

DB32

江苏省地方标准

DB32/T 5073.3—2025

政务“一朵云”安全管理体系规范  
第3部分：密码应用安全性评估

Security management system specification for the “cloud” of government  
affairs—Part 3: security assessment of 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 总体要求 .....2

5 评估指南 .....3

6 结果应用 .....6

附录A(资料性) 主要技术要求解决方法 .....8

附录B(资料性) 密钥管理要求 .....9

参考文献 .....10

## 前 言

本文件按照 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》的规定起草。

本文件是 DB32/T 5073《政务“一朵云”安全管理体系规范》的第3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。

本文件由江苏省数据局提出并组织实施。

本文件由江苏省数据标准化技术委员会(JS/TC 88)归口。

本文件起草单位：江苏省大数据管理中心。

本文件主要起草人：吴中东、忻超、黄敏、刘尧、杨扬、王文娟、刘鑫、蔡一凡、谷和启、张腾标、卢秋如、任明聪、衡帅。

## 引 言

为加强统筹规划,全面提升全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》(苏政发〔2022〕44号)、《江苏省政务“一朵云”建设总体方案》(苏政发〔2023〕36号)的要求,建立健全全省政务“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3部分：密码应用安全性评估

### 1 范围

本文件给出了政务云密码应用安全性评估总体要求,以及评估相关的阶段、类型、对象、依据、流程、内容、输出成果和参与主体。

本文件适用于政务云运行管理单位、政务云使用单位开展信息系统密码应用建设和商用密码应用安全性评估工作。

### 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 22240—2020	信息安全技术	网络安全等级保护定级指南
GB/T 37092—2018	信息安全技术	密码模块安全要求
GB/T 39786—2021	信息安全技术	信息系统密码应用基本要求
GB/T 43206—2023	信息安全技术	信息系统密码应用测评要求
GB/T 43207—2023	信息安全技术	信息系统密码应用设计指南
GM/T 0116—2021	信息系统密码应用测评过程指南	
GM/T 0094—2020	公钥密码应用技术体系框架规范	

### 3 术语和定义

GB/T 25069—2022 和 GM/Z 0001—2013 界定的以及下列术语和定义适用于本文件。

#### 3.1

**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]

#### 3.2

**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(3.1),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。

### 3.3

#### 商用密码 **commercial cryptography**

采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

[来源:《商用密码管理条例》,第二条,有修改]

### 3.4

#### 商用密码应用安全性评估 **security assessment of commercial cryptography application**

按照有关法律法规和标准规范,对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动,简称“密评”。

[来源:《商用密码应用安全性评估管理办法》,第二条]

### 3.5

#### 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]

### 3.6

#### 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]

## 4 总体要求

### 4.1 密评类型

密评包括商用密码应用方案评估(简称“方案评估”)和信息系统商用密码应用安全性评估(简称“系统评估”)。

### 4.2 密评对象

政务云密评对象包括:

- a) 方案评估对象为密码应用方案;
- b) 系统评估对象为政务云独立开展或拟开展等级保护定级的物理环境设施、网络通信设施、计算资源设施、密码基础设施、网络安全设施或其组合;或政务信息系统及其他相关对象。

### 4.3 密评要求

政务云密评总体要求包括:

- a) 应在政务云规划阶段开展方案评估;
- b) 应在政务云建设阶段开展系统评估;
- c) 应在政务云运行阶段开展系统评估或方案评估。

5 评估指南

5.1 规划阶段

5.1.1 评估对象

本文件 4.2 密评对象 a) 条款中所指对象。

5.1.2 评估依据

- 规划阶段的评估依据包括：
- GB/T 39786—2021；
  - GB/T 43207—2023；
  - 《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》；
  - 密码算法/技术/产品等相关标准规范；
  - 《密码应用方案》商用密码应用安全性评估报告(模板)；
  - 信息系统业务设计、安全需求文档；
  - 网络安全等级保护测评报告(如有)；
  - 其他相关依据。

5.1.3 评估流程

方案评估流程包括方案评估准备、开展方案评估、评估结果反馈、方案整改、形成评估报告、完成方案评估。具体流程如图 1 所示。

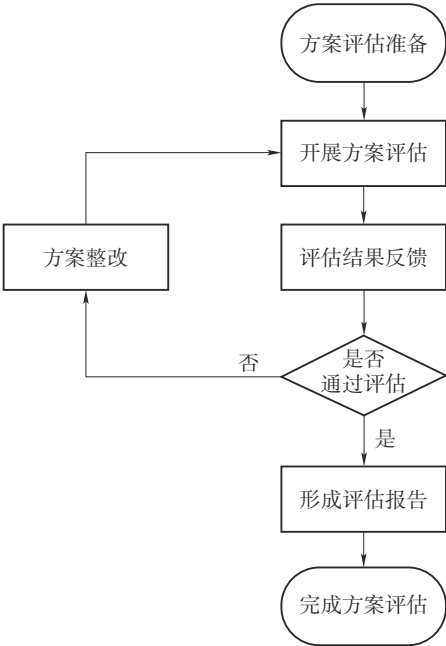


图 1 方案评估流程

#### 5.1.4 评估内容

通过形式审查和技术审查等方式对密码应用方案进行评估,具体评估内容包括:

- a) 形式审查:
  - 1) 要素完整性:是否涵盖 GB/T 43207—2023 附录 A 的全部核心要素;
  - 2) 内容一致性:描述的网络情况、服务对象、访问方式等与网络拓扑图是否一致,密码应用需求与密码应用设计是否相匹配等。
- b) 技术审查:
  - 1) 密码应用需求的全面性、合理性和针对性;
  - 2) 选取适用指标的准确性;
  - 3) 不适用指标论证的充分性;
  - 4) 安全控制措施(密码应用措施和/或风险替代措施)是否合理、有效(不存在高风险);
  - 5) 密码应用流程和机制是否具备可实施性;
  - 6) 密码保护措施是否达到相应的商用密码应用要求、相关描述是否详尽;
  - 7) 密码技术/产品/服务选用是否合规,密钥管理是否安全;
  - 8) 初步量化评估分数能否达到阈值等。

本阶段面向政务云的方案设计,建设方应依据政务云密码应用需求设计密码应用框架,按照 GB/T 43207—2023 附录 A,重点关注相应的密码应用措施(如保护对象、措施涉及的密码算法、技术、产品、服务的选用及相关密钥管理等)和替代性风险控制措施(如替代原因、具体措施风险评估论证结果等),密钥管理按照附录 B 的规定执行。

注:密码应用措施的主要技术要求解决方法参见附录 A。

#### 5.1.5 参与主体

建设单位、设计单位。

#### 5.1.6 输出成果

方案评估报告。

#### 5.1.7 评估结论

方案评估结论为通过和不通过。当评估对象论证的所有指标安全控制措施评估结果均为通过,且初步量化评估分数能够达到阈值要求,则方案评估结论为通过;否则,不通过。

### 5.2 建设阶段

#### 5.2.1 评估对象

本文件 4.2 密评对象 b) 条款中所指对象,具体组成包括:

- a) 密码产品、密码服务、密码算法及密钥管理实现;
- b) 物理和环境:机房等重要区域及其电子门禁系统和视频监控系统;
- c) 网络和通信:网络通信信道以及提供通信保护功能的设备或组件、密码产品、网络边界访问控制功能、设备入网接入认证功能的设备或组件、密码产品;
- d) 设备和计算:通用设备(及其操作系统、数据库管理系统)、网络及安全设备、密码设备、各类虚拟设备,以及提供完整性保护功能、来源真实性功能的密码产品;



- e) 应用和数据:政务云以及提供身份鉴别功能、机密性保护功能、完整性保护功能、不可否认性功能的密码产品;
- f) 安全管理:政务云相关商用密码应用安全管理制度、实施方案、操作规程类文档、记录表单类文档、系统相关人员、攻防演习报告、整改记录、应急处置记录类文档、安全事件发生情况及处置情况报告等。

5.2.2 评估依据

建设阶段的评估依据包括:

- GB/T 22240—2020;
- GB/T 39786—2021;
- GB/T 43206—2023;
- GM/T 0116—2021;
- 《信息系统密码应用方案》;
- 《〈信息系统密码应用方案〉商用密码应用安全性评估报告》;
- 《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》;
- 密码算法/技术/产品等相关标准规范;
- 网络安全等级保护测评报告(如有);
- 其他相关依据。

当政务云按照 GB/T 22240 开展等级保护定级时,应采用 GB/T 39786 对应等级密码要求开展系统评估。即等级保护第一、二、三级的政务云或政务云其支撑的政务信息系统,按照 GB/T 39786 中第一、二、三级密码要求开展评估。等级保护第四级、第五级的政务云或其支撑的政务信息系统,按照 GB/T 39786 中第四级密码要求开展评估。

当政务云未开展等级保护定级时,应至少按照 GB/T 39786 中第三级密码要求开展系统评估。

5.2.3 评估流程

系统评估流程包括系统评估准备、实施系统评估、整改建议与实施、形成评估报告、完成方案评估。具体流程如图 2 所示。

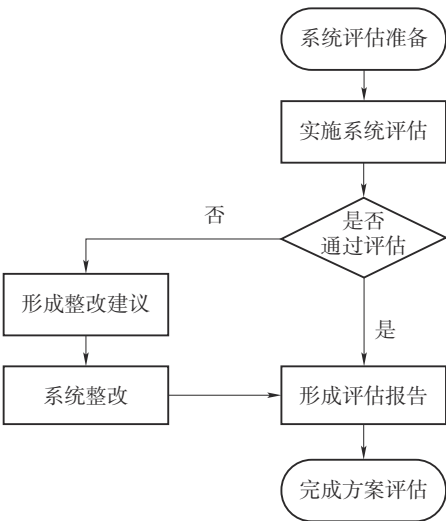


图 2 系统评估流程

#### 5.2.4 评估内容

建设阶段政务云密评具体评估包括：

- a) 政务云密码应用的合规性、正确性、有效性；
- b) GB/T 39786中规定的对应等级的评估指标内容；
- c) 通过评估的密码应用方案中设计的密码实现内容。

注：若密码应用方案在本阶段仍未通过评估，按照规划阶段的方案评估要求先行完成方案评估。

#### 5.2.5 参与主体

建设单位、开发单位、设计单位、密码厂商、密评机构等。

#### 5.2.6 输出成果

系统评估报告。

#### 5.2.7 评估结论

系统评估结论包括符合、基本符合和不符合。具体评估结论参考《信息系统密码应用高风险判定指引》和《商用密码应用安全性评估量化评估规则》。

### 5.3 运行阶段

#### 5.3.1 方案评估

政务云投入运行后，存在改建或扩建情况，且其功能或业务范围与GB/T 39786对应的评估要求超出原密码应用方案时，建设单位应对原密码应用方案进行修订，并对修改后的密码应用方案重新开展方案评估。评估过程应符合5.1的相关要求。

#### 5.3.2 系统评估

政务云投入运行后，建设单位应每年至少组织开展一次系统评估：

- a) 在开展系统评估时，当存在密码应用方案修订情况的，应提供通过评估的方案评估报告；
- b) 评估过程应符合5.2的相关要求。

### 6 结果应用

#### 6.1 结果备案

政务云密评结果的备案由政务云建设单位实施，具体按照密码管理部门备案要求执行。

#### 6.2 结果复用

政务信息系统密评应按照以下情形综合考虑对政务云密评结果的复用：

- a) 当政务云相关设施组合作为一个对象开展网络安全等级保护主体定级，且密评结论为符合或基本符合时，其支撑的政务信息系统密评结论才可能为符合或基本符合。
  - 1) 若政务信息系统等级保护级别高于政务云等级保护级别，则政务云相关密码服务无法直接被复用，应对政务信息系统按照其实际等级保护级别重新进行密评；

- 2) 若政务信息系统等级保护级别不高于政务云等级保护级别,且政务云密评结论为符合或基本符合时,则政务信息系统密评可复用政务云密评结果。
- b) 当政务云相关设施分为多个对象开展网络安全等级保护主体定级时,应分别分析不同对象密码应用和密评结果,将分析结果综合复用于政务信息系统密评。

附 录 A  
(资料性)  
主要技术要求解决方法

表 A.1 给出了主要技术要求评估整改方法。

表 A.1 主要技术要求解决方法

序号	技术要求	常见问题	解决方法
1	机密性	重要数据明文传输、存储	使用密码技术的加解密功能实现机密性
2	完整性	电子门禁系统和视频监控系统进出记录、日志记录、访问控制信息等明文存储	使用基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现完整性
3	真实性	业务应用用户仅使用用户名、口令进行身份鉴别	使用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码机制、基于公钥密码算法的数字签名机制等密码技术实现真实性
4	不可否认性	在可能涉及法律责任认定的业务应用中,信息交换主体否认其数据原发行为或数据接收行为	使用基于公钥密码算法的数字签名机制等密码技术来保证数据原发行为的不可否认性和数据接收行为的不可否认性
5	密码产品	采用的密码产品未经国家密码管理部门核准或密码产品安全等级不符合系统密码应用基本要求	选用具备商用密码产品认证证书的密码产品,且安全等级符合 GB/T 37092 的相关要求
6	密码服务	采用的第三方电子认证服务或电子政务电子认证服务未经国家密码管理部门颁发密码服务许可	选用电子认证服务使用密码许可单位名录、电子政务电子认证服务机构目录中的单位提供密码服务

附 录 B  
(资料性)  
密钥管理要求

表 B.1 给出了密钥管理要求策略。

表 B.1 密钥管理要求

序号	阶段	管理要求
1	产生	密钥可以以随机产生、协商产生等不同的方式来产生。密钥在符合 GB/T 37092 的密码产品中产生是十分必要的,产生的同时可在密码产品中记录密钥关联信息,包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等
2	分发	密钥分发是密钥从一个密码产品传递到另一个密码产品的过程,分发时应注意抗截取、篡改、假冒等攻击,保证密钥的机密性、完整性以及分发者、接收者身份的真实性等
3	存储	密钥不以明文方式存储在密码产品外部是十分必要的,并采取严格的安全防护措施,防止密钥被非授权的访问或篡改。 公钥是例外,可以以明文方式在密码产品外存储、传递和使用,但有必要采取安全防护措施,防止公钥被非授权篡改
4	使用	每个密钥一般只有单一的用途,明确用途并按用途正确使用是十分必要的。密钥使用环节需要注意的安全问题是:使用密钥前获得授权、使用公钥证书前对其进行有效性验证、采用安全措施防止密钥的泄露和替换等。另外,有必要为密钥设定更换周期,并采取有效措施保证密钥更换时的安全性
5	更新	密钥更新发生在密钥超过使用期限、已泄露或存在泄露风险时,根据相应的更新策略进行更新
6	归档	如果信息系统中有密钥归档需求,则根据实际安全需求采取有效的安全措施,保证归档密钥的安全性和正确性。需要注意的是,归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。如果执行密钥归档,则有必要生成审计信息,包括归档的密钥、归档的时间等
7	撤销	密钥撤销一般针对公钥证书所对应的密钥。当证书到期后,密钥自然撤销;也可以按需进行密钥撤销,撤销后的密钥不再具备使用效力
8	备份	对于需要备份的密钥,采用安全的备份机制对密钥进行备份是必要的,以确保备份密钥的机密性和完整性,这与密钥存储的要求是一致的。密钥备份行为是审计涉及的范围,有必要生成审计信息,包括备份的主体、备份的时间等
9	恢复	可以支持用户密钥恢复和司法密钥恢复。密钥恢复行为是审计涉及的范围,有必要生成审计信息,包括恢复的主体、恢复的时间等
10	销毁	密钥销毁要注意的是销毁过程的不可逆,即无法从销毁结果中恢复原密钥

### 参 考 文 献

- [1] 中国密码学会密评联委会. 信息系统密码应用高风险判定指引.[2021-12]
  - [2] 中国密码学会密评联委会. 商用密码应用安全性评估量化评估规则.[2023-8]
  - [3] 中国密码学会密评联委会. 商用密码应用安全性评估FAQ.[2023-10]
  - [4] 江苏省政务信息化项目密码应用与评估备案指南(试行)(苏密局字[2020]43号)
  - [5] 江苏省政务“一朵云”建设总体方案(苏政发[2023]36号)
  - [6] 中国密码学会密评联委会. 政务领域政务云密码应用与安全性评估实施指南.[2024-04]
  - [7] GB/T 38673—2020 信息技术 大数据 大数据系统基本要求
  - [8] GM/Y 5001—2019 密码标准应用指南
  - [9] GM/Y 5002—2018 云计算身份鉴别服务密码标准体系
  - [10] GW 0013—2017 政务云安全要求
  - [11] GW 0202—2014 国家电子政务外网安全接入平台技术规范
  - [12] GW 0206—2014 接入政务外网的局域网安全技术规范
-