Certificate Services 2.0 的研究与定制

Research and Customization of Certificate Services 2.0

沈士根　（嘉兴学院 信息工程学院 314001）

摘要：文章分析了 Windows . NET Server 内嵌的 Certificate Services 2.0 组件结构，通过定制策略模块和退出模块定制 Certificate Services 2.0，最后，以一个实例说明了证书生成的过程。

关键词：PKI　数字证书　Certificate Services

1　引言

要保证网络安全所要求的认证、数据完整性、数据保密性、不可否认性，基于公开密钥基础设施 PKI（Public Key Infrastructure）的网络安全体系目前已成为解决方案的首选。如电子商务、电子政务、网上银行、网上证券等，通过建立 PKI，就能满足这些业务的安全需求。2003 年，Microsoft 推出的 Windows . NET Server 中文版操作系统中嵌入了 PKI 体系，这使得我们不用购买第三方提供的 PKI 服务并且花较少代价就能建立单位自身的 PKI。而要建立基于 Windows . NET Server 的 PKI，其核心是 Certificate Services 2.0 组件。并且，Microsoft 考虑到用户的不同需求，用户还可以定制证书服务。

2　Certificate Services 2.0 概述

Certificate Services 2.0 其实是一种运行在 Windows . NET Server 上的服务。它通过 RPC 或 HTTP 方式接受新的数字证书请求，然后根据策略模块检查每个证书请求，再决定批准、拒绝或挂起证书请求。同时，管理员可通过 Certificate Services 2.0 撤消数字证书形成 CRL，并发布到 Active Directory 或一个指定文件夹。实际上，Certificate Services 2.0 实现的是一个 PKI 体系中的认证机构 CA 的功能。

在 Windows . NET Server 安装 Certificate Services 2.0 时有两种不同类型的 CA 策略：企业级 CA 和独立 CA。企业级 CA 通过 RPC 方式来扮演身份验证请求者角色并将客户端访问令牌与 Active Directory 中证书模板上的 ACL 集合进行对比，因此，它需要 Active Directory 的支持。安装企业级 CA 时自动将根结点证书放置在 Active Directory 中，并且，企业内部的所有客户端都将获得这份 CA 证书的一个拷贝，企业级 CA 生成的用户证书和 CRL 将直接发布到 Active Directory。而独立 CA 无需依赖 Active Directory，要把独立 CA 生成的用户证书和 CRL 发布到 Active Directory，必须借助 Microsoft 的 SDK 开发平台提供的 dsstore. exe 实现。

在标准支持上，Certificate Services 2.0 支持客户端为 IE，使用 VBScript 的 Xenroll 命令生成用户密钥对，以标准的 PKCS#10 提交的证书请求格式，也支持客户端为 Netscape Navigator，使用 HTML 的 KEYGEN 标签生成用户密钥对，以 BASE64 编码格式提交的证书请求，还支持 PKCS#7 证书续订格式。

3　Certificate Services 2.0 结构

Certificate Services 2.0 包括服务器引擎（Server Engine）、证书服务数据库（Certificate Services Database）、策略模块（Policy Module）、退出模块（Exit Module）、管理员工具（Admin Tools）等。

在 Windows . NET Server 中，由证书系统完成数字证书从申请到发布等的管理。证书系统除包括 Certificate Services 2.0 外，还包括中介（Intermediary）、客户端（Client）等。图 1 显示了 Certificate Services 2.0 的结构及证书系统中各部分通过不同接口实现相互通信的情况。

3.1　客户端（Client）

客户端是一种软件，如 IE 或 Netscape Navigator，用户通过客户端软件首先生成密钥对，再通过 xenroll. dll 证书注册控件保护私钥、选择不同的 CSP、密钥长度及 Hash 算法等，最后向中介提交包含上述信息和客户信息的证书申请。因为客户端软件与中介通信时涉及用户的保密信息，所以通信采用 HTTPS 方式。

3.2　中介（Intermediary）

中介是一种 Web 服务器，如 Microsoft 的 IIS。IIS 通过 CertCli. dll 动态链接库提供的 CCertConfig 和 CCertRequest 接口与服务器引擎通信。其中，CertCli. dll 随 Microsoft 的 SDK 开发平台提供。

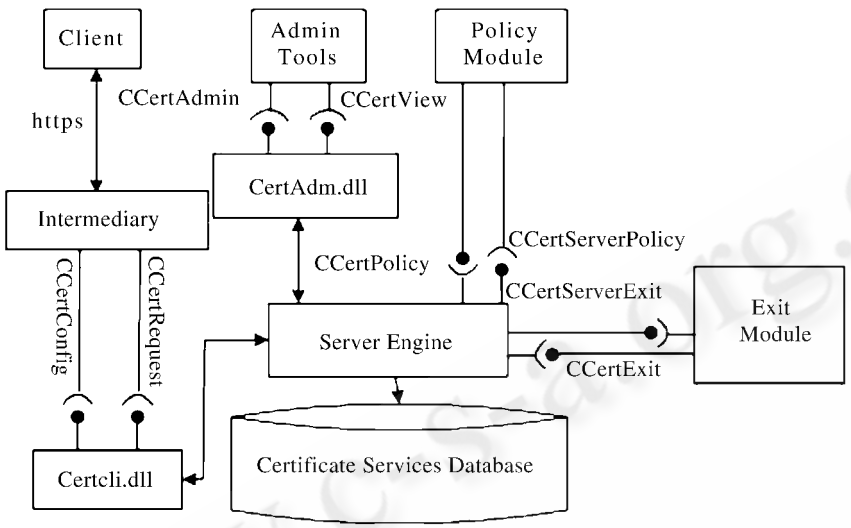

图 1　Certificate Services 2.0 结构及相互联系

3.3 超级用户工具(Admin Tools)

超级用户工具通过 CertAdm. dll 提供的 CCertAdmin 和 CCertView 接口与服务器引擎通信。在 Windows . NET Server 中，超级用户工具实质是一个 MMC 插件，可通过“开始→管理工具→证书颁发机构”启动。其中，CertAdm. dll 随 Microsoft 的 SDK 开发平台提供。

3.4 策略模块(Policy Module)

策略模块决定一个证书申请是否应被批准、拒绝或挂起，其实质是一个动态链接库文件。在 Windows . NET Server 中，缺省的策略模块文件是 Certpdef. dll，用户可根据特殊需要定制策略模块。在这里要说明的是，企业级 CA 策略使用 Active Directory 来决定申请者的身份，所以立即发布或拒绝一个申请；而独立 CA 策略将证书申请送到挂起队列，以便由一个超级用户登录后再决定是否批准、拒绝或挂起一个申请。

3.5 退出模块(Exit Module)

退出模块使用适当的传输机制或协议包装并发布证书和 CRL，在默认情况下，企业级 CA 的退出模块向 Active Directory 发布证书和 CRL，而独立 CA 向某个文件夹(默认% system% \system32 \CertSrv)发布证书和 CRL。像策略模块一样，退出模块也是一个完全可定制的动态链接库，其默认的文件是 Certxds. dll。

3.6 证书服务数据库(Certificate Services Database)

证书服务数据库记录所有证书事务。它跟踪所有证书申请，并记录这些证书申请是被批准还是被拒绝；它为发布的证书记录信息，如序列号和到期日期等；它也标志和跟踪被管理员撤消的证书。默认情况下，证书服务数据库存放在% system% \system32 \Certlog 文件夹。

4 Certificate Services 2.0 的定制

Certificate Services 2.0 的定制开发主要涉及独立 CA 的策略模块和退出模块的定制，对企业级 CA，定制模块可能会产生意想不到的后果。编写策略模块和退出模块可使用 c/c + + 或 Microsoft Visual Basic，但需要 Microsoft Visual c + + 5.0、Microsoft Visual Basic 5.0 或更高版本的编译器。笔者采用 Visual Basic 6.0 编译器。

在调试自定义的策略模块和退出模块时，可先退出到命令提示符下，然后执行 net stop Certsvc 命令停止 Certificate Services 2.0 的运行，再用 Microsoft 的 SDK 开发平台随带的 Regsvr32. exe 注册自行开发的策略模块和退出模块，再执行 Certsrv - z 命令，这时在命令提示符后会显示相应结果。若调试通过，可执行 net start Certsvc 命令重新启动 Certificate Services 2.0。

4.1 策略模块的定制

策略模块的定制开发主要涉及到被服务器引擎调用的 CCertPolicy 类和 CCertManageModule 类。对 CCertPolicy 类，要建立 Initialize 方法实现策略模块的初始化工作；要建立 VerifyRequest 方法用于通知策略模块有新的证书请求进入，策略模块再调用由服务器引擎提供的 CCertServerPolicy 接口的相应方法来判断证书请求是否该发布、拒绝或挂起；要建立 GetDescription 方法实现以文本形式返回策略模块的信息和功能；要建立 Shutdown 方法实现当服务器引擎停止工作前，由服务器引擎通知策略模块停止工作。对 CCertManageModule 类，要建立 GetProperty 方法来获得模块的属性值；要建立 SetProperty 方法来对模块的属性赋值；要建立

Configure 方法显示模块中的用户接口。

在 Visual Basic 6.0 中定制开发策略模块的流程主要包括:

(1) 创建一个新工程,并命名为 MyAPP(工程名可更改),结果将是一个 ActiveX DLL 文件。

(2) 添加一个类 Policy,要注意的是该类名不可更改,用于实现 CCertPolicy 类的功能。再添加另一个类 PolicyManage,同样,该类名不可更改,用于实现 CCertManageModule 类的功能。

(3) 如果在策略模块中需使用 CCertServerPolicy 对象,可通过"工程→引用"添加 CertClil. dll,并确信 CertIF 1.0 Type Library 已选中。其中 CCertServerPolicy 接口对象是由服务器引擎提供给策略模块调用的,它允许策略模块收集到证书申请和证书的数据项,设置某些证书属性、读写证书的扩展属性等。动态链接库 CerClil. dll 随 Microsoft 的 SDK 开发平台发布。

(4) 建立 Policy 类和 PolicyManage 类中的相应方法。

(5) 编译生成 DLL 文件,再通过 Regsvr32. exe 注册后调试定制的策略模块是否正确。

4.2 退出模块的定制

退出模块的定制开发主要涉及由服务器引擎调用的 CCertExit 类和 CCertManageModule 类。对 CCertExit 类,要建立 Initialize 方法实现退出模块的初始化工作;要建立 Notify 方法通知退出模块发生了一个事件,如证书发布、CRL 发布、服务器引擎已关闭等;要建立 CetDescription 方法实现以文本方式返回退出模块的信息和功能。对 CCertManageModule 类,同上文"4.1 策略模块"所述。

在 Visual Basic 6.0 中开发退出模块的流程类似于策略模块,但对应 CCertExit 类的类名要求为 Exit,对应 CCertManageModule 类的类名要求为 ExitPolicy。

4.3 证书生成的实例

下面笔者以一个证书生成的实例,来说明 Certificate Services 2.0 的关键处理流程,当然,实际的处理流程还要考虑更多情况。其中,假设客户端软件为 IE,中介为 IIS。

(1) 服务器引擎调用自行开发的 Policy. Initialize 和 Exit. Initialize 方法分别初始化策略模块和退出模块。

(2) IIS 调用由服务器引擎提供的 CCertConfig. GetConfig 方法收集相应配置信息,如服务器名、CA 名(在安装 Certificate Services 2.0 时指定)等。

(3) 用户通过 IE 使用证书注册控件以 HTTPS 方式向 IIS 提交原始证书请求信息,包括用户名、国家名、CSP、密钥长度等。

(4) IIS 调用 CCertRequest. Submit 方法向服务器引擎以 PKCS#10 格式向服务器引擎提交证书请求。

(5) 服务器引擎调用自行开发的 Policy. VerifyRequest 方法通知策略模块有证书请求到达,策略模块调用服务器引擎提供的 CCertServerPolicy 接口检查证书请求,再决定是否颁发、拒绝或挂起。

(6) (本过程可选)若证书请求被挂起,超级用户可通过"开始→管理工具→证书颁发机构"调用 CCertAdmin 接口向服务器引擎重新提交或拒绝证书请求。

(7) 服务器引擎将相关证书事务写入证书服务数据库;再调用自行开发的 Exit. Notify 方法通知退出模块发生了证书发布、CRL 发布等事件,再由退出模块发布证书、CRL 等到指定位置。

5 结束语

Windows . NET Server 的发布,因为其内嵌的 Certificate Services 2.0,可使企业花较少代价自建 CA,因此,深入研究 Certificate Services 2.0 有现实意义。本文分析了 Certificate Services 2.0 的结构,定制了其中的策略模块和退出模块,并以一个实例说明 Certificate Services 2.0 的证书处理流程,这对有意建立基于 Windows . NET Server 的企业 PKI 有一定的参考价值。

参考文献

1 Carlisle Adams, Steve Lloyd, 冯登国等译, 公开密钥基础设施——概念、标准和实施[M], 人民邮电出版社, 2001。

2 Microsoft. Windows Server 2003 Security[EB/OL]. http://www.microsoft.com, 2003.

3 Cyrus Peikari, Seth Fogie, 周靖译, Windows . NET Server 安全指南[M], 清华大学出版社, 2002。

4 Microsoft. MSDN Library for Visual Studio . NET 2003[M/CD], 2003.

5 Microsoft. MSDN Online [EB/OL]. http://msdn.microsoft.com/library/default.asp, 2004.