第二代农信银支付清算系统与成员机构行内系统互联规范

文档编号：	NXY_NCS2_D06
版本：	V1.0
项目编号：	NXY_2011_01
项目经理/项目负责人：	肖飞
保密级别：	机密

农信银资金清算中心
RURAL CREDIT BANKS FUNDS CLEARING CENTER

2011 年 11 月

文档修订记录

版本	状态	简要说明	修订		批准	
			日期	人员	日期	人员
1.0	M	根据反馈意见进行修订，定版。	20111216			

说明：

1. 版本栏中填入版本编号或者更改记录编号。
2. 状态分为三种状态：A——增加；M——修改；D——删除。
3. 在简要说明栏中填写变更的内容和变更的范围。
4. 表中所有日期格式为：YYYYMMDD

目 录

第一章 引言

1.1 背景

2006 年 10 月，农信银支付清算系统（NCS）正式上线运行，实现了对全国农信银机构的实时电子汇兑业务的支持，并于 2008 年相继开通了银行汇票业务和个人账户通存通兑业务，进一步丰富了全国农信银机构的异地支付结算渠道，有效解决了农信银机构长期以来无法签发银行汇票、无法办理柜面通的问题，得到了广大农信银机构的认可，逐步成为农信银机构办理异地支付结算业务的重要途径。2010 年 7 月，山西省联社综合业务系统成功接入，实现了农信银支付清算系统在全国农信银机构的全面覆盖。

农信银支付清算系统上线以来，系统运行稳定，交易量及资金清算量逐年稳步增长。截至 2010 年，全国 30 家省级农村合作金融机构以及深圳农村商业银行、天津滨海农村商业银行的行内系统均已经与农信银支付清算系统连通，32 家成员机构全面开通实时电子汇兑业务，27 家开通签发银行汇票业务，32 家开通个人账户通存通兑业务，形成了较为完善的农村支付清算网络体系，对加快社会资金周转，提高支付清算效率，促进农村经济健康平稳发展发挥了重要作用。根据系统开通上线的运行年度统计，截至 2010 年 6 月 7 日，全国农信银机构通过农信银支付清算系统共办理各类资金清算业务 5336 万笔，清算资金 10025 亿元，突破万亿元大关。农信银支付清算系统开通运行第一年清算业务量 180 万笔，清算资金 419 亿元；第二年清算业务量 903 万笔，清算资金 1971 亿元；第三年清算业务量 2049 万笔，清算资金 3590 亿元；第四年清算业务量达到 3688 万笔，清算资金 7229 亿元，分别是第一年的 20.5 倍和 17.3 倍。农信银支付已经成为国内最为重要支付结算渠道之一，为促进农村地区经济发展发挥了重要作用。

目前，农信银支付清算系统已经成为中国支付清算体系的重要组成部分，是中国人民银行支付清算体系的重要补充，是联结全国农村合作金融机构的桥梁和纽带，是农村合作金融机构实现业务创新和延伸的技术后盾。

随着农村经济发展速度加快，经济规模不断扩大，资金交易活动日益频繁，农村金融机构市场逐渐完善，市场的广度和深度不断拓展，社会公众的金融产品需求和支付需求越来越有多样性发展的趋势。农信银支付清算系统主要面临以下几个方面的市场变化和需求：

（一） 近年来，农村金融机构的行内系统相继升级换代，新兴电子支付方式及支付工具不断涌现，新兴的业务品种越来越多；

（二） 农信银支付清算系统在国内支付体系承担越来越重要的责任，国内其他商业银行及支付组织也迫切希望接入农信银支付清算体系；

（三） 根据国家支持与服务三农的政策，农信银支付清算体系应该主动承担起连接村镇银行等支付渠道建设的重任。

这些变化要求农信银支付清算系统提供更全面、更高效的服务，而现有的支付清算系统业务功能和运

行管理等方面也需要进一步优化和改进。针对第一代支付系统存在的不足，结合当前及未来一段时期社会经济发展对支付清算服务的新需求，同时考虑支付系统运行的生命周期以及进一步完善支付系统备份系统等实际情况，经过科学论证，农信银资金清算中心决定建设新一代的支付清算系统，称为“第二代农信银支付清算系统（NCS2）”。

1.2 编写目的

本规范作为参与者接入人行一代支付，人行二代支付，农信银二代支付系统，参考业务需求、业务标准及相关设计文档编写，目的是指导行内的开发人员依据本规范，开发与本系统对接的相关业务系统。

本规范的期望读者包括：各系统行内的系统分析员、程序员、测试人员、业务主管及其他相关人员。

1.3 定义和缩略语

- **农信银二代支付业务系统（Payment System，简称 NPS）**

  是农信银支付业务处理系统，处理农信银通存通兑，汇兑等各种支付业务。

- **农信银清算账户管理系统（Settlement Account Processing System，简称 NAS）**

  是支付系统的支持系统，集中存储清算账户，处理支付业务的资金清算，并对清算账户进行管理。

- **农信银支付管理信息系统（Payment Management Information System，简称 PMS）**

  是第二代农信银支付清算系统的重要辅助系统，由行名行号管理子系统、支付参数管理子系统、计费管理子系统、支付业务统计分析子系统、支付业务监控子系统和支付业务明细查询子系统等六个子系统组成。

- **农信银企业服务总线(Enterprise service bus，简称 ESB)**

  是第二代农信银支付清算项目群中各系统服务发布，管理，订阅以及调用的平台，是引入 SOA 理念实施二代支付系统的重要支撑系统。

- **成员接入前置系统(简称 MFE)**

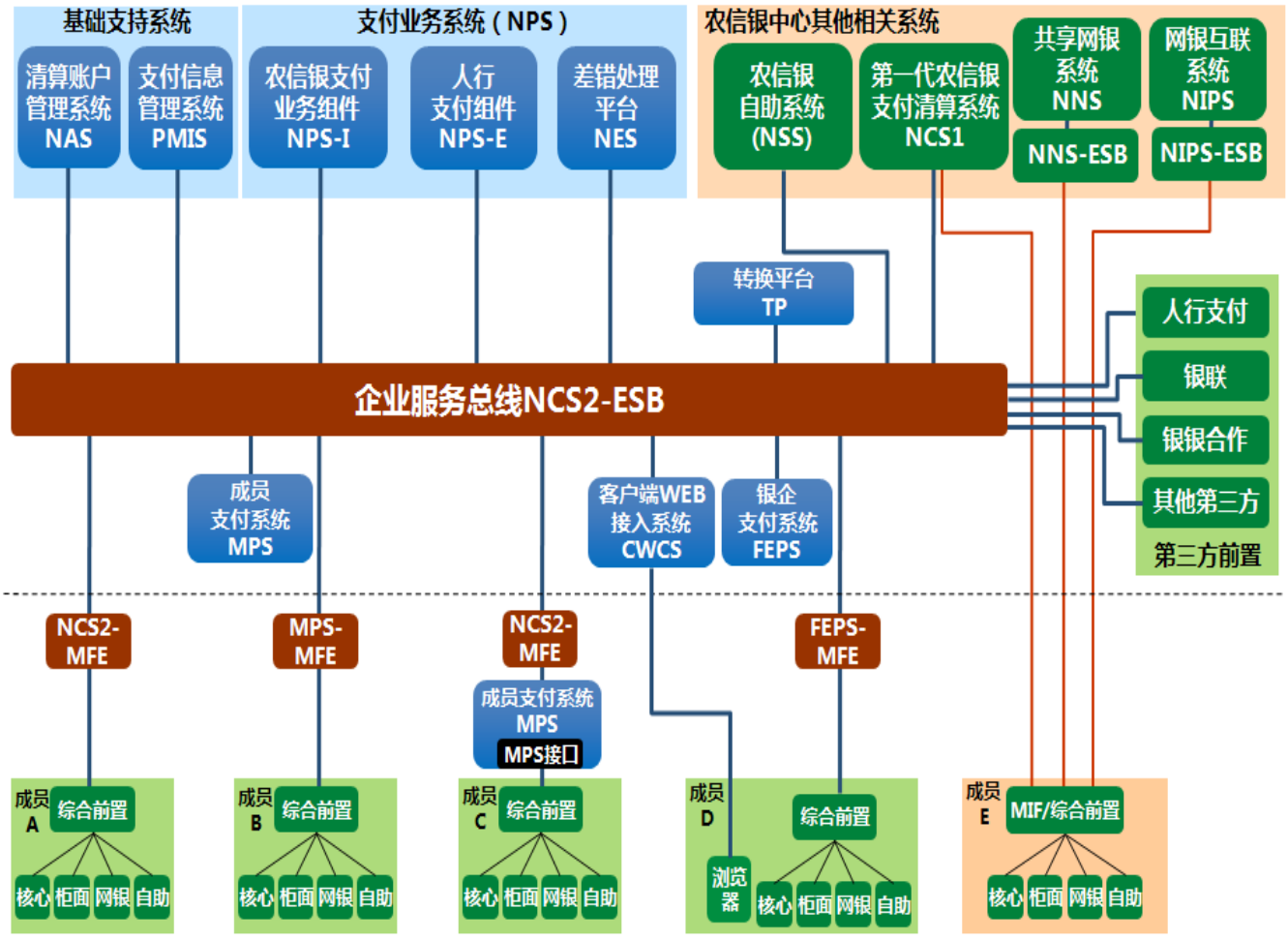
  是指摆放在支付系统行内端，连接支付系统，并负责接收、发送通过支付系统处理本行支付业务的系统。通俗称为“直联前置机”。

第二章 第二代农信银支付清算系统简介

第二代农信银支付清算系统是服务“三农“重要的金融基础设施，为各参与行提供资金清算服务。外部的参与者包括人行、银联、第三方/网络支付等。

为便于向成员机构提供灵活、可靠的接入服务，第二代农信银支付清算系统建设中，提出了基于 SOA 架构思想，通过构建一个高可用的企业服务总线(简称 ESB)，实现行内系统与第二代农信银支付清算系统之间安全可靠的支付业务报文传递与服务调用。从 ESB 的角度来看，各类金融信息系统均可接入到该平台，通过该平台提供的服务来发送/接收跨行的支付信息（即报文）；第二代农信银支付清算系统也只是接入到 ESB 的一个信息系统，从 ESB 中获取报文，进行处理和转发。

NCS2 系统总体应用架构如下图所示：



根据 NCS2 系统总体应用架构图，对 NCS2 系统的总体功能分布说明如下：

(一) 基础支持系统

包括清算账户管理系统（NAS）和支付信息管理系统（PMIS），为支付业务处理和未来业务扩展提供基础的清算管理、业务管理、业务监控和业务分析功能。

(二) 支付业务处理系统

支付业务处理系统（NPS）包括成员机构、农信银中心以及人行支付、银联、银银合作、其他第三方机构相关的支付业务的业务规则处理、业务路由、风险控制、对账处理及差错处理功能，是支付业务处理的“核心”系统。

(三) 农信银中心其他相关系统

其他相关系统包括农信银自助系统（NSS）、第一代农信银支付清算系统（NCS1）、共享网银系统和网银互联系统。根据 NCS1、NCS2 系统并行运行和未来业务发展要求，这些系统与 NCS2 系统需要建立系统连接，以保证业务的连续性。这些系统可能需要进行一定的适应性功能扩充或改造。

(四) 服务总线与成员接入系统

包括企业服务总线系统和成员端前置系统，主要完成各系统服务的统一管理、各系统间连通性的保证，是 NCS2 系统的“神经网络”。

(五) 成员支付系统

包括股东成员支付系统和银企成员支付系统，主要完成股东成员和银企成员的支付业务逻辑处理及成员机构内部客户渠道系统（如自建网银、呼叫中心、ATM/POS 等）、业务支持系统（如核心系统/综合业务系统、支付系统、信贷管理系统、国际结算系统等）的连接。

(六) 成员机构内部系统

包括成员机构内部客户渠道系统（如自建网银、呼叫中心、ATM/POS 等）、业务支持系统（如核心系统/综合业务系统、支付系统、信贷管理系统、国际结算系统等），根据 NCS2 系统业务领域与成员机构内部系统的关联性，成员机构内部系统可能需要进行一定的适应性功能扩充或改造。

(七) 第三方接入前置系统

包括人民银行、银联、银银合作、其他第三方的接入前置系统，实现农信银中心与第三方系统的安全隔离和连通性保证。

第三章 企业服务总线简介

3.1 系统概述

企业服务总线（ESB）作为一个连接支付系统和行内系统的渠道，是一个高可用的服务调用与报文传输平台，其任务是保证支付系统与各个行内系统之间的高可靠性的服务调用与报文传输。其业务功能主要是以下几点：

1、 传输安全：保证支付报文传输过程中端到端的数据完整性。

2、 报文校验：对收到的支付报文要进行格式校验，不满足格式要求的给予拒绝处理，从而实现对行内故障的有效隔离。行内故障中报文级的错误可以在支付报文传输平台得到屏蔽，不影响业务处理系统（同时业务系统也支持对行内设置故障状态，限制该行内业务的发起与接收）。

3、 智能路由：对于满足格式要求的，根据目标地址自动选择传输路径，确保最终送达支付系统或者行内系统。该平台支持行内多点接入路由的灵活调整。

4、 流量控制：可以按不同成员机构和渠道对计时应答型的交易进行流量控制，实现成员机构间和渠道间服务质量的隔离。

ESB 具备如下主要特性：

1、 兼容多种报文格式：支持 CMT/PKG/XML/ISO8583/NCS1 报文，并可以根据需要方便扩展。

2、 高可用性：系统要具有较好的容错机制，能提供 7*24 小时报文传输服务。

3、 实现报文传输与业务处理分离：各类金融信息系统均可接入到该平台，通过该平台提供的服务来发送和接收跨行的支付报文，减少系统间接口数量。各类系统只与 ESB 进行交互，由 ESB 对外提供统一的接口供接入系统调用，降低系统接口开发维护的成本。

4、 实现服务的全局共享：使各类服务资源得到有效的复用，降低系统实施的复杂度和实施成本。避免了多渠道业务重复投资，缩短业务实现周期。

5、 可建设统一监控平台：方便系统的运行维护，提高系统运行质量。

3.2 成员接入前置系统定位与功能

成员接入前置系统（MFE）是连接支付系统和行内系统的桥梁，是支付系统的重要组成部分。MFE 的主要功能包括报文转发、报文格式检查、安全管理等，即对行内系统提交的报文和支付系统发来的报文进行相应的报文格式检查，并根据系统安全规范实现报文的可靠传输和交换。MFE 不参与业务相关处理，如业务合法性检查、重账检查、业务核对等，以降低其运行维护复杂度。

MFE 只提供直连接入功能，不提供业务录入、来帐打印等间连接入功能。MFE 由农信银中心负责开发，

免费提供给系统行内使用，物理部署在行内端，并由行内进行系统维护与管理。

MFE 具备如下主要特性：

1、 报文转发：借助消息中间件，对参与者行内系统提交的报文和支付系统发来的报文进行转发。

2、 报文校验：对参与者行内系统提交的报文和支付系统发来的报文进行相应的报文格式检查。

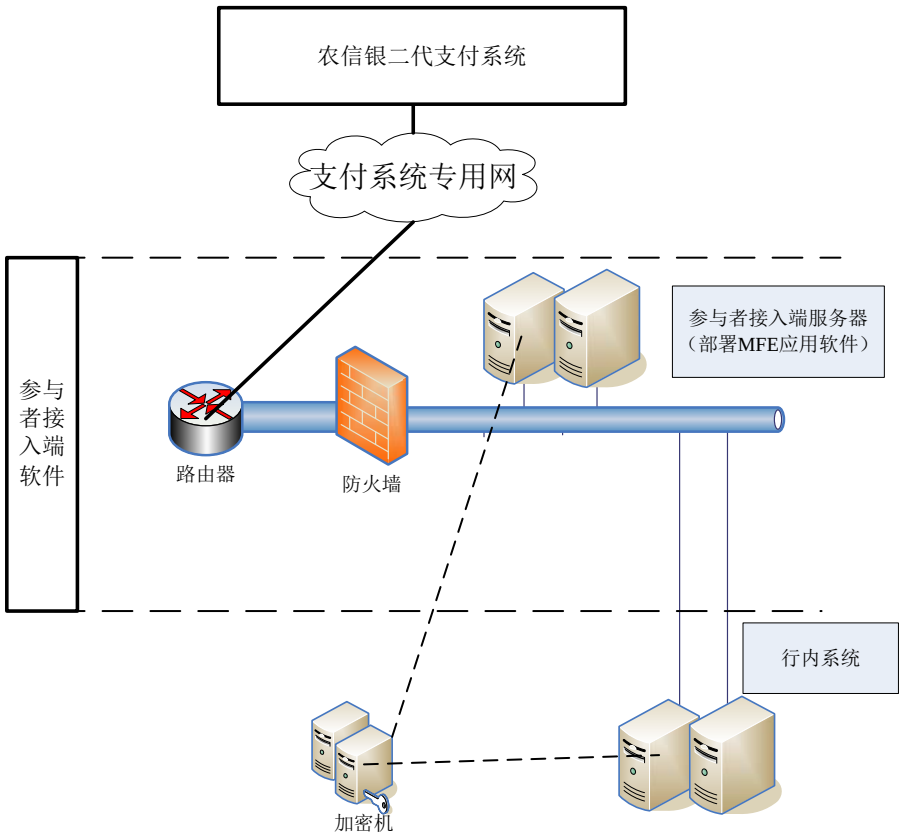
3、 报文监控：对报文流水进行登记，并提供简单的查询功能。

4、 安全传输：对报文进行数据加密，保证报文的可靠性传输。

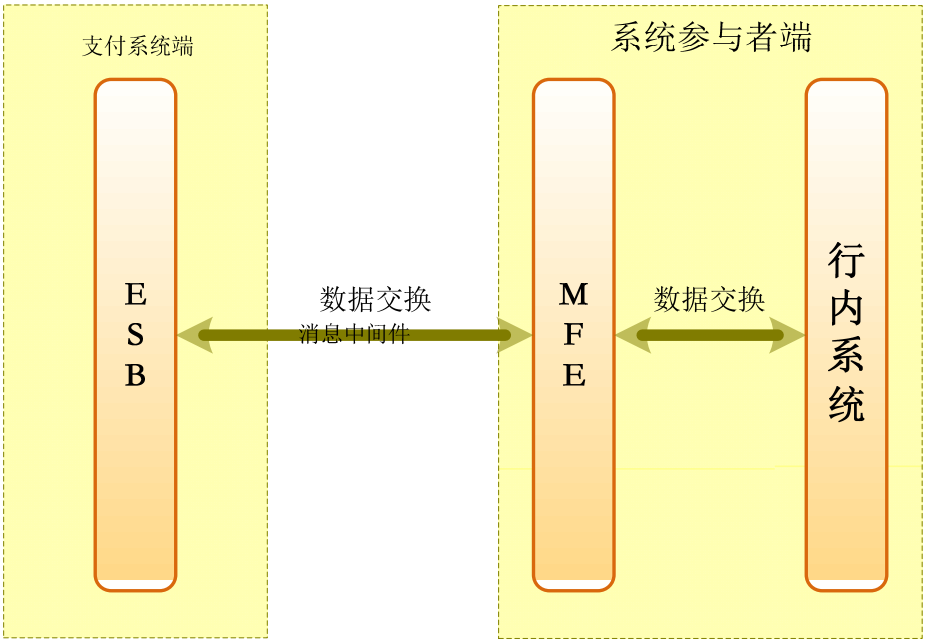
3.3 成员接入前置系统结构

行内使用 MFE 通过支付系统专用网连接第二代农信银支付系统，行内接入端服务器上部署行内接入端软件，物理摆放在行内系统内部，使用消息中间件和支付系统交换业务报文。

系统组成结构示意图如下：



行内通过 MFE 与 ESB 进行报文交换的示意图如下所示：


支付系统端
系统参与者端
ESB
数据交换
消息中间件
MFE
数据交换
行内系统

第四章 成员接入前置系统和行内系统互联说明

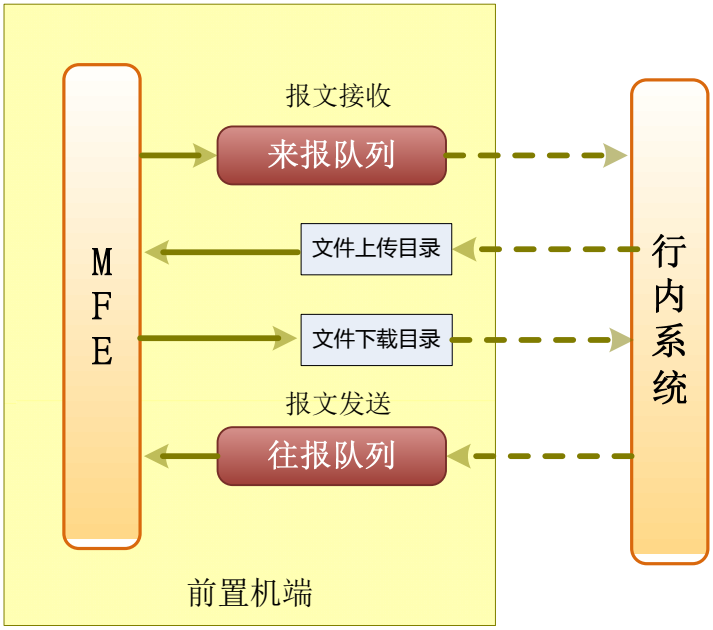
4.1 通信方式

行内系统与 MFE 间可以通过消息中间件 Server-Server 或 Client-Server 模式交换报文，也可以使用自行开发的通讯软件访问 MFE 的消息中间件（Server）实现报文交换。

行内系统向支付系统发送报文时，通过消息中间件或自行开发的通信软件将往帐报文发送到 MFE 指定的消息队列，由 MFE 负责将报文发送给支付系统；行内系统接收支付系统转发的来帐报文时，通过消息中间件或自行开发的通信软件读取 MFE 指定的消息队列获取报文。

行内系统向支付系统发送文件时，先将文件上传至 MFE 的指定发送目录，再通过消息中间件或自行开发的通信软件将文件报文发送到 MFE 指定的消息队列，由 MFE 负责将报文和文件统一发送给支付系统。行内系统接收支付系统的文件时，通过消息中间件或自行开发的通信软件读取 MFE 指定的消息队列获取报文，从 MFE 指定的下载目录中获取文件。

4.2 连接结构



4.3 队列描述

参与业务类型	队列名	
	来报队列	往报队列
农信银二代支付业务	MPS. NCS2.XXX (XXX 为直接参与者行号)	NCS2

人行支付业务	MPS. CNAPS.XXX	CNAPS

4.4 系统互联数据格式说明

4.4.1 第二代农信银支付清算系统业务

4.4.1.1 第二代农信银支付清算系统报文交换标准

为便于成员机构接入支付系统，降低报文转换复杂性，第二代农信银支付清算系统参照人民银行二代支付系统报文规范和 ISO20022 规范进行报文开发，全部报文均采用 XML 格式描述。其中，对采纳使用的 ISO20022 标准报文，根据支付系统的实际情况，进行了必要的格式约束。

行内系统发送报文给支付系统时，应将待发送的往帐报文使用XML Schema进行格式检查，检查通过后，才能提交给 MFE。

行内系统从参与者接入端软件接收报文后，行内系统应使用 XML Schema 对收到的来帐报文进行格式检查，检查通过后，才能提交给行内系统进行业务处理。对检查失败的来帐报文，行内业务人员可以选择主动联系支付系统业务管理人员，对异常来账报文做补发处理；也可选择行内系统直接丢弃，留待日终对账解决。

详细报文交换标准参考农信银《第二代农信银支付清算系统报文交换标准》。

4.4.1.2 第二代农信银支付清算系统基础数据文件格式标准

为便于各成员机构将农信银二代支付系统的各类基础数据导入行内系统或者进行其他处理，第二代农信银支付清算系统提供了基础数据文件。这些数据文件的格式标准具体参考《第二代农信银支付清算系统基础数据文件格式标准》。

4.4.2 人行二代支付系统业务

4.4.2.1 人行二代支付系统报文交换标准

参看人行二代支付系统报文交换标准相关文档。

4.4.2.2 人行二代支付系统基础数据文件格式标准

参看人行二代支付系统基础数据文件格式标准。

4.5 通信层面报文处理规则

为保证系统间报文传输的可靠性，行内系统和支付系统可在接收到对方发送的报文（含 XML/CMT/PKG 格式报文）时给予通信级报文接收确认，该报文使用“通信级确认报文”。需发送通信级确认报文的报文列表参见农信银《第二代农信银支付清算系统报文交换标准》和人行《第二代支付系统报文交换标准》。

对于需要接收通信级确认报文的报文，参与者通信软件发送报文给支付系统时，应标记该报文的发送状态为“待确认”，如果收到支付系统返回的通信级确认报文后，修改状态为“已确认”；如果收到支付系统返回的报文丢弃通知报文后，修改状态为“已拒绝”。对没有收到通信级确认报文或报文丢弃通知报文的往帐报文，应视为没有发送给支付系统，参与者通信软件可以再次提交该报文给支付系统。

对于需要返回通信级确认报文的报文，参与者通信软件收到支付系统转发的来帐报文时，应首先核验报文的数字签名值，如果核验不成功应返回报文丢弃通知报文给支付系统；如核验成功应返回通信级确认报文给支付系统。对没有收到通信级确认报文或报文丢弃通知报文的来帐报文，支付系统视为没有发送给参与者，可能会再次发送该报文给参与者。参与者通信软件应提供来帐报文的重复报文检测机制，检查来帐报文报头的报文标识号，对报文标识号重复的报文，应视为重复报文，可以直接丢弃。

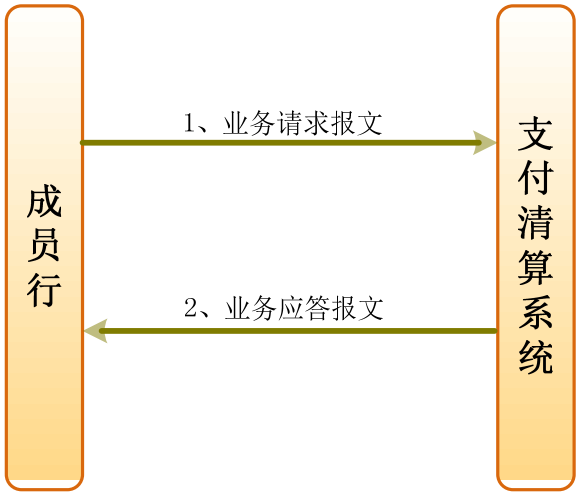
支付系统和参与者均不对对方返回的通信级确认报文或报文丢弃通知报文再返回通信级确认报文。

4.6 业务层面报文处理模式

行内系统与支付系统间有以下五种业务级报文交换模式，具体业务报文处理模式参见农信银《第二代农信银支付系统报文交换标准》和人行《第二代支付系统报文交换标准》。

4.6.1 模式一

（1） 示意图

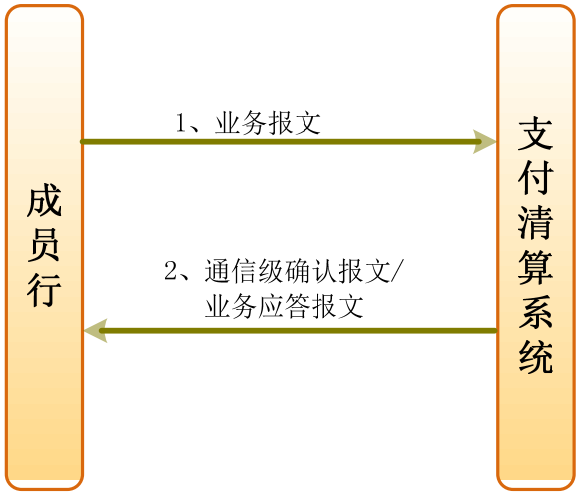


（2） 说明

成员行行内系统发送业务请求报文给支付清算系统，支付清算系统接收该报文，根据业务流程的不同，并向发起成员行返回相应业务应答报文。

4.6.2 模式二

（1） 示意图

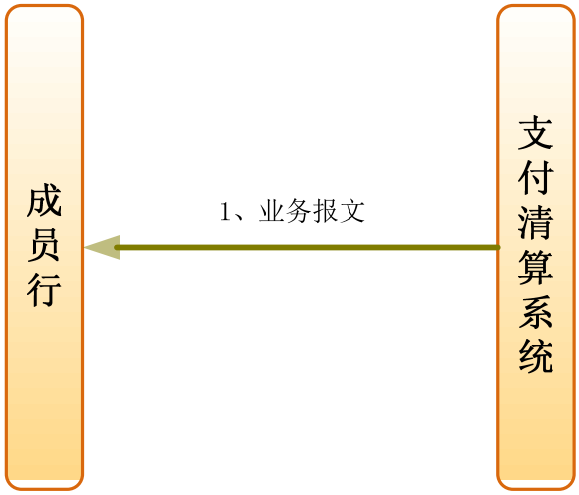


（2） 说明

成员行行内系统采用存储转发形式发送业务报文给支付清算系统，支付清算系统接收该报文，并向发起成员行返回通信级确认报文或业务应答报文。

4.6.3 模式三

（1） 示意图

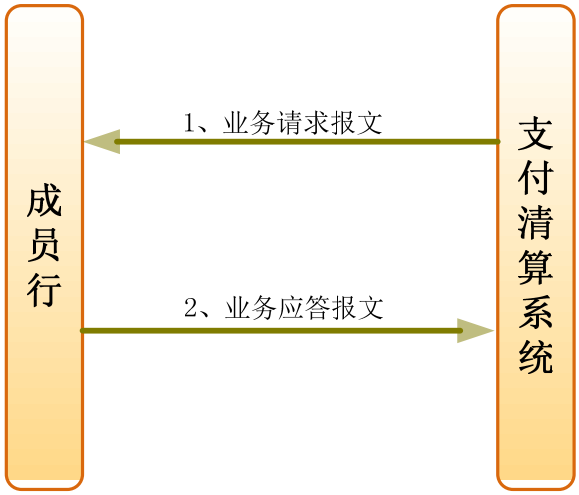


（2） 说明

支付清算系统发送报文给成员行行内系统，成员行行内系统接收该报文，无须返回报文给支付清算系统。对这类报文，成员行行内系统业务检查失败、核签失败的，应直接丢弃该报文。

4.6.4 模式四

（1） 示意图

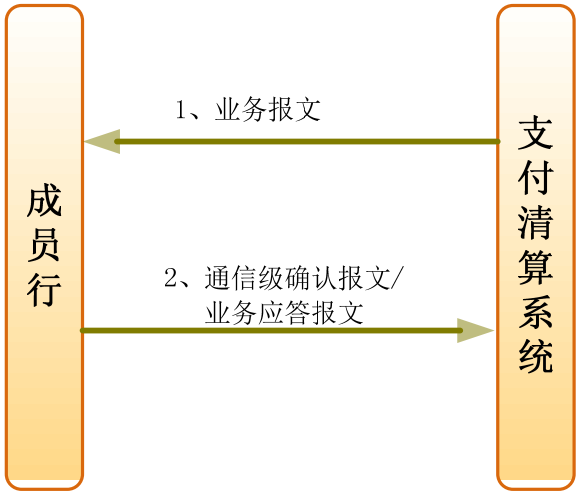


（2） 说明

支付清算系统发送业务请求报文给成员行行内系统，成员行行内系统接收该报文，并向支付清算系统返回相应业务应答报文。

4.6.5 模式五

（1） 示意图



（2） 说明

支付清算系统采用存储转发形式发送业务报文给成员行行内系统，成员行行内系统接收该报文，并向支付清算系统返回通信级确认报文或业务应答报文。

第五章 中心与成员机构应用系统安全

5.1 安全概述

第二代农信银支付清算系统与成员机构应用系统之间由于通过公众互联网络交换信息与指令。为保证支付信息的安全传输，成员系统与清算系统之间的网络连接必须采用相应的安全措施，不得与其他非支付信息传输（如办公自动化、互联网等）共用一个网络，并使用防火墙进行隔离。

第二代农信银支付清算系统安全体系针对来自网络的安全威胁进行分析，将网络的安全威胁分为以下几种：

5.1.1 信息泄密

报文中交换的客户信息与交易指令均有私密性要求。在第二代农信银支付清算系统安全规范中，需要确保在网络传输中对客户与交易信息私密性的保护。

解决方案：将双方的通信报文做加密处理，确保密文传输。

5.1.2 交易指令篡改

如果网络中传输的交易指令被入侵者截获并篡改，就会造成资金处理出现错误，给系统参与者造成损失。因此，在网络传输中，需要保证指令完整性。

解决方案：使用数字证书对对报文中的业务数据进行签名。

5.1.3 交易指令伪造

如果有入侵者冒充中心发起交易指令，就会造成资金在未得到系统参与者的授权下发生流动，给中心或客户带来损失。因此，在网络传输与系统处理中，需要保证指令的真实性。

解决方案：使用数字证书对对报文中的业务数据进行签名。

5.1.4 交易指令否认

当发生交易纠纷时，双方需要通过交易指令确定责任方。第二代农信银支付清算系统安全规范中需要为交易指令防否认提供技术支持。

解决方案：使用数字证书对报文中的业务数据进行签名，中心与系统参与方均应保留涉及资金变动的交易报文日志。

5.1.5 交易指令重播

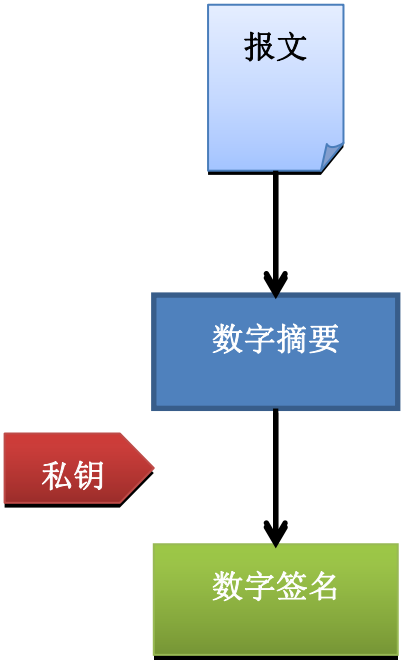
入侵者也可能尝试通过截获网络中传输的交易指令，并多次重播的方式试图发起未经授权的交易。在第二代农信银支付清算系统安全规范中，需要防止交易指令重播引起的未授权交易。

解决方案：凡涉及到资金变动的交易指令，流水号必须唯一。中心与系统参与方均需要保证同一流水号的交易指令只能执行一次。

5.2 数字签名

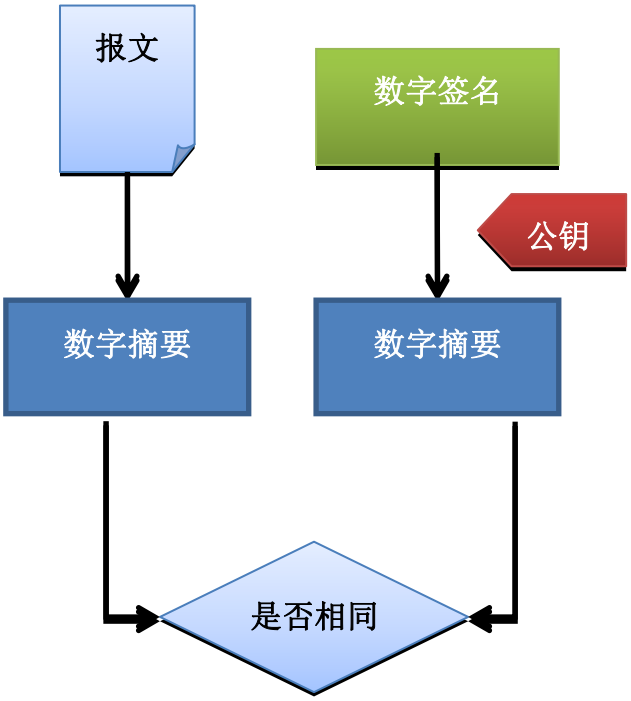
为了保证系统参与者与支付系统之间关键业务数据可靠性和不可抵赖性，系统参与者发起需加、核签业务报文时，应对其加编数字签名，而接收此类报文时，需核数字签名。对业务量较大的参与者，可以考虑在行内系统部署专用的硬件签名服务器，以实现快速的编签、核签处理。对业务量较少的参与者，可以不必部署专用的硬件签名服务器，而使用软件加、核签方式（例如：可以采用 OpenSSL 实现）。

- **发送方成员机构加签过程**



发送方成员机构首先将需要加签的报文业务要素采用摘要算法计算出摘要信息，之后使用发送方成员机构的私钥证书对数字摘要值进行数字签名，并将返回的数字签名结果放到相应的数字签名域中。

- **接收方成员机构验签过程**



接收方成员机构接收到需要核签的报文后，首先计算出报文的摘要信息一；之后获取报文中数字签名域中的数字签名值，使用发起方成员机构的公钥证书计算出对应的摘要信息二，比较两个摘要信息是否相同，如相同则代表核签成功。

5.2.1 CFCA证书申请

各系统参与者自行向 CFCA 申请数字证书，具体申请办法参见《第二代农信银支付清算系统 CFCA 证书使用指引》

5.2.2 CFCA证书绑定

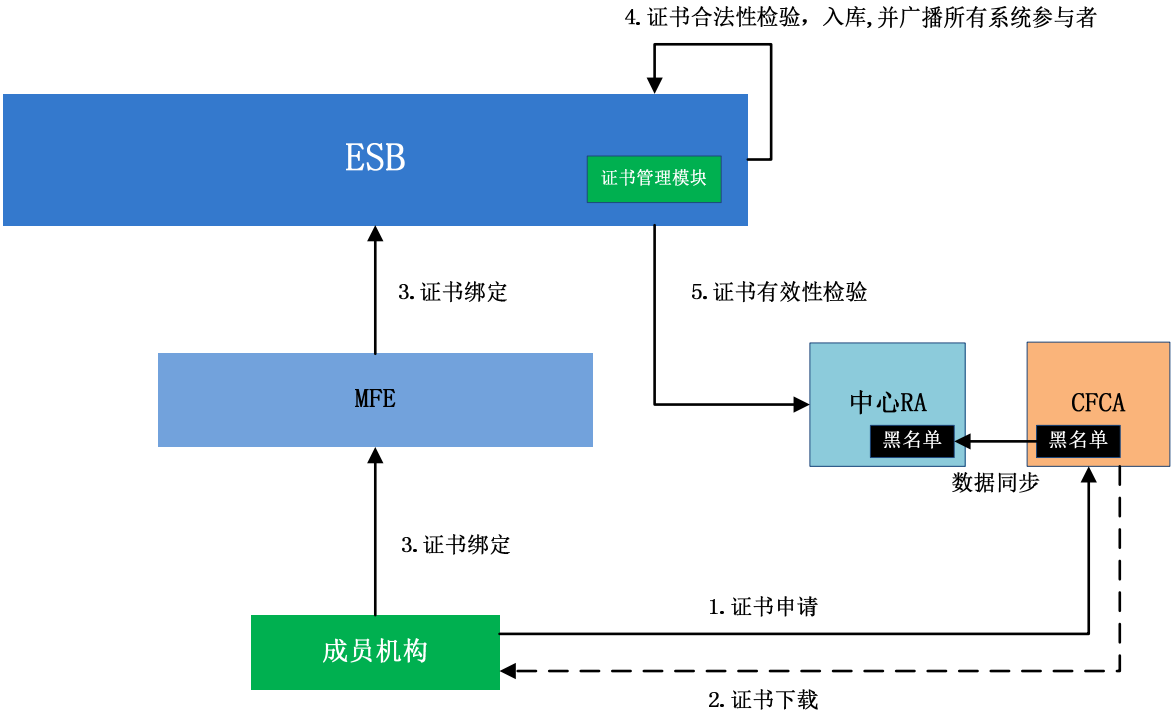
各系统参与者向 CFCA 申请数字证书。然后向中心 ESB 系统发送“数字证书绑定申请报文”报文，将证书绑定后才可以使用数字证书进行业务处理。

5.2.2.1 基本原则

1. 数字证书和系统参与者行号的绑定、解除绑定操作由各个系统参与者自行完成。
2. 数字证书的换发必须在当日业务完成后（日终）或者当日该行无往帐业务的情况下由证书管理人员完成。
3. 数字证书和行号的绑定操作必须在营业准备阶段完成，绑定解除操作可以在各个系统状态下进行。
4. 中心 ESB 收到系统参与者的数字证书绑定申请报文并处理成功后，立即组织单笔的通知报文转发申请信息给所有系统参与者。系统参与者收到此报文后，更新行内系统的数字证书绑定信息。

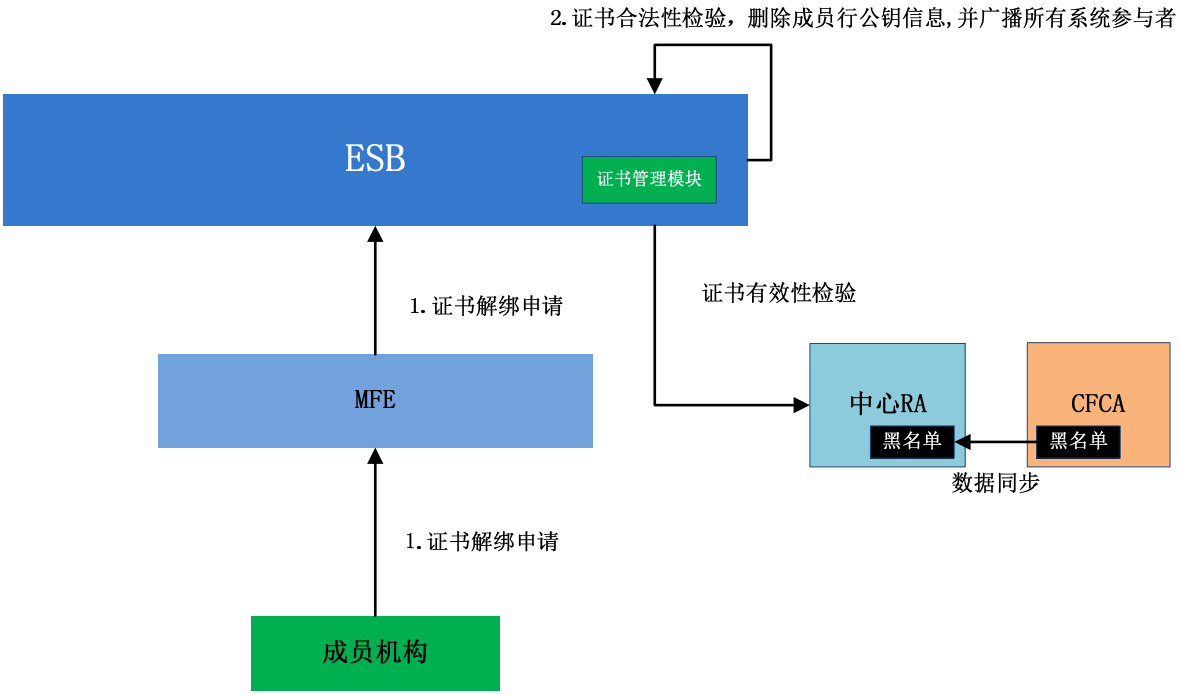
5. 数字证书绑定相关报文都必须加编数字签名。

5.2.2.2 数字证书和系统参与者的新增绑定流程



1. 系统参与者接收到密码信封，从 CFCA 得到证书文件，导入应用系统。
2. 在营业准备阶段，系统参与者录入接入点号码和变更类型，组织证书绑定申请报文发送给 ESB。
3. ESB 接收到证书绑定申请报文，进行合法性检查（核签检查、报文格式检查、系统参与者行号正确、DN 域合法、参考号合法、证书有效期合法等），检查未通过，则返回拒绝的通用确认报文；检查通过则更新该系统参与者的 DN 域、参考号域、证书启用日期等信息；更新成功向申请系统参与者返回成功的通用确认报文。并将本条新增绑定的记录组织数字证书行号绑定关系变更通知报文实时下发给所有系统参与者。

5.2.2.3 数字证书和系统参与者的绑定解除流程



1. 系统参与者由于某种原因（证书丢失等）需要进行证书和行号的绑定解除操作。
2. 系统参与者录入系统参与者行号和变更类型，组织证书绑定解除申请报文发送给 ESB。
3. ESB 接收到证书绑定解除申请报文，进行合法性检查（核签检查、报文格式检查、系统参与者行号正确、DN 域合法、参考号合法、证书有效期合法等），并比较报文中 DN 域和参考号是否和数据库中的一致，检查未通过，则返回拒绝的通用确认报文；检查通过则删除该系统参与者的 DN 域、参考号域、证书启用日期等信息，更新成功向申请系统参与者返回成功的通用确认报文，并将本条解除绑定的记录组织数字证书行号绑定关系变更通知报文实时下发给所有系统参与者。
4. 解除绑定后该行将不能做任何加签业务。

5.2.3 CFCA证书使用

中心与每个成员机构的数字证书以接入点或者系统参与者为单位申请和使用，同一接入点的系统参与者可以使用同一个数字证书，不同接入点的系统参与者不能使用相同的数字证书。

为验证签名者证书的有效性，各系统参与者需自行从 CFCA 获得 CRL 列表，导入系统参与者业务系统，并以 CRL 列表为准保证数字证书的合法性，第二代农信银支付清算系统不提供 CRL 线上更新。双方用 CFCA 标准签名 API 即可完成报文的签名和验签。

5.3 数据加密

5.3.1 PIN字段加密

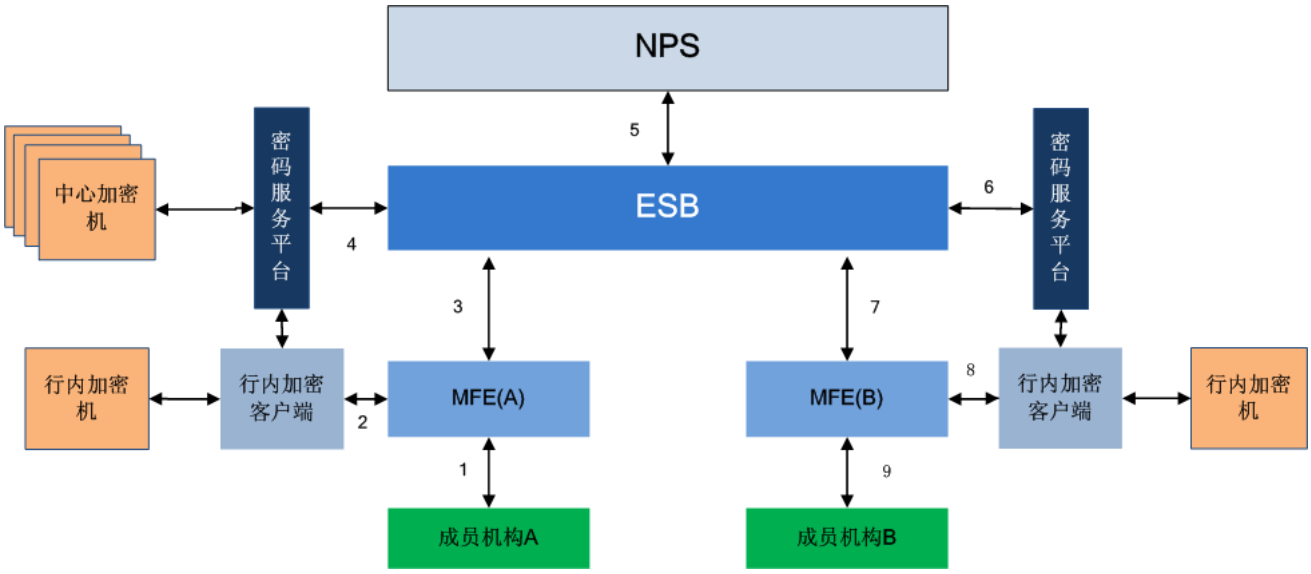
在跨中心信息交换系统中，客户个人PIN的安全性是非常重要的，它直接关系到客户资金安全问题。客户个人PIN安全反映在两个方面：网络传输和主机系统内。

- **密钥**

行内系统与清算中心系统之间的报文中的客户个人 PIN 采用密文方式传输。此密文通过硬件加密机根据标准算法进行加密，使用的密钥是系统行内与清算中心系统约定的一对密钥（zpk）。

行内系统与前置机之间的报文中的客户个人 PIN 采用密文方式传输。此密文根据标准算法进行加密，使用的密钥是成员系统与成员前置系统（MFE）约定的一对密钥（agent）。

- **PIN 字段加密流程**



从发起方行内系统的柜台或 ATM 前端使用行内的安全体系和密钥对客户个人 PIN 明文进行加密，发送给行内系统后台，算法采用标准算法（可逆算法）。在系统后台发送给成员前置系统（MFE）之前，把由行内密钥加密的密文转换为由行内系统与 MFE 约定的 agent 密钥加密的密文（进行 pinblock 的转换，保证不出现 PIN 明文）。

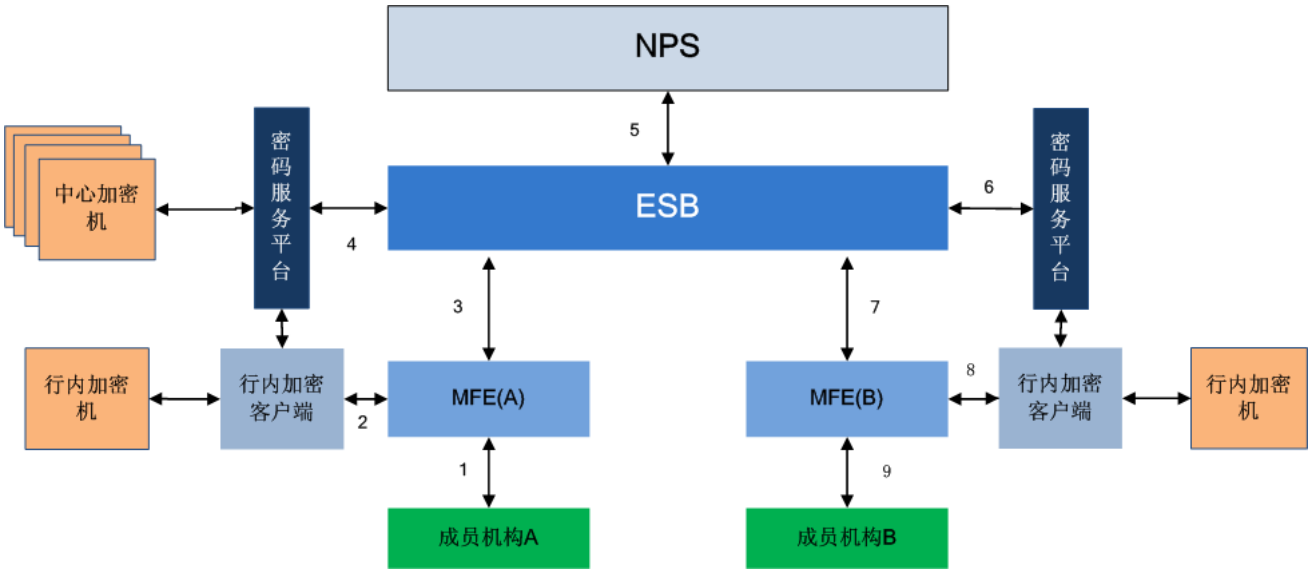
成员前置系统（MFE）接收到发起方行内系统发送的报文后，调用硬件加密机把由 agent 密钥加密的密文转换为由发起方成员机构通过行内加密客户端(BankApi)与中心密码服务平台同步的密钥(zpk)加密的密文，在广域网中以密文方式传输。

接收方行内的成员前置系统（MFE）接收到清算中心系统发送的报文后，把由接收方成员机构行内加密

客户端(BankApi)与中心密码服务平台同步的密钥(zpk)加密的密文转换为接收方行内系统与 MFE 约定的 agent 密钥加密的密文后，传给接收方行内系统。

接收方行内系统接收到前置机发送的报文后把由 agent 密钥加密的密文转换为由行内密钥加密的密文，根据行内系统的要求进行后续处理。

5.3.2 全报文加密



全报文加密与成员系统无关，由成员前置系统（MFE）使用行内加密客户端(BankApi)与中心密码服务平台同步的一对密钥(zek)对全报文进行加密和解密，以保证网络数据传输安全性。

5.3.3 金融加密机介绍

金融数据加密机是基于金融业务主机的应用层数据加密机,主要用于数据加密、消息来源正确性验证、密钥管理等,为计算机网络系统提供安全保密数据通信服务。

保证银行内及银行间各应用系统节点之间进行机密信息的安全传递，一般使用金融加密机。因为银行各应用系统已经配置并使用了金融加密机。

5.3.3.1 金融加密机概述

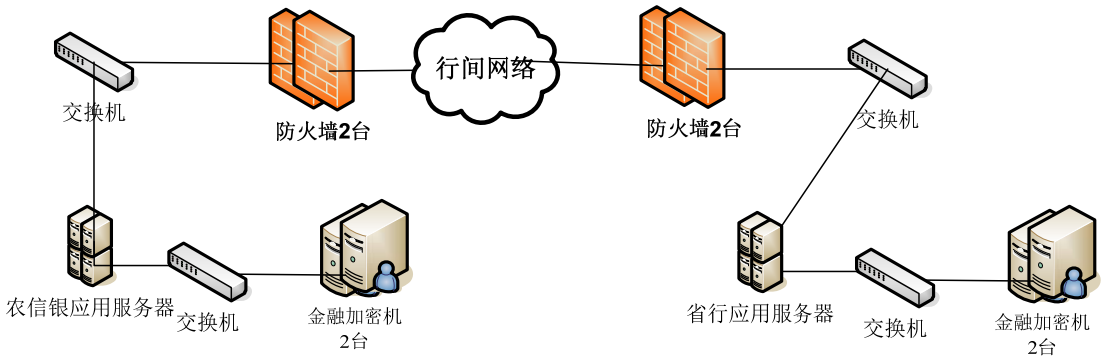
当前使用的金融加密机是被动式加密设备。只保存自己的主密钥 MK。所有的其他密钥都是由 MK 加密后提交给应用 APP 自己管理，包括密钥生成、密钥存储、密钥使用、密钥注销等密钥生命周期都由应用 APP 根据需要自己维护管理。

应用 APP 使用密钥时，将交易数据、使用的密钥密文按加密机提供的标准程序接口提交，得到返回信息。

厂商可以提供密钥管理平台软件（ESSC），ESSC 可以提供更加简单的接口调用，同时进行密钥存储。建

议采购。

5.3.3.2 金融加密机的网络联接



金融加密机是被动设备，农信银的金融加密机要求能被 ESB 服务器访问到。直接联接在 ESB 服务器访问到的区域。

金融加密机和成员机构金融加密机之间不用联接，密钥交换是由相应 APP 负责转发。

5.3.3.3 应用金融加密机需要的密钥

每台金融加密机有自己的主密钥 MK。保证信息加密传递，在两个结点之间需要三对密钥。

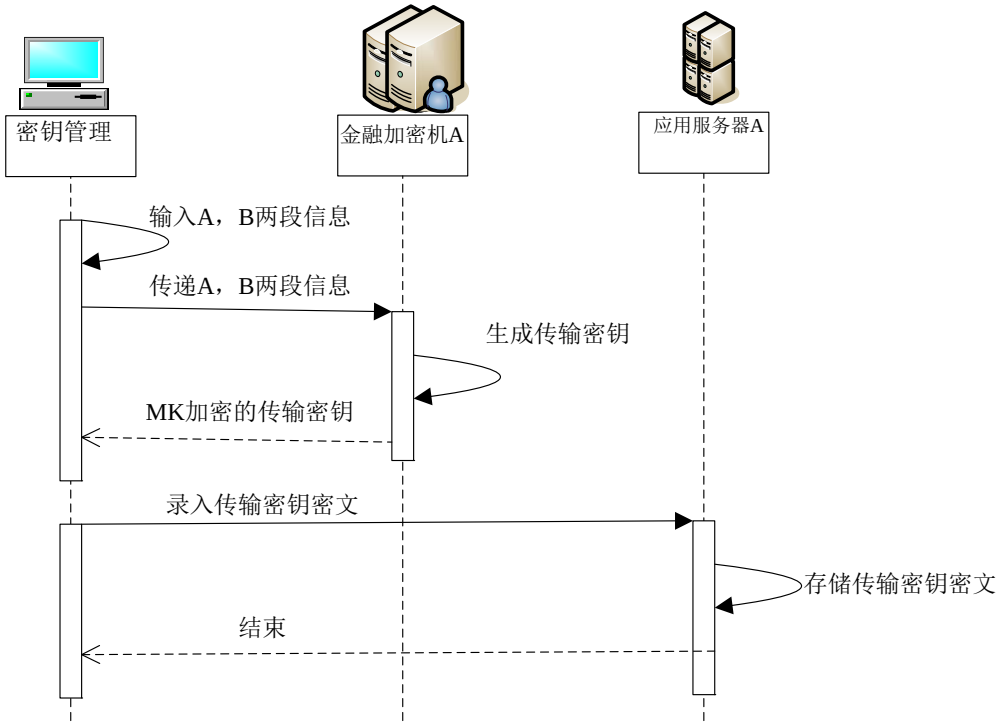
密钥名	简称	说明
传输密钥	ZAK	主要用来协商生成工作密钥，“工作密钥”传递前，使用传输密钥加密。 协作方使用传输密钥解密，获得“工作密钥”
PIN 保护密钥	ZPK	工作密钥。用来对客户 PIN 进行加密，解密的密钥。 般每天一换
消息验证密钥	ZMK	工作密钥。用来验证消息是否正确、是否完整性、是否被篡的密钥。 一般每天一换
全报文加密密钥	ZEK	工作密钥。用来进行全报文加密。 一般每天一换

5.3.3.4 第一次使用金融加密机

第一次使用初始化程序输入 A、B 两段数字，生成 MK。

可以用 IC 卡将 MK 导出备份，导入到备份的加密机。

5.3.3.5 传输密钥的生成、存储



传输密钥的生成与存储过程

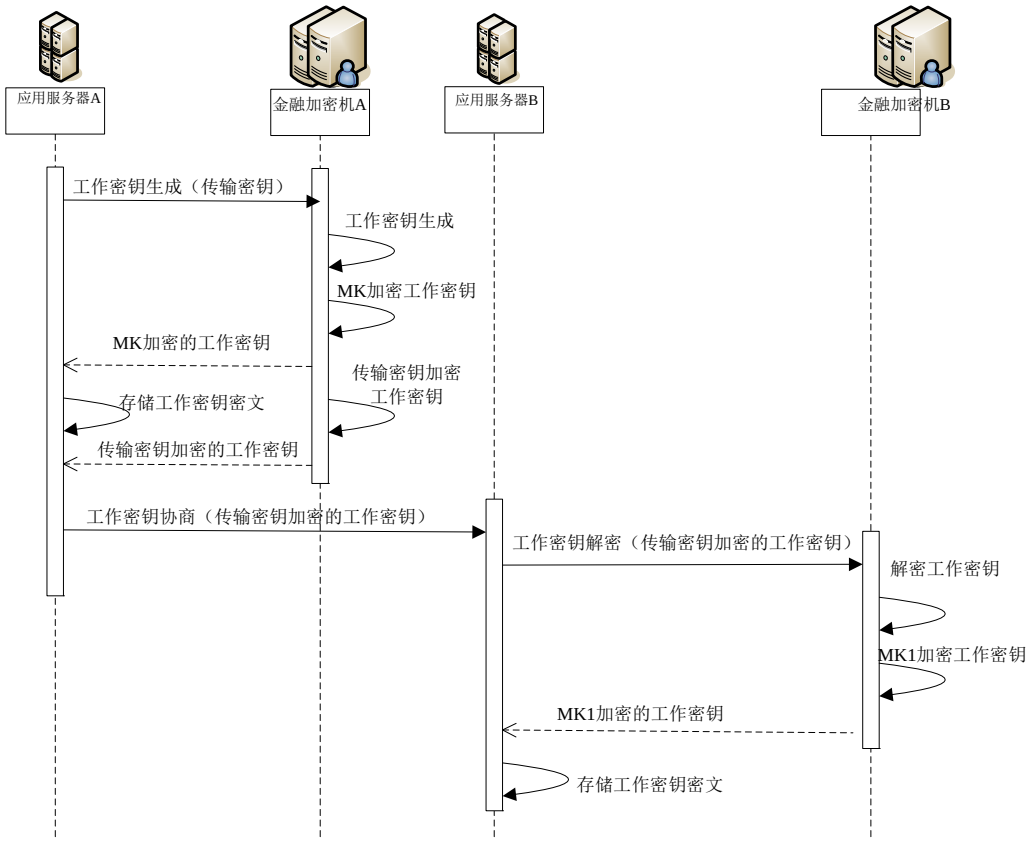
两个系统的加密机协同工作，使用工作密钥，但工作密钥的传递，需要使用共同确定的传输密钥。

由银行工作人员在 PC 上使用厂商提供的传输密钥生成程序，生成传输密钥。加密机返回使用 MK 加密的传输密钥密文。

应用 APP 存储传输密钥密文。

应用 APP 可以用传输密钥更换新的传输密钥。也可以离线重新确定传输密钥。

5.3.3.6 传输密钥的使用（工作密钥的协商生成）



工作密钥生成过程

生成工作密钥时，应用 APP 提交传输密钥密文给金融加密机。加密机将工作密钥用传输密钥加密后返回给应用 APP。

协作的应用 APP 将用传输密钥加密的工作密钥交给金融加密机，加密机返回工作密钥密文。

5.3.3.7 工作密钥的生成、销毁

两个系统的加密机协同工作，每天重新协商工作密钥，一天一密。

需要每天生成“PIN 保护密钥”ZPK，“交易 MAC”密钥 ZMK。

应用 APP 在每天工作开始前启动工作密钥协商，加密机生成工作密钥后，返回工作密钥密文，APP 将工作密钥的密文存储。

新的工作密钥产生后，应用 APP 保留前一天的副本，将前两天的密钥进行销毁。

每天的工作密钥密文 APP 可以存储，以备审计。

5.3.3.8 工作密钥的使用

（一） 客户明文 PIN 加密

APP 在接到交易请求后，提交客户 PIN 明文和“PIN 保护密钥”ZPK 的密文给加密机，生成客户 PIN 密文。

（二） 客户密文 PIN 加密

APP 在接到交易请求后，提交客户 PIN 密文、“PIN 保护密钥”ZPK 的密文、重新加密的“PIN 保护密钥”ZPK1 密文给加密机，生成客户 PIN 密文。

（三） 生成交易 MAC

APP 在接到交易请求后，提交交易信息、客户 PIN 密文、“PIN 保护密钥”ZPK 的密文、交易 MAC”密钥 ZMK 的密文给加密机，生成交易 MAC。

（四） 验证交易 MAC

APP 在接到交易请求后，提交交易信息、客户 PIN 密文、“PIN 保护密钥”ZPK 的密文、交易 MAC”密钥 ZMK 的密文给加密机，验证交易 MAC。返回验证结果。

5.3.3.9 使用金融加密机

使用金融加密机的应用系统，需要完成以下工作。

（一） 存储传输密钥密文

提供界面，由工作人员将传输密钥密文录入并存储。

（二） 启动工作密钥协商

每天工作前，提交传输密钥给金融加密机，启动工作密钥协商并将返回的工作密钥密文传递给下一个系统。

存储工作密钥密文。

（三） 客户 PIN 加密

提交客户 PIN 明文/PIN 密文、需要的密钥密文给金融加密机，生成协作系统需要的 PIN 密文。

（四） 生成交易 MAC

将交易信息提交下一个系统前，提交交易信息、客户 PIN 密文及相应密钥密文给金融加密机，生成交易 MAC。

存储并传递交易 MAC。

（五） 验证交易 MAC

接到交易请求后，提交交易信息、客户 PIN 密文、相应的密钥密文给金融加密机，验证交易 MAC。根据返回的验证结果继续下面操作。

5.4 报文权限控制说明

为了保证业务处理的安全可靠，系统行内需对收发的业务报文进行权限控制。对于无权发送的业务报文应禁止发出。

第六章 系统互联双方需要完成的工作

6.1 农信银中心需要完成的工作

1、 发布《第二代农信银支付清算系统互联规范》和《第二代农信银支付清算系统报文交换标准》。

2、 发布《第二代农信银支付清算系统成员接入前置配置指引》。

3、 发布《第二代农信银支付清算系统成员接入前置安装配置手册》。

6.2 行内系统需要完成的工作

- **行内系统接入第二代农信银支付清算系统需完成的工作：**

1. 按照《第二代农信银支付清算系统成员接入前置配置指引》，准备前置机运行环境。
2. 按照《第二代农信银支付清算系统成员接入前置安装配置手册》，部署 MFE 软件。
3. 准备和配置金融加密机(沿用第一代清算支付系统加密机)。
4. 作为农信银二代支付参与者申请 CFCA 数字证书进行支付报文数字签名。
5. 按照《第二代农信银支付清算系统报文交换标准》，完成支付系统业务报文的开发测试。

- **行内系统通过农信银接入人行二代支付系统需完成的工作：**

1. 按照《第二代农信银支付清算系统成员接入前置配置指引》，准备前置机运行环境。
2. 按照《第二代农信银支付清算系统成员接入前置安装配置手册》，部署 MFE 软件。
3. 准备和配置金融加密机(沿用第一代清算支付系统加密机)。
4. 作为人行二代支付参与者申请 CFCA 数字证书进行支付报文数字签名（证书私钥需要存放在农信银中心）。
5. 作为农信银二代支付参与者申请 CFCA 数字证书进行支付报文数字签名（此证书与上述作为人行二代支付参与者数字证书不能相同）。
6. 按照《人行二代支付系统报文交换标准》以及人行二代支付下发所有相关文档，完成互联规范中要求的有关支付系统业务报文的开发。