附录 1　政务信息系统密码应用方案模板

示例

政务信息系统密码应用方案

项目名称：

项目建设单位：

编制日期：

编制说明

1.本应用方案由项目建设单位组织编写并提交。

2.编写要求：

（1）语言规范、文字简练、重点突出、描述清晰、内容全面、附件齐全；

（2）采用 A4 幅面，上、下、左、右边距均为 2.5 厘米；正文内容仿宋四号字，1.5 倍行距；一级标题黑体三号字，二级标题楷体小三号字，三级标题仿宋四号字，各级标题均加黑；

（3）涉及到的外文缩写要注明全称；

（4）材料内容不得涉及国家秘密。

目　录

一级目录为黑体四号，二级目录为楷体四号，三级目录为仿宋小四。每级目录缩进两个字符。

1 背景

包含系统的建设规划、国家有关法律法规要求、与规划有关的前期情况概述，以及该项目实施的必要性。

2 系统概述

包含系统基本情况、系统网络拓扑、承载的业务情况、系统软硬件构成、管理制度等。

其中，系统基本情况包含系统名称、项目建设单位情况（名称、地址、所属密码管理部门、单位类型等）、系统上线运行时间、完成等保备案时间、网络安全保护等级、系统用户情况（使用单位、使用人员、使用场景等）等。

系统网络拓扑包含体系架构、网络所在机房情况、网络边界划分、设备组成及实现功能、所采取的安全防护措施等，并给出系统网络拓扑图。

承载的业务情况包含系统承载的业务应用、业务功能、信息种类、关键数据类型等。

系统软硬件构成包含服务器、用户终端、网络设备、存储、安全防护设备、密码设备等硬件资源和操作系统、数据库、应用中间件等软件设备资源。

管理制度包含系统管理机构、管理人员、管理职责、管理制度、安全策略等。

3 密码应用需求分析

结合系统安全风险控制需求，以及《基本要求》针对本政务信息系统网络安全保护等级提出的密码应用要求，对系统的密码应用需求进行分析。

对于密码应用要求在本政务信息系统中不适用的部分，做出相应的原因说明，并给出替代性措施。

4 设计目标及原则

4.1 设计目标

提出总的设计目标或分阶段设计目标。

4.2 设计原则与依据

包含方案的设计原则、所遵循的依据等，重点是所遵循的密码相关政策法规要求和《基本要求》等标准规范。

5 技术方案

5.1 密码应用技术框架

包含密码应用技术框架图及框架说明。技术框架应与第 3 章“密码应用需求”对应，根据密码应用需求设计。

5.2 物理和环境安全

描述本层密码保护的对象、采用的密码措施，包含密码子系统组成和功能、密码产品及其遵循的标准、密码服务、密码算法、密码协议、密码应用工作流程、密钥管理体系与实现等内容。

5.3 网络和通信安全

说明同 5.2。

5.4 设备和计算安全

说明同 5.2。

5.5 应用和数据安全

说明同 5.2。

5.6 密钥管理

描述系统中各密钥全生命周期涉及的密钥管理方案和使用的独立的密钥管理设备、设施（若有）。

5.7 密码应用部署

包含设备选型原则、软硬件设备清单（软硬件设备均需包含已有的密码产品清单）、部署示意图及说明等。

5.8 安全与合规性分析

针对第 3 章中安全需求的满足情况进行分析。

重点对政策法规、标准规范的符合程度进行自我评价。包含《密码应用合规性对照表》，对每一项符合性进行自评价（符合或不适用）。对于自查中不适用的项目，逐一说明其原因（比如环境约束、业务条件约束、经济社会稳定性等），并指出所对应的风险点采用了何种替代性风险控制措施来达到等效控制。

表 1 密码应用合规性对照表

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
物理和环境安全	身份鉴别			
	电子门禁记录数			

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	据完整性			
	视频记录数据完整性			
	密码模块实现			
网络和通信安全	身份鉴别			
	安全接入认证（四级）			
	访问控制信息完整性			
	通信数据完整性			
	通信数据机密性			
	集中管理通道安全			
	密码模块实现			
设备和计算安全	身份鉴别			
	远程管理身份鉴别信息机密性			
	访问控制信息完整性			
	敏感标记的完整性			
	日志记录完整性			
	重要程序或文件完整性			
	密码模块实现			
应用和数据安全	身份鉴别			
	访问控制信息和敏感标记完整性			
	数据传输机密性			
	数据存储机密性			
	数据传输完整性			
	数据存储完整性			
	日志记录完整性			
	重要应用程序的加载和卸载			
	抗抵赖（四级）			
	密码模块实现			

6 安全管理方案

包含系统采取的密码安全相关人员、制度、实施、应急等方面的管理措施。

7 实施保障方案

7.1 实施内容

根据第 5 章和第 6 章的设计内容，清晰准确地描述项目实施对象的边界及密码应用的范围、任务要求等。

实施内容包含但不限于采购、软硬件开发或改造、系统集成、综合调试、试运行等。

分析项目实施的重难点问题，提出实施过程中可能存在的风险点及应对措施。

7.2 实施计划

包含实施路线图、进度计划、重要节点等。

按照施工进度计划确定实施步骤，并分阶段描述任务分工、实施主体、项目建设单位、阶段交付物等。

7.3 保障措施

包含项目实施过程中的组织保障、人员保障、经费保障、质量保障、监督检查等措施。

7.4 经费概算

应对密码应用及应用改造项目建设和产生的相关费用进行概算，新增的密码产品和相关服务应描述产品名称和服务类型、数量等。

按照经费使用有关要求编写。