



基于 SIM 卡的金融应用移动数字签名业务研究

胡 博,严斌峰,仇剑书,董双赫

(中国联合网络通信有限公司研究院终端与测试实验室 北京 100032)

摘 要:随着智能终端和移动互联网的快速发展,在网上银行等行业应用中使用移动终端进行用户认证的方式愈发普及。传统的 USB key 用户认证方式逐渐被基于移动终端的用户认证方式取代。从移动运营商角度出发,研究分析了利用移动终端和 SIM 卡实现金融类应用用户数字签名认证的技术要求,梳理了基于智能终端和智能卡的安全技术,提出了基于电信智能卡的金融类应用用户签名和身份认证的技术架构和业务流程。

关键词:智能卡;数字签名;认证

doi: 10.11959/j.issn.1000-0801.2015157

Research on SIM Card-Based Mobile Digital Signature and Authentication for Financial Services

Hu Bo, Yan Binfeng, Qiu Jianshu, Dong Shuanghe

(Terminal and Testing Lab., Research Institute of China United Network Communications Group Co., Ltd., Beijing 100032, China)

Abstract: With the development of smart phones and mobile internet, it is a trend that leveraging mobile devices to perform user authentication for cross industry application, such as electric bank. Traditional USB key based digital signature and authentication has been replaced by authentication based on mobile devices. Requirements for mobile digital signature and authentication method based on smart phones and SIM card were analyzed, architecture and service procedures for SIM card-based mobile digital signature and authentication were proposed.

Key words: SIM card, digital signature, authentication

1 引言

随着计算机技术的高速发展,社会已步入网络经济时代。对于金融业务,移动互联网的快速发展,缩短了其交易成本和时间,拉近了金融行业与用户的距离。目前,无论是个人还是企业,对电子银行已经逐步认可和接受,但是安全问题一直使用户心存顾虑,希望能在便捷操作的同时保

障网上银行交易安全。

现阶段,USB key 签名认证方式在网上银行应用十分广泛。通过 USB key 双钥加密,私钥安全地保存在 key 中,在网络应用的环境下,可以更安全地保障用户的密码信息,从而弥补动态密码锁单钥加密的一些缺陷。然而,随着移动智能终端的快速发展和移动互联网的普及,手机购物、网上交费等新型消费形式的出现,个人终端也提出了

收稿日期:2015-01-28;修回日期:2015-06-12

论文引用格式:胡博,严斌峰,仇剑书等. 基于 SIM 卡的金融应用移动数字签名业务研究. 电信科学,2015157

Hu B, Yan B F, Qiu J S, *et al.* Research on SIM card-based mobile digital signature and authentication for financial services. Telecommunications Science, 2015157



对加密和数字签名的新需求。原有形态的 USB key 在便携性、易用性和兼容性方面已经不再适应移动互联网业务的发展。网上银行用户认证的另外一种方式——短信认证,由于明文方式传输和存储,同样存在着安全缺陷,目前仅是 USB key 签名认证的补充方式。

与此同时,SIM 卡作为移动运营商的用户侧安全硬件,一直是移动用户信赖的实体。随着智能卡技术的发展,SIM 卡的功能也不断增强,不仅能提供运营商网络鉴权能力,而且能提供基于智能卡的安全能力开放,为金融业务在移动场景下的用户签名和认证提供技术手段。充分利用 SIM 卡的安全计算能力,不仅能帮助金融行业进行移动场景下的用户认证和签名,而且有利于基于运营商智能卡构建面向安全的应用生态系统,从而提高运营商网络和业务的地位和价值。

本文从移动运营商角度提出利用电信智能卡和运营商网络构建移动用户签名认证的技术架构,以运营商网络平台为核心,以终端为用户入口,面向多金融业务系统实现了端到端的解决方案,从而弥补 USB key 和目前短信认证方案的不足,面向金融业务提供端到端的安全解决方案。

2 金融业务用户认证技术现状

2.1 传统 USB key 方式

网上银行应用中,USB key 作为网络用户身份识别和数据保护的“电子钥匙”,是目前用户最普遍的签名认证方式。USB key 的使用方法是,当登录网银系统的时候,在电脑上插入 USB key,然后输入用户 PIN 码,若验证通过,则可以进行相关交易和账户操作。使用硬件进行身份认证,有效防止了非法用户窃取存储在用户硬盘上的身份认证信息。

但这种方式存在一定缺陷。首先,在安全性方面,目前 USB key 通常采用 PIN 码保护方式,每个 USB key 都有用户自设定的 PIN 码,签名人在使用数字签名时需要在一台终端上输入 PIN 码进行确认,此过程体现了签名人的主体意愿。但是,输入 PIN 码这一过程所依赖的客户端操作系统通常不是可信计算环境,用户认证请求的发起和确认均在这一环境下完成,这种方式无法从根本上保证 USB key 安全体系的完整性;另外,PIN 码无法和签名人主体形成实时关联,是一种客观存在的密码,若密码被盗或猜中便失去了和签名主体的唯一关联性。其次,在易用性和兼容性方面,用户需要随身携带 USB key 才能够进行数字签名。USB key 依赖于具有 USB 接口的 PC 机,通常仅适用于 Windows 等主流操作系统,并不适用于移动终端。此外,每

个金融业务系统都发行和管理自己的 USB key,拥有多个银行账户的用户须随身携带多个 USB key,这种方式给用户带来不便。综上,基于 USB key 的签名认证方式,不仅存在着安全隐患,同时在易用性和兼容性方面也存在一定缺陷。

2.2 短信认证方式

短信认证方式是当前网银系统认证用户的重要技术方式之一。当用户操作网银进行交易时,系统向用户注册的移动终端发送一次性、短期有效的认证口令。用户仅可以使用该口令完成一次认证,不能重复使用该口令。短信认证方式可以更精确地确定用户的身份。短信认证从连接上与网银所在的互联网形成隔离,在安全方面具有一定的优势。

但是这种方式同样具有缺陷。在安全性方面,短信的传输和存储使用明文方式,存在口令被窃取的风险。由于认证口令的发送和接收需要签名人手动读取进行操作,短信认证方式可能被钓鱼网站或者网址嫁接等技术手段进行攻击而导致安全隐患。此外,若用户手机遗失,也可能造成认证口令被窃取。目前短信认证方式在安全性方面仅仅是 USB key 签名认证方式的补充。另外,在易用性方面,与 USB key 相比较,虽然不需要单独的硬件,需要用户操作手机读取短信并且手动输入网银交易界面,不易使用。因此,基于短信认证的方式在安全性和易用性方面同样存在不足。

2.3 有待解决的问题

综合上述 USB key 和短信认证两种主流的金融业务认证方式,利用移动终端完成金融应用移动数字签名认证需解决以下几个问题:

- 在保证效率的前提下,提供足够的安全性;
- 利用移动终端完成签名认证的过程应减少用户操作,提升用户易用性;
- 为提供便携性,应充分利用同一个硬件(如搭载电信智能卡的移动终端)完成跨平台的金融业务认证,即支持多家银行的业务请求。

2.4 现有基于 SIM 卡的认证技术研究

现有针对基于 SIM 卡进行认证服务的研究包括动态口令技术^[1]。用户使用基于 SIM 卡动态口令终端,SIM 卡中内置密码算法等数据,每次使用时产生动态口令。认证服务器系统接收到该动态口令后,使用相同算法和该终端密钥信息计算正确的动态口令,将二者进行比较,从而判断出该口令是否正确。此方法合理地利用电信智能卡完成用户认证技术,但使用动态口令无法规避钓鱼网站的安全风险。除此之外,现有基于 SIM 卡认证技术缺乏面向多金融

业务系统的针对性研究。

3 基于电信智能卡的数字签名技术架构和业务流程

3.1 业务场景

结合现有的金融业务签名认证技术和智能终端/智能卡的安全技术,笔者认为基于电信智能卡的金融应用移动数字签名认证业务场景包括以下几种。

(1)安全认证应用的发行

移动用户通过金融业务系统(如银行)柜台签署业务开通,获取授权码。用户通过运营商营业厅或者客户端向智能卡下载认证应用。

(2)安全认证业务签约

移动用户通过移动客户端或智能卡菜单选择银行进行业务开户,设定本机 PIN 码。

(3)安全认证业务执行

当移动用户通过网上银行或手机银行进行支付转账等需要进行用户签名认证操作时,金融业务系统向跨平台认证服务平台认证请求,通过运营商网络请求发送至移动终端,终端通过客户端或者智能卡 STK(SIM card tool kit, 用户识别应用发展工具)菜单呈现操作的具体信息,用户输入(2)中设定的 PIN 码后对交易操作进行签名,签名数据通过运营商网络发送至认证服务平台,通过认证后将结果返回至金融业务系统完成支付操作。

(4)安全认证业务的退订

移动用户通过移动客户端或智能卡菜单选择银行进

行业务取消和退订。

(5)安全认证应用更新

当应用进行更新时,应用平台通过运营商网络发送应用更新通知,通过移动客户端进行应用的下载更新。

3.2 技术架构

本文设计了一个基于电信智能卡的金融应用移动数字签名认证平台总体技术架构,如图 1 所示,本系统设计从业务应用到终端进行了层次划分,包括以下 4 个层次:业务域、业务聚合域、运营域、终端域。4 层结构按照业务逻辑独立部署,以运营商网络平台为核心,以终端为用户入口,面向多金融业务系统实现了端到端的解决方案。

(1)业务域部署一个至多个金融业务系统,负责认证业务的发起。

(2)业务聚合域部署跨平台金融应用服务平台,负责聚合不同金融业务系统的认证业务请求。该平台可由运营商部署并运营,也可以由可信的第三方机构部署并运营,可介于运营商网络和金融业务系统之间。

(3)运营域部署运营商卡管理平台(TSM 平台)、智能卡安全应用管理平台、智能卡安全访问控制平台、短信平台。

(4)终端域部署智能终端和智能卡,其中智能终端负责执行终端层面的智能卡访问控制和通过 STK 菜单或 SIM Alliance (智能卡行业标准组织)定义的 OM API 方式调用卡应用,完成业务呈现和机卡交互;智能卡负责执行智能卡层面的卡安全应用访问控制和智能卡安全认证应用。其中智能卡安全认证应用实现了安全认证的业务逻辑。

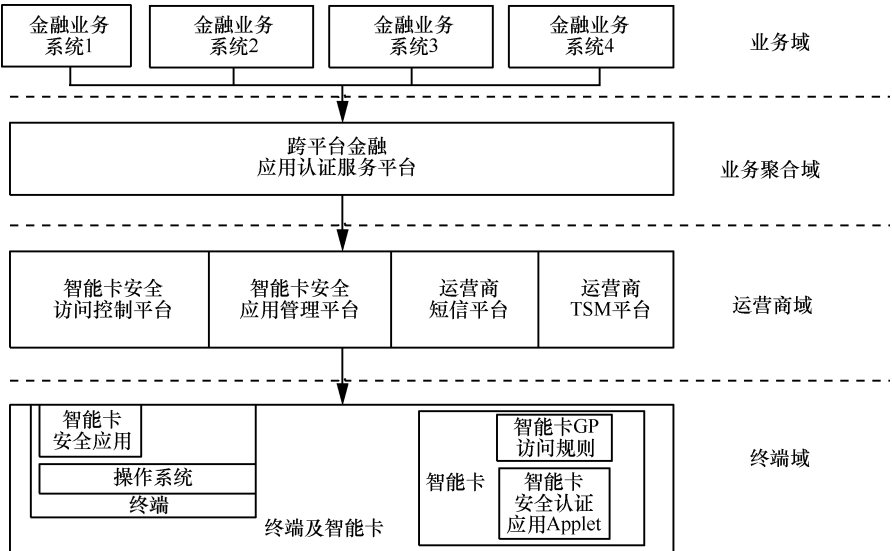


图 1 总体架构



从终端域展开看,包括移动终端和智能卡两个功能实体。其中终端中部署安全认证应用和操作系统层面的机卡访问通道和访问控制功能单元,保证仅有授权的安全认证应用可以通过机卡访问通道访问智能卡中的安全认证应用。访问控制功能单元将根据安全认证应用的散列值和应用包进行规则匹配,从而进行终端侧的访问控制。智能卡中部署符合 Global Platform 标准^[2,3]定义的访问控制规则,保证只有通过该规则的应用才能访问卡上的安全认证应用。每个安全认证应用安装在不同的辅助安全域,保证数据存储安全。

根据安全认证应用所兼容的终端和呈现方式可以有两种部署选择:“单独卡应用”方案和“客户端+卡应用”方案。

- “单独卡应用”方案:智能卡安全认证应用以 Applet 方式部署于智能卡某一专属辅助安全域中,卡应用通过标准 STK 菜单方式呈现,此方案的优点在于适用于所有支持智能卡 STK 应用的移动终端,缺点在于用户界面不够友好,STK 菜单的呈现依赖于操作系统实现,用户的某些操作终端可能导致业务认证界面消失。
- “客户端+卡应用”方案:智能卡安全认证应用以 Applet 方式部署于智能卡某一专属辅助安全域中,卡应用通过标准的面向应用的机卡访问通道(OM API)和安全认证应用进行呈现。此方案的优点是用户界面友好,开发者可以根据业务逻辑设计图文并茂的交互界面。缺点在于,并非所有终端都支持 OM API,因此无法适用于所有移动终端。

3.3 关键技术

3.3.1 用户签名认证

用户数字签名认证采用 PKI(公钥密码体制^[4]),具体流程如图 2 所示,实现了基于终端和智能卡的数字签名。当交易请求得到用户确认并输入 PIN 码后,智能卡通过 PIN 码校验后将交易信息生成散列,进而使用存在于智能卡安全认证应用中的私钥进行加密形成签名数据。上述过程由智能卡安全认证应用完成。此签名数据连同用户 ID、交易确认信息同时上报至认证平台。上报过程可依赖两种方式:短信方式或使用客户端基于 IP 网络进行数据传输。认证平台收到签名数据后通过用户 ID 提取证书,同时对数据做散列处理,对签名数据使用公钥进行解密,如解密后的

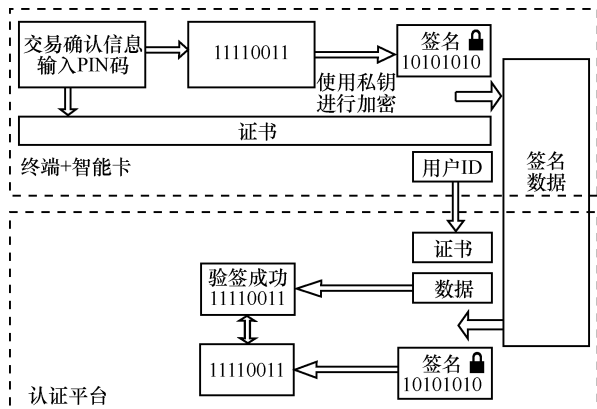


图 2 用户签名认证

数据与前散列值相同则验签通过。本方案中利用终端实现用户输入 PIN 码确认的用户交互过程,如用智能卡实现 PKI 架构中的数据加密环节,在认证平台实现解密验签环节。本方案一方面使用 PIN 码保护了本地证书数据,同时高效地利用了智能卡的安全计算能力,实现了跨平台的数字签名认证。数字签名认证过程使用的计算和通信环境独立于交易过程,只要给用户足够的安全提示,便可最大程度地降低安全风险。

3.3.2 卡应用访问控制

Global Platform^[2,3]标准组织定义了智能卡应用访问控制模型,本研究利用该模型实现了终端应用访问智能卡安全认证应用时的访问控制,以保证在“客户端+卡应用”模式中卡应用数据不被非法应用读取和篡改。如图 3 所示,Global Platform 定义的访问控制体系中,对于移动终端上的一个客户端应用而言,可以通过手机底层的 Open Mobile API^[5]访问智能卡中的一个应用。Open Mobile API 是 SIM Alliance 针对 GPAC 规定的 API,制定的具体化定义。智能卡中会存储是否允许手机客户端应用访问卡片应用的一个规则。Global Platform 技术规范要求中定义了卡安全数据访问控制的通用机制。该机制对于任何卡安全数据都可用。它支持多个应用方的应用程序管理并允许每个应用方为其加载到卡内的应用设置访问规则。卡应用访问规则数据存储在 SIM 卡中,供设备上的访问控制执行器使用。操作系统访问控制执行层将从卡安全应用里取回访问规则然后运用这些规则来控制应用客户端对卡安全应用的访问。

3.4 业务流程

3.4.1 应用发行

智能卡安全认证业务中,应用发行的主要目的是将安

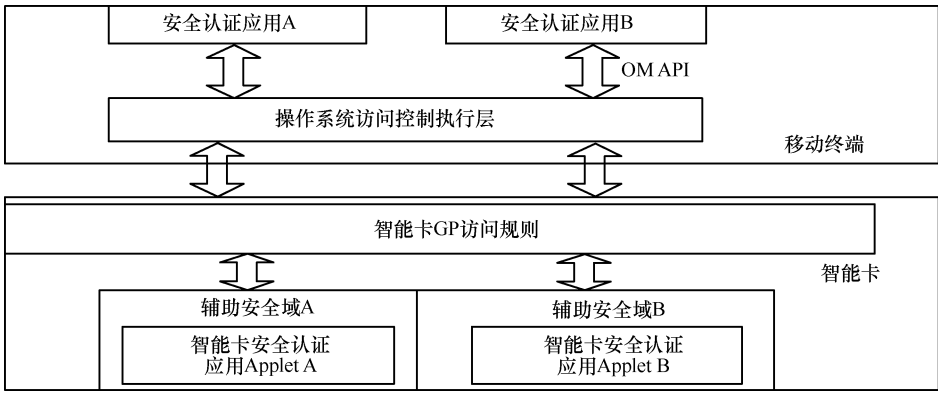


图 3 终端域安全架构

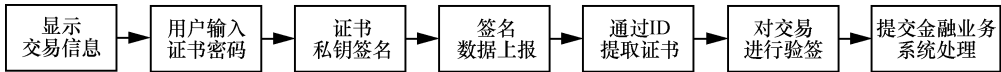


图 4 交易认证业务流程

全认证应用通过运营商网络写入智能卡辅助安全域中。这一过程涉及运营商 TSM 平台、智能卡安全应用管理平台。其中,安全应用管理平台扮演二级 TSM 的角色,对安全认证应用所在安全域进行管理,负责在其安全域内下载、安装、实例化、个性化安全认证应用 Applet。应用的发行可以采用灵活的方式,既可以在运营商营业厅使用 POS 方式下载卡安全认证应用,也可以通过移动互联网方式利用手机安装客户端进而下载卡安全认证应用,后者既可以在运营商营业厅完成,也可以在银行营业厅完成,甚至可独立于上述营业厅在任何有互联网接入之处完成。

3.4.2 管理流程

智能卡安全认证应用业务的管理功能包括用户以实名身份通过智能卡 STK 菜单或手机客户端界面进行业务开通。首先,用户需要以实名方式(身份证号)进行业务注册,获取并保存用户 ID;其次,用户在业务注册后需要选择银行进行签约并且下载银行证书至智能卡安全认证应用,这一下载过程可以通过 OTA(over the air)短信完成,也可以通过机卡访问通道由安全应用客户端完成。这种方式为业务部署提供了较大的灵活度,两种方式可以形成互补,当安全应用客户端可用时,可以节省短信通信成本,当终端无法连接 IP 网络时,OTA 短信可以确保完成证书下载。用户在证书下载后,有必要为其设置本地 PIN 码作为保护。

3.4.3 交易认证流程

在应用发行至智能卡并且用户开通了银行业务后,执行基于 SIM 卡的交易签名认证流程如图 4 所示:首先,金

融业务系统发送交易信息,终端收到并查看交易信息后提示用户进行主观确认,确认后输入证书密码,经过密码校验后,智能卡安全认证应用进行证书私钥签名生成签名数据,通过运营商网络发送签名数据至认证平台,平台通过用户 ID 在平台侧提取证书,并对签名数据进行验证,将验证的结果提交至金融业务系统处理。

4 结束语

本文研究和分析了目前金融业务用户签名认证技术问题,从移动运营商角度提出利用电信智能卡和运营商网络构建移动用户签名认证的技术架构,以运营商网络平台为核心,以终端为用户入口,面向多金融业务系统实现了端到端的基于 SIM 卡的金融应用移动数字签名业务方案。在该架构上利用了 Global Platform 定义的卡应用安全访问机制,同时定义了两种终端业务层面的认证呈现方式,进而梳理了基于智能卡的移动用户签名的应用发行流程、管理流程、交易认证流程。通过提供数字签名业务,拓展了智能卡安全技术和存储能力的使用价值,有助于构筑以智能卡安全能力为核心的生态系统和业务模式。

参考文献

1 张明杰. 基于 SIM 卡动态口令的互联网身份认证体系与应用. 电信科学, 2007, 23(12)
Zhang M J. Authentication system and application based on dynamic-password SIM. Telecommunications Science, 2007, 23(12)



- 2 Global Platform. Global platform card secure element configuration V1.0. <http://www.globalplatform.org/specificationdownload.asp>, 2015
- 3 Global Platform. Global platform device technology secure element access control V1.0. <http://www.globalplatform.org/specificationdownload.asp?id=7768>, 2013
- 4 刘知贵. 基于 PKI 技术的数字签名身份认证系统. 计算机应用研究, 2004(9)
Liu Z G. The system of digital signature authentication based on PKI. Application Research of Computers, 2004(9)
- 5 开放移动接口 V2.0. http://simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI3_1_.pdf, 2015
Open mobile API specification V2.0. http://simalliance.org/wp-content/uploads/2015/03/SIMalliance_OpenMobileAPI3_1_.pdf, 2015

[作者简介]



胡博,男,中国联合网络通信有限公司研究院终端与测试实验室工程师,主要研究方向为智能卡、智能终端、移动互联网应用等。

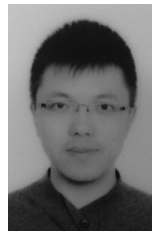
2015157-6



严斌峰,男,博士,中国联合网络通信有限公司研究院终端与测试实验室主任,主要研究方向为移动终端、智能卡、终端数据等。



仇剑书,男,中国联合网络通信有限公司研究院终端与测试实验室高级工程师,主要研究方向为智能卡、移动互联网应用、移动终端等。



董双赫,男,中国联合网络通信有限公司研究院终端与测试实验室工程师,主要研究方向为智能卡、智能终端、移动互联网应用等。

(上接 2015154-5)

- Fang J, Wu H, Bai S L. Virtualization security issues in cloud computing. Telecommunications Science, 2012,28(4):135~140
- 7 沈余锋,余小军. 云计算环境下虚拟化安全探讨. 电力信息与通信技术, 2013(11): 6~11
Shen Y F, Yu X J. Study of virtualization security in cloud computing. Electric Power Information and Communication Technology, 2013(11): 6~11
 - 8 余秦勇,童斌,陈林. 虚拟化安全综述. 信息安全与通信保密, 2012(11):41~46
Yu Q Y, Tong B, Chen L. Overview virtualized security. Information Security and Communications Privacy, 2012 (11): 41~46

[作者简介]



王笑帝,男,中国联合网络通信有限公司研究院云计算实验室工程师,主要研究方向为信息安全、云计算安全等。



张云勇,男,博士后,中国联合网络通信有限公司研究院副院长,中国通信学会、电子学会、计算机学会高级会员,主要研究方向为下一代开放网络、移动互联网及业务、云计算、智能终端等。



刘镒,男,博士后,中国联合网络通信有限公司研究院云计算实验室工程师,主要研究方向为认证安全、云计算、终端安全等。

张尼,男,博士后,中国联合网络通信有限公司研究院云计算实验室高级工程师,主要从事移动互联网安全、云计算安全、信息安全等领域研发工作。

于一鸣,男,北京邮电大学在读。

2015154-6