## 加密协议无线透传模块功能需求书

帖子名称：

STM32平台软件设计（4G SSL私有证书+SIM芯片编程）；

项目名称：

**加密协议无线透传模块**；

项目背景：

电能质量数据上传，通过UART得到数据，通过4G转发；

性能指标：

与后台数据上传正常，与下位数据收集CPU数据传输正常，连续不掉线时间〉72小时 ； 代码标注及结构清晰 。

项目预算：

设计费3万元 ；

项目周期：

15天（从设计师拿到硬件电路板开始，包含周末及节假日）；

设计师要求：

有GPRS TCP 编程经验或者SIM1/SIM2芯片应用经验，软件设计工作经验〉5年。

设计师如果是兼职，则需要在山东省境内就职，且与我方（济南市齐鲁软件园）交通时间〈4小时。专职人员则需要能出差到我方驻地。

设计师在设计完成后，可以参加系统联调调试（差旅费用由项目方负责）。

备注：

一/设计人员及EDA365需要对合作内容保密，包括设计细节及项目本身

**二/ 项目详细介绍 （硬件由我方提供，设计师完成软件）**

**1、需求简介**

根据我公司提供的硬件平台，开发一套实现串口到加密层协议传输的透传程序。主要包括的内容：

（1）通过AT指令实现APN拨号，创建TCP连接，实现TCP层数据的传输，

（2）和加密芯片进行交互，完成加密层协议需要的SM1/SM2实现，SM1和SM2的算法由芯片完成，需要通过SPI进行交互。

（3）最主要的功能即为实现TCP加密管道，即在TCP协议层之上实现加密协议的握手（根据具体协议共三步，主要实现秘钥交换），将下位芯片传输过来的串口数据包进行对称加密传输（可根据时间间隔进行分割打包）。

（4）我公司提供的硬件平台共两个芯片，本需求需要实现的是加密协议芯片MCU2的功能，存储和应用层协议转换的芯片MCU1由我公司开发程序，双方交接点为两芯片的UART。

**2、主芯片功能**

基于ARM的STM32F103系列平台进行软件平台开发；

硬件组成的结构需求如下图所示：





通讯数据管道示意图

**3、无线连接功能**

通讯传输模块具备4G无线传输功能，为SIM-7100CE芯片；

用AT指令实现无线SOCKET连接功能，以及实现APN拨号连接；

通过AT指令能够建立、监视、控制TCP连接，TCP连接的具体要求是：

为节省流量，防止重复频繁拨号，TCP连接中断后，应关闭TCP SOCKET，同时30秒后允许第二次拨号，连续拨号三次失败后，则等待15分钟后再拨号。

备注：应用层的协议是5分钟间隔的心跳包，有上传有问有应答。

**4、终端通讯接口**

留3路485通讯接口：

一路与设备进行UART通讯，实现串口明文数据的加密打包上传；

一路为模块本身的配置端口，可实现APN拨号参数的配置，TCP连接参数配置、TCP重连等待时间配置、证书导入导出等功能（需开发上位机软件）；

**5、透传转换**

通过程序操作，最终实现设备串口包数据到加密层协议的透传功能；

**6、加密传输功能**

根据主站的安全接入平台实现加密安全连接，建立安全连接传输；

与外置的加密芯片进行通讯和交换数据，结合主站的加密协议进行加密认证和加密传输；

应充分理解和使用加密协议的正常和异常处理机制，确保连接的可靠性、稳定性、可使用性（后附加密通讯协议）；

加密过程中需要进行的SM1/SM2/SM3等运算可由外置硬件加密芯片实现，一般采用SPI接口与加密芯片进行通讯；

加密传输包括两部分组成，第一部分为实现握手，共三步数据交互，最终协商出对称加密用的秘钥；第二部分为数据的对称加密机制。

**7、稳定性要求**

若基于嵌入式操作系统或其它简易操作系统进行功能开发，应充分保障操作系统的稳定性和可靠性；

程序框架易于维护，变量、代码编写规范，代码注释内容标准详尽；函数入口注释清晰全面；

**8、升级维护**

程序开发完成验收后，将源代码一次性交付，并对我方技术人员进行培训。