基于 J2EE 和 JAAS 的科技管理平台的设计与实现①

Design and Implementation of Science and Technology Management Platform Based on J2EE and JAAS

邹　江　张文绚　吴高辉　(湖北省建设信息中心 湖北 武汉 430071)

摘　要：基于 Java 的企业级计算解决方案 J2EE 和基于 Java 的安全认证授权解决方案 JAAS 的综合应用，可以为基于互联网的安全分布式应用系统的构建提供一个较好的解决方案。作者在某科技管理平台的设计与实现过程中，采用 J2EE 和 JAAS 技术，实现了一个有较好安全保障的，集科技项目管理、专家信息管理和科技项目网上申报等功能于一体的网上分布式应用系统，并在实际使用中取得了较好的效果。

关键词：J2EE JAAS 分布式计算

1　引言

随着 Internet 的迅速发展，越来越多的政府对外办公业务依赖网络来进行，采用信息化手段改造传统办公流程，并通过网络手段与外界沟通和交流，达到内部办公流程的自动化和对外公务业务流程的一体化，已成为办公自动化系统的必然发展趋势。

过去，科技计划专家库和科技计划项目的管理工作主要是由主管部门通过手工方式进行的，纸面文档是主要的处理方式，电子文档也主要是采用文件目录存放的方式，没有做到信息化管理。随着时间积累，每年的数据越积越多，以至于电子文档积累了数千个文件，基本检索都无法做到纸面文档更是堆积如山，连文档的存放都成了问题，更不必提由人工去翻阅查找了。

为了解决这一问题，主管部门提出开发一套能够服务于部门科技管理的网络信息系统，该系统对内提高部门科技管理的行政效率，降低管理成本；对外为各有关单位提供项目申报平台，为有关专家提供网上评审系统，为有关省、市级行政管理部门提供交流渠道，实现一个平台服务于多方面用户的目标。

2　系统设计

2.1 系统功能设计

为达到上述的业务目标，开发者进行了广泛深入的需求调研，了解了部门科技管理的实际业务需求细节。

系统总体层次如图 1 所示，可分为六个层次：(1)用户服务层，为用户提供对外接口服务；(2)业务模块层，实现系统的主要业务逻辑；(3)工作流服务层，实现系统的主要业务流程；(4)基础模块层，包括系统的一些基础数据模块；(5)元数据接口层，存储和管理系统的主要数据(如专家、项目、申报单位等)的元数据信息；(6)基础数据层，存储和管理系统的基础数据。

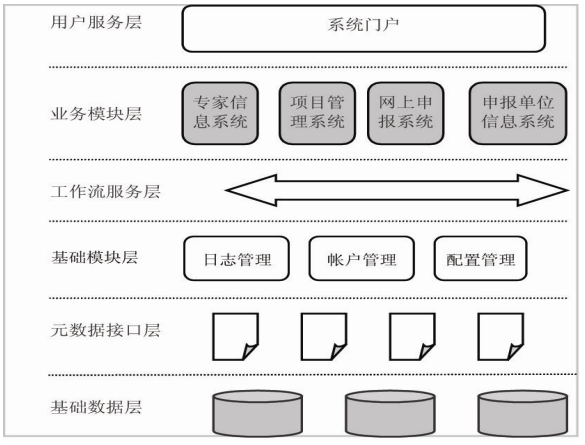

图 1　系统功能结构图

① 收稿时间:2008-08-22

2.2 系统安全设计

目前大多数的 Web 程序都是实现的单向 SSL 认证，即只验证服务器，保护用户的安全。而本系统由于涉及国家部委科技项目管理、专家管理等重要业务，需要有较高的安全性。为此，采用了既要验证服务器，又要验证用户的双向验证方案，如图 2 所示:

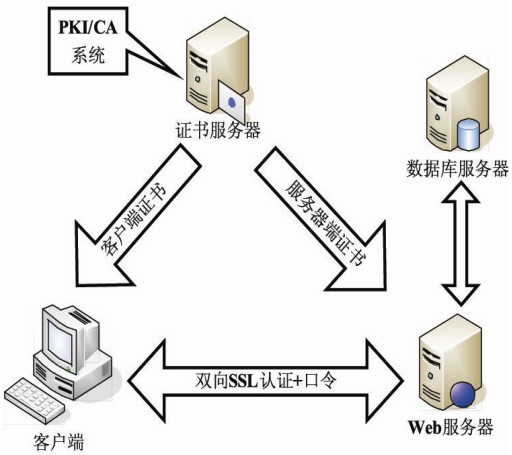

图 2　基于非对称加密体系的系统安全保障机制

首先由系统管理方将数字证书颁发给用户，该数字证书由管理方签发，用户将该证书导入浏览器，才能够访问到登录界面。在此基础上，用户正确输入帐号和密码后，才能真正进入系统。也就是说，用户必须同时拥有证书、帐号和密码三项资料，才能够进入系统；进入系统之后，用户端与服务器之间的所有数据交流都是通过安全超文本传输协议(Hypertext Transfer Protocol Secure，HTTPS)进行，这就给系统提供了较充分的安全保障。

SSL 协议为在 Internet 上进行私有通信提供了可能，它被设计为一种用于网络协议的编程接口。SSL 协议同时使用对称密钥算法和公钥加密算法。前者在速度上比后者要快很多，但是后者可以实现更好的安全验证。SSL 提供了三种基本的安全服务：机密性、完整性和认证性[1]。

2.3 系统工作流设计

部委科技管理的实际业务流程非常庞杂，且并不是一成不变的，因此，如何定义复合实际业务需要的系统工作流，使之具有灵活的适用性和可扩展性，就成为非常重要的问题。根据部委科技管理的实际业务流程，系统中定义了几个工作流，其中比较典型的是项目申报工作流，如图 3 所示:

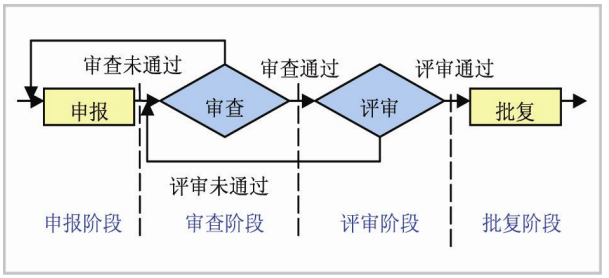

图 3　项目申报的工作流设计

该流程可以分为四个典型阶段：(1)申报阶段，由申报方提交项目申报信息，包括项目名称、目标、申请单位、参与人、工作基础、主要内容、申请经费等内容；(2)审查阶段，由管理方对申报方提交的申报信息进行审查，如果申报信息合法，申请单位符合要求，申请人具备相关工作基础等，则通过审查，否则退回申报；(3)评审阶段，由系统随机从专家库中抽取的该领域专家组成评审专家组，对该项目进行评审，如果评审无异议，则通过评审，否则退回重新进行项目审查；(4)批复阶段，由管理方对评审通过的项目进行汇总，上报上级领导同意后即予以批复立项，项目申报流程完成。

3 系统实现

3.1 系统技术方案

在系统运转模式考虑方面，由于系统用户分布于全国各地，网络条件、计算机条件差异较大，所以系统要求必须是瘦客户端访问，不能把逻辑负担放到客户端完成。针对这一需要，作者采用了浏览器/服务器(B/S)模式进行系统实现，且将服务器端部署于较高性能的采用 Linux 操作系统的部门级服务器上。

系统性能考虑方面，虽然该系统的用户数量并不大，但由于申报、评审等大都发生在一个时段内，因此短时间大批量的访问是主要的应用实境。同时，由于服务器操作系统平台可能存在的多样性，必须采用较高性能的，具有跨平台部署能力的分布式计算技术来实现。因此，经过审慎比较，选择了 J2EE[2](Java 2 Enterprise Edition，Java 2 企业版)技术作为系统技术实现方案，因为 J2EE 降低了构建多层网络分布式应用系统的成本和复杂度，可以较为方便的部署[2]。J2EE 的整体体系架构如图 4 所示。

在系统安全性考虑方面，由于系统的实际使用关

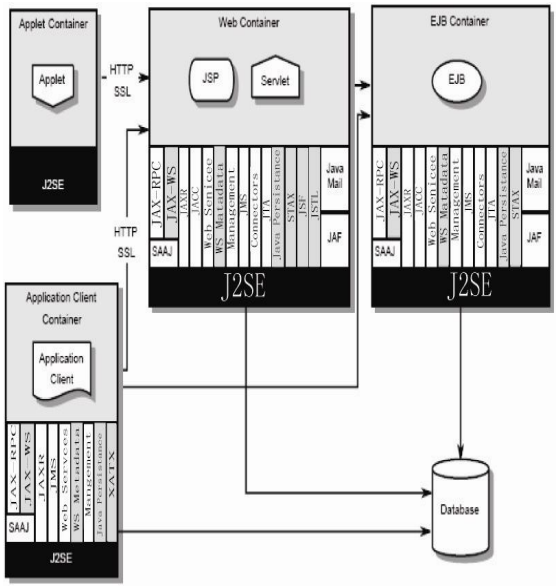

图 4　J2EE 体系架构[2]

系到各个申报单位和省级行政管理部门的科研项目、专家信息等数据，系统安全性要求较高，所以系统采用基于 Java 的 SSL 实现技术——JAAS[3](Java Authentication Authorization Service，Java 验证和授权服务)来实现系统的安全保障。JAAS 扩展了 Java 的安全模型，以对系统请求者执行基于身份验证的检查[3]。采用对各每个用户发放不同权限的用户证书的方式来限制访问[3]。JAAS 强调的是通过验证谁在运行代码以及他的权限来保护系统免受用户的攻击[4]。一段典型的采用 JAAS 生成数字证书的代码如表 1 所示。X.509 目录身份验证服务以可信赖方(CA)颁发的公钥证书为核心，以公钥密码体系和数字签名的使用为基础[5]。

表 1　使用 JAAS 生成 X509 数字证书的典型代码

```
//设置新证书的序列号
//CertificateSerialNumber csn = new CertificateSerialNumber(sn);
//cinfo_second.set(X509CertInfo.SERIAL_NUMBER, csn);
//设置新证书的签发者
cinfo_second.set(X509CertInfo.ISSUER + "."
    + CertificateIssuerName.DN_NAME, issuer);
//指定 CA 签名该证书所使用的算法为 md5WithRSA
AlgorithmId algorithm =
    new AlgorithmId(AlgorithmId.md5WithRSAEncryption_oid);
cinfo_second.set(CertificateAlgorithmId.NAME + "." +
    CertificateAlgorithmId.ALGORITHM, algorithm);
```

3.2 系统典型模块

系统登录模块是系统的安全门槛，跨过这道门槛用户才能进入系统浏览信息和进行操作，如图 5 所示。在系统实现中，首先采用 CertModule 模块对用户数字证书进行验证，然后采用 UserModule 模块对用户帐号、密码进行验证。系统实际采用了 PKCS#12 格式作为客户端证书格式。PKCS#12 是由美国 RSA 数据安全公司及其合作伙伴制定的一组公钥密码学标准之一，它描述了个人信息交换语法标准，描述了将用户公钥、私钥、证书和其他相关信息打包的语法。

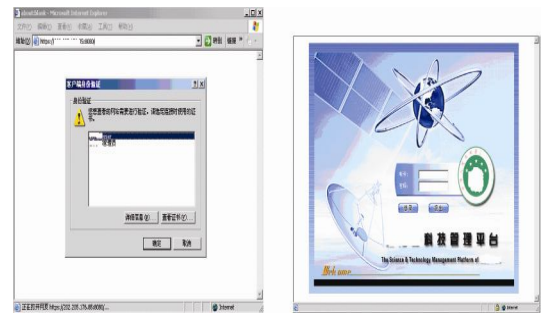

图 5　系统访问时的身份验证界面和登录界面

系统登录过程由 8 个步骤组成[6]：(1)客户端向服务器端发送握手字符串；(2)服务器端收到握手字符串，向客户端发送服务器证书；(3)客户端接收到服务器证书，验证其有效性后，向服务器端发送客户端证书；(4)服务器端接收到客户端证书，验证其有效性后，向客户端发送时间戳组成的字节数组；(5)客户端接收到该字节数组后，用自己的私钥对其进行加密，然后发送给服务器；(6)服务器接受到客户端发来的密文，用客户端证书中的公钥进行解密，并将解密结果和先前发送给客户端的字节数组进行比对，如果一致，则向客户端发送用户数字证书认证成功的信息；(7)用户进入登录页面，输入用户名和密码，并提交服务器；(8)服务器端从用户信息数据库中进行比对，如果符

(下转第 140 页)

(上接第 98 页)

合，则发送用户帐号、密码验证成功信息，并重定向到系统首页，认证过程完成。

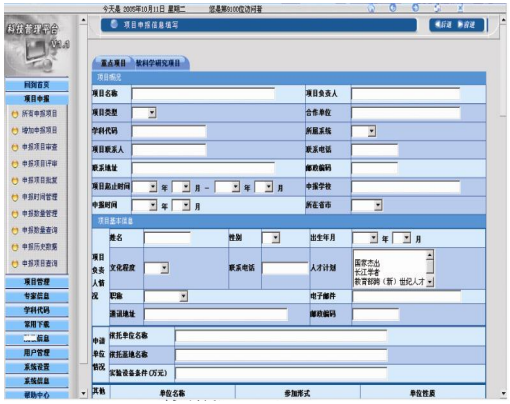

图 6　部委科技管理平台项目申报系统页面

系统项目申报页面如图 6 所示。系统中的所有页面与用户的数据交流都是加密传输的，在专家信息录入部分还提供了 Office 文档的识别能力，使用户可以上传含有多条专家信息(包括照片)的 Excel 文档，系统可以自动识别专家数据，并批量导入数据库，从而大大加快了信息录入的速度。

4　总结

作者针对部委科技管理的实际业务需要，设计和实现了一套基于 J2EE 和 JAAS 的科技管理平台。目前，该平台已经投入实际应用，取得了较好的实用效果，用户对该系统也给予了非常肯定的评价。另一方面，该系统也存在一些问题，包括工作流程的定制不够灵活，项目动态跟踪的能力有待加强等。目前，针对上述问题，该系统正在进一步改进之中。经过该平台的设计和实现体验，作者认为，基于 Web 的安全、一体化的网上业务集成管理系统将成为必然的发展趋势。

参考文献

1 Helton R, Helton J. Java Security Solutions, 2003:132 – 138.

2 Sun Microsystems, Inc, Java 2 Platform Enterprise Edition Specification, v5.0, 2005:5 – 7.

3 Sun Microsystems, Inc., Introduction to JAAS and Using JAAS, 2001: 2 – 3.[2001-07-27]http://java. sun. com/developer/JDCTechTips/2001/tt0727.html.

4 Taylor A, Layman R, Buege B.张伟,张华平等译. J2EE&Java 黑客大曝光——开发安全的 Java 应用, 北京:清华大学出版社, 2003:50 – 55.

5 Stallings W, 网络安全要素—应用与标准. 北京:人民邮电出版社, 2000:83 – 89.

6 王创,等. Java 安全认证在电子政务系统中的应用研究.微电子学与计算机, 2004,21(5):55 – 58.