第二代农信银支付清算系统

成员接入前置

配置指引

文档编号：	NXY_NCS2_D07
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	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 文档目的

本配置指引用于指导农信银第二代支付系统参与者按照配置指引描述，准备参与者接入端软件部署所需的软硬件设备。

本配置指引的期望读者包括：农信银二代支付系统参与者的系统建设人员及其他相关人员。

1.2 参考资料

《第二代农信银清算支付系统(NCS2)与成员机构行内系统互联规范》

1.3 引用标准

GB/T 8567-2006《计算机软件文档编制规范》，该标准由中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会 2006 年 3 月 14 日发布。

第二章 成员接入前置系统(MFE)简介

2.1 应用功能

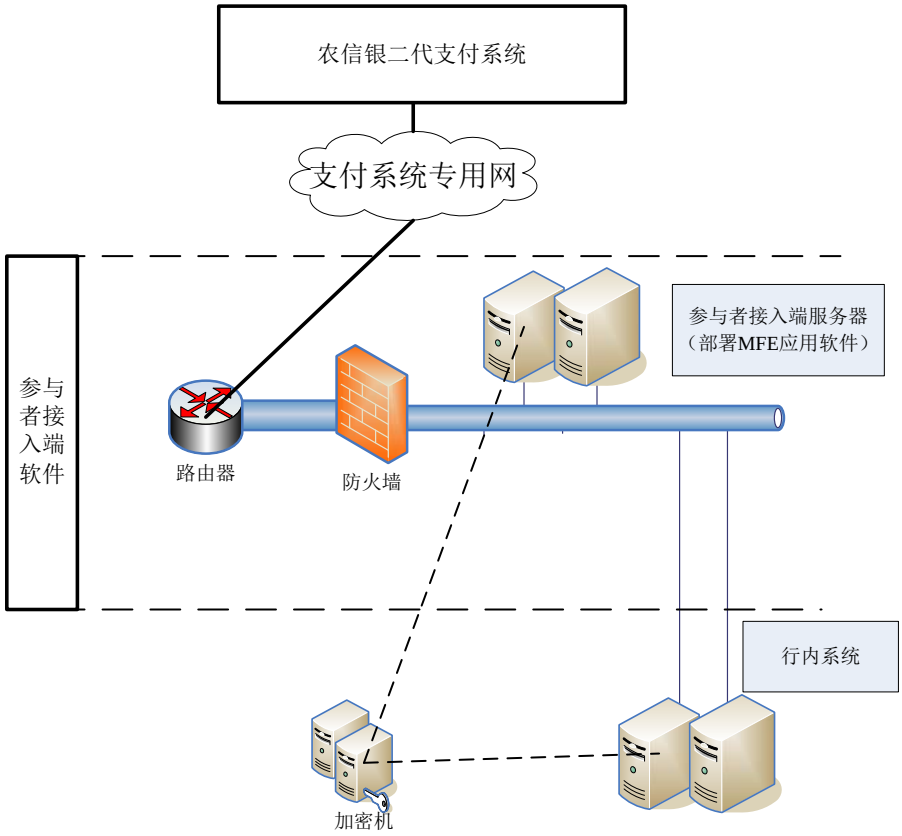
成员接入前置系统（MFE）是连接支付系统和行内系统的桥梁，是支付系统的重要组成部分。MFE 的主要功能包括报文转发、报文格式检查、安全管理等，即对行内系统提交的报文和支付系统发来的报文进行相应的报文格式检查，并根据系统安全规范实现报文的可靠传输和交换。MFE 不参与业务相关处理，如业务合法性检查、重账检查、业务核对等，以降低其运行维护复杂度。

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，物理部署在系统行内端，并由系统行内进行系统维护与管理。

2.2 系统结构

系统行内使用 MFE 通过支付系统专用网连接第二代支付系统，行内接入端服务器上部署行内接入端软件，物理摆放在系统行内系统内部，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：



第三章 成员接入前置系统软硬件配置指引

3.1 概述

按照参与者业务量的不同，推荐两类直联前置机配置分别对应不同需求：

类型	报文业务笔数/天	适用对象
基于 AIX 前置机	>20000	业务量较大的参与者；
基于 Linux 前置机	<=20000	业务量较小的参与者；

注：

1. 直联前置机的运行环境不要求必须新购设备，但运行环境需满足以下配置要求。

3.2 基于AIX操作系统的前置机配置指引

3.2.1 硬件需求

IBM P 系列服务器。

3.2.2 软件需求

- **操作系统**

AIX 6.1 以上。

- **消息中间件**

IBM WebSphere MQ 7.0 版本以上或 Tonglink/Q 7.0 版本以上。

对于该接入方式，以下系统软件通过了测试，建议用户采用：

软件	**版本**	**备注**
操作系统	AIX 6.1	
IBM WebSphere MQ	7.0.1.5	

3.2.3 性能指标参考

指 标 项	要 求	附 注
机型	低档 64 位 UNIX 服务器，采用 SMP 结构	
CPU	数目>=2，主频>=1.5G 赫	
CPU 缓存	>=2MB/CPU	

TPM-C 值	>=50000，可扩展到 100000 以上	
总线带宽	>=1GB/s	
内存	4GB 或以上	
提供 I/O 插槽	>=5	
内置硬盘	数目>=2，单盘容量>=140GB，转速>=10000 转	
网络接口	10/100/1000 以太网	
其它	配置光驱、键盘、鼠标、磁带机等等自选设备	

3.3 基于Linux操作系统的前置机配置指引

3.3.1 硬件需求

高档 PC 服务器， CPU 主频 1.5GHz 以上，内存 1G 以上。

3.3.2 软件需求

- **操作系统**

Red Hat Linux Enterprise。

- **消息中间件**

IBM WebSphere MQ 7.0 版本以上或 Tonglink/Q 7.0 版本以上。

对于该接入方式以下系统软件通过了测试，建议用户采用：

软件	**版本**	**备注**
操作系统	Red Hat Linux Enterprise	
IBM WebSphere MQ	7.0.1.5	

3.3.3 性能指标参考

指 标 项	要 求	附 注
机型	PC 服务器	
CPU 个数	≥2	
CPU 主频	≥1.5Ghz	

CPU 缓存	≥2MB	
内存	≥4GB，ECC 或更好 扩展能力>= 16GB	
RAID 阵列卡	支持 RAID1、RAID5	
RAID 卡带内置硬盘	（≥100GB）×2	
可靠性	冗余热插拔电源、风扇	
网卡	基本要求：64 位 PCI Ethernet 10Mbps/100Mbps/1000Mbps 全双工 配置数量：>=1。	
其它	配置光驱、键盘、鼠标、磁带机等等自选设备	

3.4 签名验签服务器配置指引

第二代农信银支付清算系统采用数字签名保证业务数据的可靠性和抗抵赖性。参与者发送往帐业务报文前，需加编数字签名，接收来帐业务报文后，需核验数字签名。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 CFCA 提供的 API 完成数字签名的编制和核验。根据测试结果，如参与者峰值业务量超过 10000 笔/小时，建议配置签名服务器。第二代农信银支付清算系统的数字签名机制采用的是目前业界的标准数字签名算法（PKCS#7 或 PKCS#1 裸签），参与者可根据情况自行选配符合要求的签名验签服务器，并在业务联调期间和农信银中心验证签名验签服务器的互操作性。具体测试指标如下表：

加核签方式	加签 TPS	验签 TPS	备注
硬件签名服务器加核签方式	150	500	基于格尔签名验签服务器 E-2010 参数指标
CFCA 软件加核签方式	70	80	基于 IBM P7（4 核 CPU、3G 内存）测试机测试得出，CPU 平均使用率 15%。

3.5 硬件加密机配置指引

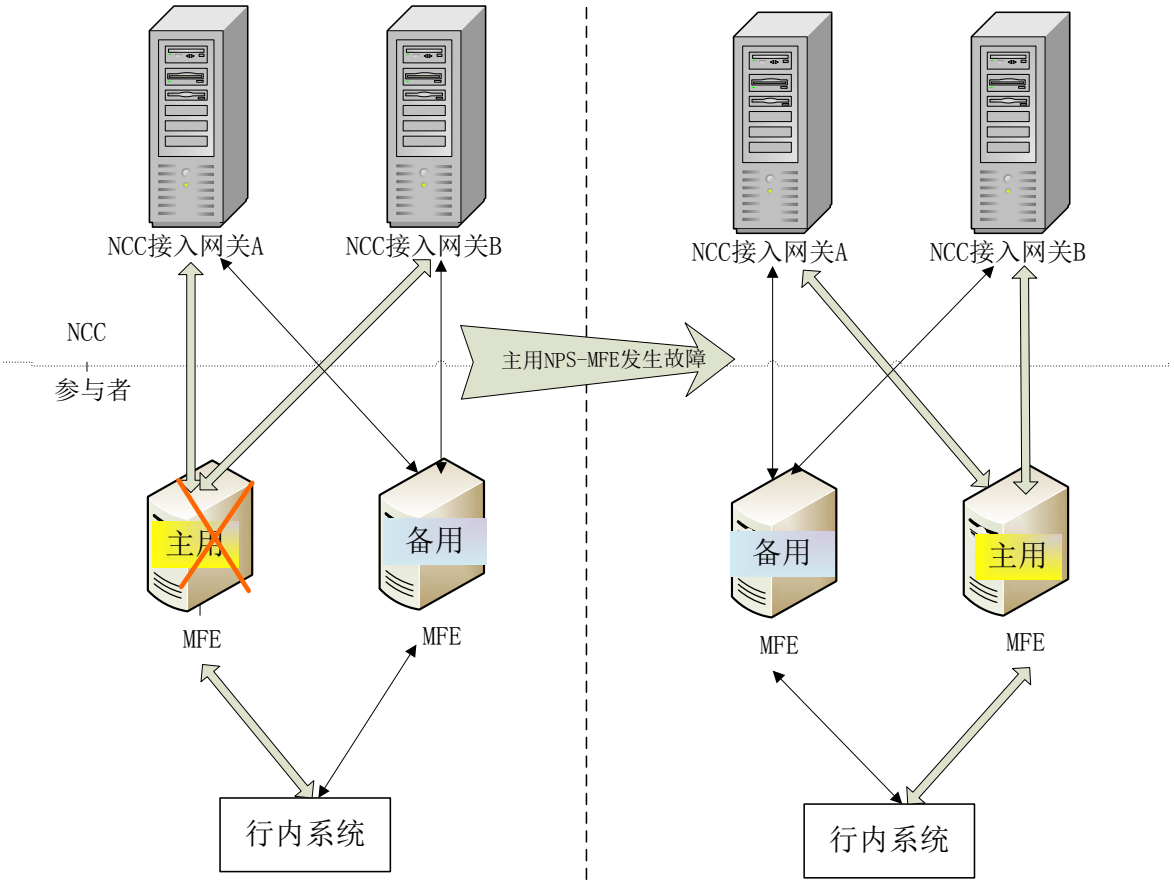
第二代农信银支付清算系统采用数字加密方式来保证数据传输的私密性。参与者接入端软件发送往帐

业务报文前，需对 PIN 字段进行转加密和对全报文加密，参与者接入端软件接收到来帐业务报文后，需对 PIN 字段进行转加密和对全报文解密。参与者接入端软件使用行内加密客户端(BankApi)与中心密码服务平台同步密钥，加密解密过程需要通过行内硬件加密机完成。需参与者配置硬件加密机，可沿用第一代支付系统使用的硬件加密机。

3.6 部署建议

3.6.1 主备模式

主备模式下，主用直联前置机与 NCC 两台服务器连接，负责完成报文收发。备用直联前置机同时保持与 NCC 服务器的连接，具备与支付系统接入网关的报文收发链路，但正常情况下不启用报文收发功能。当主用直联前置机发生故障时，可即时启用备用直联前置机的报文收发功能，将其切换为主用直联前置机，同时将原主用直联前置机置为备用模式。部署示意图如下：



注：NCC接入网关的地址，农信银中心将在上线时统一向参与者公布。