

江苏省地方标准

DB32/T 5073.2—2025

政务“一朵云”安全管理体系规范 第2部分：密码应用技术要求

Security management system specification for the "Cloud" of
government affairs —Part 2: Technical requirements for
cryptography application

2025-02-21 发布

2025-03-21 实施

江苏省市场监督管理局 发布
中国标准出版社 出版

目 次

前言 III

引言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 总体架构 3

6 基本要求 3

 6.1 产品、技术和服务要求 3

 6.2 物理和环境要求 4

 6.3 网络和通信要求 4

 6.4 设备和计算要求 4

7 密码基础设施要求 4

 7.1 电子认证要求 4

 7.2 密钥管理要求 5

8 密码资源池要求 5

 8.1 服务要求 5

 8.2 性能要求 6

9 密码资源管理平台要求 6

10 密码应用要求 7

 10.1 业务终端密码应用要求 7

 10.2 网络边界密码应用要求 7

 10.3 业务密码应用要求 7

附录 A(资料性) 典型密码服务协议和算法技术要求 8

附录 B(资料性) 对称密钥和非对称密钥全生命周期管理方式 9

附录 C(资料性) 政务云主要保护对象及密码安全需求 11

参考文献 14

前 言

本文件依据 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》编写。

本文件是 DB32/T 5073《政务“一朵云”安全管理体系规范》的第2部分。DB32/T 5073已经发布了以下部分：

- 第1部分：安全运行监测；
- 第2部分：密码应用技术要求；
- 第3部分：密码应用安全性评估。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏省国家密码管理局提出。

本文件由江苏省软件和信息技术服务标准化技术委员会归口。

本文件起草单位：江苏省电子信息产品质量监督检验研究院（江苏省信息安全测评中心）、江苏省国家密码管理局、江苏省大数据管理中心、江苏省商用密码产业协会、中电科网络安全科技股份有限公司、中国电信股份有限公司江苏分公司、江苏省国信数字科技有限公司、江苏航天七零六信息科技有限公司、江苏意源科技有限公司、无锡航天江南数据系统科技有限公司、乾讯信息技术（无锡）有限公司、江苏先安科技有限公司、江苏信创密码技术有限公司、华为技术有限公司、南京三未信安信息技术有限公司。

本文件主要起草人：张腾标、吴兰、王琦、韩磊、黄敏、刘尧、谢吉华、宋飞、赵辉、何丹、印哲然、蒋日友、朱兆国、强克华、庄昱珪、张翀、陈初、唐一铭、任明聪、徐雁飞、李国琴、卢秋如、张健、廖成军、金钧华、苏丹、王彬、赵统一、朱静。

引 言

为加强统筹规划,全面提升江苏省政务云服务能力和安全运行水平,促进政务信息基础设施建设可持续发展,根据《省政府关于加快统筹推进数字政府高质量建设的实施意见》《江苏省政务“一朵云”建设总体方案》的要求,建立健全江苏省政务“一朵云”安全保障体系,提升安全防护能力,制定本文件。

DB32/T 5073《政务“一朵云”安全管理体系规范》分为以下 3 个部分:

- 第 1 部分:安全运行监测;
- 第 2 部分:密码应用技术要求;
- 第 3 部分:密码应用安全性评估。

政务“一朵云”安全管理体系规范

第2部分：密码应用技术要求

1 范围

本文件给出了政务云密码基本技术要求,以及密码基础设施、密码资源池、密码资源管理平台等密码基础设施和资源,业务终端、网络边界、业务应用等密码应用相关的技术要求。

本文件适用于政务云密码应用建设,也可规范政务云中密码在用户终端、网络接入、应用系统、应用数据等方面的应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 7408.1—2023 日期和时间 信息交换表示法 第1部分:基本原则
- GB/T 25069 信息安全技术 术语
- GB/T 38636 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
- GB/T 43207 信息安全技术 信息系统密码应用设计指南
- GM/T 0036 采用非接触卡的门禁系统密码应用技术指南
- GM/T 0038 证书认证密钥管理系统检测规范
- GM/T 0050 密码设备管理 设备管理技术规范
- GM/T 0051 密码设备管理 对称密钥管理技术规范
- GM/Z 4001—2013 密码术语

3 术语和定义

GB/T 25069和GM/Z 4001界定的以及下列术语和定义适用于本文件。

3.1

政务“一朵云” the "Cloud" of government affairs

在省级行政区域统一建设和部署的政务云(3.2),依托电子政务外网和互联网,运用云计算技术和智能化工具,为该区域各类电子政务的业务应用系统提供计算资源、存储资源、服务支撑、安全保障等共性服务的新型信息基础设施。

3.2

政务云 e-government cloud

运用云计算技术,统筹利用机房、计算、存储、网络、安全、应用支撑等软硬件设备,发挥云计算虚拟化、高可靠性、通用性、高扩展性,以及快速、按需、弹性的服务等特征,为政务信息系统提供基础设施、支撑软件、运行保障和信息安全等的综合服务平台。

注:用“机房、计算、存储、网络、安全、应用支撑等软硬件设备”取代“机房资源、计算资源、存储资源、网络资源、信息

资源、应用支撑等资源”，用“为政务信息系统提供基础设施、支撑软件、运行保障和信息安全等的综合服务平台”取代“为各政务部门构建提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等服务的电子政务综合性服务平台”。

[来源:GB/T 34078.1—2017,2.1,有修改]。

3.3

电子认证服务 electronic authentication service

为电子签名相关各方提供真实性、可靠性验证的活动。

[来源:《电子认证服务管理办法》,第一章第二条]

3.4

密码应用方案 cryptography application scheme

用于指导信息系统责任主体合规、正确、有效地使用密码技术,部署密码保障系统的规划。

[来源:GB/T 43207—2023,3.1]

3.5

密码资源池 cryptography resource pool

一组密码物理资源或虚拟密码资源的集合,能够对密码资源进行实时监控、合理分配和负载均衡,具有可扩展性、高性能、低风险等特点(密码资源包括密码运算部件、密钥存储部件和随机数发生器等)。

[来源:GM/T 0094—2020,3.9]

3.6

响应时间 response time

在政务云密码应用中,当密码资源池收到业务应用或政务云使用单位发起的请求到密码资源池返回响应结束整个过程所耗的时间。

3.7

负载能力 load capacity

在政务云密码应用中,密码资源池利用系统硬件平台对业务应用和政务云使用单位请求进行处理的能力。

注:一般通过HPS、TPS、QPS等指标进行评价度量。

4 缩略语

以下缩略语适用于本文件。

CA:证书认证机构(Certificate Authority)

CPU:中央处理器(Central Processing Unit)

HPS:每秒点击次数(Hits Per Second)

IP:互联网协议(Internet Protocol)

IPSec:互联网安全协议(Internet Protocol Security)

MAC:消息鉴别码(Message Authentication Code)

PKI:公钥基础设施(Public Key Infrastructure)

QPS:系统每秒处理查询次数(Query Per Second)

SSL:安全套接字协议(Secure Sockets Layer)

TLCP:传输层密码协议(Transport Layer Cryptography Protocol)

TLS:安全传输层协议(Transport Layer Security)

TPS:系统每秒处理数(Transaction Per Second)

VPN:虚拟专用网络(Virtual Private Network)

5 总体架构

政务云密码应用构建以商用密码为核心的云安全密码保障体系,通过密码基础设施、密码资源池提供密码功能、服务和密钥管理能力。同时,集中对硬件及虚拟化密码资源统一调度分配,提供典型密码应用服务。政务云密码应用总体架构包括密码基础设施、密码资源池、密码应用,密码资源管理平台,如图 1 所示。



图 1 政务云密码应用总体架构

6 基本要求

6.1 产品、技术和服务要求

政务云密码应用总体要求包括：

- a) 政务云凡涉及第三方电子认证服务或电子政务电子认证服务时,应选用电子认证服务使用密码许可单位名录或电子政务电子认证服务机构目录中的服务机构提供的认证服务；
- b) 政务云凡涉及使用对称算法、非对称算法、密码杂凑算法时,应采用通过国家密码管理部门审查鉴定的商用密码算法；
- c) 政务云使用的密码产品应采用通过国家密码管理部门审查鉴定的商用密码产品,且达到 GB/T 39786 中相应等级的安全要求。

典型密码服务协议和算法技术要求按附录 A。

6.2 物理和环境要求

在物理和环境安全层面,实现对政务云密码应用技术支撑系统、服务和软硬件所在重点区域的物理防护,具体要求如下:

- a) 应部署使用符合 GM/T 0036 规定的电子门禁系统对进出机房人员进行身份鉴别,或者采用指纹识别、人脸识别等生物识别技术对进出人员进行身份鉴别,并配备视频监控系统实时监控作补充防护;
- b) 宜采用基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制等密码技术对电子门禁系统进出记录、视频监控系统的电子影像记录采集完成后的状态进行存储完整性保护。

6.3 网络和通信要求

在网络和通信安全层面,实现对政务云不同实体之间网络通信的安全防护,具体要求如下:

- a) 应对通信实体进行身份鉴别,保证通信实体身份的真实性;
- b) 政务云中客户端到服务端(如用户终端到业务应用、运维终端到各类软硬件设备)的通信信道应采用通过国家密码管理部门审查鉴定的传输层安全通信协议(如 TLSv1.1、TLCP 等);
- c) 政务云对等实体间(如不同云之间)的通信信道应采用通过国家密码管理部门审查鉴定的网络层通信协议(如 IPSec 等);
- d) 宜采用基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)等机制对通信过程中的数据和网络边界访问控制信息(如网络边界 VPN、防火墙、路由器等设备中的访问控制列表)进行完整性保护;
- e) 存在外部实体接入的情况时,可使用密码技术、密码产品对其进行安全接入认证。

6.4 设备和计算要求

在设备和计算安全层面,实现对政务云中各类服务器操作系统、数据库管理系统和堡垒机等设备的安全防护,具体要求如下:

- a) 服务器操作系统应使用密码技术对登录的人员进行身份鉴别,并使用密码技术对登录人员的权限信息和访问控制信息进行完整性保护,同时对可执行程序来源的真实性和完整性进行验证;
- b) 数据库管理系统应使用密码技术对登录的人员进行身份鉴别,并使用密码技术对登录人员的权限信息和访问控制信息进行完整性保护;
- c) 堡垒机等设备应使用密码技术对登录的人员进行身份鉴别,并使用密码技术对登录人员的权限信息、访问控制信息和日志记录进行完整性保护。

7 密码基础设施要求

7.1 电子认证要求

建立基于公钥密码技术,实现证书签发、注册审核和查询服务等功能的电子认证基础设施,具体要求如下:

- a) 提供电子认证服务的机构应具有国家相关主管部门颁发的《电子认证服务许可证》;
- b) 所使用的数字证书格式遵循《电子政务数字证书格式规范》;
- c) 提供电子签名认证证书的制作、签发、管理服务,确认签发的电子签名认证证书的真实性;
- d) 提供电子签名认证证书目录信息的查询和下载服务。

7.2 密钥管理要求

建立密钥管理基础设施,实现对密钥的全生命周期安全管理,具体要求如下。

- a) 政务云资源管理平台和密码资源管理平台由密钥管理系统等密钥管理类密码产品提供密钥管理功能,包括密钥的生成、分发、存储、备份、归档、恢复、更新、销毁等全生命周期的管理,密钥管理的设计需遵循GM/T 0038、GM/T 0050、GM/T 0051等标准要求。
- b) 采用通过认证的随机数发生器在可控环境中生成密钥。
- c) 密钥的分发采用物理和在线两种方式。使用存储介质传输明文密钥时,需使用访问控制机制或制定相关管理制度以保护其安全性。密钥在不可控的环境中分发时,需使用密码技术以保护密钥分发过程的机密性、完整性。
- d) 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。
- e) 云上业务应用中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由产品自身实现。

注:其他密钥的具体管理方式见附录B。

8 密码资源池要求

8.1 服务要求

8.1.1 概述

密码资源池基于密码基础设施和各类密码资源,通过密码服务中间件封装通用密码服务接口,面向各类密码应用提供数据加解密、数据完整性计算和验证、签名验签、时间戳、证书管理、电子签章等密码服务。

8.1.2 数据加解密服务

数据加解密服务应提供敏感字段加解密、文件/对象加解密和数据库加解密等服务,所使用的密码算法应符合法律法规规定和密码相关国家标准、行业标准有关要求,并通过密码服务中间件提供统一的对外服务接口。

8.1.3 数据完整性计算和验证服务

数据完整性计算和验证服务应采用数字摘要等密码技术提供完整性计算和验证功能,所使用的密码算法应符合法律法规规定和密码相关国家标准、行业标准有关要求,并通过密码服务中间件提供统一的对外服务接口。

8.1.4 签名验签服务

签名验签服务应支持数字证书的查询、验证、解析等功能,具有提供数字签名、验证签名的服务能力,并通过密码服务中间件提供统一的对外服务接口。

8.1.5 时间戳服务

时间戳服务应提供可信时间服务,为电子数据文件提供时间戳认证,并符合GB/T 7408.1—2023中规

定的格式要求,并通过密码服务中间件提供统一的对外服务接口。

8.1.6 证书管理服务

证书管理服务应提供证书验证、撤销列表更新、证书业务代理等证书管理功能,实现对生命周期内数字证书的全过程管理。证书管理服务依托基于PKI技术的证书管理系统等实现,并通过密码服务中间件提供统一的对外服务接口。

8.1.7 电子签章服务

电子签章服务应提供电子文件的签章功能,实现信息、行为起源和传递的不可否认服务,可依托具有签名验签、电子签章、时间戳功能的密码产品实现,并通过密码服务中间件提供统一的对外服务接口。

8.1.8 密码服务中间件

政务云密码服务中间件应提供适用于主流操作系统和CPU架构的密码应用接口,统一调用流程,屏蔽密码复杂的逻辑,提供高可靠、易复用的整套接口,为密码应用层提供密码运算服务。如政务云业务终端(包括PC端、移动终端)、服务端通过密码服务中间件调用标准化的时间戳、签名验签、加解密等各类密码服务。

8.1.9 其他密码服务

其他经国家密码管理部门审查鉴定的符合相关国家标准、行业标准的密码服务。

8.2 性能要求

8.2.1 响应时间

密码资源池应根据政务云密码服务的业务数量、用户规模及网络情况,按需扩容密码资源,使业务应用调用政务云密码服务的实际响应时间在政务云管理单位要求的最大参考临界值以内。

8.2.2 负载能力

密码资源池应支持对多台云服务器进行流量分发的负载均衡服务,扩展对外服务能力,提升应用系统的可用性,满足业务应用和政务云使用单位的需求,且系统处理能力易于扩展,随数据量和请求量的增加而扩展负载能力。

8.2.3 并发能力

密码资源池应支持来自政务云潜在的全部业务应用和政务云使用单位高并发查询、业务分析、运行计算需求,并在高并发情况下保证密码服务的业务连续性和可用性,且多集群的密码服务可并发执行、互不影响。

9 密码资源管理平台要求

密码资源管理平台作为政务云密码资源池的主控平台,对云密码资源池中的资源(网络资源、镜像资源、计算资源、操作系统等)进行池化管理,同时集成密码基础设施和密码应用相关管理能力,具有密码相关的设备管理、配置管理、运行管理、使用单位管理、应用管理、异常监测及预警告警,以及密码服务的虚拟化和弹性化、密码服务支撑、密码服务运维保障、政务云平台本身及使用单位密钥生存周期等管理功

能。具体要求包括：

- a) 应具有密码设备管理功能,包括设备基本信息管理、IP等部署信息管理、设备分组集群管理等,对密码服务提供服务名称、服务内容、服务包、服务地址、服务接口等信息管理功能;
- b) 应具有密码服务的配置管理功能,提供服务节点配置、服务集群策略、流量控制(如负载均衡、阈值设置、服务降级、服务熔断等方式)、黑白名单等功能;
- c) 应具有密码服务的运行管理功能,支持实时获取服务日志、服务成功率,并将运行数据进行留存;
- d) 应具有使用单位管理功能,提供账户注册管理、权限管理、租用资源管理、密码资源分配管理、密钥管理、计费结算(如适用)等功能(可协同政务云资源管理平台实现);
- e) 应具有政务云业务应用密码管理功能,提供业务应用密码服务正确性、合规性、有效性管理,以及密钥分发、使用、备份、撤销等管理功能;
- f) 应具有对密码资源池中密码设备运行状态、接口调用情况以及使用单位调用密码服务合规性的监测功能,监测内容具体包括密码服务运行状态、密码服务调用次数、密码资源占用率、服务接口调用频率、密码算法和密码技术应用的合规性等信息;
- g) 应提供密码资源池中安全事件的预警告警能力,通过态势分析技术和风险预警技术对密码资源池中密码设备安全风险、系统运行风险、接口调用风险、使用单位异常行为进行识别和告警。

10 密码应用要求

10.1 业务终端密码应用要求

应使用遵循密码相关国家标准和行业标准,符合法律法规相关要求的终端密码模块、安全浏览器、智能密码钥匙等密码产品、服务或技术,实现终端用户的身份真实性、数据机密性和完整性等需求。

10.2 网络边界密码应用要求

应使用遵循密码相关国家标准和行业标准,符合法律法规相关要求的SSL VPN、IPSec VPN、安全网关等密码产品、服务或技术,实现政务云使用单位终端到政务云之间的通信实体鉴别、网络边界访问控制信息完整性、通信过程中重要数据机密性和完整性等需求。

10.3 业务密码应用要求

- a) 应具有面向政务云数据库、大数据、中间件、人工智能和应用支撑等对象,数据服务、商业智能(BI)、消息服务、协同办公等对象,以及政务云资源管理等对象涉及的密码应用能力;
- b) 政务云使用单位应使用基于PKI技术的身份认证系统,对业务应用用户的登录过程提供身份鉴别服务;
- c) 政务云业务应用应遵循GB/T 39786和GB/T 43207的要求,结合自身业务的实际安全需求制定密码应用方案,提供密码技术保护重要数据在传输、存储过程中的机密性和完整性;
- d) 政务云业务应用用户所使用的身份认证服务和业务应用使用到的密码功能应由密码资源池和密码基础设施以接口调用的形式提供。

注：政务云主要保护对象及密码安全需求见附录C。

附 录 A
(资料性)
典型密码服务协议和算法技术要求

表 A.1 规定了特定安全层面中典型密码服务协议和算法的技术要求。

表 A.1 典型密码服务协议和算法技术要求

安全层面	安全指标	技术要求	应用场景示例	算法要求
网络和通信安全	重要数据传输机密性	应对传输的重要敏感数据采用通信保密性控制措施	主要针对跨网络访问的通信信道： 运维管理通道。政务云运维人员和政务云使用单位对政务云进行维护管理、操作使用的通信信道；	跨网络访问的通信信道一般采用链路加密方式，应符合 GB/T 38636 中的要求；应使用 SM2、SM4 等通过国家密码管理部门审查鉴定的加密算法对重要数据传输过程的机密性进行保护
	重要数据传输完整性	应对传输的重要敏感数据采用通信完整性控制措施； 如果传输数据的完整性被破坏，发送方应重传	用户访问业务应用通道。用户通过业务终端对业务应用进行访问的通信信道； 政务云对等实体间的通信信道； 其他跨网络访问的通信信道	跨网络访问的通信信道一般采用链路加密方式，应符合 GB/T 38636 中的要求；应使用 SM3 等通过国家密码管理部门审查鉴定的密码杂凑算法对重要数据传输过程中的完整性进行保护
应用和数据安全	重要数据传输机密性	应对传输的重要敏感数据采用传输机密性控制措施	结合通过评估的密码应用方案综合评定关键业务应用，以及关键业务应用中的关键数据为保护对象，关键数据包括但不限于鉴别数据、重要业务数据、重要审计数据、个人敏感信息，以及法律法规规定的其他重要数据类型	应使用 SM2、SM4 等通过国家密码管理部门审查鉴定的加密算法对重要数据传输过程中的机密性进行保护
	重要数据传输完整性	应对传输的重要敏感数据采用传输完整性控制措施； 如果传输数据的完整性被破坏，发送方应重传		应使用 HMAC-SM3 等密码杂凑算法，或使用 SM4 算法的 CBC 模式计算 MAC 值，或使用 SM2 算法签名验签的方式对重要数据传输过程中的完整性进行保护
	重要数据存储机密性	应对存储在文件、数据库中的重要敏感数据采用数据机密性控制措施		应使用 SM2、SM4 等通过国家密码管理部门审查鉴定的加密算法对重要数据存储过程中的机密性进行保护
	重要数据存储完整性	应对存储在文件、数据库中的重要敏感数据采用数据完整性控制措施		应使用 HMAC-SM3 算法计算重要数据哈希值，或使用 SM4 算法的 CBC 模式计算 MAC 值，或使用 SM2 算法签名验签的方式对重要数据存储过程中的完整性进行保护
	不可否认性	在可能涉及法律责任认定的应用中，应对数据原发证据和数据接收证据采用不可否认性控制措施	业务应用以及提供不可否认性功能的密码产品	必要时，应通过电子签章等方式对涉及数据处理过程采用抗抵赖性控制措施

附 录 B
(资料性)
对称密钥和非对称密钥全生命周期管理方式

表 B. 1 和表 B. 2 给出了对称密钥和非对称密钥全生命周期管理方式。

表 B. 1 对称密钥全生命周期管理

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	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	使用完成后销毁不涉及存储	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
2	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
3	数据加密存储密钥	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

表 B. 2 非对称密钥全生命周期管理

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	云平台管理员/使用单位签名私钥	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	云平台管理员/使用单位签名公钥	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	云平台管理员/使用单位加密私钥	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	云平台管理员/使用单位加密公钥	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

表 B.2 非对称密钥全生命周期管理（续）

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
5	云平台管理应用签名私钥	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	云平台管理应用签名公钥	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	云平台管理应用加密私钥	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	云平台管理应用加密公钥	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

附 录 C
(资料性)
政务云主要保护对象及密码安全需求

表 C.1 给出了政务云主要保护对象及密码安全需求。

表 C.1 政务云主要保护对象及密码安全需求

序号	相关业务	保护对象	保护对象描述	密码安全需求
1	政务云资源管理平台/云上业务应用管理/虚拟机迁移、快照恢复	身份鉴别信息	1)政务云管理员、政务云使用单位登录政务云资源管理平台、密码资源管理平台等的用户名/口令。 2)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
		政务云的重要数据	1)镜像文件和快照文件中的敏感信息、云资源管理敏感信息等重要业务数据。 2)重要审计数据。 3)政务云管理员、政务云使用单位的身份证号、手机号等个人敏感信息以及生物识别信息	<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
2		政务云资源管理平台管理云上业务应用的重要指令	虚拟机监控器(VMM)在虚拟机迁移过程中的指令等政务云资源管理平台、密码资源管理平台内部的重要指令	<input checked="" 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 type="checkbox"/> 存储完整性 <input type="checkbox"/> 不可否认性
3		镜像和快照文件	1)镜像文件。 2)快照文件	<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
4		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)政务云资源管理平台管理云上业务应用的重要业务日志	<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

表 C.1 政务云主要保护对象及密码安全需求（续）

序号	相关业务	保护对象	保护对象描述	密码安全需求
5	政务云资源管理平台/云上业务应用管理/虚拟机迁移、快照恢复	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的信息。 2)物理和虚拟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。 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	<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
6		重要信息资源安全标记	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。 2)政务云资源管理平台管理云上业务应用的重要信息资源安全标记	<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
7		重要可执行程序	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	<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
8		视频监控音像记录	政务云所在物理机房等重要物理区域的视频监控音像记录	<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
9		电子门禁系统进出记录	政务云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	<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
10		进入重要物理区域的人员的身份鉴别	进入政务云所在物理机房等重要物理区域人员的身份鉴别	<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

表 C.1 政务云主要保护对象及密码安全需求（续）

序号	相关业务	保护对象	保护对象描述	密码安全需求
11	政务云资源管理平台/云上业务应用管理/虚拟机迁移、快照恢复	通信双方的身份鉴别	1)政务云中客户端到服务端通信信道的身份鉴别。 2)政务云对等实体间(如不同云之间)通信信道的身份鉴别	<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
12		网络设备接入时的身份鉴别	从外部连接到内部网络的设备接入认证时的身份鉴别	<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
13		登录操作系统和数据库系统的用户身份鉴别	政务云管理员、政务云使用单位登录通用设备、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	<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
14		重要可执行程序来源	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	<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
15		云平台用户的身份鉴别	1)政务云管理员身份鉴别。 2)政务云使用单位身份鉴别	<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
16		数据原发行为、数据接收行为	政务云管理员和政务云使用单位的关键操作	<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

参 考 文 献

- [1] GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式规范
- [2] 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
- [3] GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法
- [4] GB/T 32907—2016 信息安全技术 SM4 分组密码算法
- [5] GB/T 33560—2017 信息安全技术 密码应用标识规范
- [6] GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范
- [7] GB/T 35291—2017 信息安全技术 智能密码钥匙应用接口规范
- [8] GB/T 36322—2018 信息安全技术 密码设备应用接口规范
- [9] GB/T 36968—2018 信息安全技术 IPSec VPN 技术规范
- [10] GB/T 37033—2018 信息安全技术 射频识别系统密码应用技术要求
- [11] GB/T 37092—2018 信息安全技术 密码模块安全要求
- [12] GB/T 38540—2020 信息安全技术 安全电子签章密码技术规范
- [13] GB/T 38556—2020 信息安全技术 动态口令密码应用技术规范
- [14] GB/T 38629—2020 信息安全技术 签名验签服务器技术规范
- [15] GB/T 43206—2023 信息安全技术 信息系统密码应用测评要求
- [16] GB/T 44230—2024 政务信息系统基本要求
- [17] GM/T 0018—2012 密码设备应用接口规范
- [18] GM/T 0024—2014 SSL VPN 技术规范
- [19] GM/T 0025—2014 SSL VPN 网关产品规范
- [20] GM/T 0026—2014 安全认证网关产品规范
- [21] GM/T 0027—2014 智能密码钥匙技术规范
- [22] GM/T 0030—2014 服务器密码机技术规范
- [23] GM/T 0104—2021 云服务器密码机技术规范
- [24] GM/T 0116—2021 信息系统密码应用测评过程指南
- [25] GM/Y 5001—2019 密码标准应用指南
- [26] GM/Y 5002—2018 云计算身份鉴别服务密码标准体系
- [27] GW 0013—2017 政务云安全要求
- [28] GW 0202—2014 国家电子政务外网安全接入平台技术规范
- [29] GW 0206—2014 接入政务外网的局域网安全技术规范
- [30] 中华人民共和国密码法(中华人民共和国主席令第三十五号)
- [31] 商用密码管理条例(中华人民共和国国务院令 第760号)
- [32] 江苏省政务“一朵云”建设总体方案(苏政办发[2023]36号)
- [33] 政务领域政务云密码应用与安全性评估实施指南
- [34] 政务领域政务服务平台密码应用与安全性评估实施指南
- [35] 信息系统密码应用高风险判定指引
- [36] 商用密码应用安全性评估量化评估规则
- [37] 商用密码应用安全性评估FAQ(第三版)
- [38] 霍炜,郭启全,马原. 商用密码应用与安全性评估[M]. 电子工业出版社,2020.