基于邮政金融信息网的安全认证系统的设计与实现

王 刚

(陕西省汉中市邮政局，陕西 汉中 723000)

摘要：随着邮政金融业务的快速发展，邮政储蓄和汇兑资金案件时有发生，全国每年涉案金额约3 500万元，网点涉案次数占全部的65%左右，金额占48%左右。网点案件高发的主要原因是由于储蓄和汇兑网点比较多且分散，人员配备不足，岗位制约机制失效，权限管理得不到有效落实造成的。

本文从解决储汇资金安全需求着手，针对智能令牌身份认证系统的建设内容，提出了基于邮政金融信息网的安全认证系统的设计方案，在此基础上建立了智能令牌身份认证系统的技术架构，并结合邮政信息网安全机制，提供了实现方式。

关键词：智能令牌；身份认证；制约机制；储蓄；汇兑；资金安全

中图分类号：TP3－05 **文献标志码**：A **文章编号**：1671－1807(2013)05－0144－05

在邮政金融业务快速发展和邮政金融信息化全面推进的同时，邮政储蓄和汇兑资金案件时有发生，从近几年的统计数字来看，全国每年涉案金额在3 500万元，仅2008年百万元以上的大案就有7起，涉案金额达到1 759万元。其中涉案环节主要发生在营业网点前台操作上，从2008年到2010年的统计数字来看，全国网点涉案次数占全部的65%左右，金额占48%左右。网点案件高发的主要原因是由于储蓄和汇兑网点比较多且分散，人员配备不足，岗位制约机制失效，权限管理得不到有效落实造成的。

为解决储汇资金安全问题，必须建设智能令牌身份认证系统，从网点操作环节入手，利用现代高科技手段，实现从传统的静态口令向动态口令的转变，解决因网点人员口令泄露造成的非法登录和虚假授权等问题。智能令牌身份认证系统是基于挑战应答机制来验证用户身份合法、有效的动态口令认证系统。通过认证中心生成并下传挑战数，在智能令牌上计算应答数，再由认证中心进行安全认证。目前已完成陕西省所有邮汇联网网点令牌发放，以及一个省处理中心和一个省管理中心和10个市中心的建设，涉及全省储汇联网网点1 150个，全省柜员及授权管理人员总数6 500人。

1 系统存在的安全风险

邮政金融信息网以Client/Server模式运行，前台系统处理储蓄、汇兑等业务，后台数据库系统储存业务交易产生的各类账务和管理信息。

1.1 口令认证过程

营业员通过口令认证系统登陆业务系统进行业务操作，其口令认证过程：营业员输入人员代码和口令，并由前台通过网络传输到后台系统。后台系统根据人员代码，将营业员提供的口令与数据库中的口令进行对比，如果二者相同，则允许其进入系统。否则，系统拒绝进行任何业务操作[1]。

1.2 系统的安全隐患

前台营业员设置和使用口令过程中，存在三方面的安全隐患。

1)为便于记忆，某些营业员的口令是重复的字母和数字，口令的复杂度很低，容易被内部人员通过猜测进行盗用；

2)出于侥幸心理，某些营业员从不按规定定期更换口令，导致口令泄露；

3)前台人员数量配备不达标，存在一位营业员兼有多个角色的情况，并拥有多个口令和权限。

经过对上述情况分析，目前的口令认证系统是把营业员输入的口令与后台口令数据库中的口令进行比对，系统存在的安全隐患没有得到有效控制，这一缺陷容易被内部人员利用，从而造成邮政金融系统的安全风险。

收稿日期：2013－04－02

作者简介：王刚(1966—)，男，陕西汉中人，汉中市邮政局工程师，硕士，主要从事计算机网络和数据库的应用研究。

2 安全认证系统的设计

由于技术条件不足，在前台营业员之间，个人的登录代码和口令是相互透明的，存在安全性问题。应用智能令牌的登录安全控制是基于代码口令登录与挑战应答登录相结合的双因素身份认证机制，在储蓄和汇兑业务系统中实施这种安全机制，可以从技术上实现安全性和权责确定性[2]。

2.1 智能令牌身份认证系统架构

储汇安全认证的系统架构分为：安全认证省中心、市(县)局安全认证网点服务器及管理系统、网点物理信息采集设备三级架构[3]，系统架构如图 1 所示：

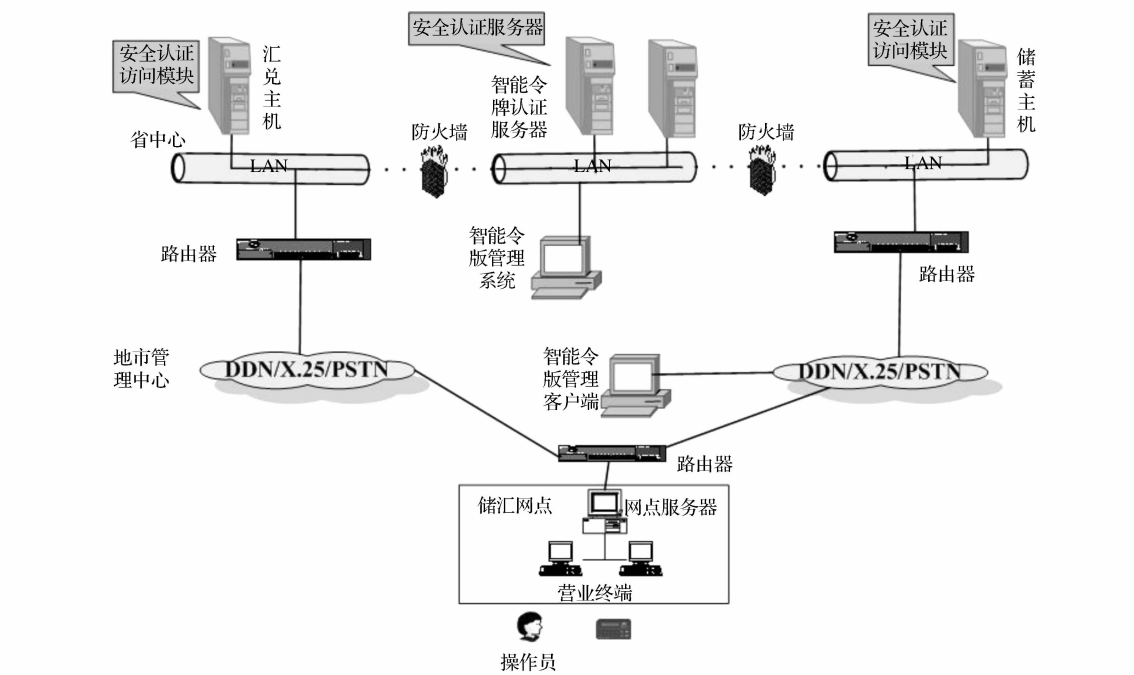

图 1 智能令牌身份认证系统结构

认证系统说明：

1)省中心建立集中认证中心采用独立于储蓄和汇兑主机的服务器，并实施双机热备方式，配置磁盘阵列。

2)省中心建立集中管理系统，包括安装一套管理服务器和管理客户端。

3)每个市中心安装一个管理客户端，操作系统为 Windows 环境。

4)各市中心的管理客户端上安装智能令牌系统监控客户端软件，实时监控认证服务器和管理服务器的工作状态，接收本地市范围内的告警认证和告警授权操作。

5)各市管理客户端配置 2 个智能令牌适配器。

6)网点操作人员和授权人员每人配备 1 块智能令牌。

2.2 系统认证流程

智能令牌身份认证系统面向广泛的安全认证领域[4]，通过如下认证流程完成系统用户的身份认证(见图 2)：

1)用户输入 ID 和固定口令通过固定口令认证；

2)系统主机访问认证中心，申请每次认证的挑战数；

3)认证中心生成并下传用于新认证流程的挑战数(每次不同)；

4)系统主机下传挑战数，系统人机界面向用户提示挑战数；

5)用户使用持有的智能令牌计算相应应答数，并输入人机界面；

6)系统人机界面向系统主机上传挑战数等认证信息；

7)系统主机向认证中心传送挑战数等信息请求认证；

8)认证中心响应认证结果，系统主机根据认证结果进行处理；

9)若认证失败，系统主机则不处理用户申请的相应事务，直接向人机界面传送认证失败信息；

10)若认证成功，系统主机则处理用户申请的相应事务，并向人机界面传送事务处理结果；

11)若认证告警,系统主机则通过预定告警方式向系统管理员发出告警信息,同时处理用户申请的相应事务,并向人机界面传送事务处理结果。

在上述认证流程中,用于系统用户身份认证的挑战数每次不同,应答数随挑战数变化而变化,可以有效防范当前系统单一采用固定口令而存在的诸多安全隐患。

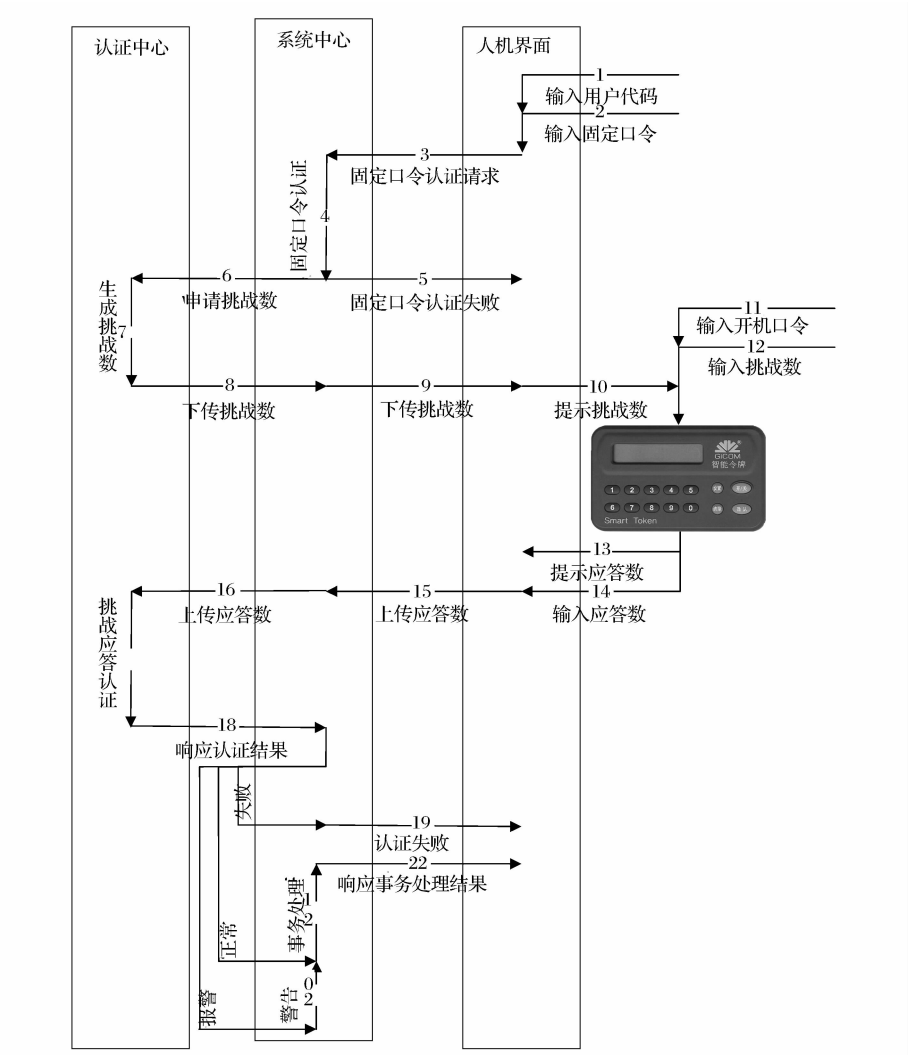

图 2　系统认证流程

3　安全认证系统的实现

陕西省邮政储汇安全认证系统的总体实现目标是:建成一个覆盖全省 10 个市局 89 个县局的安全认证系统,建设范围包含所有邮政储蓄网点。实现面向全省邮政金融系统内部人员的身份认证,实现对邮政储蓄等邮政金融业务系统操作人员的登录和业务授权进行身份认证,防止相关人员非法进入系统及业务人员越权操作,降低邮政金融风险,加强邮政金融系统安全。

3.1 系统应用功能

在邮政金融系统中实施智能令牌身份认证系统,可从技术上加强金融系统运行中的安全性和权责确定性[5]。

3.1.1　登录控制

安全登录控制实施代码口令登录和挑战应答登录两项控制,并要求只有在代码口令登录成功后才能进行挑战应答登录,并仅当挑战应答登录成功后才确认系统用户的登录申请被系统验证通过而被授权使用系统功能和分享系统服务。

实施上述验证过程的系统确保了系统用户享受服务的合法性、安全性和确定性[9]。

控制流程:

1)系统用户利用系统提供的服务终端进行登录申请;

2)用户在终端上输入代码和口令;

3)终端将用户输入的代码和口令上送至主机;

4)系统服务器对代码和口令进行验证,若验证失败则通知服务终端(服务终端向用户作相应提示),否则由系统服务器生成新的随机挑战数,并下传至服务终端,服务终端将挑战数向用户显示;

5)服务终端提示用户输入应答数;

6)用户在服务终端上输入利用智能令牌得到相应的应答数,并由服务终端上传至系统服务器。

系统服务器进行安全认证。若认证失败,系统服务器向服务终端下传该结果,服务终端提示相应信息并终止相应服务;若认证成功,系统服务器则进入向服务终端的用户提示业务服务[6]。

3.1.2 业务授权

在系统用户使用系统过程中,当其权限不足以完成某项业务功能时,可进行授权,例如冲正交易、取消交易、大额存取款交易等。实施安全控制的业务系统要求网点营业员在处理挂失等特殊业务时,要求在输入业务数据的同时,输入班组长或支局长的代码和口令,若代码和口令通过系统验证,要求拥有权限的班组长或支局长进行挑战应答式授权验证。当挑战应答式授权验证通过后,系统完成相应的业务处理请求;否则均由系统终端提示权限不足或授权失败,并拒绝处理相应业务。

控制流程:

1)系统用户在申请处理权限不足的特殊业务时,在输入相应特殊业务的数据后,输入授权的班组长或支局长的代码和口令;

2)终端将输入的代码和口令传输到系统服务器对代码和口令进行验证,若验证失败则通知服务终端;否则由系统服务器生成随机挑战数,并下传至服务终端,服务终端将挑战数向用户显示;

3)服务终端提示用户输入应答数;

4)授权的班组长或支局长亲自或以其它方式通知操作员在服务终端上输入利用智能令牌计算得到的应答数;

5)服务终端将业务数据与应答数上传至系统服务器;

系统服务器进行安全认证。若认证失败,系统服务器向服务终端下传该结果,服务终端提示相应信息并终止相应服务;若认证成功,系统服务器则对相应业务进行处理,并将处理结果通知服务终端,服务终端向实际操作员提示业务处理结果。

3.1.3 告警功能

当操作人员处于非正常环境下,可以以告警模式完成系统登录或业务授权,业务主机通过认证中心可以立即识别其告警信息,并在主机服务器或相关监控终端上响铃及消息提示通知系统管理员,并触发相应告警处理机制。

操作员只需要在智能令牌提示输入开机口令时输入告警口令,即进入告警模式,其后计算生成的应答数即为告警应答数,认证中心在验证时即可识别。

3.2 系统管理功能

智能令牌身份认证系统提供多种管理模式。根据邮政金融系统各地市网点分布等实际情况,从安全、经济的角度考虑,选用了如下管理模式。即:

1)省局中心的管理人员可以使用安装在省局中心的管理客户端进行智能令牌的发行工作,其中包括对智能令牌的初始化工作;

2)市县局中心的管理人员可以使用安装在市县局中心的管理客户端对本市县局范围内的令牌进行分配和管理,但不能对智能令牌进行初始化。

业务系统通过智能令牌管理系统对智能令牌实施统一管理:新增、删除、重新设置等;对业务操作人员实施统一管理:新增、删除、轮岗等。业务系统要求对上述管理功能的处理过程中,有相应的行政制度进行辅助,要求任何管理功能或应急处理的申请,均要求逐级申请批复[7-8]。

3.2.1 机构管理

机构管理是指对系统内的市县局、网点等机构进行管理维护,包括创建、删除、改名和批量操作等等。

3.2.2 智能令牌管理

智能令牌管理是指对系统内的智能令牌进行管理维护,包括新增、删除、设置和查询等等[9]。

3.2.3 人员管理

人员管理包括系统内的人员(实际的人,而非身份)管理(增加、删除、移动、停用、查询等)和人员与令牌的对应关系管理(指定令牌、撤销令牌、设置登录方式等)。

人员管理中移动功能是指把一个人员从当前机构移动到另外一个机构,这样,在人员变动时,就不需要重新增加删除人员了,只需要把该人员移动到新的机构下就可以了;停用是指对人员的所有权力进行禁止,停用后,该人员就不能进行任何活动。因此,对于一些暂时不用的人员,可以进行停用,使不能以任何其它身份进行活动[10-11]。

3.2.4 身份管理

身份管理是指对系统内的身份(操作员或智能令

牌系统管理员)进行管理,包括增加、删除、移动、停用、查询等。

3.2.5 应急管理

应急处理是指当操作员令牌不可用时采用的临时手段,包括使用应急静态口令或备用智能令牌两种方式。在具体使用时,智能令牌系统管理员可为操作员根据实际情况指定一种方式[12]。

应急静态口令:业务系统为操作员提供在挑战应答登录时使用的有时间限制的应急口令。当系统管理员为操作员下放应急口令后,系统会为该操作员设定应急标志;当该操作员进行挑战应答时,应输入相应的应急口令,经系统识别后确认通过安全认证。如果应急口令超过使用时限则不能认证,并提示相应错误[13]。

备用智能令牌:系统为操作员提供临时使用的智能令牌,系统管理员将不可用令牌与人员去掉关联,并将备用智能令牌与人员进行关联后,人员的相应身份就可使用备用的智能令牌进行登录和授权。备用智能令牌需要预先向各营业网点发放,在应急时,由系统管理员处理关联后,由值班主任向相应操作员发放即可。

3.2.6 审计管理

智能令牌身份认证系统提供认证流水记录和管理流水记录,管理人员可对上述流水记录进行审计、分析、备份和删除。

4 结束语

通过对邮政金融信息网的口令认证系统安全风险的分析,本文提出了智能令牌身份认证系统的架构,并根据身份认证系统的架构设计了处理流程,实现了对口令泄露等安全隐患的有效控制,确保了系统安全稳定地运行和邮政储蓄、汇兑资金的安全。但由于前台营业人员数量配备不足,仍然存在一位营业员兼有多个角色,并拥有多种权限的情况,这在一定程度上影响了系统应用的效果。邮政企业将进一步优化精简内部机构,把业务技能较高的人员充实到营业前台,以提高智能令牌身份认证系统的运行质量。

参考文献

[1]许红军,罗志强. 一般令牌网络的性能分析[J]. 北京航空航天大学学报,1995(1):16-22.

[2]陈兵,钱红燕,冯爱民. 电子政务鉴别和认证技术[J]. 电子政务,2005(8):65-79.

[3]陈春华. 通用安全框架与互联网用户认证系统[J]. 华南理工大学学报,2012(5):26-30.

[4]施荣华. 一种有效的令牌位格式捕获电路的设计和应用[J]. 长沙铁道学院学报,1993(3):17-23.

[5]苑旺清,赵振国,周广东. 工业智能令牌网的实现[J]. 信息技术,1995(4):44-48.

[6]周陆英,李人. 非对称令牌网络性能分析[J]. 计算机学报,1995(4):11-15.

[7]姜广政. 令牌在智能小区访客系统的应用[J]. 科技传播,2011(10):41-45.

[8]赖庆璋. 基于令牌的口令认证系统[J]. 技术与应用,2003(3):57-60.

[9]杨光. 主体鉴别和信息逻辑[J]. 计算机安全,2002(7):17-20.

[10]戴建中. 电子商务概论[M]. 北京:清华大学出版社,2012:7-21.

[11]汪红波,袁利永. 基于用户令牌实现服务身份验证[J]. 计算机与数字工程,2006(10):79-82.

[12]谢慧,王鲁达. 双因素身份认证令牌验证的 SSL VPN 应用网关研究与设计[J]. 湘南学院学报,2008,29(5):12-15.

[13]张秋余,梁爽. 一种新的基于 PKI 的动态身份认证系统的设计[J]. 计算机应用研究,2005(10):35-39.

Design and Fulfil in View of the Postal Financial Information Network Security Authentication System

WANG Gang

(The Postal Bureau of Hanzhong, Hanzhong Shanxi 723000, China)

Abstract: With the rapid development of postal financial business, Postal savings and remittance money case, involving about 35 million yuan a year across the country, The network involved in about 65% of the total number, amount is about 48%。Networks in case of the main causes of high incidence is due to the savings and remittances more outlets and scattered, inadequate staffing, Post restriction mechanism failure。rights management is not effective implementation。

From solution to store the remit money to security requirements, This paper aimed at intelligent token authentication system construction content, Based on the postal financial information network security authentication system design scheme, Based on the technology architecture of intelligent token authentication system, and combining the postal information network security mechanism, provides the implementation。

Key words: smart token; the identity authentication; restriction mechanism savings; remittance; money safe