



## 基于共享式存储的智能终端数字签名方案

刘国荣,刘东鑫,汪来富,沈军,金华敏

(中国电信股份有限公司广州研究院,广东 广州 510630)

**摘要:**在传统互联网中,USB key+数字证书是最成熟的应用安全保障技术,但在移动互联网领域,由于智能终端接口等方面的限制,证书难以直接使用。探讨了在智能终端使用智能卡作为数字证书存储介质,支持多个数字证书,通过统一的管理,为多个应用共享使用,降低证书在智能终端上的使用门槛,并分析了方案的安全性,探讨了数字证书与指纹识别技术相结合,提升用户使用便利性的方案。

**关键词:**智能终端;数字证书;认证;安全

**中图分类号:**TP393

**文献标识码:**A

**doi:** 10.11959/j.issn.1000-0801.2017049

## A digital signature scheme based on shared key in intelligent terminal

LIU Guorong, LIU Dongxin, WANG Laifu, SHEN Jun, JIN Huamin

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

**Abstract:** In traditional internet, digital certificate in USB key is the most mature technology of application security assurance. But it is difficult to use in mobile internet, because of the restriction of intelligent terminal interface. A digital signature scheme based on shared key in intelligent terminal was discussed to lower the threshold. The shared key supported multiple digital certificates, and was shared by multiple applications through the unified management. After that, the security of the scheme was analyzed, and a scheme integrated digital certificate and fingerprint identification was discussed to enhance user convenience.

**Key words:** intelligent terminal, digital certificate, authentication, security

### 1 引言

随着移动互联网开放化、终端智能化和应用丰富化,传统互联网的安全问题也在威胁着移动互联网应用。移动电子商务、移动办公等行业应用由于使用的特殊性,对安全具有很高的要求,特别是对用户身份的验证、交易安全的保障。然而,由于手机终端限制,传统互联网成熟的安全保障技术在移动互联网上应用时存在较多限制,制约了业

务发展。以手机银行为例,目前与身份验证相关的主要技术见表1。

除数字证书外,表1中其他技术仅具备身份验证功能,而数字证书能提供交易过程的机密性、完整性、身份验证以及不可抵赖性的安全保障,特别是采用USB key存储数字证书的方式是安全性最高、在传统互联网领域最成熟的应用安全保障技术。但由于手机系统、端口等的差异性,在手机端应用USB key存在诸多限制:USB并非手机的标

收稿日期:2017-01-20;修回日期:2017-02-16

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(No.2015AA017205)

Foundation Item: The National High Technology Research and Development Program of China (863 Program) (No. 2015AA017205)



表 1 手机银行身份验证技术

| 技术          | 说明                                                                                                           |
|-------------|--------------------------------------------------------------------------------------------------------------|
| 口令          | 手机银行最基本的验证措施,存在口令失窃、暴力破解等风险                                                                                  |
| 手势/图形       | 替代口令的登录方案,提升了便捷性,安全风险与口令相当                                                                                   |
| 短信验证码       | 除口令外应用最广泛的技术,一次一密,安全性强于单纯的口令认证,通常作为多因素认证的辅助手段;但同样存在失窃的风险,拦截短信、窃取验证码的木马是其主要威胁                                 |
| 动态令牌        | 一次一密,具有较高的安全性,PC 和智能手机可采用相同的安全机制;但须额外携带介质                                                                    |
| 指纹识别/生物特征识别 | 使用方便,通常采用 TrustZone(ARM 架构处理器安全区)等硬件安全机制进行防护,安全性有较大提升,但生物特征不可变更的特性使其存在伪造的风险,特征采集、传输、存储、验证各环节也存在受攻击、特征盗用的风险   |
| 数字证书        | 传统互联网中,以 USB key 为存储的数字证书是最成熟的应用安全保障技术,由于终端接口等限制,在手机上需要适配,如采用 micro USB 接口、蓝牙等,增加了 key 的成本,使用也不方便,目前仅有部分试点应用 |

配端口,应用提供商针对手机发放各种接口的 key、定制不同终端底层驱动,成本较高,用户针对不同应用携带、使用多个介质也不方便,目前仅有少数银行试点。

实际上,安全问题制约了手机银行的进一步发展,CFCA(中国金融认证中心)最新发布的《2016 中国电子银行调查报告》<sup>[1]</sup>显示,安全因素是个人手机银行发展的主要障碍之一,如图 1 所示。手机银行、手机支付局限于小额支付领域,也与其安全保障措施的现状有关。

2 数字证书在智能终端应用需求

我国于 2005 年实施的《电子签名法》(2015 年修正)解决了电子环境下用户身份的法律地位问题,赋予电子签名与文本签名同等的法律效力。其中,基于 PKI(public

key infrastructure,公钥基础设施)/CA 的数字签名是最为成熟、应用最广泛的电子签名技术。

PKI 是基于公钥理论和技术建立起来的安全体系,是提供信息安全服务具有普遍性的安全基础设施<sup>[2]</sup>。该体系在统一的安全认证标准和规范基础上,提供了在线身份认证、加密和数字签名等服务,还提供了所必须的密钥和证书管理体系,是 CA 认证、数字证书、数字签名以及相关安全应用组件的集合。PKI 的核心是解决信息网络空间中的信任问题,确定信息网络中行为主体身份的唯一性、真实性和合法性,是解决网上身份认证、信息完整性和抗抵赖等安全问题的技术保障体系。PKI 可满足信息机密性、完整性、身份认证及不可抵赖性的要求,是电子交易的关键保障技术。

智能终端环境下应用数字证书的主要难题是私钥的

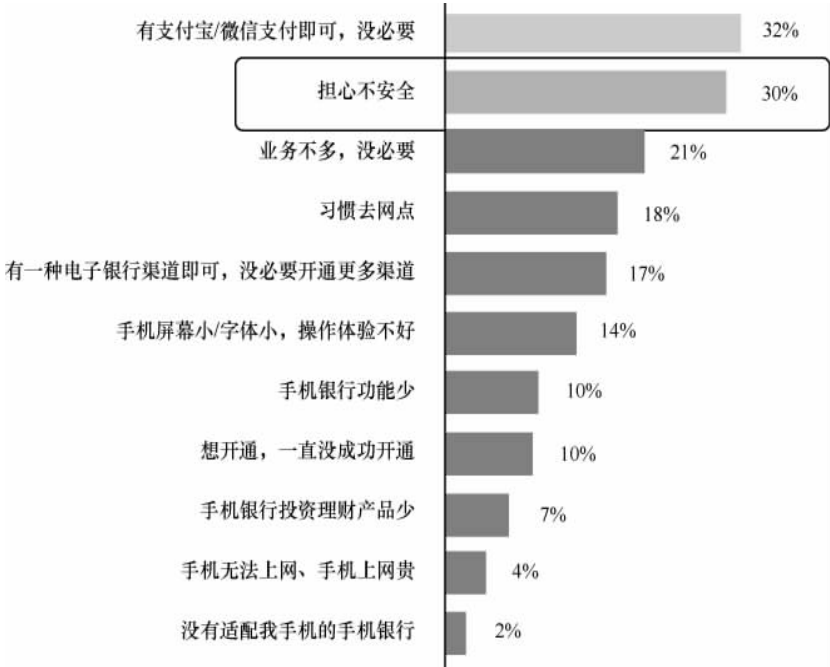


图 1 用户不开通手机银行的原因

安全存储及签名安全计算,智能卡虽可满足要求,但在智能终端应用受到限制。针对智能终端环境下接口、智能卡片资源有限的问题,GP(Global Platform)制定了多应用智能卡规范<sup>[3]</sup>,可同时运行、动态更新管理智能卡,赋予了发卡方与业务合作伙伴共享卡片的管理功能。GP智能卡架构如图2所示。

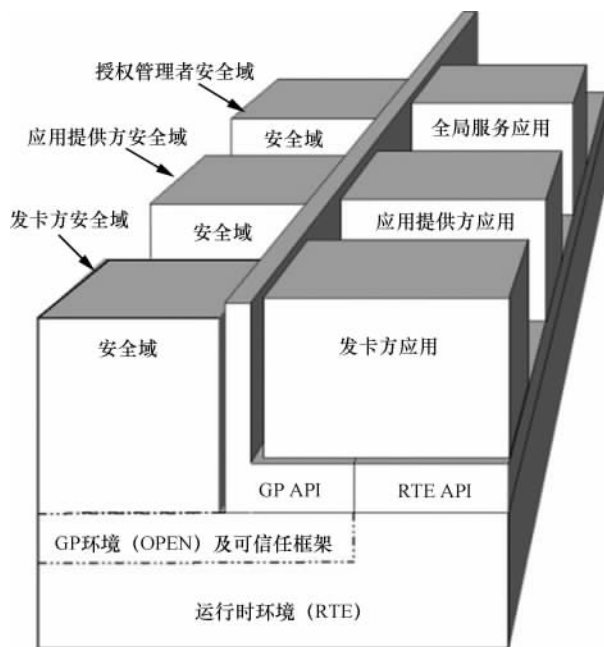


图2 GP智能卡架构

GP智能卡规范为多应用共存提供了灵活性,但也存在以下问题:多应用的动态下载、共同执行增加了智能卡自身的安全风险,运行环境或加载应用的漏洞可能被利用,危及其他应用,如德国 SRLabs 的 Karsten Nohl 在第30届混沌计算大会上演示了针对SIM卡的攻击,利用其漏洞,成功在卡上安装恶意 applet,获取卡内的关键信息;GP智能卡作为通用标准,重点关注多应用、多业务支持的通用性和灵活性,难以针对数字签名这类计算强度较高的应用进行优化,在多个数字签名应用同时安装的情况下,不仅功能重复、性能也难以优化;应用提供方须维护卡内 applet 程序,开发、维护成本较高。

本文旨在采用一种面向智能终端使用数字证书共享存储的安全方案,通过提供PKI服务支撑基础,降低智能终端各类应用使用PKI服务的门槛。

根据手机应用环境的特点和用户的需求,手机PKI支持方案,应能满足以下要求。

#### (1)多应用支持

由于接口限制,使用时更换手机key极为不便,甚至

不可能(如内置芯片)。随着移动互联网的发展,应用将越来越丰富,用户具有访问多个应用的需求,手机key应能满足该需求,提供多应用支持。

#### (2)可管可控

在支持多个PKI应用的情况下,不同应用之间相互隔离,可以确保使用的合法性、私钥的安全性,对方案能否应用至关重要。同时,对业务的可管可控、数字证书引入的控制、使用情况的监控,也是运营的关键。

#### (3)开放性

目前,国内有数十家开展PKI服务的第三方CA认证机构,也有不少实力较强的SP(service provider,服务提供商)自建了CA,为内部应用或自己开展的业务提供PKI支持。运营商不应也不可能限制SP对CA的选择,因此方案应具有开放性,不能局限于对某个CA的支持。

#### (4)标准化

根据开放性的要求,手机key应遵循标准,提供基于X.509标准CA证书及RSA、SHA-1等主流算法的支持。

#### (5)其他要求

方案改造和管理的工作量、使用的方便性,也是方案能否吸引SP和用户的重要因素,因此,应尽量减少SP改造和管理工作、提高用户使用的方便性。

### 3 基于共享式存储的智能终端数字认证方案

本文将数字证书私钥的共享式存储介质称为手机key,手机key支持多组证书,通过平台统一管理,为多个应用共享使用。在方案提供的PKI的支持下,SP可方便地提供基于PKI的身份认证、交易签名、数据加密功能,提高应用的安全性,如图3所示。

手机key可以是外置式的智能卡,如SD/TF、mini USB、蓝牙接口的智能卡、手机SIM/UIM卡,或内置的安全芯片,如TrustZone安全区。提供的主要功能包括以下几点。

#### (1)证书加载

将SP的证书加载到手机key,并生成对应的个人公私钥对、加载经签名的个人证书;手机key可独立存储多组证书,为多个应用服务。

#### (2)身份认证

用户与SP应用使用数字证书相互验证对方身份,其中,客户端采用数字证书和PIN码或指纹识别等双因素认证。

#### (3)交易签名

对客户的关键交易信息进行数字签名,确保交易的不

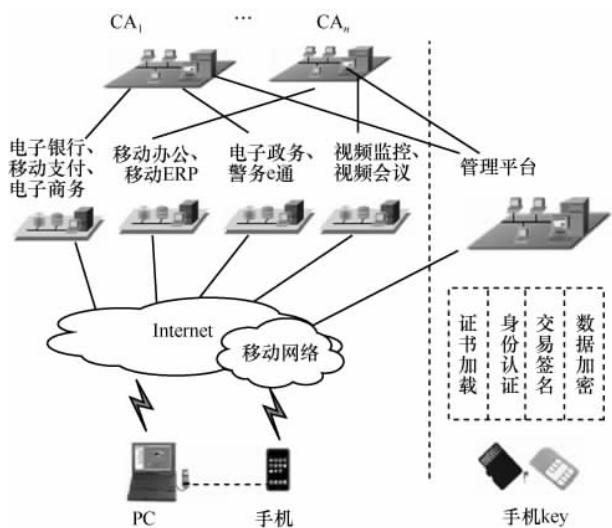


图3 基于手机key的PKI应用架构

可抵赖性。

#### (4)数据加密

利用公钥算法为用户安全分发密钥,在特定的使用场合,可扩展移动终端的计算能力,支持符合国家密码管理要求的加密算法。

为支持多个SP共享,手机key应能存储多组数字证书及其私钥。同时,由于多个SP具有访问手机key的权限,对SP证书的有效管理,包括加载、使用的权限管理,以确保证书和私钥的安全性,成为方案的关键。本方案采用多个数字证书组和SP准入认证机制来实施对SP的管理。

证书组包括SP证书、SP颁发给用户的个人证书及私钥,是用于个人和SP间相互认证的凭证。证书组存储于手机key的安全存储区,其中,私钥在卡内生成,且不能从卡内读取出来。

#### (1)SP证书

由CA颁发给SP的数字证书,私钥由SP保存,用于验证SP身份。SP在使用手机key进行加密或签名前,必须出示身份信息。手机key用存储的证书验证SP身份,通过后才能为SP提供加密和数字签名等功能。

#### (2)客户证书/私钥

SP或由SP信任的CA颁发给用户的数字证书及私钥,在用户访问SP时提供身份验证和交易签名等功能。

#### (3)管理证书

管理证书组是特殊的证书组,预制于手机key中,作为SP准入控制机制的可信根。

智能卡支持多组证书,证书组的存储形式见表2。

表2 手机key证书示意

| 证书组                 | SP证书               | 个人证书/私钥                    |
|---------------------|--------------------|----------------------------|
| 管理证书组               | 管理证书               | key管理方颁发的个人证书/私钥           |
| SP <sub>1</sub> 证书组 | SP <sub>1</sub> 证书 | SP <sub>1</sub> 颁发的个人证书/私钥 |
| ...                 | ...                | ...                        |
| SP <sub>n</sub> 证书组 | SP <sub>n</sub> 证书 | SP <sub>n</sub> 颁发的个人证书/私钥 |

初始状态下,手机key仅包括管理证书组。为了对SP实施有效的管理、确保用户证书的安全性,方案引入了SP准入认证机制:只有经key管理方认可、通过认证的SP,才能使用手机key提供相应的服务。实现上,通过SP证书组的加载来实施准入控制,即SP证书在加载进手机key之前,必须经过管理平台的认证。

认证流程如图4所示,具体有以下步骤。

**步骤1** 初始状态下,手机key内置管理证书组,手机与管理平台间建立初始信任关系。

**步骤2** SP与key管理方签署协议,允许其使用手机key开展基于PKI的服务,SP系统与管理平台建立信任关系。

**步骤3** 终端与SP首次通信时,SP身份须经管理平台验证,通过后,手机key加载SP证书,建立对SP的信任。

**步骤4** 手机key基于对SP的信任,接收SP指令,生成对应于该SP的个人证书公私钥对,经CA签发后,按传统流程(如客户号、验证码下载)加载个人证书到手机key,建立与SP的双向信任关系。

此后,SP在需要用户终端使用手机key提供的服务时,提供身份验证信息,手机key验证后,即可使用其加密、数字签名等功能。

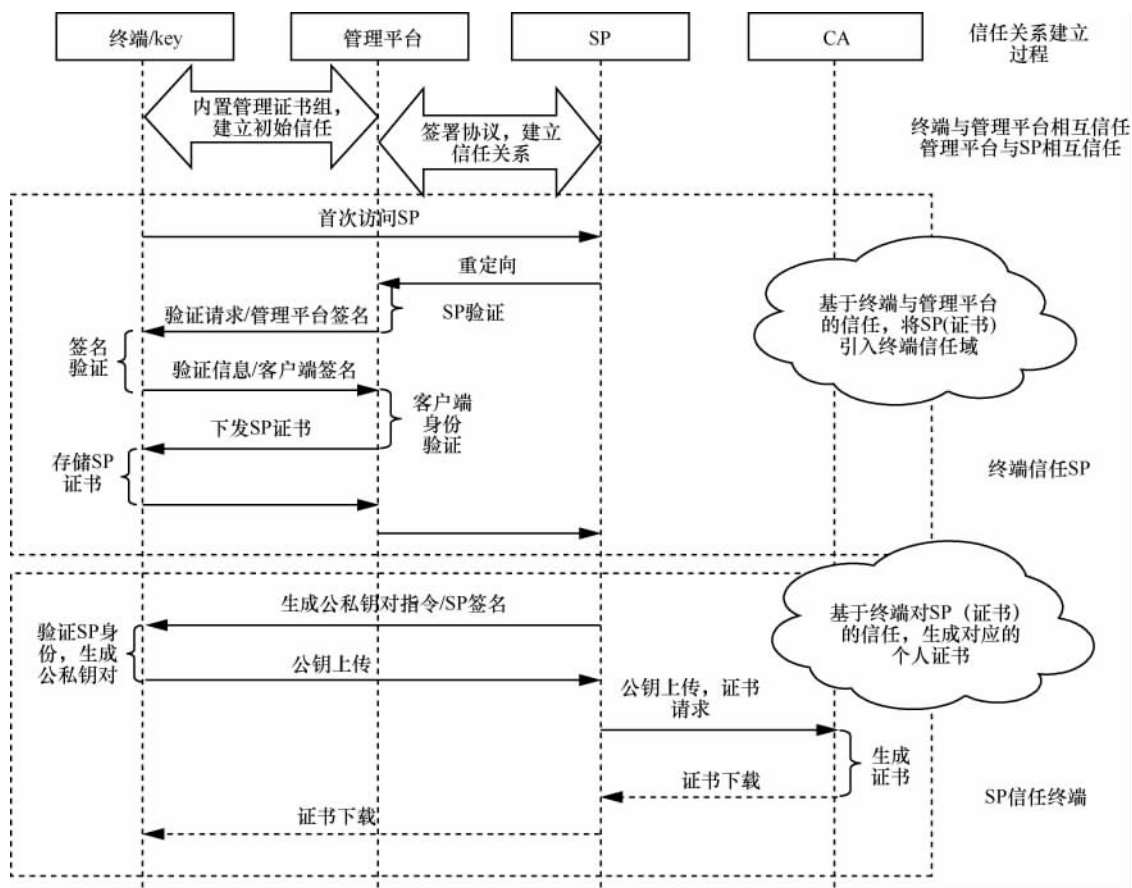
## 4 安全性分析

本方案为SP开展基于PKI的服务提供支撑基础,以提高SP应用的安全性,因此,方案自身的安全性尤为重要,尤其是手机key的共享机制,允许多个SP证书共存于同一个存储介质,对安全性具有更高的要求。

方案在充分利用PKI、智能卡安全机制的基础上,采用了信任链传递机制将SP证书组加载到手机key中,并在证书加载和使用过程中,采用双向认证、双因素认证等多种安全措施。以下分别对信任链传递、双向认证、防重放攻击等关键安全机制进行分析。

### 4.1 信任链传递

所谓信任链传递机制,是利用key管理方的管理证书





卡内生成,私钥存储、计算都在卡内完成,永不出卡,不允许从外部读取、篡改,可确保其安全性。

## (2) 用户身份验证

个人证书颁发时,通过用户的参考号、授权码(简称两码)来验证用户身份,两码采用传统的 PKI 安全发放渠道获得。该渠道一般为离线方式,用户事先到 SP 处申请 PKI 安全服务,SP 审核用户身份后,将两码以密封信件交给用户。用户请求签署个人证书时,SP 据此确认用户身份,将用户的公钥与其提交的个人信息进行关联。两码具有有效期,且仅能使用一次,SP 和用户需共同保证两码发放的安全。

## (3) SP 身份验证

SP 下发指令前,均需对指令进行签名,手机 key 收到指令后首先验证消息签名,确认消息来源可靠。

## (4) 公钥防篡改

数字证书的防篡改机制是由 CA 签名建立的,但在签署之前,公钥存在被篡改的风险。为此,采用以下两个措施来防范:

- 要求 SP 与终端之间建立安全连接,如采用 HTTPS,公钥签名请求与用户身份验证在同一个会话中完成,这些机制可降低公钥被篡改的风险;
- 手机 key 在接收到 SP 加载证书指令、验证消息可靠后,进一步检查证书的公钥与发送前的原始公钥的一致性,由于原始公钥存在卡内,外部无法篡改,因此,只要两者相同,可以确认公钥未被篡改,从而确认个人证书的有效性;同时,证书经 CA 签署之后,下发过程中可防篡改,因此,可确认 SP/CA 保留的证书未被篡改,是与用户真实身份相符、与手机 key 私钥对应的证书。

综上所述,本文方案可以保证运营商证书组、SP 证书的加载和个人证书的颁发过程的安全性,确保只有合法的 SP 证书以及该 SP 颁发的个人证书才能加载到手机 key。

## 4.2 双向认证

由于手机 key 供多个 SP 共享使用,必须能够识别并隔离不同 SP 的请求,以选择对应的证书组,为此,SP 发送指令、要求手机 key 提供服务前,须提供自己的身份信息,即 SP 用其私钥对所发送的指令签名。手机 key 接到消息后,首先验证消息的合法性,确认消息来源于可信的 SP,然后才选择该 SP 颁发的个人证书及私钥提供身份认证、数字签名等服务。

双向认证机制在隔离识别 SP 证书的同时,也提高了 SP 应用的安全性,为用户提供防范钓鱼攻击的手段。

## 4.3 双因素认证

手机 key 存在丢失的可能,对于长期在线的 key,还可能被远程控制。为防范盗用风险,需采用双因素认证,验证使用者身份。常用的是 PIN 码保护,但 PIN 码存在泄露风险,甚至可被恶意程序自动操作。除了所持有的物品(手机 key)、所知道的内容(PIN 码),双因素认证还可对使用者所拥有的特征进行验证,如指纹等生物特征识别技术,目前在中高端手机上已广泛使用,在安全环境中,采用手机 key+生物特征识别技术的验证方案,可提升验证过程的安全性和便利性。

以指纹识别为例,方案的处理过程如图 6 所示。

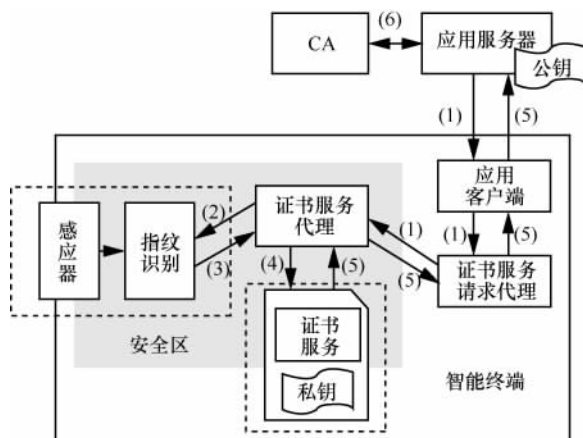


图 6 双因素认证处理过程

系统组件包括网络侧的应用服务器、CA 中心,终端侧的应用客户端、证书服务、指纹识别服务以及证书服务代理等组件,其中,私钥存储、证书服务、指纹识别服务等运算过程在可信执行环境(TEE)、TrustZone、SD/TF 智能卡等安全环境完成。

以身份验证为例,典型的处理流程如下:

- (1)应用客户端与服务器进行正常交互;
- (2)验证环节,应用服务器生成随机字符串、发起身份验证请求,应用客户端将该请求经代理发送给安全环境的证书服务代理;
- (3)证书服务代理将请求发送给指纹识别服务,并提示用户进行操作;
- (4)用户完成指纹识别验证,通过后,将结果反馈给证书服务代理;

(5)证书服务代理根据指纹验证结果,请求证书服务;

(6)证书服务对请求内容,即随机字符串等内容进行签名,并将签名结果经客户端返回给应用服务器;

(7)服务器利用证书公钥对结果进行验证,从而确定用户身份。

本文方案中,数字证书私钥存储、服务请求、运算过程在安全环境中进行,保障证书私钥的安全性。同时,由于数字证书加解密、签名等服务前须经指纹识别验证用户身份,指纹特征采集、验证过程在安全环境中,确保是由用户本人操作,从而可保证数字证书签名的有效性,防范数字证书一直在线以及双因素认证失效、证书被恶意程序盗用等风险,兼具了公钥技术的安全性和指纹识别的便利性。

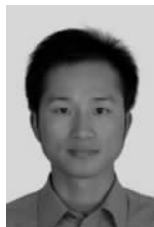
## 5 结束语

本文提出的基于共享式存储的智能终端数字认证方案,通过管理平台对安全介质的管控及信任链传递机制,建立 SP 与用户的信任关系,实现数字证书的远程写入,在单一的手机安全介质中实现多数字证书的共享,为 SP 提供基于 PKI 的安全服务,降低手机上使用数字证书进行应用安全保障的难度。最后从信任链传递、双向认证、双因素认证等方面分析了方案的安全性,并通过与指纹识别的结合,提升用户使用的方便性。

## 参考文献:

- [1] 中国金融认证中心. 2016 中国电子银行调查报告[R/OL]. (2016-12-08)[2017-01-16]. <http://www.199it.com/archives/544560.html>. 2016.
- CFCA. 2016 China e-bank survey report[R/OL]. (2016-12-08)[2017-01-16]. <http://www.199it.com/archives/544560.html>. 2016.
- [2] 关振胜. 公钥基础设施 PKI 与认证机构 CA [M]. 北京: 电子工业出版社, 2002.
- GUAN Z S. PKI & CA security institution [M]. Beijing: Publishing House of Electronics Industry, 2002.
- [3] Global Platform. Global Platform 卡片规范[S]. 2006.
- Global Platform. Global Platform card specification[S]. 2006.

## [作者简介]



**刘国荣**(1978-),男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为移动互联网安全、云计算安全。



**刘东鑫**(1985-),男,中国电信股份有限公司广州研究院工程师,获 CCIE、CISSP 和 CISA 等认证,主要研究方向为网络与信息安全、大数据安全。



**汪来富**(1976-),男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为大数据安全、云计算安全、网络安全。



**沈军**(1976-),女,中国电信股份有限公司广州研究院高级工程师,主要研究方向为云计算大数据安全及移动互联网安全。



**金华敏**(1972-),男,中国电信股份有限公司广州研究院高级工程师,主要研究方向为 IP 网、云计算、大数据安全、网络安全。