ICS 35.240.40
A11
备案号:

JR

中华人民共和国金融行业标准

JR/T 0013—2004

金融业星型网间互联安全规范

The security specification for star topology inter-networking of financial industry

2004-12-01 发布　　2004-12-01 实施

中国人民银行　发布

目　次

前　言

金融业星型网间互联系列标准预计由以下两项标准组成：

— 《金融业星型网间互联技术规范》

— 《金融业星型网间互联安全规范》

本标准是其中之一。

金融业网间互联涉及中华人民共和国境内的所有银行、保险、证券及其它金融机构之间的互联。金融业网间互联业务分为两类：各金融机构以中国人民银行为中心进行的星型网间互联和各金融机构之间的计算机网络互联。本标准主要涉及金融机构与中国人民银行为中心进行的星型网间互联。

本标准与本行业目前普遍采用的ISO 7498-2:1989 《开放系统互连——基本参考模型 第2部分：安全体系结构》、ISO/IEC 17799:2000 《信息技术 信息安全管理实用规则》、ISO/TR 13569:1997 《银行与相关金融服务——信息安全指南》、NIST SP800-47《互联信息技术系统安全指南》等技术文件和标准相协调。

本标准的附录A是资料性附录。

本标准由中国人民银行科技司提出。

本标准由全国金融标准化技术委员会归口。

本标准主要起草单位：中国人民银行科技司、中国金融电子化公司、中国人民银行成都分行、济南分行、重庆营业管理部、长春中心支行。

本标准协作起草单位：华北计算技术研究所、国家信息安全基础设施研究中心、北京启明星辰信息技术有限公司、湖南电子信息产业集团有限公司、中国电子技术标准化研究所、中国标准研究院。

本标准主要起草人：谭国安、张永福、郭全明、陈逢吉、李曙光、林中、廖飞鸣、赵呈东、刘志军、陈立军、梁玉梅、陈在、朱玉林、张德栋、余恩至、周亦鹏、贾树辉、王莉。

金融业星型网间互联安全规范

1 范围

本标准规定了金融业网间互联安全保障体系，对星型金融业网间互联涉及的信息安全保障技术、物理环境与人员安全、安全运行与管理提出了规范性要求和应遵循的标准。

本标准适用于在中华人民共和国境内开业的所有银行、保险、证券及其它金融机构。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 2887－2000	电子计算机场地通用规范
GB 17859－1999	计算机信息系统安全保护等级划分准则（NEQ DoD 5200.28-STD NCSC-TG-005）
GB 4943－2001	信息技术设备的安全（IDT IEC 60950:1999）
GB 50057－1994	建筑物防雷设计规范
GB/T 17903.2－1999	信息技术 安全技术 抗抵赖（IDT ISO/IEC 13888-2:1998）
GB/T 18018—1999	路由器安全技术要求
GB/T 18019－1999	信息技术 包过滤防火墙安全技术要求
GB/T 18020－1999	信息技术 应用级防火墙安全技术要求
GA 243－2000	计算机病毒防治产品评级准则
JR/T 0012－2004	金融业星型网间互联技术规范
ISO/IEC 17799:2000	信息技术 信息安全管理实用规则
IETF/RFC 3161	时间戳协议
IETF/RFC 1901	简单网络管理协议 V2
IETF/RFC 2865	用户远程拨号认证协议

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

外联网络 extranet

为实现金融机构间计算机网络互联，参与互联的金融机构在各自内部网络的基础上拓展出的网络区域，用于与其它机构的相应外联网络互联。

3.1.2

局部计算环境 local computing environment

由局域网内的网络和计算设施构成的环境称为局部计算环境。

根据金融业星型网间互联的技术体系结构，对应三类外联网络，相应有三类外联网络局部计算环境：

——总部级外联网络局部计算环境简称总部级外联环境；

——省级外联网络局部计算环境简称省级外联环境；

——地市级外联网络局部计算环境简称地市级外联环境。

3.2 缩略语

下列缩略语适用于本标准。

API	Application Program Interface	应用程序接口
CA	Certificate Authority	数字证书认证中心
KMC	Key Management Center	密钥管理中心
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
OCSP	Online Certificate Status Protocol	证书在线状态查询协议
PIN	Personal Identification Number	个人身份识别号
PKI	Public Key Infrastructure	公钥基础设施
RA	Registration Authority	证书审核注册中心
SNMP	Simple Network Management Protocol	简单网络管理协议

4 金融业星型网间互联安全保障体系

4.1 安全保障体系

金融业星型网间互联安全保障体系将实现安全服务所有的安全保障措施和行动，按人、技术、运作和管理四个要素划分为四个层面，如图1所示。

人、技术、实施运作和安全管理是金融业星型网间互联安全保障体系中的四个重要组成部分：具有安全意识的人利用各种技术，在良好的管理下对金融业网间互联涉及的网络和互联业务系统进行运作，从而达到确保网络和互联业务系统安全性的目的。

金融业星型网间互联安全保障体系框架由技术层面、运作层面、人的因素、管理层面、安全策略5个部分构成。如图1所示。

4.1.1 技术层面

技术层面的主题是信息安全保障（IA: Information Assurance）技术，基本的安全方针是应用纵深防御战略，注重防内和整体防外。

与技术层面相关的安全措施和行动主要包括：

a）互联应用系统安全

网间互联应用系统安全包括以下几个方面：

- 授权
- 访问控制
- 身份鉴别
- 安全审计
- 应用系统安全管理
- 数据的完整性
- 数据的保密性
- 操作和数据的抗抵赖

b）外联网络局部计算环境安全

- 操作系统安全
- 主机安全检测与响应
- Web服务器的安全
- DNS服务器安全
- 数据库安全
- 系统安全审计

c）外联网络与边界安全

- 网络设施的安全
- 防火墙
- 接入认证/远程访问控制
- 通信加密
- 入侵检测
- 漏洞扫描
- 网络防病毒
- 网络安全审计

d）互联安全支撑设施

- 证书服务系统
- 授权服务系统
- 密钥管理系统
- 密码服务系统
- 可信时间服务系统

4.1.2 运作层面

安全运作涉及日常维持网络与业务系统安全态势的所有活动。安全运作的重点是保障互联业务的持续安全可靠运行。

与运作相关的安全措施和行动主要包括：

——安全状态维护；

——安全评估；

——事件处理；

——可用与可靠性设施。

4.1.3 人的因素

人的因素的核心是提高人们积极主动的安全防范意识，形成安全的物理和文化环境。

与人的因素相关的安全措施和行动主要包括：

——人员安全；

——物理与环境安全。

4.1.4 管理层面

管理层面要强调人的因素、技术层面和运作层面三种要素的协同和均衡。信息安全是过程，安全管理必然不可缺少。安全管理涉及人与环境、安全技术以及安全运作的各个方面，良好的安全管理机制和措施是各种要素取得均衡的关键。

与管理层面相关的安全措施和行动主要包括：

——安全管理模式；

——安全管理制度；

——安全技术的管理；

——安全运行管理。

4.1.5 安全策略

金融业星型网间互联安全保障策略包括：

——总体安全策略；

——人员与物理环境相关的安全策略；

——信息保障技术相关的安全策略；

——运行和操作相关的安全策略；

——安全管理策略。

金融业星型网间互联安全保障策略由参与网间互联的各机构联合组成的互联安全小组负责制定、修订和解释。金融业星型网间互联安全保障策略应重点针对互联业务对安全的需求，兼顾风险、脆弱性、应遵守的法规和安全技术现状与发展。

4.2 金融业星型网间互联安全要求

4.2.1 金融业星型网间互联安全保障的范围

金融业星型网间互联安全保障关注的范围包括：互联应用系统安全、外联网络局部计算环境安全、外联边界与网络安全，网间互联安全支撑设施，网间互联安全运行、操作与管理，网间互联物理环境与人员安全。如图2所示。

4.2.2 互联安全域的划分

JR/T 0012－2004确定的互联业务模式是参与互联的各机构在传统的内部网络的基础上，通过部署独立的接入路由器和必要的边界防护措施（如防火墙等）设立各自的外联网络实现互联，各自的外联网络区各自维护管理，但必须遵守统一的技术和安全规范。为了便于分级管理，实现“统一规范、分级管理、各自负责”的安全管理模式，将金融业网间互联安全域按以下方式划分：

a） 金融业星型网间互联涉及的整个区域定义为一个互联网络安全域。互联网络安全域包括各参与互联机构的所有外联网络区、外联网络区内的设施、互联涉及的各种网络设施、网间互联应用系统及信息和与网间互联有关的各类人员。图 3 中的互联网络安全域仅示意了两个参与互联的机构。

b） 按地市级互联的技术模式，整个互联网络安全域分为总部级安全域、省级安全域和地市级安全域三个子安全域。总部级安全域包括所有参与互联的各机构的总部级节点外联网络区、总部级节点互联涉及的各种网络设施、网间互联应用系统及信息和与网间互联有关的各类人员；省级安全域包括所有参与互联的各机构的省级节点外联网络区、省级节点互联涉及的各种网络设施、网间互联应用系统及信息和与网间互联有关的各类人员；地市级安全域包括所有参与互联的各机构的地市级外联网络区、地市级节点互联涉及的各种网络设施、网间互联应用系统及信息和与网间互联有关的各类人员；各级节点外联网络区是该级安全域的一个子安全域。图3中的各级安全域仅示意了两个参与互联的机构。

c） 各级外联网络区划分为中立区和外联区两个部分。根据网间互联业务安全的需要，中立区可以进一步分为互联业务区、互联服务区和互联管理区。其中，互联业务区放置互联前置系统，互联服务区放置提供信息服务的设施（如 Web 服务器、DNS 域名服务器、Mail 服务器等），互联管理区放置互联网管设施、接入认证设施等。如图 4 所示。

根据业务重要程度和安全隔离的需要，在总部级外联网络和省级外联网络，互联业务区可以进一步分为A型互联业务区、B型互联业务区和C型互联业务区，分别对应特别重要类、重要类和普通类互联业务应用系统。各级外联网络区的联接边界分为内联边界和外联边界二种。内联边界是外联网络与机构内联网连接的边界；外联边界是外联网络与对端网络连接的边界（通过路由器接城域网的主干网）。

对于金融业星型网间互联涉及的联接边界，本标准采用如下约定：

- 总部级外联网络区外联边界简称总部级外联边界；
- 总部级外联网络区内联边界简称总部级内联边界；
- 省级外联网络区外联边界简称省级外联边界；
- 省级外联网络区内联边界简称省级内联边界；
- 地市级外联网络区外联边界简称地市级外联边界；
- 地市级外联网络区内联边界简称地市级内联边界。

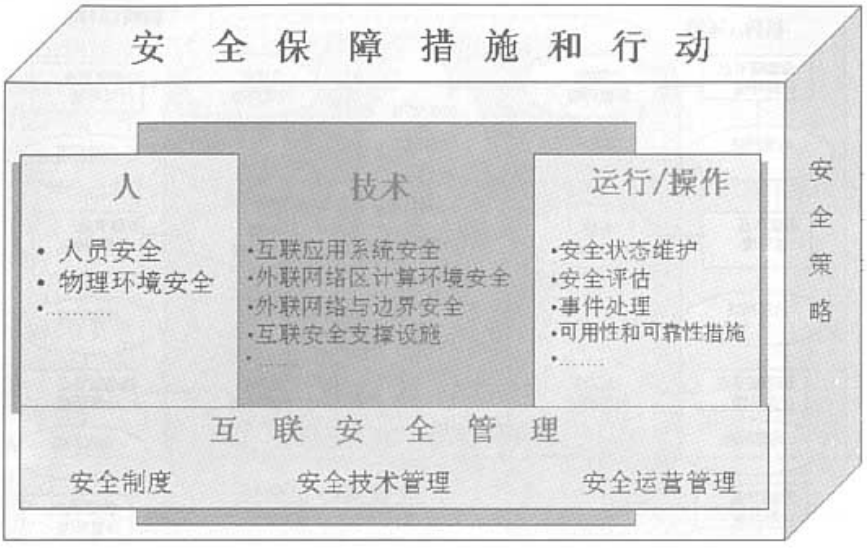


图 1　网间互联安全保障体系框架

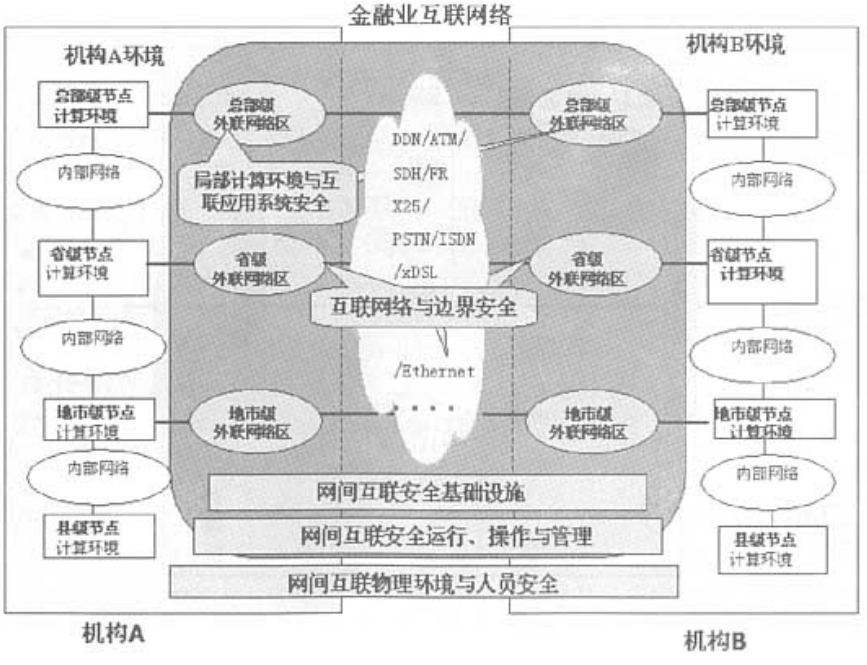


图 2　金融业星型网间互联安全保障关注的主要领域

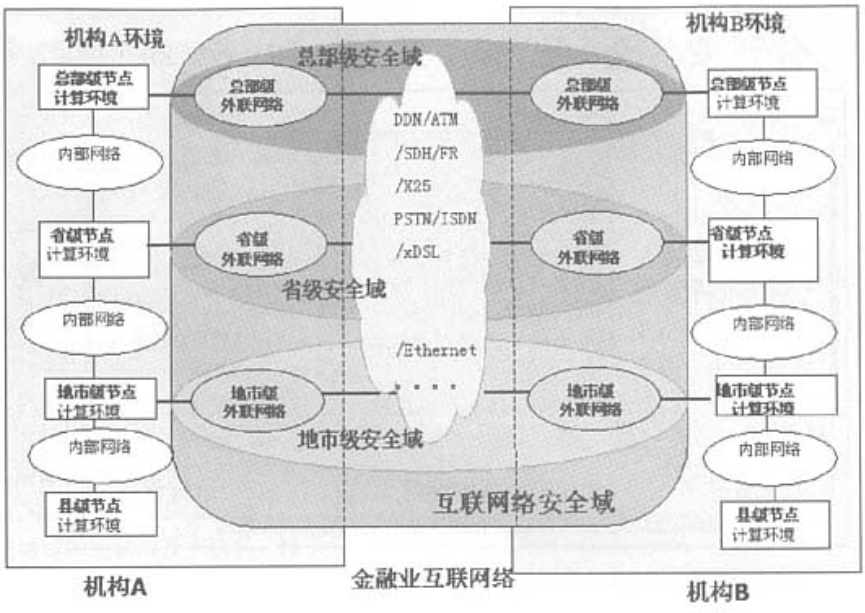
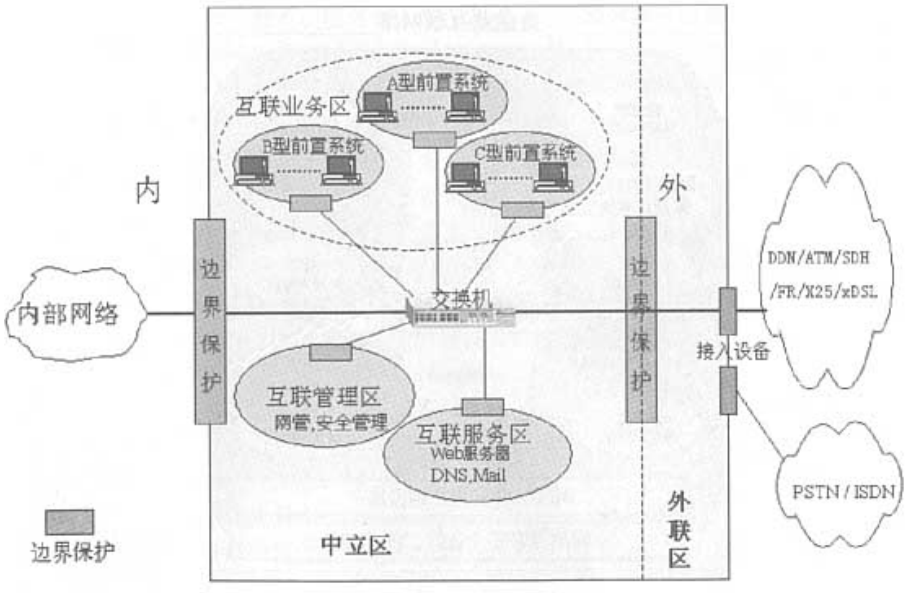


图 3　安全域划分示意图



外联网络环境

图 4　某级外联网络区示意图

4.2.3 信息、应用系统分类及安全等级要求

4.2.3.1 信息/数据的敏感程度

金融业星型网间互联涉及的信息/数据分为三类：

——金融业内部分公开；

——金融业内公开；

——向全社会公开。

4.2.3.2 应用系统分类

依据互联应用系统的特点和安全性等属性的要求，金融业星型网间互联涉及的应用系统分为三类：

——特别重要；

——重要；

——普通。

应用系统的分类主要依据应用系统的属性。本标准按表1对金融业星型网间互联涉及的应用系统进行分类。

表1 金融业星型网间互联应用系统分类

分类	属性					
	涉及信息敏感程度	业务关键性程度	对可用/可靠性的要求	对容灾备份设施的要求	涉及的互联网络	安全保护等级要求（GB17859）
特别重要	业内部分公开	特高	特高	特高	总部级和省级节点	2 至 4
重要	业内部分公开/业内公开	高/中	高/中	高/中	总部级，省级和地市级节点	2 至 3
普通	向全社会公开	低	低/中	低	总部级，省级和地市级节点	1 至 2

4.2.3.3 应用系统安全等级要求

金融业星型网间互联涉及的应用系统分为特别重要、重要和普通三类。这三类的安全保障等级要求与GB17859-1999有如下对应关系：

——普通类基本对应第一级（用户自主保护级）到第二级（系统审计保护级）；

——重要类基本对应第二级（系统审计保护级）到第三级（安全标记保护级）；

——特别重要类基本对应第二级（系统审计保护级）到第四级（结构化保护级）。

4.2.4 互联网络分类

金融业星型网间互联涉及的互联网络分为三类：

——总部级节点互联网络；

——省级节点互联网络；

——地市级节点互联网络。

5 互联应用系统安全

5.1 概述

网间互联应用系统主要涉及外联网络区的前置系统、服务器端接收部件和客户端发送部件。本章规范了网间互联应用系统的安全功能要求，对三类（特别重要类、重要类和普通类）互联应用系统分别提出了应采取的安全保护措施。

5.2 互联应用系统的安全功能要求

5.2.1 授权

在设计具体互联应用系统的授权功能时，必须考虑以下功能要求：

——提供细粒度的授权管理功能；

——禁止绕过应用界面直接查看或操作数据库；

——必须将业务权限与系统管理权限分离，防止系统管理员权力无限扩大。

5.2.2 访问控制

在设计具体互联应用系统的访问控制功能时，必须考虑以下功能要求：

——角色定义：系统必须使用角色进行访问控制的判断，而不是直接使用用户进行；

——业务权限的管理：在应用系统中，应该更多地考虑与网间互联业务相关的业务权限，包括界面操作的控制以及对数据的访问权限等；

——应用系统应提供可配置的超时键盘锁定功能；

——防止异常中断后非法进入系统。

5.2.3 鉴别/认证

鉴别/认证机制包括身份认证和数据源认证两大类。根据应用系统安全需求的不同，应用系统的身份认证可以选择口令机制、一次性口令机制或密码机制（数字证书）等方式；数据源认证可以选择加密、数字签名等方式。

对网间互联应用系统口令的要求如下：

——对口令的长度具有检查的功能，口令长度至少八位，口令长度可配置；

——对口令进行加密存储；

——应用系统在初次使用时，应提示用户修改口令；

——口令机制应能定期强制用户修改其口令，定期时间可配置；

——口令失败超过预定的次数，应对该帐户进行锁定、限时锁定等措施；

——对用过的口令作记录，以防重复使用，记录的时间段可配置；

——应用系统不提供自动保存口令的功能；

——使用验证延迟，防止计算机自动猜测口令。

采用一次性口令机制时必须考虑以下问题：

——认证发起端和接收端必须使用相同的可信时钟；

——认证发起端和接收端必须使用相同的随机序列发生器。

采用密码机制（数字证书）时必须考虑以下问题：

——密码算法符合国家规定，产品经过国家有关密码部门批准；

——密码认证协议和认证服务器必须能够抵御重放和窃听攻击；

——数字证书的支撑性设施应能提供高层的通信安全服务 API，应用开发人员只需要调用相关 API 即可实现双向的身份鉴别。

5.2.4 安全审计

在设计具体互联应用系统的安全审计功能时，必须考虑以下功能要求：

——互联应用系统要能够存储完整的交易清算记录和系统运行记录，并按安全策略的要求定期进行备份；

——系统运行记录应包括用户的登录时间、退出时间和所进行的操作；

——互联应用系统应提供审计数据接口，便于集中审计管理；

——提供丰富的审计统计和分析功能，方便检查审计追踪记录，为管理员进行决策提供充分的依据；

——在具备完善的证书服务系统、时间戳服务系统的条件下，可以考虑基于证书服务系统、时间戳服务系统等安全支撑性基础设施提供数据的安全采集、存储功能，通过数字签名保证审计数据的完整性，提供应用层次的可信审计。

5.2.5 应用系统安全管理

在设计具体互联应用系统安全管理功能时，必须考虑以下功能要求：

——提供应用软件、应用数据的备份与恢复模块，集中统一管理数据的备份与恢复；

——提供独立的用户和权限设置和管理模块。

5.2.6 数据的保密性

在设计具体互联应用系统的数据的保密性保护功能时，必须考虑以下功能要求：

——采用访问控制机制防止入侵者观察敏感信息；

——采用密码机制实现数据传输和存储的保密性。所使用的密码产品必须经过国家有关部门的批准；

——参与互联的相关机构在密码算法选择、填充方式、同步机制以及密钥管理等方面应符合国家密码管理部门的有关规定；

——所使用的公钥基础设施应符合国家有关主管部门有关要求及本标准第8章“网间互联安全支撑设施”的技术要求。

5.2.7 数据完整性

数据完整性的保护机制可以通过测试字（密押）、数字签名、封装、序列完整性等方式实现。在设计具体互联应用系统的数据完整性保护功能时，必须考虑以下功能要求：

——提供连接完整性服务、无连接完整性服务和选择字段完整性服务；

——数据的完整性遭受破坏时，必须能够检测出来，并向用户报警；

——对应用系统的输入/输出数据数据进行确认与校验，以确保输入/输出数据正确和恰当；

——使用的密码算法必须符合国家规定，产品经过国家有关部门的批准；

——参与互联的相关机构在密码算法选择、填充方式、同步机制以及密钥管理等方面应符合国家密码管理部门的有关规定；

——所使用的公钥基础设施应符合国家有关主管部门有关要求及本标准第8章“网间互联安全支撑性基础设施的技术要求”。

5.2.8 抗抵赖

抗抵赖应能支持数据源的抗抵赖和数据交付的抗抵赖。数据源的抗抵赖主要可以通过数字签名、令牌等方式实现；数据传递的抗抵赖主要可以通过数字签名、令牌、可信交付代理等方式实现。

在设计具体互联应用系统的抗抵赖功能时，必须考虑以下功能要求：

——证据必须包括以下内容：身份（在源抗抵赖中为发起者的身份，在交付抗抵赖中为接收者的身份）、数据的精确值、事件的时间和日期、对方的身份和与证据相关的所有可信第三方的身份；

——可信第三方必须能够对其代表的那一方进行密钥和身份的证明，并确保维持可信的时间源；

——可信第三方的功能承担者必须独立并能够为其他角色所信赖和接受；

——密码算法必须符合国家规定，产品经过国家有关权威部门批准，密钥管理应符合国家密码管理部门的有关规定；

——所使用的公钥基础设施应符合国家有关主管部门有关要求及本标准第8章“网间互联安全支撑性基础设施的技术要求”。

5.3 互联应用系统安全配置

本标准只涉及与外联网络区连接与交换信息的安全和前置系统与对等网络前置系统或用户端连接与交换信息的安全。

5.3.1 特别重要类

特别重要类互联应用系统需要采取强可用性和强可靠性措施，其前置系统和业务逻辑处理系统需要冗余配置，需要采取同城异地灾备措施。需要对数据进行端到端加密，需要对重要的安全配置信息进行加密存储，需要采用强的身份鉴别机制和强的访问权限控制机制。强的身份鉴别机制是指一次性口令或数字证书；强的访问控制机制是指通过数字证书的属性扩展项中的主体属性提供有效访问控制，通过在客户端提供个性化定制特定访问控制方式，并加以数字签名；具体布置如下：

a） 用户端需要的安全机制
- 数据/文件加密传输、解密
- 口令的加密
- 防拷贝（使非法用户无法利用通常的拷贝命令或拷贝软件完整复制应用软件）
- 数字签名

b） 前置系统需要的安全机制
- 前置系统主机、网卡、电源冗余配置
- 同城异地灾备措施
- 数据/文件加密传输、解密
- 重要安全配置信息的加密存储
- 身份鉴别
- 访问控制
- 数字签名

c） 业务逻辑处理系统
- 数据/文件加密传输、解密
- 强身份鉴别
- 细粒度访问控制
- 数字签名

5.3.2 重要类

重要类应用系统需要对数据传输进行加密（节点间传输加密），需要对重要的安全配置信息进行加密存储，需要采用强的身份鉴别机制和强的访问权限控制机制。强的身份鉴别机制是指一次性口令或智能IC卡；强的访问控制机制是指通过数字证书的属性扩展项中的主体属性提供有效访问控制，通过在客户端提供个性化定制特定访问控制方式，并加以数字签名；具体布置如下：

a） 用户端需要的安全机制
- 数据/文件加密传输、解密
- 口令的加密
- 防拷贝（使非法用户无法利用通常的拷贝命令或拷贝软件完整复制应用软件）
- 数字签名

b） 前置系统需要的安全机制
- 数据/文件加密传输、解密
- 重要安全配置信息的加密存储
- 高可用性配置
- 身份鉴别
- 访问控制
- 数字签名

c） 业务逻辑处理系统
- 数据/文件加密传输、解密
- 身份鉴别

- 访问控制
- 数字签名

5.3.3 普通类

普通类应用系统需要采用身份鉴别机制和访问权限控制机制，身份鉴别机制主要是指普通口令和一次性口令；访问权限控制机制是指通过访问控制列表，绑定主体与客体之间的关系提供访问控制。具体布置如下：

a) 用户端需要的安全机制
   - 口令的加密

b) 前置系统需要的安全机制
   - 身份鉴别
   - 访问控制

c) 业务逻辑处理系统需要的安全机制
   - 身份鉴别
   - 访问控制

5.4 应用系统建设中应遵循的安全原则

a) 起点进入原则：从系统建设一开始就考虑安全问题，如果在系统设计的早期没有考虑安全性，就会因为错误选择留下基础隐患，以致为保证系统的安全花更大的代价；
b) 长远安全预期原则：对安全需求要有总体设计和长远打算，包括为安全设置一些可能马上不会用到的潜在功能；
c) 最小特权原则：不给用户超出执行任务所需权力以外的权力；
d) 公认原则：参考当前在基本相同的条件下通用的安全防护措施，据此而作出自己的决策；
e) 适度复杂与经济原则：考虑机制的经济合理性，尽量减少安全机制的规模和复杂度，使之具有可操作性。

6 外联网络局部计算环境安全

6.1 概述

金融业星型网间互联涉及三种局部计算环境：总部级外联环境，省级外联环境和地市级外联环境。三种局部计算环境分属于三个安全子域，各种局部计算环境实施的安全保护的强度取决于其所属的安全域和涉及的互联业务应用系统的类别。

外联网络局部计算环境安全应包括：

——操作系统安全；
——主机安全检测与响应；
——Web 服务器的安全；
——DNS 服务器安全；
——数据库安全；
——外联网络环境安全审计。

6.2 操作系统的安全

6.2.1 操作系统的安全等级要求

总部级外联环境和省级外联环境内使用的操作系统至少达到系统审计保护级；地市级外联环境内使用的操作系统至少达到自主保护级以上。

6.2.2 操作系统的配置管理

配置和管理操作系统时要：

——及时配置最新安全补丁；
——符合最小配置原则；

——采用安全配置工具。

6.3 主机安全防护与检测

总部级外联环境和省级外联环境使用的主机，应具有如下基于主机的安全防护与检测功能：

——网络防病毒客户端；

——主机入侵检测系统（仅对特别重要的服务器，选用的产品必须与该服务器的操作系统、应用软件互相兼容）；

——主机漏洞扫描（仅对特别重要的服务器）。

6.4 互联业务数据库的安全

本标准所指互联业务数据库是指各级互联区内的互联管理和服务以及前置系统所涉及的业务数据库（如日志数据库）。各级安全域的互联业务数据库的安全要求至少达到系统审计保护级，并且在业务数据处理异常情况下能够保障数据的完整性。

6.4.1 功能要求

互联业务数据库要求具有如下安全功能：

——数据库身份鉴别：对用户标识，采用口令进行鉴别，确保用户唯一性；

——自主访问控制：要求有更细粒度的访问控制，定义属性和授权规则；

——客体重用：对动态分配与管理的资源，在确保信息安全的前提下重用；

——审计：要求与身份鉴别、自主访问控制等安全功能相结合设置审计功能；

——数据完整性：防止非授权用户修改、破坏或删除传输、处理、存储的数据。

6.4.2 配置要求

互联业务数据库在配置上要求：

——以提高数据库的安全性和运行效率为目的，根据安全策略制定合理的安全规则和安全程序（含权限设置）；

——提供运行可靠的数据库管理系统；

——备份和恢复机制要结合系统需要进行合理配置；

——及时配置当前完整的安全补丁。

6.5 Web服务器的安全

Web服务器的安全要求：

——主要防止WEB页面的篡改、未经授权的存取动作、窃取系统的信息和破坏系统；

——提供统一的接入界面，以及单向数据的发布；

——为保证金融业信息的完整性，应对重要信息提供防篡改功能；

——防篡改功能应通过对重要数据和信息添加完整性标识来体现，并应具备在一定时间内恢复原有数据和信息的功能；

——完整性标识可基于公钥基础设施技术，应用数字签名方式实现。

6.6 DNS服务器的安全

DNS服务器负责维护域名/IP地址映射数据库，实现域名和IP地址的转换。网间互联使用的DNS服务器应符合以下安全要求：

——服务器配置中对主机的命名应采用不规则的方式，以保护整个网络的拓扑结构；

——采用设置区域列表存取下限、监督DNS使用的端口，防止远程缓存溢出攻击和拒绝服务攻击；

——要保证DNS的安全动态更新和操作系统环境中区域传输安全；

——要通过活动目录安全实现DNS的安全；

——要能够有效地防止DNS欺骗、域名劫持攻击；

——要在DNS中加入动态负载平衡特性，以解决网络过载问题；

——利用防火墙有效保护DNS服务器；

——必须保证DNS处理的完整性，通过数字签名机制提供DNS信息的完整性。

7 外联网络与边界安全

7.1 概述

外联网络与边界安全针对外联网络和进出入外联网络的数据流进行有效的控制，提供安全服务。网间互联外联网络与边界安全防护措施包括网络设施的安全、防火墙系统、远程访问和接入认证、通信加密，入侵检测系统、脆弱性扫描系统、防病毒系统和外联网络的安全审计等。

7.2 网络设施的安全要求

网络设施的安全要求有：

——路由器必须提供认证机制，确保非授权主体无法将路由更新信息插入网络；

——网络管理协议采用 SNMPV2，同时应参照口令管理方式设置口令；

——访问控制表必须明确指定互联区可以互通的 IP 网段；

——禁止外联网络区用户登录访问中立区和边界的网络设施；

——根据重要性选择互联方式，对关键线路提供链路冗余和设备备份；

——选用的路由器产品应符合 GB/T 18018—1999 路由器安全技术要求。

7.3 防火墙系统

7.3.1 使用要求

防火墙在使用上的要求有：

——防火墙要适合金融业网间互联的网络带宽要求，不能成为网络瓶颈，或明显影响网络工作效率；

——防火墙至少有 3 个网络接口，分别用于外联区，内部网络和中立区；

——内部网络和中立区之间的访问设置访问策略，只允许彼此之间需要访问的地址和端口；

——内部网络对外联区的访问采用网络地址转换，同时只开放需要访问的端口；

——外联网络对中立区的访问设置严格的端口和 IP 访问策略，对不提供外部服务的 IP 地址和端口严格禁止；

——禁止从外联区直接访问内部网络；

——设置日志记录，为落实安全管理，应形成日志检查和报警机制；

——选用的防火墙产品应符合国家标准 GB/T 18019－1999 和 GB/T 18020－1999。

7.3.2 部署要求

外联网络区边界防火墙系统的配置可根据其在网间互联中的地位和作用，有选择地采用单防火墙或者双防火墙。在采取双防火墙配置时，两个防火墙应采用不同类型、相同安全等级。同时按照纵深防御的思想，在外联网络区中对特别重要类互联业务前置系统区应增加部署部门级的防火墙。

7.3.3 功能要求

用于外联网络区边界防护的防火墙系统应具有以下功能：

——支持地址转换功能，支持静态地址转换、动态地址转换以及 IP 地址与 TCP/UDP 端口的转换；

——防火墙应该含有包过滤的功能；

——必须记录审计的信息，审计的信息应容易为管理人员所理解并及时发现问题；

——要求具有良好的人机交互管理界面，管理人员能够进行集中配置管理，能够根据安全策略的变化做出相应的修改；

——防火墙具有与其他安全产品（IDS、SCANNER）联动的功能，提供必需的接口；

——防火墙能有效的防止拒绝服务攻击，能够识别一些常用的攻击手段，如端口扫描等；

——防火墙具有认证机制，或者能够附接其他厂商的认证措施。

7.4 远程访问控制与接入认证

外联网络区应提供远程访问控制和接入认证服务。网络可信接入基于网络接入认证机制来实现，主要基于两种方式进行，一是基于用户口令方式；二是基于数字证书机制。

对拨号接入用户可以采用回拨方式或要求验证主叫认证，也可以基于数字证书进行强身份认证。对特别重要的系统和数据应采用数字证书机制。

对远程用户应提供基于访问控制列表或授权管理系统机制。对重要类以上的系统应提供授权管理机制。

互联区提供远程访问控制应遵循的标准：RADIUS协议。

7.5 通信加密

通信加密：

——可以使用 IPSec 技术；

——可以使用对称加密技术的加密设备。

7.6 入侵检测系统

7.6.1 使用要求

入侵检测系统在使用上要求：

——系统记录的日志需要最少保留 6 个月的历史记录；

——及时更新入侵检测系统的事件库和系统软件版本；

——安全负责人员每周至少检查一次系统报警事件，如发现攻击事件，及时处理；

——安全负责人员每月通过入侵检测系统生成一次事件报告，提交相关主管；

——采用硬件固化的网络入侵检测产品；

——使用获得国家有关认证部门认可的产品。

7.6.2 部署要求

在部署入侵检测系统时要求：

——各级外联网络的中立区内，根据实际情况逐步部署网络入侵检测系统；

——总部级和省级外联网络的中立区内的重要服务器配置主机入侵检测系统；

——入侵检测系统将检测的结果逐级汇总，形成分布分级管理的管理方式，保证对整个中立区的安全检测；

——对于普通的省级和地市级外联网络区，入侵检测系统配置在中立区局域网；

——各机构的总部级外联网络区，入侵检测系统除在中立区进行配置外，还需要在外联区配置。

7.6.3 功能要求

网间互联使用的入侵检测系统必须具备以下功能：

——缓冲区溢出攻击：应监控并发现缓冲区溢出类型的攻击；

——拒绝服务攻击：应监测到拒绝服务攻击并能继续正常工作；

——工具扫描:应监测到扫描行为；

——网络流量监视：应监视整个网络，或者某一特定的协议、地址、端口的报文流量和字节流量；

——后门程序检测：应监测后门活动；

——协议分析：除支持默认的网络协议集外，必须允许用户定义新的协议；

——防火墙联动：应能够根据网络状态，自动调整防火墙等设备的配置，与防火墙等设备进行联动；

——事件库自动升级：产品的事件数据库可以通过有效的方式得到更新，可以通过某种安全的方式下载最新的事件数据库；

——记录日志：对所有事件记录日志；

——分级、分布管理：入侵检测的管理系统可以做到分级管理，对系统的部署可以做到逐级分布，可和网间互联的分级方式一致。

7.7 漏洞扫描系统

7.7.1 使用要求

漏洞扫描系统在使用上要求：

——及时更新漏洞扫描系统的漏洞库和扫描器版本；
——安全负责人员通过漏洞扫描系统至少每月生成一次漏洞扫描报告，并提交相关主管；
——安全负责人员对扫描发现的漏洞应及时处理，不能处理的需要通知上级主管；
——使用获得国家有关认证部门认可的产品。

7.7.2 部署要求

在部署漏洞扫描系统时要求：
——各机构的总部级、省级和地市级外联网络区部署相应的漏洞扫描系统对本级中立区进行扫描；
——漏洞扫描报告逐级汇总，形成分布、分级的管理方式。

7.7.3 功能要求

网间互联使用的漏洞扫描系统必须具备以下功能：
——具有安全策略配置功能；
——Web 脆弱性扫描，扫描 Web 系统的各种已知脚本漏洞；
——FTP 脆弱性扫描，扫描 FTP 文件服务的各种已知漏洞；
——RPC 脆弱性扫描，扫描操作系统的 RPC 漏洞；
——NIS 脆弱性扫描，扫描 NIS 服务的各种已知漏洞；
——PROXY 扫描，可以发现 PROXY 服务；
——NT 用户、组、口令、注册表等脆弱性扫描，可以发现 Windows NT 和 Windows 2000 的注册表的漏洞；
——SNMP 脆弱性扫描，扫描发现 SNMP 服务的各种已知漏洞；
——木马扫描，可以发现主机被放置木马情况；
——浏览器漏洞扫描，可以发现浏览器的各种已知漏洞；
——Dos 服务扫描，可以发现系统存在的各种拒绝服务漏洞；
——操作系统范围，可以对多种操作系统进行漏洞扫描，包括：Windwos，LINUX，SCO Unix，AIX 等；
——网络设备扫描，可以对交换机和路由器进行漏洞扫描；
——邮件服务器脆弱性扫描，可以对邮件服务器进行漏洞扫描；
——口令脆弱性扫描，可以发现系统中的弱口令；
——端口扫描，可以发现操作系统打开的服务端口；
——生成报告，可以生成多种形式的报告，如按各种统计方式，并可以同时提供修补措施报告；
——更新方式，漏洞扫描系统的扫描漏洞库能够自动更新。

7.8 防病毒系统

7.8.1 使用要求

防病毒系统在使用上要求：
——选用的产品符合 GA 243—2000 的要求；
——建立严格的规章制度和操作规范，并定期检查各防范点的工作状态；
——使用国家有关认证部门认可的产品。

7.8.2 部署要求

在部署防病毒系统时要求：
——各级外联网络中立区内基于 Windows ，LINUX，SCO Unix，AIX 等多种类型操作系统的服务器，安装计算机病毒防护软件；
——各级外联网络中立区内电子函件服务器安装邮件服务器防病毒软件；
——各级外联网络中立区内 Windows 平台的工作站，要使用网络版防病毒软件；
——所有的防病毒软件可以集中管理，自动升级。

7.8.3 功能要求

网间互联使用的防病毒系统必须具备以下功能：

——网络防病毒：对通过网络传播的病毒可以有效查杀；

——病毒查杀能力：可以有效查杀邮件病毒，宏病毒，蠕虫，后门，Win32 等类型的病毒；

——集中管理能力：对分布在各服务器、工作站上的防病毒系统可以进行集中管理，维护；

——自动安装能力：对工作站、服务器等需要防病毒软件的系统可以自动安装；

——病毒库更新：对工作站、服务器等需要防病毒软件的系统可以自动统一地更新病毒库和程序；

——病毒查杀方式：邮件、网关防护、文件扫描、压缩文件扫描。

7.9 外联网络的安全审计

外联网络的安全审计可采用自动审计和人工审计两种方式。

采用自动审计时，应符合以下要求：

——外联网络区部署的审计系统应能够对外联网络中的设备和应用的各种日志，包括应用日志、操作系统日志、防火墙日志、入侵检测日志和防病毒系统日志等自动完成分析审计，并能根据查询条件可以快速地得到相关记录的结果；

——审计系统应能定期自动生成审计报告；

——审计工具的使用要进行访问控制；

——审计工具应和正在使用的系统分开；

——除非有额外的保护，审计工具不能放在用户使用区中。

采用人工审计时，应符合以下要求：

——进行人工审计要有管理层的同意；

——仔细计划如何对正在使用的系统放置检查点，把业务停顿的风险降到最低；

——检查应只限于对软件及数据的读取操作；

——只读以外的操作只能对系统文件的隔离副本进行，并且审计完成后应予以清除；

——其它特别或额外的处理要求应该被标识出来并获得管理层的同意；

——所有访问应受到监控并记录在日志上，以备参考；

——所有程序、要求及责任应清楚说明并文档化；

——进行安全审计后，要提供安全审计报告。

8 网间互联安全支撑设施

8.1 概述

网间互联安全支撑设施包括证书服务系统、密钥管理系统、密码服务系统、授权服务系统、可信时间服务系统等，其主要功能要求是：

——提供基于数字证书的信任服务，进行证书管理；

——提供基于统一安全管理的密钥服务，进行对称密钥和非对称密钥以及相关的服务管理；

——提供基于统一安全管理的密码服务；

——以信任服务为基础，为应用系统提供资源访问控制和授权管理服务，支持权限管理；

——基于世界协调时和公钥技术，为应用系统提供可信的时间戳服务。

8.2 证书服务系统

金融业星型网间互联为提供数据的安全性，对特别重要的应用系统应基于数字证书服务系统来保证安全。证书服务系统通过构建证书认证中心、证书审核注册中心等提供数字证书的生产服务，通过构建证书目录服务系统提供证书查询验证服务。

证书服务系统应对数字证书提供全过程管理服务，为金融业网间互联安全提供支撑性服务。

详细技术要求参见附录 A。

8.3 授权服务系统

金融业星型网间互联为提供数据的安全性，对特别重要应用系统应提供基于数字证书的授权服务。授权服务系统为应用系统提供资源授权管理及访问控制服务。授权服务系统应从两个方面提供服务：集中式授权基于相对固定的授权模型，通过在数字证书的扩展项增加用户的属性或权限信息，在服务器端提供授权管理；分布式授权则采用灵活的授权方式，通过在客户端根据用户的具体情况进行个性化定制和数字签名，由资源所有者自己分配资源的访问权限。

详细技术要求参见附录 A。

8.4 密钥管理系统

对关键数据及重要应用系统应提供对称密钥和非对称密钥的有效管理，并把数字证书的生产系统和密钥管理系统进行分离。

详细技术要求参见附录 A。

8.5 密码服务系统

对关键数据及重要应用系统应提供加解密、签名及签名验证等安全服务，以支持信息的保密性、完整性和抗抵赖性。其实现机制需通过密码服务系统从客户端和服务器端两个方面进行提供。密码服务系统应构建可信计算环境，进行安全密码算法处理，采用分布式计算技术，提供系统性能的动态可扩展，并采用安全中间件技术，向上层应用提供统一稳定的服务接口。

详细技术要求参见附录 A。

8.6 可信时间服务系统

对关键数据及重要应用系统应提供充分的抗抵赖服务，应基于可信时间服务系统提供可信时间戳服务。可信时间戳服务须从世界协调时获得全系统统一的时间，并基于证书服务系统和密码服务系统提供数字签名服务。

详细技术要求参见附录 A。

9 网间互联安全管理

9.1 安全管理模式

金融业星型网间互联安全实行统一规范、分级管理、各负其责的安全管理模式。

9.1.1 统一规范

参与金融业星型网间互联的机构按照本标准的要求规范各级互联区的安全建设和与互联有关的业务系统的开发与运行。

9.1.2 分级管理

金融业星型网间互联安全管理分为总部级、省级和地市级共三级。总部级应成立由参与网间互联的各机构联合组成的互联安全小组，负责互联安全标准和互联安全策略的制定、修订、解释。各级的安全管理应在参与网间互联的各机构的安全领导小组的领导下，应有专责人员负责。省级、地市级依据总部级制定的安全标准和安全策略结合本级具体情况制定、修改本级及其下级的网间安全实施细则。各级管理机构负责本级金融业星型网间互联业务的物理与环境安全、运行安全、信息安全、网络和人员管理，并接受上级机构的领导和督促并对下级机构提供支持和检查。

9.1.3 各负其责

参与网间互联的机构各自负责其所辖外联网络区的安全管理。

9.2 互联安全要求

参与网间互联的机构必须确定对方满足互联安全条件，并且以文档的形式记录“互联安全条件”以及双方的责任和义务。

9.2.1 互联安全条件

参与互联的机构要满足如下安全条件：

——外联网络应满足本标准第6章和第7章同等级的安全要求；

——应用系统应满足本标准第5章同等级的要求；

——按本标准安全管理部分的要求制定安全管理实施细则。

9.2.2 安全符合性检查

由网间互联安全小组负责对申请进行互联的机构进行安全审查，确定互联机构是否满足互联安全条件，对评测项目和结果以文档形式记录，形成审查报告，并且与接受审查的机构共同签字。

9.2.3 责任和义务

互联的机构相互审查对方的评测报告，确定是否与对方进行互联。若双方均同意进行互联，则应签署协议以确定双方在操作、维护、系统变更、紧急事件处理等方面的责任和义务。

9.3 安全管理制度

根据网间互联的安全管理模式，外联网络区具体的安全管理规章制度由参与网间互联的各机构负责制定。安全管理规章制度至少应包括：系统运行维护管理制度、计算机处理控制管理制度、设备档案资料管理制度、物理环境安全管理制度和互联环境工作人员安全管理制度等。

9.4 安全技术管理

安全技术的管理要求：

——安全支撑性基础设施由互联安全小组委托专责组织和人员统一管理；

——证书服务系统由国家有关主管部门认可CA统一制定安全策略、证书应用管理策略，并且进行统一管理，下级CA和RA由上级CA审核批准设立；

——密钥管理基础设施遵从密码管理主管部门和信息安全主管部门的有关规定；

——参与网间互联的机构应按照JR/T 0012—2004和本标准对外联网络安全的有关要求建立各级外联网络区，规范互联区的网络结构和使用的安全产品；

——所有前置系统应放置在相应级别的互联区进行集中管理。在总部级节点，应按互联业务的分类分区管理业务前置系统；

——技术文档资料管理，应用安全管理，外联网络区的安全管理由参与网间互联的各级机构依据总部级制定的安全标准和安全策略，结合本级具体情况制定实施细则。

9.5 安全运营管理

由互联安全管理小组负责制定具体的安全运营管理规范，监督、指导参与网间互联的各级机构依据总部级制定的安全标准和安全策略，实施风险评估管理、安全监控管理、应急响应和灾难恢复计划以及审计管理等。

10 网间互联人员与物理环境安全

参与网间互联的机构各自负责其所辖外联网络环境的人员与物理环境安全。应遵循的标准是：GB 4943—2001、GB 2887—2000和GB 50057—1994。可参照的标准是ISO/IEC 17799:2000。

11 网间互联运营安全

11.1 可用性和可靠性要求

各级外联网络运行环境的供电系统、报警系统、消防系统应具有连续运行可靠性。

各级外联网络环境网络设备运行可靠性要求：

——总部级和省级外联网络区的外联接口应有备份线路；

——应根据本标准关于设备安全的有关要求，选择通过安全认证的网络设备；

——应根据本级外联网络环境的具体情况，具备一定网络设备和通信线路冗余；

——应做好网络配置数据的备份，并保证备份数据可用；

——外联网络的主路由器和主交换机应具备双电源。

服务器运行可靠性要求：

——应根据本标准关于设备安全的有关要求，选择符合 GB4943—2001 的服务器设备；

——应根据本级互联环境的具体情况，具备一定服务器设备冗余；

——服务器要提供联机备份功能，要定期对操作系统和数据进行备份，并保证备份数据的完整性和正确性；

——重要服务器应具备双电源。

11.2 安全状态维护

为保障互联区域的安全，必须制定详细的日常操作手册，以及系统变更的标准规范和流程。如，负责互联区域的网络安全人员，每天都要对所有安全设备的日志进行审查，并记录发生的事件，定期和网络安全服务商进行联系，以取得最新的漏洞列表、安全事件库，病毒更新库等。定期和设备提供商和应用提供商取得联系，以取得设备或软件的最新安全补丁。可参照的标准是：ISO/IEC 17799:2000。

11.3 安全评估

所有网间互联应用系统和外联网络区应定期进行威胁评估和脆弱性评估并提供威胁和脆弱性评估报告。可参照的标准是：ISO/IEC 17799:2000。

11.4 事件处理

参与网间互联的机构各自负责处理其所辖外联网络区的安全事件。对于重大的安全事件，参照互联安全管理小组制定的安全运营管理规范，根据安全事件处理流程进行处理和上报。可参照的标准是：ISO/IEC 17799:2000。

附录 A
（资料性附录）
安全支撑性设施详细说明

A.1 证书服务系统

A.1.1 概述

证书服务系统通过构建证书认证中心、证书审核注册中心等提供数字证书的生产服务；通过构建证书目录服务系统提供证书查询认证服务。

金融业星型网间互联平台的信任服务体系的建设采用“集中式生产、分布式服务”的模式，即证书的生产（签发、发布、管理、撤销等）集中在CA进行，而证书认证则由大量分布式的证书目录服务系统（包括LDAP服务器和OCSP服务器）完成。

如图A.1所示为证书服务系统体系结构。

金融业星型网间互联的信任服务体系采用树状结构，以中国人民银行为核心，建立金融数字证书策略和管理中心，作为整个金融业网间互联信任服务体系最高管理机构和信任源点。

金融业星型网间互联依托一级CA，建立二级CA。

金融业星型网间互联总部级节点应直接使用CA来生产证书，各个参与互联的机构只需要建设RA中心及分布式的证书目录服务系统（LDAP服务器和OCSP服务器）即可。

对于确实因业务需要建设CA的机构，原则上应以一级CA为根建立二级CA，以便于业务的开展和互联互通。

证书服务系统是对数字证书进行全过程管理的安全系统。证书业务系统采用双证书（签名证书和加密证书）、双中心（证书认证中心和密钥管理中心）机制。

金融业星型网间互联证书目录服务系统采用“分布式服务”的模式来构建。所谓分布式服务是指：对应于一个CA，证书目录服务系统根据业务量、行政部门和地域的不同进行分布式部署。

建设证书目录服务系统，有三个基本原则：

——对应中国人民银行的一级 CA，在中国人民银行部署一个证书目录服务系统，为金融业应用系统提供证书认证服务；在自己不建设 CA，采用一级 CA 的各参与互联的机构，可部署一套与中国人民银行一样的证书目录服务系统来为金融业网间业务应用服务；

——对应省级节点的二级 CA，在省级节点部署一个证书目录服务系统为金融业网间互联业务应用提供证书认证服务；下级节点如果不建设 CA，直接应用省级节点的 CA，也须部署一套与该省级节点相应的证书目录服务系统；

——对应某一具体的证书目录服务系统，如果业务量相对较大，则有必要按地域或业务的不同，增设证书目录服务系统。

证书目录服务系统在密码服务系统的基础上，基于分布式计算技术进行构建，以支持系统灵活配置和性能动态按需扩展。其主要业务单元包括LDAP服务单元和OCSP服务单元。

LDAP服务单元基于LDAP协议，提供证书撤销列表的目录发布，主要针对非实时的证书状态查询应用或服务器端应用。

OCSP服务单元基于OCSP协议，提供证书状态的在线智能查询，主要针对实时证书状态查询应用或客户端应用。

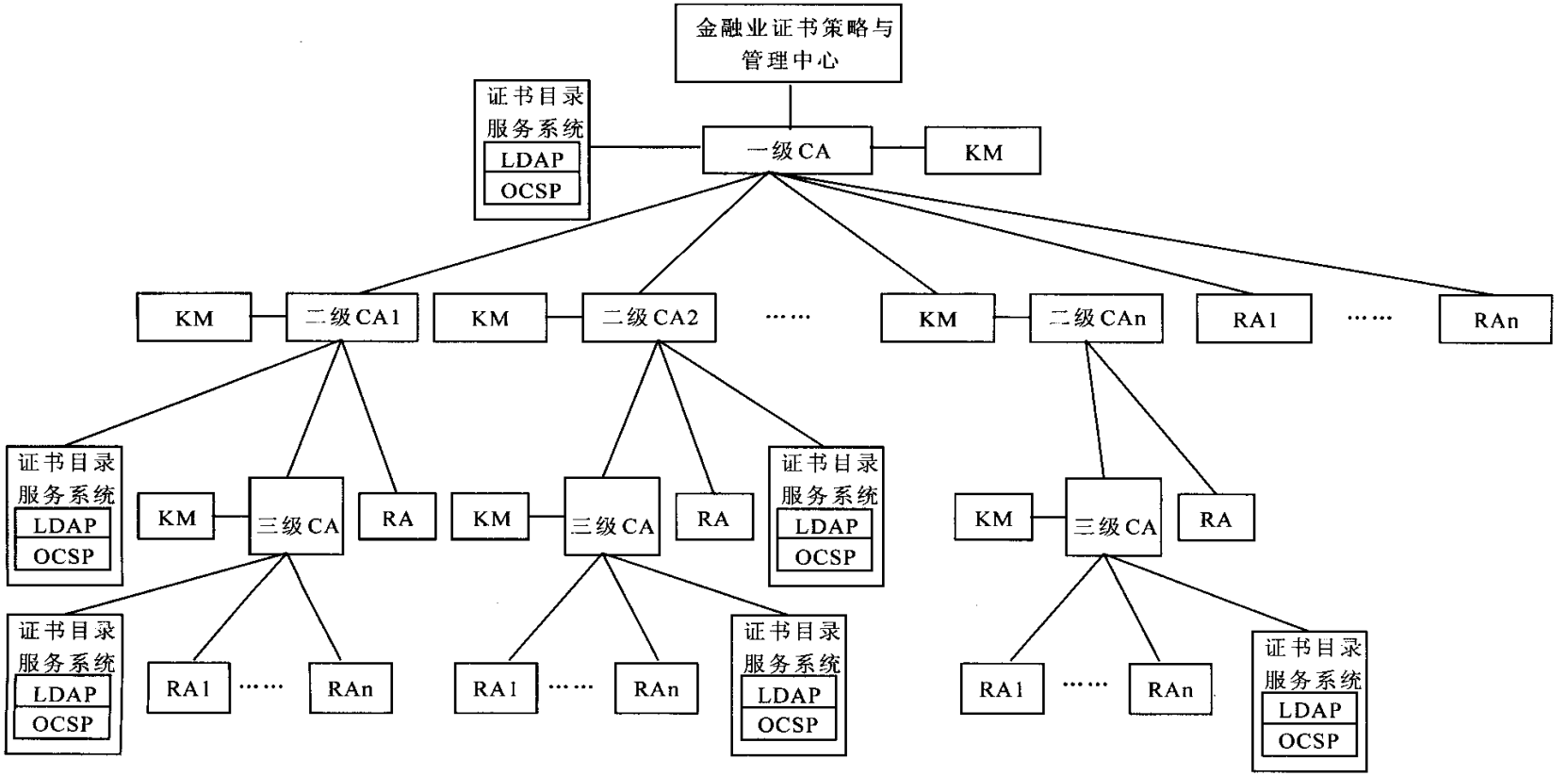


图 A1　金融业星型网间互联证书服务系统体系结构

A.1.2 功能要求

A.1.2.1 CA的功能要求

CA由Web服务器、策略服务器、CA业务服务器、证书管理服务器、证书签发服务器、密码服务系统以及信息安全防御系统等组成，提供数字证书签发、分发、撤销和管理等功能。CA应具有以下功能：

A.1.2.1.1 证书/证书撤销列表签发服务

采用国家密码主管部门审批的签名算法完成签名操作，提供各种数字证书及证书撤销列表的签发服务。

a) 证书类型

按使用对象，证书分为人员证书、设备证书、机构证书（包括银行和中介机构）三种类型。按功能，证书分为加密证书和签名证书。

b) 证书机制

数字证书采用双证书机制，每个用户拥有两张数字证书，一张用于数字签名，另外一张用于信息的加密。用于数字签名证书的密钥对由用户利用具有密码运算功能的证书载体产生；用于信息加密的数字证书的密钥对由密钥管理系统产生；签名证书和加密证书一起保存在用户的证书载体中。

c) 证书/证书撤销列表签发

根CA的数字证书/证书撤销列表由根CA自己签发；用户的数字证书/证书撤销列表由本系统的CA签发；下级CA的数字证书/证书撤销列表由上级CA签发；用于CA之间交叉认证的数字证书由CA互相签发。

证书/证书撤销列表的签发采用证书链机制。证书链的标志由相应的证书扩展项给出。

A.1.2.1.2 证书管理服务

主要是能够对系统中的各种数字证书、内部管理员证书、操作员证书及内部设备证书的有关操作进行管理。

A.1.2.1.3 证书撤销列表管理服务

证书撤销列表是在证书有效期之内，CA签发的终止使用证书的信息，分为用户证书列表和证书撤销列表两类。在证书的使用过程中，应用系统通过检查用户证书列表和证书撤销列表，获取有关证书的状态。

A.1.2.1.4 交叉认证服务

根据需要，系统应能提供各个金融业务证书认证机构之间的交叉认证服务。对属于不同结构的CA的用户，提供不同的交叉认证方式：

——层次结构 CA 的用户相互通信，按照证书链进行证书验证。

——非层次结构 CA 的用户相互通信，通过查找 CA 的信任列表进行证书验证。

——网状结构 CA 的用户相互通信，通过根 CA 为各方签发交叉证书或 CA 间双向交叉认证的证书进行证书验证。

A.1.2.2 RA的功能要求

RA由CA进行授权运作，由Web服务器、证书注册审核服务器、密码服务系统等组成。RA应具有以下功能：

a) 证书申请服务

证书申请应能支持采用在线或离线两种方式的证书申请：

- 在线方式：用户通过网络登录到注册系统申请证书；
- 离线方式：用户到指定的注册机构申请证书。

b) 身份审核服务

身份审核应能支持采用在线审核或离线审核进行身份审核：

- 在线审核：审核人员通过注册系统，连接相关权威机构的应用系统，对证书申请者进行在线身份审核。

c) 证书下载服务

证书下载应能支持可采用在线和离线两种方式的证书下载。

d) 证书管理服务

- 提供证书认证策略及操作策略的管理；
- 对自身证书进行安全管理；
- 对内部管理员数字证书、操作员数字证书进行统一管理；
- 支持个别处理和批处理方式发放数字证书。

A.1.2.3 证书目录服务系统的功能要求

证书目录服务系统应具有以下功能：

金融业星型网间互联平台证书目录服务系统采用“分布式服务”的模式来构建。所谓分布式服务是指：对应于一个CA，证书目录服务系统根据业务量、行政部门和地域的不同进行分布式部署。

建设证书目录服务系统，有三个基本原则：

——对应中国人民银行的一级 CA，在中国人民银行部署一个证书目录服务系统，为金融业应用系统提供证书认证服务；在自己不建设 CA，采用一级 CA 的各个商业银行，须部署一套与中国人民银行一样的证书目录服务系统来为金融业网间业务应用服务；

——对应省级节点的金融业务 CA，在省级节点部署一个证书目录服务系统为金融业网间互联业务应用提供证书认证服务；下级节点如果不建设 CA，直接应用省级节点的 CA，也须部署一套与该省级节点的证书目录服务系统；

——对应某一具体的证书目录服务系统，如果业务量相对较大，则有必要按地域或业务的不同，增设证书目录服务系统。

证书目录服务系统在密码服务系统的基础上，基于分布式计算技术进行构建，以支持系统灵活配置和性能动态按需扩展。其主要业务单元包括LDAP服务单元和OCSP服务单元。

LDAP服务单元基于LDAP协议，提供证书撤销列表的目录发布，主要针对非实时的证书状态查询应用或服务器端应用。

OCSP服务单元基于OCSP协议，提供证书状态的在线智能查询，主要针对实时证书状态查询应用或客户端应用。

a) 基于 LDAP 协议的证书目录管理与证书查询服务；

b) 基于 OCSP 技术的证书在线状态查询服务。

A.1.3 安全策略

CA和KM中心分开建设，符合国家安全审查要求；

CA和KM中心通信采用专用协议。

A.1.4 技术指标

CA、RA和证书目录服务系统的处理性能如证书签发性能、证书管理性能等应具备可伸缩配置及动态平滑扩展能力。业务量小时通过配置系统基本框架和相应服务单元以具备良好的性价比，业务量大时通过平滑增配相应的服务单元，以适应业务的发展。

A.1.5 接口要求

通过OCSP、LDAP协议提供证书验证服务；

通过XML格式来验证签名/验证，加密/解密文档和文件。

提供Java和C的API。

A.1.6 配置要求

根据金融业星型网间互联业务实际情况，配置环境应满足基本的业务需要，应采取集群方式，提供负载均衡，以满足一定并发服务数，同时，提供一定的冗余配置。

A.1.7 应遵循的标准

GB 15851—1995 信息技术 安全技术 带消息恢复的数字签名方案

GB 15852—1995 信息技术 安全技术 用块加密算法作校验函数的数据完整性机制

GB/T 15843.1—1999 信息技术 安全技术 实体鉴别 第1部分：概述
GB/T 15843.2—1997 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制
GB/T 15843.3—1998 信息技术 安全技术 实体鉴别 第3部分：用非对称签名技术的机制
GB/T 15843.4—1999 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制
GB/T 17902.1—1999 信息技术 安全技术 带附录的数字签名 第1部分：概述
GB/T 17903.2—1999 信息技术 安全技术 抗抵赖 第2部分：使用对称技术的机制
GB/T 17903.3—1999 信息技术 安全技术 抗抵赖 第3部分：使用非对称技术的机制
RFC 2044—1996 UTF-8,字符编码和ISO10646
RFC 2247—1998 使用域名作为LDAP（和X.500）的标识名
RFC 2252—1997 轻量级目录存取协议 第3版：属性语法定义
RFC 2459—1999 Internet X.509 公钥基础设施：证书和CRL简介
ITU-TX.509v3 信息技术——开放系统互连——目录：公钥和属性鉴别框架

A.2 授权服务系统

A.2.1 概述

授权服务系统在证书服务系统基础上，为应用提供资源的授权管理及访问控制服务。授权服务系统应提供两种工作模式：集中式授权服务与分布式授权服务。

集中式授权服务系统基于相对固定的授权模型，提供集中式管理，通过在数字证书的扩展项增加用户的属性或权限信息，在服务器端提供授权管理。

分布授权服务系统采用灵活的授权方式，提供分布式管理服务，通过在客户端根据用户的具体情况进行个性化定制，灵活地设置有效授权信息，由资源所有者自己分配资源的访问权限，并通过数字证书机制加以数字签名，具有抗抵赖性。

A.2.2 功能要求

A.2.2.1 集中式授权服务的功能要求

集中式授权服务能够：

——提供管理用户信息功能，包括用户注册、用户信息修改、用户注销；

——完成用户授权申请的审核功能；

——制定资源访问控制列表，根据实际的应用，把资源和用户角色关联起来，标识用户角色对资源的访问权限；

——提供角色的制定、编辑、更新。根据具体应用实际，制定出恰当的角色信息，以便和用户的实际身份相映射等服务。

A.2.2.2 分布式授权服务的功能要求

能够根据用户的资源授权信息等数据制定访问授权列表,并完成用户对列表的签名。

提供进行与授权有关的管理功能，如完成对用户制定的授权信息列表修改。

A.2.3 安全策略

基于证书服务系统提供有效授权；

通过在服务器端提供固定授权服务，在客户端提供灵活授权服务；

通过固定授权方式和灵活授权提供全方位的授权模式。

A.2.4 技术指标

授权管理服务系统应根据实际需要满足基本的授权服务并发数,处理性能应能根据业务量的发展动态平滑可扩展。

A.2.5 接口要求

支持X.509v4相关协议。

A.2.6 配置要求

根据金融互联业务实际情况，配置环境应满足基本的业务需要，应采取集群方式，提供负载均衡，以满足一定并发服务数，同时，提供一定的冗余配置。

A.2.7 应遵循的标准

RFC 2044—1996 UTF-8,字符编码和 ISO10646

RFC 2247—1998 使用域名作为 LDAP（和 X.500）的标识名

RFC 2252—1997 轻量级目录存取协议 第3版：属性语法定义

RFC 2459—1999 Internet X.509 公钥基础设施：证书和 CRL 简介

A.3 密钥管理系统

A.3.1 概述

密钥管理系统提供加密密钥的产生、存储、认证、分发、查询、撤销、归档及恢复等管理服务。密钥管理中心与证书认证中心按照“统一规划、同步建设、独立设置、分别管理、有机结合”的原则进行建设和管理。密钥管理中心由密钥生成、密钥管理、数据库管理、密码服务、密钥恢复、系统审计等部分组成。

A.3.2 功能要求

密钥管理系统应具有以下功能：

——密钥管理策略的制订与本系统的安全维护；

——密钥的生成：通过专用密码设备生成所需密钥，包括生成非对称密钥对和对称密钥；

——密钥的发送：采用安全协议通过 CA，把密钥对传送给用户。用户包括 CA、下级 KMC、特定用户群或设备；

——密钥的存储：密钥管理中心的各类密钥均需安全加密存储；

——密钥库管理：密钥管理中心配置的各个密钥库要安全加密管理；

——密钥的查询：个人查询，向密钥管理中心访问查询；法律凭证查询，直接到密钥管理中心查询；

——密钥的撤销：密钥撤销通过 RA-CA，访问密钥管理中心实施；

——密钥的恢复：个人要求密钥恢复，通过 RA-CA，访问密钥管理中心进行密钥恢复；法律凭证要求密钥恢复，直接到密钥管理中心实施；

——密钥管理中心的运行管理：包括密钥管理中心的审计、认证、恢复、统计等系统管理；

——密钥管理中心的安全管理：包括密钥管理中心的系统、设备、数据、人员等安全管理。

A.3.3 安全策略

密钥管理中心和CA分开进行建设。

密钥管理中心与CA之间采用基于身份认证的安全通信协议。

A.3.4 技术指标

密钥管理中心应根据实际需要满足基本的业务受理点连接数、签发在用证书数目、密钥保存期、密钥发放并发请求数。密钥管理中心应具备系统所需的最大量的密钥生成、存储、传送、发布、归档等密钥管理功能；能支持密钥5年保存期的要求；

密钥管理中心的处理性能如密钥生成性能、密钥发放性能等应具备可伸缩配置及动态平滑扩展能力，业务量小时，通过配置系统基本框架和相应的服务系统和相应的服务单元以具备良好的性能价格比，业务量大时通过平滑增配相应的服务单元，以适应业务的发展。

A.3.5 配置要求

根据金融互联业务实际情况，配置环境应满足基本的业务需要，应采取集群方式，提供负载均衡，以满足一定并发服务数，同时，提供一定的冗余配置。

A.3.6 应遵循的标准

GB/T 17903.2—1999 信息技术 安全技术 抗抵赖

A.4 密码服务系统

A.4.1 概述

密码服务系统主要提供包括加解密、签名及签名验证、数字信封等安全服务，以支持信息的保密性、完整性和抗抵赖性。在金融业星型网间互联平台中，密码服务从客户端和服务器端两个方面进行提供。所有密码算法都必须经国家密码主管部门批准。

密码服务系统要构建一个相对独立的可信计算环境，进行安全密码算法处理；要采用分布式计算技术，提供系统性能的动态可扩展；应采用安全中间件技术，兼容各种密码设备，向上层应用提供统一稳定的服务接口。

A.4.2 功能要求

密码服务系统应具有如下功能：

a）提供基础加解密服务，包括：

1） 数据加解密运算：提供对数据的加密和解密等运算功能。

2） 数字签名运算：提供对数据的签名和签名验证等运算功能。

3） 数字证书运算：提供数字证书签发和验证等基本的证书运算服务功能。

4） 数字信封：提供对数据的数字信封封装和解封装等运算功能。

5） 数据摘要和完整性验证：提供对数据进行摘要运算功能，并具有验证数据完整性功能。

6） 会话密钥生成和存储。

b） 提供统一的安全接口

利用安全中间件技术对底层的加密算法进行对象化抽象，为应用提供统一安全服务APIs。

c） 提供对多密码算法的支持，

用户根据国家密码主管部门的要求可以灵活地选择并配置合适的密码算法。

d） 采用分布式计算技术，随着业务量的逐渐增加，灵活地增加密码服务模块，实现性能动态按需平滑扩展，且不影响上层的应用系统。

密码运算须在密码硬件内运行，密钥不以明文形式暴露在系统外。

A.4.3 安全策略

密码服务系统整体构成一个可信环境；

密码运算在密码硬件内运行，密钥不以明文形式暴露在系统外；

密码算法采用国家密码主管部门批准的密码算法、密码设备和相关的安全载体、算法。

A.4.4 技术指标

——RSA 算法密钥长度：1024－2048bits

——ECC 算法密钥长度：192bits

密码服务系统的处理性能如公钥密码算法签名、验证、对称算法加解密性能等应具备可伸缩配置及动态平滑扩展能力。业务量小时通过配置系统基本框架和相应服务单元以具备良好的性能价格比，业务量大时通过平滑增配相应的服务单元，以适应业务的发展。

A.4.5 接口要求

密码函数接口采用国家密码主管部门批准认可的统一标准接口；

对互联业务系统提供 C/C++/C#和Java 应用编程接口。

A.4.6 配置要求

根据金融互联业务实际情况，配置环境应满足基本的业务需要，应采取集群方式，提供负载均衡，以满足一定并发服务数，同时，提供一定的冗余配置。

A.4.7 应遵循的标准

GB 15851－1995 信息技术 安全技术 带消息恢复的数字签名方案

GB 15852－1995 信息技术 安全技术 用块加密算法作校验函数的数据完整性机制

GB/T 15843.1—1999 信息技术 安全技术 实体鉴别 第1部分：概述
GB/T 15843.2—1997 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制
GB/T 15843.3—1998 信息技术 安全技术 实体鉴别 第3部分：用非对称签名技术的机制
GB/T 15843.4—1999 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

A.5 可信时间服务系统

A.5.1 概述

可信时间服务系统基于世界协调时和公钥技术，为金融业星型网间互联系统提供精确可信的时间戳，保证处理数据在某一时间（之前）的存在性及相关操作的相对时间顺序，为业务处理的抵赖性和可审计性提供有效支持。

可信时间服务系统必须从世界协调时获得全系统统一的时间，即从国家权威时间源获取权威的时间。

A.5.2 功能要求

——从可信时间源获取时间，校准时间戳服务器的时间；
——安全保存时间戳及相关信息，确保数据的可审计性，实现系统数据处理的抗抵赖性；
——签发可信的时间戳。

A.5.3 安全策略

从国家权威时间源采时，保证时间的同一性；
通过密码服务系统，提供时间戳的可信。

A.5.4 技术指标

——时间精度 10^{-1} 秒；
——时间戳的签发服务应根据实际情况，满足基本的时间戳并发请求，并可动态平滑扩展相应服务单元，以适应业务量的发展。

A.5.5 接口配置要求

可信时间服务系统应为应用系统提供C/C++/C#和Java 应用编程接口。

A.5.6 部署配置

根据金融互联业务实际情况，配置环境应满足基本的业务需要，应采取集群方式，提供负载均衡，以满足一定并发服务数，同时，提供一定的冗余配置。

A.5.7 应遵循的标准

RFC 3161 时间戳协议