

劳动保障机构授信证颁发与管理体的研究

汪 治,陈丽霞,沈 俊,郭丽芳

(上海普华诚信信息技术有限公司,上海 201112)

摘 要:根据我国目前社会劳动保障公共服务中存在的问题,对劳动保障机构授信证颁发与管理体进行了研究。分析了劳动保障机构授信证技术,对劳动保障机构授信证颁发与管理体中的授信证发放系统和授信证服务系统进行了详细研究,并规划了劳动保障机构授信证技术应用场景。劳动保障机构授信证颁发与管理体的研究,解决了劳动保障公共服务业务代理机构和中介机构的信任问题,为建立良好的劳动保障公共服务环境做出了积极贡献。

关键词:劳动保障机构;授信证;授信证颁发与管理体;授信证应用

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2011)11-0239-04

Research of Credit Certificate Issue and Management System of Labor Security Organs

WANG Zhi, CHEN Li-xia, SHEN Jun, GUO Li-fang

(Shanghai Puhua Trust Information Technology Co., Ltd., Shanghai 201112, China)

Abstract: A detailed research and design of the issuance of the credit certificate issue and management system of labor security organs is given on the base of labor security public service existing problems in our country. An analysis on credit certificate technology of labor security organs is made. Then the credit certificate issue system and the credit certificate service system of the credit certificate issue and management system of labor security organs was studied in detail. And the application scene of credit certificate technology is planned. The research and design of credit certificate issue and management system of labor security organs solved the confidence question in public services that provided by labor security agency and intermediary agency, and contributed tremendously to create a favorable environment of public services of labor security organs.

Key words: labor security organs; credit certificate; credit certificate issue and management system; application of credit certificate

0 引 言

我国劳动保障公共服务过程中涉及到较多的业务代理机构和中介机构,由于缺乏对业务代理机构和中介机构行之有效的信任管理,在开展劳动保障公共服务时,存在一定的虚假信息、“不法中介”等信任问题。因此,如何有效管理和规范各类业务代理机构和中介机构已成为目前社会劳动保障公共服务亟待解决的一大问题。

针对我国目前现代社会保障业存在的这种问题,需要建立完善、安全、诚信,符合我国国情的劳动保障公共服务网络环境。文中提出了一种解决方法:为劳动保障公共服务业务代理机构和中介机构发放机构电子许可证照——机构授信证,作为机构用户进行业务代理和中介服务的授权和信任证明。

由于网络中存在一系列的安全隐患,人力资源和社会保障部门在为机构发放机构授信证的时候,还要考虑到机构授信证的真实性和安全性,必须保证机构授信证确实为该业务代理机构或中介机构所有,这就要求将密码技术应用到机构授信证发放系统中,以保证业务代理机构和中介机构身份与机构授信证相对应^[1-3]。

将授信证引入到劳动保障公共服务中,可以加强业务代理机构和中介机构的诚信管理,为建立良好的劳动保障公共服务环境奠定基础,进而推动劳动保障公共服务业的健康快速发展。

1 相关技术研究

劳动保障机构授信证技术是一种基于 PKI 体系,由劳动保障业务经办机构结合本机构及业务代理机构的数字证书,为业务代理机构发放电子许可证照的机构授信证技术^[4]。

PKI (Public Key Infrastructure) 即“公钥基础设施

收稿日期:2011-04-14;修回日期:2011-07-21

基金项目:国家科技支撑计划项目(2008BAH32B04)

作者简介:汪 治(1978-),男,上海人,工程师,研究方向为电子政务信息安全领域的研究。

施”,是一种遵循既定标准的密钥管理平台,是一种基于公开密钥理论和技术来实施和提供安全服务的具有普适性的安全基础设施,提供公钥加密和数字签名服务,劳动保障机构授信证颁发与管理体系采用 PKI 体系结构的目的是为了管理密钥和劳动保障机构授信证,保证网上数字信息传输的机密性、真实性、完整性和不可否认性^[5,6]。

PKI 的灵魂来源于公钥密码技术,优势表现在:

(1)采用公开密钥技术,PKI 能够支持可公开验证并无法仿冒的数字签名。

(2)采用密码技术,PKI 不仅能够为相互认识的实体之间提供机密性服务,同时也可以为陌生用户之间的通信提供保密支持。

(3)PKI 提供营业执照电子副本的撤销机制,提供了在意外情况下的补救措施,可以让用户更加放心,不用担心被窃后身份或角色被永远作废或被他人恶意盗用。

(4)PKI 具有极强的互联能力。不论是上下级的领导关系,还是平等的第三方信任关系,PKI 都能够按照人类世界的信任方式进行多种形式的互联互通,从而使 PKI 能够很好地服务于符合人类习惯的大型网络信息系统。

作为提供信息安全服务的公共基础设施,PKI 是目前公认的保障网络安全的最佳体系。PKI 的基础技术包括加密、数字签名、数据完整性机制、数字信封等。其核心是解决信息网络空间中的信任问题,确定信息网络、信息空间中各种经济、军事、和管理行为主体(包括组织和个人)身份的唯一性、真实性和合法性,是解决网上身份认证、信息完整性和抗抵赖等安全问题的技术保障体系。它能够对所有网络应用提供加密和数字签名等密码服务及所必需的密钥,为劳动保障机构授信证应用开发奠定了基础^[7-9]。

2 劳动保障机构授信证颁发与管理研究

劳动保障机构授信证是机构用户数字证书结合机构用户信任信息为一体的身份标识,既代表了机构用户在网络上的身份,也标识了该机构用户是某一个业务经办机构认可的提供某类劳动保障公共服务业务的机构用户。作为机构用户进行业务代理和中介服务的授权和信任证明,在各类劳动保障公共服务中引入授信证,可以有效加强业务代理机构和中介机构的诚信管理。

劳动保障机构授信证颁发与管理体系基于 PKI 密码技术,提供劳动保障机构授信证的颁发、管理、授信证查询和授权等服务。从结构上分,劳动保障机构授信证颁发与管理体系主要包括机构授信证发放系统和

机构授信证服务系统两部分,其架构如图 1 所示。

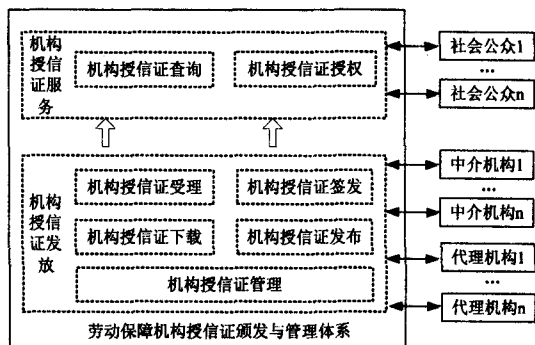


图 1 劳动保障机构授信证颁发与管理体系架构

其中,机构授信证发放系统提供授信证的受理、签发、下载、发布和管理等服务;机构授信证服务包括授信证查询和授权服务。机构授信证查询服务为用户提供任意机构的机构授信证公开信息查询服务;机构授信证授权服务为机构用户提供查询本机构授信证授权信息的授权功能,只有经过机构用户授权后方可查询该机构用户授信证的授权信息。

2.1 劳动保障机构授信证发放系统

劳动保障机构授信证发放系统由授信证/授信证注销列表(CCRL, credit certificate revocation list)生成与签发、安全管理、安全审计、数据库、目录服务以及密码设备构成,具体结构如图 2 所示。

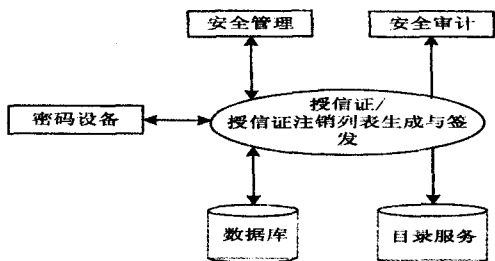


图 2 机构授信证发放系统结构图

劳动保障机构授信证发放系统处理机构授信证签发请求,根据授信证的签发请求,选择适当的授信证模板(授信证模板由安全管理模块进行管理),签发机构授信证,然后将签发完成的授信证发布到目录服务器中。此外,为保证劳动保障机构授信证发放系统内部通信及其与劳动保障机构授信证服务系统通信的安全性,由密码设备提供密码支持,如加解密、签名及签名验证、数字信封服务、产生随机数和对数据进行数字摘要等多种密码服务。

劳动保障机构授信证发放系统提供如下功能:

(1)授信证签发。

机构用户要获得劳动保障机构授信证可以向上级劳动保障业务经办机构提出申请,劳动保障机构授信证的申请方式有两种:

①机构用户通过劳动保障机构授信证颁发与管理体系直接申请。

②机构用户通过劳动保障业务专网提交授信证申请。

根据申请请求生成劳动保障机构授信证,将签发完成的授信证发布到目录服务器中。

(2)授信证注销列表签发。

机构用户接收注销信息后,签发授信证注销列表,再将签发后的授信证注销列表发布到目录服务器中。

(3)授信证变更。

劳动保障机构授信证的变更由机构用户提出申请,授信证签发模块接收到变更申请后,首先将旧的授信证注销,然后重新签发新的授信证,再将新的授信证传递给机构用户并发布到劳动保障机构授信证目录服务器上。

(4)授信证撤销。

授信证的撤销有两种情况:

①授信证的有效期已到,认证中心自动将过期的授信证撤销。

②由于机构用户的私钥泄密、丢失或是忘记保护私钥的口令等原因,造成用户授信证的撤销。

第二种情况下,用户需要向认证中心提出授信证撤销的请求,认证中心根据机构用户的请求确定是否将该授信证撤销。

证书撤销的实现方法有很多种,其中一种就是定期发布授信证撤销列表。

2.2 劳动保障机构授信证服务系统

劳动保障机构授信证服务系统由状态管理、接口服务、数据库、查询服务、授权管理、安全管理及安全审计构成,其具体结构如图 3 所示。

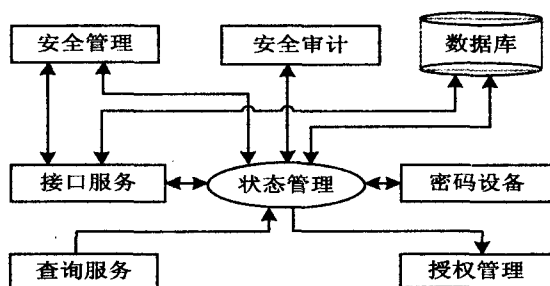


图 3 劳动保障机构授信证服务系统结构图

劳动保障机构授信证服务系统主要提供劳动保障机构授信证状态查询及授信证信息查询服务。只有持有有效的劳动保障机构授信证的最终用户才能使用查询的功能。

劳动保障机构授信证发放系统中的目录服务器与劳动保障机构授信证服务系统查询服务器之间采用主从结构的目录服务技术^[10],通过状态管理模块将签发的劳动保障机构授信证信息、授信证注销、撤销、撤销恢复等信息映射到授信证查询模块中;再通过调用接

口服务为授信证应用系统提供劳动保障机构授信证查询服务,接收应用系统的授信证查询请求,根据请求信息的劳动保障机构授信证编号从数据库中查询劳动保障机构授信证,将查询结果签名后返回给请求者。劳动保障机构授信证信息、授信证注册、撤销、撤销恢复等信息存储在数据库中。密码模块为劳动保障机构授信证服务提供加解密、签名及签名验证、数字信封服务、产生随机数和对数据进行数字摘要等多种密码服务。

授信证的合法性和有效性,是使用机构授信证的前提。因此,基于授信证的应用在使用之前,需要对授信证的合法性和有效性进行查询,验证劳动保障业务代理机构和中介机构是否持有合法有效的授信证,只有授信证合法有效,劳动保障机构才能提供相关的劳动公共保障服务。

劳动保障机构授信证服务系统提供如下功能:

(1)授信证查询。

劳动保障机构授信证查询包括劳动保障机构授信证状态查询和授信证信息查询两类。劳动保障机构授信证查询服务有以下三种形式:

①授信证注销列表查询。通过标识的授信证注销列表的地址,将授信证注销列表下载到本地,从而查询劳动保障机构授信证状态。

②状态查询。实时查询劳动保障机构授信证的状态,查询的结果经过签名后返回给请求者,从而获取劳动保障机构授信证的状态。

③信息查询。在权限范围内,用户可以查询到其他劳动保障机构的授信证的信息。

(2)授信证授权。

机构授信证授权服务为机构用户提供查询本机构授信证授权信息的授权功能,只有经过机构用户授权,最终用户方可查询该机构用户授信证的授权信息^[11,12]。

授权方式有两种:一种是最终用户已经提交授权申请,机构用户对授权申请进行审批;第二种是机构用户直接授权给一个具体的最终用户或所有的最终用户查询权限。

3 劳动保障机构授信证应用场景

劳动保障机构授信证颁发与管理体系的研究为其他劳动保障业务系统、劳动保障机构用户或中介机构开展网上亮证、网上变更、网上撤销等网上服务提供了技术基础,其应用如图 4 所示。

基于劳动保障机构授信证颁发与管理体系的研究,在服务网(内部)部署劳动保障机构授信证发放系统,提供授信证/授信证注销列表的签发、授信证变更、

授信证撤销服务;在服务网(外部)部署劳动保障机构授信证服务系统,提供授信证发布、授信证状态查询、授信证信息查询服务^[13]。为保障系统安全性,在劳动保障机构授信证服务系统中部署加密服务器,以提供加解密、签名及签名验证、数字信封服务、产生随机数和对数据进行数字摘要等多种必要的密码服务。

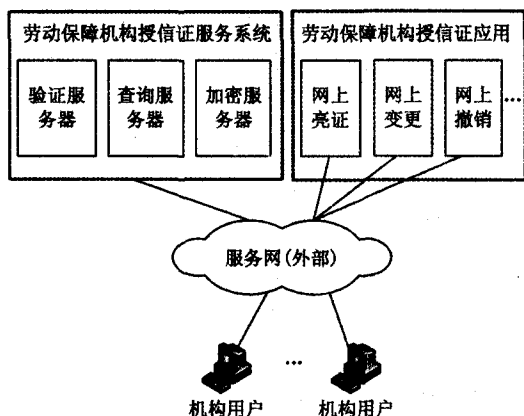


图4 劳动保障机构授信证应用场景

4 结束语

劳动保障机构授信证颁发与管理体的研究,加强了劳动保障业务代理机构和中介机构的诚信管理,解决了劳动保障公共服务中的虚假信息、“不法中介”等信任问题,对促进我国劳动保障公共服务的业务代理和中介服务市场的规范化发展,营造完善、安全、诚信、符合我国国情的劳动保障公共服务网络环境,进一步加强劳动保障业务代理机构和中介机构的 service 水平和能力做出了积极贡献。

参考文献:

[1] 姜 岚,王宏滨. PKI/CA 技术在电子政务中的应用[J]. 黑

(上接第 238 页)

相应的授权和 WPKI 技术来进一步保证移动电子商务交易过程的安全性。

参考文献:

- [1] Tarasewich P. Designing Mobile Commerce Application[J]. Communication of the ACM, 2003,46(12):57-60.
- [2] 陈 轶,邓世荣,刘 云. 基于 J2ME 平台的电影票预订系统的设计与实现[J]. 计算机与现代化,2009(7):133-135.
- [3] 丁丽梅. 关于移动电子商务安全的研究[J]. 电脑知识与技术,2008(2):966-967.
- [4] 代文锋,王玉珍. 我国移动电子商务现状与问题研究[J]. 办公自动化,2008(6):23-24.
- [5] 李必云,石俊萍. 基于 WPKI 的移动电子商务研究[J]. 计算机与现代化,2010,175(3):49-51.

龙江科技信息,2010(12):69-69.

- [2] 邓晓军. PKI 技术及其应用的分析[J]. 计算机技术与发展,2008,18(6):144-147.
- [3] 冉 艳,胡学钢. 构建市级电子政务安全平台[J]. 计算机技术与发展,2007,17(8):144-147.
- [4] 中华人民共和国国务院令 第 423 号. 劳动保障监察条例[S]. 2004.
- [5] 杨 宇. 基于 PKI 身份认证系统的研究与实现[D]. 成都:电子科技大学,2009.
- [6] 宁红宙,华 刚,金端峰. 公钥基础设施(PKI)应用中的信任问题与安全解决方案[J]. 中国安全科学学报,2007,17(10):140-144.
- [7] Shi Yanrong, Sun Danning, He Yongqiang, et al. Research and Implementation of Enterprise CA System Based on PKI[C]//International Conference on Management of e-Commerce and e-Government (ICMECG). [s.l.]:[s.n.], 2008.
- [8] Wu Jingjing, Jing Jiwei, Lin Jingqiang, et al. A Decentralized Certification Authority Based on Real World Trust Relationships[C]//International Conference on Computer Science and Software Engineering (CSSE). [s.l.]:[s.n.], 2008.
- [9] Liyo A, Marian M, Moltchanova N, et al. PKI past, present and future[J]. International Journal of Information Security, 2006,5(1):18-29.
- [10] 欧阳宏基,葛 萌,赵 蕾. 基于 JDBC 与设计模式的数据库连接池实现方法[J]. 计算机技术与发展,2011,21(1):84-87.
- [11] 孙翠翠,张永胜. 一种改进的基于角色的授权委托模型[J]. 计算机技术与发展,2010,20(11):154-157.
- [12] 黄 勤,高东群,刘益良. 工作流系统中基于任务状态的转授权模型[J]. 计算机技术与发展,2011,21(2):34-38.
- [13] 中华人民共和国人力资源和社会保障部信息中心. 人力资源和社会保障电子认证体系第 2 部分:电子认证系统技术规范[S]. 2009.

[6] 彭 博. 浅谈移动电子商务的信息安全[J]. 农业与技术,2008(6):172-174.

[7] Tang Jian, Terziyan V, Veijalainen J. Distributed PIN Verification Scheme for Improving Security of Mobile Devices[J]. Mobile Networks and Applications, 2003(8):159-175.

[8] 邓 娟,蒋 磊. 3G 网络时代移动电子商务安全浅析[J]. 电脑知识与技术,2009(2):1314-1315.

[9] 吴 章. WAP 协议的安全策略在移动电子商务中的应用[J]. 现代商业,2010(4):189-190.

[10] 范荣真. 基于 WAP2.0 的移动安全支付协议[J]. 技术研究,2010(2):47-48.

[11] 吕福春,陈特放. 基于 WAP 的移动电子商务安全研究[J]. 福建电脑,2008(12):15-16.

[12] 傅杰勇. 我国移动电子商务应用安全问题探析[J]. 中国集体经济,2008(5):65-66.