ICS 33.050
CCS M 30

团　体　标　准

T/TAF 096-2021

服务提供方可信服务管理技术要求

Technical requirements for service provider trusted service management

2021-08-17 发布　　2021-08-17 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：蚂蚁科技集团股份有限公司、中国信息通信研究院、阿里巴巴（中国）有限公司、OPPO广东移动通信有限公司、高通无线通信技术（中国）有限公司、华为技术有限公司、小米通讯技术有限公司、联想（北京）有限公司、郑州信大捷安信息技术股份有限公司、南昌黑鲨科技有限公司。

本文件主要起草人：林冠辰、杜云、孙元博、赵生波、彭晋、昌文婷、宁华、李根、杨明慧、王江胜、王思善、黄天宁、王乐、张倞诚、任冠一、李汝鑫、刘献伦、刘为华、汪国平、傅山、王嘉义。

服务提供方可信服务管理技术要求

1 范围

本文件规定了面向服务提供方可信服务管理安全技术要求，包括技术参考架构、功能要求、技术要求、安全要求等。

本文件适用于服务提供方可信服务管理平台发起的辅助安全域的生命周期管理操作，包括创建、锁定、解锁、删除等。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信服务管理 trusted service management

由可信管理者提供的载体生命周期管理、应用生命周期管理和应用管理等服务。

3.2

服务提供方可信服务管理 service provider-trusted service management

服务提供方TSM，为用户提供服务，管理安全应用及个人化数据。

3.3

辅助安全域 supplementary security domain

由ISD创建及分配权限，为发行方之外的操作者提供的安全域。

3.4

应用协议数据单元 application protocol data unit

SE芯片可执行指令的信息单元。

3.5

委托管理安全域 delegated management security domain

委托管理SD，使用该SD进行安全应用管理时需要向SEI-TSM申请授权Token，由具有token验证权限的SD验证之后才能完成操作。

3.6

授权管理安全域 authenticated management security domain

授权管理SD有自主管理安全应用的权限，业务生命周期管理时不需要向SEI-TSM申请Token。

3.7

主安全域 issuer security domain

负责对SE管理者的管理、安全、通信需求进行支持的SE上首要实体，也称发行方安全域。

3.8

安全单元发卡方可信服务管理 secure entity issuer－trusted service management

管理安全单元及其内容。

4 缩略语

下列缩略语适用于本文件。

AMSD：授权管理安全域（Authorized Management Security Domain）
APDU：应用协议数据单元（Application Protocol Data Unit）
DMSD：委托管理安全域（Delegated Management Security Domain）
ISD：主安全域（Issuer Security Domain）
SE：安全单元（Secure Element）
SEI-TSM：安全单元发卡方可信服务管理（Secure Element Issuer－Trusted Service Management）
SP-TSM：服务提供方可信服务管理（Service Provider-Trusted Service Management）
SSD：辅助安全域（Supplementary Security Domain）
TSM：可信服务管理 （Trusted Service Management）
TLCP：传输层密码协议（Transport Layer Cryptography Protocol）
TLS：传输层安全协议（Transport Layer Security）

5 技术参考架构

服务提供方可信服务管理(SP-TSM)为自有应用提供个人化的可信服务管理，技术参考架构示意图如图1所示。SP-TSM分别和SEI-TSM、终端设备建立安全通道，管理辅助安全域、管理应用提供方、应用生命周期管理等。

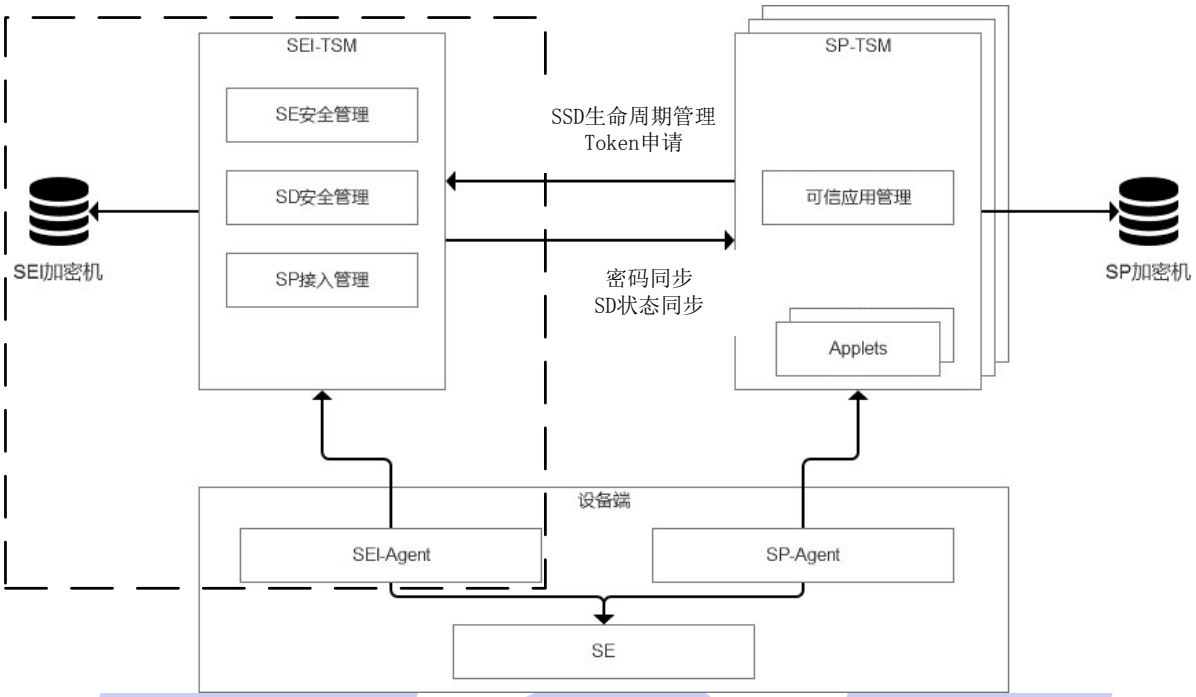

图1　技术参考架构示意图

注：虚线部分SEI-TSM不在本文件范围。

6　功能要求

6.1　SP-TSM 功能要求

6.1.1　概述

SP-TSM应具备辅助安全域生命周期管理，密钥安全管理，个人化设置，应用的安全下载、安装、锁定、解锁和删除等生命周期管理。

6.1.2　SSD 管理

应具备创建申请、锁定、解锁、删除属于自有应用的辅助安全域(SSD)。应具备辅助安全域的密钥更新功能。

6.1.3　SSD 密钥安全管理

应具备密钥产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期安全管理功能。应具备更新自有辅助安全域密钥体系的能力。

6.1.4　可信应用管理服务

应支持对智能终端（智能手机、可穿戴设备等）提供个人化的可信服应用委托管理服务、授权管理服务。应具备应用生命周期管理，包括业务应用的数据准备，应用的下载、安装、锁定、解锁、删除等。

6.1.5　安全通道

按照GP定义的相关协议规范，建立和自有辅助安全域的安全通信通道。

6.1.6 证书管理

应具备SSD中证书签发、证书吊销、证书更新、证书查询等功能。

6.2 SP-TSM 服务流程

6.2.1 SSD 管理流程

SSD可通过线上、线下等多种方式创建。当创建请求由SP-TSM向SEI-TSM申请时，其流程图如图2所示。终端/SP-Agent/SE发起可信服务下载时，判断辅助安全域是否存在。若不存在，SP-TSM向SEI-TSM发送创建SSD请求。SEI-TSM返回创建SSD响应，授权SE中的发行方安全域创建辅助安全域。

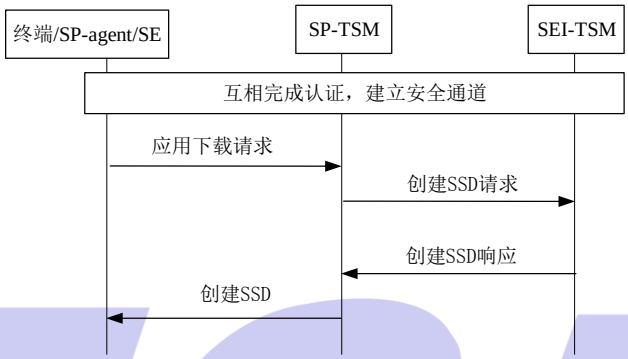

图2 SSD 创建流程图示例

根据服务运行状态或终端SE的情况，SP-TSM可向SEI-TSM发送SSD管理请求，如锁定/解锁/删除SSD请求。根据SSD管理请求，SEI-TSM返回相应的管理响应，如锁定/解锁/删除SSD响应。SP-TSM将管理响应转发给SE，授权SE中的主控制域完成辅助安全域的相关操作。

6.2.2 SSD 密钥更新流程

SSD密钥协商有多种实现方式，比如SP按约定的规则基于根密钥生成初始密钥并进行替换，或SP主动调SEI-TSM的接口去获取密钥。当密钥由SEI-TSM分配时，SEI-TSM可发送初始密钥同步请求，将分配的SSD密钥发送给SP-TSM。SP-TSM返回密钥同步响应，之后进行SSD密钥更新，并将更新的SSD密钥推送给SE，进行个人化安全配置。SSD密钥更新流程示例如图3所示。

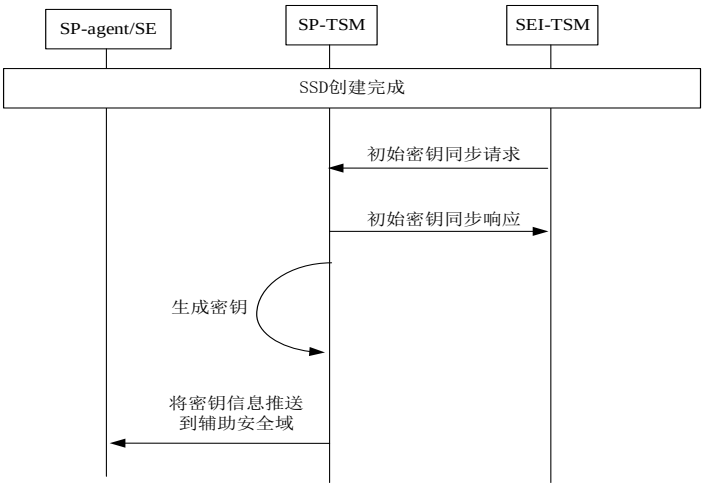

图3 SSD 密钥更新流程图示例

6.2.3 可信应用托管流程

终端SE发起创建/更新/删除安全应用的请求。在可信应用托管服务的模式中，SP-TSM向SEI-TSM发送申请Token请求，SEI-TSM根据请求信息返回申请Token响应。SP-TSM将授权令牌和应用操作一起下发给终端SE，完成相应的应用操作。可信应用托管流程图示例如图4所示：

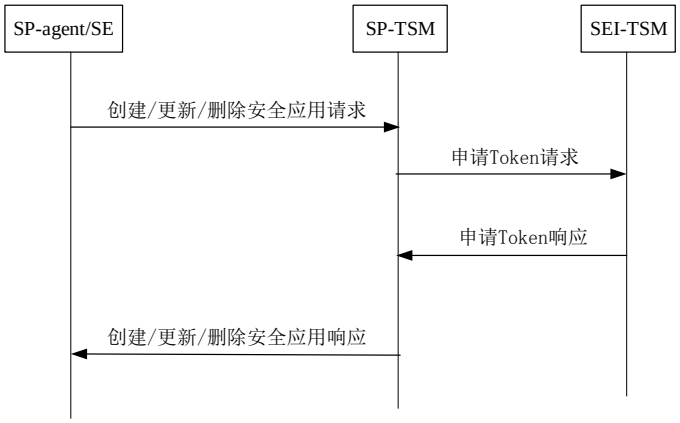

图4 可信应用托管流程图示例

6.2.4 SSD 状态同步流程

由于SE维修或更换时，会对SE中的SSD造成影响，导致SSD的状态和SP-TSM平台维护的状态信息不一致。SEI-TSM或其它设备厂商服务器发送SSD状态同步请求给SP-TSM,明确SE中的SSD及应用可能被清除。根据状态信息，SP-TSM返回SSD状态同步响应，并根据更新的SSD状态去调整服务，并通知相关服务提供方。SSD状态同步流程示例如图5所示：

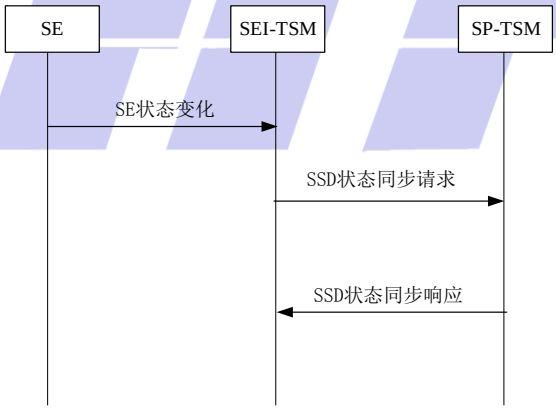

图5 SSD 状态同步流程示例

6.3 接口功能

6.3.1 SSD 管理

SP-TSM向SEI-TSM申请创建/锁定/解锁/删除归属于SP的辅助安全域(SSD)，用于后续SP管理自有应用。若不能一次完成SSD管理指令的所有信息，可通过获取指令继续执行剩余SSD管理指令。

6.3.2 Token 申请

在委托管理模式，SP-TSM执行应用的生命周期管理时，如应用下载、安装、删除、迁移等操作时需要向SEI-TSM申请当前操作的Token。

6.3.3 密钥同步

归属于SP的SSD创建完成后，SEI-TSM调用密码同步接口，将SSD的初始密钥推送给SP-TSM，用于SP-TSM对SSD进行生命周期管理。

6.3.4 SD 状态同步

当设备在SEI方进行维修或更换操作时,SE中的SSD及应用可能被清除,需要将该状态同步到SP-TSM。

7 技术要求

7.1 辅助安全域（SSD）管理

SP-TSM应提供辅助安全域的生命周期管理,包括辅助安全域的创建、删除、锁定、解锁等。

SP-TSM应支持授权模式和委托模式两种辅助安全域管理模式。

在辅助安全域删除前，如果该安全域中有相关的应用，则应与关联的应用提供方进行协商。

如果发现卡片存在威胁且与特定的安全域相关，SP-TSM可锁定该安全域。处于锁定状态的安全域，其相关安全域和应用将无法被操作。当安全域威胁解除后，SP-TSM可解锁该安全域，恢复到锁定前的状态。

SP-TSM应接受SEI-TSM或其它设备厂商服务器推送的SE状态信息，更新辅助空间域的状态，并相应地调整可信服务的管理。

7.2 可信应用管理

SE的可信应用管理包括应用查询、应用下载、应用个人化、应用的锁定/解锁、应用的删除等。对于委托管理模式，在进行应用管理前，SP-TSM应支持申请主安全域授权令牌。应用查询主要是系统侧应能查询和发现SE上已安装的应用。应用下载应支持应用文件安全可靠的下载到SE上，并成功安装；如果SE挂起或者锁定，则停止应用下载。如果安全域不存在、被锁定或者安全域剩余空间不足，均停止下载应用，待完成安全域创建或者安全域满足要求后下载应用。应用实例化后，SP-TSM应支持应用个人化配置，如证书颁发等。应用个人化即SE应用实例加载个人数据的过程，TSM平台应验证应用提供方的合法性，并且同应用提供方建立端到端加密的安全链路，以保障个人化数据的安全。个人化数据包括应用数据、密钥、指令等。根据服务需求，TSM平台可具备对应用进行锁定/解锁功能。解锁操作仅在应用锁定状态可进行。根据服务需求，TSM平台可具备删除应用功能，删除操作应在SE上应用存在是可进行，删除后应释放相应的安全域空间。

7.3 密钥安全管理

SP-TSM应支持线上或线下等方式，获得SSD的初始密钥。SP-TSM可接收SEI-TSM推送的SSD初始密钥信息，或通过其他安全的（如加密信封、安全邮件等）等获取SSD的初始密钥信息。为了保证安全需要，需对初始密钥进行替换，SP-TSM应具备密钥产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等全生命周期安全保障机制。

7.4 服务提供方管理

SP-TSM应支持提供方的管理，包括应用服务方注册、审核、更新、状态变更等。

在应用提供方注册时，提供方向SP-TSM平台提交基本信息，例如机构名称、机构代码，机构联系人等。SP-TSM平台需要审核信息提供方的信息，审核通过后，管理员设置对应用提供方的管理期限，应用提供方可以在管理期限范围内接入SP-TSM平台。SP-TSM可设置应用提供方的状态，如注销某一应用提供方，暂停对其提供服务。应用提供方注销后，其发布的应用即可停止管理。

8 安全要求

8.1 密码安全要求

本文件涉及的密码算法应符合法律、法规的规定和相关国家标准、行业标准的有关要求。并保证密码算法在应用中的合规性，正确性和有效性。

8.2 数字证书系统

CA为证书认证服务系统的主体机构，CA提供对数字证书签发、发布、更新、撤销等数字证书全生命周期服务。通过电子认证服务CA系统，实现SP-TSM和SE、SEI-TSM、应用提供方等不同实体之间的相互认证和通信安全保障。

8.3 传输安全

对SP-TSM和SE、SEI-TSM和应用提供方之间的报文关键要素计算消息鉴别码或进行签名加密，以保障接收方检验报文的真实性及保证关键要素数据的机密性。应使用足够强度的密码算法和安全协议保护SP-TSM和SE、SEI-TSM和应用提供商之间的连接，例如使用SSL/TLS、IPSEC、TLCP等协议。

9 接口要求

9.1 SSD 管理

本接口用于SP-TSM向SEI-TSM申请归属于SP的辅助安全域(SSD)的管理，如创建/锁定/解锁/删除，用于后续SP管理自有应用。

接口调用方式为SP-TSM申请调用SEI-TSM，请求必要参数如表1：

表1 请求必要参数

字段定义	类型	必要性	备注
tenantId	string	M	SP-TSM的身份标识，由SEI-TSM分配
optType	string	M	本次调用的操作类型标识，如“CREATE_SSD”
seId	string	M	SE芯片的唯一标识，从芯片中使用GET DATA指令读取
sdAid	string	M	请求创建的SSD的AID
expPrivilege	string	C	请求创建的SSD时，期望权限是必选，取值内容与GP中的priv字段一致
scpConfig	string	M	创建的SSD所使用的安全通道配置，如“0255”

响应返回数据如表2：

表2　相应返回参数

字段定义	类型	必要性	备注
resultCode	int	M	本次请求返回的结果码，如“0000”表示正常响应，“9999”表示异常响应
resultMessage	string	O	本次请求返回的结果说明字段
apduList	List<string>	M	本次请求对应返回的apdu指令集，用于下发到SE中执行相应操作
taskId	string	M	用于标识本次的任务

9.2　获取指令

当SP-TSM触发的SSD管理时，在SSD权限申请过程中，根据GP协议规范的流程，需要多次交互完成整个管理过程，因此在发起表1和表2的初次交互之后，使用该接口继续进行SSD该管理过程，直到结束。

接口调用方式：SP-TSM 申请调用SEI-TSM，请求必要参数如表3：

表3　请求必要参数

字段定义	类型	必要性	备注
tenantId	string	M	SP-TSM的身份标识，在接入SEI-TSM时由SEI分配
taskId	string	M	之前接口调用中返回的taskId
seId	string	M	SE芯片的唯一标识，从芯片中使用GET DATA指令读取
respList	List<string>	M	上一批次apdu指令在SE中执行后的返回数据及状态字

响应返回数据如表4：

表4　响应返回数据

字段定义	类型	必要性	备注
resultCode	int	M	本次请求返回的结果码
resultMessage	string	O	本次请求返回的结果说明字段
apduList	List<string>	M	本次请求对应返回的apdu指令集，用于下发到SE中执行相应操作
taskId	string	M	用于标识本次的任务

9.3　Token 申请

如果采用DMSD的方式对接，则SP-TSM在执行应用下载、安装、删除、迁移等操作时需要向SEI-TSM申请当前操作的Token。具体的Token计算方式可参照GP 2.2.1规范第9章的要求。

接口调用方式：SP-TSM申请调用 SEI-TSM。请求必要参数如表5：

表5 请求必要参数

字段定义	类型	必要性	备注
tenantId	string	M	SP-TSM的身份标识，在接入SEI-TSM时由SEI分配
optType	string	M	本次调用的操作类型标识，如“CREATE_TOKEN”
seId	string	M	SE芯片的唯一标识，从芯片中使用GET DATA指令读取
rawData	List<string>	M	SP-TSM在本次操作的apdu指令中，根据GP规范对需要签名的数据进行组装，并提供给SEI-TSM进行计算。

响应返回数据如表6：

表6 响应返回数据

字段定义	类型	必要性	备注
resultCode	int	M	本次请求返回的结果码
seId	string	M	SE芯片的唯一标识，从芯片中使用GET DATA指令读取
resultMessage	string	O	本次请求返回的结果说明字段
token	List<string>	M	本次请求对应返回的Token值，供SP-TSM在指令之后进行拼接

9.4 密钥同步

当初始密钥由SEI-TSM分配时，SEI-TSM调用下表的接口完成密钥同步。

接口调用方式：SEI-TSM申请调用SP-TSM。请求必要参数如表7：

表7 请求必要参数

字段定义	类型	必要性	备注
seiTsmId	string	M	SEI-TSM的标识
SsdAid	string	M	本次密钥所对应的ssd的AID
encryptedKey	List<string>	M	经过加密后的密钥
Alg	string	M	密钥对应的算法

表 7　请求必要参数（续）

字段定义	类型	必要性	备注
Usage	string	M	密钥的用途
checkValue	List<string>	M	用于解开密钥之后对其密钥值进行校验，保障正确性

响应返回数据如表8：

表8　响应返回数据

字段定义	类型	必要性	备注
resultCode	int	M	本次请求返回的结果码
resultMessage	string	O	本次请求返回的结果说明字段
receipt	List<string>	O	接收密钥之后返回的收条，表明该密钥已正确接收

9.5 SD 状态同步

当设备在SEI方进行维修或更换操作时，SE中的SSD及应用可能被清除，需要将该状态同步到SP-TSM。

接口调用方式：SEI-TSM申请调用SP-TSM，请求必要参数如表9：

表9　请求必要参数

字段定义	类型	必要性	备注
seiTsmId	string	M	SEI-TSM的标识
ssdAid	string	M	本次密钥所对应的ssd的AID
status	string	M	表明本次操作之后ssd的状态，例如“DELETED”，“RESETED”等

响应返回数据如表10：

表10　响应返回数据

字段定义	类型	必要性	备注
resultCode	int	M	本次请求返回的结果码
resultMessage	string	O	本次请求返回的结果说明字段

参 考 文 献

[1] GB/T 38636-2020 信息安全技术 传输层密码协议（TLCP）
[2] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
[3] JR/T 0097-2012 中国金融移动支付 可信服务管理技术规范
[4] GPC_SPE_034 GlobalPlatform Card Specification

电信终端产业协会团体标准

服务提供方可信服务管理技术要求

T/TAF 096-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn