NEUSOFT 东软

软 件 创 造 客 户 价 值

# SRQ06电子证书认证系统

## Universal CA

技　　术　　白　　皮　　书


沈 阳 东 软 软 件 股 份 有 限 公 司

# 1　信息安全与 PKI 技术

信息技术的应用使得企业的信息资产具有更多的可访问性，并且更容易使用，但需要保护系统和这些系统的信息处理的隐私和安全。电子商务、电子政务和其它应用已在公司之间、政府内部及政府与企业之间得到了广泛的实施。但是这些应用中都要通过使用密码技术来提供数据保密性、完整性、可认证性及不可否认性。使得这些普遍的安全服务成为可能的技术是公钥密码技术，通过将它在公开密钥基础设施（PKI）中运用，使得在大范围内进行认证服务成为可能。PKI 已经日益成为保证 E-government、E-Business 信息安全的基础设施。

# 2 企业级 PKI 系统概要

企业在不断完善内部信息系统的同时，信息的安全可靠性、内部人员的身份认证也是企业急需解决的当务之急。因此，企业需要一套基于自身业务流程的安全认证管理机制，以适应企业内部人员的身份认证及数据的安全管理。

东软股份针对企业内部网上信息安全及企业电子商务认证的需要提供了企业级的 CA 产品，用于保证企业内部的信息安全，并提供进行电子商务活动时所必需的认证服务。

# 3 SRQ06 电子证书认证系统功能概要

SRQ06 电子证书认证系统（Universal CA）是东软股份开发的用于企业内部构建 PKI 设施 CA 软件，它的主要功能包括：

1　生成、签发证书

SRQ06 电子证书认证系统可以接收用户的证书请求，经管理员审核通过后签发符合 X509 标准的公钥证书。

2　证书检索及保存

SRQ06 电子证书认证系统提供了证书数据库，保存了系统中所有用户的证书，并提供了证书的检索功能，方便用户的使用。

3　证书撤销及 CRL 发送

SRQ06 电子证书认证系统可以根据用户的请求，撤销颁发的证书，并把被撤销的证书，以电子邮件的方式通知系统的所有用户。

# 4 SRQ06 电子证书认证系统操作流程

SRQ06 电子证书认证系统为用户提供基于公钥证书的认证服务，认证中心的主要业务包括：用户注册、用户请求审核、证书的颁发、证书撤销请求审核、证书的撤销、证书及密钥管理、证书及 CRL 的公共访问服务等。

申请证书的用户向认证机构提交身份证明及其他证明材料，认证中心审核无误后，对证书中的身份信息、公钥及其他属性进行数字签名，生成证书颁发给用户。证书有效期满后，需产生新的证书，过程和申请新证书大致相同，只是审核手续能稍稍简化一些。特殊情况下可以提前撤销证书。

证书的申请过程：

1 用户生成密钥对，把私钥保存在本地，生成公钥证书请求
并把请求发送到 CA。

2 CA 审核用户请求，请求中的每项内容都确认无误后，为用户签发证书。

3 CA 在公共服务器上公布新证书

4 在第 2 步中，如用户不符合申请证书的条件，告知用户请求失败。

证书撤销过程：

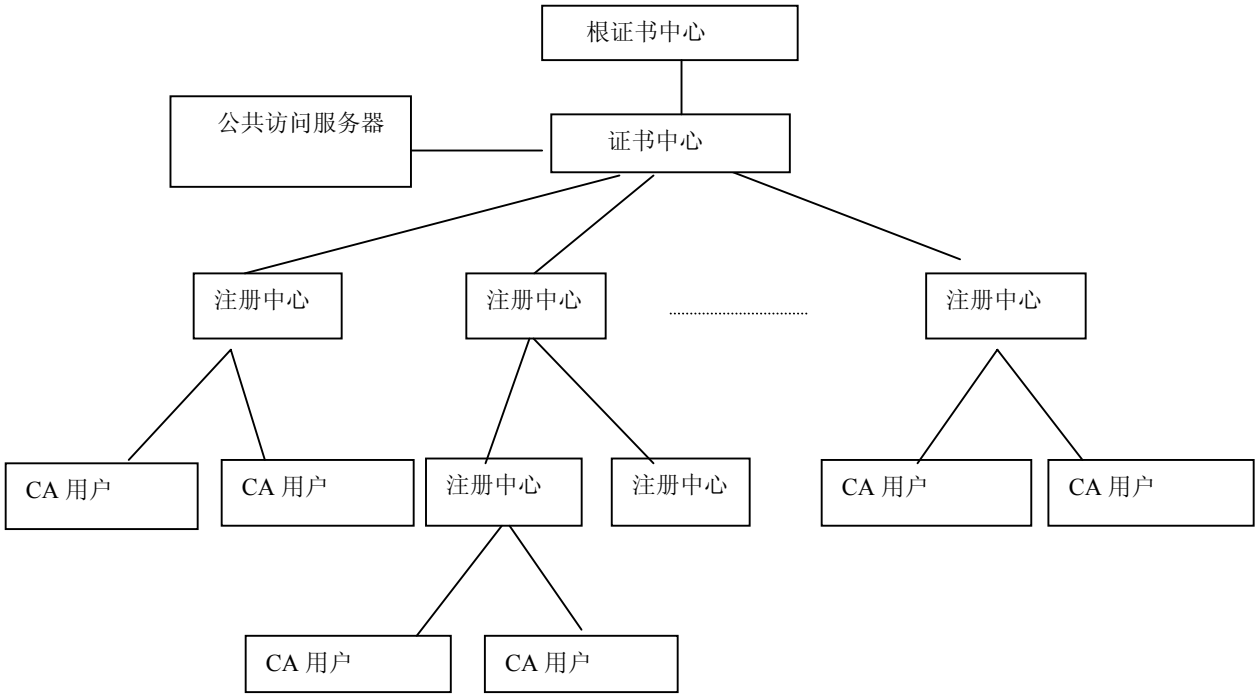
1 用户向 CA 发送证书撤销请求。

2 CA 审核是否符合撤销条件，如符合，撤销证书，把证书加入 CRL 中，并通知系统的所有用户。也可在每次进行证书验证时，由用户主动到 CA 下载。

3 用户验证证书有效性时，使用最新的 CRL，如果证书在 CRL 中，则拒绝信任该证书。

# 5 对多级 CA 体系的支持

SRQ06 电子证书认证系统还专为适应企业或政府机关中的组织形式开发了一种多级结构的认证中心软件，如下图所示：




RCA（根证书中心）是最高一级的 CA，在整个认证体系中有最高的权威性。主要负责有关安全认证服务规章的制定和管理，审批各级 CA 的设立事项，负责各级 CA 的数字证书颁发和管理。它可由企业的总部或组织中的最高管理机构来承担。

CA 就是承担网上安全认证服务、能签发数字证书并能确认用户身份的服务机构。CA 的主要任务是受理数字证书的申请、签发数字证书并对签发的证书进行管理。

RA（注册中心）即证书发放审核部门，它负责对证书申请者进行资格审查，并决定是否同意给该申请者发放证书。RA 在有 CA 的授权的情况下，也可以直接为用户颁发证书。

PA（公共访问服务器）可提供证书和 CRL 的检索服务，使用户方便地得到其它用户的证书并验证其有效性。可以设置多个 PA 以方便用户使用。

# 6 SRQ06 电子证书认证系统的技术特点

SRQ06 电子证书认证系统是按照国际通用的标准设计，采用了先进的信息安全技术开发的企业认证中心系统，具有用户申请、申请审核、证书签发、证书撤销、证书管理等功能，它具有如下的技术特点：

标准化：SRQ06 电子证书认证系统严格遵守 ITU-T X.509 标准，其中应用的全部协议都是被国际上广泛采用的标准协议。

高安全性：SRQ06 电子证书认证系统中使用国密办批准使用的专用算法，对称密钥算法的密钥长度达到了 128 位；RSA 算法的密钥长度为 1024、2048 位。并提供了专用算法替换的接口。

用户界面采用了面向对象的多窗体设计，简单明了，如下图所示：


低成本、易于使用、有良好的可扩展性，可随着企业的规模的发展不断地进行调整和重新配置。

SRQ06 电子证书认证系统内含我国自主知识产权的安全数据库系统 OpenBASE，亦可通过标准的 ODBC 接口与其它标准数据库相联，如 Oracle、SQL Server 等等。

沈 阳 东 软 软 件 股 份 有 限 公 司
地址：沈阳浑南高新技术产业开发区·东大软件园
传真：024-23784036　邮编：110179
网址：www.neusoft.com