面向海洋信息管理的轻量级 CA 的设计与实现

丁　明, 周　林, 韩京云, 宋庆磊, 宋转玲, 李新放, 刘海行

(国家海洋局第一海洋研究所 海洋信息与计算中心, 山东 青岛 266061)

摘要: 面向海洋信息管理的需求, 基于 J2EE 平台, 使用 Bouncy Castle 提供的加密算法与工具, 遵从 PKI(Public Key Infrastructure, 公钥基础设施)相关标准, 实现了一个适用于中小型海洋信息管理系统的轻量级数字证书认证机构(CA , Certificate Authority)。该 CA 提供了适用于中小型海洋信息管理系统的数据存储与传输加密功能, 为通过网络实现高效的海洋科研数据收集与共享管理提供了技术上的安全保障。

关键词: 海洋信息安全; 海洋信息管理; Bouncy Castle; 数字证书认证机构(CA, Certificate Authority); 加密

中图分类号: TP309　　**文献标识码**: A　　**文章编号**: 1000-3096(2014)02-0091-05

doi: 10.11759/hykx20121005001

信息化提高了整个社会的运行效率, 信息网络已成为社会发展的重要保证, 随着信息技术的发展, 海洋信息化应用日益普及, 海洋信息化建设取得了显著的进展, 为实现“数字海洋、生态海洋、安全海洋、和谐海洋”奠定了良好的基础[1]。数字化网络化已在海洋信息管理中普遍应用, 信息资源已经成为重要的生产要素、无形资产和社会财富[2], 而信息的核心是数据, 所以保护数据的安全是信息安全最重要的工作。

在海洋科研信息化的过程中, 数字化的信息数据必然会吸引各种人为攻击, 数据安全已经成为阻碍海洋信息化深度发展的重要原因之一。如何在尽可能不妨碍信息交流效率的前提下, 保证信息的保密性、完整性与不可否认性, 已经成为海洋信息管理与应用网络化过程面临的主要问题[3]。

密码学是信息安全的基础, 公钥密码技术相对于传统的对称密码学是一个重大的进步, 是信息安全技术中的革命性进展, 目前公钥体制广泛地应用于数字证书认证机构(CA , Certificate Authority)认证、数字签名和密钥交换等领域[4]。CA 是整个信息安全的基础, 是 PKI(Public Key Infrastructure, 公钥基础设施)的核心执行机构, 负责数字证书的产生、签发、废除等工作[5]。基于公钥密码技术的 CA 系统, 在信息安全方面具有广泛的用途, 能起到数据保密、数据完整性确认、身份认证、访问控制、行为不可否认性等作用。Bouncy Castle 是一个开源的加密包的 API 集合, 实现了大量的加密算法。通过应用数字证书结合加密技术, 能够有效地保障海洋信息管理网络化过程中的信息安全。

CA 认证系统在多个领域已经得到了广泛的应用, 网上银行是典型的基于 CA 认证体系的电子商务应用系统; 电子政务方面, 国家电子政务外网的“政务电子认证系统”已拥有最大容量为 100 万张证书的数字证书中心 CA。目前的中小型海洋信息管理系统在安全方面多侧重于身份认证与权限管理, 缺乏信息传输与存储的加密功能。由于海洋数据具有多元、多源性、时序性、海量性、异构性、标准性与机密性等特点[6], 在中小型海洋信息系统的开发与建设过程使用第三方的 CA 限制较多, 购买与集成成本较高, 所以构建一个通用, 易于集成与修改、扩展的认证中心是一个很好的选择。

本文面向海洋信息管理的应用需求, 基于开源软件体系, 采用 Bouncy Castle 加密包、J2EE 体系架构, 对 CA 进行设计和开发, 能为海洋信息管理系统提供更好的安全保障。

1　系统功能需求

信息系统安全的目的是保证信息系统所支持的业务过程运作的安全[7], 本 CA 用来保障海洋信息在服务器存储和网络传输过程中的安全性, 对相关人员提供身份验证并保障其行为不可否认性, 同时具备通用性, 轻量化的特点, 便于各中小型海洋信息管理系统集成。基于以上目标, 本 CA 将实现的功能见图 1。

收稿日期: 2012-10-05; 修回日期: 2012-12-24

基金项目: 中央级公益性科研院所基本科研业务费专项资金(2011T03); 南海海洋环境数据信息服务平台(2008AA09A40105)

作者简介: 丁明(1977-), 男, 山东潍坊人, 工程师, 学士, 主要从事海洋数据资料处理与信息系统研究, 电话: 0532-88961476, E-mail: ding@fio.org.cn; 刘海行, 通信作者, 主要从事海洋信息系统研发与数据可视化技术及并行计算研究工作, 电话: 0532-88967412, E－mail: liuhx@fio.org.cn

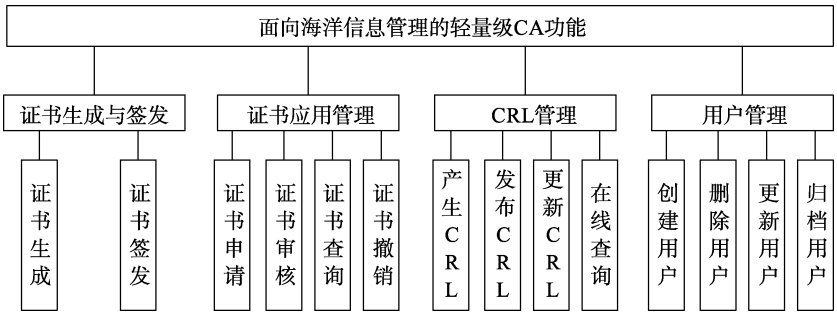

图 1　面向海洋信息管理的轻量级 CA 功能结构

Fig. 1　The functional architecture provided by lightweight CA for marine management information

1.1　证书生成与签发功能

证书生成与签发是 CA 的核心部分，本 CA 具备生成证书和签发各种不同用途的数字证书的功能。例如：X.509 V3 标准格式的身份证书；具有加密功能的 SSL 证书; Web Server 证书; S/MIME 电子邮件证书等。

1.2　证书应用管理功能

证书管理功能主要包括：证书的申请、审核、查询、撤销功能。

1.3　CRL 管理功能

具备 CRL(Certificate Revocation List)的产生、发布、更新、在线查询功能。CRL 的范围包括所有用户的作废证书以及 CA 的作废证书，能够对 CRL 有效期进行调整，管理 CRL 的更新周期。同时将 CRL 发布至 Web 页面，供用户下载。

1.4　用户管理功能

用户管理包括用户的创建、删除、更新、归档等功能。为证书使用者创建账号，从而可以对与用户相关的证书、密钥等操作进行管理，在用户注销时，从数据库里删除用户以及相关的证书、密钥等信息，将所有用户归档，以便以后对用户的行为进行追查。

2　系统结构设计

本系统采用模块化结构设计，由证书注册审批中心(RA , Registration Authority)、CA 控制认证中心、CA 服务中心几部分构成，系统结构见图 2。

证书申请与发放的主要流程：用户使用 RA 服务，申请获得证书。管理员收到请求后使用 RA 管理系统，审查和批准用户的证书申请，如果管理员批准证书的申请，CA 控制中心将签发用户证书。最后用户获得自己的证书。

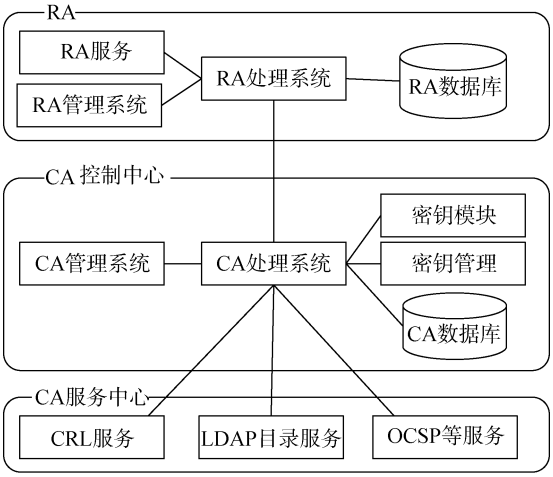

图 2　面向海洋信息管理的轻量级 CA 系统结构

Fig. 2　Architecture of lightweight CA for marine management information

证书吊销流程：首先用户提交证书吊销申请。然后管理员使用 CA 管理系统审批用户证书吊销。最后 CA 处理系统根据管理员的请求，吊销指定证书，并将吊销的证书信息发布到证书吊销列表(CRL)中，通过 LDAP、OCSP 等方式进行发布，同时对数据库中保存的用户证书的信息进行更新。

3　系统实现

3.1　开发平台

针对多数海洋信息管理系统对数据安全的需求，为确保系统具有较好的兼容性、安全性和可扩展性，本系统采用 J2EE 平台进行开发，并采用 Bouncy Castle 实现加密设计。

Java 平台具有高度的安全性，Java 的安全平台有两部分组成：Java 安全体系内核与 Java 密码体系。Java 安全体系，包括自动内存管理，字节代码验证机制，安全类加载方式等。Java 的密码体系设计得很

完善: Java Security 提供相关类和接口，位于 Java 编程语言的核心 API 内的 java.security 包，可供开发人员实现安全功能。Java 的密码体系依赖于 JCA (Java Cryptography Architecture)和 JCE(Java Cryptography Extension)。JCA 提供基本的加密框架，如证书、数字签名、消息摘要和密钥对产生器; JCE 扩展了 JCA，提供了更丰富的 API，包括对称分组算法、对称的流加密算法、非对称加密算法和信息认证码等[8]。

加密包 Bouncy Castle：由于 JCA/JCE 并不执行各种算法，它们只是连接应用和实际算法实现程序的一组接口，所以我们同时需要使用 Bouncy Castle 加密包。Bouncy Castle 是一个不受美国出口控制规定限制的开源的加密包。它功能强大，包括：JAVA 和 C#版本的轻量级加密 API、JCE/JCA 的 provider 以及对 X.509, CRLs, PKCS12, S/MIME, OCSP 等的支持。

3.2 具体实现

基于 CA 系统的功能设计和 J2EE 开发平台，本文对 CA 系统进行了设计和实现，下面给出 CA 的核心实现代码。

```
//使用 RSA 算法创建密钥对生成器，并生成密钥对 kp。
KeyPairGenerator kpg = KeyPairGenerator.getInstance("RSA");
SecureRandom random = new java.security.SecureRandom();
kpg.initialize(2048, random);
KeyPair kp = kpg.generateKeyPair();
//生成 PKCS#12 格式的根证书。
Security.addProvider(new BouncyCastleProvider());
KeyPair kp=new genKeyPair();//genKeyPair 为生成密钥对的函数使用新生成的密钥对
PrivateKey caPrivKey = kp.getPrivate();
PublicKey caPubKey = kp.getPublic();
//根证书中的各种信息，以及 DN 等参数。
String issuer = "C=CN, ST=ShanDong, O=FIO, OU=micc, CN=caOcean, L=QingDao";
X509V3CertificateGenerator v3CertGen = new X509V3CertificateGenerator();
v3CertGen.setIssuerDN(new X509Principal(issuer));
……
//生成 CDP(CRL Distribution Point)。
DistributionPoint[] dp = new DistributionPoint[1];
DistributionPointName dpn=new DistributionPointName(…);
dp[0] = new DistributionPoint(dpn, null, null);
v3CertGen.addExtension(X509Extensions.CRLDistributionPoints, false, new CRLDistPoint(dp));
v3CertGen.addExtension(X509Extensions.AuthorityKeyIdentifier, false, new AuthorityKeyIdentifierStructure(caPubKey));
v3CertGen.addExtension(X509Extensions.BasicConstraints, false, new BasicConstraints(0));
X509Certificate cert = v3CertGen.generate(caPrivKey);
//普通用户证书签发。
v3CertGen.setIssuerDN(PrincipalUtil.getSubjectX509Principal(caCert));
v3CertGen.addExtension(X509Extensions.BasicConstraints, false , new org.bouncycastle.asn1.x509.BasicConstraints(false));
//证书吊销列表(CRL)的产生。
//读取根证书。
ReadP12Cert readTheCer = new ReadP12Cert();
KeyPair kp = readTheCer.getkeyPair();
X509Certificate caCert = readTheCer.getcertificate();
//获取根证书的私钥，用来对 CRL 进行签名。
PrivateKey caPrivKey = kp.getPrivate();
PublicKey caPubKey = kp.getPublic();
org.bouncycastle.asn1.x509.X509Name issuserDDN = new org.bouncycastle.asn1.x509.X509Name(caCert.getIssuerDN().toString());
//生成 crl。
//X509V2CRLGenerator crlGenerator = new X509V2CRLGenerator();
crlGenerator.setSignatureAlgorithm("SHA1WithRSAEncryption");
crlGenerator.setThisUpdate(new java.util.Date());
//以吊销 175 号证书为例。
crlGenerator.addCRLEntry(BigInteger.valueOf(0x00af), new java.util.Date(), CRLReason.keyCompromise);
X509CRL myCrl = crlGenerator.generate (caPrivKey);
```

4 CA 系统应用实例

本文面向海洋信息管理的安全需求，对设计实现的 CA 系统在数字签名和信息加密等方面进行了具体的应用。现以某区域海洋数据收集与信息共享系统为例，介绍本 CA 在海洋信息管理系统中的使用。

该系统通过互联网实现异地数据采集、传递与共享，对数据安全有较高的要求，现结合该系统需求对本 CA 的使用进行简要阐述。

异地数据采集，实时发送数据到服务器，数据对采集者和处理者之外的人员保密。针对该需求，系统首先判断所采集数据文件的大小，如果数据文件较小，就直接使用通过 CA 服务中心获得的数据处理

者的公钥，采用 RSA 加密算法对数据进行加密，然后将加密后的数据上传到服务器保存。对于较大的数据文件，采用数字信封(Digital Envelope)技术，采用 AES(Advanced Encryption Standard)加密算法生成一个 256 位的密钥，使用该密钥对大数据文件进行加密，并使用数据处理者的公钥对该密钥进行加密，最后将加密后的密钥和加密后的数据文件打包后通过网络发送到服务器保存。

用户需要随时随地获取经授权的数据。服务器收到用户的数据使用申请后，首先判断用户是否有访问该数据的权限，如果用户有合法权限，系统将会解密指定数据，然后再使用该用户的公钥将数据加密后发送给用户，数据在网络传输过程中处于加密状态，所以用户可以随时通过网络下载数据而不必担心安全问题，下载后使自己的CA证书私钥解密即可使用。

为保证用户发布结果数据的可靠性和不可否认性，要求用户对发布的数据进行签名。该需求采用数字签名技术解决：首先采用 SHA1 算法获得要发布的数据的数字摘要值，然后用户用自己的私钥对包含数字摘要值与当前时间等信息的文件进行加密处理，实现了对数据的合法“签名”，最后将要发布的数据和私钥加密后的数据打包发布。数据使用者通过 CA 服务中心获得数据发布用户的公钥来解读收到的“数字签名”，并将解读结果与数据的 SHA1 值进行对比，从而保障接收到的数据是可靠的和完整的。

通过以上设计，使需要保密的数据在传输和服务器的存放过程中完全处于加密状态，只有指定 CA 证书私钥的拥有人员才能使用。这样保证了无论是通过网络截取数据，还是攻破服务器后获得数据文件，得到的皆是无法读取的加密后的数据，从而保证了指定的海洋信息数据的安全。

通过以上所述的设计与实现细节，可以看出本 CA 具有以下显著特点：

1) 系统采用主流开源软件、跨平台语言实现，具有较高的安全性、兼容性和可扩展性，可以通过中间件技术方便地集成到已有的海洋信息管理系统当中[9]。

2) 系统与用户交互采用 B/S 模式，通过浏览器进行，不受客户端操作系统及运行环境限制，易于部署和操作。

3) 在多数海洋信息管理系统的使用环境下，没有直接访问CA注册审批中心与控制中心的需求，可以对CA控制中心进行物理隔离，从而在不影响正常功能使用的前提下确保系统安全。

4) 本系统遵循国际化的 X.509 V3 标准，以及国家 PKI 标准 GB/T19713-2005 GB/T 19714-2005，系统具有很好的开放性，能够与各种应用结合，成为具有实用价值的真正的安全基础设施。

随着海洋信息化、数字化的深入发展，数字化管理的海洋信息具有分布性、数据和信息类型格式的多样性、数据的海量性特点[10]，保护数字化海洋信息安全已经成为海洋信息化过程中的重要任务。针对海洋信息管理快速发展过程中对信息安全的需求，结合当前信息安全技术应用的现状，本文提出了用开源软件开发构建CA的一种方法，并给出了具体实现，该 CA 有必备的功能和较好的安全性，便于不同系统集成，具有较高的应用和理论价值。

参考文献:

[1] 国家海洋局. 国家海洋事业发展规划纲要[R]. 北京: 国家海洋局, 2008.

[2] 朱建明.基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2009, 32(4): 828.

[3] 刘丰，韩伟. 海洋信息系统的安全问题与对策研究[J]. 海洋开发与管理, 2012, 7: 60.

[4] 张琳. 基于 PKI 的电子商务安全研究[J]. 电子科技大学学报, 2009, 38(增刊): 101.

[5] 关震胜. 公钥基础设施 PKI 及其应用[M]. 北京: 电子工业出版社, 2008: 69-70.

[6] 张明华，黄冬梅，熊中敏，等. 多源异构海量海洋数据综合管理平台构建研究[J]. 海洋科学, 2012, 36(02): 110.

[7] 余志伟，唐任仲，贾东浇，等. 一种基于业务过程的信息系统安全需求分析方法[J]. 中国机械工程, 2007, 18(4): 457.

[8] 马臣云，王彦. 精通 PKI 网络安全认证技术与编程实现[M]. 北京: 人民邮电出版社, 2008: 279.

[9] 肖天威，张世永，钟亦平. 基于 PKI/CA 的中间件系统的设计与实现[J]. 计算机工程, 2006, 32(4): 190.

[10] 何亚文，苏奋镇，杜云艳，等. 海洋信息网格服务平台的设计与实现[J]. 地球信息科学学报, 2010, 12(5): 681.

Design and implementation of lightweight CA for marine information management

DING Ming, ZHOU Lin, HAN Jing-yun, SONG Qing-lei, SONG Zhuan-ling, LI Xin-fang, LIU Hai-xing

(Marine Information and Computing Center, the First Institute of Oceanography, State Oceanic Administration, Qingdao 266061, China)

Received: Oct., 5, 2012
Key words: marine information security; marine management information; Bouncy Castle; CA (Certificate Authority); encryption

Abstract: In order to meet marine information management requirement, in this paper, we have successfully set up a lightweight CA (Certificate Authority) which is suitable for various small marine management information systems. The achievement of this lightweight CA was based on the J2EE platform, based on, using Bouncy Castle encryption algorithms and tools and conforming to PKI (Public Key Infrastructure) standard. The CA provides encryption function for data storage and transmission to small and medium marine management information systems, It can offer efficient protection for transfer and sharing of marine scientific information.

(本文编辑: 刘珊珊　李晓燕)