基于 PKI 的统一信任管理平台设计与实现

◆ 盛伟瑜

摘要：本文首先简要介绍了信息技术环境下企业的安全需求，以及公钥基础设施体系在满足这些安全需求上的主要机制和原理。然后阐述了企业在信息化建设中遇到的问题及其基于公钥基础设施体系技术建设的统一信任管理平台的架构和主要功能；并对系统实现的情况做了说明。最后，对平台应用的效果进行了分析和总结。

关键词：PKI；公钥基础设施；信息；安全

一、公钥基础设施体系（Public Key Infrastructure,PKI）

近年来，随着信息技术的迅速发展如今诸如互联网应用、电子商务、移动办公、云计算等计算机技术已经在企业和社会上得到了广泛的应用。由此全社会都产生了对信息安全问题的高度关注。概括起来，一个信息系统面临着以下四个最基本的安全需求：

（1）身份验证（Authentication）与防抵赖（Non-Repudiation）：当用户访问信息系统或在线进行交易时，信息系统会对用户的身份进行识别，并会采用某种机制确保用户对其行为无法进行否认。

（2）机密性（Confidentiality）：由于信息系统内部本身的功能设计、程序以及网络等方面都是相对封闭的，当用户对信息系统进行访问时，往往担心其输入的信息是否会被他人非法的获取，因此需要对信息进行加密，以避免信息被非法截取[1]。

（3）完整性（Integrity）：信息系统中的数据应确保数据在处理过程和存储中的完整，避免未经授权的篡改和删除。

（4）可用性（Availability）：信息系统应用于企业的各个关键领域，这就要求其运行应稳定可靠。很多大型的企业信息化系统往往需要具有 7*24 的访问能力，确保服务的连续。

面对上述四个方面的安全需求，利用公钥基础设施体系（Public Key Infrastructure, PKI）可以很好地加以解决。根据微软对 PKI 的定义，PKI 是由一个受信任的第三方机构将软硬件集成在一起，以对信息通信的双方进行身份识别和验证。这个第三方机构称为认证中心 CA（Certificate Authority）。在通信过程中，CA 会计算数字证书信息的 hash 值，并对 hash 值用 CA 的私钥加密，连同数字证书信息一起形成一份新的数字证书；当通信的一方获得该数字证书后，用 CA 的公钥解密其 hash 值，计算信息数据新的 hash 值，比较两个 hash，如果内容匹配，则可以确认该信息的有效性。利用 PKI 技术，可确保双方在安全可信的条件下进行信息的通信，这对于企业级信息系统的应用，特别是电子商务等应用领域，具有重要的价值[2]。

二、系统架构与主要功能

一般大型的集团企业在其信息化建设中往往投入了大量的资金和人力用于构建覆盖全集团的 OA 系统、邮件系统、ERP 系统等 IT 系统。由于各系统都是在不同的时期采用不同的技术平台开发和建设的，因此系统访问的安全性、协同性都难以保持一致。为此，通过实施一套基于 PKI 的统一信任管理系统，集团企业可以将主要的信息系统都纳入到该系统下，在加强信息安全的前提下，通过对人员身份的集中管理，实现对系统访问账号的统一认证和授权，并借助单点登录技术实现集中的访问控制，满足跨平台和系统之间的业务同步和信息共享的要求。平台的总体设计思路是：

（1）建立统一目录和用户管理，利用来自于人力资源管理系统的员工身份、职位和组织等有关信息，建立 LDAP 中的账号和组织信息、以及各应用系统账户的映射关系，并实现用户身份等信息的定期同步。

（2）搭建 LDAP 系统，按照主从部署方式，集中管理集团的人员账户信息和各个应用系统的账户信息，并与 CA 系统集成，实现数字证书和吊销列表的发布管理和查询管理。

（3）建立集团统一的信息门户，与 LDAP 和 CA 系统集成并结合单点登录功能，当用户登录集团应用系统时，首先将登录内网门户，以此实现对集团内各信息系统的集中访问控制，以及跨平台应用与协同。

（4）为满足移动办公的需要，采用多种灵活的认证方式，如采用 USB-Key 的方式将用户证书保存在移动媒介中，确保证书和密钥的安全，也可采用 Web/Form 认证或短信认证等。

统一信任管理平台是一个综合的业务系统管理服务平台，以 PKI/CA 技术为核心，实现集中的用户管理、目录管理、认证管理、访问控制和审计等功能，为多应用系统提供用户身份、系统资源、权限策略等统一、安全、有效的配置和服务。该平台逻辑架构如图 1 所示。

平台采用模块化的设计，主要功能有：统一目录管理，用于身份和组织架构信息的存储和查询，对目录结构对象的自定义管理，定义用户账户的密码管理策略；统一用户管理，对用户的身份信息和权限进行集中的管理和维护，与相关应用系统之间实现系统账户信息的同步。可与企业信息门户或 OA 等系统集成，从而实现用户对系统访问的在线申请和管理；认证管理，对用户提交的访问信息进行验证，可以提供多种验证方式，包括 CA 认证、Web 认证、短信认证以及动态口令等方式，用户一旦通过认证，即可访问集团内所有的受信应用系统；统一访问控制，提供了集中的策略控制管理的功能，可针对用户组或 IP 地址等执行不同的控制。与相关信息系统进行集成，可实现单点登录的集成应用，满足跨平台的访问和业务协同[3]。整个统一信任管理平台还拥有系统审计的功能，对认证和登录等过程提供日志记录和审计报告，并根据用户登录行为执行相应的规范，如多次登录失败后锁定账户。

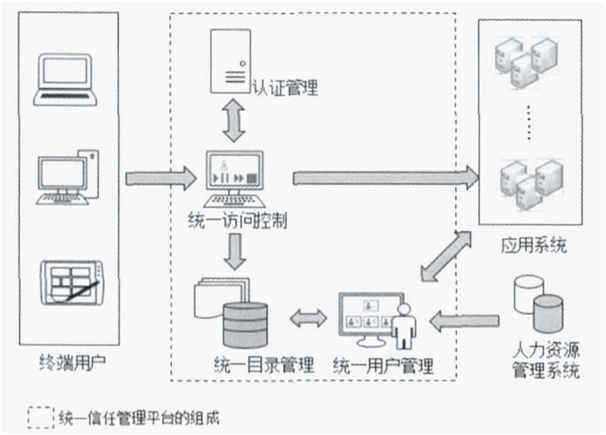

图 1 统一信任管理平台的逻辑架构

三、系统的部署

整个系统平台可集中部署在一台应用服务器中。利用企业服务总线（ESB）来实现与人力资源系统和其他应用系统的数据集成和同步。利用后台管理端实现对统一用户管理和认证管理等功能模块的操作，实现相应的日常运营和监控管理的要求。

由于主从 LDAP 分别所属不同的物理区域，所以需要通过防火墙端口开放的方式进行互连互通。平台主要通过访问从 LDAP 的方式来进行用户账户的管理和操作，主 LDAP 定期通过访问从 LDAP 的方式来进行数据的同步，以达到主从互为备份的目的。如其中任意一台 LDAP 目录服务器出现问题，都可以通过修改平台外部数据源连接配置方式进行快速切换，不至于影响正常使用，从而将风险降至最低[4]。

四、系统的实现

根据上述的业务需求和系统功能设计，某集团建设的统一信任管理平台系统于 2016 年上线。下面就该系统上线后的主要功能使用情况作简要介绍。

平台的认证管理集成了数字证书注册中心（RA）和密钥管理的功能，包括集中申请、自动审批。当用户需要制作电子证书时，系统管理员登录系统的后台管理端，进入“集中证书管理”模块，系统的 RA 接口模块会自动调用 LDAP 数据库中的用户信息；管理员通过预先定义好的路径可访问指定的 CA 系统，申请签发数字证书，并由 CA 系统返回给系统管理员；系统管理员然后将证书装入 USB-Key 中，完成制证的过程。上述过程实现了电子证书全生命周期的集中管理，系统管理员可实现对证书的创建、注销和检查等操作。

单点登录是系统集中认证管理功能的一个主要应用形式。单点登录分为基于门户的单点登录和基于应用的单点登录。对于大多数类似于本系统的 Web 应用来说，采用基于门户的单点登录在技术上更容易实现。其基本流程是：终端用户首先登录统一的 Web 门户，进入统一认证界面；选择 USB-Key 认证（证书认证）或者通行码认证。如果采用 USB-Key 认证的方式，终端用户客户端的代理程序会收集存储在 USB-Key 中的证书信息（如证书颁发机构、有效期等），并将信息提交至“认证管理”模块；“认证管理”会将用户证书信息提交到与 CA 系统联动的 CRL（证书吊销列表）服务中进行有效性检查；若通过有效性检查，则系统会返回给用户可访问的图形化应用系统列表，用户只要点击页面中相应图标链接便可访问相应的应用系统。

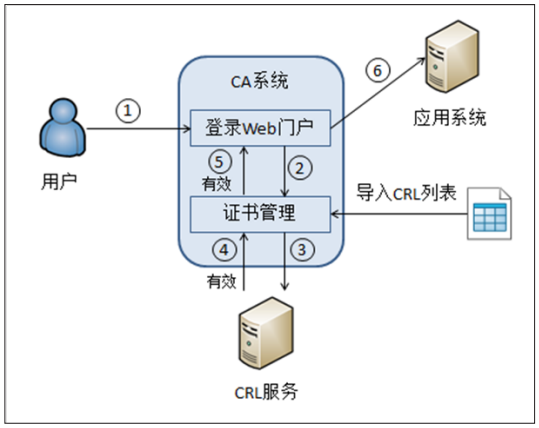

图 2 单点登录与证书有效性检查示意图

统一用户管理是要将分散且独立管理的各应用系统用户权限集中到一个系统平台下进行集中的管理。通过集中授权，可对用户组或角色进行定义，以确定其对应用系统及功能的访问权限。当有新员工入职时，通过与人力资源系统的员工身份信息同步，可对该员工开立系统访问账户，并为此分配一个组或角色。员工登录信息门户时，根据其所在的组或角色会获得相应的系统访问权限。由于运用了组和角色进行管理，当员工职位发生变动时，与人力资源管理系统同步，即可自动调整相应的组和角色，由此避免了因没有及时对员工身份信息进行调整而产生系统访问控制上的风险。

五、结语

面对企业信息系统建设和应用的不断扩展，特别是对于大型集团企业日益增长的对各种异构环境下跨平台信息系统访问和业务协同的需要，基于 PKI 的统一信任管理平台将会有效解决企业多应用系统中身份信息和账户管理的混乱，杜绝一人多账户或多人混用账户而导致的信息安全风险，以此可以确保对信息系统的访问都是在有效授权下进行。此外，利用统一用户和目录的管理以及与相关应用系统的集成，可以对企业内部各系统的账户进行集中的授权，这将极大地降低了管理的复杂度，减少信息系统运维成本。因此，该平台的应用和推广对于提高企业信息数据安全和加强信息系统管控都有着重要的现实作用。

参考文献

[1] 关振胜 . 公钥基础设施 PKI 及其应用 [M]. 电子工业出版社 ,2008,

[2] 关振胜 . 公钥基础设施 PKI 与认证机构 CA[M], 电子工业出版社 ,2002.

[3] 吴宙 .PKI 系统网络安全认证技术 [J]. 计算机安全 ,2003 ,8 :10-25.

[4]"Public Key Infrastructure". MSDN. Retrieved 26 March 2015.

（作者单位：上海纺织（集团）有限公司信息管理部）