基层电子政务应用安全解决方案

1.背景

随着基础信息网络的不断发展和延伸，基层电子政务应用日益丰富，电子政务应用的信息安全问题更加突出和严峻。建立以商用密码为基础的系统应用和安全集成解决方案，以统一门户和数据资源平台为基础，采用商用密码为用户提供身份认证、传输加密、安全存储、电子印章等安全应用支撑，从网络层、数据层、应用层为用户构建一个完善的信息安全保护体系。

2.应用安全需求

在基层电子政务平台建设过程中，围绕着政务应用的安全保障问题，可以归纳出很多安全需求和安全技术。尤其以应用层的安全需求最为突出。随着业务需求的发展和安全威胁的不断增多，应用层面上的安全问题呈现日趋多样的特点。

以公文传输为例，其最基本的一个流程为：发文—〉收文—〉回执—〉批示—〉传阅—〉下载保存—〉打印控制，在这一系列环节中，可以归纳出几个典型的应用安全需求：

- 公文来源可信：确实是某个信任的机构发出的公文；
- 经手人权限可控：对不同的用户设置不同的权限，对可见的内容和可做的操作做严格控制；
- 内容严格保密：点到点的全程密文传送；
- 收发双方不可抵赖：发送方不能否认自己的发出行为，收方通过带数字签名的回执系统，不能否认收到的事实；
- 审计记录健全：各种操作有严格的记录，保留备查。

另外，随着政务信息化建设的日益推进，很多地方的政务系统已经不再满足于简单的公文安全传输要求，而是将起草、审批、会签、办理等环节联合起来，提供完整的公文流转和办公功能，这就需要解决文件在整个应用过程的管控问题。

3．应用安全设计

针对安全需求尤其是应用安全需求，在基层电子政务平台构建过程中，可采用商用密码技术和产品，为用户提供多类安全服务。以数字证书应用为基础，通过对称密码和非对称密码应用，解决身份认证、数据保护、权限管理、安全审计以及责任认定等一系列安全问题。

主要的应用安全设计包括：

身份认证：在服务端和客户端之间实现基于数字证书的可靠身份认证，很好地解决了系统的安全登录问题。

数据传输的机密性和完整性：业务数据在进行点对点或点对中心传输时，采用以商用密码为基础的密码服务中间件，对传输内容进行加密和电子签名，防止对信息的非法获取和篡改，在应用层建立安全的数据传输通道。

数据存储的机密性和完整性：系统数据采用商用密码产品进行加密存储，辅以校验措施来保证数据存储的机密性和完整性，防止数据的非授权访问和修改。

权限管理：系统提供基于数字证书的权限管理，通过验证数字证书，确定用户身份，实现对用户权限的可靠分配。

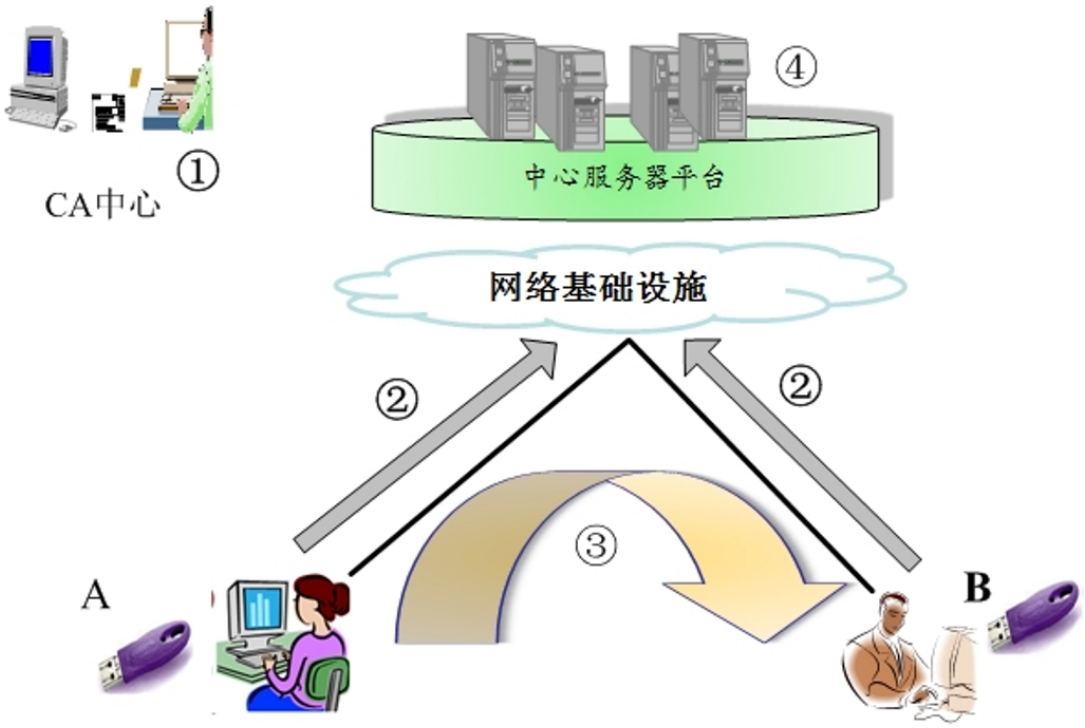
责任认定：通过电子签名技术为电子政务应用中的数据录入、审批、修改、删除等操作提供事后追踪、审核手段，使得对任何越权操作企图以及安全事件具有良好的可追溯性，并为司法举证提供依据，实现对关键操作的责任认定。

安全审计：通过系统的审计模块可以记录每个用户的重要操作，拥有权限

的人员可以查看审计日志记录。并对用户的网络行为、各种操作进行实时的监控，对各种行为进行分类管理，规定行为的范围和期限。

基层电子政务平台在建设中，还可集成部署其他安全设备，如：防火墙、入侵检测、防病毒等，配合安全管理制度，构建一个完善的信息安全体系。

4．应用实例



如上图所示，一个典型的 B/S 架构基层电子政务平台中，A、B、C 等多个客户端通过浏览器登录到中心服务器平台，使用系统各项功能。如果 A 点需要向 B 点发送一个带有敏感信息的公文，则通过在上图中标示出的几个环节，发挥商用密码的安全保障作用:

① 通过电子认证服务机构，可提供具有法律效力的数字证书和相关的证书管理服务；

② A、B 两个客户端，使用智能密码钥匙中存储的数字证书，分别与中心服务器平台中的认证服务器建立基于数字证书的可靠身份认证过程，并依靠验证过的身份，实现基于角色的权限管理，使 A 和 B 都在自己的权限范围内，严格受控的使用系统功能；通过单点登录技术，一个身份角色可以使用平台中的多个应用系统；

③ 从 A 点发往 B 点的公文，通过使用加密和电子签名/电子签章等手段，实现文件数据的全程机密性和完整性保护；同时，归档公文和客户端上的公文都可实现加密存储；B 点在同意接收公文后,会自动向 A 发送带有数字签名的回执,证明确实收到了该公文；

④ 在中心服务器平台中，实现严格的用户权限控制和安全审计；通过运用系统的多项安全功能，实现任意操作的事后追溯和责任认定；另外，系统中心端可酌情部署边界保护设备、漏洞扫描系统、入侵检测系统等。

1. 商用密码产品清单

（1） 电子认证服务机构（CA）

（2） 智能密码钥匙及数字证书

（3） 认证服务器

（4） 电子签章系统

（5） 密码服务中间件

（北京海泰方圆科技有限公司供稿）