电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0025-V1.0.0:2018

基于 TEE 的 eSIM 技术要求

Technical Requirements for eSIM Based on TEE

2018 - 09 - 03 发布　　2018 - 09 - 03 实施

电信终端产业协会　　发 布

目　　次

前　　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、中国电信移动终端管理中心、中国联合网络通信有限公司、上海果通通信科技股份有限公司、北京豆荚科技有限公司、上海瓶钵信息科技有限公司。

本标准主要起草人： 翟世俊、国炜、潘娟、王海兰、胡博、吴俊、冯希顺、利文浩

引　　言

随着物联网终端和可穿戴设备的快速发展，传统SIM卡无法满足终端设备小型化、轻薄化和远程管理的需求，适应更加复杂苛刻的外部环境，嵌入式SIM（eSIM）应运而生。搭载支持可信执行环境（TEE）处理器芯片的终端设备也越来越多，TEE提供了硬件芯片、操作系统、应用软件等多个层面的隔离和安全措施，能够为用户或终端的敏感数据与敏感操作提供一定程度的保护，TEE也可用于SIM数据的保护，基于TEE的eSIM方案符合部分物联网终端和可穿戴设备等应用场景的需求，将会被部分物联网模组厂商或终端厂商所采用。目前国内外尚没有制定基于TEE的eSIM的相关标准，因此有必要根据基于TEE的eSIM的技术需求，制定基于TEE的eSIM的技术要求，为国内该领域的卡产品实现提供技术参考，为相关产品的测评提供依据。

基于 TEE 的 eSIM 技术要求

1 范围

本标准规定了本标准规范了基于TEE的eSIM的技术要求，包括总体架构、功能要求、接口要求、安全要求等。

本标准适用于所有搭载TEE的设备，指导基于TEE的eSIM的安全设计、开发、生产和评估等。

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 2844.1-2015 移动终端可信环境技术要求 第1部分：总体

YD/T 2844.2-2015 移动终端可信环境技术要求 第2部分：可信执行环境

YD/T 2844.3-2015 移动终端可信环境技术要求 第3部分：安全存储

YD/T 2844.4-2015 移动终端可信环境技术要求 第4部分：操作系统的安全保护

YD/T 2844.5-2016 移动终端可信环境技术要求 第5部分：与输入输出设备的安全交互

YD/T 2845-2015 嵌入式通用集成电路卡（eUICC）及其远程管理的安全技术要求（第一阶段）

YD/T 3198-2016 支持远程管理的嵌入式通用集成电路卡(eUICC)技术要求(第一阶段)

ISO/IEC 7816-3:2006 Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols

GSMA：SGP.02-Remote Provisioning Architecture for Embedded UICC Technical Specification

GSMA：SGP.22-Remote SIM Provisioning Technical Specification

SIMalliance：eUICC Profile Package: Interoperable Format Technical Specification

3 术语、定义和缩略语

3.1 术语和定义

《YD/T 2844.1-2015 移动终端可信环境技术要求 第1部分：总体》中界定的以及下列术语、定义和缩略语适用于本文件。

3.1.1 嵌入式 SIM 卡 Embedded SIM

通过物理方式集成到终端中，不能随便拔出和替换的SIM卡。

3.1.2 profile

配置在或出现在eSIM上的文件结构、数据和应用程序的集合。

3.1.3 嵌入式 UICC Embedded UICC

嵌入式eUICC即嵌入式通用集成电路卡，能够支持安全的远程/本地Profile配置管理。

3.1.4 远程管理平台

远程管理平台主要有两部分功能：准备激活和配置profile，并在eSIM上进行安全配置；安全地执行eSIM上直接管理激活和配置profile。

3.2 缩略语

下列缩略语适用于本文件。

CA	Client Application	客户端应用
ECASD	eUICC Controlling Authority Security Domain	eUICC控制授权安全域
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
LPA	Local Profile Assistant	本地Profile助理
MNO	Mobile Network Operator	移动网络运营商
REE	Rich Execution Environment	普通执行环境
RSP	Remote Sim Provisioning	远程SIM卡数据配置
SM-DP	SubscriptionManager-Data Preparation	用户签约数据管理—数据准备
SM-DS	Subscription Manager-Discovery Server	用户签约数据管理—发现服务器
TA	Trusted Application	可信应用
TEE	Trust Execution Environment	可信执行环境

4 基于 TEE 的 eSIM 的总体架构

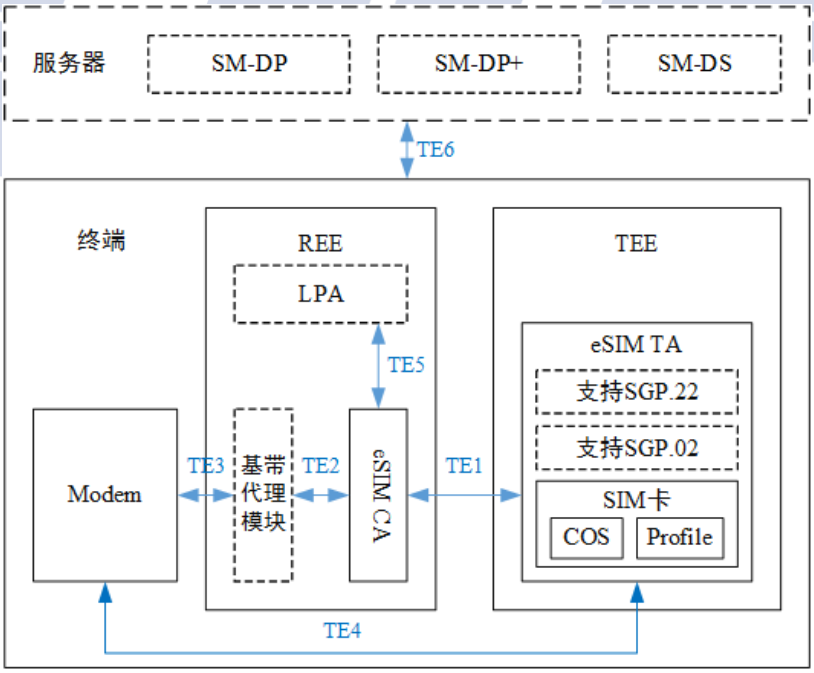

图1 基于TEE的eSIM的总体架构

基于TEE的eSIM的总体架构如图1所示，主要包括eSIM TA和eSIM CA两部分。

- eSIM TA工作在终端TEE环境下，实现SIM卡的功能，主要包括密钥生成与存储、证书的存储与验证、加密Profile的解密、eSIM应用中的密钥存储与管理、网络鉴权数据的计算等工作。
- eSIM CA工作在终端的REE环境下，主要负责与Modem交互，实现eSIM功能的开关，以及Modem指令的转发。如果eSIM CA不存在，modem应直接将指令发送给eSIM TA。
- 基带代理模块为TEE eSIM方案中的可选组件，用于Modem指令转发和Modem的访问，获得系统卡槽信息；
- LPA为TEE eSIM方案中的可选组件，其功能参考GSMA SGP.22规范的相关要求。

5 基于 TEE 的 eSIM 功能要求

5.1 eSIM TA 功能要求

5.1.1 eSIM TA 基本功能要求

eSIM TA主要用于模拟SIM、UIM、USIM和CSIM卡功能，eSIM TA应至少具备以下功能：

(1) 网络鉴权算法的实现，满足3GPP TS31.102等标准规范要求；
(2) 网络鉴权密钥的加密存储与计算；
(3) 网络鉴权的核心参数加密存储与计算；
(4) 规范所定义的标准文件的加密存储与读写；
(5) 智能卡标准安全机制和访问控制机制的实现；
(6) 接口要求满足ISO/IEC 7816。

5.1.2 支持 GSMA SGP.02 规范的 eSIM TA 功能要求

支持GSMA SGP.02规范的eSIM TA还应具备以下功能：

(1) 根据GSMA规范实现ISD-R功能；
(2) ECASD功能的实现；
(3) CI公钥的存储；
(4) eUICC证书的存储和管理；
(5) 安全通道的建立和维护；
(6) Profile的格式应遵循SIMalliance规范，Profile的解密和解析功能的实现；
(7) 在下载并安装了Profile之后，eSIM TA还需要根据Profile的配置模拟实现SIM、UIM、USIM和CSIM卡，并根据本文5.1.1节的要求实现卡所需要的所有功能。

5.1.3 支持 GSMA SGP.22 规范的 eSIM TA 功能要求

支持GSMA SGP.22规范的eSIM TA还应具备以下功能：

(1) 根据GSMA规范实现ISD-R功能；
(2) ECASD功能的实现；
(3) CI根证书的存储；
(4) EUM及eUICC证书的存储和管理；
(5) 安全通道的建立和维护；
(6) Profile的格式应遵循SIMalliance规范，Profile的解密和解析功能的实现；
(7) Profile规则管理功能；
(8) 在下载并安装了Profile之后，eSIM TA还需要根据Profile的配置模拟实现SIM、UIM、USIM和

CSIM卡，并根据本文5.1.1节的要求实现卡所需要的所有功能。

5.2 eSIM CA 功能要求

eSIM CA不承载任何与安全有关的功能，所有安全相关的指令必须转发给eSIM TA进行处理。eSIM CA应具备以下功能：

(1) eSIM CA执行modem指令转发功能。eSIM CA接收从基带代理模块转发的Modem的APDU指令，将其转发给eSIM TA进行处理，并把eSIM TA的处理结果发回给Modem，完成指令转发的功能。在处理大数据量的APDU时，为了避免eSIM TA的调用过于频繁，eSIM CA可以缓存部分非敏感数据以便加快对Modem的响应速度。

(2) eSIM CA执行LPA指令转发功能。将LPA发送的指令转发给eSIM TA进行处理，并把eSIM TA的处理结果发回给LPA，完成指令转发功能。

(3) TEE eSIM功能开关，eSIM CA接收从系统发送过来的开关指令并执行，完成eSIM功能的打开或关闭。

5.3 基带代理模块功能要求

具备基带代理模块的终端应具备以下功能：

(1) Modem指令转发功能；

(2) 访问Modem，获得系统卡槽信息；

(3) 注册虚卡，接收Modem指令，并通过eSIM CA发给eSIM TA。

5.4 LPA 功能要求

LPA是TEE eSIM方案中的可选组件，当TEE eSIM模拟实现eUICC芯片并实现GSMA规范SGP.22所定义的功能时应具备该组件。LPA的功能需完全遵循GSMA规范SGP.22的要求，实现LDS、LPD，LUI的所有功能。

LPA在终端内部，运行于REE中，与终端外部SM-DP+、证书和EID颁发实体通过相应接口连接。

终端LPA在应具备如下功能：

(1) eSIM的初始化

申请EID，并协助eSIM TA申请eSIM证书。

(2) Profile的下载

获取eSIM TA信息，并与eSIM TA协作从eSIM管理平台下载Profile密文，并下传到eSIM TA。

(3) 为业务受理App提供Profile管理的访问接口

接收终端用户通过业务受理App发出关于Profile的管理指令。

(4) Profile的激活

对eSIM TA中已安装的Profile发出激活指令。

(5) Profile的去激活

对eSIM TA中已安装的Profile发出去激活指令。

(6) Profile的删除

对eSIM TA中已安装的Profile发出删除指令。

(7) 提供Profile信息

向业务受理App提供Profile的相关信息。

5.5 支持 RSP 的 eSIM 标识和证书管理

5.5.1 支持 RSP 的 TEE eSIM 标识管理

TEE eSIM 标识分配与管理应符合相关行业标准的要求。

5.5.2 支持 RSP 的 TEE eSIM 证书管理要求

TEE eSIM证书分配与管理应由具有相应资质的证书发行机构发行。证书分配与管理可根据需求采用出厂预置或空中发行方案。

(1) 对于采用出厂预置TEE eSIM证书的方案，eSIM相关证书应在设备出厂前完成预置，按照相关标准对证书进行相应的存储和管理。

(2) 对于采用空中发行TEE eSIM证书的方案，在发行前应在线验证TEE终端的合法性和eSIM TA的合法性。TEE eSIM应使用TEE本身的根密钥对证书的申请信息进行加密及签名，同时服务器下发的证书也必须采用TEE的根密钥进行签名保护。

5.6 TEE eSIM 相关业务流程要求

5.6.1 SIM 卡基本业务流程要求

5.6.1.1 Modem 通过 eSIM CA 与 eSIM TA 交互流程

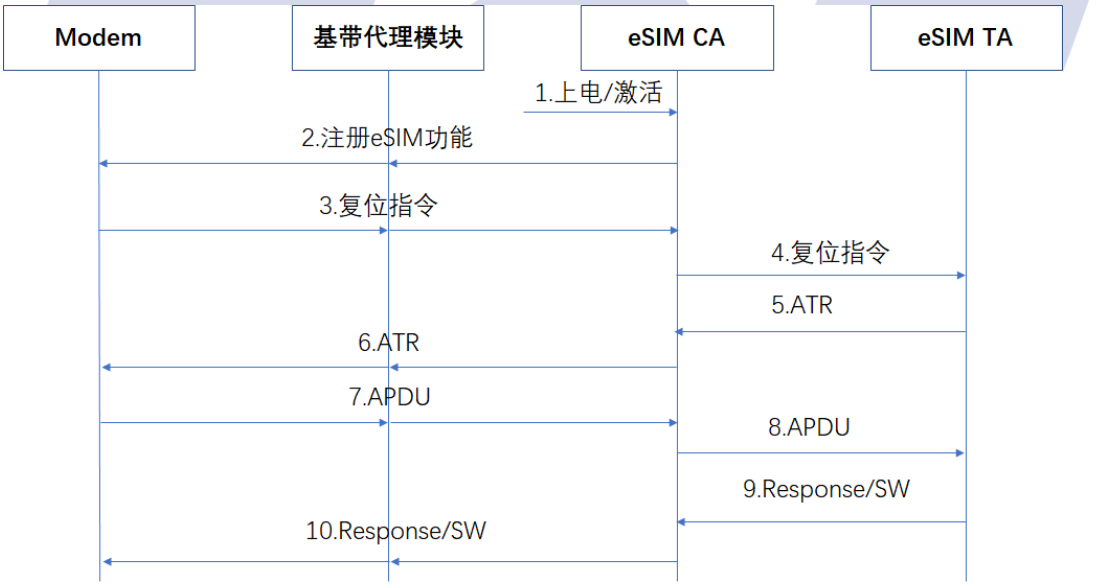

图2 Modem通过eSIM CA与eSIM TA交互流程

(1) 用户选择打开eSIM服务，应用程序发送“启动eSIM”指令给eSIM CA；

(2) eSIM CA调用基带代理模块接口，向Modem芯片发送注册eSIM功能指令；

(3) Modem接收到注册eSIM指令，向eSIM程序发送复位指令，基带代理模块将复位指令转发给eSIM CA；

(4) eSIM CA接收到复位指令，转发给eSIM TA进行处理；

(5) eSIM TA返回复位响应（ATR）；

(6) eSIM CA调用基带代理模块接口，向Modem芯片发送复位响应；

(7) Modem芯片根据SIM卡处理流程，向eSIM程序发送APDU，APDU经由基带代理模块转发给eSIM CA；

(8) eSIM CA将APDU转发给eSIM TA进行处理；

(9) eSIM TA返回APDU响应内容及状态字（Status Word）；

(10) eSIM CA调用基带代理模块接口，将响应内容及状态字发送给Modem芯片。

5.6.1.2 Modem 直接与 eSIM TA 交互流程

图3 Modem直接与eSIM TA交互流程

参照5.6.1.1，本流程示意Modem芯片如何与eSIM TA交换内容

(1) Modem向eSIM TA发送复位指令；

(2) eSIM TA返回复位响应（ATR）；

(3) Modem芯片根据SIM卡处理流程，向eSIM TA发送APDU；

(4) eSIM TA返回APDU响应内容及状态字（Status Word）。

5.6.2 支持 SGP.02 规范的相关业务流程要求

5.6.2.1 开启 HTTPS 通道及双向认证的流程

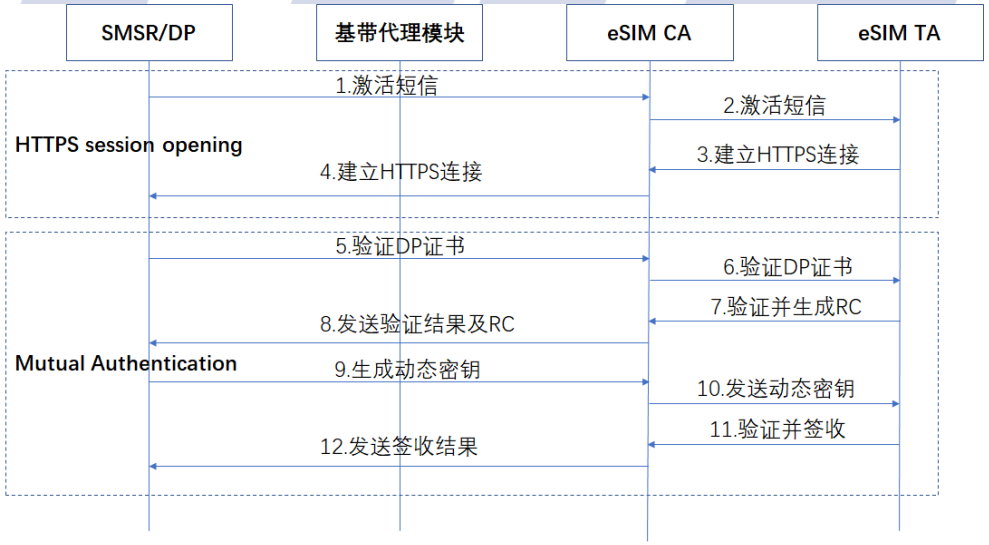

图4 开启HTTPS通道及双向认证的流程

(1) SMSR系统向用户设备发送激活短信，Modem收到短信后，以APDU形式将短信转发给eSIM CA进行处理；

(2) eSIM CA将激活短信（APDU形式）转发给eSIM TA进行处理；

(3) eSIM TA根据短信内容，请求建立HTTPs连接；

(4) eSIM CA调用OS接口，向指定DP服务器建立HTTPs连接；

(5) SMDP服务器通过HTTP发送DP证书给eSIM CA；
(6) eSIM CA将DP证书转发给eSIM TA进行验证；
(7) eSIM TA验证DP证书，并生成随机挑战码（Random Challenge）；
(8) eSIM CA向DP服务器返回验证结果及随机挑战码；
(9) SMDP生成用于协商加密密钥的公钥（ePK），并对此进行签名；
(10)eSIM CA向eSIM TA转发用于协商密钥的的公钥；
(11)eSIM TA验证签名正确性，并生成协商密钥，eSIM TA向SMDP发送签收结果
(12)eSIM CA向SMDP发送签收结果。

5.6.2.2 创建 ISD-P 的流程

开启HTTPS流程参见5.6.2.1节

(1) SMDP服务器向eSIM发送创建ISD-P指令；
(2) eSIM CA向eSIM TA转发创建ISD-P指令；
(3) eSIM TA发送响应；
(4) eSIM CA向SMDP服务器发送响应。

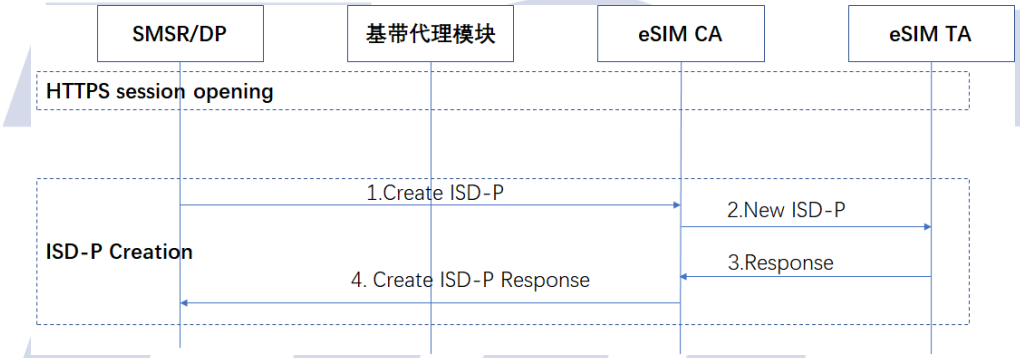

图5 创建ISD-P的流程

5.6.2.3 下载安装 Profile 的流程

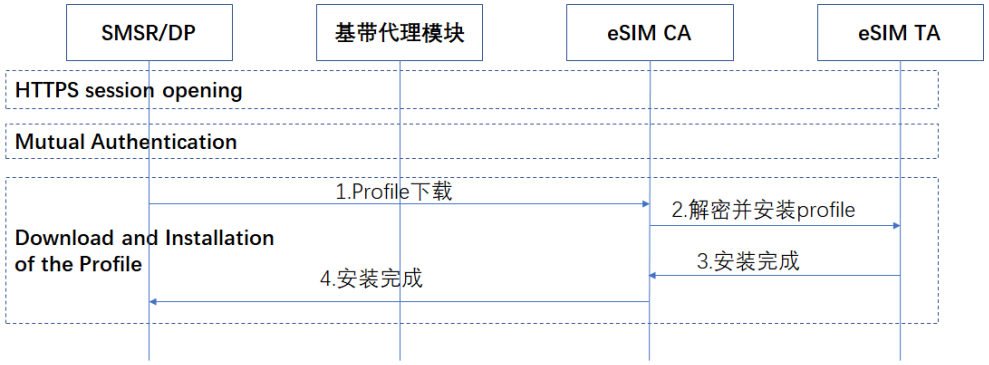

图6 下载安装Profile的流程

开启HTTPS及双向鉴权流程参见5.6.2.1节，

(1) SMDP服务器向eSIM发送Profile下载指令；
(2) eSIM CA向eSIM转发Profile下载指令，eSIM TA进行解密并安装Profile；

(3) eSIM TA返回Profile安装结果；

(4) eSIM CA向SMDP服务器返回安装结果。

5.6.3 支持 SGP .22 规范的相关业务流程要求

5.6.3.1. 支持 SGP.22 规范的 eSIM TA 初始化流程

eSIM TA通过初始化过程配置成为完整的eUICC功能：

(1) LPA向eSIM TA发起认证请求；

(2) eSIM TA生成认证信息；

(3) 向初始化服务器发起认证申请；

(4) eSIM TA对服务器进行认证；

(5) 向初始化服务器申请初始化数据；

(6) 执行初始化命令；

(7) 通知LPA初始化完成。

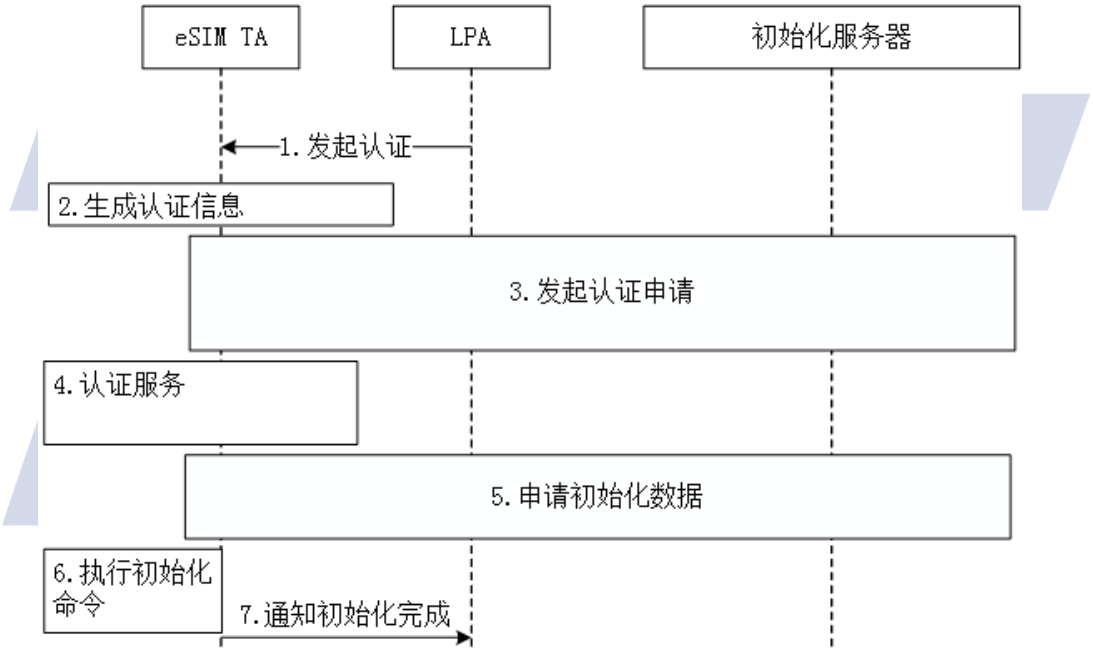

图7 支持SGP.22规范的eSIM卡初始化流程

5.6.3.2. 支持 SGP.22 规范的 eSIM 卡下载流程

支持SGP.22规范的eSIM卡下载流程如下：

(1) 用户通过APP选择下载eSIM电子卡，APP发送下载指令给LPA；

(2) LPA向eSIM TA发送获取eUICCinfo指令；

(3) eSIM TA返回eUICCinfo；

(4) LPA向eSIM TA发送获取eUICC挑战码指令；

(5) eSIM TA生成挑战码；

(6) eSIM TA返回挑战码；

(7) LPA向SM-DP+服务器发起初始认证请求；

(8) SM-DP+服务器返回服务器认证结果；

(9) LPA向eSIM TA发送服务器认证；
(10) eSIM TA认证服务器签名，并计算eUICC签名；
(11) eSIM TA返回eUICC签名；
(12) LPA向SM-DP+服务器发送客户端认证请求；
(13) SM-DP+服务器返回客户端认证结果；
(14) LPA向eSIM TA发送下载准备指令；
(15) eSIM TA返回下载准备公钥；
(16) LPA向SM-DP+服务器获取Profile包；
(17) SM-DP+服务器返回Porfile包；
(18) LPA向eSIM TA发送Profile下载安装指令，eSIM TA返回profile安装结果；
(19) LPA向SM-DP+服务器返回profile安装结果；
(20) SM-DP+服务器确认profile开通；
(21) LPA通知用户APP eSIM电子卡已下载。

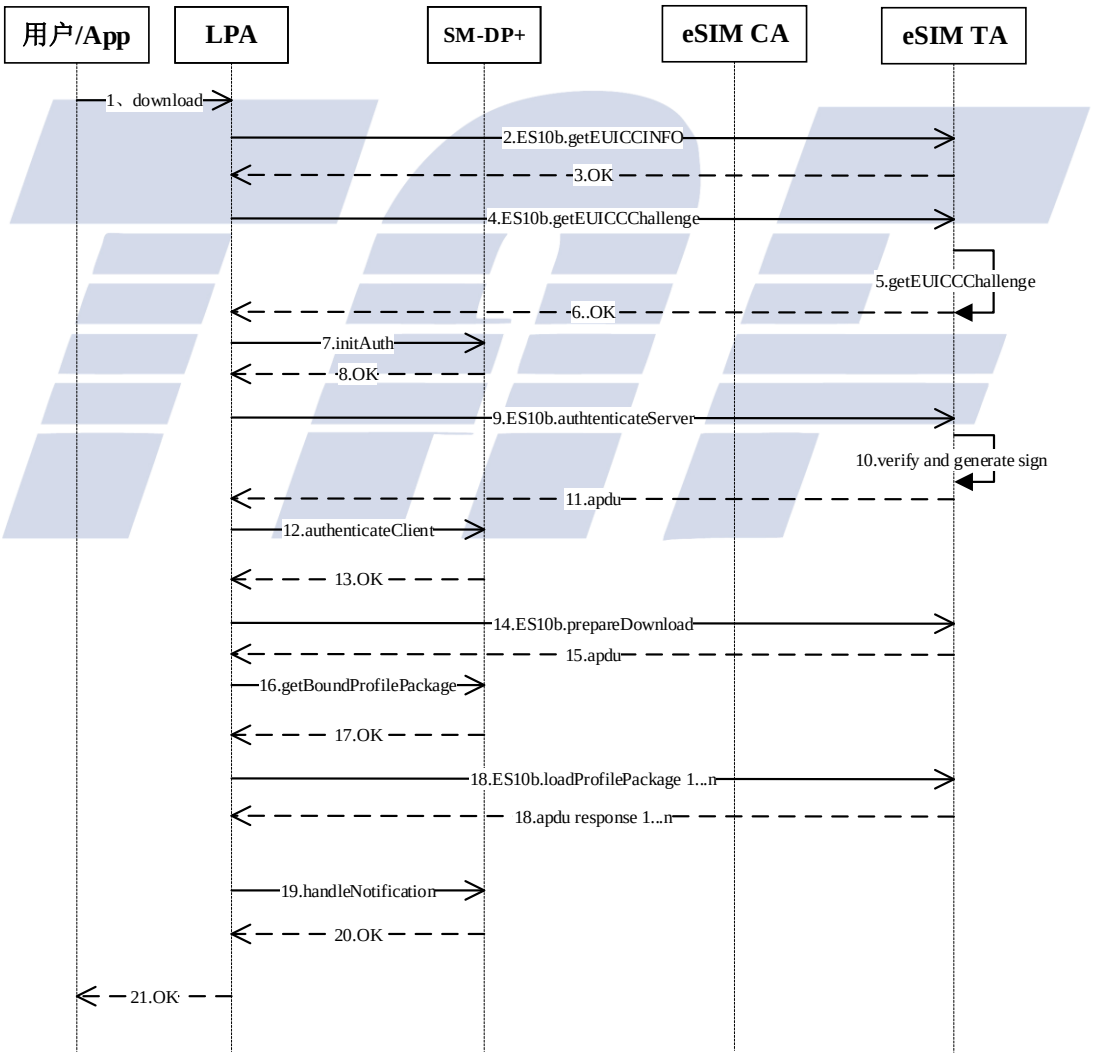

图8 支持SGP.22规范的eSIM卡下载流程

5.6.3.3. 支持 SGP.22 规范的 eSIM 卡工作流程

SIM卡工作流程说明可参考5.6.1.1节。

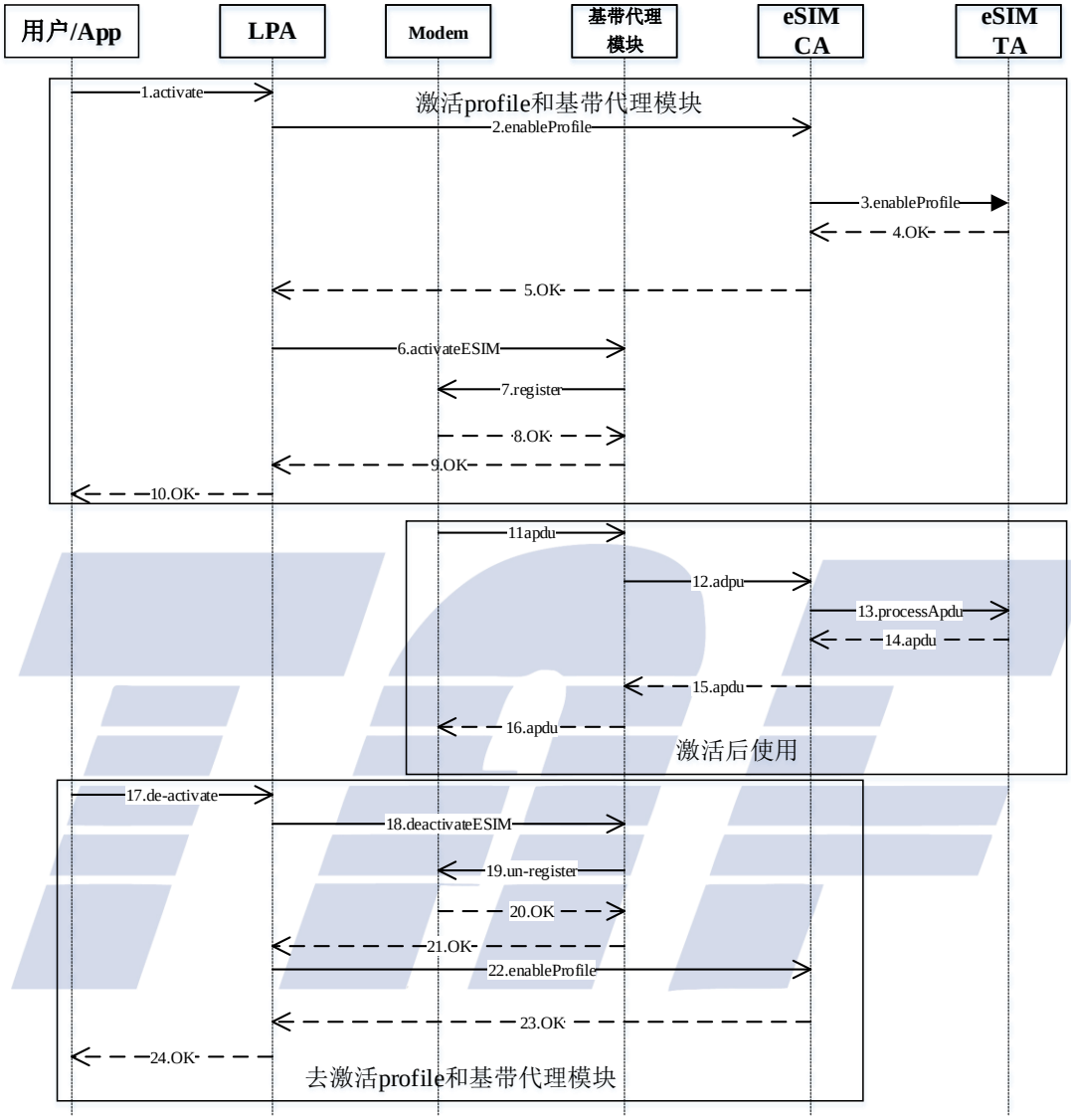

图9 支持SGP.22规范的eSIM卡工作流程

6 基于 TEE 的 eSIM 接口要求

6.1 eSIM TA 向 eSIM CA 提供的接口 TE1

TE1接口包括eSIM TA实现部分和TEE实现部分。其中eSIM TA须实现APDU相关接口，TEE部分需实现算法相关接口。

6.1.1 APDU 指令处理

本节中各函数的业务逻辑由 eSIM TA 实现，处理包括 ISO-7816 定义的相关指令。支持 RSP 的 eSIM

TA 须实现 ES10+、ES8+相关业务处理逻辑。

uint32_t apdu_process_entry(uint8_t * input, uint32_t input_len, uint8_t * output, uint32_t * output_len)

参数	类型	说明
input	uint8_t *	输入：APDU 指令信息
input_len	uint32_t	输入长度
output	uint8_t *	输出：APDU 响应信息
output_len	uint32_t *	输出长度

6.1.2 Reset 指令处理

uint32_t esim_reset_entry(uint8_t * output, uint32_t * output_len)

参数	类型	说明
output	uint8_t *	输出：ATR
output_len	uint32_t *	输出长度

6.1.3 通用指令处理

uint32_t command_process_entry (uint32_t cmdId,uint8_t* input, uint32_t input_len,uint8_t* output, uint32_t * output_len)

指令ID	参数	类型	说明	返回值
0x00000001 激活eSIM TA	cmdId	uint32_t	指令ID：0x00000001	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：TAversion、algorithm、signature	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t *	输出长度	
0x00000002 禁用eSIM TA	cmdId	uint32_t	指令ID：0x00000002	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：TAversion、algorithm、signature	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t *	输出长度	
0x00000003 恢复出厂设置	cmdId	uint32_t	指令ID：0x00000003	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：TAversion、algorithm、signature	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t *	输出长度	
	input	uint8_t*	输入：TAversion、EUICCcertId、algorithm、signature	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t *	输出长度	

6.2 eSIM CA 与基带代理模块接口要求 TE2

6.2.1 eSIM CA 向基带代理模块的提供的接口

eSIM CA向基带代理模块的提供的接口主要是APDU指令处理和执行Reset指令，具体要求参考6.1.1节和6.1.2节。

6.2.2 基带代理模块向 eSIM CA 的提供的接口

uint32_t processCommand(uint32_t cmdId,uint8_t* input, uint32_t input_len,uint8_t* output, uint32_t * output_len)

指令ID	参数	类型	说明	返回值
0x10000001 激活通道	cmdId	uint32_t	指令ID：0x10000001	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t*	输出长度	
0x10000002 关闭通道	cmdId	uint32_t	指令ID：0x10000002	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t*	输出长度	
0x10000003 激活eSIM	cmdId	uint32_t	指令ID：0x10000003	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t*	输出长度	
0x10000004 禁用eSIM	cmdId	uint32_t	指令ID：0x10000004	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t*	输出长度	
0x10000005 获得基带模块能力	cmdId	uint32_t	指令ID：0x10000005	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：基带模块信息	
	output_len	uint32_t*	输出长度	
0x10000006 配置基带代理模块	cmdId	uint32_t	指令ID：0x10000006	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version、config	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：空	
	output_len	uint32_t*	输出长度	
0x10000007 注册eSIM CA	cmdId	uint32_t	指令ID：0x10000007	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version	

	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：version、标识信息	
	output_len	uint32_t*	输出长度	
0x10000008 注销eSIM CA	cmdId	uint32_t	指令ID：0x10000008	0x00000000：处理成功 0x00000001：处理失败
	input	uint8_t*	输入：version、标识信息	
	input_len	uint32_t	输入长度	
	output	uint8_t*	输出：版本	
	output_len	uint32_t*	输出长度	

6.3 基带代理模块与 Modem 接口要求 TE3

Modem提供注册、启用或禁用eSIM功能，获取SIM卡槽参数信息。

6.4 eSIM TA 与 Modem 接口要求 TE4

eSIM TA与Modem接口主要是APDU指令处理和执行Reset指令，具体要求参考6.1.1节和6.1.2节。

6.5 eSIM CA 与 LPA 接口要求 TE5

eSIM CA与LPA接口TE5应实现GSMA SGP.22规范中的ES10+接口，该接口连接终端内部LPA与TEE中的eSIM TA，实现了包括调取相关信息进行eSIM TA初始化，以及Profile的相关管理等功能，具体参见GSMA SGP.22规范中的第5.7小节所述。

6.6 LPA 与远程管理平台接口要求 TE6

该接口连接终端内部LPA与eSIM管理平台，实现RSP规范中定义的ES9+接口功能，具体参见GSMA SGP.22规范中的第5.6小节所述。

与eSIM TA初始化相关的接口不在本规范范围内。

7 基于 TEE 的 eSIM 安全要求

7.1 TEE 安全要求

7.1.1 启动安全

安全启动从最初的可信代码开始，在执行其它的安全启动代码前应验证这些代码的可靠性和完整性，通过签名校验的方法来保证信任链的传递。且在TEE启动过程中，要确保启动镜像与数据加载的完整性。如果代码更新镜像安装失败，则代码更新必须恢复到安装之前的版本；如果验证启动代码的完整性失败，则整个启动过程应终止。

7.1.2 存储安全

可信执行环境应能提供安全存储功能，保证数据存储在安全存储器中，或对所存储的数据进行加密存储，且对存储的数据有访问控制机制；

安全存储应保证所存储的数据具有机密性、可用性、一致性和原子性；

当数据为加密存储时，存储密钥应由根密钥派生，且仅仅由密钥管理者访问和处理，同时要保证密钥的机密性和完整性。

7.1.3 随机数

TEE内随机数的产生应结合硬件机制，并保证随机数的随机性和熵。

7.1.4 安全隔离

TEE代码、数据和密钥不应被TA访问，除非这种访问是被访问控制策略所授权。
TEE代码、数据和密钥不应被CA访问，除非这种访问是被访问控制策略所授权。

7.1.5 设备绑定

通过信任根进行设备绑定，确保数据与代码无法被克隆使用。

7.2 eSIM TA 安全要求

eSIM TA实现了SIM卡的功能，包括密钥生成与存储、证书的存储与验证、加密Profile的解密、eSIM应用中的密钥存储与管理、网络鉴权数据的计算等工作。

7.2.1 数据与代码完整性

eSIM TA在加载数据与代码时需要进行校验，确保加载代码与数据的完整性。

7.2.2 环境隔离性

eSIM TA的内存、数据需要与REE、其他TA间实现隔离，防止eSIM TA的数据被非法访问与篡改。

7.2.3 访问控制

eSIM TA应能识别客户端应用标识，包括来自eSIM CA的请求与来自其他TA的请求，并对访问者进行验证（如采用签名认证）。访问规则导入移动终端的过程应是安全可信的，例如可以在终端生产时导入，或者通过安全可信的通道由可信后台系统下发。

7.2.4 存储安全

eSIM TA存储的数据应确保完整性和隐私性，不可被其它非法实体访问或篡改。证书、密钥等安全数据需要加密存储在RPMB区域或者SE中。

7.2.5 数据处理安全

加解密工作、数据校验、鉴权等应在完全隔离的内存中进行，避免在共享内存等可被其他实体访问的内存中进行。

7.2.6 运行时安全

通过对TEE、密钥、配置数据等的保护策略保证TEE自身运行时的安全性，为运行在其中的应用提供可信的执行环境。

7.2.7 密钥服务强度

eSIM TA所采用的摘要算法、对称密码算法、非对称密码算法和签名算法应符合相关国家或行业标准的要求。

7.3 eSIM CA 及 LPA 安全要求

7.3.1 访问控制

eSIM CA和LPA应能识别客户端应用标识和来自其他应用的请求，对访问者进行验证，应只接受通过认证的对象的访问。同时应对敏感数据进行访问权限控制。

7.3.2 数据安全保护

应加密存储敏感数据，敏感数据存储路径应设置严格的访问控制机制，避免数据泄露。用于加密的密钥应妥善保存，避免被直接反编译获取。

应禁止日志数据包含与用户数据或与程序调试相关的数据。

7.3.3 反逆向保护

应对eSIM CA、LPA代码采取代码混淆、加壳等防护措施，实现eSIM CA和LPA反编译保护。

应对应用的链接库、资源文件、配置文件、本地敏感文件等数据进行加密，防止被窃取、篡改。

7.3.4 反盗版保护

应采取自我签名比对或第三方证书校验方式，防止eSIM CA和LPA被重打包。

应对eSIM CA和LPA完整性进行校验，防止eSIM CA和LPA程序的代码、图片、配置、布局等被增加、修改或删除。

7.3.5 反调试保护

应采取一定机制，防止运行时的内存数据、存储信息被获取。

应具有反动态调试的能力。

应采取地址空间随机化等机制，防止运行时数据或代码被修改并执行，防止被注入恶意代码。

7.3.6 防篡改攻击

应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。

7.3.7 防重放攻击

应采取时间戳、消息序号，以及问答响应机制等措施，以防御重放攻击。

7.3.8 防数据信息泄漏

应支持TLS等安全协议，对传输中的敏感数据进行加密处理，保护数据传输的机密性。

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容
2018.3	V1.0.0	报批稿

参 考 文 献