电子支付风险控制个人可信确认方案研究*

樊 凯[1],韩小军[2],汪 书[3]

(1.西安电子科技大学,陕西 西安 710126;2.睿丰宝科技有限公司,北京 102600;3.北京大学,北京 100871)

摘 要:通过研究电子支付业务风险的个人自主控制模式,分析了电子支付个人风险控制系统和个人可信确认基本过程,提出个人可信确认风险控制机制的密码应用需求。同时,设计了基于密码应用技术的个人可信确认方案,包括系统构成、使用的密钥、方案原理、个人可信确认报文、密码安全应用流程、密码应用相关安全技术要求等部分。该方案可供支付机构、电子支付个人风险控制领域相关系统和设备厂商作为技术参考。

关键词:电子支付;风险控制;个人可信确认;密码应用

中图分类号:TN918.9 文献标识码:A DOI:10.19358/j.issn.2096-5133.2021.01.002

引用格式:樊凯,韩小军,汪书. 电子支付风险控制个人可信确认方案研究[J].信息技术与网络安全,2021,40(1):10-14.

Research on personal trusted confirmation scheme for risk control of electronic payment

Fan Kai[1], Han Xiaojun[2], Wang Shu[3]

(1.Xi′an University of Electronic Science and Technology, Xi′an 710126, China;
2.Ruifengbao Technology Limited Company, Beijing 102600, China; 3.Peking University, Beijing 100871, China)

Abstract: Through the study of individual autonomous control mode of electronic payment business risk, this paper analyzes the electronic payment personal risk control system and the basic process of personal credible confirmation, and puts forward the password application requirements of personal credible confirmation risk control mechanism. At the same time, this paper designs a personal trusted authentication scheme based on cryptographic application technology, including system structure, key used, scheme principle, personal trusted authentication message, cryptographic security application process, cryptographic application related security technology requirements and so on. This scheme can be used as technical reference for payment agencies, electronic payment personal risk control systems and equipment manufacturers.

Key words: electronic payment; risk control; personal credible confirmation; cryptographic application

0 引言

在电子支付业务模式日趋多样化的背景下,个人用户的支付行为往往存在众多安全隐患,当前主要由支付机构协助个人进行统一风险控制[1]。为了适应多元个性化的个人风险控制需求,支付机构也陆续推出了用户可自主配置、自主操作的个人风险控制系统和设备。

本文面向基于个人可信确认的电子支付个人风险控制系统,提出了个人可信确认密码应用方案,包括系统构成、使用的密钥、方案原理、报文协议、密码应用流程、相关安全技术要求等内容。

1 电子支付个人风险控制系统概述

1.1 系统构成

电子支付个人风险控制系统主要由个人可信确认服务系统和个人可信确认设备构成,如图1所示。

电子支付个人风险控制系统主要分为:

(1)个人可信确认服务系统:接收支付系统发送的个人可信确认判断请求,经过个人可信确认判断后将判断结果返回给支付系统。

(2)个人可信确认设备:接收个人可信确认服

*国家重点研发计划项目“安全支付及其运行监管的关键技术”资助(2017YFB0802601)

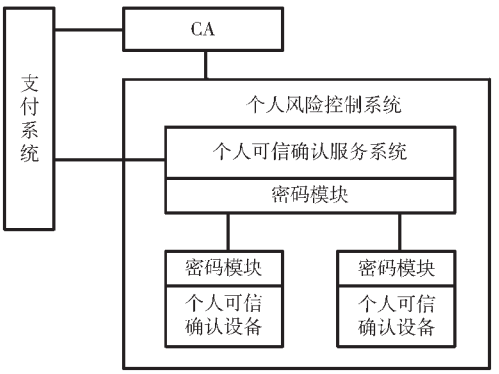

图 1 支付系统个人可信确认模型

务系统发送的需由个人控制或处理的个人可信确认信息,经由个人处理或确认完成后将结果返回个人可信确认服务系统,如个人可信确认策略设置、支付确认等。

支付系统、支付终端、CA(Certificate Authority)认证中心是电子支付业务的构成元素,作为个人风险控制系统的相关外部系统。

1.2 个人可信确认基本过程描述

个人可信确认基本过程可描述如下:

(1)个人用户在支付终端发起支付业务后,支付系统进行风险识别与判断;

(2)支付系统完成相关风险判断后,将最终是否支付提交个人风险控制系统;

(3)个人风险控制系统的服务系统根据用户个人设置的个人可信确认策略进行相关处理;

(4)支付系统收到个人风险控制系统返回的信息后,执行或中止该项支付。

1.3 密码应用安全需求

1.3.1 总体需求

电子支付个人风险控制系统密码应用安全的总体需求为:

(1)数据机密性

在支付系统个人可信确认过程中,需对个人可信确认服务系统与个人可信确认设备之间的数据传输进行加密保护。

传输用户或系统鉴别数据时,应以非明文(密文或杂凑值)形式传输,可采用密码杂凑算法、对称密码算法或非对称密码算法。

传输用户个人敏感数据和业务数据时,应以密文形式传输,可采用对称密码算法或非对称密码算法。

(2)数据完整性

在个人可信确认服务系统与个人可信确认设备之间传输用户鉴别数据、用户个人敏感数据、业务数据时,应计算和校验数据的完整性,可采用 SM3 密码杂凑算法。

(3)数据来源真实性

个人可信确认服务系统与个人可信确认设备之间传输用户鉴别数据、用户个人敏感数据、业务数据时,应计算和校验数据的真实性,可采用 SM3 密码杂凑算法。

(4)数据不可否认性

个人可信确认服务系统与个人可信确认设备之间传输用户鉴别数据、用户个人敏感数据、业务数据时,应确保该数据传输过程具有合法的抗抵赖效力,可采用数字签名和签名验证实现数据来源的身份鉴别。采用 SM2 椭圆曲线公钥密码算法进行数字签名和签名验证。

1.3.2 相关系统密码应用需求

相关系统密码应用需求主要为个人可信确认服务系统密码应用需求和个人可信确认设备密码应用需求。具体为:

(1)个人可信确认服务系统密码应用需求

个人可信确认服务系统向个人可信确认设备传输数据时,通过密码模块保障数据机密性、数据完整性、数据来源真实性和数据不可否认性。

(2)个人可信确认设备密码应用需求

个人可信确认设备向个人可信确认服务系统传输数据时,通过密码模块保障数据机密性、数据完整性、数据来源真实性和数据不可否认性。

2 个人可信确认密码应用方案

2.1 系统构成

本方案采用国家密码管理机构认可的支持 SM2、SM3、SM4 算法加密机作为个人可信确认服务系统的密码模块,采用支持 SM2、SM3、SM4 算法的安全芯片作为个人可信确认设备的密码模块,采用 CA 系统作为各密码模块的证书管理中心。

其中,个人风险控制系统中的个人可信确认服务系统、个人可信确认设备需要分别部署密码模块,提供密钥管理和密码运算服务。

2.2 系统使用的密钥

2.2.1 密钥种类

系统使用双证书认证体系的总体思路,即签名证书与加密证书。签名证书用于数字签名验证,加

密证书用于密钥协商。

系统使用的密钥总体划分为签名密钥、加密密钥、会话密钥三种类型。

2.2.2 使用的密钥

CA 系统使用认证机构公私钥,为个人风险控制系统提供证书签发和签名服务。

个人风险控制系统使用的密钥包括:个人可信确认服务系统的服务端签名公私钥、服务端加密公私钥、服务端会话密钥;个人可信确认设备的用户端签名公私钥、用户端加密公私钥、用户端会话密钥。

(1)服务端签名公私钥

服务系统公私钥由个人可信确认服务系统部署的密码模块采用 SM2 算法生成。

服务系统公钥提交至 CA 系统,用于申请服务系统证书、对协商会话密钥数据进行签名。

服务系统公钥导入个人可信确认设备密码模块。

(2)服务端加密公私钥

由个人可信确认服务系统的密码模块采用 SM2 算法产生,公钥导入个人可信确认设备。

用于对协商会话密钥数据进行加密。

(3)服务端会话密钥

由个人可信确认服务系统的密码模块采用 SM4 算法随机产生,用于个人可信确认服务系统和个人可信确认设备之间的通信加密。

(4)用户端签名公私钥

用户端公私钥由个人可信确认设备部署的密码模块采用 SM2 算法生成。

用户端私钥用于在个人可信确认设备对外通信时对数据进行签名或解密。

用户端公钥提交至 CA 系统,用于申请用户模块证书、对协商会话密钥数据进行签名。

用户端公钥导入个人可信确认服务系统密码模块。

(5)用户端加密公私钥

由个人可信确认设备的密码模块采用 SM2 算法产生,公钥导入个人可信确认服务系统。

用于对协商会话密钥数据进行加密。

(6)用户端会话密钥

由个人可信确认设备的密码模块采用 SM4 算法随机产生,用于个人可信确认设备和个人可信确认服务系统之间的通信加密。

2.3 方案原理

本方案采用国家密码管理机构指定的 SM2、SM3 和 SM4 算法,其中个人可信确认服务系统和个人可信确认设备之间采用 SM3 杂凑和 SM2 椭圆曲线公钥密码算法实现双向认证及会话密钥协商,用协商的会话密钥进行 SM4 加密的数据通信。个人可信确认通信包括服务端发起和用户端发起两种方式,本方案描述用户端发起方式,包含会话协商和数据传输两个过程。服务端发起方式与用户端发起方式原理相同。

用户端发起原理如图 2 所示,1~9 是会话协商过程,10~15 是数据传输过程。

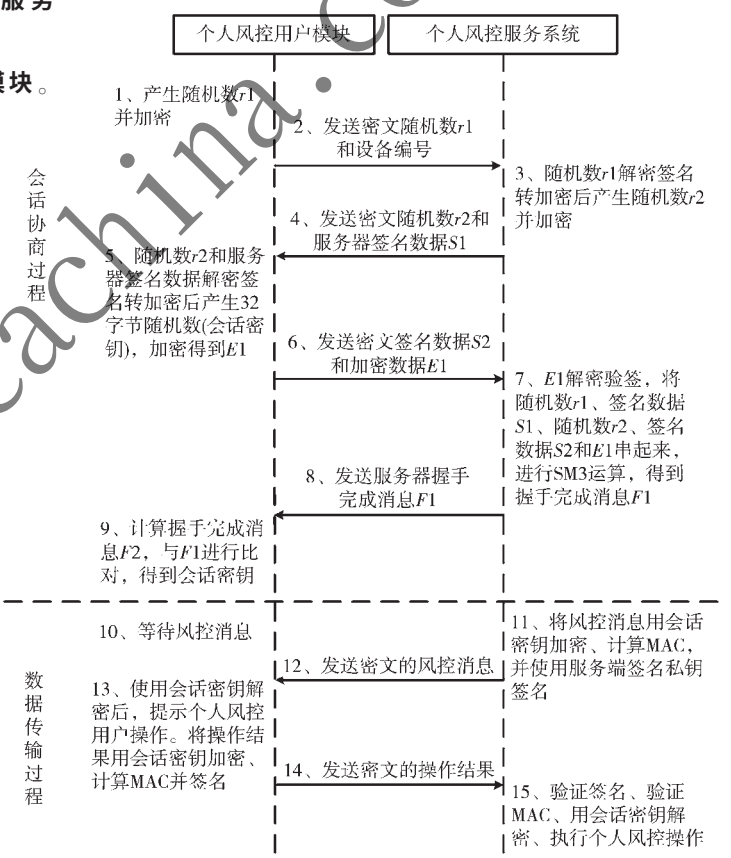

图 2 个人风险控制系统密码应用方案原理

(1)会话协商过程。该过程是个人可信确认设备与个人可信确认服务系统之间进行双向认证及协商会话密钥的过程。其中,双向认证过程使用用户端签名密钥和服务端签名密钥实现,协商会话密钥过程使用用户端加密密钥和服务端加密密钥实现。

(2)数据传输过程。该过程是个人可信确认设备与个人可信确认服务系统之间进行数据传输的过程。

2.4 个人可信确认报文

2.4.1 协议框架

协议框架如图 3 所示。

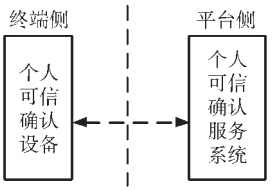

图 3 协议框架

在进行协议通信时,终端侧和平台侧分别提前生成 SM2 算法的设备证书和服务系统证书,在个人可信确认设备主动连接到个人可信确认服务系统时,先进行握手通信,个人可信确认服务系统获取个人可信确认设备中的设备证书和签名来验证其身份。同时个人可信确认设备获取个人可信确认服务系统的签名来验证服务系统的身份。

握手过程中,个人可信确认设备生成一组随机数作为主密钥,通过密钥交换算法与服务系统共享主密钥。每次通信的主密钥都是随机的,不可预测,增强了个人可信确认设备和个人可信确认服务系统通信的安全性。

握手结束时,个人可信确认设备和个人可信确认服务系统同时用共享的主密钥对一些随机因子进行哈希计算得到会话密钥。

2.4.2 协议报文

报文数据的逻辑结构包括:设备唯一标识、用户唯一标识、自定义信息和签名数据,它们都采用标签-长度-值(Tag-Length-Value,TLV)的格式。具体标签值不做规定。

将设备唯一标识、用户唯一标识和自定义信息按顺序串联得到原文信息。

在传输过程中,用会话密钥对原文信息进行加密得到密文信息;用发送方的签名密钥对原文信息进行签名,得到签名数据。

发送数据为密文信息和签名数据。

2.4.3 安全通信机制

安全通信机制参考标准 SSL 密码协议中的密钥交换协议。密钥交换协议是指让两方或多方在不安全的信道上协商会话密钥,从而建立安全的加密通信。

(1)安全保护

在安全通道上的数据传输过程中,为保证数据的安全性进行数据加密处理。具体操作为:用会话密钥对原文数据进行 SM4 的对称加密。

(2)数据合法性

在数据通信传输的时候,数据的来源合法性需要进行验证。具体操作为:发送方使用私钥对数据原文进行 SM2 签名;接收方需要发送方的公钥对签名信息进行 SM2 验签。

2.5 密码安全应用流程

2.5.1 密钥准备

密钥准备包括个人可信确认服务系统的服务端签名公私钥、个人可信确认服务系统的服务端加密公私钥、个人可信确认设备的用户端签名公私钥、个人可信确认设备的用户端加密公私钥的准备过程。

完成以上流程后,个人可信确认设备和个人可信确认服务系统方可进行数据传输过程。

2.5.2 数据传输通信

个人可信确认设备和个人可信确认服务系统之间进行数据传输过程时,双向通信,互为数据发送方和接收方,通信报文处理机制如图 4 所示。

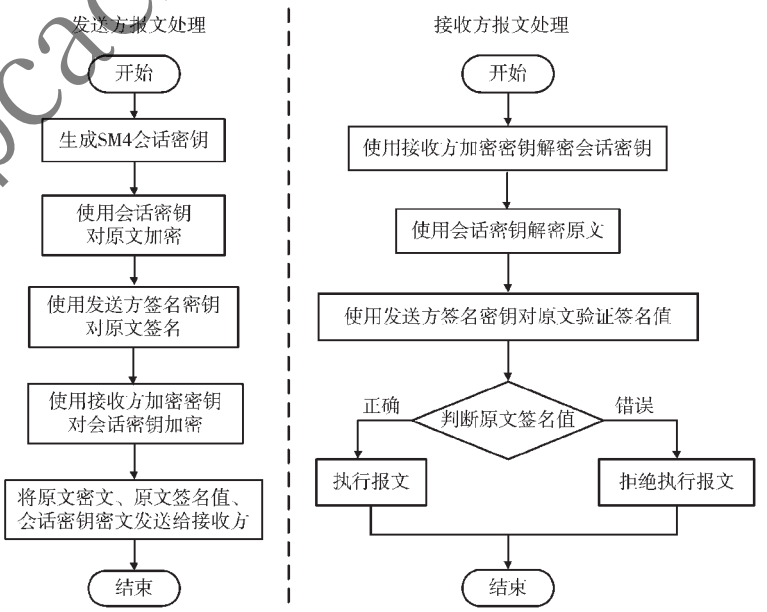

图 4 数据传输通信报文处理机制

(1)发送方报文处理

发送方生成 SM4 会话密钥并使用该密钥对原文进行加密处理;

发送方使用 SM2 签名密钥(私钥)对原文进行

签名处理;

使用接收方 SM2 加密密钥(公钥)对会话密钥进行加密处理;

原文密文、原文签名值和会话密钥密文作为报文进行通信。

(2)接收方报文处理

接收方接收到报文数据后,使用接收方 SM2 加密密钥(私钥)对会话密钥密文进行解密,解出会话密钥;

接收方使用会话密钥对原文密文进行解密,解密出原文;

接收方使用发送方公钥对原文和原文签名值进行验签,验签通过后进行业务处理。

该协议保障通信过程中原文报文的机密性、完整性、真实性以及不可否认性。

2.6 密码应用相关安全技术要求

2.6.1 密码设备安全技术要求

个人可信确认服务系统密码模块应满足 GM/T 0028-2014《密码模块安全技术要求》安全三级或以上安全等级[2]。

个人可信确认设备密码模块要求应满足 GM/T 0028-2014《密码模块安全技术要求》安全二级[2]。

2.6.2 密码算法安全技术要求

当使用静态口令时,应提示用户设置高强度的口令,宜定期更换。

当使用动态口令时,应遵循 GM/T 0021-2012《动态口令密码应用技术规范》[3]。

随机数生成器应符合 GM/T 0005-2012《随机性检测规范》的相关要求[4]。

当使用时间戳时,应符合 GM/T 0033-2014《时间戳接口规范》相关要求[5]。

当使用对称密码算法时,应符合 GM/T 0002-2012《SM4 分组密码算法》[6]、GM/T 0019-2012《通用密码服务接口规范》相关要求[7]。

当使用非对称密码算法时,应符合 GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》[8]、GM/T 0009-2012《SM2 密码算法使用规范》[9]、GM/T 0019-2012《通用密码服务接口规范》[7]。

当使用密码杂凑算法时,应符合 GM/T 0004-2012《SM3 密码杂凑算法》相关要求[10]。

3 结论

在电子商务和互联网金融业务蓬勃发展的时代潮流下,用户提出了越来越多的个性化风险控制需求。支付机构一方面通过大数据分析提升自身风险控制能力,另一方面也为用户提供自主配置风险控制策略、自主执行风险控制操作的便捷。支付机构在构建支付系统配套的个人风险控制系统时,应考虑用户终端、个人风控系统、支付系统之间的通信安全,借助密码应用技术进行用户身份的个人可信确认。

本文通过研究基于个人可信确认的电子支付个人风险控制系统情况,提出个人可信确认的密码应用技术方案相关要求,包括方案原理、个人可信确认报文、密码安全应用流程等。本研究可为支付机构、电子支付个人风险控制领域相关系统和设备厂商提供技术参考。

参考文献

[1] 李美.电子商务网上支付安全问题的探究[J].中国科技博览,2009(28):198-198.

[2] 国家密码管理局.GM/T 0028-2014 密码模块安全技术要求[S].2014.

[3] 国家密码管理局.GM/T 0021-2012 动态口令密码应用技术规范[S].2012.

[4] 国家密码管理局.GM/T 0005-2012 随机性检测规范[S].2012.

[5] 国家密码管理局.GM/T 0033-2014 时间戳接口规范[S].2014.

[6] 国家密码管理局.GM/T 0002-2012 SM4 分组密码算法[S].2012.

[7] 国家密码管理局.GM/T 0019-2012 通用密码服务接口规范[S].2012.

[8] 国家密码管理局.GM/T 0003-2012 SM2 椭圆曲线公钥密码算法[S].2012.

[9] 国家密码管理局.GM/T 0009-2012 SM2 密码算法使用规范[S].2012.

[10] 国家密码管理局.GM/T 0004-2012 SM3 密码杂凑算法[S].2012.

(收稿日期:2020-11-15)

作者简介:

樊凯(1978-),男,博士,教授,主要研究方向:电子商务安全、网络与信息安全。

韩小军(1979-),男,学士,主要研究方向:通信与电子系统、密码应用技术。

汪书(1992-),女,硕士,主要研究方向:互联网金融。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所