机关电子公文系统密码应用示例

1.系统概要

党政机关电子公文系统是党政机关日常办公的重要信息系统，提供公文拟制、公文办理、公文管理等业务过程的信息化管理，以安全保密为基础，以强化服务、降本增效为目标，重点解决纸质办文带来的人力、物力、时间成本损耗问题，**解决传统方式带来的工作效率低、易出错等问题**。

电子公文系统典型应用由电子公文标准化套件、电子公文处理系统、电子公文交换系统组成。

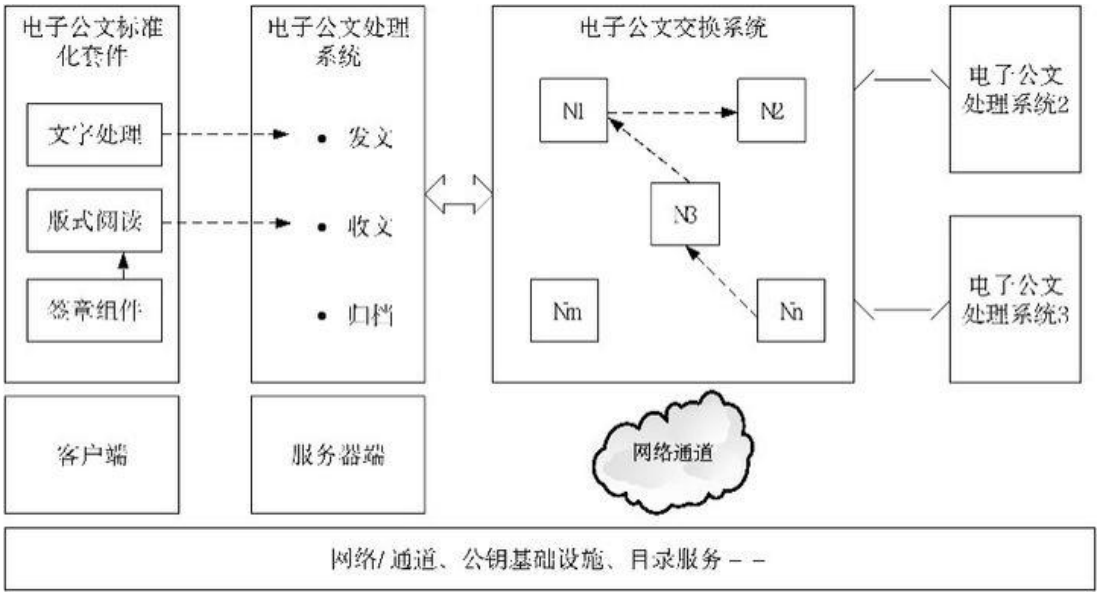


图 党政机关电子公文系统典型应用模式

- 电子公文系统的运行依托统一的基础设施，包括网络/通道、公钥基础设施、目录服务等。其中公钥基础设施为公文传递与交换提供信任基础保障和身份验证、签名验签等信任服务。
- 电子公文标准化套件运行于系统的客户端，包含文字处理、版式阅读、电子签章等组件，为电子公文处理系统提供公文编辑、阅读、签章等功能支持。
- 电子公文处理系统实现电子公文的收发文管理和公文归档等功能，支持根据用户需求定制公文处理流程。
- 电子公文交换系统支持电子公文处理系统间或收发文单位之间的电子公文传输。

2.密码安全需求

（1）电子公文处理系统

电子公文处理系统需要对访问系统的用户身份进行鉴别，以确保用户身份的真实性，避免非法用户进入系统。

电子公文处理系统需要对存储的大量电子文件进行加密保护，以确保电子文件的机密性，避免被非授权人员窃取。

电子公文处理系统需要对用户权限信息进行签名处理，以确保权限信息的真实性和完整性，避免非授权人员伪造权限信息。
电子公文处理系统需要对系统日志进行完整性保护，避免非法人员篡改日志记录。

（2）公文处理终端

公文处理终端需要配合电子公文处理系统，完成对用户身份的鉴别，以确保用户身份的真实性。
公文处理终端需要对用户关键操作进行签名处理，以确保关键业务操作的不可否认性。
公文处理终端需要对成文的电子公文加盖电子签章，确保文件的真实性和不可否认性，为电子文件赋予法律效力。

（3）电子公文交换系统

电子公文交换系统需要对访问系统的用户身份进行鉴别，以确保用户身份的真实性，避免非法用户进入系统。
电子公文交换系统需要对用户权限信息进行签名处理，以确保权限信息的真实性和完整性，避免非授权人员伪造权限信息。
电子公文交换系统需要对应用间传递的交换数据进行签名处理，作为数据来源真实性的证明。
电子公文交换系统需要对系统日志进行完整性保护，避免非法人员篡改日志记录。

（4）公文交换终端

公文交换终端需要配合电子公文交换系统，完成对用户身份的鉴别，以确保用户身份的真实性。
公文交换终端需要对待发的电子公文进行源数据加密，在接收方进行解密处理，以确保电子文件的机密性，避免内外部用户对文件的非法访问。

3.密码应用技术方案

电子公文系统密码应用方案参考电子公文、密码应用、信息安全相关标准规范，为电子公文系统提供密码应用的技术支撑，并参照等级保护的要求进行安全管理。

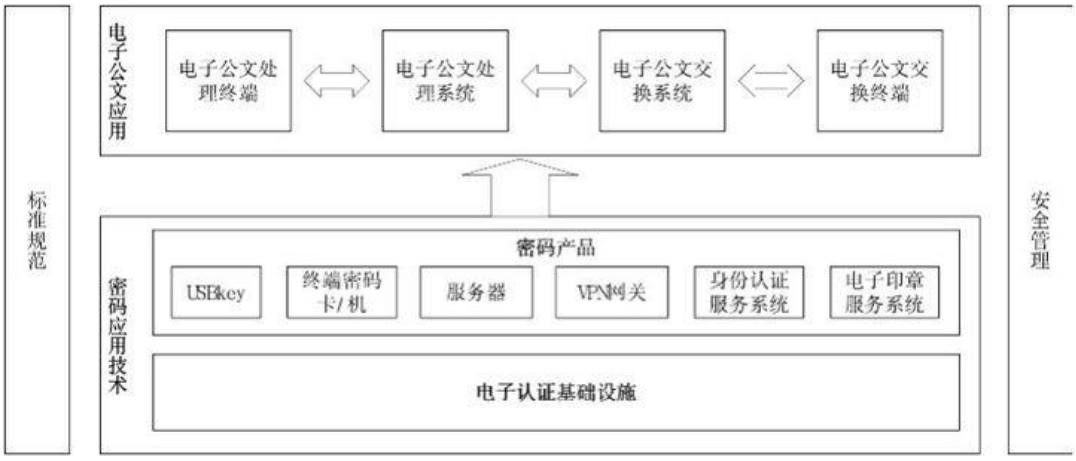


图 电子公文系统密码应用技术框架

电子认证基础设施

电子认证基础设施提供数字证书的注册审核与签发服务，为基于数字证书的信任服务提供支撑。

- **密码产品**

密码产品	主要功能
USBKey	主要提供签名验签、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书或电子印章等用户数据。 根据用途的不同，USBKey又细分为身份认证Key和电子印章Key。 身份认证Key中存放标识用户身份的数字证书，主要用于对用户身份真实性的鉴别。 电子印章Key中存放遵循《GM/T 0031 安全电子签章密码技术规范》的电子印章数据。本示例电子公文系统中用到的电子印章指单位公章，用于对电子公文进行签章，实现电子公文真实性和不可否认性保护。
终端密码卡/机	主要为终端用户提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护，同时提供安全、完善的密钥管理功能。
服务器密码机	主要为应用系统提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护，同时提供安全、完善的密钥管理功能。
VPN网关	VPN网关主要用于在网络上建立安全的信息传输通道，通过对数据包的加密和数据包目标地址的转换实现远程访问，进行加密通信。
身份认证系统	通过对用户、应用、设备等实体提供基于数字证书的身份识别和访问控制服务，实现身份的互信互认、网络访问和信息共享的安全可控。
电子签章系统	为各级政务部门提供电子公章的签章、验章服务，有效保障电子文件的真实性、完整性和签章行为的不可否认性，是实现电子公文流转，部门协同办公的重要信任支撑。

部署示例

遵循网络总体设计，并依托统一的信任服务设施，部署电子公文系统应用。通过在各级网络结点及接入单位部署 VPN 网关，实现省、市、县三级网络安全互通和各级横向接入单位的安全接入。

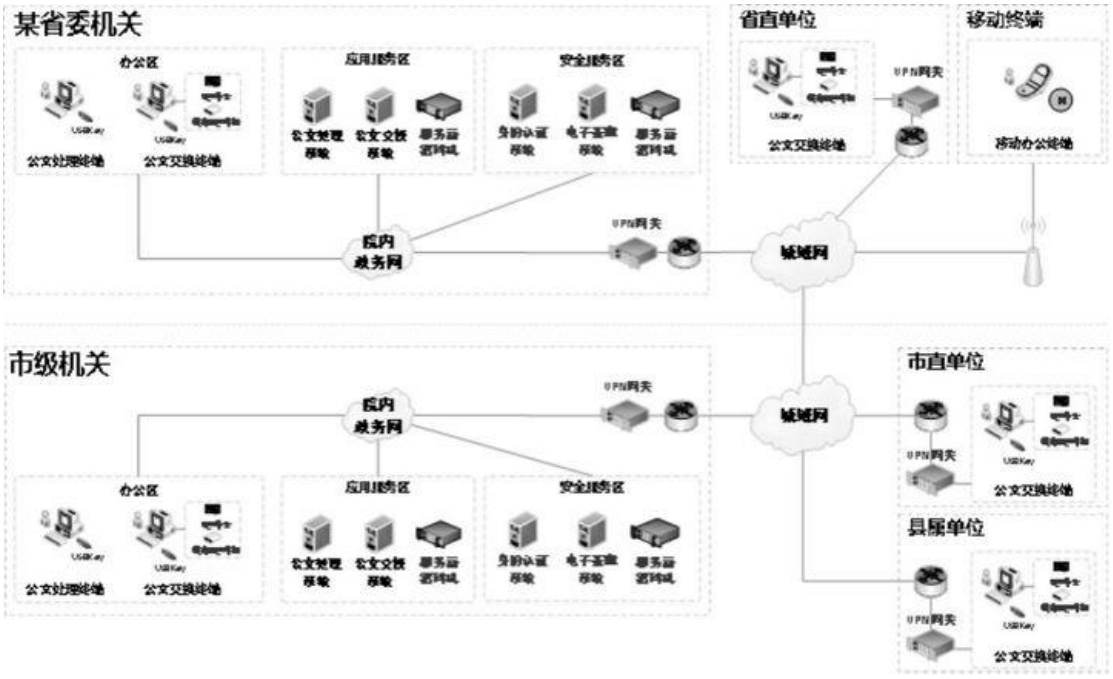


图 党政机关电子公文系统总体部署图

密码系统	主要功能
电子公文处理系统	采用集中式部署模式，在省级应用服务区、各市级应用服务区部署，为本级办公厅及业务处室提供电子公文处理功能服务。
公文处理终端	电子公文处理系统配套使用，用户使用身份认证Key进行身份认证，访问电子公文处理系统；在涉及公文签章业务的终端配置电子印章Key，实现电子公文的签章操作。
移动办公终端	电子公文处理系统移动端应用，使用专用的VPN安全应用实现远程连接电子公文处理系统。
电子公文交换系统	采用分级部署模式，在省级应用服务区和各市级应用服务区部署。实现省、市、县公文交换业务互联互通。
公文交换终端	电子公文交换系统配套使用，用户使用身份认证Key进行身份认证，访问电子公文交换系统。使用终端密码卡或终端密码机实现公文收发文件的加解密处理。
身份认证系统	在安全服务区部署，为应用系统提供身份认证服务。
电子签章系统	在安全服务区部署，为应用系统提供电子签章服务。
服务器密码机	在应用服务区和安全服务区部署，为电子公文处理系统、电子公文交换系统、身份认证系统、电子签章系统提供密码服务。
VPN网关	在网络边界部署，为通过城域网访问系统的终端或应用系统之间建立安全的信息传输通道。

物理环境安全

依托于现有的机房环境和办公环境的安全措施，利用电子门禁系统对人员身份进行确认，防止非法人员进入；利用视频监控系统对人员行为进行记录。

选用符合 GM/T 0036 标准的电子门禁系统，对人员进出记录等数据进行保护。

在视频监控系统中部署视频采集加密系统，对视频监控音像记录等数据进行保护。

网络和通信安全

在网络边界部署 VPN 网关，为通过城域网访问系统的终端或应用系统之间建立安全的信息传输通道，对网络传输的数据进行加密保护，保障网络和通信安全。

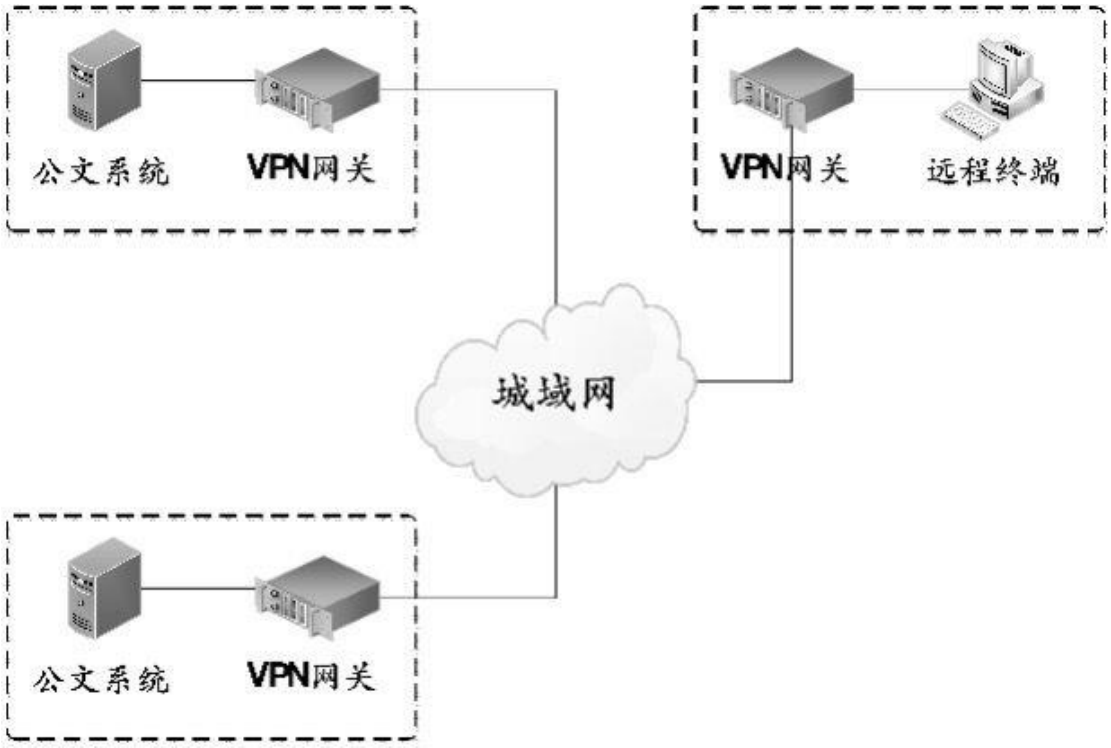


图 电子公文系统网络和通信安全密码应用方案

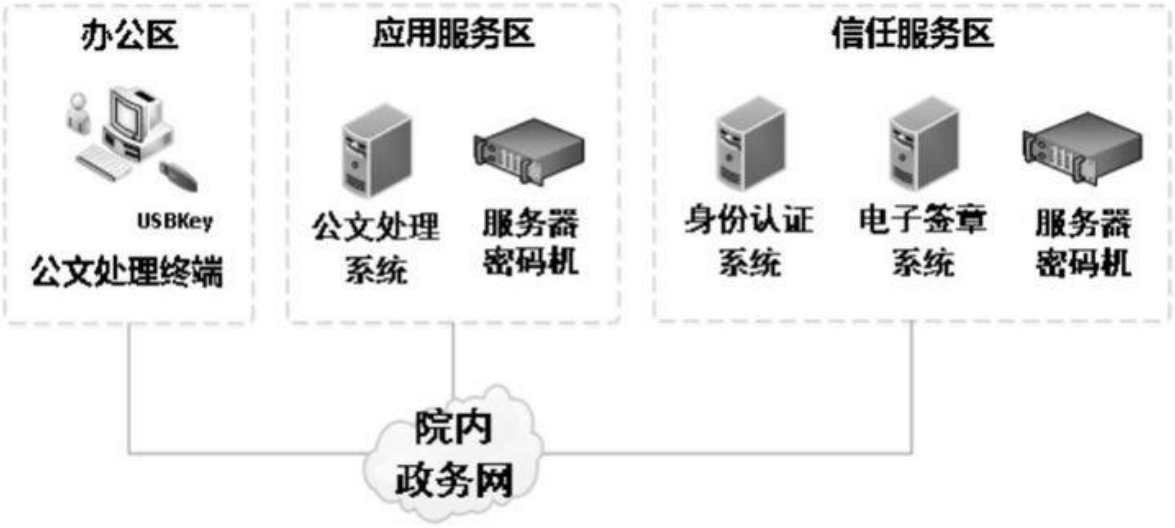
设备和计算安全

部署终端安全防护系统，结合身份认证 Key，通过数字证书方式，对登录计算机终端操作系统的用户身份进行鉴别，并对终端操作系统进行防护

应用和数据安全

1）电子公文处理系统

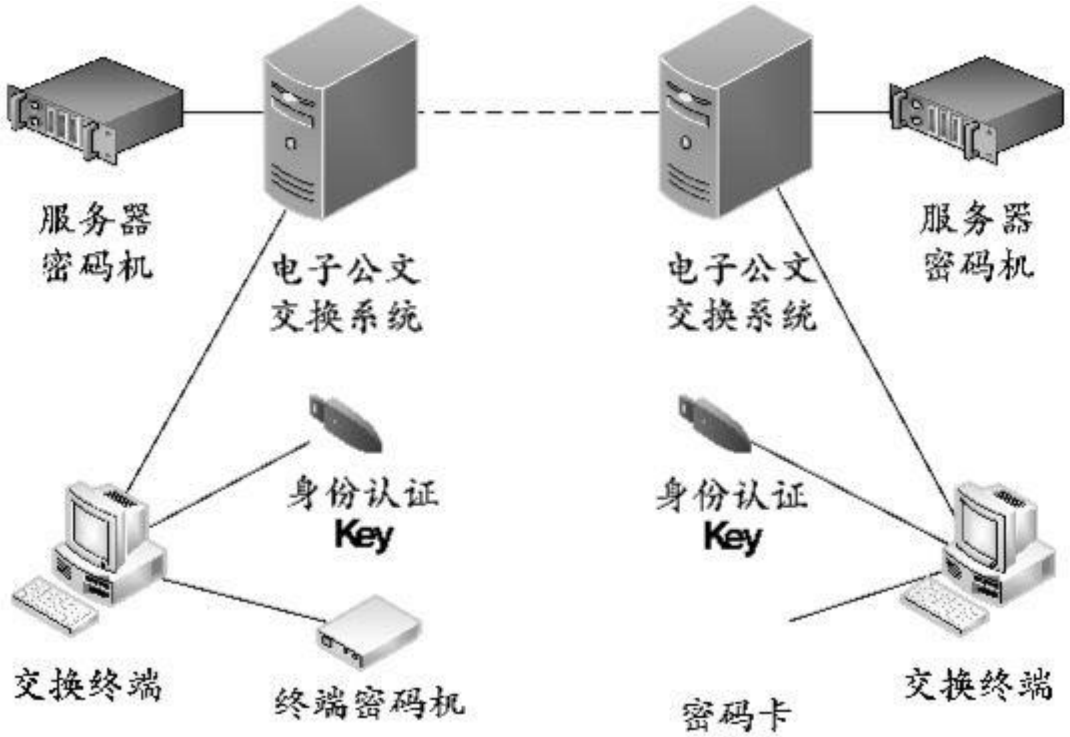
在应用服务区和安全服务区部署服务器密码机，为公文处理系统、身份认证系统以及电子签章系统提供密码支撑；在客户端配置身份认证 Key 用于鉴别用户身份，按业务需要配置电子印章 Key 用于电子公文签章。



电子公文处理系统应用和数据安全密码应用方案

2）电子公文交换系统

在电子公文交换系统服务端部署服务器密码机；在交换终端配置身份认证 Key 用于鉴别用户身份，部署终端密码机或密码卡用于电子文件的加解密。



电子公文交换系统应用和数据安全密码应用方案

4.密钥管理方案

在电子公文系统密码应用建设方案中包含密钥管理体系，**明确**密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节涉及的技术实现方式，并通过专家评审。

电子公文系统中主要用到**数字证书**，包括加密证书和签名证书，通过电子政务电子认证基础设施统一发放和管理。

电子公文系统中用到的**密码产品**，包括服务器密码机、终端密码卡/机、VPN 网关、身份认证系统、电子签章系统等。密码管理人员在密码设备投入使用前，按照密码操作规程在用户环境中对设备进行初始化，完成密钥生成；在密码产品运维管理过程中，按照密码操作规程对密钥进行备份（恢复）、归档、销毁等管理操作。

密码管理人员应按照密码操作规程对密钥存储介质进行安全管理。

5. 安全管理方案

本示例的某省委机关建立了密码安全管理制度和操作规范，覆盖密码建设、运维、人员、设备、密钥等密码管理相关内容。制度的制定、修订、发布都有明确的流程。

在电子公文系统规划设计阶段，某省委机关首先组织编制形成《某省委机关电子公文系统密码应用方案》，并组织专家进行评审；然后选用国家密码主管部门核准的硬件密码产品、采用某电子政务电子认证服务机构提供的电子认证服务，遵循《某省委机关电子公文系统密码应用方案》建设电子公文系统，并在系统通过应用安全性评估后投入运行。

某省委机关补充针对电子公文系统的密码安全管理相关制度和操作规范，并明确负责电子公文系统密码管理工作及应急处理的人员，对人员选拔、工作执行、考核、培训、调离形成相关的执行记录。在电子公文系统运行期间，密码管理工作人员遵循相关的密码安全管理制度，按照电子公文系统相关密码操作规程，对电子公文系统进行安全管理。

在《某省委机关电子公文系统密码应用方案》中包含应急处置方案，并制定了一套应急处置预案。当发生意外事件时，相关人员按照应急处置预案进行处理，并形成应急事件报告。

6. 密码产品配置清单

序号	产品名称	用途	形态	部署说明
1	身份认证系统	为应用系统提供身份认证服务	软件	在安全服务区部署
2	身份认证Key	用于终端用户身份认证	硬件	与身份认证系统配套，在所有终端部署
3	电子签章系统	为应用系统提供电子印章服务	软件	在安全服务区部署
4	电子印章Key	用于公文签章	硬件	与电子签章系统配套，在执行签章业务的终端部署
5	终端密码卡/机	用于电子公文的源数据加密和解密	硬件	在公文交换终端部署
6	服务器密码机	为应用系统提供密码服务	硬件	在应用服务区、安全服务区部署
7	VPN网关	用于建立安全的信息传输通道	硬件	在网络边界部署

电子公文系统密码产品配置清单