XX 公司

WY 项目

概要设计说明书

版本： V0.1

部　门	**研发部**
撰　写	**WY 项目组**
文档编号	WY_PD_V0.1

修订记录

版本号	日期	章节号	简单描述	修订者
V0.1	2014-02-15		拟定框架	秦金卫

目录

1. 简介

根据 WY 系统的功能性需求和非功能性需求，提出系统的总体技术架构和设计框架。

1.1 目的

指导详细设计、开发、测试等工作。解决系统中的技术问题。

1.2 范围

本文档依据对《WY 项目功能需求分析》的分析结果编制，阐述了即将开发的软件系统必须提供的功能和特点以及它所要考虑的约束条件，对总体功能以及功能实现流程有明确的描述。

1.3 概念与名词定义

WY：

1.4 参考资料

- 《软件需求规格说明书》
- 《小额支付系统报文格式标准》
- 《WY 项目功能需求分析》

2. 关键需求说明

2.1 项目背景

随着

2.2 功能性需求简介

2.2.1 系统使用范围及业务管理模式

2.2.2 基本业务流程要求

2.2.2.1 用户管理子系统

XX

。

2.2.2.2 公共管理子系统

XX。

2.2.2.3 报文接口子系统

XX。

2.2.2.4 准入审批子系统

XX。

2.2.2.5 参数维护需求

参数维护是对联网系统中涉及到的可变项目进行增删、修改等设置，使系统可以适应不同资金清算方式、不同业务类型的需求。参数维护是联网系统正常运行的核心所在。

2.2.3 系统用户管理需求

系统分系统管理、查询、监控、操作等四个类型。

为保证联网系统的安全与可靠，系统应建立用户管理信息库，用来设置用户代号、口令和权限

用于操作员定时或不定时地修改自已进入联网系统的口令。

2.2.4 异常处理需求

当系统在运行过程中，发生死机、断电、日志满、程序出错等异常，系统不能正常运行，需要系统维护人员进入系统进行异常情况处理，保证系统能够正常运行。

2.2.5 系统初始化需求

系统初始化将清除系统所有数据及参数，置初始化状态。

2.2.6 数据备份与恢复需求

数据备份是指将全部的 WY 系统数据保存在硬盘、软盘、磁带、光盘等介质中。WY 系统数据包括业务数据的备份和环境参数的备份，一般情况下凡是变化的业务数据及环境参数都需备份；能按日、按月、按年进行备份；能选择备份的目的盘，如硬盘、软盘、光盘或远程备份等。为保证 WY 系统处理的连续性与安全，系统应实现以下备份方式:

(1) 双机热备份。

(2) 定时备份。如系统未配备两个服务器，则系统定时将数据库备份到本机或另外一台微机上，备份时不能采取覆盖方式。

(3) 重要时刻备份。在进行对账表信息有重要改变时，且这种改变有可能因故障而中断的重要操作前，如日终轧账，系统应在重要操作前自动在硬盘上完成数据的备份。系统只保留最近一次重要操作前的硬盘备份

①自由时间备份。用户可在任何时间完成对数据的备份。

②系统可根据用户要求，有选择地进行备份。

数据恢复是将当日、上日或以前的备份数据恢复到系统的操作。

由于意外原因导致系统数据出现错误，可利用自己备份数据进行恢复，恢复到

所备份的数据的那一时刻状态。因为联网系统系统是一个实时信息处理系统，与各子系统、物流企业、金融机构、担保公司存在着实时信息往来，因此数据恢复要非常谨慎。恢复只有 WY 系统主管或系统管理员才能操作。进行此操作须谨慎，操作前系统应有警告提示。

系统应提供稳定可靠的恢复操作，保证国库账务处理的及时与连续。数据恢复分以下三种情况处理：

1、无信息往来数据恢复

无信息往来数据恢复是指在做数据恢复操作前到要恢复的数据段之内，WY 系统与各子系统、物流企业、金融机构、担保公司之间无信息数据的发送和接收。

2、有信息往来数据恢复是指在作数据恢复操作前到要恢复的数据段之内，WY 系统与各子系统、物流企业、金融机构、担保公司之间有信息数据的发送和接收。

2.2.7 运行管理需求

系统应提供包括设定日切时间、系统时钟管理、各交换单位连接状态、用户登录情况等等涉及保证系统正常运行及反映、监控系统状态的功能。

2.3 非功能性需求说明

2.3.1 可靠性

2.3.1.1 系统可用率

系统需要 7*12 小时连续不间断运行；

一部分子系统需要 7*24 小时运行。

2.3.1.2 系统故障处理要求

系统正常运行连续无故障时间不得低于 1000 小时，出现故障时，平均修复时间不得超过 1 小时，重大故障修复时间不得超过 4 小时。

2.3.2 性能

2.3.2.1 系统响应时间

(1) 在不考虑外部其他系统的处理时间的情况下，信息在 WY 系统内部的处理时间最长不超过 3 秒。

(2) 系统登录时间最长 3 秒；

(3) 从报文或文件进入系统到接收回执时间不超过 5 秒；

(4) 报文或文件传输不成功时，在 3－5 秒时间内通知发送者；

(5) 因某种原因，报文或文件滞留在系统中时，应在 30 秒时间内向发送者发出提示信息。

2.3.2.2 系统吞吐量

(1) 系统的最大处理能力要求能够达到 2000 笔/秒；

(2) 系统的平均处理能力要求能够达到 300 笔/秒；

(3) 系统最大并发在线连接用户数要求能够达到 4500 个；

(4) 系统平均并发在线连接用户数要求能够达到 2000 个；

(5) 系统 CPU 最高利用率不能超过 70%；

(6) 工作时间系统 CPU 平均利用率最好不低于 10%；

(7) 系统存储容量最高需求为 6TB，当前需要 3TB。

2.3.3 可支持性

代码标准参考人民银行代码标准体系

2.3.4 设计约束

2.3.4.1 运行环境

(1) 系统运行基于互联网；

(2) 安全认证采用统一的安全认证措施；

(3) 数据存储基于数据中心统一存储区域；

(4) 充分利用水平扩展能力实现负载均衡；

(5) 代码标准参考人民银行代码标准体系。

2.3.4.2 开发环境

(1) 采用多层架构；

(2) 符合互联网金融系统的总体技术路线；

(3) 基础软件如数据库、中间件遵循成熟开源软件的选型要求；

(4) 支持异构硬件平台，可与其他系统进行整合。

2.3.4.3 系统结构

(1) 适应业务发展需要，灵活的采用水平或垂直的扩展技术提升性能；

(2) 多机房多线部署，提升不同地域不同网络用户的访问体验；

(3) 数据采取两地三中心的容灾备份结构，保证数据的高可用和安全性；

(4) 整个系统结构遵循 SOA 架构风格，满足 WY 系统内部业务子系统的快速扩展、业务和流程的全面治理、与不同的外部系统高效集成整合需要。

3. 需求分析

3.1 系统逻辑框架

系统逻辑框架如上图所示：

3.2 机构组织结构设计

3.3 系统配置参数管理设计

3.4 系统运行流程设计

3.5 子系统 xxx

xxx。

3.6 子系统 xxx

xxx。

3.7 子系统 xxx

xxx。

3.8 子系统 xxx

xxx。

3.9 子系统 xxx

xxx。

3.10 用户授权管理方案

3.11 日志管理需求分析

系统日志可分为底层平台日志、应用运行日志、交易跟踪日志三类。其中：

- 底层平台日志：指由底层平台或中间件记录的日志。如 MQ、WebServer 记载的各种日志。
- 应用运行日志：指由应用框架程序记录的各种日志。
- 交易跟踪日志：指由上层应用记录在数据库中的各种日志。包括报文流水日志、业务操作日志等。

这三类日志中底层平台日志负责记录详尽的系统平台运行状况，主要用于联调测试阶段的错误追踪和调试；应用运行日志负责记录系统应用框架运行状况和任务运行情况，主要用于联调测试阶段的错误追踪、调试，以及系统运行过程中的对异常数据的追查和锁定；交易跟踪日志记录在数据库中，负责记录交易运行轨迹和关键业务操作动作，主要用于异常数据的追查、锁定和重大业务操作的监督、审计。

3.12 定时任务管理需求

3.12.1 概述

WY 为全国性的系统，系统中各种任务多种多样。为简化人员操作复杂程度，减轻维护人员工作量，保证系统自动运行，WY 应提供定时任务自动调度机制，并可灵活调整任务执行时序。

3.12.2 定时任务调度分类:

为了清楚的说明系统中对定时任务的控制需求。下面根据业务需求和业务流程要求简要归纳了一下系统任务运行时序。同时，为说明问题，特意假设了各个任务的执行时间。

序号	起始时点	任务启动方式	系统状态	工作日	任务	执行人
1.	16：00～次日16：00		日间	T		
2.	8：00～16：00	手工/自动	日间	T		
3.	8：00～16：00	自动	日间	T		
4.	16：00～次日16：00	自动/手工	日间/日切窗口	T		
5.	16：00～16：10	自动/手工	日切窗口	T+1		
6.	16：10～17：00	自动/手工	日间	T+1		
7.	17：00～17：30	自动/手工	日间	T+1		
8.	17：30～20：00	手工	日间	T+1		

9.	20：00~21：00	后台自动服务	日间	T+1		
10.	22：00 开始	自动/手工	日间	T+1		
11.	24：00 开始	自动/手工	日间	T+1		
12.	1：00 开始	自动/手工	日间	T+1		
13.		自动/手工	日间	月末日		
14.	6：00 开始	自动/手工	日间	T+1		

如上表所示，我们可以从不同的角度出发，将任务分为不同的类别。

按执行日期分类，可以分为工作日依赖型和自然日依赖型两类任务。其中，工作日依赖型任务指任务的启动依赖工作日期而非系统日期（自然日），如开启日切窗口、关闭日切窗口只能在每个工作日执行一次，遇到节假日需要顺延；自然日依赖型任务指任务的启动依赖系统日期（自然日）而非工作日期，如数据转移任务、转发批量扣税业务等等，只要到达指定时间立即启动。

按执行时间分类，可以分为每日一次和多次执行两类任务。其中，每日一次执行任务指每日只执行一次，不允许多次执行的任务，如开启日切窗口、关闭日切窗口等等；每日多次执行任务指每日可以执行多次的任务，如转发批量扣税业务、银行端缴税核对任务等等。

按任务关联性分类，可以分为关联任务和非关联任务两类。关联任务指此任务执行是以其它任务作为前置或后置条件的，如开启日切窗口、关闭日切窗口、与商业银行进行日切对账、与征收机关进行核对就是一组关联任务，前一任务不完成不得进行后一任务；非关联任务指此任务执行是独立的，不以其它任务作为前置或后置条件，如数据转移、转发批量扣税业务等等。

3.12.3 定时任务调度器的设计要求:

通过上面的分析，可以看出定时任务调度器应具备以下功能:

- 任务可以定时启动执行;
- 可以控制节假日顺延执行，并可对节假日进行管理;
- 可以设置关联任务的关联关系;
- 一个任务可以多次执行，并且时间可调;

3.13 历史数据的保留和清理

每日夜间或系统不繁忙的时候，系统会将已完成的交易转入历史数据库。为避免运行数据库中历史数据逐步增加占用过多空间，保证系统实时交易处理效率，系统中应提供数据整理功能。在系统中设置统一的可调整的数据清理周期（如 90 天），通过数据整理功能，将超过该时间的历史数据自动或手动清除。

对于 xxx

对于实时操作、批量同步、手工录入业务（税票、退库、更正、免抵调），由于交易的生命周期在可控范围内，因此系统在执行数据清理功能时，应清除“当前工作日 – 最后操作日期（时间戳）＞数据清理周期”，且交易已经处理完成的数据。

系统中还存在一些其他辅助交易，如冲正、止付、自由格式报文、日志和键值登记表等等。这些信息的清理采用清除“当前工作日 – 最后操作日期（时间戳）＞数据清理周期”的原则。

3.14 功能列表

xxx
xxx
xxx
xxx

4. 总体技术框架和实现策略

4.1 技术路线选型

4.1.1 选型原则

WY 系统技术路线的选型遵循以下原则：

1、采用多层架构；

2、符合人民银行的总体技术路线；

3、基础软件如数据库、中间件遵循人民银行的选型要求；

4、支持异构硬件平台，可与人民银行其他系统进行整合；

5、灵活适应省级数据集中处理或全国数据集中处理两种部署模式；

6、广泛支持外联机构从地市、省会城市甚至全国任一节点接入。

4.1.2 J2EE 技术路线的选择

在对系统业务需求和性能需求分析的基础上，我们对系统所面临的关键技术问题进行了分析。由于所要建设的 WY 系统不仅服务于人民银行国库部门，同时还将与财政部门、征收机关（国税、地税、海关）和商业银行等横向联接，是未来预算收入和支出的关键性联网交换系统，系统建成以后意义重大，影响面广。特别是系统要能够支撑省级集中部署，未来能支撑全国集中部署，尤其是要满足全国集中交换的实时性要求，这给系统的设计、开发提出了很高的要求。我们经过认真分析和研究，在分析系统总体逻辑架构和数据中心部署模式的基础上，确定了基于 J2EE 架构（采用消息中间件进行连接）的系统解决方案。

5.1.1. 基于 J2EE 技术路线的方案设计特点

本方案的设计特点如下：

1、松耦合 (Loosely-Coupled) 集成方式

WY 系统的一个典型特点就是实现与联网机构的有机集成。系统设计将应用程序定义为不同组件（或称为服务），通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的，它独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以松耦合的方式集成，并采用一种统一和通用的方法进行交互。

基于上述思想，我们建议将横跨多个部门的一个业务流程 (Process) 分解为多个相对独立的活动 (Activity)，再通过一个集中控制的服务进行业务完整性控制。一旦某个

环节出现异常或超时，则进行相应的冲正处理。这也要求与 WY 相联的系统提供对冲正处理的支持。

2、适应性 (Flexibility)

由于需要集成的系统相当多并且复杂，系统设计必须能够方便地适应当前相关系统的不同情况以及未来变化，包括一定范围内支撑技术、产品版本以及业务需求等方面的变化，同时也能通过描述的方式适应集成环境的改变。本系统应尽可能减少对现有系统的改变。

遵循关注分离 (Seperation of Concerns) 的原则，WY 通过将显示服务、交易和集成服务、企业服务总线、数据存储服务和数据仓库/分析服务等相分离。同时服务之间通过标准的接口进行集成。如果某一个服务需要修改时，其他服务可以保持不变。同时，利用企业服务总线，可以将与本系统集成的其他系统的改变 (如系统 IP、报文格式等) 进行屏蔽，使得系统的其他部分保持不变。

3、成熟性

使用的产品都经过了市场考验，并且在全球范围内有广泛的用户。尽量避免采用一些小的厂商开发的、或者自己开发的中间件产品。

4、先进性

设计方案中采用市场领先并成熟的技术，使项目居于国内同业领先的地位。

4.2 系统总体划分

5.1.2. 总体逻辑架构

依据“WY 系统规划”，当前建设的国库信息处理系统（WY），处于规划中的第一阶段：第一步骤，即建设国库信息处理系统，现有系统保持不变；第二步骤，在 TBS 上增加接口，实现 WY 通过小额支付系统与商业银行的连接。第一阶段其总体逻辑架构如下图所示：

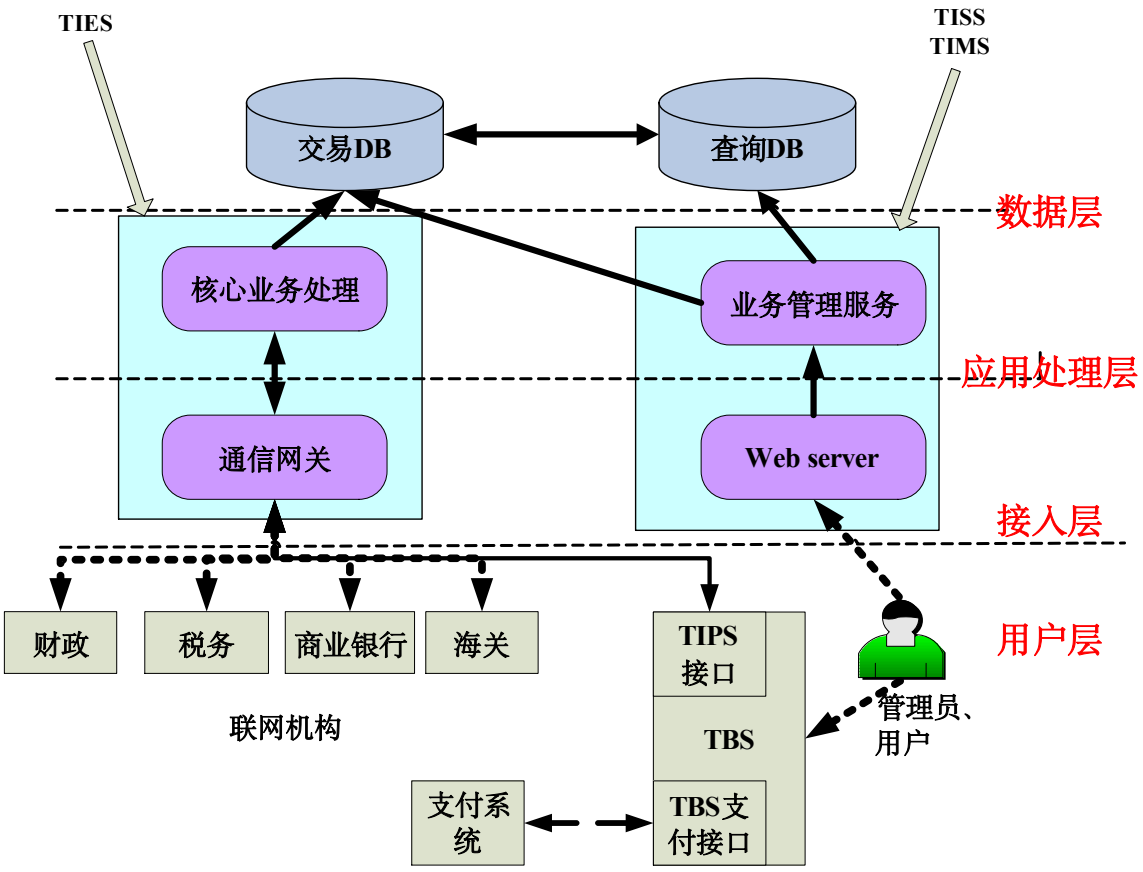


图 5-1 WY 系统总体逻辑架构图

如图 5-1，TIES、TISS、TIMS 三个系统均为多层架构。

其中 TIES 包括通信网关、核心业务处理、交易 DB 三部分，实现联网机构（财政、税务、商业银行、海关、TBS）之间的联网信息交换。

TISS 包括 Web server、业务管理服务、交易 DB、查询 DB 四部分，实现对联网交换后信息的下载（在 TBS 没有集中前，还需要将税票下载到各地 TBS 报解、分成、入库记账），TBS 核算后信息的上传集中，以及信息的补录、清分等。

TIMS 包括 Web server、业务管理服务、交易 DB、查询 DB 四部分，用以实现对 WY 系统参数维护、运行监控、异常处理等。

各个部分的功能如下：

1、交易 DB 和查询 DB

交易 DB 负责交易数据的存储。存放一个月内交易信息，包括：税票交易信息，退库交易，更正交易等。

查询 DB 负责历史数据的存储。存放 2 年的信息，包括：税票交易信息，退库交易，更正交易，以及辖内各级 TBS 入库税票、退库、更正信息和核算报表信息。

交易 DB 和查询 DB 的功能和关系如下图所示：

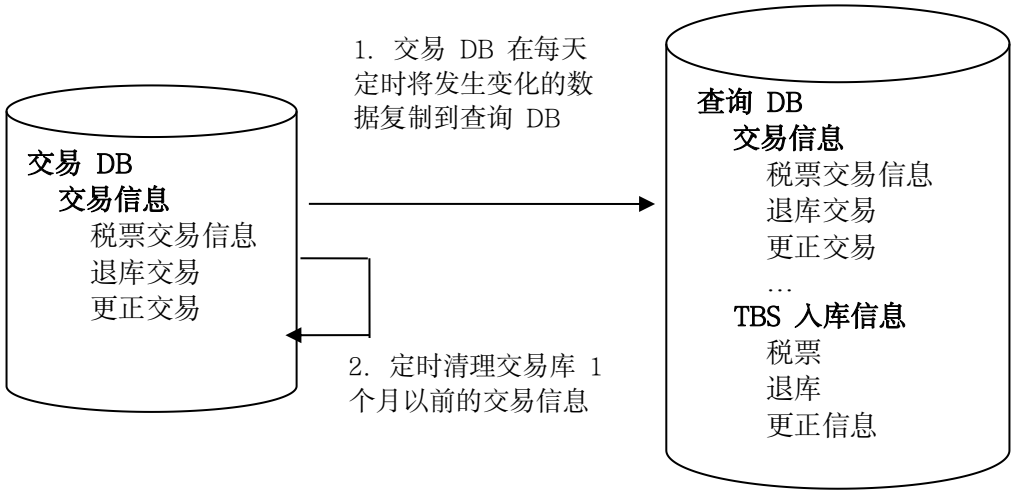


图 5-2 交易 DB 和查询 DB 功能和关系

2、核心业务处理层

负责核心的业务处理，对各方传输来的报文进行处理，对数据库进行操作，并生成响应报文。

3、业务管理服务层

对数据库查询、分析类的请求进行响应，并将结果返回给表示层。同时提供对核心业务处理层的管理、修改配置等功能。

3、通信网关

该层是本系统的重要部分，负责与各联网机构进行通信，交换报文，查找路由等。

4、表示层

负责收集一般用户（如管理员）的请求，提交给业务管理服务层，并将业务管理服务层的结果以一定的格式显示给用户。

第二阶段,TCBS 也将采用基于 J2EE 的多层架构，TPPS 也将采用多层架构（是否基于 J2EE,将遵循支付系统接口方案），WY、TCBS、TPPS 整合后，WY 的总体逻辑架构如下图所示。整合后 WY 的总体逻辑架构没有发生变化。

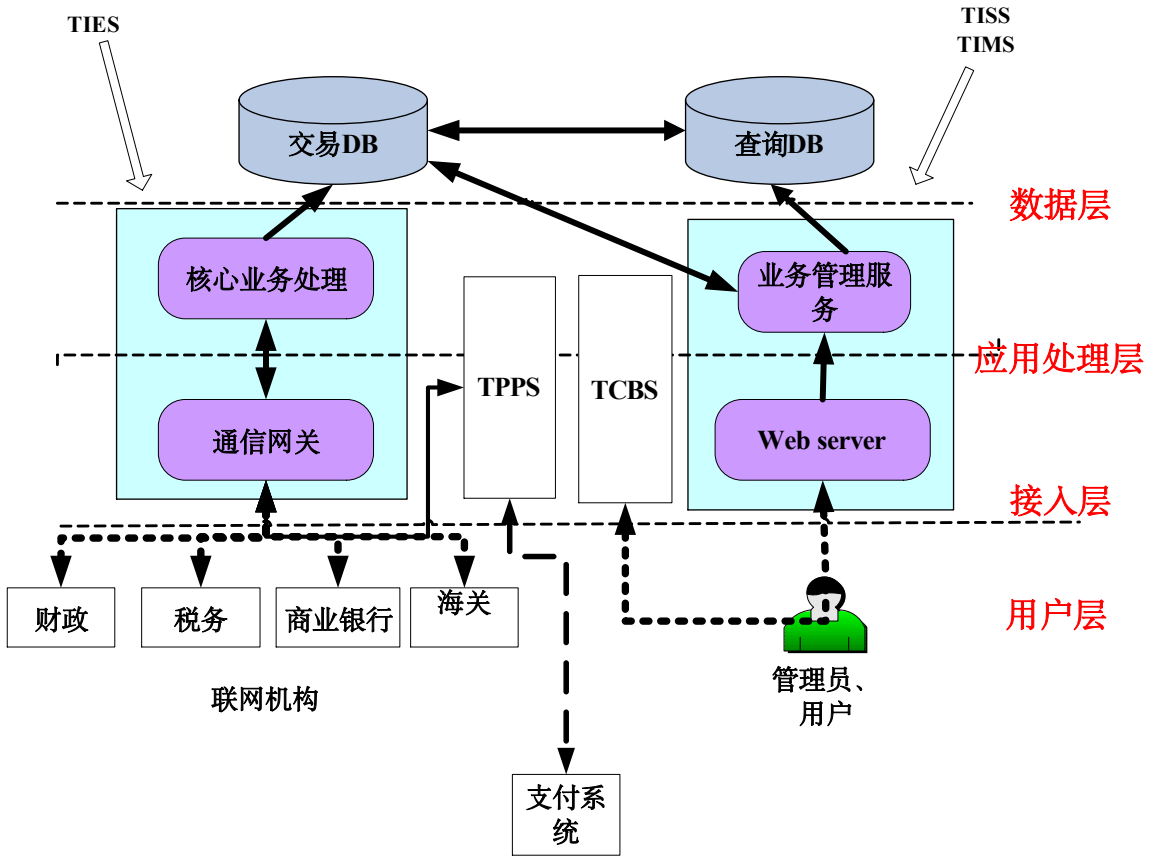


图 5-3 整合后的 WY 系统总体逻辑架构图

5.1.3. 系统逻辑架构

依据 WY 的业务功能需求，WY 的逻辑架构设计如下图所示。

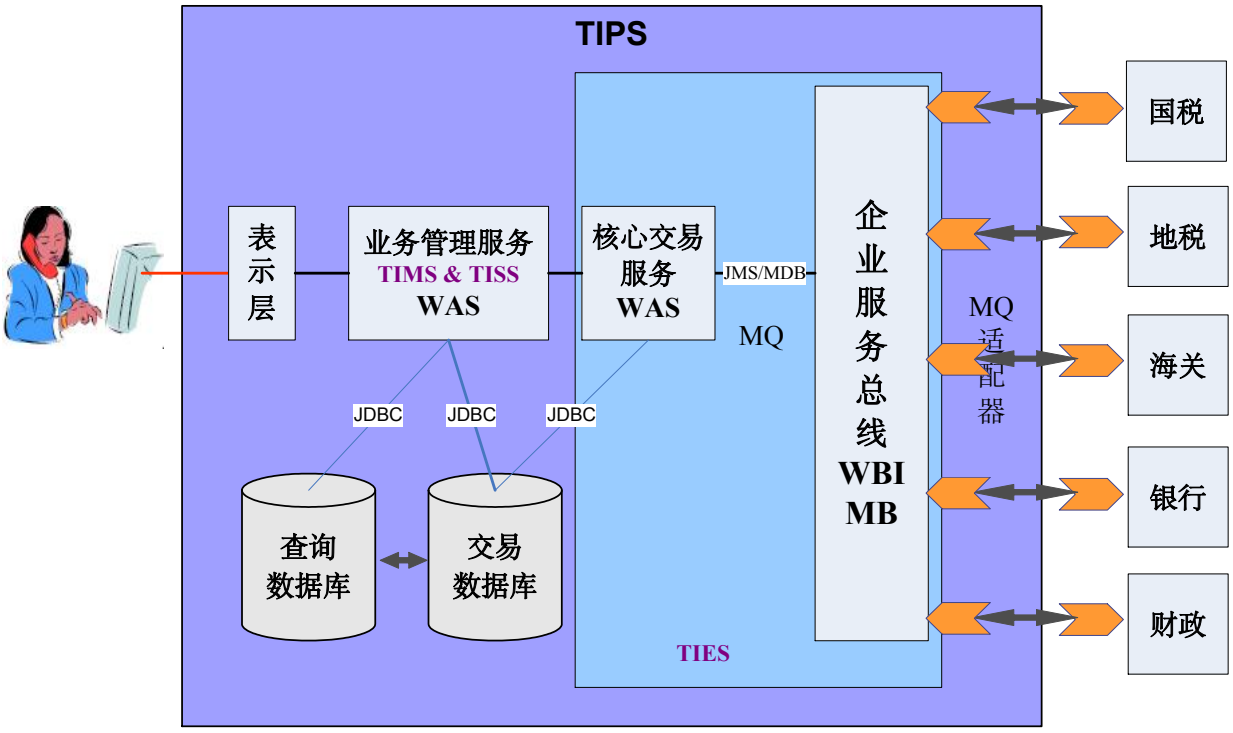


图 5-4 WY 系统架构概要图(Architecture Overview Diagram)

其中，WY 由表示层、管理查询服务、核心交易服务、企业服务总线以及与相关系统集成的适配器 (Adapter) 组成，各个部分功能如下。

1) 表示层支持用户通过 Browser 或定制的 Java 客户端访问系统，表示层将基于 J2EE 的技术架构。

2) 管理查询服务 (TIMS & TISS) 提供系统的配置管理和从业务角度的监控能力，同时提供数据分析、查询的处理能力。

3) 核心交易服务提供国库信息处理 (如实时扣税) 工作中各个环节的流程和业务完整性控制，并将相关信息保存到数据库中。

4) 数据库提供数据的存储，主要用来记录交易业务的日志和跟踪其状态信息。

5) 企业服务总线 (ESB) 主要提供相关系统的接入，消息 (Message) 的转换 (Transformation) 和路由 (Routing) 功能。通过 ESB 能够大大增强系统的适应性 (Flexibility)。

6) MQ 适配器提供联网机构和联网中心间稳定、可靠、安全的数据传输服务，能够保证数据的可靠传输——只传一次，保证传到。

本系统架构中各部分均采用 J2EE 三层 (多层) 架构进行构建，以确保系统的开

放性和可扩展性。

5.1.4. 系统逻辑运行模型

在本小节中，我们描述系统的拓扑结构、逻辑处理节点及其网络连接，以及系统与用户和相关系统的关系。

利用交换机和防火墙 (Firewall) 将系统划分为不同的安全域，包括接入环境 (中国人民银行内联网)、停火区 (DMZ)、生产域和集成域 (Extranet)。

利用工作负载均衡节点来完成工作负载在多个 Web 服务器间的均衡，以提升系统的吞吐率。

在生产域中，将应用服务器分为显示应用服务器和交易应用服务器两类节点。通过企业服务总线与外部相关系统集成。

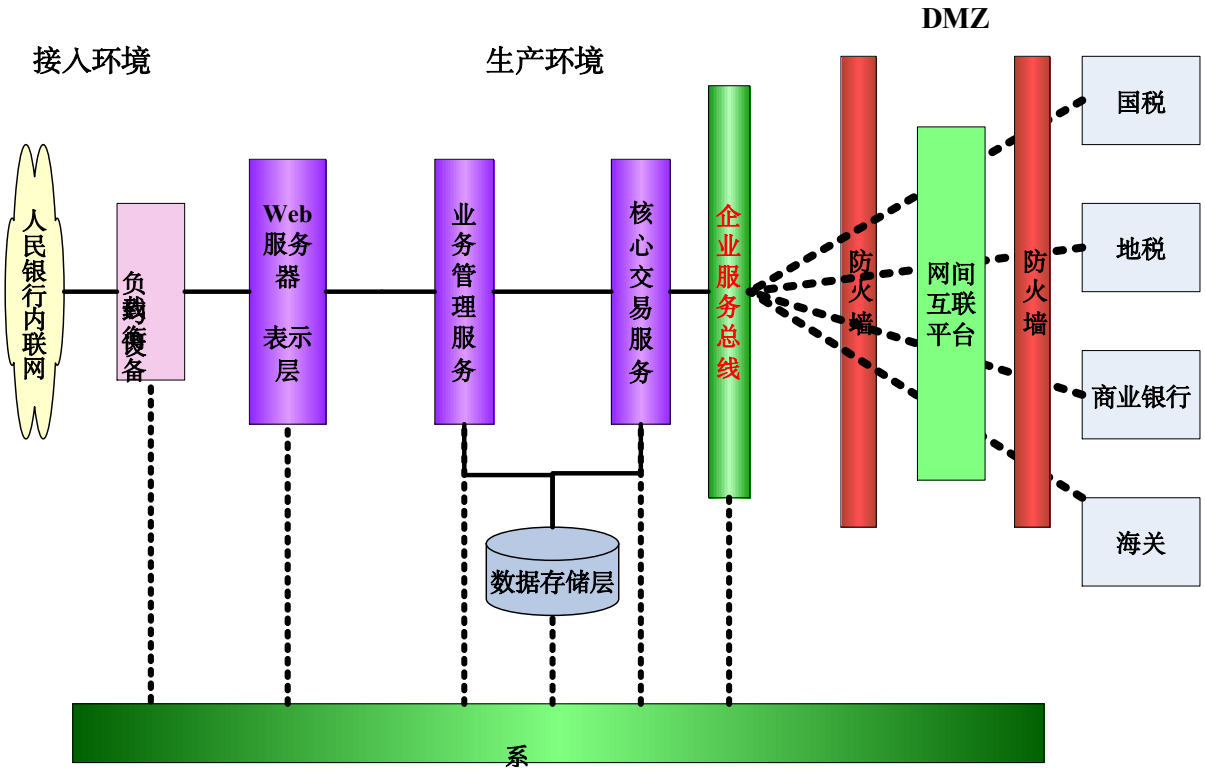
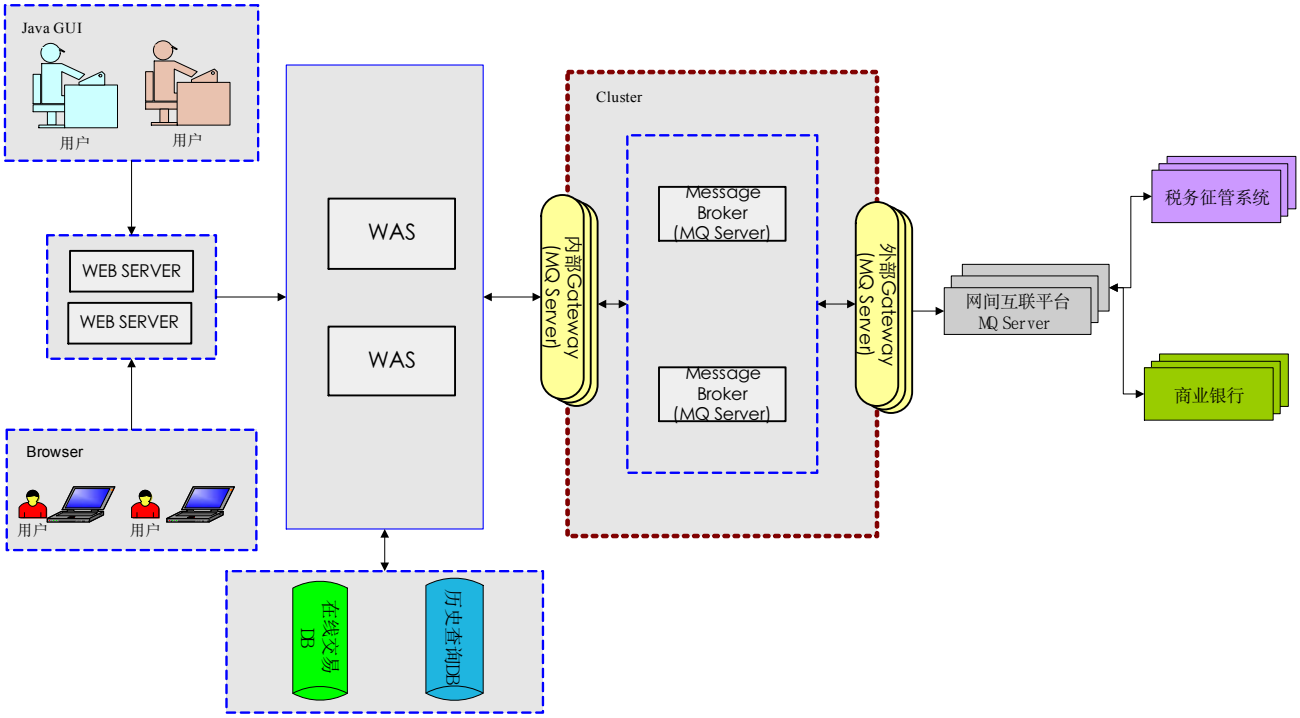


图 5-5 WY 系统逻辑运行模型 (Logical Operational Model)

4.3 系统总体软件架构

WY 系统涉及国库、税务、商业银行、财政、海关等各家机构，处理复杂，系统的软件架构基本如下图：



WY软件系统部署架构说明

1. WY包含的逻辑部件有：

外部Gateway, 内部Gateway, ESB, WAS, DB, WEB SERVER

2. 每个逻辑部件的作用，以及和别的部件的关系

. 外部Gateway（MQ Server）：负责接入外部系统。各个外部系统（例如税务机关、商业银行等）通过网间互联平台和外部Gateway连接。

. 内部Gateway（MQ Server）：WAS系统通过内部Gateway和ESB进行消息的交互。

. ESB：ESB通过消息流对消息进行报文头的预处理，以及消息路由的操作。它通过内外Gateway分别从外系统和WAS进行消息的交互。

. WAS：WAS进行报文的业务处理，是WY的核心业务处理模块，ESB收到的消息均要转发到WAS进行逻辑处理，同时WAS也为WEB用户提供服务。

. DB：包含系统的交易数据和历史数据库。

. WEB SERVER：处理用户的Http请求，将其转发给WAS服务器，还包含一些静态页面和客户端下载包

3. 消息流转的机制

以单笔实时扣税交易为例，消息的流转过程如下所示：

税务征管系统提交请求报文，发送到网间互联平台；

网间互联平台将请求报文转发到WY的外部Gateway；

外部Gateway通过MQ的Cluster机制将请求报文转发到ESB系统；

ESB系统收到请求报文，进行预处理，然后通过内部Gateway转发到WAS系统；

WAS系统进行业务处理后，将请求报文通过内部Gateway转发给ESB，并通知ESB将请求报文转给某商业银行；

转发的请求报文经过外部Gateway和网间互联平台，到达商业银行；

商业银行进行相应的业务处理后，发送回执信息；

回执信息经过网间互联平台和外部Gateway，到达ESB系统；

ESB系统进行回执报文的预处理，然后通过内部Gateway转发给WAS系统；

WAS系统进行业务处理后，将回执报文通过内部Gateway转发给ESB，并通知ESB将回执报文发送给税务征管系统；

回执报文经过外部Gateway和网间互联平台，到达税务征管系统，扣税交易结束。

4.4 ESB/MQ 系统逻辑结构

方案中我们采用 IBM WBI Message Broker 作为系统的信息总线。它在本系统中起到以下方面的作用：

1、所有相关单位的接入服务，支持多种接入方式，并且进行各种接入协议之间的转换；

2、数据路由服务，根据数据体标识，把数据路由到正确的目的地，当接入单位增、删、改时，灵活地维护系统的路由表。

与自行开发的或其他类似产品比较，它的优势在于：

1、具有优异的处理性能，该产品在业界同类产品中的性能是无可比拟的，它内部用于数据处理的消息流是以多线程方式工作的，同一个消息流还可以分配到不同的执行组，从而提高整个系统的运行效率；

2、具有交易完整性保证，该产品支持不同层次的交易完整性要求，例如：可以设定整个消息流为一个完整的交易，当某一环节发生错误时，整个消息流回滚，保证数据一致性，这一点在该系统中是非常重要的；

3、具有高可靠性，该产品支持 HA，在本方案中，通过四层交换机（硬件）或

IBM 的 MQ Cluster，可以实现多个 Message Broker 同时工作；

4、具有方案的可扩展性，该产品功能完善，随着今后系统新需求的出现，可以不断发挥其强大功能，如消息格式转换的功能。

ESB 基于消息中间件 MQ，通过网间互联平台，与外联机构（征收机关或商业银行）进行信息交换；在 WY 系统内部，消息中间件 MQ 作为 ESB 和 WAS Server 之间的桥梁，将 ESB 和 WAS Server 有机集成起来。ESB 系统总体逻辑图如下所示：

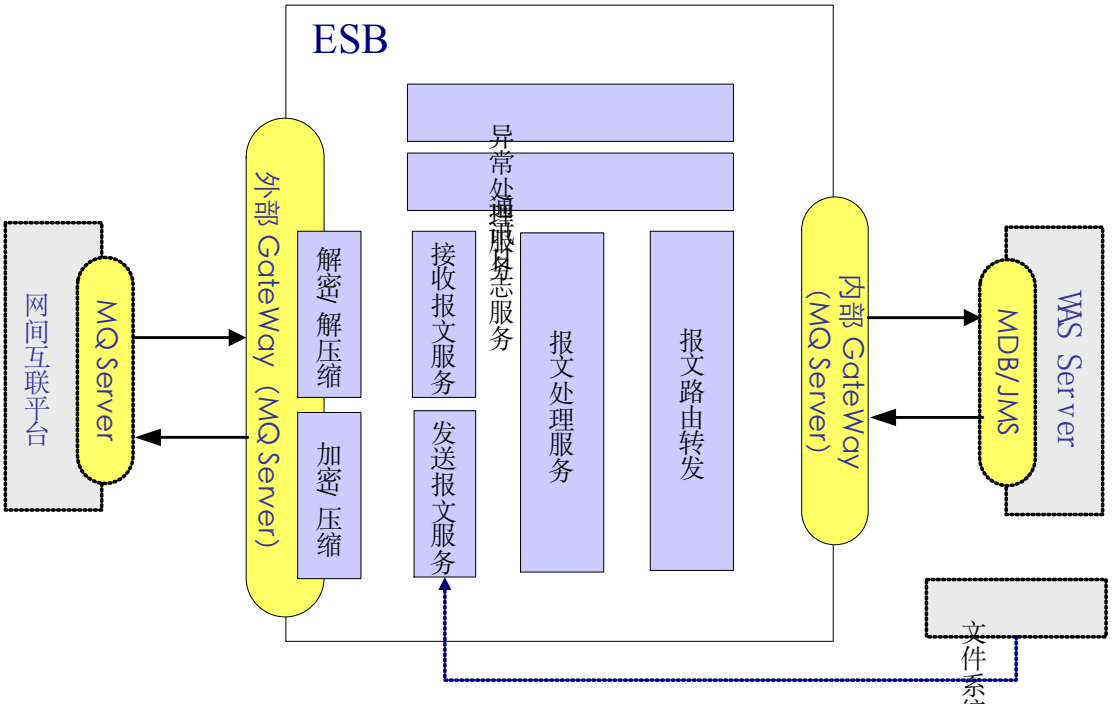


图 5-6 ESB 系统总体逻辑图

ESB 作为 WY 的交易转接系统，由接收报文服务、发送报文服务、报文处理服务、报文路由转发服务、通讯日志服务、异常处理服务共计六部分组成。各部分的主要功能如下：

接收报文服务：本部件主要负责接收外联机构（征收机关或商业银行）发送给 WY 系统的各类交易报文，并实时交由报文处理服务进行处理；

发送报文服务：本部件主要负责发送报文给外联机构（征收机关或商业银行）；

报文处理服务：本部件主要负责报文的初步解析和必要的格式转换；在接收外联机构发起的报文时，本部件负责解析报文头信息，并转换成 WAS Server 容易处理的报文格式；在发送报文到外联机构时，本部件负责转发报文，对于文件类报文，还负责报文由文件到报文格式的转换；报文处理完毕后，统一交由报文路由转发服务进行

处理；

报文路由转发服务：将收妥的报文转发给 WY 系统的 WAS Server；将需要发送的报文路由到正确的接收者；

通讯日志服务：负责记录接收或发送的报文日志；

异常处理服务：在上述部件的任何一点出现异常时，本部件将自动接管报文的后续处理，在系统中主要起到跟踪作用。

另外，ESB 基于安全和通讯效率的考虑，通过 MQ Server 实现了加密和压缩功能。

下面是 ESB 系统的基本逻辑流程：

a) ESB 系统接收报文逻辑流程

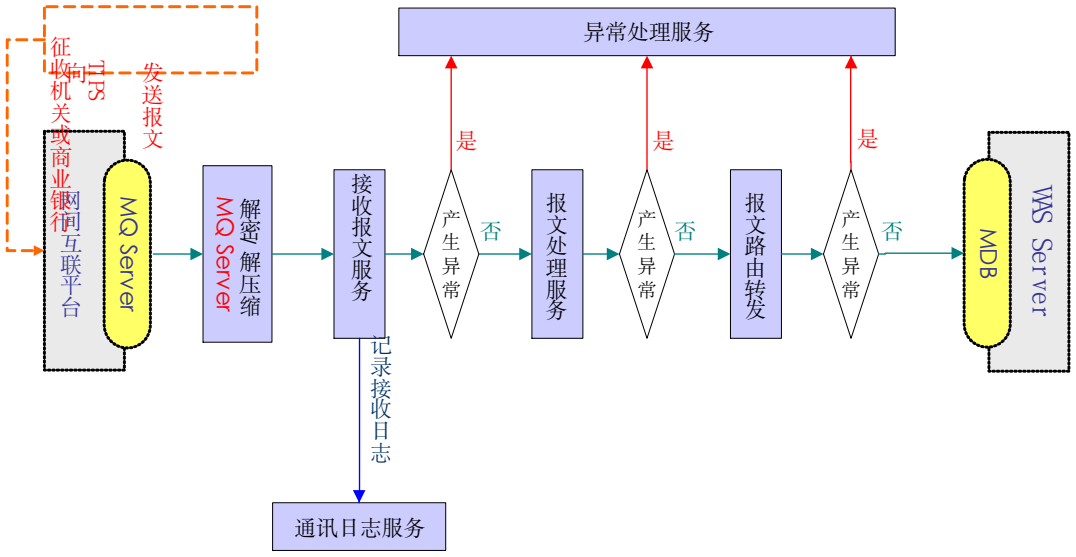


图 5-7 接收报文处理逻辑流程图

对于 ESB 接收报文的处理逻辑，当征收机关或商业银行发送报文给 WY 系统时，ESB 通过 MQ Server 进行解密和解压缩，接收报文，对报文进行格式转换预处理，以便于 WAS Server 处理，并通过报文路由转发服务，转发个 WAS Server。

在报文通过接收报文服务时，记录接收日志。在上述处理任意环节出现异常，报文都将交由异常处理服务进行后续处理。

b) ESB 系统发送报文逻辑流程

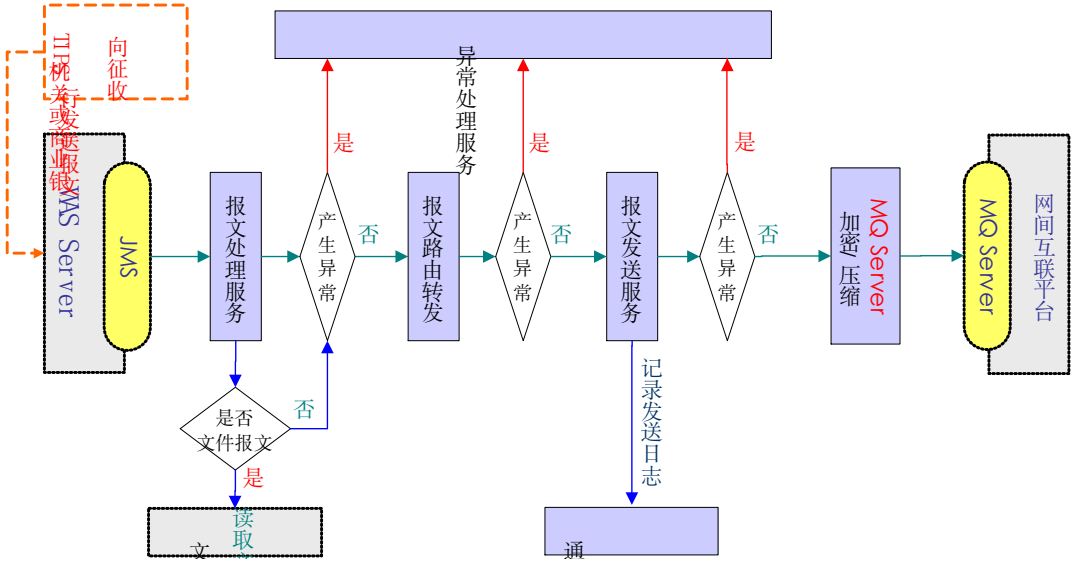


图 5-7 发送报文处理逻辑流程图

对于 ESB 发送报文的处理逻辑，当 WY 系统发送报文给征收机关或商业银行时，ESB 通过报文处理服务对报文进行解析，并对于文件类报文，从文件系统读取文件，转换成报文格式；与非文件类报文以统一的方式，交由报文路由转发服务进行路由，由报文发送服务负责发送给征收机关或商业银行，途经 MQ Server 时，进行加密和压缩。

在报文通过发送报文服务时，记录发送日志。在上述处理任意环节出现异常，报文都将交由异常处理服务进行后续处理。

4.5 WAS 系统逻辑结构

方案中我们采用 IBM WAS 作为系统的应用服务器，两台 (或多台) 应用服务器通过 WAS 配置为 Cluster 模式，实现负载均衡。当需要扩充系统的处理能力时，应用服务器既可以添加更多的主机节点 (水平扩展)，也可以增强主机节点的配置 (垂直扩展) 实现。WAS 系统逻辑结构如下所示：

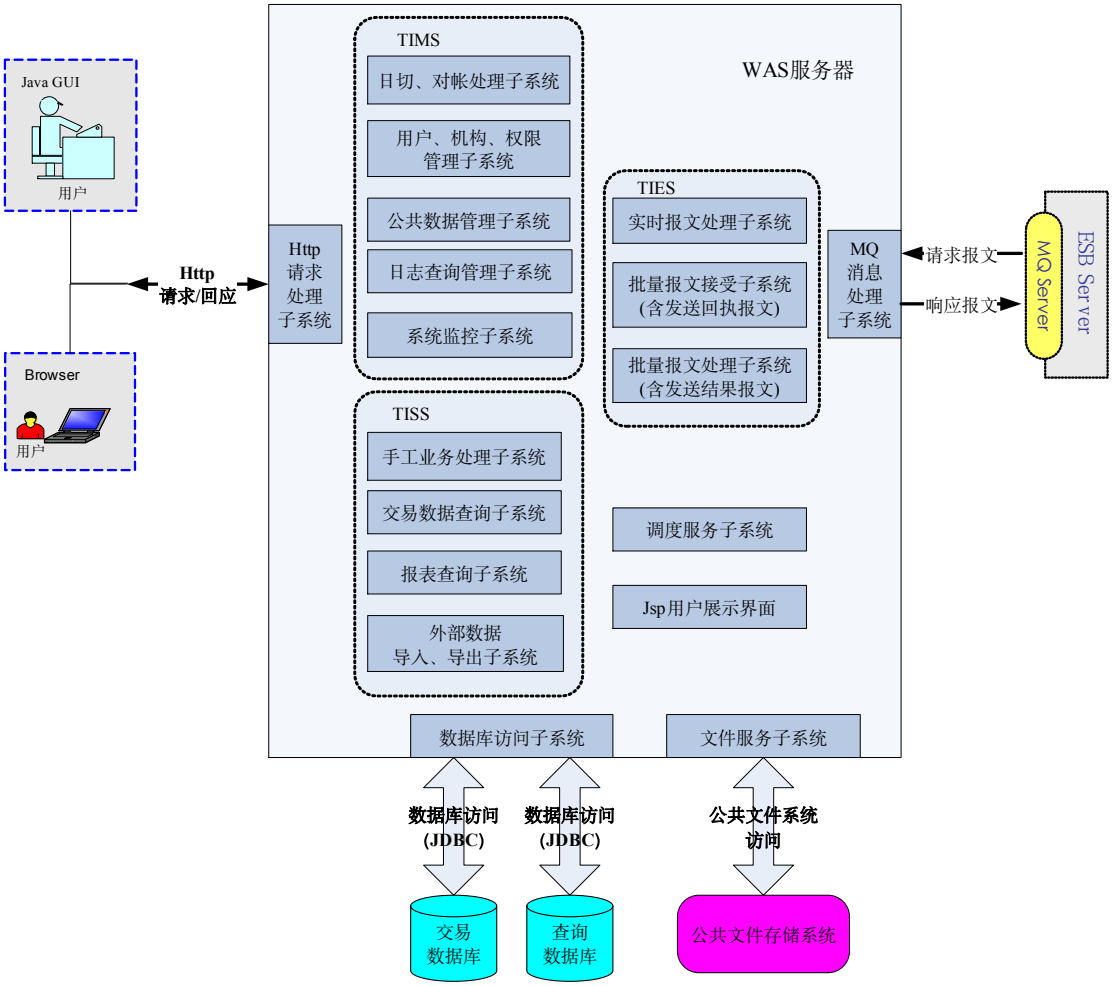


图 5-8 WAS 系统逻辑结构

各个子系统说明如下：

1、 公共部分

a) Http 请求处理子系统

负责处理客户端（含 Browser 和 Java Gui）传来的 Http/Https 请求，并调用相应的 TISS、TIMS 中的服务，并将请求处理结果返回给客户端。（如果客户端是 Browser，需要将处理结果用 JSP 进行处理，返回给用户可视的 HTML 页面）

b) MQ 消息处理子系统

负责监听 MQ 队列，对传入的消息进行处理（格式验证、验签名），并根据报文的类型调用 TIES 中的服务。同时负责将服务处理完的结果打包、签名、发送到 MQ 队列中。

c) 数据库访问子系统

负责系统中与数据库的交互，包含 ORmap 工具、JDBC 调用接口、常用的数据库查询及缓存等等。几乎所有的业务子系统都回调用该服务。

d) 文件服务子系统

负责与外部公共文件系统的交互，同时提供文件下载、上传服务。

e) 调度服务子系统

负责系统定时任务的调度，调用日切、对帐、核对、批量报文处理等服务进行处理。

f) Jsp 用户界面

负责将 TISS、TIMS 处理结果转化为用户 Browser 可以处理的 HTML 格式。

2、 TIMS

a) 日切、对帐处理子系统

包含日切、对帐、核对、过期清除等服务。被调度服务激活。

b) 用户、机构、权限管理子系统

包含用户、机构、权限、密码等信息的管理服务。

c) 公共数据管理子系统

包含系统字典表、公共信息数据的管理服务.

d) 日志查询管理子系统

包含系统日志的查询服务。

e) 系统监控子系统

包含系统运行情况监控管理服务。

3、 TIES

a) 实时报文处理子系统

包含实时报文交易处理服务

b) 批量报文接受子系统(含发送回执报文)

包含批量报文接受，存储到公共文件系统，并发送回执报文的服务。需要调用文件服务子系统。

c) 批量报文处理子系统(含发送结果报文)

包含批量报文的处理、并发送处理结果报文得服务。被调度服务激活，同时需要调用

4、 TISS

a) 手工业务处理子系统

包含 WY 手工业务的处理服务。

b) 交易数据查询子系统

包含交易数据、交易状态的查询服务。

c) 报表查询子系统

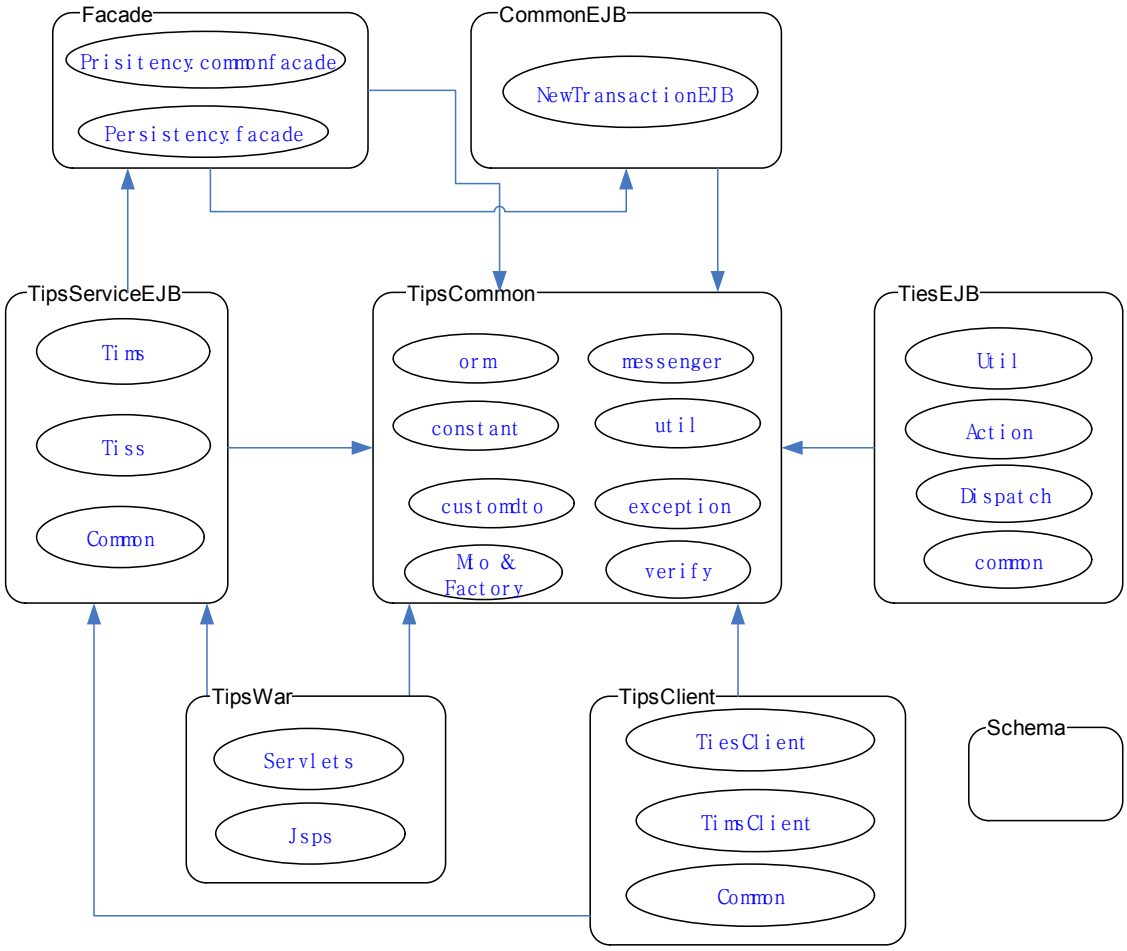
包含报表查询、打印服务。

d) 外部数据导入、导出子系统

包含外部数据（TBS）的导入、导出服务。

4.6 WAS 应用组件关系与包结构划分

WY 系统需要提供各种外围机构的介入，同时提供个人用户的访问接口，其结构非常复杂，应用软件包结构如下图所示：



4.6.1 WYCommon

该项目包含系统所有底层组件。具体包路径和功能如下：

com.cfcc.WY.persistency.ormap.*：

包含数据库表映射对象（OR-Map），提供对数据库的访问接口。

com.cfcc.WY.persistency.constant.*：

包含系统中定义的常量。

com.cfcc.WY.persistency.customdto.*：

com.cfcc.WY.persistency.customtype.*：

包含系统中定义的特殊的数据类型，用于数据库查询和前台、后台之间交换数据。

com.cfcc.WY.mto.*：

包含报文解析处理对象，可以将报文对象（MTO:Message Transfer Object）转换为 XML，或将 XML 转换为 Mto，同时提供 XML 报文的签名和验签名功能。

com.cfcc.WY.common.*：

包含 WY 中一些通用的应用对象，如配置参数、异常类型、消息类型、校验、常用工具等。

4.6.2 CommonEJB

包含 WY 系统中通用的 EJB，目前主要包括一个启动新事务的 EJB，包路径为 com.cfcc.WY.commonejb.*。提供在一个新的事务中修改数据库和发送消息的功能。

4.6.3 Façade

该项目包含系统对数据库和消息队列的访问接口。包含通用访问接口（CommonFacade）和专用访问接口（Facade）两部分。包路径如下：

com.cfcc.WY.persistency.facade.commonfacade.*：

包含 WY 通用的对数据库和消息队列的访问接口，提供单表、多表数据的增、删、改、查等功能。同时提供对消息队列的读、写功能。

com.cfcc.WY.persistency.facade.facade.*：

包含专用的访问数据库的接口，与一定的业务相关，提供对特定表和记录的操作功能。如根据用户 Code 查找其权限列表。

4.6.4 TiesEJB

该项目包含 Ties 的核心处理模块，主要包括消息监听模块（MDB）、消息分发模块、消息处理模块等，其包路径和功能分别如下：

com.cfcc.WY.ties.common.mdb.*：

包含 MDB 消息监听模块，用以监听各个消息队列，调用消息分发模块进行消息处理。

com.cfcc.WY.ties.common.dispatcher.*：

包含消息分发模块，解析 XML 消息，转换为 Mto，根据消息的类型调用不同的消息处理模块（Action）进行处理，并根据不同的处理结果放到相应的队列中。

com.cfcc.WY.ties.action.*：

针对各种消息的处理模块，此处有很多 Action，分别处理不同的报文，Action 是可配置的，根据系统功能的增加，可以增加新的 Action，而不用修改其它基本结构。

com.cfcc.WY.ties.util.*：

包含 Ties 使用的一些工具方法。

4.6.5 WYServiceEJB

com.cfcc.WY.ejb.*：

包含 WY 客户端访问服务器使用的一些 EJB，包含一个建立服务调用的 Invoker EJB，建立系统定时任务和其它定时任务的 Timer EJB。

com.cfcc.WY.service.*：

包含 WY 客户端访问服务器的 Service，分别处理不同的客户端调用，以及用户身份认证、权限检查等功能。

com.cfcc.WY.advice.*：

包含 WY 客户端访问服务器的一些切面处理方法，包含一些日志记录、后续任务设置、消息发送等 Advice。

4.6.6 WYWar

包含 WY 使用的一些 Servlet、Jsp、和其它的 Jar 包，其中有提供远程客户端调用的 Servlet；初始化 CA 的 Servlet 等。

4.6.7 WYClient

包含 WY 客户端，包含如下内容：

com.cfcc.WY.client.common.*：

包含 WY 客户端应用程序的通用部分。

com.cfcc.WY.client.report.*：

包含 WY 客户端应用程序的报表部分。

com.cfcc.WY.client.tims.*：

包含 WY 客户端应用程序的 Tims 部分。

com.cfcc.WY.client.tiss.*：

包含 WY 客户端应用程序的 Tiss 部分。

4.6.8 Schema

交换报文（XML）的格式定义。

4.7 DB 系统逻辑结构

国库信息处理系统不仅需要联机处理来自省辖乃至全国范围内财政、税务、海关、商业银行等各种参与国库预算收支业务机构的大量交易数据，因此对系统的处理性能有很高的要求；同时由于它还需要兼顾全省乃至全国范围内的数据集中，向相关部门提供统计分析报表。基于这一特定需求，将 WY 的系统存储结构分为两个数据库，即联机交易数据库(WYODB)和历史查询数据库(WYQDB),具体的数据库标识如下表所示,其关系如图 5-9 所示。

标识符	数据库名称	版本号	用途说明	状态
WYODB	联机交易数据库	0.0.1	用于处理各种联机交易	设计中
WYQDB	查询数据库	0.0.1	用于处理各种查询统计	设计中

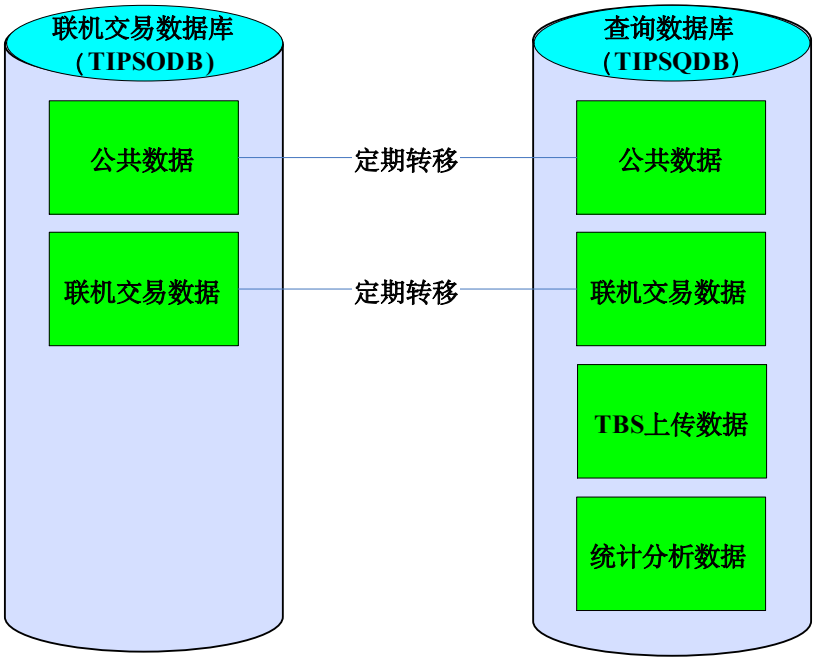


图 5-9 DB 系统逻辑结构

说明：

1、联机交易数据库用于存储最新的公共数据和联机交易数据；

2、历史查询数据库用于存储历史的公共数据、联机交易数据、TBS 上传的入库明细和各种财政预算收支报表数据以及将来用于统计分析用的统计分析数据，公共数据中需要保留更新前后的公共数据并记录各自的版本号。原则上，该数据库中的数据一旦存在不再允许修改。

系统采用定期转移的方式维护两个数据库中的数据。当计划时点到来时自动从联机交易数据库中转移部分历史数据到历史查询数据库中，并删除联机交易库中的该部分历史数据。同时为了改善数据库的处理性能，系统将自动实施一定的性能调优策略（包括重新建立大表索引，运行 reorgchk、reorg、runstats 等），自动进行数据库的优化处理。

系统对外提供联机交易查询和历史交易查询两种方式的查询，联机交易查询主要指以报文为载体的查询，仅仅提供单笔查询，通过查询联机交易数据库实现；历史交易查询主要指通过 Http 协议，基于 Web 方式的查询访问，支持批量查询，主要针对历史查询数据库。

国库信息处理系统数据库的设计思路、存储结构和安全处理措施详见《数据库设

计说明书》。

4.8 WEB 系统逻辑结构

Web 系统包括传统的 Web 服务和下载服务两部分，其 WEB 系统逻辑结构如下所示：

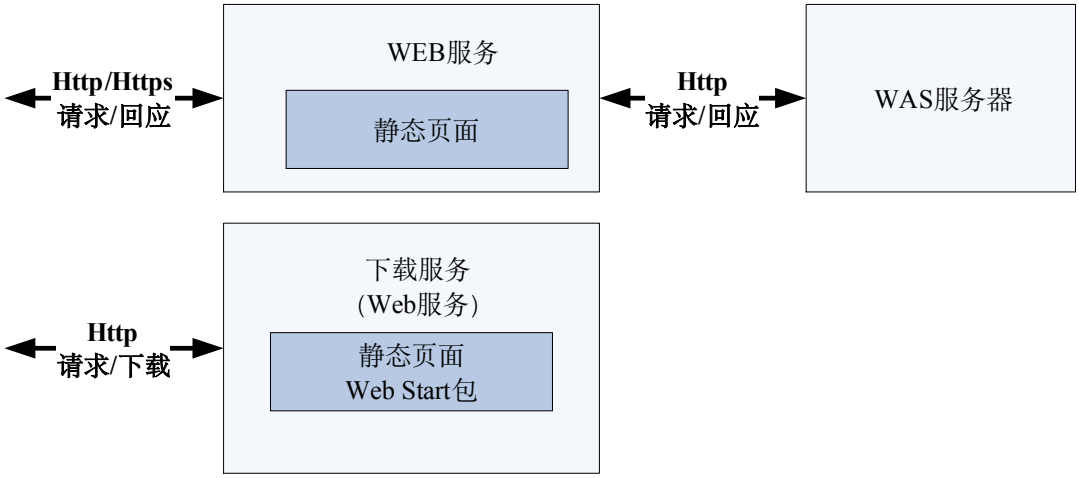


图 5-10 WEB 系统逻辑结构

WEB 系统功能分别如下：

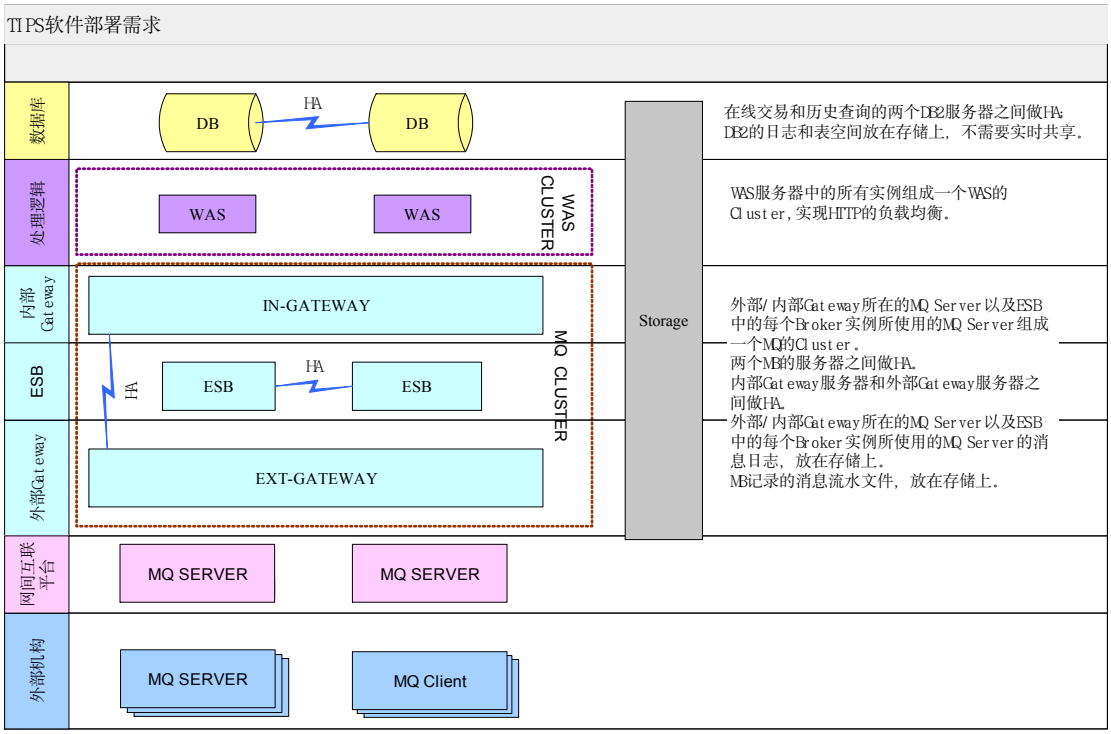
1、Web 服务

负责将客户端用户 Http/Https 请求转发到 WAS 服务器上，并通过其上的 Plug In 组件实现 WAS 服务器的负载均衡。同时，针对 browser 的用户，其上还会保存一部分静态的 HTML 页面。

2、下载服务

提供客户端应用程序的下载、升级服务。

4.9 WY 系统对物理部署的需求



WY软件部署需求

1. Cluster需求

为了满足WY的性能以及扩展性的要求，我们需要对WY进行Cluster的部署。

其中，外部/内部Gateway所在的MQ Server以及ESB中的每个Broker实例所使用的MQ Server一起组成一个MQ的Cluster，实现消息的负载均衡。

WAS服务器中的所有实例组成一个WAS的Cluster,实现HTTP的负载均衡。

2. HA需求

为了满足WY的高可用性的要求，避免系统中的单点故障，我们需要对WY进行HA的配置，共有三组：

. 在线交易的DB2服务器和历史查询的DB2服务器之间做HA，以保证数据库运行的可靠性。

. 两个MB的服务器之间做HA，当一台MB服务器出现故障时，可以保证另一台MB继续处理故障MB服务器上还未处理的持久消息。

. 内部Gateway服务器和外部Gateway服务器之间做HA，以避免系统中的单点故障。

3. 存储需求

使用存储，是为了实现WY的大报文处理逻辑，以及满足到系统的性能要求和系统HA的需求。共有以下几种情况：

. DB2的日志和表空间放在存储上，不需要实时共享。

. 外部/内部Gateway所在的MQ Server以及ESB中的每个Broker实例所使用的MQ Server的消息日志，需要放在存储上，不需要实时共享。

. MB记录的消息流水文件，需要放在存储上，不需要实时共享。

. 批量以及对帐等产生的大报文需要放在存储上，同时需要共享给ESB和WAS。（建议采用ＮＡＳ）

4. 时钟同步需求

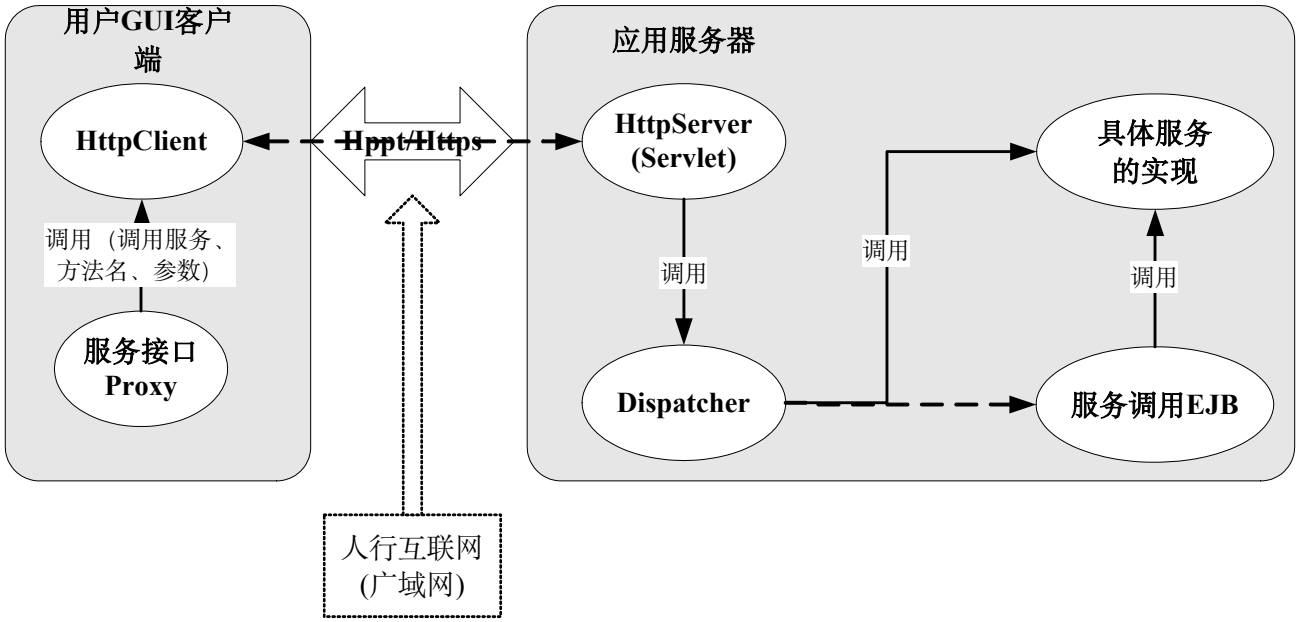
. WY系统中存在大量依赖于系统时钟的应用，为保证各个应用之间能够协调运行，需要保证系统各个服务器时钟的一致性，所以在物理部署上需要实现各个服务器的时钟同步，建议采用WYODB数据库服务器作为WY系统的时钟服务器，其它服务器都与此服务器保证时钟同步。

4.10 客户端接入方式

4.10.1 GUI 客户端

WY的客户端绝大部分都是进行业务处理的用户，对服务器的响应要求较高，对键盘操作、打印机控制等也有特殊的要求，传统的B/S结构应用系统在这些方面较难满足用户需求，所以我们采用Java GUI客户端的方式提供单个用户的接入。

Java GUI客户端访问服务器的结构如下图：



具体步骤如下：

1、 客户端调用远程服务接口的 Proxy（代理，JDK 中一种开发类包，用于调用远程的类，调用方式与使用本地类的方式一样，只是初始化时需采用特殊的语法）如下：

IExampleService service =

(IExampleService) ServiceFactory.getService(IExampleService.class);

然后就可以直接执行 service 上的代码。

2、 IExampleService 是 ExampleService 的接口：

3、 Proxy 调用 HttpClient Invoker，将需要调用的 Service 名、方法名、调用的参数传给类 HttpClient Invoker。

4、 HttpClient Invoker 将所用的调用参数形成一个二进制流，经过压缩、加密后加入 HttpRequest，请求 Web 服务器执行。

5、 Web 服务器监听服务端口，如有请求，激活一个 HttpServer（Servlet 的子类），从 HttpRequest 中读取二进制流，解密、解压后得到调用参数。

6、 如果该服务不需要事务，直接调用该服务的实现。

7、 如果该服务需要事务，通过一个 Session EJB 调用该服务的实现。

4.10.2 GUI 客户端程序安装、升级模式

Java GUI 客户端采用 Java WebStart 技术进行远程安装、升级。

首先，每个客户端安装一个支持软件：JRE 1.4.2。它包含了底层支持环境和一个远程安装程序：Java Web Start。大小大约为 15M，可以安装在 Windows、Unix、Linux 系列操作系统上。（现在很多品牌微机已经将 JRE 1.4.2 作为标准的预装软件）

然后用户启动浏览器，访问内联网上指定的网页，点击特定的链接后 Java Web Start 自动下载并运行 WY 客户端应用程序，并可以在客户端的桌面上建立客户端程序的快捷图标。

以后每次使用 WY 客户端应用程序时，用户可以双击桌面上客户端程序的快捷图标，客户端应用程序在启动之前会自动检查服务器上的下载包是否已经升级。如果已经升级，将自动下载最新的应用程序并运行；否则直接运行已经保存在本地的应用程序。

采用 Java 编写的 Java GUI 的应用程序经过编译、压缩、打包后一般都比较小，最大不过 1M 左右，进行网络远程维护和升级不会对内联网产生太大的负担。而支持软件 Java 2 SDK 1.4.2 只要安装一次，而且不会有升级，对于网络条件比较差的县支行可以采用下发光碟的形式进行安装。

4.10.3 Browser 客户端（目前尚未实现）

对于外联机构，如税务、财政等，一般对 WY 的要求是进行一些查询操作，采用下载的客户端不太方便，这里选用纯 B/S 结构的应用。用户通过通用的 Browser，采用 Http/Https 协议访问 WY 系统。

WY 系统采用 Structs 将应用逻辑、数据和控制分离，实现 MVC 结构。

4.11 外部机构接入方式

4.11.1 Server-Server

此种模式为对等模式。联网中心和联网机构均配置 MQ Server。联网中心通过自身的 MQ manager 为每个接入机构分别创建发送队列 Q1 和接收队列 Q2，发送队列

用于联网机构向联网中心发送数据，接收队列用于各联网机构从联网中心接收数据。联网机构通过自身的 MQ manager 创建自己的发送队列 Q3 和接收队列 Q4。当联网机构与联网中心建立连接以后，会创建从联网机构到联网中心之间的通道（channel）。联网机构通过调用 MQ API 将请求消息写入本地的发送队列 Q3 中，消息经通道传输至联网中心为该联网机构分配的发送队列 Q1 中，联网中心处理完成后，将返回结果写到对应机构的接收队列 Q2 中，消息经通道传输至联网机构。

这种方式主要用于需要提供服务的商业银行、农村信用（联）社和 TBS。

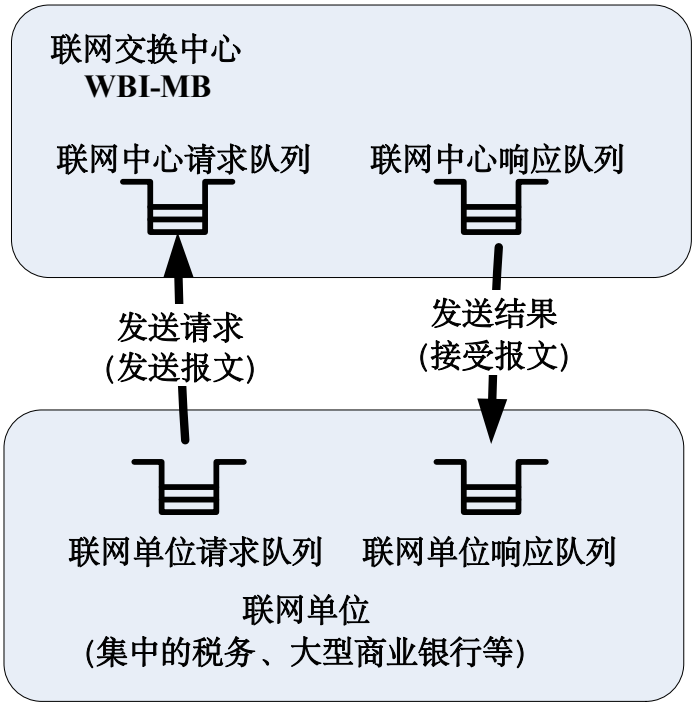


图 5-8 对等模式示意图

以上两种方式都能够保证各自的数据的安全送达，也各有优缺点。

采用方式 1，联网单位不用购买额外的 MQ Server，使用免费的 MQ Client 即可，成本较低。但如果交互的报文较频繁，此方式难以保证高效的报文传送，联网单位的轮询响应进程负担会比较重。所以这种方式适合于交易量较小的联网机构，如分散接入的地税、财政以及农信社等。

采用方式 2，联网单位需要购买额外的 MQ Server，成本较高。但这种方式效率非常高，针对与联网中心交易量很大的单位，如大型商业银行、集中接入的税务、海关部门等，每分钟的交易数量在几百笔以上。为保证交易的高效、稳定，可采用这种连接方式。对于这种联网单位，MQ 服务器软件的成本并不会是太大的问题。此外 IBM 提供 MQ Server 的简化版本 MQ Express，其 List Price 约为 4 万/CPU，在大量

采购下还会有更多的优惠（最后的价格将取决于商业谈判），较适合本系统的联网单位使用（包括 TBS）。

4.11.2 Client-Server

联网机构通过 MQ 与 WY 进行连接并交互数据，具体连接的方式分为两类：

1、中心节点模式（C-S 模式）

联网中心配置 MQ Server。通过 MQ manager 为每个接入机构分别创建发送队列 Q1 和接收队列 Q2。发送队列 Q1 用于联网机构向联网中心发送数据，接收队列 Q2 用于各联网机构从联网中心接收数据。当联网机构与联网中心建立连接以后，会创建从联网机构到联网中心之间的通道（channel）。联网机构通过调用 MQ Client API 将请求消息通过通道写入远程的联网中心分配的发送队列 Q1 中，联网中心处理完成后，将返回结果写到对应机构的接收队列 Q2 中，联网机构调用 MQ Client API 从对应的接收队列 Q2 中轮询处理结果。

这种方式主要主要适应于财政、国税、地税和海关，也可用于小的商业银行或农村信用（联）社。

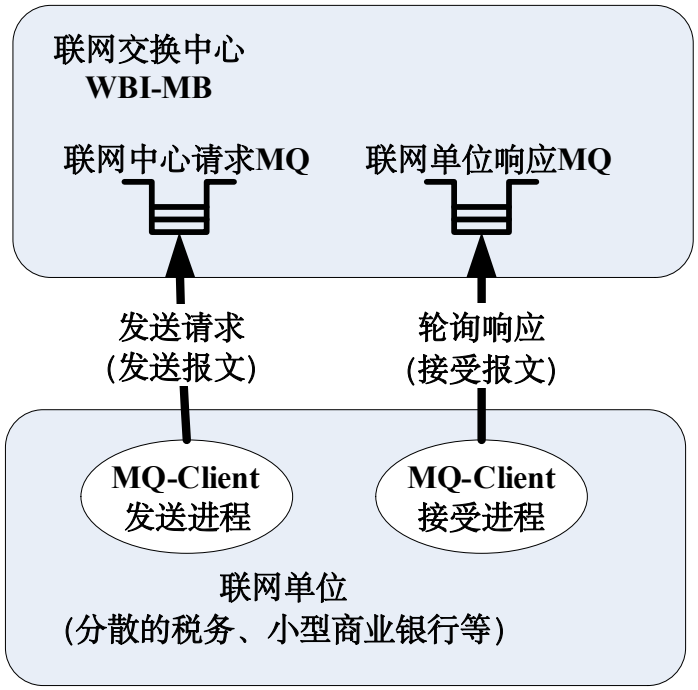


图 5-7 中心节点模式示意图

4.12 批量、大报文解决方式

为了保证网络传输的快速、及时、高效，系统限定联网单位发起的批量包封装的业务在 1 万笔以内（小于一万笔）。

WY 发起的与商业银行对账报文（包括日间和日切对账）明细笔数如果超过了一万笔，进行分包发送，并在对账包的汇总信息中列出总笔数以及当前包在总包里的序号，商业银行业务系统应负责进行包的组装。

4.13 定时任务解决方案

WY 为全国性的系统，系统设计了多种需进行后台处理的任务，为简化人员操作复杂程度，减轻维护人员工作量，保证系统自动运行，WY 提供定时任务自动调度机制，并可灵活调整任务执行时序。

1、定时任务分类

按执行日期分类，可以分为工作日依赖型和自然日依赖型两类任务。其中，工作日依赖型任务指任务的启动依赖工作日期而非系统日期（自然日），如开启日切窗口、关闭日切窗口只能在每个工作日执行一次，遇到节假日需要顺延；自然日依赖型任务指任务的启动依赖系统日期（自然日）而非工作日期，如数据转移任务、转发批量扣税业务等等，只要到达指定时间立即启动。

按执行时间分类，可以分为每日一次和多次执行两类任务。其中，每日一次执行任务指每日只执行一次，不允许多次执行的任务，如开启日切窗口、关闭日切窗口等等；每日多次执行任务指每日可以执行多次的任务，如转发批量扣税业务、银行端缴税核对任务等。

按任务关联性分类，可以分为关联任务和非关联任务两类。关联任务指此任务执行是以其它任务作为前置或后置条件的，如开启日切窗口、关闭日切窗口、与商业银行进行日切对账、与征收机关进行核对就是一组关联任务，前一任务不完成不得进行后一任务；非关联任务指此任务执行是独立的，不以其它任务作为前置或后置条件，如数据转移、转发批量扣税业务等。

定时任务调度器应具备以下功能：

1）任务可以定时启动执行；

2）可以控制节假日顺延执行，并可对节假日进行管理；

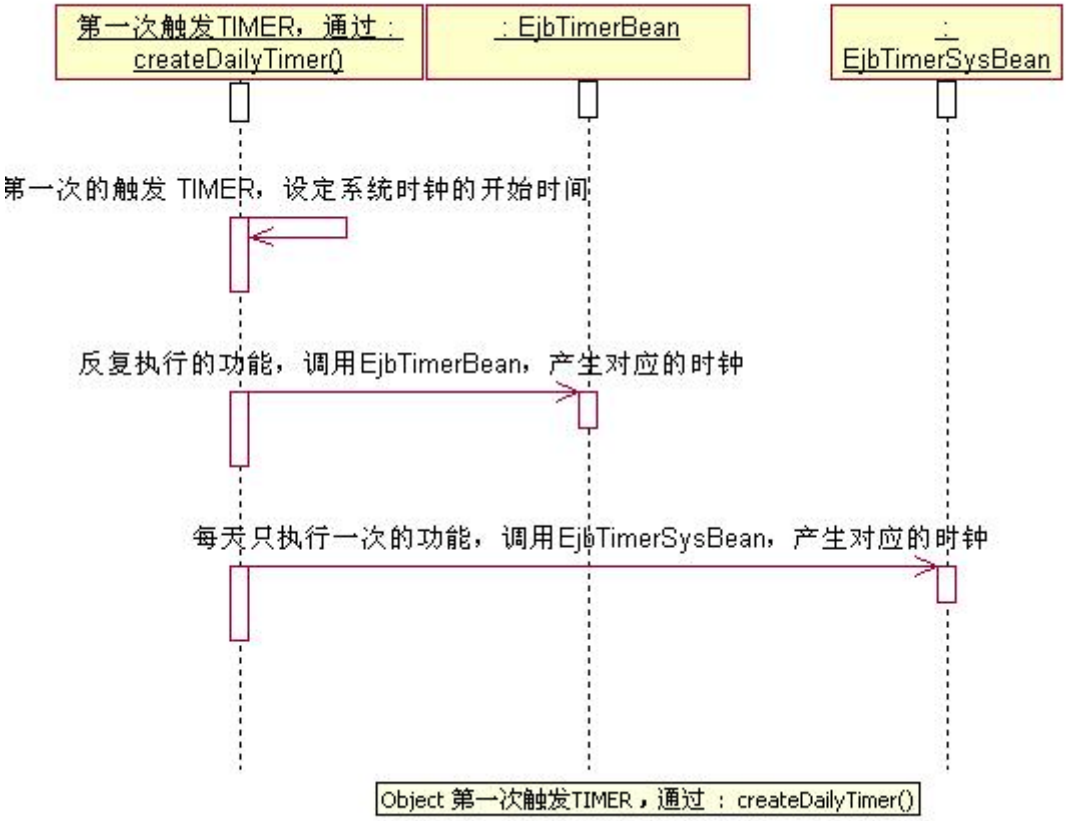
3) 可以设置关联任务的关联关系；

4) 一个任务可以多次执行，并且时间可调；

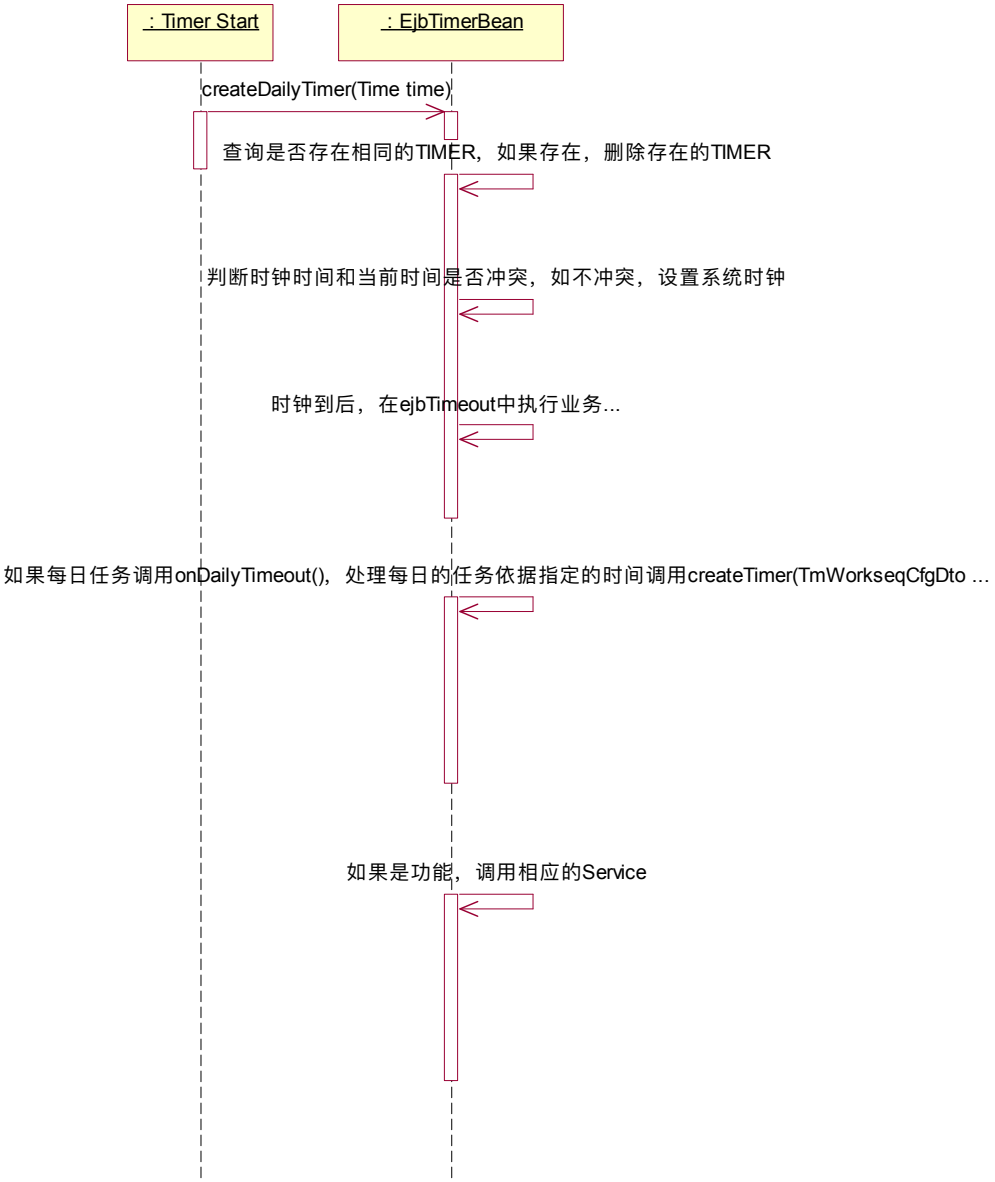
2、总体架构

为了更好的实现时钟控制，定时触发的功能，采用 J2EE1.4 所支持的 EJB2.1 的功能 TimerService 实现，达到时钟控制的目的。从使用效率的角度出发，按执行时间分类，把每日一次的和多次执行的任务，分为两个 TimerBean，这样做到一次性任务和多次性任务业务逻辑分别执行，不会相互影响，可以提高执行效率。实现逻辑全部在 ejbTimeout(time)中实现。对于 Timer 时钟的产生，通过去读数据库信息，去自动产生指定时间的 Timer。第一次触发一个 Timer 后，由一个 Timer 时钟去产生各功能对应时钟的 Timer，从而达到自动定时触发各功能的要求。

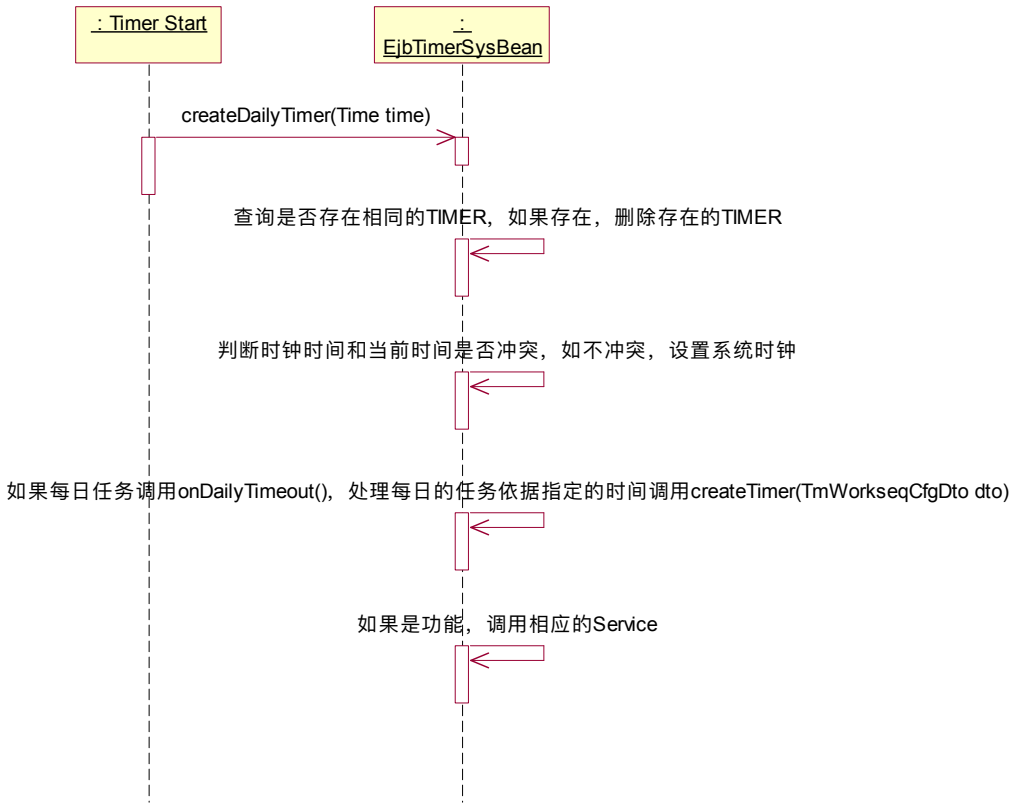
结构图如下：



EjbTimerBean：


: Timer Start
: EjbTimerBean
createDailyTimer(Time time)
查询是否存在相同的TIMER，如果存在，删除存在的TIMER
判断时钟时间和当前时间是否冲突，如不冲突，设置系统时钟
时钟到后，在ejbTimeout中执行业务...
如果每日任务调用onDailyTimeout()，处理每日的任务依据指定的时间调用createTimer(TmWorkseqCfgDto ...
如果是功能，调用相应的Service

EjbTimerSysBean：



4.14 系统日志设计方案

4.14.1 ESB 部分

1、 MessageBroker 底层平台日志管理

MessageBroker 的底层平台日志主要记载到操作系统的系统日志中，对于 Broker 及执行组的异常日志，记载到 MessageBroker 的错误日志目录下，如：如果在 Windows 系统环境下，错误日志目录为（D:\Program Files\IBM\WebSphere Business Integration Message Brokers\errors）；如果在 HP-UX 系统环境下，错误日志目录为（/var/mqsi/errors）；

MQ 的底层平台日志除了记载到操作系统的系统日志外，对于每个队列管理器，分别拥有一个 errors 目录，用于记载 MQ 的异常信息。如果在 Windows 系统环境

下，错误日志目录为（D:\Program Files\IBM\WebSphere MQ\Qmgrs\队列管理器名称\errors）；如果在 HP-UX 系统环境下，错误日志目录为（/var/mqm/Qmgrs/队列管理器名称/errors）；

2、 MessageBroker 应用运行日志及交易跟踪日志

本部分的日志管理从日志记载的详细程度上分为三个等级：

NONE： 不记录日志信息；

GENERAL：记录报文信息；

DETAIL： 记录报文及 MQ 的消息头信息。

日志的记录方式，为保证消息流的处理效率，日志采用异步方式记录。日志的记录采用 log4j 工具进行记载，日志文件的大小及路径通过 log4j 的配置文件进行配置实现。

报文流水日志采用异步记录方式，分时段打印到不同的通讯日志文件中；

MB 消息流的异常日志采用同步记录方式，为便于测试，目前也记载到通讯日志文件中，将来如果需要，可以通过配置，单独记载到 MB 的异常日志文件中。

4.14.2 WAS 部分

WAS 部分的日志分为三类：底层平台日志、应用运行日志、交易跟踪日志

1 **底层平台日志**：此类日志由 WAS 本身提供的机制进行记录，纪录的内容包括 JVM 日志、进程日志、IBM 服务日志，可以针对每个应用服务器实例进行设置。日志的存放位置、纪录信息的详细级别、历史文件的最大数、日志文件的大小、日志文件的存放时间等都可以通过 WAS 本身的配置文件进行设置。

2 **应用运行日志**：此类日志在 WAS 应用中通过 log4j 进行纪录，纪录的内容包括系统的跟踪调试信息、处理过程中的异常信息，可以针对应用的每个组件进行设置。日志的存放位置、纪录信息的详细级别、历史文件的最大数、日志文件的大小、日志文件的存放时间等都可以通过 log4j 的配置文件进行配置。

3 **交易跟踪日志**：交易跟踪日志又分为两类：报文日志和操作日志。

4 **报文日志**：报文日志纪录收发报文的概要信息，可以按接收报文进行设置是否纪录报文日志。日志内容包括报文关键字、接收或发送时间等。由于报文日志的数

量会比较多，出于对系统性能的考虑，报文日志采用异步的方式进行纪录，所有日志先发送到消息队列中，由日志处理组件异步的将数据保存到数据库中。日志处理组件的并发数量可以通过配置文件进行设置，这样不至于占用过多的系统资源，日志处理组件也可以和业务处理组件部署在不同的服务器上以减轻日志处理对正常业务处理的压力。

5 **操作日志**：纪录操作人员的手工操作，仅当可能对数据进行写操作（新增、修改、删除）的时才纪录，内容包括业务发生时间、操作员、操作内容、成功或失败、业务关键字等信息。该日志纪录直接纪录到数据库中。

5. 接口规范设计

5.1 概述

为了 WY 与各接入机构、WY 系统中各个不同模块间能够实时交换信息。系统专门制定了外部接口报文规范和内部接口报文规范。其中，外部接口报文规范是用来约定在 WY 与各接入机构实时报文交换的规则；内部接口报文规范是用来约定在 WY 中各个子系统间实时报文交换的规则。两种报文规范中都采用 XML 格式，并制定了统一的报文结构。

5.2 外部接口

WY 为外部系统的接口提供了两种接口途径，即报文接口方式和文件接口方式。其中：

报文接口方式，指 WY 与接入机构通过报文进行联机交互的连接方式。是 WY 主要工作模式。

文件接口方式，指 WY 与接入机构通过交换文件进行脱机交互的连接方式。是 WY 在网络故障时的辅助工作模式。

5.2.1 报文接口结构说明

报文基本结构如下图所示：

说明：总体上，报文全部内容封装在一个 XML 报文中，报文分为三大部分：报文头部分、报文体部分及数字签名部分。

- 报文头部分

报文头部分用于标识 XML 报文的基本属性，包括当前应用版本、发起节点代码、接收节点代码、应用名称、 报文的编号、版本号、标识号、参考号及 WY 的工作日期。

- 报文体部分

报文体部分用于存放具体的交易报文，其内容由具体应用的交易种类决定。

- 数字签名部分

数字签名部分用于存放报文的数字签名信息，用于交易参与方的身份认证。算法对报文开始至</CFX>之间的全部内容（不包括</CFX>之后的任何字符）进行签名，并以 XML 注释的形式存储于原 XML 报文的尾部。

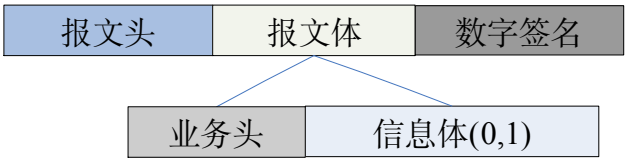
具体格式示例如下：

```
<?xml version="1.0" encoding="gb2312"?>
<CFX>
  <HEAD>报文头内容</HEAD>
  <MSG>报文体内容</MSG>
</CFX>
<!—数字签名 ==-->
```

WY 使用的报文按报文所含交易笔数分为两种：单笔报文和批量报文。

5.2.1.1 单笔报文结构

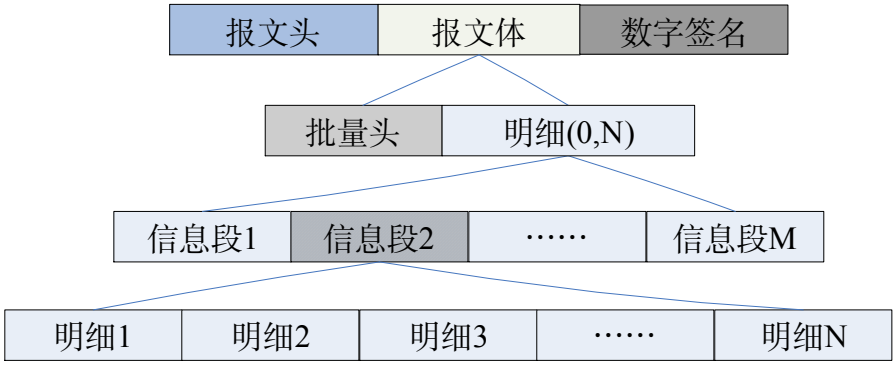
单笔报文指报文所含内容为单笔交易信息，而对于某些特殊报文甚至可以没有报文体(比如连接测试报文)。该类报文的结构如下图所示：



该类报文主要包括征收机关实时扣税请求、WY 转发实时扣税请求、实时扣税回执、实时冲正请求、实时冲正回执、与银行税票明细对账回执、止付请求、止付应答、撤销请求、撤销应答、交易状态查询请求、交易状态查询应答、自由格式报文、连接测试请求、通用应答、通用确认应答、通用处理结果通知、银行申报请求、银行申报回执、登录请求、登录应答、退出请求、退出应答、三方协议验证请求、三方协议验证应答、包明细重发请求和对账信息下载请求等;

5.2.1.2 批量报文结构

批量报文，批量头必选，并且将明细信息根据信息内容的不同划分为不同的信息段。某些信息段下又包含各个明细，其他信息段内容则属于各个明细的公共部分，并具有特殊的作用(比如定时批量扣税中的转账信息段还具有辅助路由的功能)。该类报文的结构如下图所示:



如征收机关批量扣税请求、WY 转发批量扣税请求、批量扣税回执、征收机关自缴核销请求、退库请求、更正请求、免抵调请求、与银行税票明细对账通知、与银行信息包核对通知、银行端缴款信息包核对通知、银行端缴款核对回执、与征收机关已扣税税票核对通知、与征收机关已入库税票核对通知、与征收机关退库核对通知、与征收机关更正核对通知、与征收机关免抵调核对通知、公共数据更新通知等。

5.2.2 文件接口结构设计

文件分两类分别是: WY 与征收机关和商业银行交互文件、TBS 和 WY 导入导

出文件内容。这两类文件均采用 XML 格式。系统为识别文件内容，制定了统一的文件名命名规范。文件内容与报文接口的结构相同。

5.3 内部接口

WY 内部接口采用报文接口方式，出于系统结构统一性和开发复杂性考虑，报文结构与外部接口统一。内部接口报文规范仅用来约定在 WY 中各个子系统间实时报文交换的规则。

6. 系统安全设计

6.1 安全体系总体建设思路

6.1.1 安全建设目标

根据 WY 系统的特点，在分析其应用环境和安全需求的基础上，建立完整、可靠的 WY 系统安全体系，对 WY 系统实施物理层面、网络系统层面、应用层面及运维管理方面等全方位的安全保护，从而保证 WY 系统的安全、可靠运行；保证 WY 系统重要信息的安全，确保相关实体的身份、操作的真实、可靠。

6.1.2 安全体系设计原则

1、最小影响

安全方案的建设应当尽可能小地影响 WY 系统和网络的正常运行，不能对现有的网络和业务运行产生显著影响，特别是不能造成业务系统性能明显下降、网络拥塞、服务中断、目标系统数据的破坏和泄露等问题。

2、整体性

WY 系统安全方案所涉及的范围和内容应当尽可能地整体、全面，应当包括安全涉及的各个层面，避免由于遗漏而造成未来的安全隐患。

3、标准性和规范性

安全方案的设计和具体实施应当依据国内和国外的相关标准、规范以及理论模型，避免杂乱无章、无序建设。

4、先进性

WY 系统安全方案的设计起点要高，应当采用成熟、先进、高效的软硬件平台和

技术，保证安全系统具有长久的生命力。

5、充分利用现有安全资源

WY 系统也是依托于人民银行内联网，充分利用内联网已经建设的安全系统，节约资源，最大发挥已有安全系统的效率。

6、易用性

WY 系统的安全措施最终要由人来完成，如果安全措施过于复杂，对操作人员的技术要求过高，反而可能造成安全隐患，因此易用性也是非常重要的一个原则。

6.1.3 安全体系总体架构

根据 WY 系统的安全需求，建设其安全保护体系，应该从物理、网络、应用、运维管理多个方面进行全面的考虑，最终实现这些不同层次和不同方面的全面、完善的安全防护体系，其最终要实现的安全体系总体架构如下图所示：

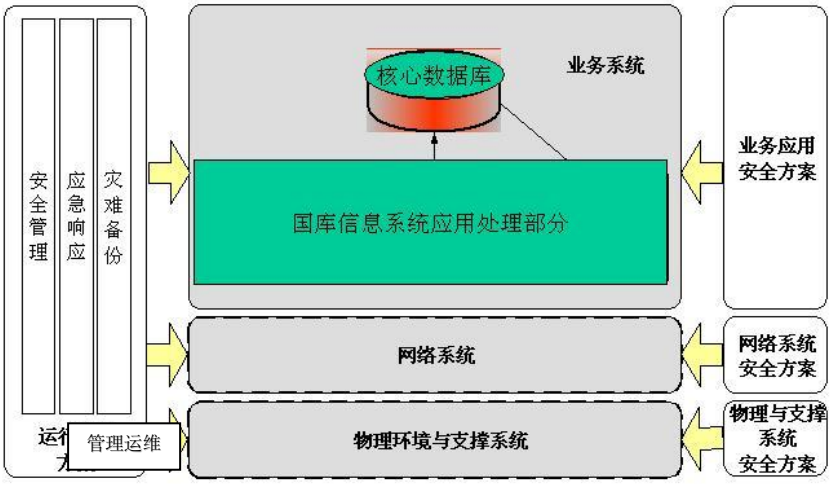


图 7-1 安全体系总体架构图

如图中纵向所示，安全系统总体可分为物理环境和支撑系统、网络系统及业务应用系统三个大的层面。每个层面要逐步实施和完善其所需的安全措施。

图中左侧部分给出了系统管理运维的安全要求，从管理运维方面提出了系统要实现的安全措施。

总体架构中安全体系所要求完善的各层面安全系统及不同方面的安全要求，需要

根据系统建设和运维中轻重缓急的需要，统筹规划，分步骤实施。

6.2 应用安全体系设计

WY 系统是人民银行的一个重要应用系统，其应用层面的安全措施需要建立在人民银行应用系统统一安全平台的基础之上。人民银行已经建设了内网统一 CA 认证基础设施，为人民银行应用系统提供了统一的安全服务平台，通过数字签名技术等密码技术为应用系统提供所需要的强身份认证、不可抵赖性、数据保密性、完整性等安全服务。

根据应用系统不同的结构，可以分为客户端到服务器端和应用系统到应用系统（即服务器到服务器）两种结构来讨论安全应用模式。

6.2.1 客户端接入

客户端到服务器结构的证书应用模式如下图描述：

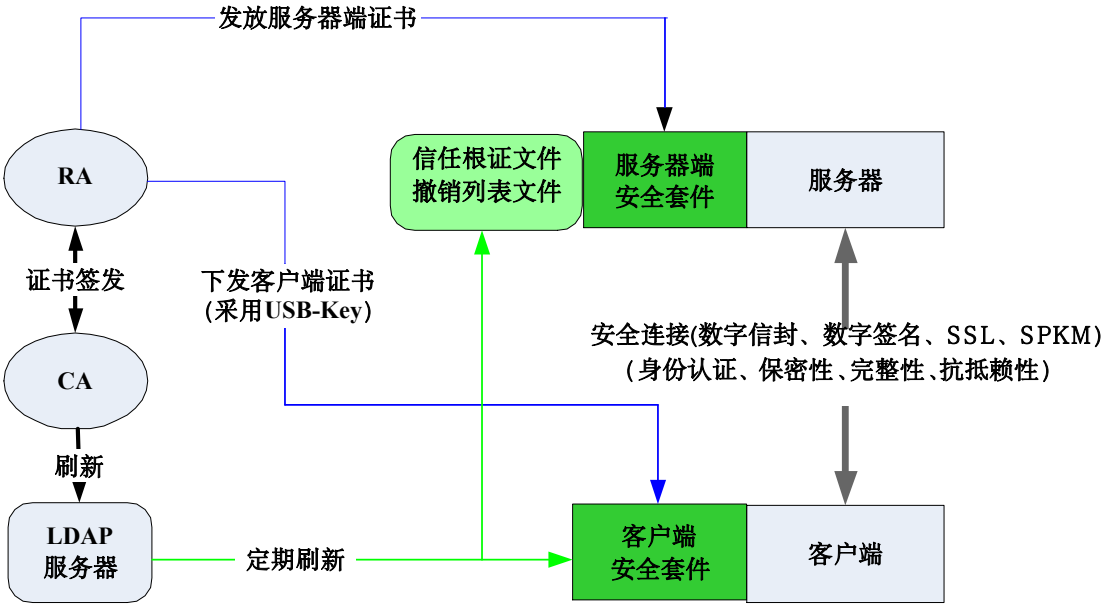


图 7-2 客户端到服务器端结构的证书应用示意图

对上图从以下几个方面说明：

（1）证书签发

如图中蓝色线条所示，应用系统的客户端和服务器首先将证书申请提交给 RA，RA 服务器完成审核后将证书申请请求提交给 CA 服务器，CA 服务器进行证书的签发，并将生成的证书发送给 RA 服务器，RA 服务器通过离线的方式将证书发送到用户，图中蓝颜色线条表示该业务。

(2) 证书验证

如图中绿颜色线条所示，在证书应用的过程中，应用系统需要查询目录服务器的证书撤消列表（CRL），以验证证书是否有效。对于客户端到服务器的结构模式，一般只是服务器端对客户端进行认证，在实际应用中为了提高应用系统的处理效率，通常做法是将证书撤消列表下载到应用系统服务器端的本地，定期刷新，以保证本地的 CRL 与服务器中一致。这样服务器端可以直接在本地查询，提高验证效率。

(3) 安全连接

客户端到服务器的结构模式中，两端可以通过多种方式建立安全连接（例如：数字信封、SSL 等），如图中在客户端和服务器端的安全连接示意。

(4) 安全服务

安全服务的实现通过在客户端和服务器端部署 CA 安全套件，实现所需的安全服务，如图中客户端和服务器端的左侧方框所示。所实现的安全服务如下：

a) **身份认证**。客户端和服务端在彼此的身份确认时，需要获得对方的数字证书，然后对数字证书进行有效性检查（其中包括上图的证书查询验证过程），只有证书被确认合法和有效的情况下方能确认对方的身份是有效的即完成身份认证。上图中的安全 SSL 连接协议中就集成基于数字证书身份认证的过程。WY 系统中涉及隐私、资金、重要报表、统计信息的相关操作和访问中，要实现对相关实体的身份认证。

b) **保密性**。数据的保密性主要是使用数字证书结合密码算法对原始数据进行密码运算。常用的算法有 RSA、DES、3DES 等。上图中的安全 SSL 连接协议建立成功后，在上面传输的数据的都是经过保密处理的。WY 系统中涉及隐私、资金、重要报表、统计信息的传输和存储中，需要保密。

c) **完整性**。数据完整性可以使用数字证书结合相关的签名算法。对于一般的 B/S 应用系统，在浏览器端可以使用插件的方式对需要的数据进行完整性处理，而在服务器端则可以对其进行完整性确认。而对于其他形式的应用系统，可以直接使用签名和验证的接口来保证完整性。在 WY 系统中，为了保证业务的顺利、可靠进行，通信和存储中的业务数据都要进行完整性保护。

d) **抗抵赖**。对相关行为或数据做签名处理，并在需要的时候加盖时间戳，可以保证一个行为确是一个实体在某一个特定的时间点上的行为。这些可以使用 CA 系统提供的安全接口服务组件对数据或者行为做抗抵赖性处理。WY 系统中与隐私、资

金、重要的报表和统计方面的信息、相关操作和访问都要实施基于数字签名技术的防抵赖安全服务。

6.2.2 外部机构接入

基于服务器到服务器结构的证书应用模式如下图所示：

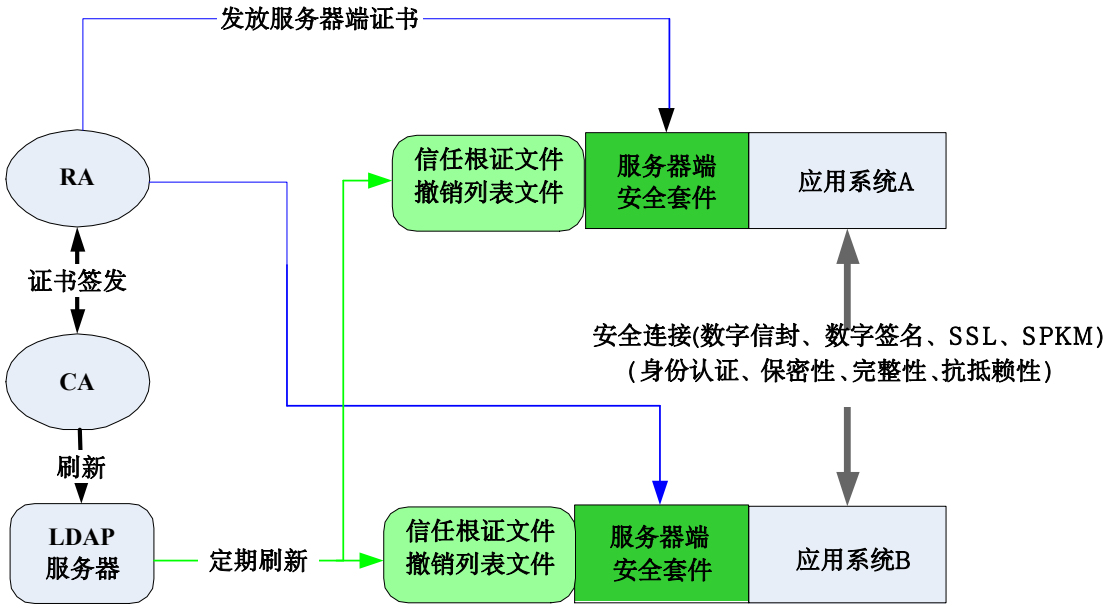


图 7-3 服务器端到服务器端结构的证书应用示意图

对上图从以下几个方面说明：

(1) 证书签发

如图中蓝色线条所示，应用系统 A 和应用系统 B 将证书申请提交给 RA，RA 服务器完成审核后将证书申请请求提交给 CA 服务器， CA 服务器进行证书的签发，并将生成的证书发送给 RA 服务器，RA 服务器通过离线的方式将证书发送到用户，图中蓝颜色线条表示该业务。

(2) 证书验证

如图中绿颜色线条所示，在证书应用的过程中，应用系统 A 与应用系统 B 需要查询目录服务器的证书撤消列表（CRL），以验证证书是否有效。实际应用中为了提高应用系统的处理效率，通常做法是将证书撤消列表下载到应用系统本地，定期刷新，以保证本地的 CRL 与服务器中一致。这样应用系统可以直接在本地查询，提高验证效率。

(3) 安全连接

应用系统 A 与应用系统 B 之间服务器到服务器结构的模式中，两端可以通过多种方式建立安全连接（例如：数字信封、SSL 等），如图中在应用系统 A 和应用系统 B 的安全连接示意。

（4）安全服务

安全服务的实现通过在应用系统 A 和应用系统 B 部署 CA 安全套件，实现所需的安全服务，如图中应用系统 A 和应用系统 B 的左侧方框所示。所实现的安全服务如下：

a) **身份认证**。客户端和服务端在彼此的身份确认时，需要获得对方的数字证书，然后对数字证书进行有效性检查（其中包括上图的证书查询验证过程），只有证书被确认合法和有效的情况下方能确认对方的身份是有效的即完成身份认证。上图中的安全 SSL 连接协议中就集成基于数字证书身份认证的过程。WY 系统中涉及隐私、资金、重要报表、统计信息的相关操作和访问中，要实现对相关实体的身份认证。

b) **保密性**。数据的保密性主要是使用数字证书结合密码算法对原始数据进行密码运算。常用的算法有 RSA、DES、3DES 等。上图中的安全 SSL 连接协议建立成功后，在上面传输的数据的都是经过保密处理的。WY 系统中涉及隐私、资金、重要报表、统计信息的传输和存储中，需要保密。

c) **完整性**。数据完整性可以使用数字证书结合相关的签名算法。直接使用签名和验证的接口来完成完整性保证。在 WY 系统中，为了保证业务的顺利、可靠进行，通信和存储中的业务数据都要进行完整性保护。

抗抵赖。对相关行为或数据做签名处理，并在需要的时候加盖时间戳，可以保证一个行为确是一个实体在某一个特定的时间点上的行为。这些可以使用 CA 系统提供的安全接口服务组件对数据或者行为做抗抵赖性处理。WY 系统中与隐私、资金、重要的报表和统计方面的信息、相关操作和访问都要实施基于数字签名技术的防抵赖安全服务。

6.2.3 应用系统的权限管理

在 WY 系统中，不同的外部机构具有不同的权限，人民银行内部不同人员具有不同的操作权限，对各种资源的访问和操作需要进行相应的权限管理和访问控制，避免非授权访问和操作造成的危害。为了实现对不同实体的权限管理，需要对系统中的相

关实体进行唯一标识，根据该标识对应实体的权限大小分配相应访问、操作权限。

在基于 CA 系统的安全体系中，比较方便的方式是提取系统中相关实体数字证书中的唯一标识即 DN(Distingshed Name)，作为该实体分配权限的标识。

6.2.4 数据中心的安全设计

对于 WY 系统来说，数据安全是前端应用支持核心动力和基本保障。从技术角度看，保证应用系统数据安全在计算机和存储系统有以下几个方面功能:

1. 主机操作系统安全要求 C2 级以上的安全标准
2. 设备安全。选择把数据安全性放在产品设计的首要位置的存储产品，选择那些经过长期实践证明的安全可靠的和存储设备；
3. 系统冗余。避免采用会造成单点故障的结构设计，避免使用缺乏热交换能力的系统设备；
4. 存储设备要有多级保护。从 RAID、冗余部件、远程镜像、集群等各个级别实施数据保护；
5. 对应用集群的支持。在设计本工程的体系架构时，已经考虑到应用服务器实施集群保护。所采购的设备应具备支持各种主流集群软件的柔韧性。
6. 24x7 应用支持。由于用户系统的特殊性，许多应用都属于 7x24 全天候运行的，一旦出现问题会带来难以挽回的巨大损失，针对这种需求，高性能的系统应该能够支持在 7x24 的应用条件下的实时数据应用，系统长时间运行应稳定如初，不能对应用系统有影响和对数据产生破坏。
7. 数据隔离与安全保护。访问系统的人员可能需要不同的权限、同一存储系统上运行多种应用等问题，试点工程中所采购的计算机和存储设备均可以保证不同用户的数据安全性，避免由于数据的混存、恶意入侵破坏等行为造成不必要的麻烦。
8. 网络和系统层面的安全保护。在网络和系统层面主要实施的安全系统包括防火墙系统，入侵检测系统、漏洞扫描系统和病毒防护系统，人民银行内联网已经部署了这些安全系统。其中防火墙系统用以 WY 系统网络层面的边界保护和访问控制；入侵检测系统是防火墙之后的第二道安全闸门；在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时检测；漏洞扫描系统把极为烦琐的安全检测，通过程序来自动完成，这不仅减轻管理者的工

作，而且缩短了检测时间，使问题发现更快；在网络环境下，计算机病毒有不可估量的威胁性和破坏力，计算机病毒的防范是 WY 系统安全防护系统建设中的重要环节。

6.2.5 数据审计

WY 系统涉及银行、税务、财政、海关等多方机构的资金往来业务，必须提供完整的数据审计能力。WY 系统日志设计中对所有往来的报文（含报文的签名）进行记录，保证了原始数据不会丢失和遗漏，为后续的数据审计奠定了良好的基础。

同时，WY 系统的数据库设计包含了实时交易库和历史查询库两部分，历史交易库中包含了所有的历史数据，不会被清除，实时交易库定期将最新的数据更新到历史查询库中。这样有效地保证了交易的快速、实时，同时也能保证所有的数据不会丢失，方便对历史数据的查询和审计。

6.3 安全管理运维建议

WY 系统的安全管理体系设计立足于总体安全防护策略，并与技术防护体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。安全管理体系主要体现在安全管理组织结构的建立和安全管理制度的制订与执行。

在这里，从技术的角度，就 WY 系统的安全管理和运维方式提出建议。

6.3.1 安全管理组织机构的建立

1、组织机构

为了保证 WY 系统的安全稳定运行，需要建立完善的 WY 系统安全管理组织，设置专门的安全管理组织机构，由国库机构的主要负责人担任安全组织的领导，从组织上保证系统运行的安全。

安全组织的职能主要是做好与有关信息安全管理部门的协调、协同；组织制定和执行信息系统的安全规划、安全策略、安全标准、应急计划等；组织建立健全并监督执行信息安全管理规章制度，强化内部控制和内部安全审计，实施安全监督、检查和风险分析，提出相应的对策；负责信息安全的宣传教育与培训。

WY 系统的安全管理体系的设计立足于总体安全防护策略，并与技术防护体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。安全管理体系主要体现在安全管理组织结构的建立和安全管理制度的制订与执行。

2、岗位设置及职责

在人员管理指定中主要是根据系统的需要，划分角色，配置人员，设置权限，制定相应的人员管理制度和管理策略，保证人员管理的安全性。

WY 系统需要配备系统安全员、网络安全员、系统管理员、网络管理员及系统和网络的操作人员。

1) WY 系统安全员的职责包括:

(1) 对整个所管范围的 WY 系统安全问题负责。在安全方面网络安全员、系统管理员、网络管理员和操作员要服从信息系统安全员的领导和管理。

(2) 负责系统安全策略、计划和事件处理程序的决策

(3) 负责安全建设和运营方案的决策

(4) 负责安全事件处理的决策

(5) 负责系统的安全培训

2) 网络安全员的职责

(1) 对整个所管范围的国库网络系统安全问题负责，接受系统安全员的领导和管理。与系统管理员和网络管理员进行有效合作

(2) 负责国库网络系统安全策略、计划和事件处理程序的制定

(3) 负责国库网络安全建设和运营的方案制定

(4) 承担国库网络安全事件的处理

3) 系统管理员的职责

(1) 对所管范围的计算机系统问题负责（不仅是安全问题），接受信息系统安全员的领导和管理。系统管理员要与网络管理员进行负责任的有效合作

(2) 参与计算机系统安全策略、计划和事件处理程序的制定

(3) 参与计算机安全建设和运营方案的制定

(4) 承担计算机安全事件的处理

4) 网络管理员的职责

(1) 对所管范围的网络系统管理问题负责（不仅是安全问题），接受网络安全员的领导和管理。与系统管理员进行负责任的有效合作。

(2) 参与网络系统安全策略、计划和事件处理程序的制定

(3) 参与网络安全建设和运营方案的制定

(4) 承担安全事件的处理

5) 操作人员的职责

(1) 接受系统安全员的领导，从事系统安全员分派的各种工作

(1) 完成管理章程和条例规定的日常工作

6.3.2 安全管理制度的制订与执行

WY 系统中的安全管理制度应该涵盖系统安全、可靠运行的各个方面。其中有的制度有国际、国内、行业标准可供参考制定与执行，有的需要在系统的建设和运行中逐步建立和完善。

WY 系统作为典型的信息处理系统，应该包含以下的安全管理制度：

(1) 安全教育与人员管理制度

(2) 物理环境安全管理制度

(3) 主机设备与系统安全管理制度

(4) 网络设备与系统安全管理制度

(5) 应用系统安全管理制度

(6) 业务系统安全运行管理制度

(7) 用户标识与密码管理制度

(8) 加密安全管理制度

6.3.3 WY 系统备份

备份业务是 WY 系统运维方面的重要内容。WY 系统是一个高度集中的信息系统，对其关键设备、数据、甚至整个系统的备份和恢复是系统建设必须考虑的重要问题之一。

为了保障业务数据的安全性，降低突发意外事件所带来的安全风险，需要考虑对应用系统和数据进行备份和恢复。WY 系统应根据自身的实际情况制定了关键系统和业务数据的备份和恢复制度，并且由专人负责监督该制度的实施和贯彻。

数据备份范围包括核心数据库的各种统计报表、国家财政收入、支出等关系国家经济运行重要数据等，需要考虑同时部署本地备份和异地容灾备份等多种备份方式，实现全方位多层次的数据保护。

各种备份工作将是 WY 系统运营的日常工作之一。如果备份方式不当，将会占用大量的人力资源和设备资源，不但容易发生操作失误，也会影响系统的运行效率。必须保证备份工作能高效、有序的进行，为此应该采用专用备份管理系统进行数据的自动备份与恢复，集中管理，简化维护工作，避免手工干预可能带来的误操作风险。必须有专人负责维护备份管理系统，进行数据备份工作，应该明确数据备份的策略、人员职能、以及操作规程。

国库信息处理系统备份解决方案可以参考国际标准 SHARE 78，如下表所示：

级别	特征	灾难恢复时间	灾难恢复解决方案涉及的技术和产品
级别 0	无异地备份数据	难以恢复	使用备份软件进行本地备份，备份数据不远离本地
级别 1	用交通工具将备份带放在异地	几周	使用备份软件工具进行本地备份，使用交通工具将备份数据传输到异地保存
级别 2	级别 1+热备份站点	几天	使用备份软件工具进行本地备份，同时在异地构建备份站点，使用交通工具将备份数据传输到异地保存
级别 3	通过电子链路将数据送往热备份站点	小于 1 天	使用光纤或者电信线路，将本地备份数据传送异地，同时异地有热备份站点
级别 4	活动状态的备援站点，主机	几个小时	使用专用软件工具进行远程复制

	的文件传送		
级别 5	两点两阶段提交，应用级别的数据镜像	小于 1 个小时	专用应用软件如数据库并行软件等，或者 TURECOPY 等异步硬件
级别 6	无数据丢失	即刻	存储控制系统实时远程拷贝技术 TURECOPY 等，同时采用集群技术

表 7-1 国库信息处理系统备份解决方案