摩石观察

密码是保障网络安全的核心技术和基础支撑，在维护国家安全、促进经济社会发展、保护人民群众利益中发挥着不可替代的重要作用。“云物移大智”的蓬勃发展，5G、智慧城市、互联网 + 政务服务的全力推进，离不开用密码技术来保障网络安全、保护数据安全、保证网上诚信。实现网络安全需要密码学与其他学科深入合作，需要密码产业与其他产业的深度融合，需要产学研管用的真诚协作，更需要全社会共同传播密码知识与政策、研究密码应用技术、推进密码应用方案。

为激浊扬清，构建以密码技术为核心、多种技术相互融合的新网络安全体系，推进密码技术科学规范应用，长期深耕于信息安全一线的卫士通公司凝聚了一批国内顶尖的密码专家于 2016 年建立了摩石实验室。依托密码基础理论，探索密码创新实践，解决密码应用难题，培养密码专业人才，摩石实验室致力于让密码技术更好地服务于网络强国、数字中国和智慧社会。

本着共同的愿景，《信息安全与通信保密》杂志社与摩石实验室精诚合作，专门开辟《摩石观察》栏目。立足于密码本真，反思密码实践，《摩石观察》将以密码人的细致严谨叩问密码创新的真理之门，为广大读者了解、认识、掌握、使用密码技术提供准确规范的参考依据；同时我们期望以密码会友，与理想作伴，热忱邀请有志之士共同探索密码理论与应用的最佳实践，为推动金融等重要领域密码应用与创新发展而奋斗。

非银行支付机构电子支付系统密码应用

周君平，钟博
（成都卫士通信息产业股份有限公司，北京 100070）

[摘要] 非银行支付机构的商用密码应用，是贯彻执行国务院关于金融领域密码应用的指导意见，是加强电子支付领域尤其是移动支付领域商用密码应用规模化发展的重要举措。本文围绕非银行支付机构的电子支付系统模型与基本构成，调研各主流非银行支付机构的密码应用需求，提出密码应用保障框架，研究电子支付过程中采用商用密码技术实现的安全保障措施，形成一套成熟的第三方电子支付系统密码应用方案，可引导、带动其他非银行支付机构的商用密码应用推进工作。

[关键词] 安全电子支付；移动支付；电子支付系统；商用密码应用
[中图分类号] TP393　　[文献标识码] A　　[文章编号] 1009-8054(2019)04-0067-11

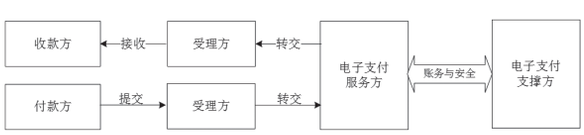
1 非银行支付机构的安全电子支付

1.1 电子支付基本概念

电子支付，指采用数字化方式在电子终端、信息传输通道以及相关系统的支持下进行支付的行为，是金融活动的一种新兴支付方式。相较于传统支付，电子支付具有操作方便、及时快捷、成本低廉等特点，为人们的工作及生活提供了便利，并呈现出良好的发展势头。

电子支付的基本活动由电子支付收款方、电子支付付款方、电子支付服务方、电子支付服务支撑方构成。付款方与收款方交互，提出付款申请；受理方将获取的支付请求发送到电子支付服务方；电子支付服务方完成相应的支付服务，并在必要时通过受理方转交或通知收款方。电子支付支撑方提供账户管理、账务核算、安全措施与管理等功能。电子支付的概念如图 1 所示。

图 1 电子支付概念图

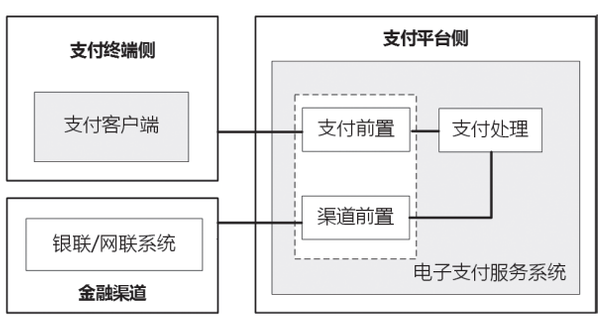


其中，付款方一般映射为支付客户；收款方一般映射为收款客户或商户；收款受理方可看成一个实体，一般映射支付终端；电子支付服务方一般映射支付服务的电子支付平台或支付系统，当其通过银行进行支付时，需要通过支付网关进行支付请求；电子支付支撑方一般映射连接银行的金融渠道，以及提供安全基础支撑的认证中心。

1.2 第三方电子支付系统模型

电子支付系统，是指通过通信、计算机和信息安全技术，在商家和银行间建立连接，从而实现从消费者到金融渠道及商家间货币支付、现金流转、资金清算、查询统计的支付平台。非银行支付机构是指依法取得《支付业务许可证》，获准为支付客户办理互联网支付、移动电话支付（远程支付）业务的非银行机构。非银行支付机构基于客户的银行账户或按照《非银行支付机构网络支付业务管理办法》规定为客户开立支付账户提供网络支付服务。非银行支付机构的电子支付系统，也称为第三方电子支付系统。第三方电子支付系统模型参见图 2。

图 2 第三方电子支付系统模型



从系统模型来看，由支付前置、支付处理、渠道前置等核心功能组成的电子支付服务系统，为第三方电子支付系统的内部关键系统；支付终端、金融渠道系统分别为其外部关键系统。网络支付客户通过支付客户端发起支付指令，对接电子支付服务系统，通过支付前置、支付处理、渠道前置，转发金融渠道，处理支付交易请求，最终完成一套完整的支付流程。

1.3 关键业务流程

第三方电子支付的关键业务流程，指不同支付交易类型的支付服务在电子支付系统的全流程实现，如账户充值、提现、转账、查询、消费等支付服务。主要包括支付交易发起与完成、支付处理、支付服务接入金融渠道三个关键环节。

1.3.1 支付交易发起与完成

该环节是指支付终端应用的个人用户或商户系统与电子支付服务系统的支付前置间发生的系统通信与数据处理。

支付交易发起，指支付客户从支付终端应用发起支付交易请求，支付交易请求发送至支付前置处理；支付完成，指支付请求已被完成支付处理，形成支付处理结果，并由支付前置通知支付用户。

1.3.2 支付处理

该环节是指电子支付服务系统内部各主要实体间发生的系统通信与数据处理，如支付指令交换、支付清分结算等处理。内部各实体主要指支付前置、支付处理及渠道前置三部分，支付处理的支付清分结算，是指资金变动在系统内部的支付处理环节进行处理。

1.3.3 支付服务接入金融渠道

该环节是指电子支付服务系统与金融渠道间发生的系统间通信与数据处理，金融渠道的接入由渠道前置来完成。

1.4 安全电子支付

非银行支付机构的安全电子支付，是以商用密码应用为核心，保障第三方电子支付关键业务流程安全的一种方法或方案，核心是支撑安全支付的各项密码技术的应用，如用于电子支付的密码算法、数字证书、密钥管理、密码协议、实现密码功能的各项密码技术以及密码基础设施等应用。

2 电子支付系统商用密码应用需求分析

2.1 商用密码应用背景

近年来，与第三方支付机构安全要求相关的政策法规主要有中国人民银行发布的《非金融机构支付服务管理办法》《非金融机构支付服务管理办法实施细则》《非金融机构支付服务业务系统检测认证管理规定》《非银行支付机构网络支付业务管理办法意见稿》等管理办法，国办发 [2014]4 号《关于加强重要领域密码应用的重要意见》、国办 [2014]6 号《国务院办公厅转发密码局等部门关于金融领域密码应用指导意见的通知》，以及中华人民共和国发布的《中华人民共和国电子商务法》。经过总结提炼，针对非银行支付机构及其电子支付系统在网络支付业务中的关键安全要素有如下几个方面：

（1）非银行支付机构纳入国家监管体系，拥有了合法的身份。

（2）第三方电子支付系统应符合网络安全等级保护第三级安全保护等级的基本要求。

（3）为贯彻执行国务院关于金融领域密码应用的指导意见，中国人民银行发布了非银行支付机构关于数字证书应用的要求，其中规定支付机构采用数字证书、电子签名作为验证要素的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》《金融电子认证规范》以及国家密码管理局等有关规定，确保数字证书的唯一性、完整性及交易的不可抵赖性。

（4）第三方电子支付系统针对电子支付安全的基本要素包括身份识别、交易验证、交易信息保护、支付指令保护。其中身份识别，指客户在发起支付指令进行支付交易之前，需先对客户身份进行识别，针对支付账户的客户实行实名制管理；交易验证指按规定采取客户支付指令的验证措施；交易信息保护，是指电子支付系统应当确保交易信息的真实性、完整性、

可追溯性以及在支付全流程中的一致性，不得篡改或者隐匿交易信息；支付指令保护是指电子支付系统应当确保电子支付指令的完整性、一致性、可跟踪稽核和不可篡改。这些安全要素的实现需应用密码技术。

（5）国办发 [2014]4 号文件要求加强我国能源、交通、金融等涉及国计民生和基础信息资源重要信息系统的商用密码应用，其中包括了第三方支付系统商密应用的要求。国办 [2014]6 号文件要求紧紧围绕在金融 IC 卡、网上银行、移动支付、网上证券、电子保单等重点领域中应用商用密码。

综上政策法规规定的各项安全要素，意在促进作为电子支付服务提供者的非银行支付机构建立起完整的、以商用密码技术应用为核心的网络信息安全保障机制，增强抵御外界风险的能力。因此，如何有效促进第三方电子支付系统在互联网支付、移动支付等应用场景的商用密码规模化应用，满足行业监管要求，成为非银行支付机构迫切需要解决的问题。

2.2 电子支付系统面临的安全风险

在网络支付服务业务中，第三方电子支付的关键业务流程体现了支付客户从支付交易发起、支付处理到支付服务接入金融渠道、支付交易完成等支付活动在电子支付系统的资金流转移全过程。研究发现，客户在网络支付过程中由于木马、钓鱼网站和账户、密码被盗原因带来资金损失所占的比例最高，比如资金在转移过程中出现丢失、诈骗、盗用等风险。资金转移全过程的核心支撑平台是第三方电子支付系统，因此网络支付过程的风险主要指电子支付系统的风险，其安全风险分析参见表 1。

表 1 电子支付系统安全风险分析

风险内容	可能的危害或后果	涉及关联方	安全保障措施
付款方个人账号及密码在终端输入时被窃取	付款方敏感信息被泄露，资金风险增大	付款方、攻击者	关键支付数据保护；个人支付安全防护
支付交易中开户人身份冒充，以及接入不信任的支付服务站点	身份假冒，支付服务站点钓鱼	付款方、支付服务提供方、攻击者	参与支付过程的各关联方均须向彼此表明身份
付款方个人账号及密码在网上传输时被泄露	付款方敏感信息被泄露，资金风险增大	付款方、攻击者	关键支付数据保护
攻击者盗用合法账号、密码发起支付指令	身份假冒		
付款方账户资金受损	付款方、支付服务提供方、攻击者	对发起付款指令的终端用户进行身份认证；支付指令的发出必须经过付款方签名	
伪造支付指令	付款方账户资金受损	付款方、支付服务提供方、攻击者	付款方对支付指令进行签名，支付服务提供方进行核验
伪造付款凭证（如电子支票）进行支付	付款方账户资金受损	付款方、支付服务提供方、攻击者	支付服务提供方对付款凭证的真实性进行验证，确保该付款凭证确实由付款方签发

风险内容	可能的危害或后果	涉及关联方	安全保障措施
伪造电子货币进行支付	支付服务提供方资金受损	付款方、支付服务提供方、攻击者	对电子货币等的有效性进行验证
攻击者利用截获的合法支付指令进行重放攻击	付款方账户资金遭受损失	付款方、支付服务提供方、攻击者	支付指令防重放攻击
支付过程各关联方均可能否认其操作，受害方无法举证	引发争议	支付过程有关各方	各方对支付过程由本方发出操作进行签名确认，对对方发出的操作验证其真实有效性
收款方否认收到货款	引发争议	付款方、收款方、支付服务提供方	对支付行为跟踪，争议取证与仲裁；支付协同安全保障

上述安全风险点的安全保障措施，通过在电子支付关键业务流程的各关键环节采用密码技术来实现。采用密码技术等手段提升第三方电子支付系统安全，加强政府对非银行支付机构的监管，成为保障客户利益、维护金融安全的当务之急。

2.3 商用密码应用需求

依据《非银行支付机构支付业务设施密码应用技术要求》（草案），第三方电子支付系统受保护的关键数据为身份鉴别数据、支付交易数据、用户个人敏感数据等。第三方电子支付系统商用密码应用需求，即指如何实现非银行支付机构的安全电子支付，如何采用密码技术应用等安全保障措施，保护电子支付关键数据的安全，包括实现针对支付各方身份进行身份真实性鉴别，针对交易关键数据进行信息保护如数据机密性、完整性、不可否认性。

本文针对上述电子支付系统面临的安全风险点，总结得出实现安全的电子支付所需商用密码应用的几个重点安全要素。

（1）支付接入安全，即参与支付过程的各关联方均须向彼此表明身份。

（2）支付交易认证，即非银行支付机构须确认支付发起方就是支付账户的所有者，或由支付账户所有者授权。

（3）支付过程中敏感信息安全，即保证敏感信息的机密性和完整性。

（4）支付指令防抵赖，即指令的发出必须经过账户所有者的（签名）确认，或经过其明确授权由被授权人发出且被授权人须对此进行（签名）确认。

（5）支付数据通信安全，即保证支付数据的机密性和完整性。

2.4 主流第三方电子支付系统商密应用现状

主流非银行支付机构以支付宝、财付通为代表，其他包括安付通、网付通、快钱、百度钱包、拉卡拉等，小规模的非银行支付机构有摩宝、易极付、现代金服、联付通、国付宝等。

主流第三方电子支付系统安全现状总体来看，各家支付系统均有良好的网络安全防护措施；均配备了风控措施与监管机制；在电子支付安全环节中，均支持了登录、支付密码的独立应用，均实现了 SSL 安全传输通道，在数字证书使用方面，支付宝率先采用了合规的客户

数字证书实现客户交易报文数字签名，使其支付操作不可否认；在密码模块合规性方面，大部分支付机构采用了合规的服务端密码模块，但使用合规的终端密码模块的支付机构仍是少数。

从第三方电子支付系统的商用密码应用来看，早于 2016 年支付宝就在支付交易环节采用了基于商用密码的 PKI/CA 数字证书认证方案；2017 年起，支付宝、财付通纳入商密应用试点单位，建立以密码技术为核心的商密改造规划。支付宝还参与到相关安全支付的国家重大研发计划研究及密码行业标准的制定中，积极推进电子支付系统的商密应用技术与标准的研究工作。

以支付宝、财付通为代表的主流支付机构，通过有序开展商用密码应用改造，将形成一套成熟的第三方电子支付系统密码应用方案，同时，也必将引导、带动其他非银行支付机构推进商用密码的规模化应用。

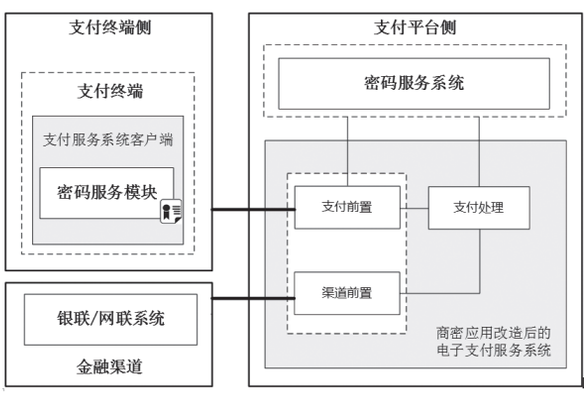
3 第三方电子支付系统密码应用方案

3.1 密码应用保障框架

第三方电子支付系统密码应用保障框架建立在电子支付系统模型之上，依据电子支付的商用密码应用需求进行设计，为电子支付服务系统提供认证管理服务、密码基础服务、密钥管理服务等功能。

保障框架分为支付终端侧、支付平台侧、金融渠道三个部分，其中支付平台侧由商密应用改造后的电子支付服务系统与密码服务系统组成；支付终端侧由商密应用改造后的支付服务系统客户端与终端密码服务模块组成，保障框架示意图参见图 3。

图 3 电子支付系统密码应用保障框架示意图



3.2 证书应用

电子支付系统采用双证书认证体系，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。其证书种类及用途如表 2 所示。

表 2 证书种类及用途

序号	证书种类	用途
1	根 CA 证书	根 CA 证书是非对称密码体系的信任根，需用于签发支付平台服务器证书及支付客户端证书。
2	支付平台证书	是支付平台的合法性标识，需用于实现支付平台身份鉴别、数字签名。
3	支付服务器证书	用来实现与支付终端实体的安全通信。
4	支付客户端用户证书	是支付客户端的合法性标识，需用于实现支付终端实体的身份鉴别、数字签名、密钥协商等功能。
5	其他机构服务器证书	金融机构的服务器证书，支付平台需通过安全途径获取这些证书，用于与金融系统的安全通信功能。
6	其他机构平台证书	金融机构的平台证书，支付平台需通过安全途径获取这些证书，用于实现金融机构的身份鉴别、数字签名。

3.3 密钥管理

支付系统的密钥管理，包括支付过程关联的所有密钥种类，其密钥种类及用途如表 3 所示。

表 3 支付系统的密钥种类及用途

序号	证书种类	用途
1	用户密钥	用户密钥是客户端中最为核心的密钥数据，用于用户对交易信息进行确认签名和验证，当使用软件密码模块来实现对用户密钥的安全保护和实现数字签名、签名验证等密码运算服务时，用户密钥可采用协同模式。 协同模式的密钥产生和运算需支付客户端和支付平台的协作完成，私钥被分成两部分，一部分存储在客户端，另一部分存储在平台端。
2	服务器私钥	主要解决客户端和支付平台之间身份认证和通信时的安全，以及平台与 CA 系统之间的通信安全，通过加密和签名手段，保证通信数据的完整和可靠。
3	设备私钥	用于标识软密码模块使用设备的身份，用于保护通信安全。此外，设备密钥对协同模式的用户密钥进行保护。
4	平台私钥	主要用于保护和金融渠道服务器系统间的通信安全。主要是在支付平台和金融渠道服务器进行通信时使用平台私钥进行签名，金融渠道系统通过平台公钥进行验签，验证表明报文数据合法，保证通信数据的完整和可靠。
5	数据传输静态对称密钥	平台内部系统间互通数据，可使用固定对称密钥对数据进行安全传输。对称密钥由密码服务设备产生与存储。
6	数据存储密钥	用于持久化存储敏感数据时，可使用固定对称密钥对数据进行安全存储，也可使用非对称密钥对数据进行安全存储。
7	金融渠道服务器公钥	主要解决支付平台系统和金融渠道系统间身份认证和通信时的安全。
8	金融渠道平台公钥	金融渠道平台返回支付平台数据时，用金融渠道平台私钥签名，支付平台接收到反馈数据时用金融渠道平台公钥进行验签。平台私钥由金融渠道机构密码服务设备产生并存储。

3.4 商密应用改造方案

3.4.1 支付终端侧商密改造

支付终端需应用数字签名与加密技术，在通信和交易过程中使用的加解密算法采用SM4算法，数字签名算法采用 SM2 算法，摘要算法采用 SM3 算法。支付终端密码应用商密改造内容如表4所示。

表 4 支付终端商密改造内容

模块	功能	密码改造内容
支付客户端	实现支付交易时对接受方进行身份鉴别，确保发送支付交易数据报文的机密性、完整性和不可抵赖性。	客户端调用密码服务模块，作为发送方对数据报文加密和计算数字签名。
	实现接收支付服务系统反馈的数据报文时鉴别身份、校验数据的完整性和不可抵赖性。	主要解决客户端和支付平台之间身份认证和通信时的安全，以及平台与 CA 系统之间的通信安全，通过加密和签名手段，保证通信数据的完整和可靠。
支付终端侧证书管理	实现证书管理功能，对证书申请等上传数据报文进行不可抵赖性保护。	客户端调用密码服务模块，进行证书申请、下载、更新等证书管理，证书申请签发之前先鉴别用户身份。

3.4.2 支付平台侧商密改造

支付服务系统需要应用数字签名与加密技术，在通信过程中使用的加解密算法采用 SM4 算法，数字签名算法采用 SM2 算法，摘要算法采用 SM3 算法。支付平台侧密码应用改造内容如表 5 所示。

表 5 支付平台侧商密改造内容

模块	功能	密码改造内容
支付平台侧支付前置	实现接收数据报文时对发送方进行身份鉴别，确保接收支付交易数据报文完整性、机密性和不可抵赖性。	支付前置与客户端通信时调用密码服务系统，作为接收方对数据报文进行解密和验证数字签名。
	实现支付交易时对接收方进行身份鉴别，确保发送支付交易数据报文的完整性、机密性和不可抵赖性。	支付前置与客户端通信时调用密码服务系统，作为发送方对数据报文加密和计算数字签名。
支付平台侧渠道前置	实现支付交易时对接收方进行身份鉴别，确保发送支付交易数据报文的完整性、机密性和不可抵赖性。	渠道前置与客户端通信时调用密码服务系统，作为发送方对数据报文加密和计算数字签名。
	实现接收数据报文时对发送方进行身份鉴别，确保接收支付交易数据报文的完整性、机密性和不可抵赖性。	渠道前置与客户端通信时调用密码服务系统，作为接收方对数据报文进行解密并验证数字签名。
内部各系统	实现敏感数据机密性保护。	系统内部各系统通信时，调用密码服务系统对支付服务系统内部传输的敏感数据进行机密性保护。
支付平台侧证书管理	连接 CA 系统，实现证书管理，对证书申请等请求数据进行机密性、不可否认性保护。	支付服务系统接受来自支付终端的用户证书申请、证书下载、更新等请求，一方面调用密码服务系统认证管理服务模块，连接 CA，进行证书申请、下载、更新等证书管理；另一方面可按需实现协同密钥运算服务。

3.5 密码应用方案部署

依据商用密码应用需求分析与总体框架，密码应用方案部署分为支付终端侧密码服务模块部署与支付平台侧密码服务系统部署，其基本要求如表 6。

表 6 支付平台侧商密改造内容

序号	密码服务部署	功能	基本要求	产品形态
1	支付终端侧密码服务模块部署	密码基础服务	（1）需为支付客户端提供密钥对生成、密码运算等基础密码服务； （2）模块应满足 GM/T 0028《密码模块安全技术要求》相关安全要求。	不同终端可配备不同形态密码服务模块： （1）外置密码服务模块（硬件设备）适用于互联网支付应用； （2）内置密码服务模块（软件模块），适用于移动互联网环境下支付终端如手机终端应用。
		密钥管理服务	需提供支付业务相关密钥的统一管理服务。	
		认证管理服务	（1）支付交易用户身份验证、数字签名服务； （2）设计需满足 GM/T 0029《签名验签服务器技术规范》《移动终端数字证书应用标准》。	

序号	密码服务部署	功能	基本要求	产品形态
2	支付平台侧密码服务系统部署	密码基础服务	（1）需为支付服务系统提供基础密码运算服务； （2）系统需满足GM/T 0028《密码模块安全技术要求》相关安全要求。	（1）密码服务系统。应包括密钥管理、证书管理、密码运算等功能，可连接第三方CA； （2）密码服务设备集群。应提供安全高效的密码运算、密钥管理等功能。
		密钥管理服务	需为支付平台提供相关密钥的管理服务。	
		认证管理服务	（1）提供通信用户身份鉴别、签名验证服务； （2）提供系统间通信数据安全服务； （3）连接CA系统实现对用户证书管理； （4）设计需满足GM/T 0029《签名验签服务器技术规范》。	

3.6 非银机构安全电子支付的推广研究

全面使用商用密码应用技术及相关产品，在第三方支付行业是一种密码应用创新，极大提升了电子支付系统的安全性和规范性，满足国家“大力推进重点领域网络信息系统密码应用”的战略目标。鉴于移动支付新兴支付方式的崛起，非银机构安全电子支付的推广应重点研究以下几个方面。

3.6.1 推广支付终端采用商用密码软件密码模块实现的技术方案

目前，在第三方支付系统的支付交易环节建立基于商用密码的PKI/CA数字证书认证方案，用户在手机终端的交易签名作为第三方支付服务系统判断交易合法的主要因素。但考虑在移动互联网业务发展的背景下，基于硬件的传统数字证书技术路线在现阶段很难覆盖支付系统海量的用户需求，因此可大力发展既符合国家密码管理相关要求，又符合移动互联网业务特点的软件密码模块实现技术方案。

3.6.2 推广支付平台采用高性能商用密码服务系统实现的技术方案

高性能商用密码服务系统，用于满足电子支付系统大用户量高并发交易环境下对高性能密码服务的需求。可通过支付服务的高性能签名验证技术、分布式密码服务技术、密码服务设备集群调度与负载均衡技术、高性能并行计算技术等关键技术的研究来提升密码服务能力及密码运算能力。

3.6.3 商密SSL服务器证书的普遍采用指日可期

SSL服务器证书用于各种网站的证书需要被大众信任，目前众多重要信息系统均采用国内品牌的证书，如沃通SSL证书，自主可控能支持所有浏览器和移动终端，可满足多域名、多服务器、负载均衡等不同应用场景。商密SSL服务器证书的使用，要求对客户端浏览器须采用支持商密算法的安全浏览器，但鉴于我国SM2、SM3算法刚刚纳入国际标准，常用的客户端浏览器并不支持商密算法，因此在电子支付

系统中，SSL 服务器证书应用目前是推荐使用商密，相信随着商密算法的国际化进程的推进，普遍使用商密 SSL 服务器证书将指日可期。

参考文献：

[1] GB/T 31502《信息安全技术 电子支付系统安全保护框架》.

[2] 国家密码管理局，《非银行支付机构支付业务设施密码应用技术要求》（草案）.

[3] 中国电子认证服务产业联盟，《移动终端数字证书应用标准》（草案）.

[4] 中国人民银行，《非银行支付机构网络支付业务管理办法意见稿》，2015.7.31.

[5] 中国人民银行，中国人民银行令〔2010〕第 2 号《非金融机构支付服务管理办法》，2010.6.14.

[6] 中国人民银行，中国人民银行公告〔2010〕第 17 号《非金融机构支付服务管理办法实施细则》，2010.12.1.

[7] New and efficient conditional e-payment systems with transferability. Future Generation Comp. Syst, 2014, 37: 252-258.

作者简介：

周君平，成都卫士通信息产业股份有限公司，高级工程师。主要研究方向为网络信息安全、商用密码应用，承担过多项国家重大研发计划、重大专项。

钟博，成都卫士通信息产业股份有限公司副总裁，高级工程师。从事密码学、国家金融能源等重要领域密码应用等研究工作，承担过多项国家级重大专项，四次荣获省部级科技进步奖。

Domestic Cryptographic Applications in Electronic Payment System of Non-bank Payment Institutions

ZHOU Jun-Ping,ZHONG Bo

（Chendu Westone Information Industry Inc, Beijing 100070, China）

[Abstract] Domestic Cryptographic Applications in Electronic Payment System of Non-bank Payment Institutions is an important measure to implement the guidance of the State Council on the cryptographic applications in the financial field. It is an important measure to strengthen the large-scale development of electronic payment, especially in the field of mobile payment. Focusing on the model and basic composition of electronic payment system of non-bank payment institutions, this paper investigates the cryptographic application requirements of mainstream non-bank payment institutions, puts forward a cryptographic application safeguard framework, studies the security safeguard measures implemented by domestic cryptographic technology in the process of electronic payment, and forms a mature cryptographic application scheme of third-party electronic payment system, which can guide and drive other non-bank payment institutions to promote the application of domestic cryptographic.

[Keywords] Secure Electronic Payment; Mobile Payment; Electronic Payment System; Domestic Cryptographic Applications