



中华人民共和国通信行业标准

YD/T 2522-2013

CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口测试方法 支持 CSIM 应用的 UICC

CDMA digital cellular mobile telecommunication network UICC-ME
interface test method-UICC supporting CSIM application

2013-04-25 发布

2013-06-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	1
4 测试环境	2
5 支持 CSIM 应用的 UICC 的物理、电气及逻辑特性测试方法	2
6 CSIM 应用一致性测试	2
6.1 基本文件的内容	2
6.2 安全特性	4
6.3 CSIM 命令	5

前 言

本标准是 CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口系列标准之一。该系列标准的名称如下:

a) YD/T 2525-2013《CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口技术要求 支持 OMH 功能的 CSIM 应用特性》

b) YD/T 2522-2013《CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口测试方法 支持 CSIM 应用的 UICC》

c)《CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口测试方法 终端 CSIM 应用特性》

d) YD/T 2524-2013《CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口技术要求 CCAT 应用特性》

e) YD/T 2523-2013《CDMA 数字蜂窝移动通信网通用集成电路卡 (UICC) 与终端间接口测试方法 终端 CCAT 应用特性》

本标准按照 GB/T 1.1-2009 给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位:工业和信息化部电信研究院。

本标准主要起草人:杨红梅、于 力、潘 娟、杜志敏。

CDMA数字蜂窝移动通信网

通用集成电路卡（UICC）与终端间接口测试方法

支持CSIM应用的UICC

1 范围

本标准规定了CSIM应用的测试环境和主要测试内容，包括安全特性、CSIM命令等内容。

本标准适用于支持 CSIM 应用的 UICC。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 1762.1-2011	TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡（UICC）与终端间 Cu 接口技术要求 第 1 部分：物理、电气和逻辑特性
YD/T 1763.4-2011	TD-SCDMA/WCDMA 数字蜂窝移动通信网 通用集成电路卡(UICC)与终端间 Cu 接口测试方法 第 4 部分：支持通用用户识别模块(USIM)应用的 UICC
YD/T 2525-2013	CDMA 数字蜂窝移动通信网通用集成电路卡（UICC）与终端间接口技术要求 支持 OMH 功能的 CSIM 应用特性

3 缩略语

下列缩略语适用于本文件。

ADF	Application Dedicated File	应用专用文件
AKA	Authentication and key agreement	认证和密钥协商
BCMCS	Broadcast/Multicast Services	广播/组播业务
CDMA	Code Division Multiple Access	码分复用接入
CHAP	Challenge Handshake Authentication Protocol	查询握手认证协议
CSIM	cdma2000 Subscriber Identify Module	cdma2000用户识别模块
DF	Dedicated File	专用文件
EF	Dedicated File	基本文件
ESN	Electronic Serial Number	电子序列码
HRPD	High Rate Packet Data	高速分组数据
ME	Mobile Equipment	移动设备
MEID	Mobile Station Equipment Identifier	移动终端设备标识符
PIN	Personal Identification Number	个人识别号码
SFI	Short (elementary)File Identifier	短文件标识
SSD	Shared Secret Data	共享秘密数据
TLV	Tag Length Value	标签长度值
UICC	Universal Integrated Circuit Card	通用集成电路卡
UMAC	UIM-Present MAC	UIM(户识别模块)中的MAC(媒体访问控制)
VPM	Voice Privacy Mask	语音加密掩码

4 测试环境

UICC根据卡的类型，可以是ID-1型UICC或Plug-in型UICC或mini型UICC，CSIM卡应至少包含一个CSIM应用。本标准中出现的CSIM卡指包含CSIM卡应用的UICC，UICC指包含CSIM应用的UICC，两者在本标准中的定义是相等的。

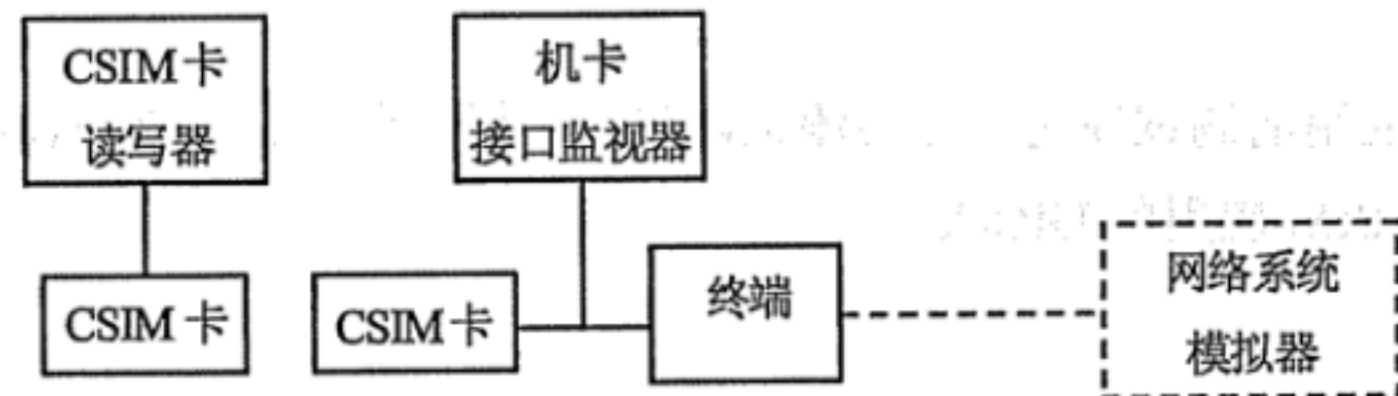


图1 测试环境

如图1所示，CSIM应用特性测试环境中的测试设备包括：CSIM卡、CSIM卡读写器、机卡接口监视器、终端、网络系统模拟器。终端直接对CSIM卡进行操作，在操作过程中，通过Cu接口监视器监视Cu接口的信号和数据流；终端对CSIM卡中数据的读写操作结果，通过CSIM卡读写器读取CSIM卡中的文件来验证。各测试项所需的CSIM卡中的测试数据可以通过CSIM卡读写器写入到CSIM卡中。

需要说明的是，当检测CSIM卡的机卡接口时，终端可使用模拟器，终端模拟器对CSIM卡进行操作，在操作过程中，终端模拟器或可外接机卡接口监视设备监视机卡接口的信号和数据流，终端模拟器对CSIM卡的数据读写操作结果，可以通过CSIM卡读写器来确认接口上的各种操作的结果是否正确。CSIM卡中各测试项所需的CSIM卡中的测试数据文件由CSIM卡读写器预先写入。

5 支持 CSIM 应用的 UICC 的物理、电气及逻辑特性测试方法

CSIM卡应完成YD/T 1763.4-2011中定义的所有物理、电气、逻辑特性和通用命令测试，其中AUTHENTICATE和GET CHALLENGE命令可不做要求。

对CSIM卡进行测试时，YD/T 1763.4-2011中所有的“USIM”应被理解和替换为“CSIM”，例如ADF(USIM)应被换成ADF(CSIM)。

6 CSIM 应用一致性测试

6.1 基本文件的内容

注：本节测试项用来验证被测设备是否包含电信会话所需要的所有EF。因为卡中各文件的内容是卡所特有的或是个性化的，因此本节不对卡的文件内容进行测试。

测试编号：6.1
测试项目：CSIM 卡的 CSIM 应用一致性测试
分 项 目：基本文件的内容
测试目的： 验证 CSIM 卡的文件内容符合下列要求： a) 在ADF(CSIM)下或相应DF下的每一个存在的EF都应可以使用该EF相应的表格中所给出的标识来被选择； b) CSIM卡应包含所有的必选文件； c) EF标识应与EF相应的表格中所给出的标识一致； d) EF的结构和类型应与EF相应的表格中所给出的结构和类型一致；

- e) 文件大小应至少为EF相应的表格中所给出的值;
- f) 如果EF相应的表格中要求SFI为必选, 则该EF必须有SFI;
- g) 访问条件应与EF相应的表格中所给定的访问条件一致

预置条件:

CSIM卡连接到ME模拟器

测试步骤:

- 1) ME模拟器复位CSIM卡;
- 2) ME模拟器向CSIM卡发送SELECT命令来选择EF对应的DF;
 - 响应数据中标签为‘83’的TLV数据对象应指示MF的标识为‘3F00’;
 - CSIM卡返回的状态条件为SW1=‘90’、SW2=‘00’—正常的命令结尾;
- 3) ME模拟器向CSIM卡发送SELECT命令来选择YD/T 2522-2013《CDMA数字蜂窝移动通信网通用集成电路卡(UICC)与终端间接口技术要求 支持OMH功能的CSIM应用特性》第5章的第一个EF;
 - CSIM卡返回的状态条件为SW1=‘90’、SW2=‘00’—正常的命令结尾;
 - 响应数据应满足以下要求:

标签为‘83’的TLV数据对象应指示所选文件的标识;

标签为‘82’的TLV数据对象不应为‘38’和‘78’;

标签为‘82’的TLV数据对象应指示在YD/T 2522-2013《CDMA数字蜂窝移动通信网通用集成电路卡(UICC)与终端间接口技术要求 支持OMH功能的CSIM应用特性》第5章中该EF所给定的结构;

如果EF为透明文件, 则标签为‘80’的TLV数据对象应至少为本系列标准技术要求的第5章中该EF所给定的最小文件大小;

如果文件为线性定长结构或循环结构, 则标签为‘82’的TLV DO的第5和第6字节应与YD/T 2522-2013《CDMA数字蜂窝移动通信网通用集成电路卡(UICC)与终端间接口技术要求 支持OMH功能的CSIM应用特性》要求的第5章中该EF所给定的记录长度相一致;

如果文件为线性定长结构或循环结构, 则标签为‘80’的TLV DO应为一个整数乘以记录的长度;

对于YD/T 2522-2013《CDMA数字蜂窝移动通信网通用集成电路卡(UICC)与终端间接口技术要求 支持OMH功能的CSIM应用特性》要求的第5中节分配了SFI值的EF文件, 标签为‘88’的TLV 数据对象应呈现并与所分配的SFI值一致; 对于没有分配SFI值的文件, 标签为‘88’的TLV数据对象应呈现为空值;

标签为‘86’‘8B’‘AB’‘8C’的TLV DO应指示了该EF所给出的访问条件。
- 4) 依次选择YD/T 2522-2013《CDMA数字蜂窝移动通信网通用集成电路卡(UICC)与终端间接口技术要求 支持OMH功能的CSIM应用特性》第5章中的其他EF; 依据步骤3)的要求进行检查。
- 5) 如果访问条件指示为引用安全, 必要时在该点应读取EF(ARR)中的被引用的记录

预期结果:

CSIM卡满足测试项目的所有要求

测试说明:

本测试项除检查与CDMA接入相关的文件外, 也检查为支持OMH功能而定义的文件, 即与EF(CST)中业务n35、n37、n38、n39和n40相关的文件

6.2 安全特性

测试编号: 6.2
测试项目: CSIM 卡的 CSIM 应用一致性测试
分项目: 安全特性
<p>测试目的:</p> <p>验证 CSIM 卡的文件内容符合下列要求:</p> <p>a) CSIM 应用应使用 '01' 作为 PIN 的密钥引用, 使用 '81' 作为 PIN2 的密钥引用;</p> <p>b) 使用 PIN2 的访问仅局限于 CSIM 应用 (也就是仅用于 ADF);</p> <p>c) 对于具有多认证能力的 UICC 上的 CSIM 应用, 使用限定的有效值是 '00' 和 '08', '00' 表示不使用认证要求, '08' 表示使用 PIN 来认证 (基于用户知识的密钥引用数据);</p> <p>d) CSIM 应用中的每一个文件都应引用存储在 EF(ARR) 中的一个访问规则;</p> <p>e) 在 DF(TELECOM) 下的每一个文件都应引用存储在 DF(TELECOM) 下的 EF(ARR) 中的一个访问规则;</p> <p>f) 具有多认证能力的 UICC (从安全角度来看) 应支持 YD/T 1762.1-2011 中定义的使用 SE ID 的格式引用;</p> <p>g) 具有多认证能力的 UICC (从安全角度来看) 应支持使用通用 PIN (密钥引用 '11') 来替代 UICC 应用 PIN, 如 YD/T 1762.1-2011 所定义。只有通用 PIN 可以用做替代的 PIN</p>
<p>预置条件:</p> <p>CSIM 卡连接到 ME 模拟器</p>
<p>测试步骤:</p> <p>1) 对于具有多认证能力的 CSIM 卡执行下列步骤:</p> <ul style="list-style-type: none"> - ME 模拟器复位 CSIM 卡; - ME 模拟器向 CSIM 卡发送 SELECT 命令来选择 DF(TELECOM)。 - ME 模拟器向 CSIM 卡发送 SELECT 命令选择 DF(TELECOM) 下的第一个 EF; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性;</p> <ul style="list-style-type: none"> - 对 CSIM 卡中 DF(TELECOM) 下的所有 EF 发送 SELECT 命令; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性;</p> <ul style="list-style-type: none"> - ME 模拟器向 CSIM 卡发送 SELECT 命令来选择并激活 CSIM 应用; <p>响应数据应满足以下要求: 标签为 'C6' 的 TLV DO (PS 模版 DO) 应包含对于通用 PIN 标签为 '95' 的 TLV DO (使用限定), 并且该 TLV 的值为 '00' 或 '08';</p> <ul style="list-style-type: none"> - ME 模拟器向 CSIM 卡发送 SELECT 命令来选择 CSIM 卡应用中的第一个 EF; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性; 响应数据还应包含 SE ID 和 EFARR 记录编号;</p> <ul style="list-style-type: none"> - 对 CSIM 卡中所选 ADF 下的所有 EF 发送 SELECT 命令; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性; 响应数据还应包含 SE ID 和 EFARR 记录编号;</p> <p>2) 对于具有单认证能力的 CSIM 卡执行下列步骤:</p> <ul style="list-style-type: none"> - ME 模拟器复位 CSIM 卡; - ME 模拟器向 CSIM 卡发送 SELECT 命令来选择 DF(TELECOM); - ME 模拟器向 CSIM 卡发送 SELECT 命令在选择 DF(TELECOM) 下的第一个 EF; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性; 响应数据还应包含对存储在 EFARR 中的一个访问规则的引用;</p> <ul style="list-style-type: none"> - 对 CSIM 卡中 DF (TELECOM) 下的所有 EF 发送 SELECT 命令; <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性;</p> <ul style="list-style-type: none"> - 对 CSIM 卡中所选 ADF 的所有 ADF(CSIM) 下的 EF 发送 SELECT 命令。 <p>响应数据应包含标签为 '8B' 的 TLV DO, 它指示了引用的安全属性</p>
<p>预期结果:</p> <p>CSIM 卡满足测试项目的所有要求</p>

6.3 CSIM 命令

6.3.1 安全相关命令

测试编号: 6.3.1.1
测试项目: 管理共享秘密数据(SSD)
分项目: 更新共享秘密数据 (Update SSD)
<p>测试目的:</p> <p>验证 Update SSD 用于产生新的 SSD, 在 BSC (BASE STATION CHALLENGE) 模式下, 这个功能只能在 BASE STATION CHALLENGE 功能执行之后执行一次</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDSSD=7 字节 16 进制数, RANDSeed=4 字节 16 进制数, Process_Control="00", ESN="00 00 00 00"</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 UPDATE SSD 命令, 参数是 RANDSSD, Process_Control, ESN; 5) ME 模拟器向 CSIM 卡发送 BASE STATION CHALLENGE 命令, 参数是 RANDSeed; 6) ME 模拟器向 CSIM 卡发送 UPDATE SSD 命令, 参数是 "BSC" 模式, 参数为 RANDSSD, Process_Control, ESN
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误;</p> <p>b) 步骤 6) 后, CSIM 卡返回状态为 SW1="90", SW2="00" ——命令正常结束</p>

测试编号: 6.3.1.2
测试项目: 管理共享秘密数据 (SSD)
分项目: 确认共享秘密数据 (Confirm SSD)
<p>测试目的:</p> <p>验证 Confirm SSD 满足下列要求:</p> <p>a) Confirm SSD 用于确认网络和卡片之间的认证是否成功, CONFIRM SSD 功能生成 "AUTHBS" 并将它与网络传来的 AUTHBS 比较。如果网络传来的 AUTHBS 和 CSIM 卡计算得到的 AUTHBS 相同, 就将新 SSD 值写入当前 SSD 的存储位置;</p> <p>b) 在 BSC 模式中, CONFIRM SSD 功能只能在 "UPDATE SSD" 功能之后执行一次;</p> <p>c) 如果网络传来的 AUTHBS 和 CSIM 卡计算得到的 AUTHBS 不相等, 那么 CSIM 卡返回 SW1="98", SW2="04"</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDSSD=7 字节 16 进制数, RANDSeed=4 字节 16 进制数, Process_Control="00", ESN="00 00 00 00"</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 卡发送 BASE STATION CHALLENGE 命令, 参数为 RANDSeed; 5) ME 模拟器向 CSIM 卡发送 UPDATE SSD 命令, 使用 "BSC" 模式, 参数为 RANDSSD, Process_Control="00" 和 ESN; 6) ME 模拟器向 CSIM 卡发送 CONFIRM SSD 命令, 参数为根据步骤 4 中 CSIM 所返回的 RANDBS 计算得到的正确 AUTHBS 值; 7) ME 模拟器向 CSIM 卡发送 CONFIRM SSD 命令, 参数为根据步骤 4 中 CSIM 所返回的 RANDBS 计算得到的正确 AUTHBS 值; 8) ME 模拟器复位 CSIM 卡; 9) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 10) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 11) ME 模拟器向 CSIM 卡发送 BASE STATION CHALLENGE 命令, 参数是 RANDSeed; 12) ME 模拟器向 CSIM 卡发送 CONFIRM SSD 命令, 参数为根据步骤 11 中 CSIM 所返回的 RANDBS 计算得到的正确 AUTHBS 值; 13) ME 模拟器向 CSIM 卡发送 BASE STATION CHALLENGE 命令, 参数是 RANDSeed; 14) ME 模拟器向 CSIM 卡发送 UPDATE SSD 命令, 使用 "BSC" 模式, 参数为 RANDSSD, Process_Control="00" 和 ESN; 15) ME 模拟器向 CSIM 卡发送 CONFIRM SSD 命令, 参数为不是根据步骤 13 中 CSIM 所返回的 RANDBS 计算得到的正确 AUTHBS 值
<p>预期结果:</p> <p>a) 步骤 6) 后, 新的 SSD 存储在 CSIM 卡中, 新值在接下来的认证计算中使用, CSIM 卡返回状态为 SW1="90", SW2="00" ——命令正常结束;</p> <p>b) 步骤 7) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误;</p> <p>c) 步骤 12) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误;</p> <p>d) 步骤 15) 后, CSIM 卡返回状态为 SW1="98", SW2="04" ——认证错误</p>

测试编号: 6.3.1.3
测试项目: 安全相关命令
分项目: 基站检验 (Base Station Challenge)
<p>测试目的:</p> <p>Base Station Challenge 是为了产生一个将被发送到网络侧的随机数, 验证 CSIM 卡能满足下列要求:</p> <p>a) Base Station Challenge 功能应返回 RANDBS;</p> <p>b) 如果连续两次输入相同的随机数 RANDSeed, 该功能返回随机数 RANDBS 应是不同的</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDSeed 值为 4 字节 16 进制数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Base Station Challenge 命令, 参数是 RANDSeed; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器向 CSIM 卡发送 Base Station Challenge 命令, 参数是和步骤 4) 相同的 RANDSeed; 7) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡返回状态为 SW1 = "9F", SW2 = "04" —— 命令正常结束;</p> <p>b) 步骤 5) 后, CSIM 卡返回 4 字节随机数 RANDBS;</p> <p>c) 步骤 6) 后, CSIM 卡返回状态为 SW1 = "9F", SW2 = "04" —— 命令正常结束;</p> <p>d) 步骤 7) 后, CSIM 卡返回 4 字节随机数 RANDBS, 与步骤 5) 的 RANDBS 不同</p>

测试编号: 6.3.1.4
测试项目: 安全相关命令
分项目: 生成密钥 (Generate Key/VPM)
<p>测试目的:</p> <p>验证 Generate Key/VPM 的作用是为终端生成密钥。RUN CAVE 命令先于该命令执行, 并将 Process Control 字段第 4 位 (Save Registers On) 设置为 1。验证 Generate Key/VPM 能满足下列要求:</p> <p>a) Generate Key/VPM 功能可以在设置 Save Registers On 的 RUN CAVE 功能之后任何时候执行。RUN CAVE 可能在 Save Registers Off 的情况下执行多次, 但是只有最近一次在 Save Registers On 情况下执行的 RUN CAVE 所产生并内部存储的数据才能作为 Generate Key/VPM 的输入参数。如果该次序条件不满足, 那么 Generate Key/VPM 返回 SW1=“98”, SW2=“34”。</p> <p>b) Generate Key/VPM 命令执行后, 用 GET RESPONSE 命令取回执行结果: 64 位定长密钥和用户指定长度的 VPM。用户指定的长度是根据 Generate Key/VPM 命令参数的“第一字节位”和“最后字节位”计算出来的</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDU=3 字节 16 进制数, RAND=4 字节 16 进制数, ESN=“00 00 00 00”</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Generate Key/VPM 命令, 参数为: VPM 输出的第一个字节位=“00”、VPM 输出的最后一个字节位=“40”; 5) ME 模拟器向 CSIM 卡发送 RUN CAVE 命令, 参数是 RANDTYPE=“00”, RAND, DigLength=“00”, DIGIT=“00 00 00”, Process_Control=“00”和 ESN; 6) ME 模拟器向 CSIM 卡发送 Generate Key/VPM 命令, 参数为: VPM 输出的第一个字节位=“00”、VPM 输出的最后一个字节位=“40”; 7) ME 模拟器复位 CSIM 卡; 8) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 9) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 10) ME 模拟器向 CSIM 卡发送 RUN CAVE 命令, 参数是 RANDTYPE=“00”, RAND, DigLength=“00”, DIGIT=“00 00 00”, Process_Control=“10”和 ESN; 11) ME 模拟器向 CSIM 卡发送 Generate Key/VPM 命令, 参数为: VPM 输出的第一个字节位=“00”、VPM 输出的最后一个字节位=“40”; 12) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令取出 key 和 VPM 计算结果, 参数 P3=49; 13) ME 模拟器复位 CSIM 卡; 14) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令;

- 15) ME模拟器向CSIM卡发送SELECT命令, 选择ADF (CSIM);
- 16) ME模拟器向CSIM卡发送RUN CAVE命令, 参数是RANDTYPE="00", RAND, DigLength="00", DIGIT="00 00 00", Process_Control="10"和ESN;
- 17) ME模拟器向CSIM卡发送RUN CAVE命令, 参数是RANDTYPE="00", RAND, DigLength="00", DIGIT="00 00 00", Process_Control="00"和ESN;
- 18) ME模拟器向CSIM卡发送Generate Key/VPM命令, 参数为: VPM输出的第一个字节位="00"、VPM输出的最后一个字节位="40";
- 19) ME模拟器向CSIM卡发送GET RESPONSE命令取出key和VPM计算结果, 参数P3=49;
- 20) ME模拟器复位CSIM卡;
- 21) ME模拟器向CSIM卡发送VERIFY PIN命令;
- 22) ME模拟器向CSIM卡发送SELECT命令, 选择ADF (CSIM);
- 23) ME模拟器向CSIM卡发送RUN CAVE命令, 参数是RANDTYPE="00", RAND, DigLength="00", DIGIT="00 00 00", Process_Control="10"和ESN;
- 24) ME模拟器向CSIM卡发送Generate Key/VPM命令, 参数为: VPM输出的第一个字节位="FF"、VPM输出的最后一个字节位="FF";
- 25) ME模拟器向CSIM卡发送Generate Key/VPM命令取出key, 参数P3=08

预期结果:

- a) 步骤 4) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误;
- b) 步骤 6) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误;
- c) 步骤 11) 后, CSIM 卡返回状态为 SW1="9F", SW2="49" ——输出 key 和 VPM;
- d) 步骤 12) 后, 返回数据的 1~8 字节是 key, 其他数据是 VPM;
- e) 步骤 18) 后, CSIM 卡返回状态为 SW1="9F", SW2="49" ——输出 key 和 VPM;
- f) 步骤 19) 后, 返回数据的 1~8 字节是 key, 其他数据是 VPM;
- g) 步骤 24) 后, CSIM 卡返回状态为 SW1="9F", SW2="08" ——输出 key;
- h) 步骤 25) 后, CSIM 卡返回数据的 1~8 字节为 key

测试编号: 6.3.1.5
测试项目: 认证 (Authenticate)
分项目: 运行 CAVE 算法 (RUN CAVE)
<p>测试目的:</p> <p>验证 RUN CAVE 能满足下列要求:</p> <p>a) RUN CAVE 功能使 CSIM 卡运行 CAVE 算法完成认证操作 (AUTHR/AUTHU) 并且根据之后的命令完成密钥计算;</p> <p>b) RUN CAVE 功能应成功计算 AUTHR/AUTHU 并使用 CAVE 测试向量完成密钥的正确计算</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) ESN = "00 00 00 00", RAND 为一个 4 字节 16 进制数, RANDU 为一个 3 字节 16 进制数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80' (表示进行 RUN CAVE 认证), 命令携带参数 RANDTYPE = "00", RAND, DigLength = "00", DIGIT = "00 00 00", Process_Control = "00" 和 ESN; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "00", RAND, DigLength = "00", DIGIT = "00 00 00", Process_Control = "10" 和 ESN; 7) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 8) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "01", RANDU, DigLength = "00", DIGIT = "00 00 00", Process_Control = "00" 和 ESN; 9) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 10) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "01", RANDU, DigLength = "00", DIGIT = "00 00 00", Process_Control = "10" 和 ESN; 11) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 12) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "00", RAND, DigLength = "04", DIGIT = "00 00 01", Process_Control = "00" 和 ESN; 13) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 14) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "00", RAND, DigLength = "04", DIGIT = "00 00 01", Process_Control = "10" 和 ESN; 15) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 16) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2 = '80', 命令携带参数 RANDTYPE = "01", RANDU, DigLength = "04", DIGIT = "00 00 01", Process_Control = "00" 和 ESN;

- 17) ME模拟器向CSIM卡发送GET RESPONSE命令;
- 18) ME模拟器向CSIM卡发送Authenticate命令, 其中的P2= '80', 命令携带参数RANDTYPE= "01", RANDU, DigLength= "04", DIGIT= "00 00 01", Process_Control= "10" 和ESN;
- 19) ME模拟器向CSIM卡发送GET RESPONSE命令

预期结果:

- a) 步骤4) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03";
- b) 步骤5) 后, CSIM卡返回数据为输入参数用CAVE算法计算出的正确值;
- c) 步骤6) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- d) 步骤7) 后, 返回数据为输入参数用CAVE算法计算出的正确值;
- e) 步骤8) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- f) 步骤9) 后, 返回数据为输入参数用CAVE算法计算出的正确值;
- g) 步骤10) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- h) 步骤11) 后, 返回数据为输入参数用CAVE算法计算出的正确值;
- i) 步骤12) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- j) 步骤13) 后, 返回数据为输入参数用CAVE算法计算出的正确值;
- k) 步骤14) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- l) 步骤15) 后, 返回数据为输入参数用CAVE算法计算出的正确值;
- m) 步骤16) 后, CSIM卡返回状态为 SW1= "9F", SW2= "03".
- n) 步骤17) 后, 返回数据为输入参数用CAVE算法计算出的正确值。
- o) 步骤18) 后, UIM返回状态为 SW1= "9F", SW2= "03".
- p) 步骤19) 后, 返回数据为输入参数用CAVE算法计算出的正确值

测试编号: 6.3.1.6
测试项目: 认证 (Authenticate)
分项目: 3G 认证加密算法 (3G Authentication AKA) (可选)
<p>测试目的:</p> <p>验证 3G Authentication AKA 能满足下列要求:</p> <p>a) 3G Authentication AKA 功能使 CSIM 卡根据卡中存储的 3G AKA 根密钥运行 AKA 完成密钥计算;</p> <p>b) 如果 MAC 匹配失败, 则 CSIM 卡应返回状态字 SW1= '98' 和 SW2= '04';</p> <p>c) 如果 CSIM 卡检测出序列号无效, 则 3G Authentication AKA 命令应使 CSIM 卡设置 Synchronization Failure Tag 为 '01', 并返回 AUTS;</p> <p>d) 如果 CSIM 卡检测出 MAC 匹配且序列号有效, 则 3G Authentication AKA 命令应使 CSIM 卡设置 Synchronization Failure Tag 为 '00', 并返回计算出的 CK、IK、RES Length 和 RES</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDA 为一个 16 字节 16 进制数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '81' (表示进行 3G Authentication AKA 认证), 命令携带参数 RANDA, Length of AUTN 和正确的 AUTN; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 9) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '81', 命令携带参数 RANDA, Length of AUTN 和 AUTN, 其中 AUTN 包含的 MAC 不正确; 10) ME 模拟器复位 CSIM 卡; 11) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 12) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 13) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '81', 命令携带参数 RANDA, Length of AUTN 和 AUTN, 其中 AUTN 包含的序列号 SQN 超出范围; 14) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡返回状态为 SW1= "9F", SW2=XX (XX=34+RES 的长度);</p> <p>b) 步骤 5) 后, 返回数据为输入参数用 AKA 计算出的 CK、IK 和 RES 参数;</p> <p>c) 步骤 9) 后, CSIM 卡计算出的 XMAC 与 AUTN 包含的 MAC 不匹配, 停止执行该命令, 并返回状态字 SW1= '98' 和 SW2= '04';</p> <p>d) 步骤 13) 后, CSIM 卡返回状态为 SW1= "9F", SW2= "0F";</p> <p>e) 步骤 14) 后, 因 CSIM 卡检测出序列号无效, 设置 Synchronization Failure Tag 为 '01', 并返回携带 AUTS 的响应</p>

测试编号: 6.3.1.7
测试项目: 认证 (Authenticate)
分项目: 生成 UIM 中的 MAC (UMAC Generation) (可选)
测试目的: 验证 CSIM 卡能正确支持 UMAC Generation 命令, CSIM 卡使用 UAK 将 MAC-I 转换成 UMAC
预置条件: CSIM 卡连接到 ME 模拟器上
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送正确的 3G Authentication AKA 命令, 以使卡生成 UAK; 5) ME 模拟器向 CSIM 卡发送 UMAC Generation 命令, 命令携带参数 MAC-I; 6) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 7) ME 模拟器复位 CSIM 卡; 8) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 9) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 10) ME 模拟器向 CSIM 卡发送错误的 3G Authentication AKA 命令, 以使卡清除 UAK; 11) ME 模拟器向 CSIM 卡发送 UMAC Generation 命令, 命令携带参数 MAC-I; 12) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
预期结果: a) 步骤 5) 后, CSIM 卡返回状态为 SW1 = "9F", SW2 = "05". b) 步骤 6) 后, CSIM 卡返回 Success Tag = "0x01" 和转换后的 UMAC. c) 步骤 11) 后, CSIM 卡返回状态为 SW1 = "9F", SW2 = "01". d) 步骤 12) 后, CSIM 卡返回 Success Tag = "0x00"

测试编号: 6.3.1.8
测试项目: 认证 (Authenticate)
分项目: 确认密钥 (CONFIRM_KEYS) (可选)
测试目的: 验证 CSIM 卡能正确支持 CONFIRM_KEYS 命令
预置条件: CSIM 卡连接到 ME 模拟器上
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送正确的 3G Authentication AKA 命令, 以使卡生成 CK, IK, UAK; 5) ME 模拟器向 CSIM 卡发送 Confirm Keys 命令, 命令不携带任何参数
预期结果: 步骤 5) 后, CSIM 卡返回状态为 SW1 = "9F", SW2 = "00"

测试编号: 6.3.1.9
测试项目: 认证 (Authenticate)
分项目: WLAN 认证加密算法 (WLAN Authentication AKA) (可选)
<p>测试目的:</p> <p>验证 WLAN Authentication AKA 能满足下列要求:</p> <p>a) WLAN Authentication AKA 功能使 CSIM 卡根据卡中存储的 WLAN 根密钥运行 AKA 完成密钥计算;</p> <p>b) 如果 MAC 匹配失败, 则 CSIM 卡应返回状态字 SW1= '98' 和 SW2= '04';</p> <p>c) 如果 CSIM 卡检测出序列号无效, 则 WLAN Authentication AKA 命令应使 CSIM 卡设置 Synchronization Failure Tag 为 '01', 并返回 AUTS;</p> <p>d) 如果 CSIM 卡检测出 MAC 匹配且序列号有效, 则 WLAN Authentication AKA 命令应使 CSIM 卡设置 Synchronization Failure Tag 为 '00', 并返回计算出的 CK、IK、RES Length 和 RES</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) RANDA 为一个 16 字节 16 进制数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '82' (表示进行 WLAN Authentication AKA 认证), 命令携带参数 RANDA, Length of AUTN 和 AUTN; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 9) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '82', 命令携带参数 RANDA, Length of AUTN 和 AUTN, 其中 AUTN 包含的 MAC 不正确; 10) ME 模拟器复位 CSIM 卡; 11) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 12) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 13) ME 模拟器向 CSIM 卡发送 Authenticate 命令, 其中的 P2= '82', 命令携带参数 RANDA, Length of AUTN 和 AUTN, 其中 AUTN 包含的 SQN 不正确; 14) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡返回状态为 SW1= "9F", SW2= "XX" (XX=34+RES 的长度);,</p> <p>b) 步骤 5) 后, 返回计算出的 CK、IK 和 RES 参数;</p> <p>c) 步骤 9) 后, CSIM 卡计算出的 XMAC 与 AUTN 中包含的 MAC 不匹配, 停止执行该命令, 并返回状态字 SW1='98'和 SW2= '04';</p> <p>d) 步骤 13) 后, CSIM 卡返回状态为 SW1= "9F", SW2= "0F";</p> <p>e) 步骤 14) 后, 因 CSIM 卡检测出 SQN 无效, 设置 Synchronization Failure Tag 为 '01', 并返回携带 AUTS 的响应</p>

6.3.2 终端标识管理命令

测试编号: 6.3.2
测试项目: 电子序列码_移动终端设备标识符管理命令(ESN_MEID 管理命令)
分项目: 存储 ESN_MEID_ME (Store ESN_MEID_ME)
测试目的: 验证 Store ESN_MEID_ME 的功能是更新 EFESN_ME 中的 ESN 或 MEID 长度和值, 并返回 Change Flag, Usage Indicator 字段
预置条件: a) CSIM 卡连接到 ME 模拟器上; b) EF (ESN_ME) 的 ESN 或 MEID 为全 0
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Store ESN_MEID_ME 命令, 参数是 ESN, 其值为全 0 (和 EF (ESN_ME) 中的 ESN_ME 有同样的长度和值); 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器向 CSIM 卡发送 Store ESN_MEID_ME 命令, 参数是 MEID, 其值为全 0; 7) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 8) ME 模拟器向 CSIM 卡发送 Store ESN_MEID_ME 命令, 参数是 MEID, 其值为非全 0; 9) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 10) ME 模拟器向 CSIM 卡发送 Store ESN_MEID_ME 命令, 参数是 MEID, 其值与步骤 8) 相同; 11) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 12) ME 模拟器向 CSIM 卡发送 Store ESN_MEID_ME 命令, 参数是 ESN 其值为非全 0; 13) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
预期结果: a) 步骤 4) 后, CSIM 卡返回状态为 SW1="9F", SW2="01" ——命令正常结束; b) 步骤 5) 后, CSIM 卡返回的第 1 字节第 0 位为 0, 表示 ESN/MEID 没有改变; 第 1 字节第 4 位为 Usage 指示器, 与 EF (USGIND) 中的标志位 b1 的值相同; c) 步骤 6) 后, CSIM 卡返回状态为 SW1="9F", SW2="01" ——命令正常结束; d) 步骤 7) 后, CSIM 卡返回的第 1 字节第 0 位为 1, 表示 ESN/MEID 有改变; 第 1 字节第 4 和 5 位为 Usage 指示器, 与 EF (USGIND) 中的标志位 b1 和 b2 的值相同; e) 步骤 8) 后, CSIM 卡返回状态为 SW1="9F", SW2="01" ——命令正常结束; f) 步骤 9) 后, CSIM 卡返回的第 1 字节第 0 位为 1, 表示 ESN/MEID 有改变; 第 1 字节第 4 和 5 位为 Usage 指示器, 与 EF (USGIND) 中的标志位 b1 和 b2 的值相同; g) 步骤 10) 后, CSIM 卡返回状态为 SW1="9F", SW2="01" ——命令正常结束; h) 步骤 11) 后, CSIM 卡返回的第 1 字节第 0 位为 0, 表示 ESN/MEID 没有改变; 第 1 字节第 4 和 5 位为 Usage 指示器, 与 EF (USGIND) 中的标志位 b1 和 b2 的值相同; i) 步骤 12) 后, CSIM 卡返回状态为 SW1="9F", SW2="01" ——命令正常结束; j) 步骤 13) 后, CSIM 卡返回的第 1 字节第 0 位为 1, 表示 ESN/MEID 有改变; 第 1 字节第 4 位为 Usage 指示器, 与 EF (USGIND) 中的标志位 b1 的值相同

6.3.3 计算 IP 认证 (Compute IP Authentication)

测试编号: 6.3.3.1
测试项目: 计算 IP 认证 (Compute IP Authentication)
分项目: 计算 IP 认证——查询握手认证协议 (CHAP) 功能 (可选)
测试目的: 验证 Compute IP Authentication-CHAP 命令能返回正确的 CHAP 响应
预置条件: a) CSIM 卡连接到 ME 模拟器上; b) 输入参数包括: P1=00 (CHAP), ME 模拟器提供的 1 字节长的 CHAP_ID, ME 模拟器提供的 1 字节长的 NAI_Entry_index, CHAP_Challenge=32 字节随机数。注意: NAI_Entry_index 是 4 比特参数, 用字节的低四位表示, 高四位为 0
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数为: P1='0', 输入参数有 CHAP_ID, NAI-Entry-Index 和 CHAP-Challenge; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
预期结果: a) 步骤 4) 后, CSIM 卡返回状态字为 SW1="9F", SW2="10" ——命令正常结束; b) 步骤 5) 后, CSIM 卡返回数据为基于输入数据的正确 CHAP 响应
说明: 该功能用于为 Simple IP 认证生成 CHAP 响应

测试编号: 6.3.3.2
测试项目: 计算 IP 认证 (Compute IP Authentication)
分项目: MN-HA 认证功能 (可选)
<p>测试目的:</p> <p>a) Compute IP Authentication-MN-HA 为单独 Registration-Data 数据块返回正确的 MN-HA 认证结果;</p> <p>b) Compute IP Authentication-MN-HA 为多个 Registration-Data 数据块返回正确的 MN-HA 认证结果;</p> <p>c) 如果输入的数据块次序错误, CSIM 卡返回 SW1 = “98”, SW2 = “34”;</p> <p>d) 在执行 P1=MN-HA 认证的 Compute IP Authentication 命令对单独 Registration-Data 数据块操作后, 紧接着再执行一次 P1=MN-HA 认证的 Compute IP Authentication 命令对单独 Registration-Data 数据块操作, 仍能返回正确的 MN-HA 认证结果</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) 参数包括: P1=01(MN-HA 认证), ME 模拟器提供的 1 字节长的 NAI_Entry_index, Registration-Data= 可变长度登记数据。注意: NAI_Entry_index 是 4 比特长参数, 用字节的低四位表示, 高四位为 0</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=02 (单独数据块), NAI-Entry-Index 和 Registration-Data; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=02 (单独数据块), NAI-Entry-Index 和 Registration-Data; 7) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 8) ME 模拟器复位 CSIM 卡; 9) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 10) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 11) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=00 (第一数据块), NAI-Entry-Index 和 Registration-Data (第一数据块); 12) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=01 (下一数据块) 和 Registration-Data (第二数据块); 13) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1= MN-HA Authenticator, P2=03 (最后数据块) 和 Registration-Data (最后数据块); 14) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 15) ME 模拟器复位 CSIM 卡; 16) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令;

- 17) ME模拟器向CSIM卡发送SELECT命令, 选择ADF(CSIM);
- 18) ME模拟器向CSIM卡发送Compute IP Authentication命令, 参数是: P1= MN-HA Authenticator, P2=03 (最后数据块) 和Registration-Data

预期结果:

- a) 步骤4) 后, CSIM卡返回状态为 SW1= "9F", SW2= "10" ——命令正常结束;
- b) 步骤5) 后, UIM 返回数据为基于输入数据的正确 MN-HA 认证字结果;
- c) 步骤6) 后, CSIM卡返回状态为 SW1= "9F", SW2= "10" ——命令正常结束;
- d) 步骤7) 后, CSIM卡返回数据为基于输入数据的正确 MN-HA 认证结果;
- e) 步骤11) 后, CSIM卡返回状态为 SW1= "90", SW2= "00" ——命令正常结束;
- f) 步骤12) 后, CSIM卡返回状态为 SW1= "90", SW2= "00" ——命令正常结束;
- g) 步骤13) 后, CSIM卡返回状态为 SW1= "9F", SW2= "10" ——命令正常结束;
- h) 步骤14) 后, CSIM卡返回数据为基于输入数据的正确 MN-HA 认证结果;
- i) 步骤18) 后, CSIM卡返回状态为 SW1= "98", SW2= "34" ——命令次序错误

说明: 这个命令的作用是为 Mobile IP 认证生成 MN-HA 认证响应

测试编号: 6.3.3.3
测试项目: 计算 IP 认证 (Compute IP Authentication)
分项目: MIP-RRQ Hash 功能 (可选)
<p>测试目的:</p> <p>a) Compute IP Authentication-MIP-RRQ Hash 为单独的 Preceding MIP-RRQ 数据块计算 MIP-RRQ Hash, 并将得到的数据暂时存储在 CSIM 卡中作为认证下一步操作的输入数据;</p> <p>b) Compute IP Authentication-MIP-RRQ Hash 为多个的 Preceding MIP-RRQ 数据块计算 MIP-RRQ Hash, 并将得到的数据暂时存储在 CSIM 卡中作为认证下一步操作的输入数据。</p> <p>c) 如果命令的数据块没有按顺序给出, CSIM 卡返回 SW1=“98”, SW2=“34”;</p> <p>d) 如果命令顺序错误, CSIM 卡返回 SW1=“98”, SW2=“34”</p> <p>注意: 如果 MIP-RRQ Hash 或 MN-AAA 认证命令次序错误, CSIM 卡都返回 SW1=“98”, SW2=“34”</p> <p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) 参数: P1=“02”(MIP-RRQ Hash), ME 模拟器提供可变长度的 Preceding MIP-RRQ 数据, MN-AAA 扩展报头=8 字节扩展数据</p> <p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=02 (单独数据块), NAI-Entry-Index 和 Registration-Data; 5) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MIP-RRQ Hash, P2=02 (单独数据块), Preceding MIP-RRQ 数据和 MN-AAA 扩展报头; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 9) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=00 (第一数据块), NAI-Entry-Index 和 Registration-Data (第一数据块); 10) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-HA Authenticator, P2=01 (下一数据块) 和 Registration-Data (第二数据块); 11) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1= MN-HA Authenticator, P2=03 (最后数据块) 和 Registration-Data (最后数据块); 12) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1= MIP-RRQ Hash, P2=00 (第一数据块) 和 Preceding MIP-RRQ Data Block 1; 13) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1= MIP-RRQ Hash, P2=01 (下一个数据块), Preceding MIP-RRQ Data Block 2;

- 14) ME模拟器向CSIM卡发送Compute IP Authentication命令, 参数是: P1= MIP-RRQ Hash, P2=03 (最后数据块), Preceding MIP-RRQ Data Block 3和MN-AAA扩展报头;
- 15) ME模拟器复位CSIM卡;
- 16) ME模拟器向CSIM卡发送VERIFY PIN命令;
- 17) ME模拟器向CSIM卡发送SELECT命令, 选择ADF(CSIM);
- 18) ME模拟器向CSIM卡发送Compute IP Authentication命令, 参数是: P1=MN-HA Authenticator, P2=02 (单独数据块), NAI-Entry-Index和Registration-Data;
- 19) ME模拟器向CSIM卡发送Compute IP Authentication命令, 参数是: P1= MIP-RRQ Hash, P2=03 (最后数据块), Preceding MIP-RRQ数据块和MN-AAA扩展报头;
- 20) ME模拟器执行复位卡、VERIFY PIN和SELECT ADF(CSIM)操作;
- 21) ME模拟器向CSIM卡发送Compute IP Authentication命令, 参数是: P1= MIP-RRQ Hash, P2=02 (单个数据块), Preceding MIP-RRQ数据块和MN-AAA扩展报头, 而不事先发送Compute IP Authentication – MN-HA Authentication

预期结果:

- a) 步骤 5) 后, CSIM 卡返回状态为 SW1= “90”, SW2= “00” ——命令正常结束;
- b) 步骤 12) 后, CSIM 卡返回状态为 SW1= “90”, SW2= “00” ——命令正常结束;
- c) 步骤 13) 后, CSIM 卡返回状态为 SW1= “90”, SW2= “00” ——命令正常结束;
- d) 步骤 14) 后, CSIM 卡返回状态为 SW1= “90”, SW2= “00” ——命令正常结束;
- e) 步骤 19) 后, CSIM 卡返回状态为 SW1= “98”, SW2= “34” ——命令次序错误;
- f) 步骤 21) 后, CSIM 卡返回状态为 SW1= “98”, SW2= “34” ——命令次序错误

说明: 这个命令的作用是为 Mobile IP 认证生成 MIP-RRQ Hash 响应

测试编号: 6.3.3.4
测试项目: 计算 IP 认证 (Compute IP Authentication)
分项目: 计算 IP 认证-- MN-AAA 认证功能 (可选)
<p>测试目的:</p> <p>a) Compute IP Authentication-MN-AAA 认证操作根据前面的 MIP-RRQ Hash 结果计算出正确的 MN-AAA 认证响应数据;</p> <p>b) 如果命令次序错误, CSIM 卡返回 SW1="98", SW2="34"。注意: 如果 MIP-RRQ Hash 或 MN-AAA 认证命令次序错误, CSIM 卡都返回 SW1="98", SW2="34"</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) 参数: P1="03"(MN-AAA 认证), ME 模拟器提供 1 个字节长的 NAI_Entry_index, CHAP_Challenge 为长度小于等于 238 字节的随机数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器已先发送了 Compute IP Authentication -- MN-HA Authenticator 和 Compute IP Authentication - MIP-RRQ 指令, ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-AAA Authenticator, NAI-Entry-Index 和 Challenge; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=MN-AAA Authenticator, NAI-Entry-Index 和 Challenge, 但事先不发送 Compute IP Authentication - MIP-RRQ
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡返回状态为 SW1="9F", SW2="10" ——命令正常结束;</p> <p>b) 步骤 5) 后, CSIM 卡返回数据为基于输入数据的正确 MN-AAA 认证响应;</p> <p>c) 步骤 6) 后, CSIM 卡返回状态为 SW1="98", SW2="34" ——命令次序错误</p>
<p>说明: 这个命令的作用是为 Mobile IP 认证生成 MN-AAA 认证响应</p>

测试编号: 6.3.3.5
测试项目: 计算 IP 认证 (Compute IP Authentication)
分项目: 计算 IP 认证-高速分组数据 (HRPD) 接入认证功能
测试目的: 验证 Compute IP Authentication 能根据输入参数, 计算后给出正确的 HRPD Access 认证响应数据
预置条件: a) CSIM 卡连接到 ME 模拟器上; b) 参数: P1=04 (HRPD), ME 模拟器提供 1 字节长的 CHAP_ID, CHAP_Challenge=32 字节随机数
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 3) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=HRPD Access Authenticator, CHAP_ID 和 CHAP-Challenge; 4) ME 模拟器复位 CSIM 卡; 5) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 6) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 7) ME 模拟器向 CSIM 卡发送 Compute IP Authentication 命令, 参数是: P1=HRPD Access Authenticator, CHAP_ID 和 CHAP-Challenge; 8) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令
预期结果: a) 步骤 3) 后, CSIM 卡返回状态为 SW1="98", SW2="04" ——访问条件不满足; b) 步骤 7) 后, CSIM 卡返回状态为 SW1="9F", SW2="10" ——命令正常结束; c) 步骤 8) 后, CSIM 卡返回数据为基于输入数据的正确 HRPD 认证响应
说明: 这个命令的作用是为 Mobile IP 生成 HRPD 接入认证响应

6.3.4 广播/组播业务 (BCMCS) 相关命令

测试编号: 6.3.4.1
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: 取回 SK (Retrieve SK) (可选)
<p>测试目的:</p> <p>验证 ME 使用该命令来请求 CSIM 卡计算与特定的 BCMCS 流标识 (BCMCS_Flow_ID) 相关的 BCMCS 短期密钥 (SK)。该命令能满足下列要求:</p> <p>a) 如果 CSIM 卡从 Retrieve SK 命令中获得的 BCMCS_Flow_ID 和 BAK_ID 参数匹配 EF(BAKPARA) 或 EF(UpBAKPARA) 中存储的任何记录, 则 Retrieve SK 响应消息应返回计算后的业务密钥 SK;</p> <p>b) 如果 BCMCS_Flow_ID 和 BAK_ID 不与 EF(BAKPARA) 或 EF(UpBAKPARA) 中存储的任何记录相匹配, 则 CSIM 卡应返回错误状态字 '6A88', 表示 "没有找到引用的数据"</p>
<p>预置条件:</p> <p>a) CSIM 卡连接到 ME 模拟器上;</p> <p>b) CSIM 卡 EF(BAKPARA) 或 EF(UpBAKPARA) 中已存储对应于 BAK 的 BCMCS_Flow_ID, BAK_ID 参数</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 卡发送 Retrieve SK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID, BAK_ID 和 SK RAND, 其中 BCMCS_Flow_ID 和 BAK_ID 能够在 EF(BAKPARA) 或 EF(UpBAKPARA) 中找到匹配记录; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 命令; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 9) ME 模拟器向 CSIM 卡发送 RETRIEVE SK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID, BAK_ID 和 SK RAND, 其中 BCMCS_Flow_ID 和 BAK_ID 不与 EF(BAKPARA) 或 EF(UpBAKPARA) 中的任何记录相匹配
<p>预期结果:</p> <p>a) 步骤 4) 后, CSIM 卡应返回状态字 SW1= '9F'、SW2= '12';</p> <p>b) 步骤 5) 后, CSIM 卡应返回计算后得到的 SK;</p> <p>c) 步骤 9) 后, CSIM 卡应返回错误状态字 '6A88'</p>

测试编号: 6.3.4.2
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: 更新 BAK (Update BAK) (可选)
<p>测试目的:</p> <p>验证 CSIM 卡在收到 Update BAK 指令后, 能根据输入参数正确解密 BAK, 并将 BCMCS 流标识 (BCMCS_Flow_ID)、BAK_ID 和 BAK_Expire 等相关参数存储在 EFUpBAKPARA 中的一个条目下, 同时将解密的 BAK 进行隐秘存储</p>
<p>预置条件:</p> <p>CSIM 卡连接到 ME 模拟器上</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 Update BAK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID, BAK_ID, BAK_Expire, TK RAND, 加密后的 BAK
<p>预期结果:</p> <p>步骤 4) 后, CSIM 卡应根据 RK 和输入参数正确解密 BAK, 将解密的 BAK 进行隐秘存储, 并在 EF (UpBAKPARA) 中创建一个新的条目, 以存储相应的 BCMCS_Flow_ID、BAK_ID 和 BAK_Expire 参数。CSIM 卡返回状态字 SW1= '9F'、SW2= '00'</p>

测试编号: 6.3.4.3
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: 删除 BAK (Delete BAK) (可选)
<p>测试目的:</p> <p>该命令满足下列要求:</p> <p>a) 如果 CSIM 卡从 Delete BAK 命令中接收到的 BCMCS_Flow_ID 和 BAK_ID 参数匹配 EF(BAKPARA) 中存储的某一记录, 则 CSIM 卡应将 EF(BAKPARA) 中的相应记录 (BCMCS_Flow_ID、BAK_ID 和 BAK_Expire 参数对) 删除, 同时将 BAK 秘密列表中与该 BCMCS_Flow_ID 和 BAK_ID 参数对对应的 BAK 值删除或设置为 'FF.....FF';</p> <p>b) 如果 CSIM 卡从 Delete BAK 命令中接收到的 BCMCS_Flow_ID 和 BAK_ID 参数匹配 EF(UpBAKPARA) 中存储的任一记录, 则 CSIM 卡应将 EF(UpBAKPARA) 中对应记录, 以及更新后 BAK 秘密列表中该 BCMCS_Flow_ID 和 BAK_ID 参数对标记的 BAK 移除;</p> <p>c) 如果 CSIM 卡从 Delete BAK 命令中接收到的 BCMCS_Flow_ID 为无效值, 则 Delete BAK 响应消息应返回状态字 '9404';</p> <p>d) 如果 CSIM 卡从 Delete BAK 命令中接收到的 BAK ID 为无效值, 则 Delete BAK 响应消息应返回状态字 '9402'</p>
<p>预置条件:</p> <p>CSIM 卡连接到 ME 模拟器上</p>
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 卡发送 Delete BAK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID 和 BAK_ID, 该 ID 对与 EF(BAKPARA) 中某记录相匹配; 5) ME 模拟器复位 CSIM 卡; 6) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 7) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 8) ME 模拟器向 CSIM 卡发送 Delete BAK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID 和 BAK_ID, 该 ID 对与 EF(UpBAKPARA) 中某记录相匹配; 9) ME 模拟器复位 CSIM 卡; 10) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 11) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 12) ME 模拟器向 CSIM 卡发送 Delete BAK 命令, 参数为 Service Type= '01' (即 3GPP2 BCMCS), 无效 BCMCS_Flow_ID, BAK_ID; 13) ME 模拟器复位 CSIM 卡; 14) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令;

- 15) ME模拟器向CSIM卡发送SELECT命令, 选择ADF(CSIM);
- 16) ME模拟器向CSIM卡发送Delete BAK命令, 参数为Service Type= '01' (即3GPP2 BCMCS), BCMCS_Flow_ID, 无效BAK_ID

预期结果:

- a) 步骤 4) 后, CSIM 卡应删除 EF(BAKPARA)中的相应记录, 并删除隐秘存储的对应 BAK 或将它置为无效 ('FF.....FF')。CSIM 卡返回正常结束状态字 SW1= '9F'、SW2= '00';
- b) 步骤 8) 后, CSIM 卡应删除 EF(UpBAKPARA)中的相应记录, 并删除隐秘存储的对应 BAK 或将它置为无效 ('FF.....FF')。CSIM 卡返回正常结束状态字 SW1= '9F'、SW2= '00';
- c) 步骤 12) 后, CSIM 卡应返回状态字 '9404' ——无效 BCMCS_Flow_ID;
- d) 步骤 16) 后, CSIM 卡应返回状态字 '9402' ——无效 BAK_ID

测试说明: 本测试项中的第 1 个子测试可在正常执行了有相同 BCMCS_Flow_ID 和 BAK_ID 输入参数的“Update BAK”和“Retrieve SRTP SK”后进行;

第 2 个子测试可在正常执行了有相同 BCMCS_Flow_ID 和 BAK_ID 输入参数的“Update BAK”后进行;

第 4 个子测试可在正常执行了有相同 BCMCS_Flow_ID 和不同 BAK_ID 输入参数的“Update BAK”后进行

测试编号: 6.3.4.4
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: 取回 SRTP SK (RETRIEVE SRTP SK) (可选)
测试目的: 验证 RETRIEVE SRTP SK 响应消息能返回 BCMCS SRTP 短期密钥 (SK)
预置条件: CSIM 卡连接到 ME 模拟器上
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF (CSIM); 4) ME 模拟器向 CSIM 卡发送 RETRIEVE SRTP SK 命令, 参数 Service Type = '01' (即 3GPP2 BCMCS), BCMCS_Flow_ID, BAK_ID, SK_RAND, Packet Index。其中 BCMCS_Flow_ID 和 BAK_ID 能够在 EF (BAKPARA) 中找到匹配记录; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 指令; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 发送 SELECT 命令, 选择 ADF (CSIM); 9) ME 模拟器向 CSIM 发送 Retrieve SRTP SK 命令, 输入参数有 Service Type = '01' (即 3GPP2 BCMCS)、BCMCS_Flow_ID、BAK_ID 和 Packet Index。其中 BCMCS_Flow_ID 和 BAK_ID 能够在 EF (UpBAKPARA) 中找到匹配记录; 10) ME 模拟器向 CSIM 卡发送 GET RESPONSE 指令; 11) ME 模拟器复位 CSIM 卡; 12) ME 模拟器向 CSIM 发送 VERIFY PIN 命令; 13) ME 模拟器向 CSIM 发送 SELECT 命令, 选择 ADF (CSIM); 14) ME 模拟器向 CSIM 卡发送 Retrieve SRTP SK 命令, 输入参数为 Service Type = '01' (即 3GPP2 BCMCS)、BCMCS_Flow_ID、BAK_ID 和 Packet Index, 但其中的 BCMCS_Flow_ID 和 BAK_ID 不能与 EFBAKPARA 或 EFUpBAKPARA 中的任何记录相匹配
预期结果: a) 步骤 4) 后, CSIM 卡应正确计算 SRTP SK, 并返回正常结束状态字 SW1 = '9F'、SW2 = '12'; b) 步骤 5) 后, CSIM 卡应将 SK 结果返回给 ME 模拟器; c) 步骤 9) 后, CSIM 应首先将 BCMCS_Flow_ID 和 BAK_ID 所对应条目从 EF (UpBAKPARA) 复制到 EF (BAKPARA) 中, 再将其从 EF (UpBAKPARA) 中删除; 然后正确计算 SRTP SK; 最后返回正常结束状态字 SW1 = '9F'、SW2 = '12'; d) 步骤 10) 后, CSIM 卡将 SRTP SK 结果返回给 ME 模拟器; a) 步骤 14) 后, CSIM 卡应返回错误状态字 '6A88', 表示 “没有找到 BAK 密钥”

测试编号: 6.3.4.5
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: 生成鉴权标记 (Generate Authorization Signature) (可选)
测试目的: 验证 Generate Authorization Signature 响应消息能返回 Auth Signature
预置条件: CSIM 卡连接到 ME 模拟器上
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADF(CSIM); 4) ME 模拟器向 CSIM 发送 Generate Authorization Signature 命令, 输入参数有 Service Type= '01' (即 3GPP2 BCMCS)、BCMCS_Flow_ID、BAK_ID 和 Timestamp。其中的 BCMCS_Flow_ID 和 BAK_ID 能够在 EF(BAKPARA) 或 EF(UpBAKPARA) 中找到匹配记录; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 指令; 6) ME 模拟器复位 CSIM 卡; 7) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 8) ME 模拟器向 CSIM 发送 SELECT 命令, 选择 ADF(CSIM); 9) ME 模拟器向 CSIM 发送 Generate Authorization Signature 命令, 输入参数有 Service Type= '01' (即 3GPP2 BCMCS)、BCMCS_Flow_ID、BAK_ID 和 Timestamp。其中的 BCMCS_Flow_ID 和 BAK_ID 无法在 EF(BAKPARA) 和 EF(UpBAKPARA) 中找到匹配记录
预期结果: a) 步骤 4) 后, CSIM 卡应正确计算认证签名, 并返回正常结束状态字 SW1= '9F'、SW2= '06'; b) 步骤 5) 后, CSIM 卡应将签名结果返回给 ME 模拟器; c) 步骤 9) 后, CSIM 卡应返回错误状态字 '6A88', 表示“没有找到 BAK 密钥”

测试编号: 6.3.4.6
测试项目: 广播/组播业务 (BCMCS) 相关命令
分项目: BCMCS 认证 (BCMCS Authentication) (可选)
测试目的: 验证 BCMCS Authentication 响应消息能返回 BCMCS 摘要响应
预置条件: CSIM 卡连接到 ME 模拟器上
测试步骤: 1) ME 模拟器复位 CSIM 卡; 2) ME 模拟器向 CSIM 卡发送 VERIFY PIN 命令; 3) ME 模拟器向 CSIM 卡发送 SELECT 命令, 选择 ADFCSIM; 4) ME 模拟器向 CSIM 卡发送 BCMCS Authentication 命令, 参数有 Service Type= '01' (即 3GPP2 BCMCS)、RAND 和 Challenge; 5) ME 模拟器向 CSIM 卡发送 GET RESPONSE 指令
预期结果: a) 步骤 4) 后, CSIM 卡返回正常结束状态字 SW1= '9F'、SW2= '12'; b) 步骤 5) 后, CSIM 卡返回正确的 BCMCS 摘要响应

中华人民共和国
通信行业标准
CDMA 数字蜂窝移动通信网通用集成电路卡
(UICC) 与终端间接口测试方法
支持 CSIM 应用的 UICC

YD/T 2522-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码: 100061

宝隆元(北京)印刷技术有限公司印刷
版权所有 不得翻印

*

开本: 880×1230 1/16

2013 年 5 月第 1 版

印张: 2.25

2013 年 5 月北京第 1 次印刷

字数: 61 千字

15115·220

定价: 30 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922