox */
url('https://at.alicdn.com/t/font_1426748170_7530262.ttf') format('truetype'), /* chrome、firefox、opera、Safari, Android, iOS 4.2+*/
u
19->rl('https://at.alicdn.com/t/font_1426748170_7530262.svg#iconfont') format('svg'); /* iOS 4.1- */
}
</style> <style>
body,ol,ul,h1,h2,h3,h4,h5,h6,p,th,td,dl,dd,form,fieldset,legend,input,textarea,select,img {margin: 0;padding: 0;}
body { font: 12px/1.5 "Microsoft YaHei",Tahoma,arial,Hiragino Sans GB,\5b8b\4f53; overflow: hidden;position: relative;}
html,body,.am-page,.am-body,.am-bg{height:100%; width:100%;}
html,body,.am-page{ overflow:hidden; }
ul,li {list-style:none;}
.am-body { position: absolute; top: 0; left: 0; }
.iconfont {font-family: "alipayhome";-webkit-font-smoothing: antialiased;font-style: normal; display: block;}
.clearfix {zoom:1;}
.clearfix:after {content: "";display: block;height: 0;clear: both;visibility: hidden;}
.fl {float: left !important;}
.fr {float: right !important;}
.w320 { width: 320px;}
.fr-hide { display: none !important; }
.arrow-down { display: inline-block; width: 0px; height: 0px; border-width: 5px 5px 0 5px; border-color: #eeeeee transparent transparent transparent; border-style:
.am-page,.am-bg { background-size: cover; background-repeat: no-repeat; background-position: center center;}
.am-page { overflow: hidden; position: relative; z-index: 1;}
.am-bg { position: absolute; z-index: 9; top: 0; left: 0;}
.main-content, .ft-content {width: 1200px; margin: 0 auto; height: 100%;}
.main-content { position: relative; z-index: 99;}
.onepage-pagination { position: absolute; right: 25px; top: 50%; z-index: 996;}
.onepage-pagination a, onepage-pagination .dotted {display: block; width: 10px; height: 10px;}
.onepage-pagination a { padding: 8px;}
.onepage-pagination .dotted {border: 1px #cccccc solid; position: relative; display: block; border-radius: 50%; -webkit-transition: all 500ms ease; -o-transition: all
onepage-pagination .active .dotted {border-color: #0cf; background-color: #0cf !important;}

.ftbar { height: 60px; overflow: hidden; z-index: 101; position: absolute; left: 0; bottom: 0; width: 100%; background: rgba(0, 0, 0, .3); }
.ft-content { }
```

图 5

## 附录 A：有人联系方式

---

公 司： 济南有人物联网技术有限公司  
地 址： 济南市高新区会展国际城北塔 724~729 室  
网 址： <http://www.usr.cn>  
邮 箱： sales@usr.cn tec@usr.cn  
企 业 QQ： 8000 25565（谐音：爱我物联网）  
电 话： 4000 255 652（免长途费）或者 0531-88826739  
公司文化：有人在认真做事！

价 值 观：天道酬勤 厚德载物 共同成长

有人愿景：国内联网通讯第一品牌

有人使命：让联网通讯更简单

产品理念：简单 可靠 价格合理

说明：因我们正在不断的改进和完善产品，本手册中的图片和文字仅供参考，所有信息均以实物和实际销售情况为准。

---

## 附录 B：免责声明

本文档提供有关产品的信息，本文档未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除在其产品的销售条款和条件声明的责任之外，我公司概不承担任何其它责任。并且，我公司对本产品的销售和/或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性，适销性或对任何专利权，版权或其它知识产权的侵权责任等均不作担保。本公司可能随时对产品规格及产品描述做出修改，恕不另行通知。

## 附录 C：版本记录

V 1.0 14-05-2015. 第一次创建

〈结束〉