XXXXXXX
XXXX

WS

中 华 人 民 共 和 国 卫 生 行 业 标 准

WSXXXX—2018

电子健康卡技术规范 第 4 部分：密码机

Technical specification for electronic health card Part 4：

Cipher machine

（征求意见稿）

2018-XX-XX 发布　　2018-XX-XX 实施

国家卫生健康委员会 发布

目　次

1　适用范围 1
2　规范性引用文件 1
3　定义和缩略语 1
3.1 定义 1
3.1.1 居民健康卡 2
3.1.2 电子健康卡 2
3.1.3 密钥 2
3.2 缩略语和符号表示 2
4　技术要求 2
4.1 外观和结构 2
4.2 功能 2
4.3 高级应用编程接口要求 3
4.3.1 密码机连接和断开 3
4.3.1.1 连接密码机 3
4.3.1.2 断开密码机 3
4.3.2 主索引 ID 生成接口 4
4.3.3 电子健康卡 ID 接口 4
4.3.3.1 电子健康卡 ID 生成接口 4
4.3.3.2 电子健康卡 ID 验证接口 4
4.3.3.3 有效性信息接口 5
4.4 通讯方式 5
4.5 电源适应性 5
4.6 安全性要求 5
4.7 气候环境条件 6
5　检测要求 6
5.1 检测条件 6
5.2 外观和结构 6
5.3 功能 6
5.4 高级应用编程接口 6
5.5 通讯方式 7
5.6 电源适应性 7
5.7 安全性要求 7
5.8 气候环境试验 7
5.8.1 一般要求 7
5.8.2 工作温度下限 7
5.8.3 工作温度上限 7
5.8.4 贮存温度下限 7
5.8.5 贮存温度上限 8
5.8.6 工作恒定湿热 8
5.8.7 贮存恒定湿热 8
附录 A 密钥灌装接口说明 9
A.1 连接加密机 9

A.2 断开加密机.....9
A.3 SM1 解密计算 9
A.4 导入密钥.....9
附录 B 接口调用示例和测试验证数据 11
B.1 基本信息.....11
B.2 测试验证示例.....11
B.3 验证数据.....13

前　言

本标准由卫生部卫生信息标准专业委员会提出。

本标准主要起草单位：国家卫生健康委员会

本标准主要起草人：

电子健康卡技术规范 第4部分：密码机

1 适用范围

本规范规定了电子健康卡应用过程中涉及到的密码机的外观和结构、功能、通讯方式、电源、安全性、气候环境条件、接口等方面的技术细节和要求。

本规范适用于所有设计、生产、发放、使用电子健康卡密码机的研制单位、管理机构、发放机构、以及使用单位等。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括刊物的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

中华人民共和国国务院令第273 号.商用密码管理条例.1999年10月7日

GM/T 0002-2012　　SM4分组密码算法

GM/T 0003-2012　　SM2 椭圆曲线公钥密码算法

GM/T 0004-2012　　SM3 杂凑密码算法

GM/T 0009-2012　　SM2 密码算法使用规范

GM/T 0018-2012　　密码设备应用接口规范

GM/T 0030-2014　　服务器密码机技术规范

WS/T 543.5-2017　　居民健康卡技术规范 第5 部分：终端技术规范

卫办综发〔2012〕26 号《居民健康卡密钥管理办法》

卫办综发〔2012〕26 号《居民健康卡密钥管理系统技术方案》

3 定义和缩略语

3.1 定义

3.1.1 居民健康卡

居民健康卡是中华人民共和国居民拥有的，在医疗卫生服务活动中用于身份识别，满足健康信息存储，实现跨地区和跨机构就医、数据交换和费用结算的基础载体，是计算机可识别的 CPU 卡。

3.1.2 电子健康卡

通过用户身份标识建立的居民健康卡电子账户。健康卡电子账户使用时，可通过二维码形式展现为电子健康卡，功能与实体居民健康卡相同。

3.1.3 密钥

加密转换中控制操作的符号序列。

3.2 缩略语和符号表示

以下缩略语和符号表示适用于本规范。

SM1 一种商用密码分组标准对称算法

SM3 密码杂凑算法

SM4 一种商用分组密码算法

4 技术要求

4.1 外观和结构

(1) 结构应完整、整洁；表面涂镀层应均匀，不应起泡、龟裂、脱落和磨损；不应有明显的凹痕、破损、划痕、变形和污染等；金属零部件不应有锈蚀及其他机械损伤。

(2) 终端的零部件连接应紧固无松动。

(3) 指示灯应有明显标识。

(4) 终端应有铭牌和标牌。铭牌可以标识产品型号、设备编号、工作电源、工作功率等主要信息。

4.2 功能

安全存储数据加密和解密密钥，支持国产密码算法，并按照一定的程序对信息进行加密和解密。

支持居民健康卡密钥管理系统通过密码机提供的灌装接口实现电子健康卡应用密钥的灌装，密码机密钥灌装接口详细描述见附录A。

支持电子健康卡管理系统通过密码机提供的高级应用编程接口实现居民健康卡跨域主索引ID、电子健康卡ID、有效性信息等的生成、验证和加解密功能。

4.3 高级应用编程接口要求

本章节给出密码机提供给电子健康卡应用管理系统的高级应用编程接口。

高级应用编程接口是提供给开发商系统开发来与密码机进行交互操作的函数集。所有高级应用编程接口应具有本规范所规定的统一的库名、函数名、参数类型和顺序。应用开发者或用户在对密码机编程时，可使用相应的库名和函数名，接口调用示例可参见附录 B。

注：本规范仅针对 Windows 32 位系统 C 语言函数给出定义，其他操作系统和编程语言请自行进行转编译，实现相同功能。

4.3.1 密码机连接和断开

4.3.1.1 连接密码机

名称	hsm_connect		
功能	建立与密码机的连接		
说明	连接前请检查白名单是否已设置，长连接只需执行一次。		
	参数名称	参数类型	说明
输入参数	ip	char *	密码机 IP 地址
	port	int	密码机服务端口
返回值	ret	long	>0 连接句柄　<=0 连接失败

4.3.1.2 断开密码机

名称	hsm_disconnect		
功能	断开与密码机的连接		
说明	调用完相关接口后，应执行断开连接操作，释放系统资源。		
	参数名称	参数类型	说明
输入参数	handle	long	连接句柄（hsm_connect 接口的返回值）
返回值	ret	int	0 断开成功

			1 断开失败

4.3.2 主索引 ID 生成接口

名称	hsm_api_indexid		
功能	使用 SM3 算法产生主索引 ID		
说明	无		
	参数名称	参数类型	说明
输入参数	handle	long	连接句柄（hsm_connect 接口的返回值）
	datalen	int	输入数据的长度
	data	unsigned char*	输入数据（证件类型+证件号码+姓名，16 进制字符串）
输出参数	indexid	unsigned char*	主索引 ID
返回值	ret	int	0-成功 其它-失败

4.3.3 电子健康卡 ID 接口

4.3.3.1 电子健康卡 ID 生成接口

名称	hsm_api_ecid		
功能	采用 SM4 加密生成电子健康卡 ID		
说明	无		
	参数名称	参数类型	说明
输入参数	handle	long	连接句柄（hsm_connect 接口的返回值）
	indexid	unsigned char*	主索引 ID
	datalen	int	输入数据的长度
	data	unsigned char*	输入数据（证件类型+证件号，16 进制字符串）
	ver	int	密钥版本，数值为 1-4
输出参数	ecid	unsigned char*	电子健康卡 ID
返回值	ret	int	0-成功 其它-失败

4.3.3.2 电子健康卡 ID 验证接口

名称	hsm_api_valecid

功能	采用 SM4 解密电子健康卡 ID		
说明	无		
	参数名称	参数类型	说明
输入参数	handle	long	连接句柄（hsm_connect 接口的返回值）
	indexid	unsigned char*	主索引 ID
	ecidlen	int	输入电子健康卡 ID 的长度
	ecid	unsigned char*	电子健康卡 ID
	ver	int	密钥版本，数值为 1-4
输出参数	data	unsigned char*	证件类型+证件号码+填充数据
返回值	ret	int	0-成功 其它-失败

4.3.3.3 有效性信息接口

名称	hsm_api_vtime		
功能	采用 SM4 加密/解密有效时间		
说明	无		
	参数名称	参数类型	说明
输入参数	handle	long	连接句柄（hsm_connect 接口的返回值）
	mode	int	0-加密 1-解密
	indata	unsigned char*	Mode=0 时间信息（格式：YYYYMMDDHHMMSS，7 字节） Mode=1 有效性信息密文（16 字节）
	ver	int	密钥版本，数值为 1-4
输出参数	outdata	unsigned char*	输出信息
返回值	ret	int	0-成功 其它-失败

4.4 通讯方式

应具有 RJ45 以太网口，可采用 TCP/IP 协议进行数据通讯。

4.5 电源适应性

应能在 220V 55V、50Hz 条件下正常工作。

4.6 安全性要求

应符合 GB4943.1-2011 中信息技术设备的安全规定。

4.7 气候环境条件

适用的气候条件如表 1 所示。

表 1 气候环境条件

环境温度（℃）		相对湿度（%）		大气压（kPa）
工作	贮存	工作	贮存	
0～40	-10～45	20～80	20～90（45℃）	86～106

5 检测要求

5.1 检测条件

除气候环境试验以外，其他试验均在正常大气条件下进行，即：

温度：15℃～35℃

相对湿度：45%～75%

大气压：86 kPa～106 kPa

5.2 外观和结构

目测检测密码机的外观质量，应符合4.1条规定。

5.3 功能

利用居民健康卡密钥管理系统的测试模拟环境和生产商提供的密钥灌装动态链接库进行测试密钥灌装，应灌装成功。

利用软件模拟电子健康卡应用管理系统对密码机的高级应用编程接口进行调用，可正确完成居民健康卡跨域主索引ID生成、电子健康卡ID的生成和验证、有效性信息加解密等功能。

5.4 高级应用编程接口

利用软件模拟电子健康卡应用管理系统对密码机的高级应用编程接口进行调用，可正确调用连接密码机、断开密码机、主索引ID生成、电子健康卡ID、有效性信息等接口。

5.5 通讯方式

连接密码机的 RJ45 以太网口、配置 TCP/IP 协议参数，利用 PC 机端的软件与密码机进行数据通讯，应通讯正常。

5.6 电源适应性

密码机应在交流电压 165V、220V、275V，频率 50Hz 下加电运行检查程序，应工作正常。

5.7 安全性要求

按照GB4943.1-2011的规定进行。

5.8 气候环境试验

5.8.1 一般要求

环境试验方法总则按GB/T 2421的规定。

5.8.2 工作温度下限

受试样品进行初始检测，严酷等级按4.7条表1中“工作状态”规定的下限值，试验时间2h，期间样品加电工作，受试样品应工作正常，恢复时间为2h。

5.8.3 工作温度上限

受试样品进行初始检测，严酷等级按4.7条表1中“工作”状态规定的上限值，试验时间2h，期间样品加电工作，受试样品应工作正常，恢复时间为2h。

5.8.4 贮存温度下限

受试样品进行初始检测，严酷等级按4.7条表1中“贮存”状态规定的下限值，在不加电的情况下存放16h，恢复时间为2h，进行最后检测，应能正常工作。

5.8.5 贮存温度上限

受试样品进行初始检测，严酷等级按4.7条表1中“贮存”状态规定的上限值，在不加电的情况下存放16h，恢复时间为2h，进行最后检测，应能正常工作。

5.8.6 工作恒定湿热

受试样品进行初始检测，严酷等级按4.7条表1中“工作”状态规定的工作温度、湿热上限值，试验时间2h，期间样品加电工作，受试样品应工作正常，恢复时间为2h。

5.8.7 贮存恒定湿热

受试样品进行初始检测，严酷等级按4.7条表1中“贮存”状态规定的贮存运输温度、湿热上限值，在不加电的情况下存放48h，恢复时间为2h，进行最后检测，应能正常工作。

附录 A 密钥灌装接口说明

A.1 连接加密机

名称	hsm_connect		
功能	建立与加密机的连接		
说明	连接前请检查白名单是否已设置，长连接只需执行一次。		
	参数名称	参数类型	说明
输入参数	ip	char *	加密机 IP 地址
	port	int	加密机服务端口
返回值	ret	int	>0 连接句柄　<0 连接失败

A.2 断开加密机

名称	hsm_disconnect		
功能	断开与加密机的连接		
说明	调用完相关接口后，应执行断开连接操作，释放系统资源。		
	参数名称	参数类型	说明
输入参数	handle	int	连接句柄（hsm_connect 接口的返回值）
返回值	ret	int	0 断开成功 1 断开失败

A.3 SM1 解密计算

名称	Hsm_SM1_Decrypt		
功能	解密所需信息，如 KEK 密钥，待灌装的密钥		
说明	接口要实现八条密钥的导入功能		
	参数名称	参数类型	说明
输入参数	handle	int	连接句柄（hsm_connect 接口的返回值）
	KeyValue	unsigned char*	解密所需要的密钥
	DataIn	unsigned char*	要解密的数据
	OutData	unsigned char*	解密得到的结果
返回值	ret	unsigned short	0x9000　解密成功 其他　解密失败

A.4 导入密钥

名称	Hsm_Import_Key		
功能	向加密机中导入密钥		
说明	接口要实现八条密钥的导入功能		
	参数名称	参数类型	说明
输入参数	handle	int	连接句柄（hsm_connect 接口的返回值）
	KeyValue1	unsigned char*	需要导入加密机的保护密钥明文，版本 1
	KeyValue2	unsigned char*	需要导入加密机的保护密钥明文，版本 2
	KeyValue3	unsigned char*	需要导入加密机的保护密钥明文，版本 3
	KeyValue4	unsigned char*	需要导入加密机的保护密钥明文，版本 4
	KeyValue5	unsigned char*	需要导入加密机的安全密钥明文，版本 1
	KeyValue6	unsigned char*	需要导入加密机的安全密钥明文，版本 2
	KeyValue7	unsigned char*	需要导入加密机的安全密钥明文，版本 3
	KeyValue8	unsigned char*	需要导入加密机的安全密钥明文，版本 4
返回值	ret	unsigned short	0x9000　导入成功 其他　　导入失败

附录 B 接口调用示例和测试验证数据

附录 B 给出了接口调用的完整示例和一组测试验证数据。调用示例部分采用伪代码表示。

B.1 基本信息

证件类型	身份证
证件号码	11010020171225006X
姓名	电子健康卡
安全密钥	0123456789ABCDEFFEDCBA9876543210
保护密钥	11223344556677888877665544332211
有效时间	20180117115003
密码机地址	192.168.1.101
密码机端口	2345

B.2 测试验证示例

```
/* 连接密码机 */
ip = “192.168.1.101”; // 密码机 IP
port = 2345; // 密码机端口
handle = hsm_connect( ip, port );

/* 输入信息 */
idtype = “3031”;
// 身份证 : 01
idnum = “31313031303032303137313232353030365 8”;
// 身份证号 : 11010020171225006X
name = “E794B5E5AD90E581A5E5BAB7E58DA1”;
// 姓名 : 电子健康卡(UTF-8 编码格式)

/* 生成主索引 ID */
```

```
input = idtype + idnum + name;

datalen = 0x23;

// 长度 35 字节，16 进制表示为 0x23

ret = hsm_api_indexid( handle, datalen, input, indexid );

// ret : 0

// indexid :

ABD17E7ED399EF68AB5660155D6E226D2C92EAC3254A4A66BED83AED0ADA1E9E


/* 生成电子健康卡 ID */

datalen = 0x14;

// 长度 20 字节，16 进制表示为 0x14

data = idtype + idnum;

// data: 30313131303130303230313731323235303036 58

ver = 1;

// 选择密钥版本为 1

ret = hsm_api_ecid( handle, indexid, datalen, data, ver, ecid );

// ret : 0

// ecid :

// 98FF9F2C05145CB9305E9D8A57E072BB51180CA49E5BE5E9D41BCE3A9A571928


/* 验证电子健康卡 ID */

ecidlen = 0x20;

// 长度 32 字节，16 进制表示为 0x20

ret = hsm_api_valecid( handle, indexid, ecidlen, ecid, ver, outdata);

// ret : 0

// outdata : 30313131303130303230313731323235303036580000000000000000000000000


/* 生成有效性信息 */
```

```
time = "20180117115003";

ret = hsm_api_vtime( handle, 0, time, ver, valid);

// valid: 92FD69141DFE1553A42251E2B0196148


/* 解密有效性信息 */

ret = hsm_api_vtime( handle, 1, valid, ver, outdata );

// outdata: 20180117115003000000000000000000
```

B.3 验证数据

	以 16 进制表示
证件类型	3031
证件号码	31313031303032303137313232323530303658
姓名	E794B5E5AD90E581A5E5BAB7E58DA1
主索引 ID 输入	303131313031303032303137313232323530303658 E794B5E5AD90E581A5E5BAB7E58DA1
主索引 ID	ABD17E7ED399EF68AB5660155D6E226D2C92EAC3254A4A66BED83AED0ADA1E9E
分散因子	92CDCE45A16799FD
分散因子（取反）	6D3231BA5E986602
用户身份认证密钥	86C63180C2806ED1F47B859DE501215B
电子健康卡 ID 输入	303131313031303032303137313232323530303658
电子健康卡 ID	98FF9F2C05145CB9305E9D8A57E072BB51180CA49E5BE5E9D41BCE3A9A571928
时间信息	20180117115003
有效性信息	92FD69141DFE1553A42251E2B0196148