采集类终端的安全防护

版本历史

版本	日期	作者	描述
V1.0	2012-2-5	南瑞信通	初稿
V1.1	2012-3-12	南瑞信通	方案修改、细化
V1.2	2012-3-31	南瑞信通	完善
V1.3	2012-5-31	南瑞信通	报文格式修改
V1.4	2012-7-24	南瑞信通	添加出错提示的报文
V1.5	2012-11-8	南瑞信通	修正 sm3 hash 时一处公钥说明错误
V1.6	---	---	未公布，略
V1.7	2013-7-18	南瑞信通	修改了密钥协商，添加了 x509 证书，添加了异常情况下明文通信方式等内容

1 概述

对采集类的终端，统一采用**专用芯片+安全协议规范**来实现安全防护，终端需要进行相应的软硬件改造才能实现。

2 硬件改造

采集类终端的硬件板子在设计时必须预留位置，用于接入南瑞专用安全芯片NRSEC3000，NRSEC3000 芯片主要用于实现 SM1、SM2 加密算法，采用 48 引脚封装，支持 ISO7816 接口和 SPI 接口，建议优先支持 SPI 接口，有条件的也可以两种接口同时支持。

NRSEC3000 安全芯片的具体信息请参看《安全芯片 NRSEC3000 介绍》。

3 软件改造

南瑞提供安全芯片的通信协议及调用示例、采集终端与主站系统之间的安全协议规范。对用户而言，主要涉及到操作系统的改造、系统初始化工作和应用程序的改造。

3.1 操作系统改造

由于安全芯片采用的是 ISO7816 接口和 SPI 接口，因此，用户终端装置的操作系统需要支持对 ISO7816 接口、SPI 接口进行读写操作，由于 SPI 接口速度较快，如果终端支持 SPI 接口，建议优先使用 SPI 接口。

注：对于不带操作系统的终端，只要终端能够读写 ISO7816 接口和（或）SPI 接口就可以了。

考虑到终端的硬件结构、采用的操作系统等形式各异，南瑞无法提供统一的安全芯片的调用程序库，对于如何调用安全芯片的功能，用户可参考南瑞提供的安全芯片的通信协议及调用示例，自行编写终端调用安全芯片所需要的代码。

3.2 系统初始化工作

为了应用安全防护功能，终端装置在上线之前需要进行额外的初始化工作，初始化工作主要包括：

1、 初始化安全芯片，生成密钥对；

2、 生成安全芯片的证书请求，把证书请求提交证书签发机构进行签发，签发出终端自身的证书；

3、 导入终端自身的证书及远端装置（即主站端）的证书。

注：终端的密钥对与最后签发出来的终端的证书是一一对应的，在终端的证书签发出来后，如果又重新生成了密钥对，则终端原来签发的证书就没用了，因此需要特别注意，签完终端证书后就不要再生成密钥对了。

3.3 应用程序改造

包括正常情况（即可以正常使用安全芯片的情况）及异常情况（即检测到安全芯片无法使用的情况）。

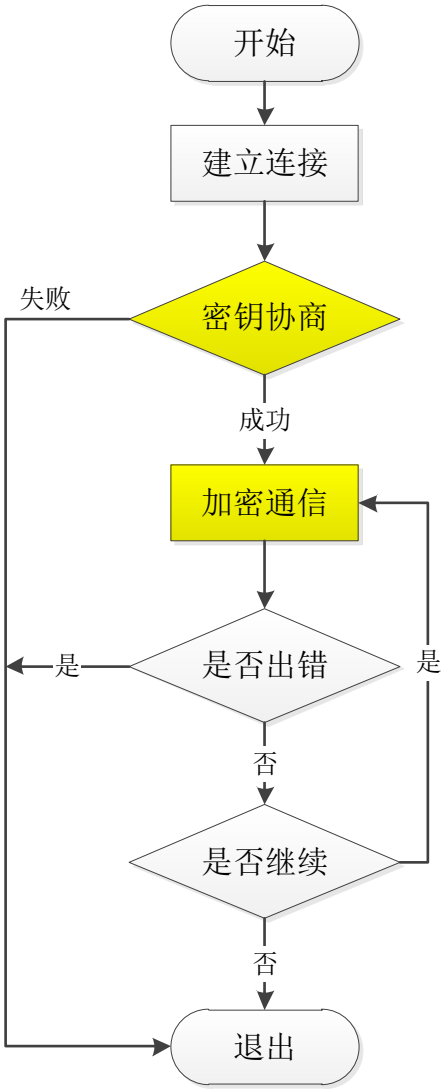
3.3.1 正常情况

应用程序需要做一些额外的工作，以便使用上安全防护功能。

1、 应用程序在和远端（即主站端）进行连接之后，数据交互之前，需要进行双向的身份认证。只有通过身份认证，才能进行后续的数据通信。

2、 应用程序在与远端进行正常数据通信的时候，需要对通信的数据进行加解密操作

具体流程如下图所示（图中黄色部分为应用程序需要添加或改动的部分）：



密钥协商和数据加密等过程的帧结构如下：

报文类型	子类型	报文总长度	报文内容
1 byte	1 byte	2 bytes（网络序）	n bytes

注：由于报文总长度为 2 字节，最大为 65535，因此，原始单个报文的帧长度不得高于 65463（已考虑到了报文填充、IP、TCP 头等）。

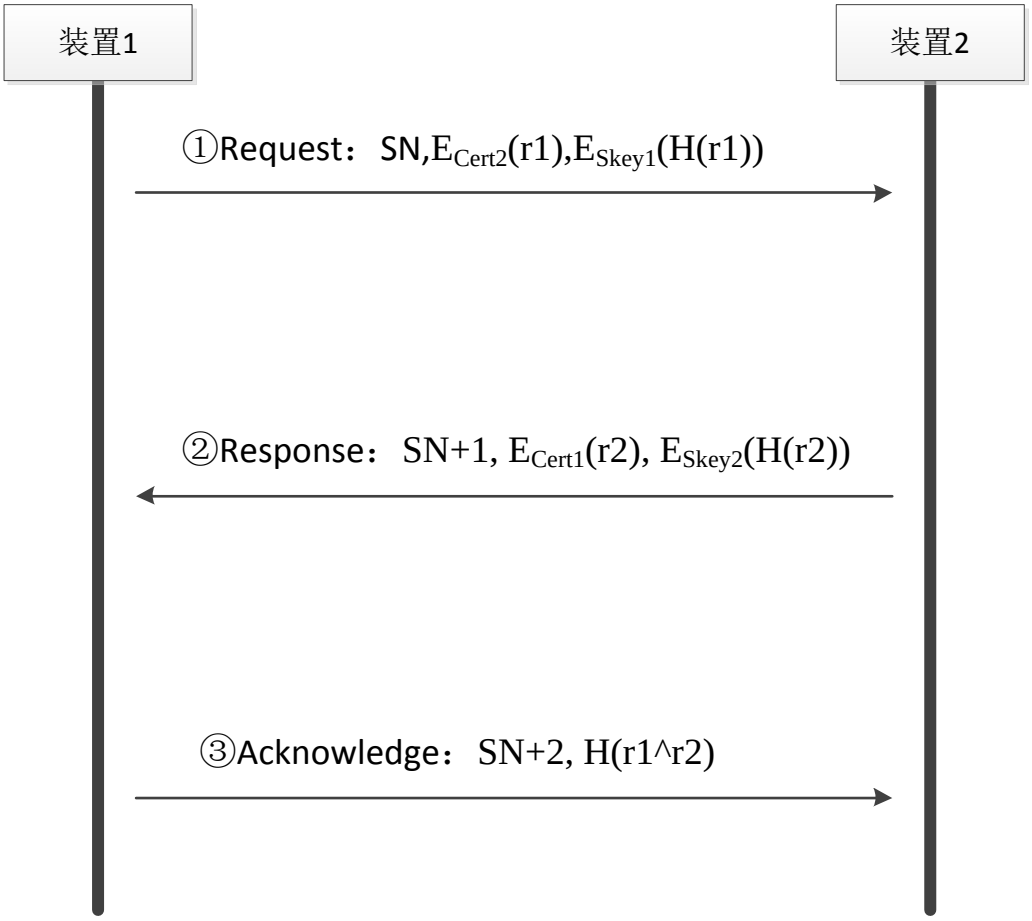
3.3.1.1密钥协商过程

应用程序在建立完 TCP 连接之后，需要立即与远端进行会话密钥协商，只有协商好会话密钥之后，才能进行后续的数据加密通信，**在密钥协商完成之前，不得进行任何其他数据信息（非密钥协商的数据信息）的发送，否则，TCP 连接将被关闭**。

在进行描述之前，对用到的一些符号进行如下说明：

rN	装置 N 产生的随机数
DK	会话密钥
Cert N	装置 N 的公钥（SM2 公钥）
Skey N	装置 N 的私钥（SM2 私钥）
EX(Y)	用 X 对 Y 作加密运算
H(Y)	对 Y 作散列运算（SM3 算法）
‖	连接

密钥协商由 TCP 连接的发起端发起，协商过程的形象描述如下：



协商过程的简述如下：

1. 装置 1 产生随机数 r1，作：

   A=ECert2(r1) ‖ ESkey1(H(r1))，将 A 发送到装置 2；

2. 装置 2 对 A 解密并验证装置 1 的签名，产生随机数 r2，作：

   B=ECert1(r2) ‖ ESkey2(H(r2))，将 B 发送到装置 1；

合成会话密钥：DK=r1⊕r2；

3. 装置 1 对 B 解密并验证装置 2 的签名，作：

合成会话密钥：DK=r1⊕r2，

C=H(r1⊕r2)，将 C 发送到装置 2；

装置 2 做 D=H(r1⊕r2)，并比较 C 与 D 是否相同。

若相同，则此时双方已经验证的对方身份，并持有会话密钥：DK=r1⊕r2；若不同，则装置 2 给出协商失败告警信息，通知装置 1，由装置 1 重新发起协商。

注：SN 由协商发起方随机设置，SN 的引入是为了抗重放攻击。

具体的报文结构为

1. 密钥协商请求报文

名称	长度	内容	说明
类型 Type	1	1	表示协商过程
子类型 Subtype	1	1	发起密钥协商
长度 Len	2	234+n	报文总长度（网络序）
版本 Ver	2	定值，依次为：0x01,0x00	本协议的版本号
SN	2	序列号	协商发起端预置的一个序列号（网络序）
SIM 卡号	16	卡号	目前最多 15 字节，不足的在前面补 0x0
设备 ID	18	设备唯一 ID 号	目前最多 17 字节，不足的在前面补 0x0
证书 Cert1	n	设备自身证书	X509 标准格式证书
$E_{Cert2}(r1)$	128	加密的随机数	本端产生的随机数 r1，用对端证书 Cert2 加密
$E_{Skey1}(H(Type\|\|Subtype\|\|Len\|\|Ver\|\|SN\|\|SIM\|\|ID\|\|Cert1\|\|E_{Cert2}(r1)))$	64	签名	先对前面的报文做 HASH 运算（SM3 算法），然后对 HASH 结果用本端私钥进行签名

注：

1) 产生的随机数为 16 字节，需要填充到 32 字节后进行加密，填充方法为：前 16 字节为 0，后 16 字节为产生的随机数。下同。

2) SM3 时使用的公钥是自身的公钥，pucID 使用 16 个 0x01。

2. 密钥协商应答报文

名称	长度	内容	说明
类型 Type	1	1	表示协商过程
子类型 Subtype	1	2	密钥协商应答
长度 Len	2	230	报文总长度（网络序）
SN+1	2	序列号	协商发起端预置的序列号+1（网络序）
安全认证因子 Auth	32	安全认证因子	用于安全认证的一组随机因子
E_{Cert1}(r2)	128	加密的随机数	本端产生的随机数 r2，用对端证书 Cert1 加密
E_{Skey2}(H(Type||Subtype||Len||SN+1 ||Auth||E_{Cert1}(r2)))	64	签名	先对前面的报文做 HASH 运算（SM3 算法），然后对 HASH 结果用本端私钥进行签名

注：

1) SM3 时使用的公钥是自身的公钥，pucID 使用 16 个 0x01。

3. 密钥协商确认

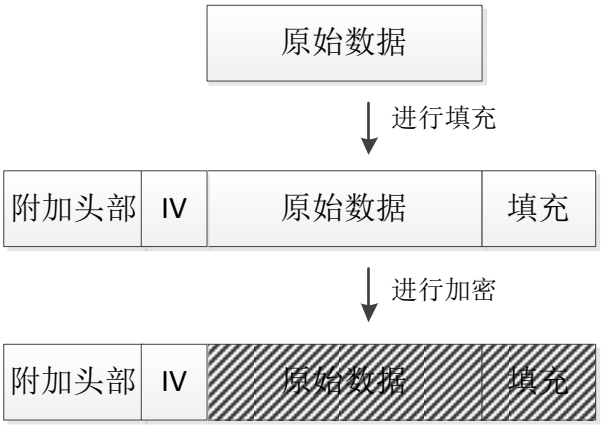
名称	长度	内容	说明
类型	1	1	表示协商过程
子类型	1	3	密钥协商确认
长度	2	184	报文总长度（网络序）
SN+2	2	序列号	协商发起端预置序列号+2（网络序）
安全认证结果 R_{Auth}	146	对安全认证因子 Auth 进行安全认证的结果	本端调用安全芯片的安全认证接口对对端发来的安全认证因子 Auth 进行安全认证的返回值
H(r1 $\oplus$ r2)	32	密钥 DK 的 HASH	本端随机数 r1 与对端随机数 r2 异或后，进行 HASH 运算（SM3 算法）

注：

1) SM3 时使用的公钥是自身的公钥，pucID 使用 16 个 0x01。

3.3.1.2数据加密过程

在协商好会话密钥之后，进行数据通信的时候，需要对应用层的数据报文使用 SM1 算法进行加解密，加密的过程如下图所示：



加密过程的详细描述如下：

1) 对原始的数据报文填充 1～16 字节，使其长度为 16 的倍数（原始长度为 16 的倍数时填充 16 字节），填充的第一个字节为 0x80，后续的填充字节内容为 0x0。附加加密报文的头部信息及初始向量 IV（IV 为 16 字节随机数，由加密侧随机生成）。

2) 对填充后的原始报文+填充报文使用之前协商好的会话密钥 DK 进行加密。

注：解密过程为加密的逆过程，解密后需要检查填充报文是否正确。

具体的报文结构：

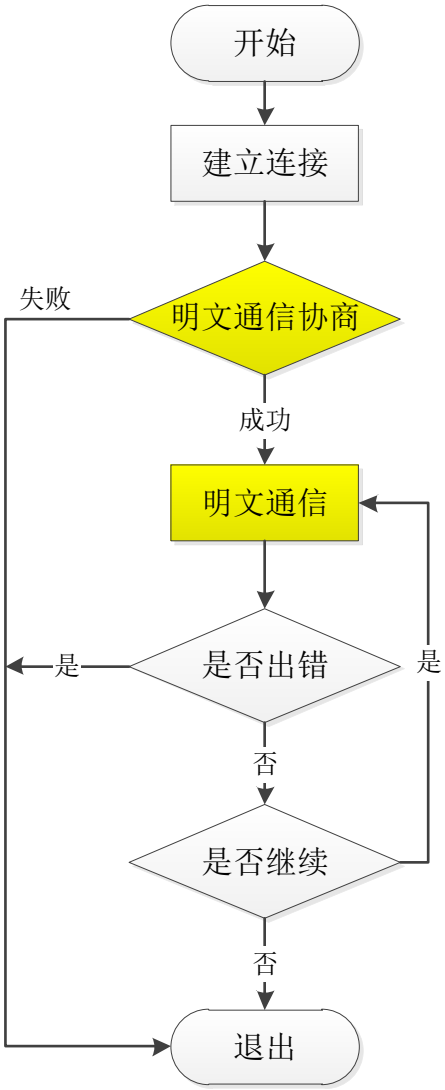
4. 加密包

名称	长度	内容	说明
类型	1	2	表示加密数据包
子类型	1	0	无
长度	2	20+n	报文总长度（网络序）
IV	16	加密时使用的初始向量 IV	IV 由加密端随机生成
密文数据	n	密文数据	原始数据 m 经填充到 n 后，进行加密

注：对于收到的加密包，必须收到完整的一帧之后（长度要匹配）才可以进行解密。

3.3.2 异常情况

当终端发现安全芯片故障，无法使用的时候，为了保证业务能够正常通信，采用下面的方式处理。**在明文通信协商过程完成之前，不得进行任何其他数据信息（非明文通信协商的数据信息）的发送，否则，TCP 连接将被关闭**。具体流程如下：



3.3.2.1明文通信协商过程

明文通信协商的过程比较简单，终端发起明文通信请求，主站收到后，验证通过后进行明文通信确认，终端收到主站的明文通信确认报文后，即可开始进行明文通信。

1. 明文通信请求报文

名称	长度	内容	说明
类型 Type	1	1	表示协商过程
子类型 Subtype	1	4	发起明文通信请求
长度 Len	2	58	报文总长度（网络序）
版本 Ver	2	定值，依次为：0x01,0x00	本协议的版本号
SN	2	序列号	请求发起端预置的一个序列

			号（网络序）
SIM 卡号	16	卡号	目前最多 15 字节，不足的在前面补 0x0
设备 ID	18	设备唯一 ID 号	目前最多 17 字节，不足的在前面补 0x0
Magic	16	从 0x0 依次递增到 0xf	一段确定的数据，最大限度避免可能存在的干扰

2. 明文通信确认

名称	长度	内容	说明
类型 Type	1	1	表示协商过程
子类型 Subtype	1	5	明文通信确认
长度 Len	2	22	报文总长度（网络序）
SN+1	2	序列号	请求发起端预置序列号+1（网络序）
Magic	16	从 0x0 依次递增到 0xf	一段确定的数据，最大限度避免可能存在的干扰

3.3.2.2 明文通信过程

异常情况下的明文通信协商过程完成后，就可以按照下面的格式进行数据通信了。

名称	长度	内容	说明
类型	1	3	表示采用明文通信
子类型	1	0	无
长度	2	4+n	报文总长度（网络序）
数据	n	进行填充的通信数据内容	原始数据 m 经填充到 n

对原始的数据报文填充 1～16 字节，使其长度为 16 的倍数（原始长度为 16 的倍数时填充 16 字节），填充的第一个字节为 0x80，后续的填充字节内容为 0x0。

3.3.3 出错提示

在通信的过程中，产生的某些错误将会通知对端，其报文格式如下。

名称	长度	内容	说明
类型	1	4	表示出错信息
子类型	1	0	无
长度	2	8	报文总长度（网络序）

错误码	4	错误码（具体参见下面的错误码说明）	int 型，网络序

注：为了防止重放攻击等对主站网关的恶意攻击的可能，主站网关可能会抑制某些出错信息的频繁发送。

错误码：

值	说明	出错场景
1	类型，子类型错误 （不支持的数据包类型或子类型，或者该类型出现的场景不对）	ALL
2	超时错误 （TCP 连接建立后，协商过程超时，包括长时间不去协商或者协商过程中的超时）	协商过程
3	长度错误 （报文的长度错误或者在一定时间内没有能够接收到一个完整的包）	协商过程、通信过程
4	SN 错 （报文的 SN 号顺序出错）	协商过程
5	安全认证结果出错 （使用安全认证因子对终端进行的安全认证不通过）	密钥协商 （略）
6	证书文件格式错误 （终端传来的证书不是一个符合 X509 格式标准的证书）	密钥协商
7	证书非法 （证书不是由被认可的 CA 系统所颁发）	密钥协商
8	证书已过期 （证书的有效期已过）	密钥协商
9	证书被吊销 （证书已经被 CA 系统吊销）	密钥协商
10	证书重复 （相同证书信息的终端已经连接了。注：不同的终端必须自行产生密钥对，并由 CA 签发形成各自的证书，不得使用相同的密钥对和证书）	密钥协商
11	证书错误 （其他以上未提及到的证书的错误）	密钥协商
12	身份标识信息非法 （对端给的 SIM 卡号、设备 ID 号等信息是非法的）	协商过程
13	验证签名出错 （可能的原因：对端给的公钥不对、对端的签名不对）	密钥协商
14	SM2 解密出错 （可能的原因：对端 SM2 加密的结果不对）	密钥协商
15	随机数 PADDING 出错	密钥协商

	（SM2 解密后，发现随机数填充的 padding 出错）	
16	状态机错误 （密钥协商时的状态机不对）	密钥协商
17	密钥协商出来的 key 不一致 （对端发来的协商 key 确认信息与本端计算出来的不一致）	密钥协商
18	密钥协商未完成 （密钥协商未完成时，收到了加密通信的数据包）	加密通信
19	报文填充出错 （SM1 解密之后，或异常情况明文通信时，检查发现报文的填充信息错误）	协商过程、通信过程
20	其他加解密错误 （其他以上未提及的加解密错误）	加密通信
21	连接不上服务端 （密钥协商完成后，网关会立即去连接真正的业务服务端，如果连接不上，则返回此错误通知终端，此后网关会立即关闭与客户端的连接）	通信过程
22	服务端连接关闭 （服务端的连接被关闭了，当然，这不一定是错误，这里只是为了通知终端，此后网关会立即关闭与客户端的连接）	通信过程
23	不支持的版本	协商过程
24	Magic 数错误	明文通信协商过程
255	未知错误	ALL

注：这里的错误均是与终端相关的一些错误，若是本端系统自身产生的错误，则一般不会通知对端，若影响到与终端的通信，则会以未知错误的形式通知到对端。