DOI: 10.13657/j.cnki.gxkxyxb.2005.s1.023

基于 PKI的网上社会保险业务平台设计

Design of Business Platform for Social Security Based on PKI

兰 剑

Lan Jian

(广西数字证书认证中心有限公司,广西南宁 530022)

(Gangxi Certificate Authority Center Ltd., Nanning, Guangxi, 530022, China)

摘要: 基于 PKI(Public Key Infratructure)技术,采用身份认证和访问控制安全策略,设计了一个社会保险业务平台,该平台综合业务系统由系统终端用户和 Web服务器构成,平台的安全结构由证书解析模块、签名及证书验证模块、个人信任代理模块组成,平台具有相关机密文件下载、申报数据上传、网上审核和不可抵赖功能.

关键词: 社会保险 平台 PKI 数字证书 加密 签名

中图法分类号: TP393.092 文献标识码: A 文章编号: 1002-7378(2005)S0-0068-03

Abstract According to PKI, with the certificate authority and access control, an on-line social insurance infrastructure was founded. This infrastructure system consists of its terminal users and web server, and also its security construction includes four modules: certification analysis, signature, certification identification and personal belief. The functions of top secret document download, accessible data upload, online verification and non-repudiation have also been added to this infrastructure.

Key words social insurance, platform, PKI, digital certificate, encryption, signature

社会保险业务平台是指社会保险部门建立专门的网上综合业务平台。各办事单位通过 Internet访问该网站上的综合业务平台,使用分配好的用户名和密码登录,进行相应的业务操作。目前国内已有二三十个省市地区社会保险所开展网上社会保险业务,东莞市社会保险所、深圳市社会保险所、广东省社会保险所、北京市社会保险所、福建省社会保险所开始使用数字证书。由于综合业务平台基于 Internet,综合业务平台应用中不可避免地存在着由于 Internet自由、开放所带来的信息安全隐患,而且综合业务涉及很多敏感的数据,不仅需要保密,更需要抗抵赖。本文基于 PKI(Public Key Infratructure)技术,采用身份认证和访问控制的安全策略,设计了网上综合业务平台,提高了单位办事人员的效率,减轻了社会保险所的工作量。

收稿日期: 2005-09-12

修回日期: 2005-09-20

作者简介: 兰 剑(1971-),男,广西柳州人,工程师,主要从事计算机网络及 PKI研究。

1 平台功能

社会保险所平台综合业务系统由系统终端用户和 Web服务器等构成,其中系统终端用户包括社会保险所操作员、各单位办事员和其它浏览人员。为了遵循公证、公平原则,保证社会保险所综合业务平台参与各方的利益,从相关机密文件下载、申报数据上传、社会保险所操作员审核整个过程中,必须保证参与各方的业务行为不可抵赖。该平台具有以下功能:

1.1 相关机密文件下载

下载机密文件是指社会保险所操作员下载各单位上报的数据或者单位下载社会保险所提供的相关重要表格。下载文件必须保证其通信安全。下载操作方需要获取下载的资格,并获取登录凭证(数字证书)后,登录到社会保险所综合业务平台。

1.2 申报数据上传

在企业申报数据上传过程中,首先上传操作方需要取得授权,获取申报和上传的资格,并获取能够证实用户真实身份的登录凭证,才能登录管理页面、上传数据。与下载文件一样,上传的数据也必须保证

其通信安全。

1.3 网上审核

网上审批是社会保险所管理人员在规定的某一时间对进行上报的单位进行的资料审核操作。这一系列操作需要负相当大的责任,不允许有人进行冒名顶替或者被恶意的破坏分子进行修改,所以必须保证这个过程是安全的。

1.4 不可抵赖

在社会保险管理人员和单位办事人员参与网上综合业务的各个核心环节中,他们所提交的数据、审核意见等所有核心数据都是不可以抵赖的。一旦有任何一方进行抵赖都会严重影响社会保险所综合业务的权威性,会严重损害社会保险管理所的形象。

2 平台设计

2.1 设计思路

社会保险所综合业务平台的设计思路如下:

(1)利用 CA中心的 PKI认证系统为参与社会保险所综合业务的用户颁发数字证书。

(2)给 Web服务器颁发服务器数字证书,使社会保险所综合业务集成数字证书的应用,利用安全套接字协议技术、加密技术和数字签名技术,实现网上综合业务的安全功能。

(3)用户在网上办理综合业务活动时,必须使用颁发的数字证书才能访问社会保险所综合业务平台,通过用户的数字证书来实现对用户的身份认证和访问控制。在进行相关业务操作时,如上传数据、下载文件和审核等,使用颁发的数字证书对于传输的数据进行加密、签名,确保应用系统的信息机密性、完整性和不可抵赖性需求。

2.2 平台模块设计

社会保险所综合业务平台按照资源划分权限,保证只有经过授权的用户才能使用被授权的资源,它通常采用身份认证和访问控制两种方式。

系统中客户端浏览器与 Web服务器间的通信通过双向鉴别的 SSL实现。在 SSL会话产生时,服务器会传送它的证书,用户端浏览器自动分析服务器证书,并根据不同版本的浏览器,产生 40位或 128位的会话密钥,用于对交易的信息进行加密。所有的过程都会在几秒钟内自动完成,对用户是透明的。当用户访问相应页面时,系统自动访问后台数据库中的访问控制列表来决定是否授权访问。社会保险业务平台主要由以下模块组成:

2.2.1 服务器证书

服务器证书通过建立客户端浏览器和 Web服务器之间的 SSL安全通道,保证双方传递信息的安全性,而且用户可以通过服务器证书验证所访问的网站的真实可靠性。服务器证书建立 SSL通道时协商使用 128位密钥长的会话密钥。

2.2.2 客户端证书

客户端证书由 CA中心为各单位、操作员颁发,这些证书中包含用户的名字以及其他相关信息。建立 SSL通道时,服务器会要求浏览器提交客户端的证书。提交后,服务器会验证客户端证书的有效性。

2.2.3 证书解析模块

证书解析模块以动态库、ActiveX控件等方式提供给各种 Web服务器。证书分解模块可以解析证书中包含的各种信息。在用户访问招投标系统时,用户提供的客户端证书在服务器中由服务器解析,并将解析出的用户信息提交给后台数据库查询访问控制列表(ACL),确定用户的访问权限。

2.2.4 访问控制列表(ACL)

在数据库中建立访问控制列表。整个列表中设定了用户的访问权限。

3 平台的业务流程

持有数字证书的单位用户使用网上业务、登录业务平台的流程如下:

(1)单位用户可以在公众区下载表格,输入业务信息,完成后使用硬件载体进行签名、加密操作,保证提交的信息安全性、完整性和身份确认性,同时也保证了其不可抵赖;

(2)单位用户通过互联网访问综合业务平台,使用单位身份证书登录系统;

(3)系统提取用户登录信息,根据登录信息与社会保险业务内部系统数据进行核实;

(4)返回核实通过与否的相关信息;

(5)单位填写上传等业务信息后提交;

(6)综合服务系统把该企业的业务信息及附件发送到业务系统;

(7)社会保险操作人员同样使用数字证书(个人身份证书)登录业务平台,将企业上传的资料下载到本地,以及进行一些别的操作;

(8)下载到本地的信息可以使用文档签名软件进行验证签名有效性。

4 平台安全构架

我用采用证书应用接口对系统进行安全集成,平台安全结构如图 1所示。平台可分为 3个安全模块:证书解析模块、签名及证书验证模块、个人信任代理模块。

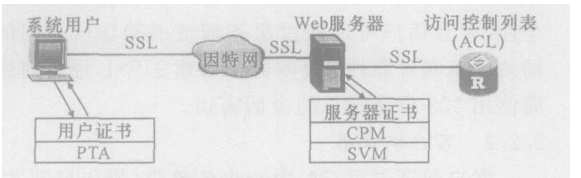

图 1 平台安全构架

4.1 证书解析模块

证书解析模块是一系列平台下的动态链接库,用于解析 DER或 PEM编码的 X.509数字证书,将证书中的信息,包括用户名、证书有效期等信息分解为字符串。证书解析模块作为服务器的功能插件安装在 Web服务器上,解析用户证书,获用户信息,根据用户信息查询社会保险网配置的访问控制列表(ACL),获取用户的访问权限,实现系统的访问控制。

4.2 签名及证书验证模块

证书验证模块也是一系列平台下的动态链接库,要实现服务器端对数字签名以及数字证书的验证,数字证书可选使用 CRL或 OCSP来验证其有效性。签名验证模块以插件的方式提供给社会保险网 Web服务器,实现对用户提交的数字签名的验证。

4.3 个人信任代理模块

个人信任代理是客户端的软件包,既包括安装在客户端的文件加密解密程序,也包括用于数字签名和签名验证的 ActiveX控件。文件加/解密模块可以产生随机数密钥对文件进行加密,以及使用输入的密钥对文件进行解密。Active控件由用户访问相关网页时下载到客户端浏览器中,实现使用本地的证书对文件数字签名、以及签名验证。个人信任代理要在保证数据安全的 Web页面下配置,随 Web页面下载并注册,它使用用户证书的私钥对提交的表单数据进行数字签名。

社会保险平台的 Web服务器配置服务器证书和 SSL功能,用户必须使用 HTTPS访问,并要求用户证书,配置服务器的可信 CA为本方案设计的根 CA,只有 CA体系下的用户证书才能访问系统。客户端必须从 CA认证系统申请用户证书,才能进行社会保险网登录。申请的用户证书代表了用户的身份,登录时必须提交用户证书。用户向社会保险网网上申报业务系统提交请求与审核数据时,必须使用该用户证书的私钥进行数字签名。客户端和系统服务器之间的所有数据通信都是通过 SSL安全通道进行加密传输。

5 结束语

社会保险业务平台申报系统中使用数字证书不仅增加了社会保险机构的政务透明度,避免了由于人为因素给企业社会保险注册等工作带来的不便,而且方便了企业的申报工作,提高了社会保险管理业务的工作效率。最重要的是,它为社会保险机构和企业双方都提供了必要的法律保障,从法律上认定了双方在网上的行为。应用 CA证书进行的企业网上社会保险,将使社会保险工作得到明显改观。

(责任编辑:黎贞崇)