

政务领域政务服务平台
密码应用与安全性评估实施指南

中国密码学会密评联委会

二〇二四年四月

目 录

前 言.....	I
1 场景概述	1
1.1 场景相关政策要求	1
1.2 典型场景介绍	2
1.2.1 场景代表性.....	2
1.2.2 政务服务平台场景介绍	3
1.3 技术标准和指导性文件	6
2 密码应用需求	7
2.1 风险分析和安全需求	7
2.1.1 物理和环境安全	7
2.1.2 网络和通信安全	7
2.1.3 设备和计算安全	8
2.1.4 应用和数据安全	9
2.1.5 安全管理	10
2.1.6 主要保护对象	10
2.2 场景对密码应用的特殊要求	14
3 密码应用实施指南.....	14
3.1 典型场景业务的密码应用设计	14
3.1.1 物理和环境安全	15
3.1.2 网络和通信安全	16
3.1.3 设备和计算安全	16
3.1.4 应用和数据安全	16
3.1.5 密钥管理安全	17
3.1.6 安全管理	19
3.1.7 密码应用工作流程示例	20
3.2 密码产品/服务选择和部署	22
3.3 与 GB/T 39786 对照情况说明	24
3.4 注意事项	27
4 密码应用安全性评估实施指南.....	27
4.1 主要测评指标的选择和确定	27
4.2 主要测评内容	29
4.2.1 现场测评方法	29
4.2.2 测评实施	30
4.3 主要测评结果	36

4.4 注意事项	37
----------------	----

前 言

为贯彻落实《中华人民共和国密码法》《商用密码管理条例》等法律法规，促进政务领域政务服务平台场景中商用密码的合规、正确、有效应用，依据国家密码政策要求和标准规范，制定本指南。本指南可用于指导各级政务服务平台相关系统建设单位和使用单位以及商用密码应用安全性评估机构规范开展商用密码应用和安全性评估工作，也可供集成单位参考。

本指南主要依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等密码应用与安全性评估标准规范编制。本指南中任何与当前或后续发布的密码国家标准和行业标准不一致之处，以相关密码国家标准和行业标准为准。必要时本指南将根据最新的管理要求与相关技术标准进行更新。

本指南分为四章。第一章主要梳理政务服务平台典型应用场景；第二章主要对政务服务平台相关风险、密码应用需求、保护对象进行梳理；第三章主要对政务服务平台进行密码应用设计；第四章主要对政务服务平台密码应用安全性评估工作进行梳理。

本指南针对网络安全等级保护第三级信息系统密码应用要求进行设计，三级以下及四级信息系统可根据 GB/T 39786 结合系统实际进行相应调整。相关密码应用措施和技术路线不限于固定方式，政务服务平台相关建设单位和使用单位可根据自身已有密码应用基础，结合实际进行密码应用改造，以满足相关密码管理要求。

本指南主要起草单位：国家信息中心、中电科网络安全科技股份有限公司、格尔软件股份有限公司、长春吉大正元信息技术股份有限公司、中国科学院信息工程研究所、国家信息技术安全研究中心、智巡密码（上海）检测技术有限公司、西安得安信息技术有限公司、北京信安世纪科技股份有限公司、同智伟业软件股份有限公司、国家密码管理局商用密码检测中心、四川省大数据中心、海南省大数据管理局、福建省密码管理局、安徽省大数据中心。

本标准主要起草人：魏连、王笑强、杨绍亮、杜小建、李元龙、南旭东、郭宏杰、郭元元、王姁力、秦小龙、王小勇、李丹、阎亚龙、马原、魏东宾、牟杰、朱典、冯世宇、徐辉、陈天宇、吴冬宇、刘军荣、王珂、朱立通、王永起、唐鸣、宋晓勇、王泉景。

1 场景概述

1.1 场景相关政策要求

《商用密码应用安全性评估管理办法（国家密码管理局令第3号）》要求，重要网络与信息系统建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。重要网络与信息系统运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。网络与信息系统未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。未通过商用密码应用安全性评估的，运营者应当进行改造，并在改造期间采取必要措施保证网络与信息系统运行安全。

《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55号）要求，加强网络和信息安全保护。按照国家信息安全等级保护制度要求，加强各级政府网站信息安全建设，健全“互联网+政务服务”安全保障体系。明确政务服务各平台、各系统的安全责任，开展等级保护定级备案、等级测评等工作，建立各方协同配合的信息安全防范、监测、通报、响应和处置机制。加强对电子证照、统一身份认证、网上支付等重要系统和关键环节的安全监控。提高各平台、各系统的安全防护能力，查补安全漏洞，做好容灾备份。建立健全保密审查制度，加大对涉及国家秘密、商业秘密、个人隐私等重要数据的保护力度，提升信息安全支撑保障水平和风险防范能力。

《国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知》（国办函〔2016〕108号）要求，遵循国家信息安全等级保护相关规范以及国家保密管理和密码管理的有关要求，建立健全“互联网+政务服务”安全保障体系。整体考虑、顶层规划“互联网+政务服务”安全保障体系的建设，按照信息系统安全等级保护要求构建数据存储环境、应用系统环境、运行管理机制，确保政务数据安全和公民个人数据合法应用。安全保障体系要与“互联网+政务服务”应用系统同步建设，对所建安全保障体系要进行重点保护、实施动态调整。加大对平台中各类公共信息、个人隐私等重要数据的保障力度，加强平台中各类公共信息、个人隐私等重要数据的安全防护，建立数据安全规范。在系统后台对每类数据的安全属性进行必要的定义和设置，详细规定数据的开放范围和开放力度，并严格执行相应的权限管理。

《国务院关于加快推进全国一体化在线政务服务平台建设的指导意见》（国办函〔2018〕27号）要求，加强政务大数据安全管理，制定平台数据安全管理办法

法，加强对涉及国家利益、公共安全、商业秘密、个人隐私等重要信息的保护和管理。应用符合国家要求的密码技术产品加强身份认证和数据保护，优先采用安全可靠软硬件产品、系统和服务，以应用促进技术创新，带动产业发展，确保安全可控。应用基于商用密码的数字签名等技术，依托国家政务服务平台建设权威、规范、可信的国家统一电子印章系统。

《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）要求，政务信息化项目建设单位，应同步规划、同步建设、同步运行密码保障系统并定期进行评估。项目备案文件应当包括项目名称、建设单位、审批部门、绩效目标及绩效指标、投资额度、运行维护经费、经费渠道、信息资源目录、信息共享开放、应用系统、等级保护或者分级保护备案情况、**密码应用方案和密码应用安全性评估报告**等内容，其中改建、扩建项目还需提交前期项目第三方后评价报告。国家政务信息化项目建成后半年内，项目建设单位应当按照国家有关规定申请审批部门组织验收，提交验收申请报告时应当一并附上项目建设总结、财务报告、审计报告、安全风险评估报告、**密码应用安全性评估报告**等材料。对于不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统，不安排运行维护经费，项目建设单位不得新建、改建、扩建政务信息系统。各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用**密码技术，并定期开展密码应用安全性评估**，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。

《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）要求，加强关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查，提升数字政府领域关键信息基础设施保护水平。

《全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102号）要求，形成制度规范、技术防护和运行管理三位一体的全国一体化政务大数据安全保障体系。

1.2 典型场景介绍

1.2.1 场景代表性

政务服务平台是建设“数字政府”的重要组成，是政府机关面向办事群众提供政务服务的重要环节。截至目前，各省（区、市）人民政府、国务院有关部门普遍建成网上政务服务平台，已经形成了覆盖全国的整体联动、部门协同、省级统筹、一网办理的“互联网+政务服务”技术和服务体系，实现政务服务的标准化、精准化、便捷化、平台化、协同化，政务服务流程显著优化，服务形式更加多元，服务渠道更为畅通，群众办事满意度显著提升。

在基于大数据技术的政务数据全面共享背景下，各级政务服务平台的数据安全体系并未有效打通，数据安全边界消失，公民个人隐私数据、企业商业秘密数

据等重要数据泄露的威胁日益加剧，需要利用密码技术建立统一的数据安全支撑体系，保障政务服务数据在流转和使用中得到有效的管控。

1.2.2 政务服务平台场景介绍

政务服务平台是各级政务服务实施机构运用互联网、大数据、云计算等技术手段，整合各类政务服务事项和业务办理等信息，通过网上大厅、办事窗口、移动客户端、自助终端等多种形式，结合第三方平台，为自然人和法人提供一站式办理的政务服务的网上服务平台。

政务服务平台体系由国家级平台、省级平台、地市级平台三个层级组成，各层级之间通过政务服务数据共享平台进行资源目录注册、信息共享、业务协同、监督考核、统计分析等，实现政务服务事项就近能办、同城通办、异地可办。政务服务平台层级体系如图 1 所示。

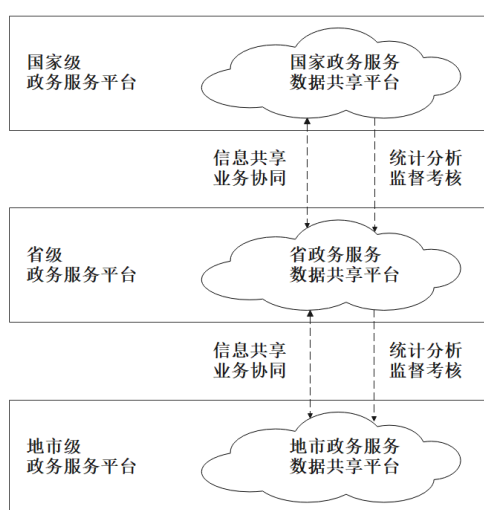


图 1 政务服务平台层级体系图

政务服务平台主要由互联网政务服务门户、政务服务管理平台、业务办理系统和政务服务数据共享平台四部分构成。平台各组成部分之间需实现数据互联互通，各组成部分之间的业务流、信息流如图 2 所示。

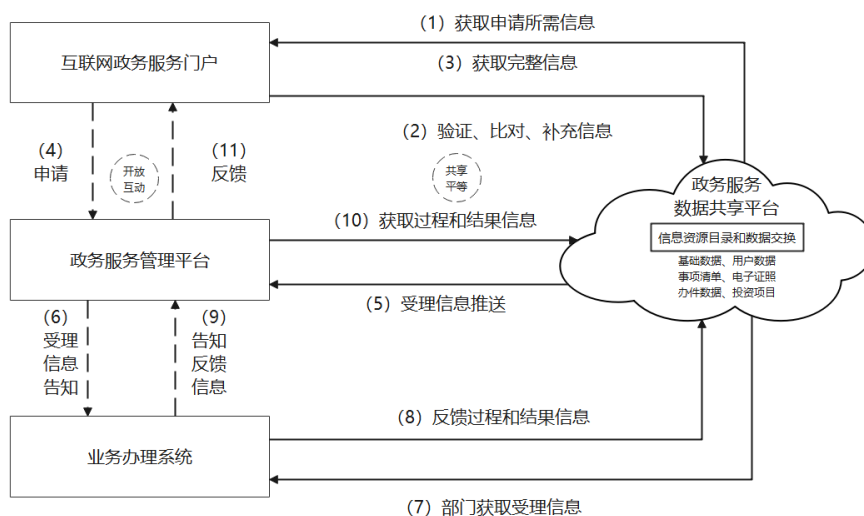


图 2 政务服务平台系统组成图

互联网政务服务门户统一展示、发布政务服务信息，接受自然人、法人的政务服务申请信息，经与政务服务数据共享平台进行数据验证、比对和完善后，发送至政务服务管理平台进行处理，将相关受理、办理和结果信息反馈申请人。

政务服务管理平台把来自互联网政务服务门户的申请信息推送至政务服务数据共享平台，同步告知业务办理系统；政务服务管理平台从政务服务数据共享平台获取并向互联网政务服务门户推送过程和结果信息，考核部门办理情况。

业务办理系统在政务服务数据共享平台取得申请信息和相关信息后进行业务办理，将办理过程和结果信息推送至政务服务数据共享平台，同步告知政务服务管理平台。

政务服务数据共享平台汇聚政务服务事项、电子证照等数据，以及来自互联网政务服务门户的信息、政务服务管理平台受理信息、业务办理系统办理过程和结果，实现与人口、法人等基础信息资源库的共享利用。

政务服务平台技术架构由基础设施层、数据资源层、应用支撑层、业务应用层、用户及服务层五个层次组成，政务服务平台技术架构如图 3 所示。

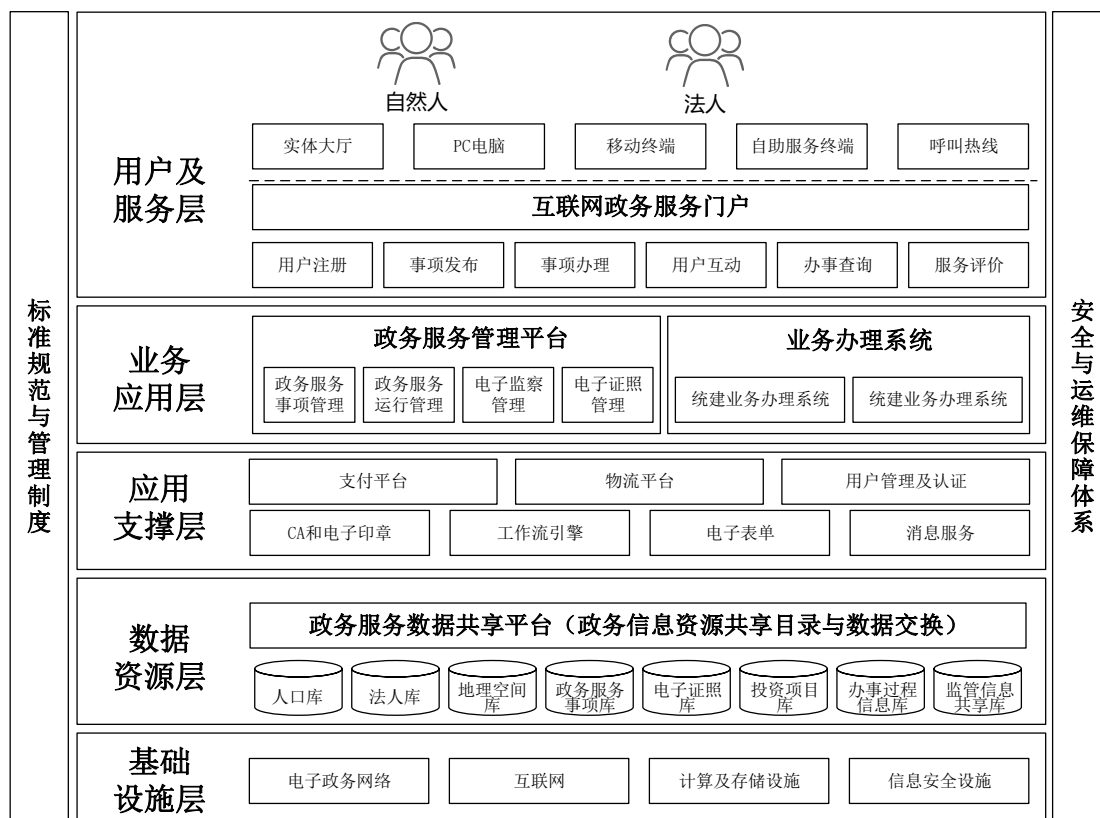


图 3 政务服务平台技术架构图

政务服务业务办理全过程依托政务服务数据共享平台支撑，业务数据在互联网政务服务门户、政务服务管理平台、业务办理系统之间流转，政务服务平台具体全过程业务流程示意图如图 4 所示。

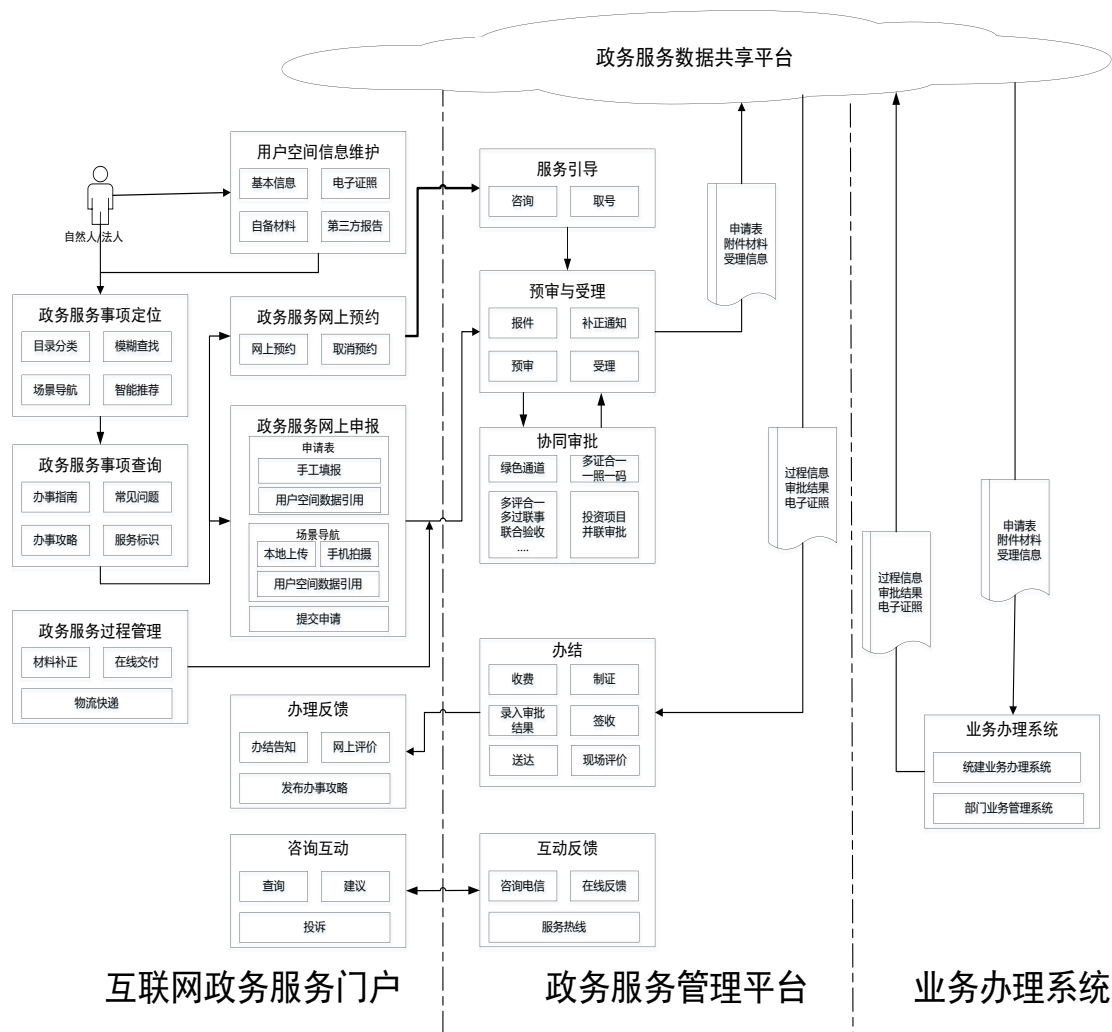


图 4 政务服务平台业务流程图

用户注册登录、用户空间信息维护、政务服务事项定位和查询，以及政务服务的网上预约、申请、过程管理、办理反馈和互动咨询功能在互联网政务服务门户实现；服务引导、政务服务事项受理、协同审批、事项办结和互动反馈功能在政务服务管理平台实现。业务办理系统对申请表、附件材料、受理信息的抓取，对过程信息、审批结果和电子证照的发送通过政务服务数据共享平台完成。

政务服务平台典型场景业务流程如表 1 所示。

表 1 政务服务平台典型场景业务流程

序号	业务名称	业务流程描述
1	信息发布	政务部门通过互联网政务服务门户，统一展示、发布政务服务信息。
2	前台业务受理	自然人、法人通过政务服务门户提交政务服务申请信息。
3	政务数据共享交换	政务部门通过政务服务数据共享平台开展跨部门政务数

		据、政务服务事项办理信息的共享交换。
4	后台业务办理	政务人员通过后台业务办理系统进行业务办理审批、电子证照制作发放。

1.3 技术标准和指导性文件

本文件参考的技术标准和指导性文件如下：

- GB/T 20518-2018 《信息安全技术 公钥基础设施 数字证书格式规范》
- GB/T 25056-2018 《信息安全技术 证书认证系统密码及其相关安全技术规范》
- GB/T 32905-2016 《信息安全技术 SM3 密码杂凑算法》
- GB/T 32907-2016 《信息安全技术 SM4 分组密码算法》
- GB/T 33560-2017 《信息安全技术 密码应用标识规范》
- GB/T 35276-2017 《信息安全技术 SM2 密码算法使用规范》
- GB/T 35291-2017 《信息安全技术 智能密码钥匙应用接口规范》
- GB/T 36322-2018 《信息安全技术 密码设备应用接口规范》
- GB/T 36968-2018 《信息安全技术 IPsec VPN 技术规范》
- GB/T 37033-2018 《信息安全技术 射频识别系统密码应用技术要求》
- GB/T 37092-2018 《信息安全技术 密码模块安全要求》
- GB/T 38540-2020 《信息安全技术 安全电子签章密码技术规范》
- GB/T 38556-2020 《信息安全技术 动态口令密码应用技术规范》
- GB/T 38629-2020 《信息安全技术 签名验签服务器技术规范》
- GB/T 38636-2020 《信息安全技术 传输层密码协议（TLCP）》
- GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
- GM/T 0018-2012 《密码设备应用接口规范》
- GM/T 0024-2014 《SSL VPN 技术规范》
- GM/T 0025-2014 《SSL VPN 网关产品规范》
- GM/T 0026-2014 《安全认证网关产品规范》
- GM/T 0027-2014 《智能密码钥匙技术规范》
- GM/T 0030-2014 《服务器密码机技术规范》
- GM/T 0036-2014 《采用非接触卡的门禁系统密码应用技术指南》
- GM/T 0050-2016 《密码设备管理 设备管理技术规范》
- GM/T 0051-2016 《密码设备管理 对称密钥管理技术规范》
- GM/T 0104-2021 《云服务器密码机技术规范》
- GM/T 0115-2021 《信息系统密码应用测评要求》
- GM/T 0116-2021 《信息系统密码应用测评过程指南》
- GM/Y 5001-2019 《密码标准应用指南》
- GM/Y 5002-2018 《云计算身份鉴别服务密码标准体系》
- GM/Z 4001-2013 《密码术语》

- GW 0013-2017 《政务云安全要求》
- GW 0202-2014 《国家电子政务外网安全接入平台技术规范》
- GW 0206-2014 《接入政务外网的局域网安全技术规范》
- 《信息系统密码应用高风险判定指引》
- 《商用密码应用安全性评估量化评估规则》
- 《商用密码安全性评估 FAQ》

2 密码应用需求

2.1 风险分析和安全需求

2.1.1 物理和环境安全

(一)风险分析

(1) 存在非法人员进入政务服务平台所在物理机房等重要物理环境，对软硬件设备和数据进行直接破坏的风险。

(2) 存在政务服务平台所在物理机房等重要物理环境电子门禁进出记录和视频监控记录遭到篡改，非法人员进出情况被掩盖的风险。

(二)密码应用需求

(1) 部署符合 GM/T 0036 等标准的电子门禁系统，采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对进入政务服务平台所在物理机房等重要物理区域人员进行身份鉴别。

(2) 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对政务服务平台所在物理区域的视频监控音像记录数据及电子门禁系统进出记录等数据进行存储完整性保护。

2.1.2 网络和通信安全

(一)风险分析

(1) 浏览器与业务系统、政务服务 App 与互联网政务服务门户、VPN 客户端与 VPN 网关、各级政务服务平台之间、政务服务数据共享平台与政务信息系统等通信信道存在非法通信实体接入网络的风险。

(2) 数据在各网络通信信道传输过程中存在被篡改的风险。

(3) 重要数据在各网络通信信道传输过程中存在被非授权截取的风险。

(4) 网络边界的 VPN 中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等进行网络边界访问控制的信息存在被篡改，导致非法通信实体接入网络的风险。

(5) 非法设备从外部接入内部网络，或网络边界被破坏的风险。

(二)密码应用需求

(1) 采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码

(MAC) 机制、基于公钥密码算法的数字签名机制等密码技术对浏览器与业务系统、政务服务 App 与互联网政务服务门户、VPN 客户端与 SSL VPN、各级政务服务平台之间、政务服务数据共享平台与政务信息系统等通信信道中的通信实体进行身份鉴别，保证通信实体身份的真实性。

(2) 采用基于对称密码算法或密码杂凑算法的消息鉴别码 (MAC) 机制、基于公钥密码算法的数字签名机制等密码技术对申请人通过 PC 端登录到互联网、申请人通过移动端登录到互联网、办公人员通过 PC 端登录到政务外网、办公人员通过移动端登录到政务外网、运维管理通道及互联网与政务外网之间等通信通道通信过程中的数据进行完整性保护。

(3) 采用密码技术的加解密功能对申请人通过 PC 端登录到互联网、申请人通过移动端登录到互联网、办公人员通过 PC 端登录到政务外网、办公人员通过移动端登录到政务外网、运维管理通道及互联网与政务外网之间等通信通道通信过程中的重要数据进行机密性保护。

(4) 采用基于对称密码算法或密码杂凑算法的消息鉴别码 (MAC) 机制、基于公钥密码算法的数字签名机制等密码技术对网络边界的 VPN 中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等网络边界访问控制信息进行完整性保护。

(5) 采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码 (MAC) 机制、基于公钥密码算法的数字签名机制等密码技术对从外部连接到内部网络的设备进行接入认证。

“安全接入认证”指标在 GB/T 39786 中针对网络安全等级保护第三级信息系统要求为“可”，建设单位和使用单位可结合实际情况自行决定是否纳入标准符合性测评范围。

2.1.3 设备和计算安全

(一) 风险分析

(1) 政务服务平台通用设备、网络及安全设备、密码设备、各类虚拟设备等设备、数据库管理系统存在被非法人员登录的风险。

(2) 远程管理政务服务平台中各类物理及虚拟设备时，存在搭建的远程管理通道被非法使用，或传输的管理数据被非授权获取和篡改的风险。

(3) 设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等被篡改，导致设备资源被登录设备的其他用户获取的风险。

(4) 通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要信息资源安全标记存在被篡改的风险。

(5) 通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的日志记录存在被篡改，以掩盖非法操作的风险。

(6)通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要可执行程序及政务服务 App 存在被篡改或来源不可信的风险。

(二)密码应用需求

(1)采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

(2)采用密码技术建立安全的信息传输通道，实现对远程管理人员的身份鉴别，以及传输数据的机密性和完整性保护。

(3)采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等进行完整性保护。

(4)采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要信息资源安全标记进行完整性保护（根据密码应用方案决定是否纳入）。

(5)采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的日志记录进行完整性保护。

(6)采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要可执行程序及政务服务 App 进行完整性保护并实现其来源的真实性保护。

2.1.4 应用和数据安全

(一)风险分析

(1)互联网政务服务门户、政务服务数据共享平台、业务办理系统等业务系统存在被非法人员登录的风险。

(2)应用系统的权限、标签等能够决定系统应用访问控制的措施等信息存在被篡改，导致应用资源被登录应用的其他用户获取的风险。

(3)政务服务平台的重要信息资源安全标记存在被篡改的风险。

(4)政务服务平台中传输或存储的重要数据被外部攻击者非法获取或篡改的风险。

(5)自然人、法人的政务事项申请行为、政务人员的业务办理审批行为等关键行为中，数据发送者或接收者不承认发送或接受到数据，或者否认其所做的操作的风险。

(6)政务服务平台的重要业务日志存在被篡改，导致非法操作被掩盖的风险。

(7) 互联网政务服务门户统一展示、发布的政务服务信息及业务办理入口等发布内容存在被篡改的风险。

(二) 密码应用需求

(1) 采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，在自然人、法人登录互联网政务服务门户时、政务人员登录业务办理系统时、政务人员登录政务服务数据共享平台时、系统管理员登录应用系统时对登录用户进行身份鉴别。

(2) 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对应用系统的权限、标签等能够决定系统应用访问控制的措施等信息进行完整性保护。

(3) 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对信息系统应用的重要信息资源安全标记做完整性保护（根据密码应用方案决定是否纳入）。

(4) 采用密码技术的加解密功能，对政务服务平台中的鉴别数据、重要业务数据、重要审计数据、个人敏感信息等重要数据进行传输和存储过程中的机密性保护。

(5) 采用基于公钥密码算法的数字签名机制等密码技术，对自然人、法人的政务事项申请行为、政务人员的业务办理审批行为等关键行为进行签名，实现数据原发行为和接收行为的不可否认性。

(6) 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对政务服务平台的重要业务日志做完整性保护。

(7) 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对信息系统应用中的鉴别数据、重要业务数据、重要审计数据、个人敏感信息等重要数据进行传输和存储过程中的完整性保护；对互联网政务服务门户统一展示、发布的政务服务信息及业务办理入口等发布内容进行完整性保护。

2.1.5 安全管理

(一) 风险分析

政务服务平台密钥管理规则、安全管理制度、管理流程不健全，执行不到位，职责不明确等，存在密码未进行合规、正确、有效使用的风险。

(二) 密码应用需求

制定密码应用方案，并委托密评机构或组织专家对密码应用方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度；系统改造完成后，委托密评机构对系统进行密码应用安全性评估。

2.1.6 主要保护对象

政务服务平台主要保护对象如表 2 所示。

表 2 政务服务平台主要保护对象

序号	相关业务	保护对象	保护对象描述	安全需求
1	业务受理 / 数据共享 / 业务办理	身份鉴别信息	1) 自然人、法人登录互联网政务服务门户的口令。 2) 政务人员登录业务办理系统的口令。 3) 政务人员登录政务服务数据共享平台的口令。 4) 系统管理员登录应用系统的口令。 5) 管理人员登录堡垒机、应用/数据库服务器等设备的口令。 6) 如果涉及动态口令、短信验证码等身份鉴别方式，还应注意对相关一次性口令的传输机密性保护，防止中间人攻击。	<input type="checkbox"/> 真实性 <input checked="" type="checkbox"/> 传输机密性 <input checked="" type="checkbox"/> 存储机密性 <input checked="" type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
		信息系统应用中的重要数据	1) 重要业务数据 2) 重要审计数据 3) 个人敏感信息	<input type="checkbox"/> 真实性 <input checked="" type="checkbox"/> 传输机密性 <input checked="" type="checkbox"/> 存储机密性 <input checked="" type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
		日志记录	1) 通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的日志记录。 2) 政务服务平台的重要业务日志。	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
		访问控制信息	1) 网络边界的 VPN 中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等进行网络边界访问控制等信息。 2) 设备操作系统的系统权限访问控制信息、系统文件目录的访问控制	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性

		<p>信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等。</p> <p>3) 应用系统的权限、标签 等能够决定系统应用访问控制的措施等信息。</p>	
	互联网政务服务门户内容	<p>互联网政务服务门户统一展示、发布的政务服务信息及业务办理入口。</p>	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input checked="" type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
	重要信息资源安全标记	<p>1) 通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要信息资源安全标记。</p> <p>2) 政务服务平台中的重要信息资源安全标记。</p>	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
	重要可执行程序	<p>通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要可执行程序。</p>	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input checked="" type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
	视频监控音像记录	<p>政务服务平台所在物理机房等重要物理区域的视频监控音像记录。</p>	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
	电子门禁系统进出记录	<p>政务服务平台所在物理机房等重要物理区域的电子门禁系统的进出记录。</p>	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input checked="" type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性

		<p>进入重要物理区域的人员的身份鉴别</p>	<p>进入政务服务平台所在物理机房等重要物理区域人员的身份鉴别。</p>	<p><input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性</p>
		<p>通信双方的身份鉴别</p>	<p>1) 浏览器与业务系统通信信道的身份鉴别。 2) 政务服务 App 与互联网政务服务门户通信信道的身份鉴别。 3) VPN 客户端与 SSL VPN 通信信道的身份鉴别。 4) 各级政务服务平台之间通信信道的身份鉴别。 5) 政务服务数据共享平台与政务信息系统通信信道的身份鉴别。</p>	<p><input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性</p>
		<p>网络设备接入时的身份鉴别</p>	<p>从外部连接到内部网络的设备接入认证时的身份鉴别。</p>	<p><input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性</p>
		<p>登录操作系统和数据库系统的用户身份鉴别</p>	<p>管理人员登录通用设备、网络及安全设备、密码设备、各类虚拟设备等设备、数据库管理系统的身份鉴别。</p>	<p><input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性</p>

		重要可执行程序来源	1) 通用设备、网络及安全设备、密码设备、各类虚拟设备等设备中的重要可执行程序来源。 2) 政务服务 App 来源。	<input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
		应用系统的用户的身份鉴别	1) 自然人、法人登录互联网政务服务门户的身份鉴别。 2) 政务人员登录业务办理系统的鉴别。 3) 政务人员登录政务服务数据共享平台的身份鉴别。 4) 系统管理员登录应用系统的身份鉴别。	<input checked="" type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
		数据原始行为、数据接收行为	1) 自然人、法人的政务事项申请行为。 2) 政务人员的业务办理审批行为。	<input type="checkbox"/> 真实性 <input type="checkbox"/> 传输机密性 <input type="checkbox"/> 存储机密性 <input type="checkbox"/> 传输完整性 <input type="checkbox"/> 存储完整性 <input checked="" type="checkbox"/> 不可否认性

2.2 场景对密码应用的特殊要求

政务服务平台中的互联网政务服务门户（前台业务受理），面向数量庞大的自然人、法人用户，全部使用合规的商用密码技术解决用户身份鉴别、传输机密性、完整性存在资源消耗大、用户体验无法保障的实际困难。

政务服务平台可能存在跨越不同的物理机房以及跨越不可控区域的情况，需保证密码设备调用的安全性。

政务服务平台涉及业务办理系统众多，业务交叉点繁杂，密码应用改造周期长、改造范围广，且政务服务是政府机关面向办事群众提供政务服务的重要环节，业务不可中断，若出现上下级密码应用建设不同步的情况，可能存在数据无法读取或使用，政务服务无法保障的问题。

3 密码应用实施指南

3.1 典型场景业务的密码应用设计

政务服务平台整体密码应用设计框架如图 5 所示：

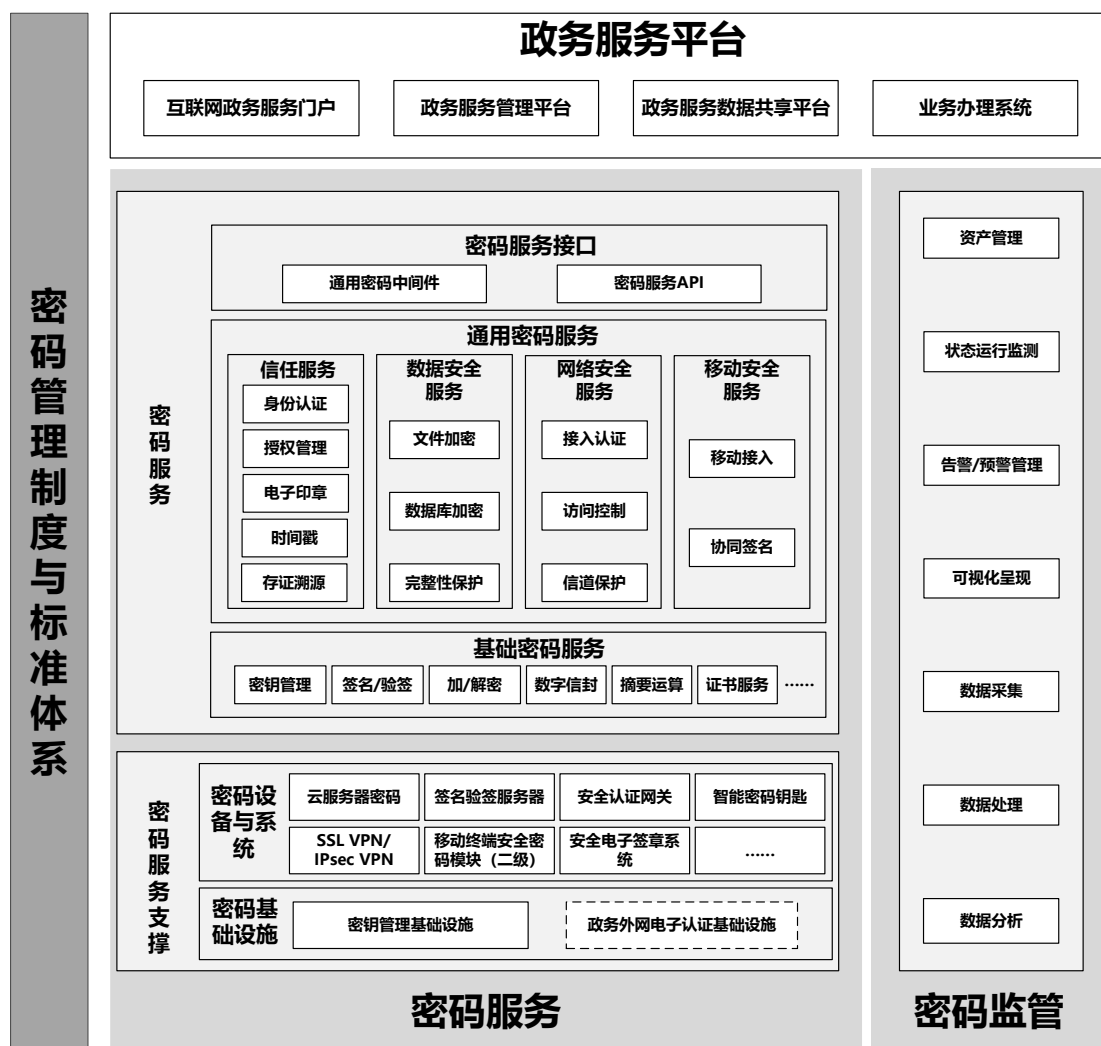


图 5 政务服务平台密码应用设计图

依托密钥管理、电子认证基础设施，结合各类密码设备与系统等密码产品，为政务服务平台提供基础及通用密码服务，满足政务服务平台密码应用需求。对接各类密码产品实现密码资产、运行状态、密码应用情况等监测能力，满足政务外网密码监管需求，形成政务外网一体化密码应用监管能力，输出至国务院办公厅、国家密码管理局等主管部门。

3.1.1 物理和环境安全

在政务服务平台物理机房等重要物理区域部署符合 GB/T 37033 标准、GM/T 0036 等标准的电子门禁系统，对进入物理区域人员身份进行鉴别。

部署视频加密系统或使用符合相关国家、行业标准要求的服务器密码机、签名验签服务器，对视频监控系统视频记录进行完整性保护。

电子门禁系统自身实现或使用符合相关国家、行业标准要求的服务器密码机、签名验签服务器，对电子门禁进出记录进行完整性保护。

3.1.2 网络和通信安全

在政务服务平台的网络边界建议部署符合 GM/T 0024、GM/T 0025 标准的 SSL VPN 网关，在客户端部署 VPN 客户端及符合 GM/T 0027 标准的智能密码钥匙或符合 GB/T 38556 标准的动态令牌，通过 VPN 对客户端进行身份鉴别，实现政务人员和运维管理人员的跨网接入认证、传输信道加密和完整性保护。

在政务数据共享平台、业务办理系统服务端部署服务器证书，可在客户端部署国密浏览器，使用合规的 SSL 协议，实现客户端对应用系统的身份鉴别（或双向身份鉴别）、传输信道机密性和完整性保护。若采用基于商用密码的数字证书，密钥的安全性应由签名验签服务器、服务器密码机、网关、密码卡等合规的密码产品保证。

在互联网政务服务门户服务端部署服务器证书，使用合规的 SSL 协议，实现自然人/法人 PC 端、移动端对应用系统的身份鉴别、传输信道加密和完整性保护。

在各级政务服务平台网络边界部署符合 GB/T 36968 标准的 IPsec VPN，实现政务数据共享平台之间通信信道的身份鉴别、传输加密和完整性保护。

可在政务服务平台中部署符合密码相关国家、行业标准要求的服务器密码机或签名验签服务器，对网络边界的 VPN 中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等网络边界访问控制信息进行完整性保护。

3.1.3 设备和计算安全

目前应用服务器、数据库服务器、数据库管理系统等通用设备的身份鉴别采用密码技术实现难度较大，可部署符合 GM/T 0024、GM/T 0025 标准的 SSL VPN 或符合 GM/T 0026 标准的安全认证网关或符合 GB/T 38556 标准的动态令牌认证系统对接堡垒机，或部署通过商用密码检测认证的堡垒机，设备运维管理人员通过使用智能密码钥匙或动态令牌实现登录堡垒机的身份鉴别，通过堡垒机统一运维管理设备。设备运维管理人员通过使用智能密码钥匙或动态令牌实现密码设备的本地运维管理。

在堡垒机部署服务器证书，在运维终端部署国密浏览器或网关客户端，使用合规的 SSL 协议建立安全管理数据传输通道。

在政务服务平台中部署符合密码相关国家、行业标准要求的服务器密码机或签名验签服务器，对设备访问控制信息、日志记录、重要可执行程序（重要信息资源安全标记根据密码应用方案决定是否纳入）等进行完整性保护。

通用设备、网络及安全设备、各类虚拟设备等设备中的重要可执行程序更新、升级以及政务服务 App 下载安装，提供者进行数字签名以实现其来源的真实性保护。

3.1.4 应用和数据安全

可在自然人/法人移动端政务服务 App 中部署符合 GM/T 0028 的标准的移动终端安全密码模块（二级），在服务端部署安全认证网关、协同签名系统向用

户发放数字证书，实现公众用户的移动端政务服务 App 登录、PC 端网上办事大厅登录。在政务服务平台服务端部署安全认证网关或动态令牌认证系统，政务人员和系统管理员通过使用智能密码钥匙或动态令牌或移动终端安全密码模块实现应用系统登录。

在政务服务平台服务端部署服务器密码机或签名验签服务器，对应用系统的访问控制信息、重要业务日志、重要数据（重要信息资源安全标记根据密码应用方案决定是否纳入）进行存储完整性保护。

在政务服务平台服务端部署密钥管理系统、服务器密码机、数据库加密系统、加密数据库系统、密码卡、密码模块等，对应用系统的重要数据进行存储机密性保护。

政务人员通过 PC 端智能密码钥匙，应用服务端通过密码设备可对系统中的重要数据封装数字信封，实现重要数据传输过程中的机密性、完整性保护。

若存在政务人员使用移动端进行移动办公的场景，可通过移动端使用移动终端安全密码模块，应用服务端使用密码设备，对系统中的重要数据封装数字信封的方式，实现重要数据传输过程中的机密性、完整性保护。

政务服务平台服务端部署符合 GM/T 38540 标准的电子签章系统、符合 GM/T 0033 标准的时间戳服务器，客户端通过移动终端安全密码模块、智能密码钥匙等对自然人、法人的政务事项申请行为、政务人员的业务办理审批行为等关键行为进行数字签名，实现数据原发行为、数据接收行为的不可否认性。

采用密码技术对互联网政务服务门户统一展示、发布的政务服务信息及业务办理入口等发布内容进行完整性保护。

3.1.5 密钥管理安全

系统密钥管理由密钥管理系统完成，为政务服务平台系统提供密钥的生成、分发、存储、备份、归档、恢复、更新、销毁等密钥的全生命周期的管理。密钥管理的设计遵循 GM/T 0038、GM/T 0050、GM/T 0051 等标准。

采用通过认证的随机数发生器在可控环境中生成密钥或密钥协商过程中的随机值，并在密钥协商之前及协商过程中验证对方身份的真实性。

使用带有访问控制机制的存储介质传输明文密钥，或指定相关管理制度以保证密钥在分发过程中的安全性，若密钥在不可控环境中分发，需使用密码技术保护密钥的机密性和完整性。

密钥在存储过程中，加密密钥的口令应以密文存储，除公钥外的密钥在不可控环境中需以密文形式存储，并保证密钥不被非授权的访问、使用、泄露、修改和替换。

规范密钥的使用及管理，按照密钥用途正确使用密钥，防止出现因操作不当导致的密钥泄露问题。公钥在使用过程中需与实体间存在关联关系，可使用经过完备的公钥验证机制的 PKI 技术进行关联，若存在多个实体使用密钥的场景，需要建立完备的密钥使用控制机制。

需建立密钥已泄露或存在泄露风险时的密钥更新、销毁/撤销机制及密钥恢复使用时的鉴别机制。

政务服务平台包括对称和非对称两种密钥体系，密码产品内部工作流程涉及的密钥管理策略不做描述。

(1) 对称密钥体系

政务服务平台涉及到的主要对称密钥包括数据加密密钥及 MAC 密钥，对称密钥的全生命周期管理如表 3 所示。

表 3 对称密钥列表

序号	密钥名称	产生	分发	存储	使用	导入和导出	归档	备份和恢复	销毁
1	网络传输加密密钥	按照标准握手协议协商生成	不涉及该密钥的分发	存储在密码设备易失性存储介质中	在密码设备内使用	不涉及该密钥的导入和导出	不涉及该密钥的归档	不涉及该密钥的备份和恢复	在连接断开或设备断电时应销毁
2	应用传输加密密钥	在密码设备内产生	经非对称密钥加密后分发	使用完后销毁不涉及存储	在密码设备内使用	不涉及该密钥的导入和导出	不涉及该密钥的归档	不涉及密钥备份和恢复	在密码设备内完成销毁
3	数据存储加密密钥	在密码设备内产生	不涉及该密钥的分发	在密码设备中存储	在密码设备内使用	不涉及该密钥的导入和导出	不涉及该密钥的归档	利用密码设备自身的密钥备份和恢复机制实现	在密码设备内完成销毁
4	MAC 密钥	在密码设备内产生	不涉及该密钥的分发	在密码设备中存储	在密码设备内使用	不涉及该密钥的导入和导出	不涉及该密钥的归档	利用密码设备自身的密钥备份和恢复机制实现	在密码设备内完成销毁

(2) 非对称密钥体系

政务服务平台涉及到的非对称密钥包括：用户签名密钥对、用户加密密钥对、服务器签名密钥对及服务器加密密钥对，非对称密钥的全生命周期管理如表 4 所示。

表 4 非对称密钥列表

序号	密钥名称	产生	分发	存储	使用	导入和导出	归档	备份和恢复	销毁
----	------	----	----	----	----	-------	----	-------	----

1	用户签名私钥	在智能密码钥匙内生成	不进行分发	在智能密码钥匙内存储	在智能密码钥匙内使用	不进行导入和导出	不涉及该密钥的归档	不涉及该密钥的备份和恢复	在智能密码钥匙内部销毁
2	用户签名公钥	在智能密码钥匙内生成	以证书形式分发	以证书形式存储	以证书形式使用	以证书形式导入和导出	以证书形式归档	以证书形式备份恢复	由 CA 进行撤销
3	用户加密私钥	由 CA 生成	由 CA 以离线方式进行分发	在智能密码钥匙内存储	在智能密码钥匙内使用	由签名密钥进行加密后导入	由 CA 归档	由 CA 进行备份和恢复	在智能密码钥匙内部销毁
4	用户加密公钥	由 CA 生成	以证书形式分发	以证书形式存储	以证书形式使用	以证书形式导入和导出	以证书形式归档	以证书形式备份恢复	由 CA 进行撤销
5	服务器签名私钥	在密码设备内生成	不进行分发	在密码设备内存储	在密码设备内使用	不进行导入和导出	不涉及该密钥的归档	不涉及该密钥的备份和恢复	在密码设备内部销毁
6	服务器签名公钥	在密码设备内生成	以证书形式分发	以证书形式存储	以证书形式使用	以证书形式导入和导出	以证书形式归档	以证书形式备份恢复	由 CA 进行撤销
7	服务器加密私钥	由 CA 生成	由 CA 以离线方式进行分发	在密码设备内存储	在密码设备内使用	由签名密钥进行加密后导入	由 CA 归档	由 CA 进行备份和恢复	在密码设备内部销毁
8	服务器加密公钥	由 CA 生成	以证书形式分发	以证书形式存储	以证书形式使用	以证书形式导入和导出	以证书形式归档	以证书形式备份恢复	由 CA 进行撤销

3.1.6 安全管理

根据 GB/T 39786 中安全管理相关要求，结合部门已有制度，制定完善政务服务平台相关安全管理制度、密钥管理规则及应急处置预案，根据制度执行，并定期开展密码应用安全性评估及攻防对抗演习。

密码应用安全管理制度至少应包含密钥管理规则、操作规程、发布流程、岗位职责、上岗人员培训、安全岗位人员考核、关键岗位人员保密和调离等相关内容。

建设运行阶段应制定密码应用方案、密钥安全管理策略、实施方案，投入运行前应进行密码应用安全性评估。

应严格根据相关制度执行并对相关过程记录进行留存。如：

- a) 建立政务服务平台的安全管理机构，分配各部门安全管理职责，制定机构安全管理制度及策略；
- b) 明确政务服务平台管理人员组成，分配职责，制定人员安全管理策略，明确各管理员的岗位职责和作业流程；
- c) 制定政务服务平台的机房及办公区等物理环境密码应用的安全管理策略；
- d) 制定政务服务平台的介质、设备等密码应用的安全管理策略；
- e) 制定政务服务平台的运行安全管理策略；
- f) 针对所有设备相关的安全策略定期或不定期备份，并制定管理办法；
- g) 制定政务服务平台的安全事件处置和应急管理策略。

3.1.7 密码应用工作流程示例

本章节对常见密码应用工作流程进行举例说明，相关密码技术、密码产品等不限于以下方式，仅作参考。

(1) 政务人员跨网接入密码应用流程

在客户端部署 VPN 客户端及智能密码钥匙，政务服务平台网络边界部署 SSL VPN 服务端，政务人员通过智能密码钥匙及 VPN 客户端与 SSL VPN 间建立安全传输通道，实现政务人员的跨网安全接入认证以及数据传输通道的机密性和完整性。

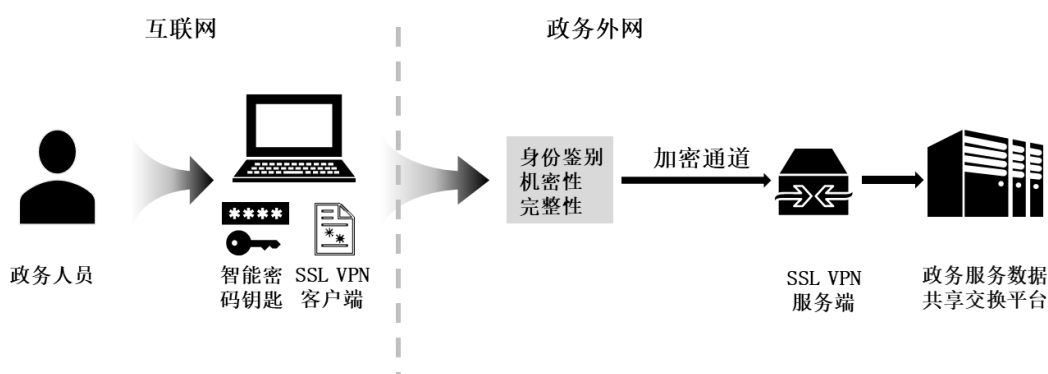


图 6 政务人员跨网接入密码应用流程

(2) 运维人员远程管理密码应用流程

通过客户端部署 VPN 客户端及智能密码钥匙，政务服务平台网络边界部署 SSL VPN 服务端，实现运维人员的跨网安全接入认证，继而通过堡垒机对系统相关设备进行统一远程运维管理。

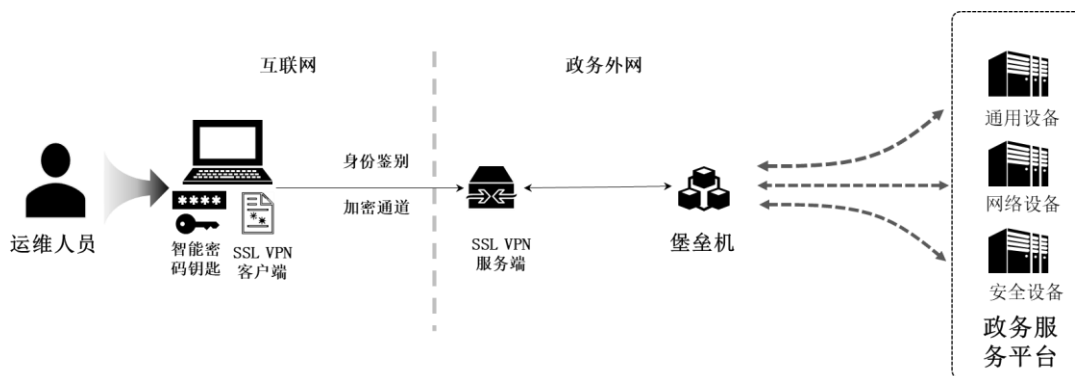


图 7 运维人员远程管理密码应用流程

(3) 政务人员登录应用密码应用流程

移动办公 App 中部署符合 GM/T 0028 的标准的移动终端安全密码模块（二级），在服务端部署安全认证网关、协同签名系统向用户发放数字证书，实现政务人员的移动办公应用登录。在政务服务平台服务端部署安全认证网关或动态令牌认证系统，PC 端用户（政务人员和系统管理员）通过使用智能密码钥匙或动态令牌实现应用系统登录。

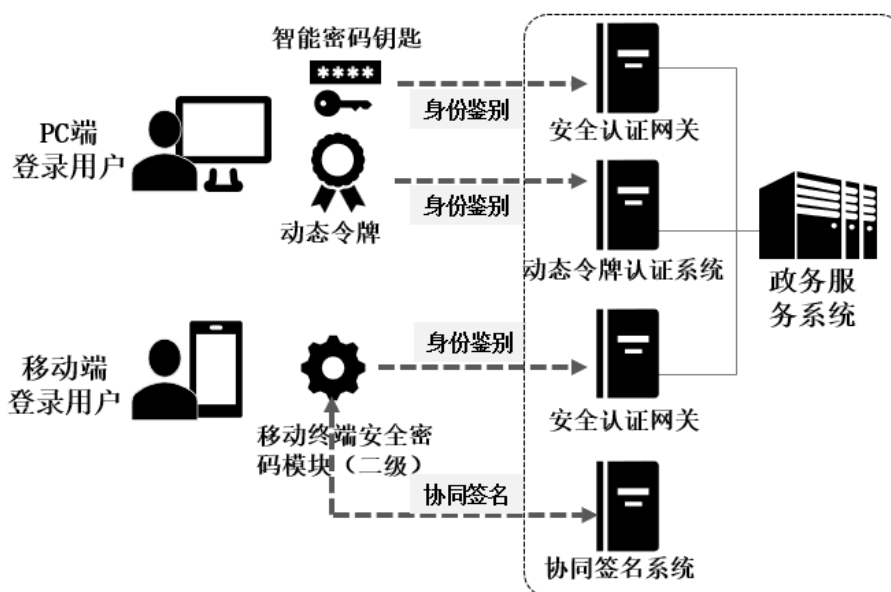


图8 政务人员登录应用密码应用流程

(4) 重要数据存储及应用过程密码应用流程

政务服务平台业务系统调用密码资源池加解密服务将重要数据以密文形式存放至数据库中，实现重要数据的存储过程的机密性。

政务服务平台业务系统从数据库中获取密文形态的重要数据，通过调用密码资源池加解密服务对获取到的密文进行解密。

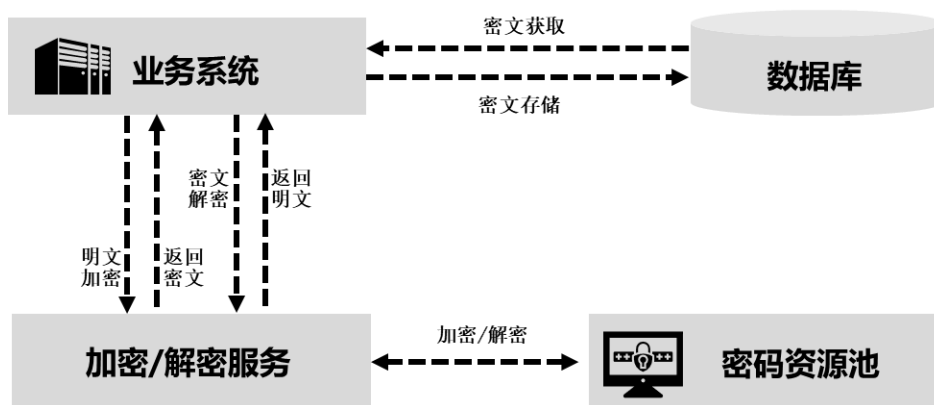


图 9 重要数据存储及应用过程密码应用流程

(5) 电子文件流转及电子证照签发密码应用流程

政务服务平台服务端部署电子签章系统及时间戳服务器，业务办理人员通过智能密码钥匙对业务办理审批行为进行数字签名，并对电子文件及电子证照加盖电子印章及时间戳，实现业务办理人员原发行为的不可否认性、电子文件的可靠流转、电子证照的权威颁发。

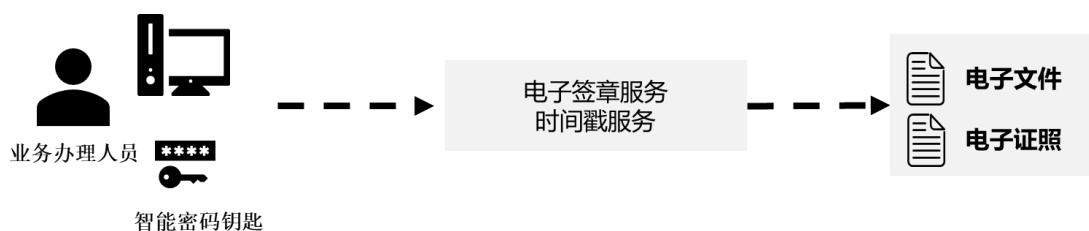


图 10 电子文件流转及电子证照签发密码应用流程

3.2 密码产品/服务选择和部署

政务服务平台密码产品部署如图 11 所示。

在政务服务平台政务外网侧、互联网侧可按需部署云服务器密码机、SSL VPN、IPsec VPN、安全认证网关、签名验签服务器、数据库加密系统、加密数据库系统、时间戳服务器、服务器密码机、动态令牌认证系统、密钥管理系统、安全电子签章系用户等密码产品。客户端按需配置智能密码钥匙、动态令牌、国密浏览器、VPN 客户端等密码模块，满足客户端密码应用需求。

政务服务平台在满足自身密码应用需求的同时，还需关注各级间政务服务平台的数据共享过程的密码应用，保证数据在共享交换过程中的完整性、机密性。

政务服务平台密码应用建设涉及到的产品及服务如表 5 所示，政务服务平台管理者可结合自身实际需求选择部署或增加其他必要的密码产品与服务。

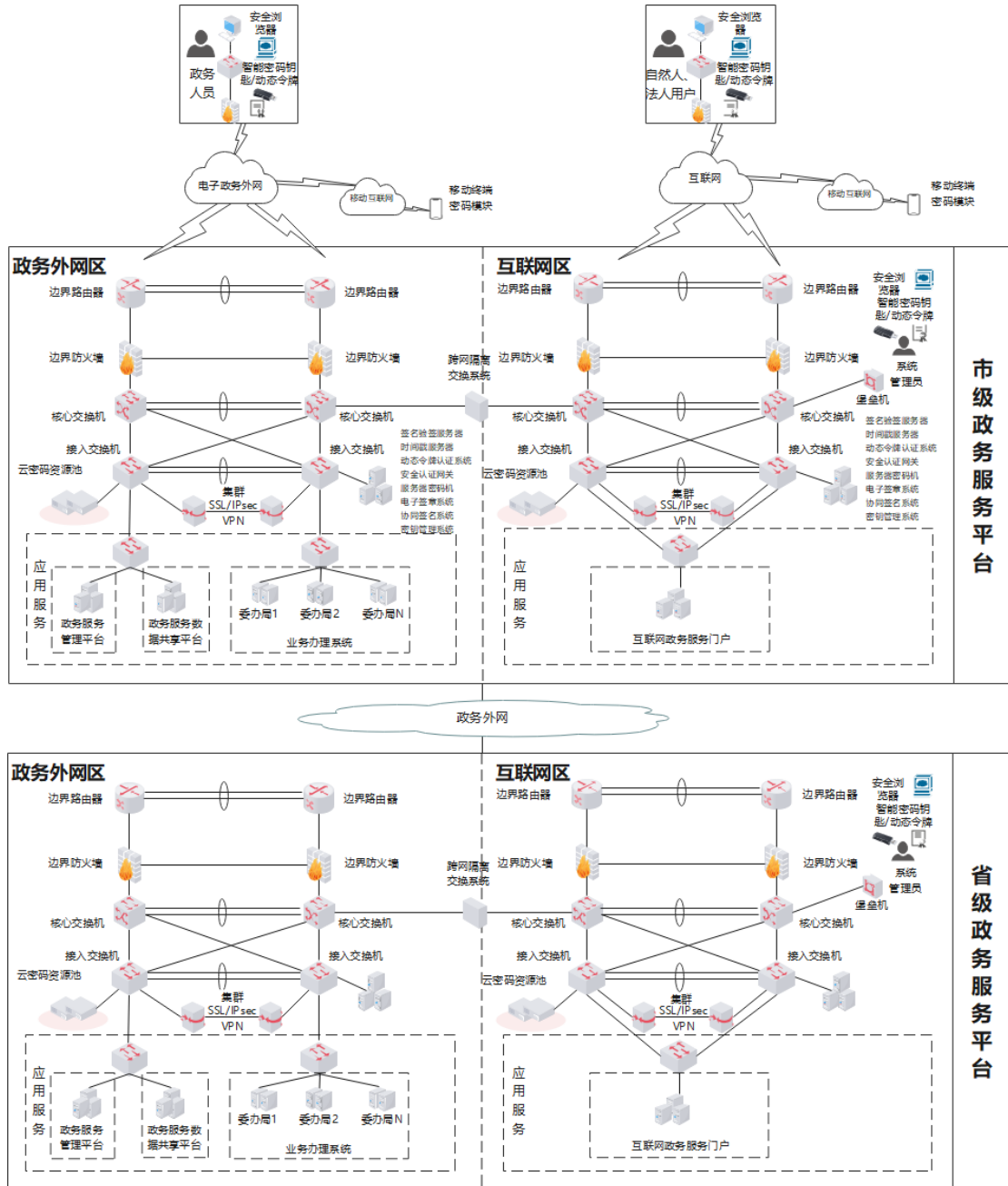


图 11 政务服务平台密码应用部署图

表 5 密码产品/服务

序号	密码产品/服务名称	在场景中提供的密码功能
1	电子门禁系统	保证政务服务平台所在机房等重要区域的人员进出身份真实性。
2	云服务器密码机/服务器密码机/密码卡	提供 SM2/3/4 等标准密码服务接口，为政务服务平台提供密码运算、密钥生成及存储等功能，实现重要数据、日志记录等信息的机密性、完整性保护。

3	签名验签服务器	提供数字签名、验签服务接口，为政务服务平台提供证书管理和验证等功能。
4	智能密码钥匙	存储政务人员的密钥对，提供 SM2/3/4 等标准密码服务接口，实现政务人员、系统管理员身份鉴别、信源加密和关键行为的不可否认性。
5	动态令牌认证系统 动态令牌	客户端令牌介质，结合服务端动态令牌认证系统提供动态口令认证，实现政务人员、系统管理员身份鉴别。
6	SSL VPN/ IPsec VPN	IPSec VPN 用于实现政务服务数据共享平台之间安全通信信道的建立。 SSL VPN 用于实现政务人员和运维管理人员的跨网访问安全通信信道的建立。
7	安全浏览器密码模块	配合政务服务平台服务端服务器证书使用合规的 SSL 协议，建立 HTTPS 安全通信信道。
8	安全认证网关	为设备、应用系统提供基于数字证书的身份鉴别、传输信道加密、应用代理、访问控制等功能。
9	时间戳服务器	提供时间戳服务接口，配合数字签名技术实现数据原发行为的不可否认性。
10	安全电子签章系统	提供电子签章和验证服务，实现政务审批事项中的行政许可等电子证照发放、验证。
11	数据库加密系统/加密数据库系统	提供数据加解密功能。
12	移动终端安全密码模块 协同签名系统	实现移动端用户的身份鉴别和电子签名。
13	密钥管理系统	对政务服务平台应用系统中各种密钥进行全生命周期集中管理。

3.3 与 GB/T 39786 对照情况说明

本实施指南针对网络安全等级保护第三级信息系统密码应用要求进行设计，三级及以下四级信息系统的建设单位和使用单位可根据 GB/T 39786 结合系统实际进行相应调整。政务服务平台密码应用设计与 GB/T 39786 对照情况说明如表 6 所示。

表 6 与 GB/T 39786 对照情况说明

安全层面	指标项	采取的密码措施
物理	身份鉴别	

和环境安全	电子门禁进出记录数据的存储完整性	1) 在政务服务平台物理机房等重要物理区域部署符合 GB/T 37033 标准、GM/T 0036 等标准的电子门禁系统，对进入物理区域人员身份进行鉴别。 2) 部署视频加密系统或使用符合相关国家、行业标准的服务器密码机、签名验签服务器，对视频监控系统视频记录进行完整性保护。
	视频监控音像记录数据的存储完整性	3) 电子门禁系统自身实现或使用符合相关国家、行业标准的服务器密码机、签名验签服务器，对电子门禁进出记录进行完整性保护。
网络和通信安全	身份鉴别	1) 在政务服务平台的网络边界部署符合 GM/T 0024、GM/T 0025 标准的 SSL VPN 网关，在客户端部署 VPN 客户端及符合 GM/T 0027 标准的智能密码钥匙或符合 GB/T 38556 标准的动态令牌，通过 VPN 对客户端进行身份鉴别，实现政务人员和运维管理人员的跨网接入认证、传输信道加密和完整性保护。
	通信数据完整性	2) 在政务服务数据共享平台、业务办理系统服务端部署服务器证书，在客户端部署国密浏览器，使用合规的 SSL 协议，实现客户端对应用系统的身份鉴别（或双向身份鉴别）、传输信道加密和完整性保护。
	通信过程中重要数据的机密性	3) 在互联网政务服务门户服务端部署服务器证书，使用合规的 SSL 协议，实现自然人/法人 PC 端、移动端对应用系统的身份鉴别、传输信道加密和完整性保护。
	网络边界访问控制信息的完整性	4) 在各级政务服务平台网络边界部署符合 GB/T 36968 标准的 IPsec VPN，实现政务服务数据共享平台之间通信信道的身份鉴别、传输加密和完整性保护。
	安全接入认证	5) 在政务服务平台中部署符合密码相关国家、行业标准的服务器密码机或签名验签服务器，对网络边界的 VPN 中的访问控制列表、防火墙的访问控制列表、边界路由的访问控制列表等网络边界访问控制信息进行完整性保护。
设备和计算安全	身份鉴别	1) 部署符合 GM/T 0024、GM/T 0025 标准的 SSL VPN 或符合 GM/T 0026 标准的安全认证网关或符合 GB/T 38556 标准的动态令牌认证系统对接堡垒机，或部署通过商用密码检测认证的堡垒机，运维管理人员通过使用智能密码钥匙或动态令牌实现登录堡垒机的身份鉴别，通过堡垒机统一运维管理设备。运维管理人员通过使用智能密码钥匙或动态令牌实现密码设备的本地运维管理。
	远程管理通道安全	
	系统资源访问控制信息完整性	

	重要信息资源安全标记完整性	<p>2) 在堡垒机部署服务器证书, 使用合规的 SSL 协议, 建立安全管理数据传输通道。</p> <p>3) 在政务服务平台中部署符合密码相关国家、行业标准要求的服务器密码机或签名验签服务器, 对设备访问控制信息、重要信息资源安全标记、日志记录、重要可执行程序等进行完整性保护。</p> <p>4) 通用设备、网络及安全设备、各类虚拟设备等设备中的重要可执行程序更新、升级以及政务服务 App 下载安装, 提供者进行数字签名以实现其来源的真实性保护。</p>
	日志记录完整性	
	重要可执行程序完整性、重要可执行程序来源真实性	
应用和数据安全	身份鉴别	<p>1) 可在自然人/法人移动端政务服务 App 中部署符合 GM/T 0028 的标准的移动终端安全密码模块 (二级), 在服务端部署安全认证网关、协同签名系统向用户发放数字证书, 实现公众用户的移动端政务服务 App 登录、PC 端网上办事大厅登录。在政务服务平台服务端部署安全认证网关或动态令牌认证系统, 政务人员和系统管理员通过使用智能密码钥匙或动态令牌或移动终端安全密码模块实现应用系统登录。</p> <p>2) 在政务服务平台服务端部署服务器密码机或签名验签服务器, 对应用系统的访问控制信息、重要业务日志、重要信息资源安全标记、重要数据进行存储完整性保护。</p> <p>3) 在政务服务平台服务端部署密钥管理系统、服务器密码机、数据库加密系统、加密数据库系统、密码卡、密码模块等, 对应用系统的重要数据进行存储机密性保护。</p> <p>4) 政务人员通过 PC 端智能密码钥匙, 应用服务端通过密码设备可对系统中的重要数据封装数字信封, 实现重要数据传输过程中的机密性、完整性保护。</p> <p>若存在政务人员使用移动端进行移动办公的场景, 可通过移动端使用移动终端安全密码模块, 应用服务端使用密码设备, 对系统中的重要数据封装数字信封的方式, 实现重要数据传输过程中的机密性、完整性保护。</p> <p>5) 政务服务平台服务端部署符合 GM/T 38540 标准的电子签章系统、符合 GM/T 0033 标准的时间戳服务器, 客户端通过移动终端安全密码模块、智能密码钥匙等对自然人、法人的政务</p>
	访问控制信息完整性	
	重要信息资源安全标记完整性	
	重要数据传输机密性	
	重要数据存储机密性	
	重要数据传输完整性	
	重要数据存储完整性	

	不可否认性	<p>事项申请行为、政务人员的业务办理审批行为等关键行为进行数字签名，实现数据原发行为、数据接收行为的不可否认性。</p> <p>6) 采用密码技术对互联网政务服务门户统一展示、发布的政务服务信息及业务办理入口等发布内容进行完整性保护。</p>
--	-------	--

3.4 注意事项

(1) 自然人、法人用户登录可采用短信验证码、生物识别等措施进行互联网政务服务门户登录，在登录后涉及办理个人敏感信息填报、证明材料上传等业务场景时进行基于密码技术的二次认证和数字签名等处理。

(2) 互联网政务服务门户网站面向公众，现阶段通用浏览器（IE、谷歌）对 SM2 算法站点证书无法有效支持，用户体验差，可采用经通用浏览器认证的 2048 位以上 RSA 算法站点证书。

(3) 因政务服务平台后端涉及大量外部系统的业务对接接口，与外部进行数据交换的场景。建议可采用密码技术确保双方身份的合法性，同时重要数据的传输可通过数字信封机制予以保障。确保以项目为边界的应用系统密码应用安全合规。

(4) 针对政务服务平台所处不同机房或跨域不可控区域的情况，应分别部署密码资源池（物理设备）。若存在业务数据跨机房传输，或跨机房调用密码支撑能力的情况，应在两机房分别部署密码设备（如 IPSec VPN）保证传输通道的安全性。

(5) 因政务服务平台涉及业务系统数量众多，业务交叉点繁杂，共享交换平台涉及多层级数据传输，各级系统间存在大量业务与数据交换接口，在进行密码应用建设时可统筹分步建设，规划进行信息系统新老接口接替，在保障业务连续性的前提下完成密码应用建设。

4 密码应用安全性评估实施指南

4.1 主要测评指标的选择和确定

本指南密码应用安全评估实施选择 GB/T 39786 中第三级安全要求作为测评工作的基本指标，结合政务服务平台密码应用情况给出测评建议。主要测评指标的选择和确定如表 7 所示。

表 7 主要测评指标的选择和确定

类型	指标项			不适用情况 说明
主要适用指标	技 术	物理和	身份鉴别	无
		环境安	电子门禁记录数据存储完整性	

要求	全	视频监控记录数据存储完整性
		身份鉴别
	网络和通信安全	通信数据完整性
		通信过程中重要数据的机密性
		网络边界访问控制信息的完整性
		身份鉴别
	设备和计算安全	远程管理通道安全
		系统资源访问控制信息完整性
		日志记录完整性
		重要可执行程序完整性、重要可执行程序来源真实性
		身份鉴别
	应用和数据安全	访问控制信息完整性
		重要数据传输机密性
		重要数据存储机密性
		重要数据传输完整性
		重要数据存储完整性
		不可否认性
		管理制度
	密钥管理规则	
	建立操作规程	
	定期修订安全管理制度	
	明确管理制度发布流程	
	制度执行过程记录留存	
	人员管理	了解并遵守密码相关法律法规和密码管理制度
建立密码应用岗位责任制度		
建立上岗人员培训制度		
定期进行安全岗位人员考核		
建立关键岗位人员保密制度和调离制度		
建设运行	制定密码应用方案	
	制定密钥安全管理策略	
	制定实施方案	
	投入运行前进行密码应用安全性评估	

		定期开展密码应用安全性评估及攻防对抗演习	
	应急处置	应急策略	
		事件处置	
		向有关主管部门上报处置情况	
常见不适用指标	网络和通信安全	安全接入认证	建设单位和使用单位可结合实际情况自行决定是否纳入标准符合性测评范围
	设备和计算安全	重要信息资源安全标记完整性	根据信息系统的密码应用方案和方案评估意见（以及信息系统是否存在重要信息资源安全标记）决定是否纳入标准符合性测评范围
	应用和数据安全	重要信息资源安全标记完整性	根据信息系统的密码应用方案和方案评估意见（以及信息系统是否存在重要信息资源安全标记）决定是否纳入标准符合性测评范围

4.2 主要测评内容

测评实施主要是采用相应的测评方法对系统中需要保护的对象进行测评，获取需要的证据。本章节将依据 GM/T 0116、GM/T 0115 及《商用密码应用安全性评估 FAQ》，结合政务服务平台主要保护对象（见“表 2”），确定各个层面的测评对象和测评方法。

4.2.1 现场测评方法

(1) 现场测评方法

商用密码应用安全性评估使用的测评方法包括：

1) 访谈：通过与受测单位的相关人员进行交谈和问询，了解信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认；

2) 文档审查：审核受测单位提交的有关信息系统安全的各个方面的文档，如：受测系统总体描述文件，受测系统密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，受

测单位的信息化建设与发展状况以及联络方式；密码应用方案及评审意见，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次评估报告等等。通过对这些文档的审核与分析，确认测评的相关内容是否达到安全保护等级的要求；

3) 实地查看：现场查看测评对象所处的环境、外观等情况；

4) 配置检查：查看测评对象的相关配置；

5) 工具测试：根据被测信息系统的实际情况，密评人员使用适合的技术工具对其进行测试。

(2) 测评工具

政务领域政务服务平台密评工作参照 GM/T 0115，结合具体实际需求，使用如表 8 所示的密评工具。

表 8 主要测评指标的选择和确定

序号	工具名称	主要功能
1	协议分析工具	1) 捕获并解析通信数据，分析通信协议密码算法协商过程。 2) 解析密码算法或密码套件标识是否属于已发布为标准的商用密码算法。 3) 分析传输的重要数据或鉴别信息是否为密文，数据格式(如分组长度等)是否符合预期。 4) 分析受完整性保护的数据在传输时的数据格式(如签名长度、MAC 长度)是否符合预期。
2	算法验证工具	对密码算法进行分析校验。
3	数字证书格式合规性检测工具	用于验证生成或使用的证书格式是否符合 GB/T 20518 的有关要求。

4.2.2 测评实施

4.2.2.1 密码技术应用测评

(1) 物理和环境安全

1) 测评对象

物理和环境安全层面的测评对象为政务服务平台所在物理机房，具体为机房的电子门禁系统、视频监控系统。物理和环境安全层面涉及的测评对象和采用的测评方式如表 9 所示。

表 9 测评对象和测评方式

层面(类)	测评对象	测评方式
-------	------	------

物理和环境安全	政务领域政务服务平台所在物理机房(具体为电子门禁系统和视频监控系统)	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查 <input checked="" type="checkbox"/> 实地查看 <input checked="" type="checkbox"/> 配置检查 <input checked="" type="checkbox"/> 工具测试
---------	------------------------------------	--

2)测评实施要点

物理和计算安全层面测评指标包括人员进入机房时采用身份鉴别方式,电子门禁记录数据和视频监控记录数据保护措施。测评时可按照 GM/T 0115 中 6.1 章节描述的测评方法实施测评。

如果政务服务平台部署涉及多个物理机房,所有物理机房均应进行测评。

(2) 网络和通信安全

1)测评对象

根据政务服务平台中的各典型业务及其密码应用实现,分析网络和通信安全层面涉及的测评对象,测评对象包括浏览器与业务系统、政务服务 App 与互联网政务服务门户、VPN 客户端与 SSL VPN、各级政务服务平台之间、政务服务数据共享平台与政务信息系统等通信信道。网络和通信安全层面可能涉及的测评对象和采用的测评方式如表 10 所示。

表 10 测评对象和测评方式

层面(类)	测评对象	测评方式
网络和通信安全	浏览器与业务系统的通信信道	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查 <input checked="" type="checkbox"/> 实地查看 <input checked="" type="checkbox"/> 配置检查 <input checked="" type="checkbox"/> 工具测试
	政务服务 app 与互联网政务服务门户的通信信道	
	VPN 客户端与 SSL VPN 的通信信道	
	各级政务服务平台之间的通信信道	
	政务服务数据共享平台与政务信息系统的通信信道	
	网络边界访问控制信息	
	提供设备入网接入认证功能的设备或组件、密码产品	
	运维管理人员远程管理数据传输通道	

2)测评实施要点

网络和通信安全层面测评指标包括对通信实体身份鉴别、通信数据完整性、重要数据的机密性、网络边界访问控制信息的完整性、安全接入认证等。

测评实施要点包括以下三个方面:

- 访谈安全管理人员,了解各通信信道在通信过程中采用的通信协议。了解各数据传输信道的传输保护机制及其中涉及的密钥生命周期管理需求。
- 核查密码产品是否符合法律法规的相关要求,需依法接受检测认证的,核查是否经商用密码认证机构认证合格;了解密码产品的型号和版本等

配置信息，核查密码产品是否符合密码模块标准中相应安全等级及以上安全要求，并核查密码产品的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件。

- c) 在检查点接入协议分析工具抓取通信数据包，捕获并分析各通信信道的通信数据，并结合代码片段审查、配置核查、日志核查、算法校验、数字证书校验等方式，对访谈了解到的各数据传输信道机制进行确认。确认相关通信信道是否采用密码技术实现通信实体身份鉴别、通信数据完整性保护、重要数据机密性和网络边界访问控制信息完整性保护。

(3) 设备和计算安全

1) 测评对象

政务服务平台设备和计算层面的测评对象主要包括通用设备、网络及安全设备、密码设备、各类虚拟设备等。设备和计算安全层面可能涉及的测评对象和采用的测评方式如表 11 所示。

表 11 设备和计算安全测评对象和测评方式

层面（类）	测评对象	测评方式
设备和计算安全	通用设备	<input checked="" type="checkbox"/> 访谈
	网络及安全设备	<input checked="" type="checkbox"/> 文档审查
	密码设备	<input checked="" type="checkbox"/> 实地查看
	各类虚拟设备	<input checked="" type="checkbox"/> 配置检查
	数据库管理系统	<input checked="" type="checkbox"/> 工具测试

注：交换机、网闸、防火墙、WAF 等未使用密码功能的网络设备、安全设备一般不纳入设备和计算安全层面的测评范围。

2) 测评实施要点

设备和计算安全层面测评指标包括登录设备时采用的身份鉴别方式、远程管理通道安全、系统资源访问控制信息完整性、日志记录完整性、重要可执行程序完整性与来源真实性等。测评时可按照 GM/T 0115 中 6.3 章节描述的测评方法实施测评。如果设备存在远程管理情况，还应分析信息传输通道安全。

(4) 应用和数据安全

1) 测评对象

政务服务平台在应用和数据安全层面涉及的测评对象为互联网政务服务门户、政务服务管理平台、业务办理系统、政务服务数据共享平台，应用和数据安全层面涉及的测评对象和采用的测评方式如表 12 所示。

政务服务平台涉及的应用用户包括互联网政务服务门户的自然人、法人用户、业务办理系统的政务人员用户、政务服务数据共享平台的政务人员用户、各应用系统的系统管理员，应用和数据安全身份鉴别需求如表 13 所示。

政务服务平台涉及的关键数据包括自然人、法人登录互联网政务服务门户的

口令、政务人员登录业务办理系统的口令、政务人员登录政务服务数据共享平台的身份鉴别、系统管理员登录应用系统的口令、管理人员登录堡垒机、应用/数据库服务器等设备的口令、重要业务数据、重要审计数据、个人敏感信息、政务服务平台的重要业务日志、互联网政务服务门户内容等，应用和数据安全关键数据密码保护需求如表 14 所示。

政务服务平台涉及的不可否认性需求如表 15 所示。

表 12 应用和数据安全测评对象和测评方式

层面（类）	测评对象	测评方式
应用和数据安全	互联网政务服务门户	<input checked="" type="checkbox"/> 访谈
	政务服务管理平台	<input checked="" type="checkbox"/> 文档审查
	业务办理系统	<input checked="" type="checkbox"/> 实地查看
	政务服务数据共享平台	<input checked="" type="checkbox"/> 配置检查 <input checked="" type="checkbox"/> 工具测试

表 13 应用和数据安全身份鉴别需求

序号	应用用户	真实性
1	互联网政务服务门户的自然人、法人用户	√
2	业务办理系统的政务人员用户	√
3	政务服务数据共享平台的政务人员用户	√
4	应用系统的系统管理员	√

表 14 应用和数据安全关键数据密码保护需求

序号	关键数据	密码保护需求			
		传输 机密性	传输 完整性	存储 机密性	存储 完整性
1	自然人、法人登录互联网政务服务门户的口令	√	√	√	√
2	政务人员登录业务办理系统的口令	√	√	√	√
3	政务人员登录政务服务数据共享平台的身份鉴别	√	√	√	√
4	系统管理员登录应用系统的口令	√	√	√	√
5	管理人员登录堡垒机、应用/数据库服务器等设备的口令	√	√	√	√
6	重要业务数据	√	√	√	√

7	重要审计数据	√	√	√	√
8	个人敏感信息	√	√	√	√
9	政务服务平台的重要业务日志	—	—	—	√
10	互联网政务服务门户内容	—	—	—	√

表 15 应用和数据安全不可否认性测评结果汇总

序号	关键数据	不可否认性
1	自然人、法人的政务事项申请行为	√
2	政务人员的业务办理审批行为	√

2) 测评实施要点

应用和数据安全层面测评指标包括身份鉴别、访问控制信息完整性、重要数据传输机密性和完整性、重要数据存储机密性和完整性、关键操作行为不可否认性。

测评实施要点包括：

a) 身份鉴别

在测评实施过程中，首先，通过访谈方式了解自然人/法人、政务人员、系统管理员登录相关政务服务平台应用时的身份鉴别方式，了解是否使用密码技术进行身份鉴别以及涉及的密钥生命周期管理。

其次，采取机制分析、代码片段审查、配置核查、日志核查、数字证书校验等方式，对访谈了解到的身份鉴别机制进行确认。具体包括但不限于：通过审查代码片段、查看密码产品调用日志、校验数字证书格式、分析签名值等方式，确认采用的密码技术，确认密码产品是否被正确调用；通过分析其身份鉴别过程相关密码运算环境，相关密钥生命周期管理机制等，分析其密码运算环境、密钥管理是否安全。

b) 访问控制信息完整性

可通过核查数据库、数据库敏感字段设置策略、代码实现片段、密码产品调用日志等方式核查互联网政务服务门户、政务服务管理平台、业务办理系统、政务服务数据共享平台是否使用密码技术对访问控制信息进行完整性保护。基于以上核查结果，并通过核查数据库中存储的完整性字段，分析其长度是否与声称采用密码算法输出长度一致，确认采用的密码技术。

c) 重要数据传输机密性、完整性

首先，通过访谈方式了解政务服务平台中互联网政务服务门户、政务服务管理平台、业务办理系统和政务服务数据共享平台应用在实际业务应用中传输的重要数据；了解相关重要数据在传输过程中是否使用密码技术实现信源到信宿的传输机密性、完整性和来源真实性保护以及涉及的密钥生命周期管理。

其次，采取机制分析、代码片段审查、配置核查、日志核查、算法校验、数

字证书校验等方式，对访谈了解到的关键数据传输机密性、完整性保护实现机制进行确认。具体包括但不限于：通过对互联网政务服务门户、政务服务管理平台、业务办理系统和政务服务数据共享平台梳理的传输关键数据进行核实和确认；通过审查代码片段、查看密码产品调用日志、分析签名值或分析 HMAC 长度是否与声称采用密码算法输出长度一致等方式，确认采用的密码技术，通过分析其数据传输机密性、完整性和来源真实性保护运算环境，相关密钥生命周期管理机制等，分析其密码运算环境、密钥管理是否安全。

d)重要数据存储机密性、完整性

在测评实施过程中，首先，通过访谈方式了解政务服务平台中互联网政务服务门户、政务服务管理平台、业务办理系统和政务服务数据共享平台应用在实际业务应用中存储的重要数据，了解相关数据在存储时是否采用密码技术进行机密性和完整性保护以及涉及的密钥生命周期管理。

其次，采取机制分析、代码片段审查、配置核查、日志核查、端口扫描、算法校验、数字证书校验等方式，对访谈了解到的关键数据存储机密性、完整性保护实现机制进行确认。具体包括但不限于：通过对互联网政务服务门户、政务服务管理平台、业务办理系统和政务服务数据共享平台梳理存储的关键数据进行核实和确认；然后，通过审查代码片段、查看应用运行日志、分析签名值或分析 HMAC 长度是否与声称采用密码算法输出长度一致、对存储的重要数据进行分析等方式，确认采用的密码技术，确认密码产品是否被正确调用，确认数据存储机密性、完整性保护实现是否正确；通过分析其数据存储机密性、完整性保护运算环境，相关密钥生命周期管理机制等，分析其密码运算环境、密钥管理是否安全。

e)关键操作行为不可否认性

在测评实施过程中，首先，通过访谈方式了解政务服务平台应用在实际业务应用中涉及需要进行不可否认性保护的关键操作行为，了解相关操作在实施时是否采用密码技术进行不可否认性保护以及涉及的密钥生命周期管理。

其次，采取机制分析、代码片段审查、配置核查、日志核查、端口扫描、算法校验等方式，对访谈了解到的关键操作不可否认性实现机制进行确认。具体包括但不限于：通过分析报文数据确认是否包含签名数据；然后，通过审查代码片段、查看应用运行日志、分析签名值或分析 HMAC 长度是否与声称采用密码算法输出长度一致、对存储的操作报文数据进行分析等方式，确认采用的密码技术，确认密码产品是否被正确调用，确认关键操作行为不可否认性保护实现是否正确；通过分析其不可否认性保护运算和校验环境，相关密钥生命周期管理机制等，分析其密码运算环境、密钥管理是否安全。

4.2.2.2 安全管理测评

(1) 测评对象

安全管理测评包括管理制度、人员管理、建设运行和应急处置四个层面。涉

及的测评对象和采用的测评方式如表 16 所示。

表 16 安全管理测评对象和测评方式

层面（类）	测评对象	测评方式
管理制度	管理体系（包括安全管理制度类文档、密码应用方案、密钥管理制度及策略类文档、操作规程类文档、记录表单类文档、系统相关人员）	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查
人员管理	管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查
建设运行	密码应用方案、密钥管理制度及策略类文档、密码实施方案、密码应用安全性评估报告、密码应用安全管理制度、攻防对抗演习报告、整改文档	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查
	管理体系（包括安全管理制度类文档、记录表单类文档、系统相关人员）	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查
应急处置	管理体系（包括密码应用应急处置方案、应急处置记录类文档、安全事件发生情况及处置情况报告、系统相关人员）	<input checked="" type="checkbox"/> 访谈 <input checked="" type="checkbox"/> 文档审查

（2）测评实施要点

安全管理测评实施主要通过访谈和文档审查，检查管理制度是否全面、规范、合理；访谈系统相关人员，确认人员是否了解并遵守密码相关法律法规、是否正确使用密码相关产品。具体可按照 GM/T 0115 中 6.5 至 6.8 章节描述的测评方法实施测评。

4.3 主要测评结果

结合 4.1、4.2 章节确定的测评指标和测评内容，根据 GM/T 0115 结果判定规则，得出各个测评对象和测评单元的测评结果。进一步从单元间、层面间进行测评和综合安全分析，得出整体测评结果。

由于部分测评对象测评结果的得出需要结合系统具体实现，且测评结果判定依据比较明确，此处不再进行具体描述。

在整体测评阶段，应依照 GM/T 0115 的整体测评要求，考虑是否存在单元间和层面间的弥补情况。

在风险分析和评价阶段，应依照 GM/T 0115 的风险分析和评价中的要求执行。另外，可根据安全威胁严重程度、安全威胁发生频率和关联资产价值等方面进行具体分析和评价工作。

4.4 注意事项

在测评过程中应注意以下事项。

(1) 在实施系统测评前，应根据被测单位需求和系统业务情况，明确被测系统的网络边界和测评范围。

(2) 政务人员移动端登录和 PC 端登录身份鉴别机制存在差异，其中，移动端一般通过协同签名方式，通过前后端密码模块和协同签名系统实现身份鉴别，PC 端一般通过数字证书方式，通过智能密码钥匙和签名验签服务器实现登录身份鉴别。应注意在测评实施过程中，应根据不同实现机制采用不同的测评方式。

(3) 对于通过互联网或者其他跨网络使用 VPN 进行运维管理的情况，此时远程管理终端与 VPN 之间的通信信道也应作为网络和通信安全层面的测评对象进行测评。

(4) 系统实现过程中，可能会采用多种缓解措施降低未使用密码技术带来的安全问题。此时应该根据具体场景和实际情况分析缓解措施如何降低风险，判断缓解措施是否有效等。如在设备和计算安全层面，用户登录堡垒机时应使用密码技术对用户身份进行鉴别。如果未采用密码技术，但采用了多因素鉴别机制且只能在内部网络登录)，在风险判定时应判断缓解措施是否能有效降低风险。