ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0285—2024

基于数字证书的移动终端金融安全身份认证规范

Specification for mobile terminal financial security identity authentication based on digital certificate

2024－01－15 发布　　2024－01－15 实施

中国人民银行　　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。

本文件由中国人民银行科技司提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：北京金融科技产业联盟、中国人民银行数字货币研究所、中国工商银行股份有限公司、中国农业银行股份有限公司、中国银行股份有限公司、中国建设银行股份有限公司、中国银联股份有限公司、中金金融认证中心有限公司、北京国家金融科技认证中心有限公司、北京银联金卡科技有限公司、华为技术有限公司、荣耀终端有限公司、小米科技有限责任公司、OPPO广东移动通信有限公司、北京紫光展锐科技有限公司、北京豆荚科技有限公司、北京一砂信息技术有限公司、无锡融卡科技有限公司、北京扬帆伟业科技有限公司、恒宝股份有限公司、北京握奇数据股份有限公司、上海奥航智能科技有限公司、国泰君安证券股份有限公司、国民认证科技（北京）有限公司。

本文件主要起草人：潘润红、聂丽琴、黄本涛、胡达川、李明艳、李璐、于鹏、洪宝南、金驰、王麒麟、金鑫、陈维开、何伟明、周小淋、李定洲、詹成初、陈成钱、于文海、鲁欣、张海燕、唐辉、黄江、章盼、王鑫、杨波、张友奖、李坤、张有科、韩业飞、罗广文、王磊、薛升俊、李根、张寒冰、杨子光、张楚、路如毅、王涛、熊帅、赵李明、鲁洪成、李勃、丁宁、陶惠勇、柴海新、邬大港。

引　言

随着移动互联网产业的创新发展，移动终端金融业务得到了快速普及，移动金融的需求也已经向安全、便捷、高效的方向发展。基于数字证书电子认证方式的传统网银智能密码钥匙设备有效地满足了网银系统的安全需求，但无法适应当前移动终端金融业务对安全产品便携易用、体验平滑和场景深度嵌入的需求。

近年来，在移动终端上采用数字证书的电子认证方式逐渐成为保障金融交易安全和客户资金安全的重要手段。为规范在移动终端上开展数字证书电子认证服务，提升金融行业业务安全水平，特制定本文件。

基于数字证书的移动终端金融安全身份认证规范

1 范围

本文件规定了基于数字证书的移动终端金融安全身份认证的服务描述、移动终端生命周期管理、服务生命周期管理、密钥管理、安全及功能、风险控制和运营管理的要求。

本文件适用于银行业金融机构、非银行支付机构，以及相关终端厂商、电子认证服务商等。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

GM/T 0062—2018 密码产品随机数检测要求

JR/T 0089.2—2012 中国金融移动支付 安全单元 第2部分：多应用管理规范

JR/T 0098.2—2012 中国金融移动支付 检测规范 第2部分：安全芯片

JR/T 0098.5—2012 中国金融移动支付 检测规范 第5部分：安全单元（SE）嵌入式软件安全

JR/T 0118—2015 金融电子认证规范

JR/T 0156—2017 移动终端支付可信环境技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

移动终端 mobile terminal

可移动的便携式计算设备。

注：移动终端包括带有无线上网功能的智能移动通信终端、平板式计算机、便携式计算机。

[来源：GB/T 25069—2022，3.719]

3.2

安全单元 secure element；SE

负责身份认证服务的密钥和数字证书等关键数据的存储和运算的高安全性硬件部件。

注：安全单元包括移动终端集成的安全芯片和外置的安全芯片。

[来源：JR/T 0088.1—2012，2.11，有修改]

3.3

富执行环境 rich execution environment；REE

在移动终端内，由通用操作系统管理和控制的环境。

注：通用操作系统及运行在其中的应用程序具有不可信的特点。

3.4

可信执行环境 trusted execution environment；TEE

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注：硬件级隔离是基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环境访问的一种安全机制。

[来源：GB/T 41388—2022，3.3]

3.5

可信环境 trusted environment

个人移动终端上基于硬件和软件结合的安全技术，为移动支付相关业务提供的运行环境。

注：本文件中的可信环境指TEE安全环境和TEE+SE安全环境。

[来源：JR/T 0156—2017，3.1，有修改]

3.6

可信用户接口 trusted user interface；TUI

在可信执行环境内为可信应用与用户提供具有输入或输出安全交互能力的接口。

3.7

电子认证机构 certificate authority；CA

对数字证书进行全生命周期管理的实体。

[来源：JR/T 0118—2015，3.2]

3.8

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的电子认证机构进行数字签名的一个可信的数字化文件。

[来源：GB/T 20518—2018，3.7，有修改]

3.9

智能密码钥匙 cryptographic smart token

内置单片机或智能卡芯片，具备存储用户私钥以及数字证书能力的终端硬件设备。

[来源：JR/T 0068—2020，3.7，有修改]

3.10

个人标识码 personal identification number；PIN

用于鉴别用户身份和防止私钥被未授权使用的字符序列。
[来源：JR/T 0114—2015，3.8，有修改]

3.11

可信应用 trusted application；TA

运行在可信执行环境中的应用程序。
[来源：GB/T 41388—2022，3.8]

3.12

安全应用 secure application；SA

运行在SE中，通过预置或者空中下载的方式进行安装的应用程序。

3.13

可信服务管理 trusted service management；TSM

由可信第三方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。
[来源：JR/T 0088.1—2012，2.20]

4 安全身份认证服务

4.1 概述

本文件中安全身份认证服务指基于数字证书的金融安全身份认证服务。安全身份认证服务在金融机构的手机银行、网上银行等金融业务中使用。

根据移动终端可信环境不同的安全能力级别，安全身份认证服务由多个应用组成。各部分应用分别装载及运行在移动终端的不同运行环境中，提供不同的功能和安全能力，相互协作共同提供完整的安全身份认证服务，服务应用包括以下内容。

a）在 REE 中的客户端应用。

b）在 TEE 中的可信应用。

c）在 SE 中的安全应用。

4.2 服务体系构成

服务体系由用户方、服务提供方（金融机构、平台提供方）、设备提供方和CA组成。服务体系构成如图1所示。

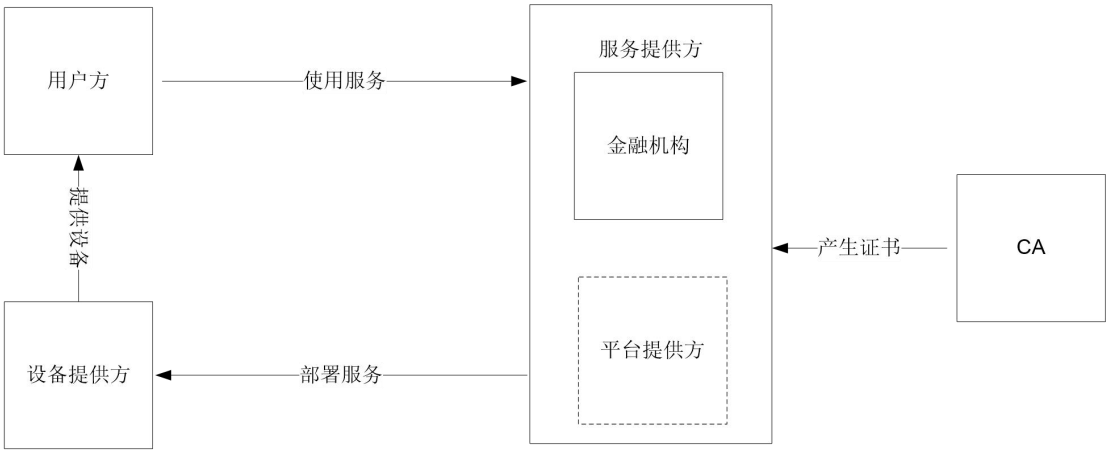


图 1　服务体系构成

服务体系中业务参与方的角色及其之间的关系如下。

a）用户方：使用安全身份认证服务的对象。在不同的场景下具有不同的含义，例如移动终端的拥有者、安全身份认证服务的申请者及使用者。

b）服务提供方：向用户提供安全身份认证服务，处理用户提交的服务申请，并对服务相关的系统、平台等进行管理。在不同的实施方式中可再细分为金融机构、平台提供方，平台提供方主要是向金融机构提供系统、平台等服务。

c）设备提供方：安全身份认证服务载体的生产制造方，为服务提供方在设备上部署安全身份认证服务提供必要的技术支撑。

d）CA：采用公开密钥基础技术，提供证书的签发和管理的机构。

4.3　一般结构

4.3.1　概述

根据移动终端可信环境不同能力级别（分类分级参见JR/T 0156—2017），身份认证实现方式采用TEE+SE安全能力和采用TEE安全能力2种方式。身份认证在商业银行中的具体实现方式参见附录A。

4.3.2　采用 TEE+SE 安全能力的方式

采用TEE+SE安全能力的一般结构如图2所示。

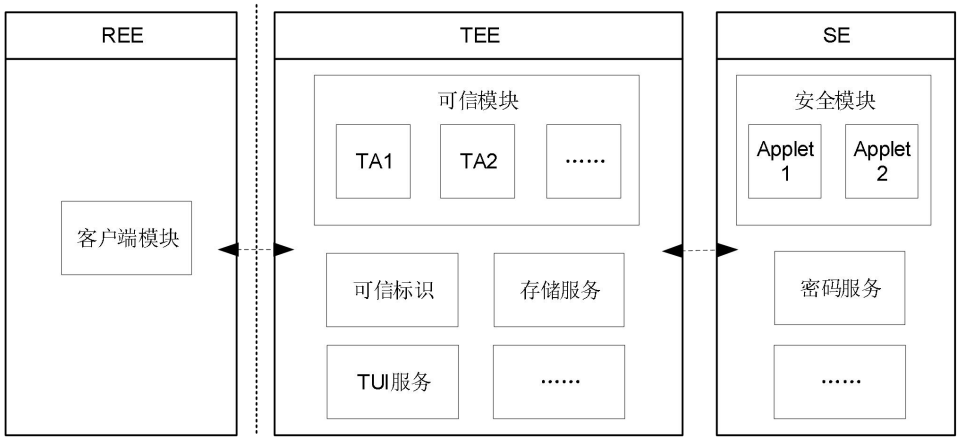


图 2　一般结构（采用 TEE+SE 安全能力的方式）

采用TEE+SE安全能力的一般结构时，应符合以下规则。

a）在 REE 中的客户端模块：

——运行在 REE 中，是用户使用服务的入口。

——提供身份认证应用管理的接口，实现下载、安装、更新、删除等功能。

——实现证书管理，包括申请、下载、更新及删除等操作。

b）在 TEE 中的可信模块：

——运行在 TEE 中。

——实现用户 PIN 码的安全输入及管理。

——实现交易信息的显示和确认。

——提供 SE 安全访问通道。

c）在 SE 中的安全模块：

——运行在 SE 中。

——只接受 TEE 的安全访问。

——提供密码服务，实现签名密钥的生成和私钥管理功能。

——提供密码服务，实现 PIN 码管理功能。

——提供密码服务，实现交易信息签名功能。

4.3.3　采用 TEE 安全能力的方式

采用TEE安全能力的一般结构如图3所示。

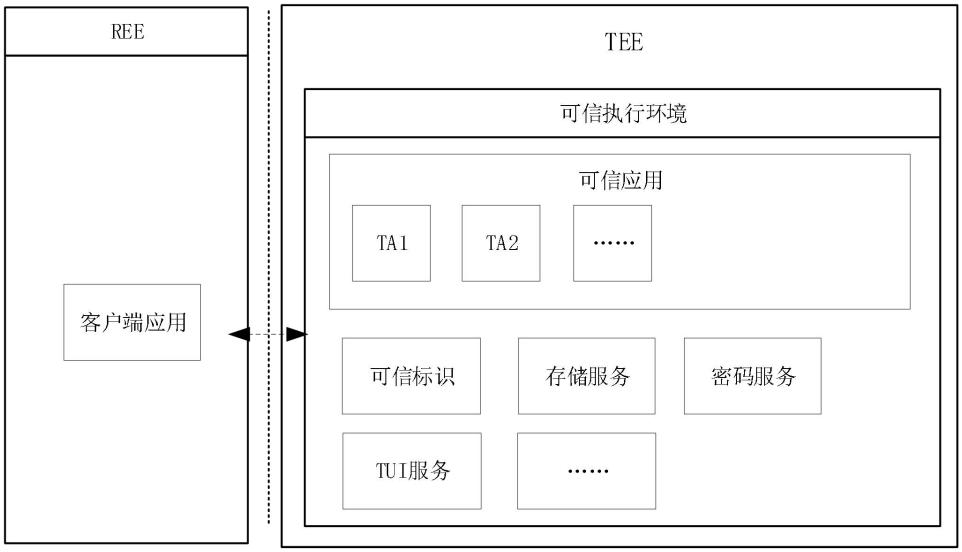


图 3　一般结构（采用 TEE 安全能力的方式）

采用TEE安全能力的一般结构时，应符合以下规则。

a）在 REE 中的客户端应用：

——运行在 REE 中，是用户使用服务的入口。

——提供身份认证应用管理的接口，实现下载、安装、更新、删除等功能。

——实现证书管理，包括申请、下载、更新及删除等操作。

b）在 TEE 中的可信应用：

——运行在 TEE 中。

——实现交易信息的显示和确认。

——提供密码服务，实现签名密钥的生成和私钥管理功能。

——提供密码服务，实现 PIN 码的安全输入及管理功能。

——提供密码服务，实现交易信息签名功能。

5　移动终端生命周期管理

5.1　概述

作为安全身份认证服务的载体，移动终端的生命周期划分为生产、使用、转让、丢失、维护和恢复出厂设置阶段。

5.2　生产

移动终端生产制造环境（例如机房、设备、网络、运输、人员及管理等）应符合相关行业要求。

移动终端数据预置过程（例如SE操作系统、TEE操作系统、工厂密钥、其他敏感数据等）应符合相关行业要求。

5.3　使用

用户在具有安全身份认证服务能力的移动终端上，通过服务提供方客户端应用进行相关服务操作。

设备提供方宜在移动终端系统功能层，提供安全身份认证服务启用开关。用户通过该功能管理安全身份认证服务状态（打开、关闭），以及管理允许访问安全身份认证服务的客户端应用。

5.4 转让

服务提供方应提供用户提示机制，提示用户在转让已经启用安全身份认证服务的移动终端前，进行安全身份认证服务注销，并告知用户转让行为发生后的原终端安全身份认证服务补注销方式。补注销方式包括但不限于客户本人持有效身份证件到柜台办理或通过金融机构客服电话办理等，金融机构应核实客户信息、网银账户信息并对预留手机号码进行验证。

5.5 丢失

服务提供方应提供用户提示机制，提示用户在丢失已经启用安全身份认证服务的移动终端后，进行安全身份认证服务注销，并告知用户丢失发生后的原终端安全身份认证服务补注销方式。

5.6 维护

服务提供方应提供用户提示机制，提示用户在维修已经启用安全身份认证服务的移动终端前，进行安全身份认证服务注销，并告知用户维护发生后的原终端安全身份认证服务补注销方式。

设备提供方在对具备安全身份认证服务能力的移动终端进行返厂维修时，应首先将安全身份认证服务相关的数据全部删除。

5.7 恢复出厂设置

设备提供方提供的移动终端“恢复出厂设置”功能，应删除REE和TEE中服务提供方和用户的数据，宜删除SE中服务提供方和用户的数据。

6 安全身份认证服务生命周期管理

6.1 概述

安全身份认证服务的完整生命周期包括服务申请、服务初始化、证书管理、服务应用和服务注销。

6.2 服务申请

安全身份认证服务应由用户本人申请，服务提供方应对申请用户进行身份鉴别。

用户身份鉴别通过后，服务提供方应向用户提供相关凭证（例如授权码、参考号等）或其他安全方式，用于用户后续证书下载操作。

如用户在服务提供方已经存在安全身份认证服务，则先发起服务注销。

安全身份认证服务申请及移动终端关联方式参见附录B。

安全身份认证服务申请主要有以下2种方式。

a）柜面人工方式：用户须携带有效身份证件及服务提供方所要求的其他材料，服务提供方工作人员鉴别用户身份并保留鉴别过程数据以备查，应符合 JR/T 0118—2015 中 5.2.2 身份鉴别的要求。

b）网络自助方式：用户通过网络自助方式向服务提供方发起服务申请，服务提供方应提供用户身份鉴别的技术方法，并保留鉴别过程数据以备查。服务提供方对通过该种方式开通的安全身份认证服务进行一定的功能限制、业务限制。鉴别方式如下。

——基于已拥有智能密码钥匙的鉴别：用户拥有已实名制的、合法的智能密码钥匙设备，在服务提供方的网上银行等客户端上发起服务申请。服务提供方通过智能密码钥匙的签名数据对用户身份进行鉴别。

——基于令牌的鉴别：用户拥有已实名制的、合法的令牌设备，在服务提供方的网上银行、手机银行等客户端上发起服务申请，服务提供方通过用户硬件产生的随机动态口令对用户身份进行鉴别。在令牌验证流程中，宜添加其他身份核验方式以提升安全性，或根据风险控制机制适当降低限额。

——基于金融安全身份认证的鉴别：用户已存在金融安全身份认证服务，申请将金融安全身份认证服务迁移到其他移动终端上时，可采用此方式。服务提供方通过用户当前金融安全身份认证服务的签名数据对用户身份进行鉴别。

——基于其他身份认证的鉴别：通过包括网络身份证、生物识别、网关认证等多种认证方式组合开通数字证书身份认证。

6.3 服务初始化

6.3.1 概述

安全身份认证服务初始化分为REE中的服务初始化、TEE中的服务初始化和采用TEE+SE安全能力情况下SE中服务初始化。

6.3.2 REE 中的服务初始化

客户端安装方式如下。

a）集成在安全身份认证服务相关的客户端软件中，依托客户端软件的下载和安装进行相应操作。

b）客户端模块单独形成安装包，供下载安装。

6.3.3 TEE 中的服务初始化

通过服务提供方平台下载安装包或随REE中的客户端应用统一下载，并在安装后进行实例化操作。

6.3.4 采用 TEE+SE 安全能力情况下 SE 中服务初始化

SE服务初始化要求如下。

a）在移动终端 SE 中创建安全身份认证服务专用的安全域，安全域被 1 个服务提供方所独有，不应被其他应用非法访问。

b）安全域在移动终端出厂前预置或后期创建，安全域宜符合 JR/T 0089.2—2012 的要求。

c）安全应用在终端出厂前预置或后期安装，应用安装宜符合 JR/T 0089.2—2012 的要求。

d）安全应用安装后，应进行实例化操作。

e）如存在实例，则应先删除存在的实例，再重新进行实例化操作。

6.4 证书管理

6.4.1 概述

证书管理操作应由用户本人发起，包括证书下载、证书更新、证书删除等功能，应符合证书管理相关行业规范。

6.4.2 证书下载

用户在移动终端上的客户端中发起证书下载操作，由客户端向服务提供方发起证书下载请求，在收到证书后将证书写入移动终端中，完成证书下载。

6.4.3 证书更新

用户在移动终端上的客户端中发起证书更新操作，并用新证书替换当前证书，适用于证书即将过期、已过期、挂起、注销或用户主动发起更新的情况。证书更新方式如下。

a）当前证书可用时，服务提供方对当前证书进行验证，验证通过后下发新证书。

b）当前证书不可用时，分为以下 2 种情况：

——若证书已过期，用户先注销安全身份认证服务，再重新发起服务申请流程。

——若证书挂起或注销，用户持有效身份证件到服务提供方柜台办理，参照服务申请流程。

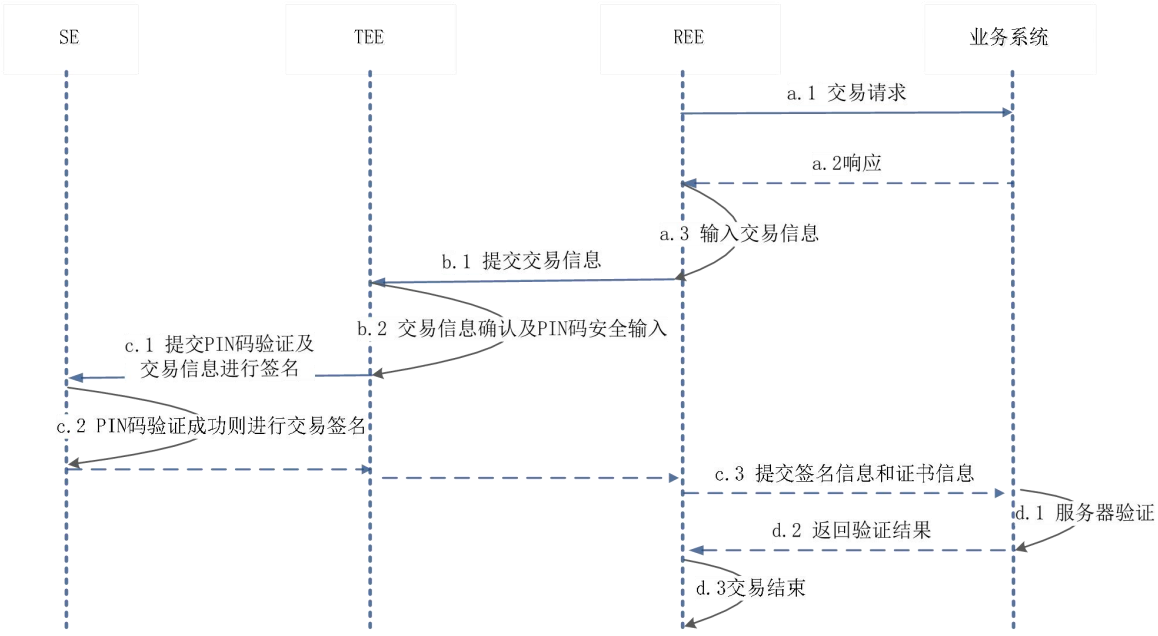
6.4.4 证书删除

证书删除过程参照服务注销（见6.6）。

6.5 服务应用

6.5.1 采用 TEE+SE 安全能力的交易签名流程

在采用TEE+SE安全能力的情况下，交易签名流程如图4所示，关键步骤主要包括交易信息确认、交易信息签名、服务器验证。

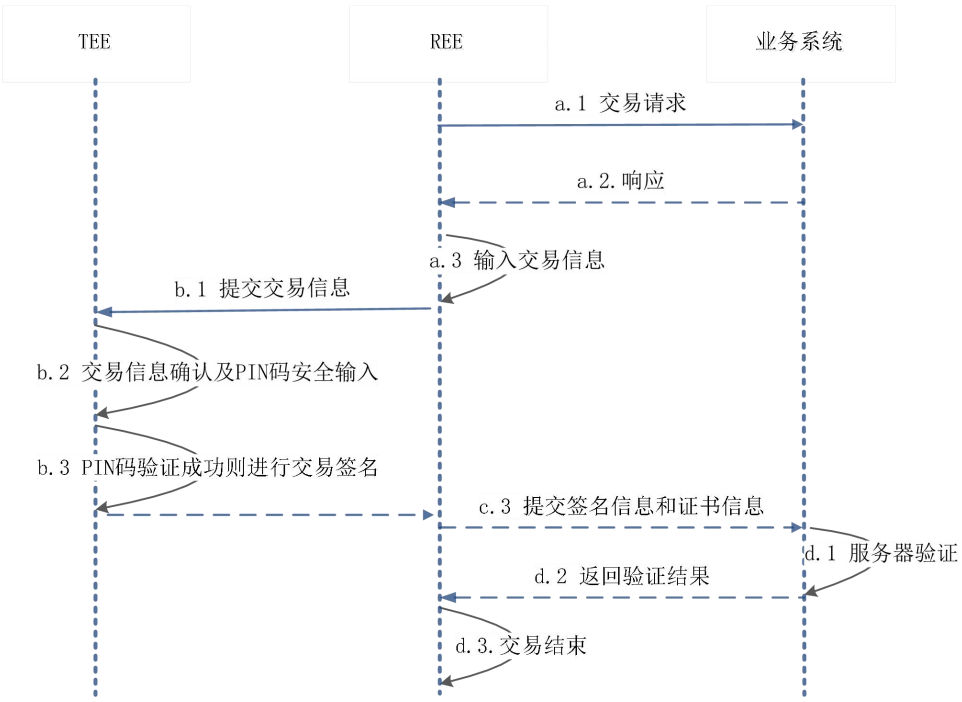


注：PIN码验证宜采用本地免密方式代替，包括指纹、人脸、虹膜等生物特征输入验证方式。

图 4 采用 TEE+SE 安全能力的交易签名流程

6.5.2 采用 TEE 安全能力的交易签名流程

在采用TEE安全能力的情况下，交易签名流程如图5所示，关键步骤主要包括交易信息确认、交易信息签名、服务器验证。



注：PIN码验证宜采用本地免密方式代替，包括指纹、人脸、虹膜等生物特征输入验证方式。

图 5 采用 TEE 安全能力的交易签名流程

6.5.3 交易信息确认

用户在客户端中输入交易信息后，客户端将交易信息传输到TEE的可信模块中，然后通过TUI向用户显示交易信息，用户对交易信息确认后，进行后续签名操作。交易信息确认过程应设置交易超时时间，超时后终止交易。

交易信息的显示及确认应在TUI中进行。应通过技术手段提示用户当前操作是在TEE中，技术手段可选择声、光、独特图像等标识信息。

用户确认交易信息（例如转出账号、转入账号、转入账户名、转出金额等）。服务提供方可选择显示为防止交易伪造攻击的用户预留信息内容。

在TUI界面中宜显示以下信息。

a）安全身份认证服务名称。

b）身份认证标识。

c）金融机构标识。

d）PIN 码输入框。

e）生物特征（例如指纹、人脸、虹膜）确认提示（可选）。

f）确认按钮。

g）取消按钮。

用户对显示的交易信息确认无误后，在TUI界面的输入框中输入PIN码，用户点击确认按钮。确认界面提供取消按钮，如果交易信息存在错误，用户可通过点击取消按钮进行交易取消。

6.5.4 交易信息签名

用户在TUI中点击确认按钮后，由可信环境中的密码服务模块进行PIN码验证，采用TEE安全能力的情况，PIN码验证在TEE中实现；采用TEE+SE安全能力的情况，PIN码验证在SE中实现。若验证不通过，则拒绝对交易数据进行签名；若验证通过，则对交易数据进行签名。

6.5.5 服务器验证

客户端应用接收到签名数据后，将签名数据、交易数据及数字证书一同发送到服务提供方，进行交易信息验证，验证通过后同意交易，否则拒绝交易，将处理结果通知客户端应用。

6.6 服务注销

用户不再使用安全身份认证服务时，通过以下2种方式注销服务。

a）柜面人工方式：用户须携带有效身份证件及服务提供方所要求的其他材料，服务提供方工作人员应现场鉴别用户身份，鉴别通过后，服务提供方工作人员注销安全身份认证服务。

注：此方式适用于当前安全身份认证服务无法使用（例如移动终端丢失、移动终端损坏等）或用户到柜面主动申请注销安全身份认证服务。

b）网络自助方式：用户通过移动终端上的客户端发起操作，在用户身份鉴别（例如PIN码）通过后，客户端发起注销申请，申请数据宜使用安全身份认证服务签名。

用户通过以上2种方式注销服务时，服务提供方验证注销申请数据，验证通过后，服务提供方在安全身份认证服务系统中删除相关数据，保留非用户敏感数据以备查。同时保证相关数据不再分配，避免出现数据不唯一的情况。移动终端客户端同步删除移动终端上的身份认证相关数据。

7 密钥管理

7.1 总体要求

密钥管理应符合国家密码管理部门和行业主管部门要求。

7.2 密钥生命周期管理

7.2.1 随机数生成

参与密钥运算的随机数的相关指标，应遵循GB/T 32915—2016和GM/T 0062—2018中的相关要求。

7.2.2 密钥生成

移动终端可信环境中TEE和SE应根据指定的密钥生成算法生成非对称密钥和对称密钥。

移动终端可信环境中TEE和SE应支持非对称密钥用于签名，应支持对称密钥用于本地或远程数据和密钥的加密。

7.2.3 密钥更新

密钥更新要求与密钥生成要求相同。

7.2.4 密钥存储

密钥存储安全要求见表1。

表1　密钥存储安全要求表

密钥类型	安全要求
TEE密钥	TEE应为密钥提供安全存储能力，保证密钥的真实性、完整性、机密性以及原子性。
SE密钥	SE应为密钥提供安全存储能力，保证密钥的真实性、完整性、机密性以及原子性。 确保导入SE的密钥（例如对称密钥）信息，在任何情况下均不会被导出。 SE中生成的私钥，在任何情况下均不会被导出。 可采用存储对称密钥分量的方式存储密钥，但应保证分量保管在安全的物理环境中并确保不同分量分离保管。

7.2.5　密钥销毁

明文密钥在生命周期结束后应进行销毁，遵循密钥销毁方法如下。

a）清除密钥的目标源和存储位置。

b）应销毁所有不再需要的明文密钥材料。

7.3　安全域密钥转移

转移过程在于设备提供方和服务提供方对密钥的转移，保证密钥的授权转移和管理。宜选择的2种方式如下。

a）设备提供方生成初始化密钥，在设备生产后通过足够安全的方式将初始化密钥移交给服务提供方，不应以明文传输。

b）服务提供方生成初始化密钥，在设备出厂前通过足够安全的方式将初始化密钥移交给设备提供方，设备提供方将其预置在移动终端中。

若由设备提供方生成初始化密钥，则服务提供方在接收到初始化密钥后，应立即使用初始化密钥生成新密钥，再进行后续的业务操作。

任何一方所导出的密钥都应以集成电路（IC）卡、密码信封或其他安全方式传给对方，再以安全的方式注入到加密设备中。

安全域密钥传输交接过程应履行严格的操作审批手续，详细记录，相关人员签名确认，文档资料应妥善保管，保存期限应不低于记录对象的生命周期，确保各类密钥传输的安全性与规范性。

8　安全及功能要求

8.1　通用要求

通用要求如下。

a）安全身份认证服务宜具备唯一认证标识信息。

b）不应向SE写入私钥、不固化密钥对和用于生成密钥对的素数。

c）私钥存储在SE中，且不可导出。

d）对SE中密钥的授权处理，由TEE和SE之间的安全通道进行保护。

e）敏感性信息传递和用户身份的验证等由可信环境进行保护。

f）证书下载宜使用安全传输通道。

g）应提供交易敏感信息显示及确认机制。

h）应提供PIN码验证机制，验证通过后才能进行数据签名。

i）电子签名信息在可信环境中生成（采用TEE安全能力的方式，在TEE中生成；采用TEE+SE安全能力的方式，在SE中生成）。
j）不应在日志中记录用户敏感信息。

8.2 TUI 要求

TUI要求如下。
a）应显示交易确认信息。
b）应提供确认及取消按钮。
c）字符集至少应支持英文、简体中文语言的显示。
d）应支持PIN码输入。
e）应支持图片显示。

8.3 PIN 码要求

PIN码要求如下。
a）证书下载、更新操作，应验证PIN码。
b）交易过程中的私钥签名，每次都应验证PIN码。
c）PIN码输入和修改应在TUI中进行。
d）PIN码验证应在可信环境中进行（采用TEE安全能力的情况，在TEE中实现；采用TEE+SE安全能力的情况，在SE中实现）。
e）PIN码验证应具备防重放机制，并且在任何时候均不应以明文形式传输。
f）PIN码字符集由键盘上的可见字符组成，区分大小写。
g）应设置PIN码尝试次数，尝试超过次数后，安全身份认证服务被锁死。
h）安全身份认证服务锁死后，即使再输入正确PIN码，服务也为不可用状态。
i）解锁过程需先注销安全身份认证服务，并再次申请服务。

8.4 凭证要求

服务提供方向用户提供相关凭证（例如授权码、参考号等）要求如下。
a）应经安全处理。
b）保证安全性和机密性。
c）保证使用过程可追溯性。
d）对有效期进行严格设定。
e）在使用后，立即失效。
f）如果是输入型凭证（例如授权码、参考号等），宜在TUI中输入。

8.5 生物特征身份鉴别要求

生物特征身份鉴别要求如下。
a）用于身份鉴别的生物信息（例如指纹、人脸、虹膜等），应使用密码技术保证其机密性、完整性，且应配合TEE、SE等技术安全地存储在采集设备中，采集到的生物特征信息不应移出移动终端可信环境。
b）采用客户本人生物特征作为验证要素的，应符合国家标准、金融行业标准和相关信息安全管理要求，防止被非法存储、复制或重放。
c）用于身份鉴别的生物信息，未经用户同意，不应应用于生成用户画像或进行个性化推荐。

8.6 SE 要求

SE要求如下。

a）SE安全芯片应符合JR/T 0098.2—2012的要求。

b）SE嵌入式软件应符合JR/T 0098.5—2012的要求。

c）SE安全应用管理应符合JR/T 0089.2—2012的要求。

8.7 TEE 要求

TEE要求如下。

a）应提供可信应用生命周期管理，包括但不限于在TEE中安装、更新、锁定、解锁及卸载。

b）可信应用生命周期通过可信服务管理平台远程管理。

c）执行管理操作前可信服务管理平台和TEE通过安全预置的密钥相互认证后建立安全通道。

d）确保数据来源的真实性和传输数据的完整性、机密性以及真实性，并具备防止重放攻击的能力。

e）TEE应在安全环境中生产，安全要求应符合相关行业规范。

8.8 客户端要求

客户端要求如下。

a）客户端应用卸载时，客户端应用的附属数据和用户数据应被清除。

b）客户端应用卸载完成后，文件系统中不应残留任何用户数据及交易数据等。

c）客户端应用卸载时，SE中的数据（例如辅助安全域、安装包、实例、个性化数据等）应保留。

9 风险控制要求

9.1 测试评估

在安全身份认证服务首次上线和发生重大变更时，服务提供方或金融机构应对相关软硬件产品进行安全风险测试评估。

9.2 交易监控

交易监控要求如下。

a）宜建立交易监控系统，能甄别并预警潜在风险交易。

b）在交易前应对移动终端的安全环境状态进行必要的安全检测。

c）宜采用大数据分析、用户行为建模等手段，建立交易风险监控模型和系统，对异常交易进行及时告警，并采取调查核实、风险提示等处理措施。

d）宜根据交易的风险特征建立风险交易模型，有效监测可疑交易，对可疑交易建立报告、排查复核、调查终结等机制。

e）宜依据已识别并确认的风险数据，建立黑名单数据库。

f）宜通过分析用户交易习惯和群体用户行为习惯，提高交易监控的效率和准确率。

g）宜通过分析欺诈行为特征创建反欺诈规则，对交易数据实时分析，根据风险高低产生预警信息，实现欺诈行为的侦测、识别、预警和记录。

9.3 客户教育

针对安全身份认证服务过程中的客户信息保护和操作流程，应采用以下方式提高客户熟悉度。

a）加强对用户PIN码等身份认证信息的保护管理和客户安全教育，提示客户及时修改密码。

b）让客户充分了解功能实现和操作流程，例如提供对外服务功能的演示版等。

10 运营管理要求

10.1 多服务管理要求

同一个移动终端支持多家服务提供方的安全身份认证服务业务。

10.2 服务访问控制

安全身份认证服务在默认情况下是离线状态，客户端软件检测到安全身份认证服务离线，需提示无法建立与安全身份认证服务的连接。用户通过移动终端的其他部件进行物理方式控制或逻辑方式控制，保证安全身份认证服务在没有授权的情况下，不被恶意应用滥用。

用户在通过客户端应用发起业务操作前，通过对客户端应用进行授权，使得客户端应用与安全身份认证服务建立连接。在客户端应用完成交易后，安全身份认证服务应处于离线状态。

11 证实方法

11.1 生命周期管理要求的验证

按照第6章安全身份认证服务生命周期管理的要求，通过文档审查和服务操作，对服务申请、服务初始化、证书管理、服务应用和服务注销进行验证。

11.2 密钥管理要求的验证

按照第7章密钥管理的要求，通过文档审查和日志查验，对随机数生成、密钥生成、密钥更新、密钥存储、密钥销毁和安全域密钥转移进行验证。

11.3 安全及功能要求的验证

按照第8章安全及功能要求，通过文档审查、服务操作、指令扫描等方法，对通用性、TUI、PIN码、凭证、生物特征身份鉴别、SE、TEE、客户端的安全及功能进行验证。

11.4 风险控制要求的验证

按照第9章风险控制要求，在安全身份认证服务首次上线和发生重大变更时，服务提供方或金融机构应对相关软硬件产品进行安全风险测试评估，形成测试报告和评审记录。交易监控系统在建立后形成完整日志记录。客户教育形成培训记录。

11.5 运营管理要求的验证

按照第10章运营管理要求，检查安全身份认证服务在默认情况下是否为离线状态。在客户端应用完成交易后，安全身份认证服务是否恢复至离线状态。

附 录 A
（资料性）
安全身份认证服务在商业银行中的参考实现

A.1 概述

本附录针对移动终端可信环境安全能力级别多样化的特点，综合运用CA体系、TEE、SE等安全机制，为安全身份认证服务在可信环境安全能力级别不同的移动终端中的产品化实践提供指导。

A.2 安全身份认证分类分级

根据移动终端可信环境不同能力级别（分类分级参见JR/T 0156—2017），安全身份认证实现方式分为以下2类。

a）终端能够提供 SE 安全能力，则由 SE 提供密码服务功能，即 TEE+SE 方式实现身份认证。

b）终端不能提供 SE 安全能力，则由 TEE 提供密码服务功能，即 TEE 方式实现身份认证。

商业银行在本行和跨行转账、单笔和批量转账、对私和对公转账、投资理财、生活服务、跨境汇款等业务场景中，以安全身份认证TEE实现或TEE+SE实现方式作为账户风险分级管控的主要因素，辅以其他风险管控手段，从而提高商业银行账户管理风险管控能力，也从源头上遏制更多违法犯罪行为的发生，为银行资金和客户资金提供更有效的保障。

安全身份认证架构参考实现如图A.1所示。

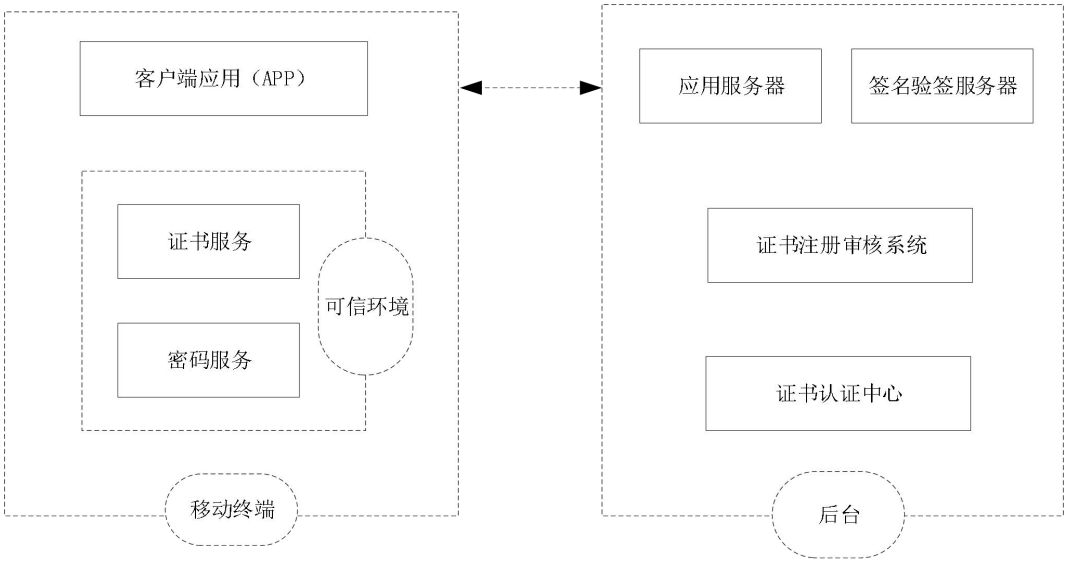


图 A.1 安全身份认证架构

在移动终端中，证书服务模块负责证书申请、证书存储、证书更新等；密码服务模块负责密钥的生成、存储和签名、PIN码设定修改及重置。

A.3 采用TEE+SE安全能力的身份认证终端

在采用TEE+SE安全能力的情况下，身份认证终端架构如图A.2所示。

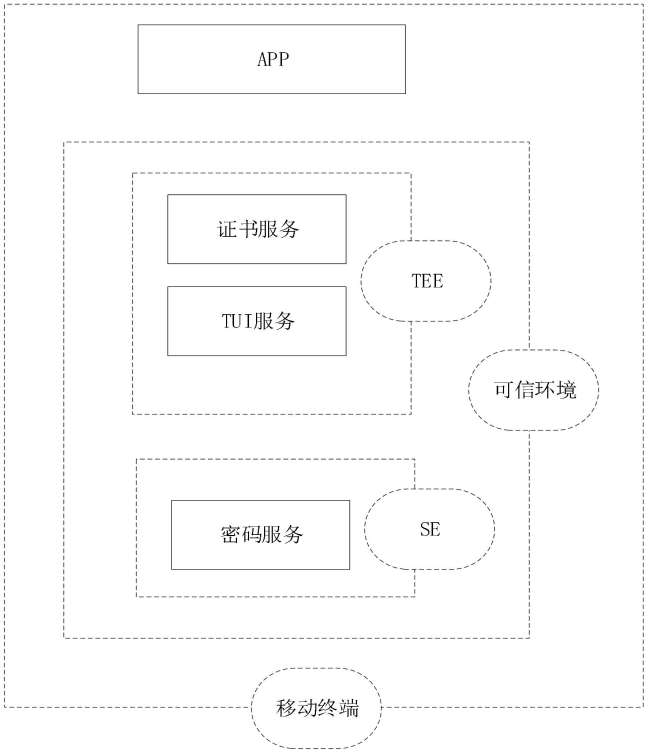


图 A.2 采用 TEE+SE 安全能力的身份认证终端架构

证书服务和TUI服务宜在TEE中实现，密码服务宜在SE中实现。其中，TUI服务模块负责证书PIN码设置界面、PIN码验证输入界面、转账界面等场景下的信息展示和安全输入。

A.4 采用TEE安全能力的身份认证终端

在采用TEE安全能力的情况下，身份认证终端架构如图A.3所示。

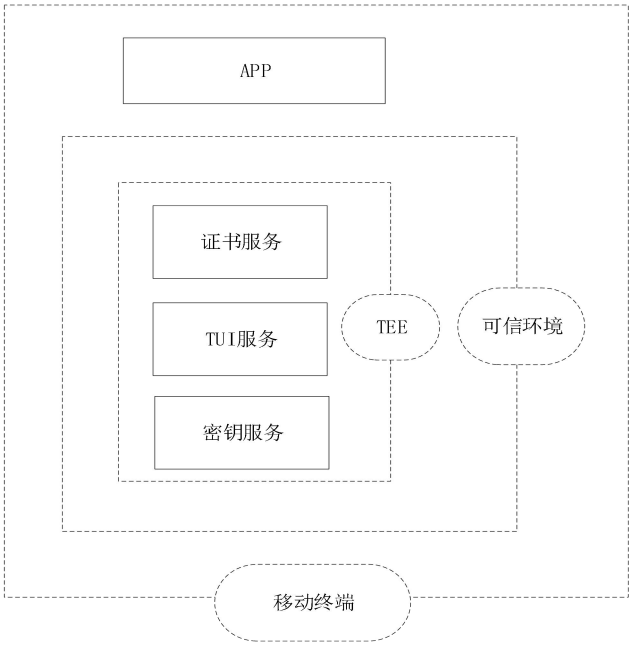
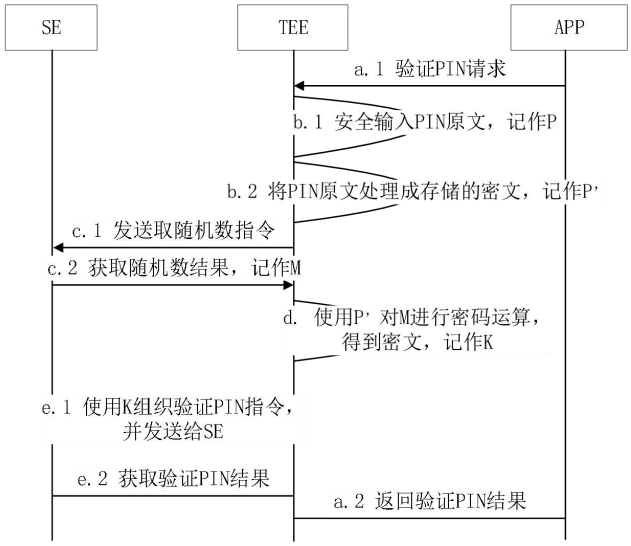


图 A.3　采用 TEE 安全能力的身份认证终端架构

其中，证书服务、TUI服务、密码服务在TEE中实现。

A.5　安全身份认证防重放机制

图A.4以验证PIN码为例描述了防重放攻击的实现机制。



注：1.SE中处理PIN码验证过程为密码服务实现，也可在TEE中密码服务实现。

2.实现原理：每次发送给密码服务进行PIN码验证的指令都随随机数而改变，配合验证PIN码的错误计数器使用，可有效防止重放攻击。

图 A.4　验证 PIN 码过程防重放机制流程

附 录 B
（资料性）
安全身份认证服务申请及移动终端关联方式

B.1 概述

移动终端作为安全身份认证服务的载体，主要由用户购买并使用，而传统网银智能密码钥匙设备主要由金融机构统一采购并向用户发放，二者有较大的区别。针对流程差异，附录B介绍了服务提供方在处理用户开通安全身份认证服务申请时，安全身份认证服务的载体与用户信息的关联，以及数字证书下载至载体中的实现方式。

B.2 实现方式

B.2.1 在移动终端上自助申请

在移动终端上自助申请适用于已经拥有实名制的智能密码钥匙设备的用户。用户在移动终端上自助开通服务，不需要到服务提供方网点进行操作。此方式的优势是用户自助申请并完成服务开通不需要到服务提供方网点进行操作。服务提供方对通过该种方式开通的身份认证服务进行一定的限制（例如转账金额限制等），在经过再次身份鉴别后（例如通过人工核验）解除相应的功能限制。此方式的主要步骤如下。

a）用户自助在移动终端上安装服务提供方客户端软件。
b）用户在客户端上按服务提供方要求输入信息（例如姓名、身份证件号码等）。
c）用户点击申请按钮。
d）用户信息及身份认证服务信息（例如认证标识等）传输至服务提供方业务系统。
e）服务提供方处理用户申请，记录安全身份认证服务信息，生成用户数字证书并下载至SE中，但此时用户数字证书处于未激活状态。
f）用户使用智能密码钥匙设备登录网银系统，在网银系统中发起申请，激活用户数字证书。

B.2.2 在柜面人工申请

在柜面人工申请适用于用户在了解到安全身份认证服务后，直接到服务提供方网点申请开通服务。此方式的优势是用户申请开通服务前，不需要安装服务提供方客户端，用户在服务提供方完成申请后，自助或在服务提供方工作人员协助下完成后续操作。此方式的主要步骤如下。

a）用户提供有效身份证件及服务提供方所要求的其他材料，由服务提供方鉴别用户身份。
b）用户身份鉴别通过后，服务提供方向用户提供相关凭证（例如授权码、参考号等）。
c）用户在移动终端上安装服务提供方客户端。
d）用户在客户端中输入凭证信息，完成安全身份认证服务开通的后续流程（例如数字证书下载等）。

B.2.3 在终端申请由柜面人工关联

在终端申请由柜面人工关联适用于用户在去服务提供方柜面申请服务前，已经安装了服务提供方客户端或在服务提供方网点由工作人员协助用户安装客户端。此方式的优势是与智能密码钥匙设备的发放模式相类似，服务提供方业务系统不需要做较大改动。此方式的主要步骤如下。

a）用户先在移动终端上安装服务提供方客户端。

b）用户提供有效身份证件及服务提供方所要求的其他材料，由服务提供方鉴别用户身份。

c）用户身份鉴别通过后，用户向服务提供方工作人员出示客户端上显示的标识信息（例如身份认证标识等）。

d）服务提供方工作人员在业务系统中输入标识信息，并在服务提供方业务系统中记录。

e）用户自助在移动终端的客户端中发起申请，客户端将申请及标识信息（例如身份认证标识等）传输至服务提供方业务系统。

f）服务提供方业务系统在核验申请后，完成安全身份认证服务的后续流程（例如数字证书下载等）。

参 考 文 献

[1] GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式
[2] GB/T 25069—2022 信息安全技术 术语
[3] GB/T 41388—2022 信息安全技术 可信执行环境 基本安全规范
[4] JR/T 0068—2020 网上银行系统信息安全通用规范
[5] JR/T 0088.1—2012 中国金融移动支付 应用基础 第1部分：术语
[6] JR/T 0114—2015 网银系统USBKey规范 安全技术与测评要求