社保接口 API 说明

1.函数定义：

1.1C 语言

```
int UnionAPIService_EAJ0(
                                const char *data,
                                char *outData
);
```

服务代码	EAJ0
函数名称	UnionAPIService_EAJ0
功能	社保卡读取信息
输入参数	✧ data 输入数据（长度小于 512）
输出参数	✧ outData 输出数据（长度小于 512）
返回值	<0：函数执行失败，值为失败的错误码 >=0：函数执行成功
密钥	

1.2JAVA 语言

函数名称	读基本信息-JAVA					
语法	public String UnionIESS_hsm (String inmsg) throws Exception					
功能描述	基于加密机完成社保卡基本信息的读取					
参数说明	序号	参数	输入/输出	类型	10 进制长度	含义
	1	inmsg	业务类型|IN	字符串	< 512	输入数据
返回值	非 NULL（pOutInfo）表示成功，并返回认证码； NULL 表示失败。					

--

2.接口说明

- 业务类型 01 说明

输入参数 inmsg

由业务编号|发卡地区行政区划代码（卡识别码前 6 位）卡复位信息|算法标识|卡识别码|内部认证过程因子|内部认证鉴别所需的原始信息|外部认证过程因子|外部认证鉴别所需的原始信息。其中外部认证相关数据项全部不为空或全部为空。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

一代卡、二代卡：

01|370001|0081544B31869B370000067046|01|370001D156000005000412DD7BD172E2|3688D8D42C5D94D3|57CE879B10C47FAE|||

三代卡：

01|370001|00814A444686603700000323D8|03|370001D1560000050004A06E0BAF274D|3C5CA4D179AA3C00|7D79B86BCFC3174C|9B040E163D209F8C|0C70EA1AE04B7500|

（2） 返回值/输出参数 pOutInfo

内部认证鉴别数据|外部认证鉴别数据|

序号	数据项名称	数据类型	长度	填写说明
1	内部认证鉴别数据	Char	32	内部认证鉴别数据+原始信息
2	外部认证鉴别数据	Char	32	外部认证鉴别数据+原始信息

如果输入的外部认证过程因子|外部认证鉴别所需的原始信息存在时需要计算外部认证。

一代卡，二代卡

C5B2B30B4C4ED24857CE879B10C47FAE||

三代卡：

C5B2B30B4C4ED2487D79B86BCFC3174C|AF321F804C4CA2930C70EA1AE04B7500|

（3） 2.3 sPF_GenerateAuthCode 所需参数

顺序	要素名称	长度	备注

1	发卡地行政区划代码	6	
2	算法标识	2	算法标识
3	密钥地址(索引)	4	
4	分散次数（N）	1	省级是 2， 地市是 1
5	分散因子	N×16	2 级分散时：行政区划因子+卡片因子 1 级分散时：卡片分散因子
6	过程密钥因子	16	内部/外部认证过程因子
7	数据	16	内部/外部认证鉴别所需的原始信息

- 业务类型 02 说明

输入参数 inmsg

由业务编号 | 发卡地行政区划代码|卡复位信息|算法标识|外部认证密钥地址|外部认证过程因子（从卡片获得的随机数）|外部认证鉴别所需的原始信息（从卡片获得的随机数）|。各数据项之间以 “|” 分割，且最后一个数据项以“|”结尾。

02|370001|0081544B31869B370000067046|01|004C|3688D8D42C5D94D3|57CE879B10C47FAE|

02|370001|0081544B31869B370000067046|03|RKMFEF0C_370000|3688D8D42C5D94D3|57CE879B10C47FAE|

（2） 返回值/输出参数 pOutInfo

外部认证鉴别数据外部认证鉴别所需的原始信息|

数据项名称	数据类型	长度	填写说明
鉴别数据	Char	32	外部认证鉴别数据+外部认证鉴别所需的原始信息（从卡片获得的随机数）

9446307CD2E03B7257CE879B10C47FAE|

（3） sPF_GenerateAuthCode 所需参数

密钥地址：由算法标识和外部认证密钥地址，由客户自己输入索引地址（如：004C）。

顺序	要素名称	长度	备注
1	发卡地行政区划代码	6	
2	算法标识	2	算法标识
3	密钥地址(索引)	4	
4	分散次数（N）	1	省级是 2， 地市是 1
5	分散因子	N×16	2 级分散时：行政区划因子+卡片因子 1 级分散时：卡片分散因子
6	过程密钥因子	16	外部认证过程因子
7	数据	16	外部认证鉴别所需的原始信息

- 业务类型 03 说明

（1） 第一步输入参数 inmsg

由业务编号|发卡地行政区划代码|卡复位信息|算法标识|外部认证密钥地址|外部认证过程因子（从卡片获得的随机数）|外部认证鉴别所需的原始信息（从卡片获得的随机数）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

02|370001|0081544B31869B370000067046|01|0090|3688D8D42C5D94D3|57CE879B10C47FAE|

（2） 第一步返回值/输出参数 pOutInfo

外部认证鉴别数据外部认证鉴别所需的原始信息|

数据项名称	数据类型	长度	填写说明
鉴别数据	Char	32	外部认证鉴别数据+外部认证鉴别所需的原始信息（从卡片获得的随机数）

9446307CD2E03B7257CE879B10C47FAE|

（2） 第二步输入参数 inmsg

由业务编号|发卡地行政区划代码|卡复位信息|算法标识|安全报文计算密钥地址|安全报文计算过程因子（从卡片获得的随机数）|APDU 命令头|APDU 命

令明文数据（新PIN， 解锁时是空字符串）。各数据项之间以 “|” 分割，且最后一个数据项以 “|” 结尾。

03|370100|0081544B31869B370000067046|01|0173|CEA1DB2F4623FE89|842400010C|33445566|

03|370100|0081544B31869B370000067046|01|0173|535068CE66733B7A|8424000004||

（3） 第二步返回值/输出参数 pOutInfo

将入参数据传入加密机，加密机计算返回：

安全报文|

数据项名称	数据类型	长度	填写说明
安全报文（命令头+加密数据+MAC）	Char	≥14	如果 APDU 命令数据域数据为空，则加密数据为空

842400010C2816EE77FA4450B630E76859|

（4） 4.3 sPF_GenerateSecMsg 所需参数

顺序	要素名称	长度	备注
1	发卡地行政区划代码	6	
2	算法标识	2	算法标识
3	密钥地址(索引)	4	
4	分散次数（N）	1	省级是 2，地市是 1
5	分散因子	N×16	2 级分散时：行政区划因子+卡片因子 1 级分散时：卡片分散因子
6	过程密钥因子	16	安全报文计算过程因子
7	数据		APDU 命令头、APDU 命令明文数据

基于加密机的读基本信息密钥地址：由算法标识和外部认证密钥地址，根据 38 号文附录 B 确定。

数据：842400010C CD9A496F2D05EDAA 800000

注：如 PIN 解锁时，不做加密，直接计算 APDU 的 MAC。

- 业务类型 04 说明

输入参数 inmsg
由业务编号|发卡地行政区划代码|卡复位信息|终端交易序号|算法标识|密钥地址|伪随机数|医疗消交易序号|交易金额（转换成十六进制向卡片发送命令时的后两个金额拼接组成）|交易类型|终端机编号|交易时间（格式为 YYYYMMDDHHMMSS）。各数据项之间以“|”分割，且最后一个数据项以“|”结尾。

04|371400|0081544B31869B370000067046|00000005|01|017F|F962FAD6|0007|000

0010000000200|32|449900810027|20150624183211|

（2） 返回值/输出参数 pOutInfo
将入参数据传入加密机，加密机计算返回：
终端交易序号|交易时间|MAC1|MAC2|TAC|

序号	数据项名称	数据类型	长度	填写说明
1	终端交易序号	Char	8	00000005
2	交易时间	Char	14	20150624183211
3	MAC1	Char	8	26FA9B2E
4	MAC2	Char	8	B20034B8
5	TAC	Char	8	B745CA87

00000005|20150624183211|26FA9B2E|B20034B8|B745CA87|

（3） sPF_GenerateMac1Mac2 所需参数

顺序	要素名称	长度	备注
1	发卡地行政区划代码	6	
2	算法标识	2	算法标识
3	密钥地址(索引)	4	
4	分散次数（N）	1	省级是 2，地市是 1
5	分散因子	N×1	2 级分散时：行政区划因子+卡片因子 1 级分散时：卡片分散因子

		6	
6	过程密钥因子	16	安全报文计算过程因子（4 个字节伪随机数+2 个字节医疗消费交易序号+2 个字节终端机编号）
7	交易金额		连续 4 个要素用于产 MAC1； 交易金额用于产生 MAC2
8	交易类型		
9	终端机		
10	交易时间		

（4） 5.4sPF_GenerateTac 所需参数

顺序	要素名称	长度	备注
1	发卡地行政区划代码	6	
2	算法标识	2	算法标识
3	密钥地址(索引)	4	
4	分散次数（N）	1	省级是 2，地市是 1
5	分散因子	N×16	2 级分散时：行政区划因子+卡片因子 1 级分散时：卡片分散因子
6	交易金额	24	用于产生 TAC
7	交易类型	2	
8	终端机编号	12	
9	终端交易序号	8	
10	交易时间	14	