

### 电子政务公共服务云平台服务目录

E-Government public service cloud platform service catalogue

2026 - 08 - 19 发布

2026 - 10 - 01 实施

目 次

前言 ..... II

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 1

5 服务分类概述 ..... 3

6 IaaS 服务..... 3

    6.1 计算服务 ..... 3

    6.2 存储服务 ..... 5

    6.3 网络服务 ..... 7

    6.4 备份及容灾服务 ..... 8

7 PaaS 服务..... 8

    7.1 操作系统服务 ..... 8

    7.2 数据库服务 ..... 8

    7.3 中间件服务 ..... 9

8 云安全保障服务 ..... 9

参考文献 ..... 13

## 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。

本标准由德州市大数据局提出并归口。

本标准起草单位：德州市大数据局。

本标准主要起草人：李广云、曹晓东、王艳红、邢冠宇、田宁宁、王承元、陈慧建、梁帅、李程。

# 电子政务公共服务云平台服务目录

## 1 范围

本文件规定了德州市电子政务公共服务云平台所提供云服务的分类与规格、服务描述等内容。  
本文件适用于德州市电子政务公共服务云平台所提供云服务的分类、规格及目录规划管理。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 25647—2010 电子政务术语
- GB/T 34078.1—2017 基于云计算的电子政务公共平台总体规范 第1部分：术语和定义

## 3 术语和定义

GB/T 25647—2010、GB/T 34078.1—2017界定的以及下列术语和定义适用于本文件。

### 3.1

**平均无故障时间** mean time between failures

衡量产品的可靠性指标。单位为“小时”。它反映了产品的时间质量，是体现产品在规定时间内保持功能的一种能力。

### 3.2

**平台可用性** platform availability

在要求的外部资源得到保证的前提下，服务在规定的条件下和规定的时刻或时间区间内处于可执行规定功能状态的能力。

## 4 缩略语

下列缩略语适用于本文件，见表1：

表1 缩略语

| 缩略语  | 英文全称                                | 中文含义      |
|------|-------------------------------------|-----------|
| API  | Application Programming Interface   | 应用程序编程接口  |
| CA   | Certificate Authority               | 证书颁发机构    |
| CPU  | Central Processing Unit             | 中央处理器     |
| DDoS | Distributed Denial of Service       | 分布式拒绝服务攻击 |
| DHCP | Dynamic Host Configuration Protocol | 动态主机配置协议  |
| FTP  | File Transfer Protocol              | 文件传输协议    |

|        |                                                 |              |
|--------|-------------------------------------------------|--------------|
| GPU    | Graphics Processing Unit                        | 图形处理器        |
| 缩略语    | 英文全称                                            | 中文含义         |
| HA     | High Availability                               | 高可用性         |
| HTTP   | HyperText Transfer Protocol                     | 超文本传输协议      |
| HTTPS  | HTTP Secure                                     | 安全超文本传输协议    |
| I/O    | Input/Output                                    | 输入输出         |
| IPSec  | Internet Protocol Security                      | 网络协议安全协议     |
| MAC    | Media Access Control                            | 媒体访问控制（地址）   |
| Mbps   | Megabits per second                             | 兆位每秒         |
| NVME   | Non-Volatile Memory Express                     | 非易失性存储器快速通道  |
| OS     | Operating System                                | 操作系统         |
| POP3   | Post Office Protocol 3                          | 邮局协议第三版      |
| RAID   | Redundant Array of Independent Disks            | 独立磁盘冗余阵列     |
| Redis  | Remote Dictionary Server                        | 远程字典服务器（数据库） |
| SAS    | Serial Attached SCSI                            | 串行连接 SCSI    |
| SATA   | Serial ATA                                      | 串行高级技术附件     |
| SDN    | Software Defined Network                        | 软件定义网络       |
| SMB    | Server Message Block                            | 服务器消息块协议     |
| SMTP   | Simple Mail Transfer Protocol                   | 简单邮件传输协议     |
| SQL    | Structured Query Language                       | 结构化查询语言      |
| SSD    | Solid-State Drive                               | 固态硬盘         |
| SSL    | Secure Sockets Layer                            | 安全套接字层       |
| TCP    | Transmission Control Protocol                   | 传输控制协议       |
| TLS    | Transport Layer Security                        | 传输层安全协议      |
| URL    | Uniform Resource Locator                        | 统一资源定位符      |
| USB    | Universal Serial Bus                            | 通用串行总线       |
| VxLAN  | Virtual Extensible LAN                          | 虚拟可扩展局域网     |
| Geneve | Generic Network Virtualization<br>Encapsulation | 通用网络虚拟化封装协议  |
| VM     | Virtual Machine                                 | 虚拟机          |
| VPN    | Virtual Private Network                         | 虚拟专用网络       |
| vCPU   | Virtual CPU                                     | 虚拟中央处理器      |
| WAF    | Web Application Firewall                        | Web 应用防火墙    |

|      |                             |         |
|------|-----------------------------|---------|
| IaaS | Infrastructure as a Service | 基础设施即服务 |
| PaaS | Platform as a Service       | 平台即服务   |

## 5 服务分类概述

电子政务公共服务云平台提供的服务包括云资源服务及云相关服务，为政府部门提供IT资源服务与安全服务。本标准包括将其分为IaaS服务、PaaS服务、安全保障服务三类，并对各类服务的功能和性能进行要求。

## 6 IaaS 服务

### 6.1 计算服务

计算服务要求如下：

- a) 以弹性云服务器方式提供计算服务，弹性云服务器应包括虚拟机和物理机；
- b) 计算服务还应提供容器服务，包括容器引擎和容器镜像；
- c) 应支持国内外主流计算平台，如x86、ARM、C86、LoongArch架构等；
- d) 云平台应采用自主可控云平台产品；
- e) 应提供隔离手段保障计算、存储、管理接入等域的安全隔离；
- f) 应提供虚拟机热迁移功能，在迁移的过程中不影响用户对虚拟机的使用；
- g) 应提供故障迁移【虚拟机 HA(High Available)】机制；
- h) 应提供从镜像创建和从卷创建的虚拟机的重建功能；
- i) 应提供虚拟机模板功能，可实现基于虚拟机实例的模板创建；
- j) 应提供虚拟机快速部署功能，并支持集群自动搭建；
- k) 应支持虚拟机生命周期管理，并可根据标签执行查找、过滤等操作；
- l) 应支持虚拟机镜像生命周期管理，以及镜像的创建、上传、删除、下载、查询等操作；
- m) 应提供虚拟机和虚拟磁盘快照功能，可利用快照对虚拟机或虚拟磁盘数据进行恢复；
- n) 应提供根据业务需要跨存储迁移虚拟机数据盘的功能；
- o) 应提供单盘可共享给多个虚拟机的功能；
- p) 应支持对虚拟机按照不同的用户权限进行创建、删除、启动、关闭、重启、修改、迁移等各类管理；
- q) 虚拟机之间应做到隔离保护；
- r) 需提供灵活的主机组管理功能，支持虚拟机对特殊硬件（如 SSD 盘）的需求；
- s) 应支持虚拟机规格动态调整，虚拟化平台可以灵活调整虚拟机的配置规格，包括调整 vCPU个数，内存大小，磁盘卷个数，调整虚拟卷的大小；
- t) 云平台应支持基于国产操作系统部署；
- u) 云平台支持创建虚拟机时指定网络、IP 地址和允许/禁止的端口，支持未开启DHCP 协议场景使用指定 IP 地址配置虚拟机。
- v) 云平台应规划测试区域，为上云业务系统提供测试资源。
- w) 弹性云服务器规格包括CPU规格、内存大小、硬盘规格、网卡服务等指标，见表2所示；

表2 计算服务目录

| 服务分类 | 服务项目       | 服务描述                                                                                                                                     | 规格配置               |                  |      |      |      |
|------|------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------------------|------|------|------|
|      |            |                                                                                                                                          | 架构类型               | 处理器规格            | 内存规格 | 硬盘规格 | 网卡服务 |
| 计算服务 | X86 云计算服务器 | X86 架构计算服务，CPU 每次最小增加单位为 2 核，最高上限为 128 核，CPU 主频≥2.2GHz；内存每次最小增加单位为 2GB，最高上限为 512GB。                                                      | -                  | CPU 核数           | 内存容量 | -    | -    |
|      | 国产云计算服务器   | 国产化 cpu 计算服务，CPU 主频≥2.0GHz，每次最小配置单位为 2 核，最高上限为 128 核。国产化云主机内存，内存≥DDR4，每次最小配置单位为 2GB，最高上限为 512GB。CPU 符合《安全可靠测评结果公告》要求，注：根据测评结果实时更新。       | -                  | CPU 核数           | 内存容量 | -    | -    |
|      | 国产 GPU 云主机 | 基于国产化 CPU 和算力卡的云物理主机服务，用于云上私有化部署或训练生成式大模型，单台处理器≥4 路，单颗处理器≥48 核，主频≥2GHz，内存≥1024G。包含 8 张算力卡，单卡显存容量≥64GB，INT8 算力≥512 TOPS，FP16 算力≥256TFLOPS | -                  | CPU 核数 + GPU 卡数量 | 内存容量 | -    | -    |
|      | 云物理服务器     | 基于海光等 x86/c86 架构 CPU 的云物理主机服务，单台处理器≥2 路；单路处理器≥32 核，主频≥2GHz；内存≥128G，RAID 卡≥1                                                              | 基础 I 型（x86/c86 架构） | -                | -    | -    | -    |

|  |      |                                                                               |                     |   |     |             |         |
|--|------|-------------------------------------------------------------------------------|---------------------|---|-----|-------------|---------|
|  |      | 基于鲲鹏、飞腾等 ARM 架构国产化 CPU 的云物理主机服务，单台处理器≥2 路；单路处理器≥48 核，主频≥2GHz；内存≥128G，RAID 卡≥1 | 基础 II 型<br>(ARM 架构) | - | -   | -           | -       |
|  | 扩展配件 | 云物理服务器增配配件，32G 内存*1                                                           | -                   | - | 32G | -           | -       |
|  |      | 云物理服务器增配配件，1TB SAS 硬盘*1                                                       | -                   | - | -   | 1TB SAS 硬盘  | -       |
|  |      | 云物理服务器增配配件，1TB SSD 硬盘*1                                                       | -                   | - | -   | 1TB SSD 硬盘  | -       |
|  |      | 云物理服务器增配配件，1TB NVME 硬盘*1                                                      | -                   | - | -   | 1TB NVME 硬盘 | -       |
|  |      | 提供物理机增配配件，万兆网卡（配置光模块）*1                                                       | -                   | - | -   | -           | 万兆网卡    |
|  |      | 云物理服务器增配配件，200G 网卡（配置光模块）*1                                                   | -                   | - | -   | -           | 200G 网卡 |
|  |      | 云物理服务器增配配件，400G 网卡（配置光模块）*1                                                   | -                   | - | -   | -           | 400G 网卡 |
|  |      | 云物理服务器增配配件，800G 网卡（配置光模块）*1                                                   | -                   | - | -   | -           | 800G 网卡 |

## 6.2 存储服务

存储服务要求如下：

### 1、基本功能

- 存储服务以块存储（云硬盘）提供存储服务；
- 存储服务应支持国内外主流计算平台，如x86、ARM、C86、LoongArch架构等；
- 块存储（云硬盘）服务规格包括磁盘容量、读写性能等指标；
- 高性能存储与普通存储可按应用需求选择不同磁盘类型，实现数据按需存储；
- 应提供高性能存储和普通存储两种不同 IO 级别的存储资源池
- 需支持快照的创建、挂载、升级、删除、查询等操作；
- 需支持卷/卷类型的创建、升级、删除、查询等操作；

### 2、安全性

- h) 高性能存储与普通存储采用先进的磁盘容错技术;
- i) 提供分布式存储或集中式存储两种存储架构;
- j) 分布式存储可实现数据传输过程中的用户鉴权处理;
- 3、扩容性/扩展性
- k) 需支持在线扩容, 调整期间不影响存储服务
- l) 具有 IO 优先级控制和 QoS 保证
- m) 具有增量扩容和自动数据平衡能力
- n) 需提供面向关键业务的高可用持续服务能力;
- 4、存储空间分配
- o) 具备按照业务使用要求分配存储空间的功能;
- p) 服务目录, 见表3所示。

表3 存储服务目录

| 服务分类 | 服务项目    | 服务描述                                                                                                         | 规格配置         |           |
|------|---------|--------------------------------------------------------------------------------------------------------------|--------------|-----------|
|      |         |                                                                                                              | 容量规格         | 配置规格      |
| 存储服务 | X86 块存储 | 为云服务器提供块级别存储空间, 一块云硬盘只能挂载到单台云服务器上, 单盘不大于 32768GB (32TB), 物理存储设备为 SATA 机械硬盘。普通云盘适用于数据不经<br>常访问的低 I/O 负载的业务场景。 | 磁盘容量<br>(GB) | 普通 IO 云硬盘 |
|      |         | 为云服务器提供块级别存储空间, 一块云硬盘只能挂载到单台云服务器上, 单盘不大于 32768GB (32TB), 物理存储设备为 SAS 机械硬盘。高效云盘适用于一般工作<br>负载的业务场景。            | 磁盘容量<br>(GB) | 高 IO 云硬盘  |
|      |         | 为云服务器提供块级别存储空间, 一块云硬盘只能挂载到单台云服务器上, 单盘不大于 32768GB (32TB), 物理存储设备为固态硬盘。SSD 云盘适用于数据访问频繁<br>的高 I/O 负载的业务场景。      | 磁盘容量<br>(GB) | 超高 IO 云硬盘 |
|      | 国产块存储   | 为云服务器提供块级别存储空间, 一块云硬盘只能挂载到单台云服务器上, 单盘不大于 32768GB (32TB), 物理存储设备为 SAS 机械硬盘。高效云盘适用于一般工作<br>负载的业务场景。            | 磁盘容量<br>(GB) | 国产化高效云硬盘  |

|  |  |                                                                                                 |              |             |
|--|--|-------------------------------------------------------------------------------------------------|--------------|-------------|
|  |  | 为云服务器提供块级别存储空间，一块云硬盘只能挂载到单台云服务器上，单盘不大于 32768GB（32TB），物理存储设备为固态硬盘。SSD 云盘适用于数据访问频繁的高 I/O 负载的业务场景。 | 磁盘容量<br>(GB) | 国产化 SSD 云硬盘 |
|--|--|-------------------------------------------------------------------------------------------------|--------------|-------------|

### 6.3 网络服务

网络服务要求如下：

- a) 需支持整体网络通过控制器统一管理，全程可视化配置；
- b) 需支持并提供网络虚拟化功能，具备弹性扩展能力；
- c) 需支持对云平台内的网络设备进行统一监控、告警；
- d) 网络分为业务平面、管理平面和存储平面；
- e) 核心骨干设备、出口设备、骨干线路等需要支持冗余备份；
- f) 具备虚拟路由功能，支持定制虚拟路由器的路由规则；
- g) 交换机具备虚拟化部署能力；
- h) 支持用户可自定义虚拟主机的网络拓扑和 IP；
- i) 实现具备虚拟机之间、虚拟机与云平台之外进行网络通信；
- j) 需支持 SDN 架构，支持 VxLAN/Geneve 技术；
- k) 支持与互联网、电子政务外网及行业部门专网的连接；
- l) 平台内网络至少划分为业务网、存储网、管理网等；
- m) 云平台应具备虚拟安全组服务，实现重要业务网络安全隔离；
- n) 具备网络隔离功能，实现隔离子网之间 IP、端口、协议的访问控制；
- o) 在 Overlay 环境下，可以给不同的租户分配相同 IP 网段；
- p) 需支持并提供负载均衡器功能；
- q) 具备支持业务 IPv6 单栈、IPv6/IPv4 双栈运行的能力；
- r) 网络服务应支持国内外主流计算平台，如 x86、ARM、C86、LoongArch 架构等。
- q) 服务目录，见表4所示。

表4 网络服务目录

| 服务分类 | 服务项目 | 服务描述                                                                | 规格配置      |
|------|------|---------------------------------------------------------------------|-----------|
| 网络   | 互联网  | 提供 1 个互联网 IP 地址，可以分配到云服务器、负载均衡、物理主机上，带宽另行计费。                        | 互联网 IP 地址 |
|      |      | 1Mbps 的互联网带宽资源，上下行带宽一致，单位 Mbps，1024Mbps=1Gbps。                      | 互联网带宽     |
|      | 负载均衡 | 最大连接数 50000，支持包含 TCP 协议的四层、HTTP 协议和 HTTPS 协议的七层负载均衡；支持对应用程序的健康状态检查  | 标准型       |
|      |      | 最大连接数 100000，支持包含 TCP 协议的四层、HTTP 协议和 HTTPS 协议的七层负载均衡；支持对应用程序的健康状态检查 | 增强型       |

6.4 备份及容灾服务

备份及容灾服务要求如下：

- a) 备份服务应提供对弹性云服务器的整机备份服务，包括虚拟机及物理机的备份服务；
- b) 容灾服务应根据用户要求提供容灾服务，包括同城及异地容灾；
- c) 容灾及备份服务应支持国内外主流计算平台，如x86、ARM、C86、LoongArch架构等；
- d) 备份及容灾服务具体描述见表5所示；

表5 备份及容灾服务目录

| 服务分类 | 服务项目     | 服务描述                                                                             | 规格配置 |
|------|----------|----------------------------------------------------------------------------------|------|
| 备份服务 | 同城异地数据备份 | 安全基线类服务。同城异地备份，提供数据备份、文件备份、云主机定时备份服务                                             | GB   |
|      | 同城异地数据归档 | 同城异地归档，采用归档型对象存储，提供数据归档、文件归档服务                                                   | GB   |
| 容灾服务 | 同城异地实时备份 | 同城异地灾备服务，支持利用政务外网或者专线将数据实时传送数据。包括数据库灾备、云主机灾备服务。灾备数据库和云主机所需的 CPU、内存、网络、安全等服务另行计费。 | GB   |

7 PaaS 服务

7.1 操作系统服务

提供存量X86服务器操作系统。提供国产操作系统，符合《安全可靠测评结果公告》《操作系统政府采购需求标准（2023 年版）》要求的操作系统，见表6所示。

表6 操作系统软件服务目录

| 服务分类     | 服务项目   | 服务描述                                                                        | 规格配置              |
|----------|--------|-----------------------------------------------------------------------------|-------------------|
| 操作系统软件服务 | 商业操作系统 | 提供存量 X86 服务器操作系统。                                                           | Windows<br>Server |
| 操作系统软件服务 | 商业操作系统 | 符合《安全可靠测评结果公告》《安全可靠测评工作指南 v3.0》《操作系统政府采购需求标准（2023 年版）》要求的操作系统，注：根据测评结果实时更新。 | 国产操作系统            |

7.2 数据库服务

用于存量X86服务器的数据库软件计费，及提供国产集中式数据库软件，符合安全可靠测评结果公告要求的数据库软件，见表7所示；

表7 数据库服务目录

| 服务分类    | 服务项目           | 服务描述                                          | 规格配置       |
|---------|----------------|-----------------------------------------------|------------|
| 数据库软件服务 | x86 集中式数据库软件   | 标准版，提供激活、安装服务                                 | MySQL      |
|         |                | SQL Server 标准版，提供激活、安装服务；                     | SQL Server |
|         |                | 标准版，提供激活、安装服务；                                | Redis      |
|         | 国产集中式/分布式数据库软件 | 符合《安全可靠测评结果公告》《数据库政府采购需求标准（2023 年版）》要求的数据库软件。 | 数据库软件      |

7.3 中间件服务

中间件服务应提供国产中间件软件服务，见表8所示；

表8 中间件服务目录

| 服务分类    | 服务项目    |
|---------|---------|
| 中间件软件服务 | 国产应用中间件 |

8 云安全保障服务

安全保障服务要求如下：

- a) 云平台安全建设必须符合《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》三级标准、《GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南》和《GW0013—2017 政务云安全要求》；
- b) 云平台部署出口防火墙、DDOS 防护、主机安全、web 应用防火墙、安全审计、运维安全管理、集中日志审计等产品为云平台建设安全通信网络、安全区域边界、安全计算环境、安全管理中心。具体见表9所示；

表9 云安全保障服务目录

| 服务分类    | 服务项目   | 服务描述                                                                                                                                                | 规格配置   |
|---------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| 云安全保障服务 | 业务安全防护 | 安全基线类服务。为云主机提供边界防护、访问控制、入侵防御、网络防病毒功能；支持独立的入侵防护规则特征库，支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源 MAC、地址范围、应用、用户，实现对特定报文进行快速过滤。 | 虚拟边界防护 |

|  |                                                                                                                                                                                                                                                                          |        |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|  | 安全基线类服务。针对 1 台云主机的安全防护，具备资产管理、风险发现、威胁监测、安全基线、病毒查杀、微隔离等功能。                                                                                                                                                                                                                | 云主机安全  |
|  | 安全基线类服务。为云使用方提供 vpn 安全接入、堡垒机运维安全管理及审计服务                                                                                                                                                                                                                                  | 云堡垒机   |
|  | 安全基线类服务。管理资产数 1，提供对操作系统、中间件、数据库、网络设备、安全设备等资产的日志收集、关联分析、日志存储和综合展示                                                                                                                                                                                                         | 日志审计   |
|  | 安全基线类服务。针对 1 个 IP 或 1 个网站的漏洞扫描，1 年内不限次数扫描，支持扫描主流操作系统、web 服务器、数据库、网络主机、移动设备、应用及软件的安全漏洞；支持扫描系统漏洞数量大于 56000 种，web 漏洞数量大于 1000 种。                                                                                                                                            | 漏洞扫描   |
|  | 针对 1 个数据库实例的审计。支持主流数据库 SQL 语句操作审计，高危操作识别和告警。对无法镜像流量的审计场景，支持多种类型操作系统的探针部署，支持插件方式和非插件方式的业务关联审计，实现 100%精准审计与灵活部署配置；支持会话回放功能，并至少支持 0.5 倍速、1 倍速、1.5 倍速、2 倍速、4 倍速五级播放速度调节；支持抓包工具（可配置抓包个数、源和目的 IP、协议等）、系统巡检、网络诊断、规则库升级；支持不少于 20000 条 SQL 错误码，错误码至少体现 SQL 错误码、出错信息、出错原因、解决办法等内容。 | 数据库审计  |
|  | 针对 1 个保护站点的防护。支持 sql 注入、跨站脚本、跨站请求伪造、畸形 http 报文等主流 web 攻击防护。支持上传文件的病毒检测功能，支持虚拟补丁功能，支持爬虫协议保护，支持多服务器的负载均衡，对 ddos 流量支持检测清洗和强制防御两种模式，支持 WEB 缓存，URL 重写，HTTP 压缩等应用交付功能，支持网关型网页防篡改功能。                                                                                            | 云 WAF  |
|  | 两个独立的网络通过网闸进行隔离，使系统间不存在通信的物理连接、逻辑连接及信息传输协议，不存在依据协议                                                                                                                                                                                                                       | 安全交换通道 |

|        |                                                                                                                                                                                                                                                                                                                                                               |            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
|        | 进行的信息交换，而只有以数据文件形式进行的无协议摆渡。                                                                                                                                                                                                                                                                                                                                   |            |
|        | 采用系统底层文件过滤驱动技术，拦截与分析文件增、删、改操作，实现对网页文件的完整性检查和保护；支持 windows/Linux 系统，1 套支持 1 个 OS 的网页防篡改能力                                                                                                                                                                                                                                                                      | 网页防篡改      |
|        | 通过对租户业务系统网络内部 API 资产的分析和分类，实现对 API 高危、中危、低危的涉敏等级的感知和标记。同时，根据 API 画像、漏洞类型、异常事件、数据标签、API 访问基线等多个维度，全面梳理 API 资产，避免遗漏导致的安全漏洞。通过异常流量分析，实时监测和分析 API 使用过程中的攻击流量。具备脆弱性分析和主动探测技术，对 API 进行全面的安全测试。通过异常流量分析和验证 API 访问结果，实现对未发现的漏洞和安全隐患的检测，提前发现并解决安全问题。具备数据安全分析功能，对 API 的请求和响应数据进行深入分析和检测。通过敏感数据标签和自定义敏感数据识别规则，实时感知敏感数据的泄露和不当使用。同时，采取授权管理、数据脱敏等措施，确保 API 使用过程中数据的安全性和隐私性。 | API 安全监测服务 |
| 密码安全服务 | 提供用户身份鉴别服务，支持基于数字证书、对称加密、哈希算法等多种鉴别方式，校验速率 $\leq 50\text{TPS}$ ，并发能力 $\geq 100$ 连接。                                                                                                                                                                                                                                                                            | 应用登录鉴别服务   |
|        | 提供支持 SM3、哈希运算消息认证码（HMAC）运算的数据完整性保护和验证服务。并发连接数 $\geq 100$ ，计算速度 $\geq 80\text{Mbps}$ （建议 120Mbps）。                                                                                                                                                                                                                                                             | 完整性保护服务    |
|        | 提供数据加解密服务，支持文件、卷、数据库存储透明加密和数据字段接口加解密等场景。文件读写操作性能损耗 $\leq 20\%$ ，文件加密速率 $\geq 200\text{Mbps}$ ，数据库加解密速率 $\geq 60\text{Mbps}$ ，卷加解密速率 $\geq 200\text{Mbps}$ 。                                                                                                                                                                                                   | 数据存储加解密    |
|        | 校验速率 $\geq 100\text{TPS}$ ，P1 签名验签速度 $\geq 150$ 次/秒，P7 签名验签速度 $\geq 130$ 次/秒。使用场景：为用户应用提供 1 套证书签名和验证服务能力，支持密钥加密保护和信封服务功能，支持数据签名验签、文件签名验签，保证用户身份                                                                                                                                                                                                               | 签名验签服务     |

|  |  |                                                                                                                                                                            |           |
|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|  |  | 的真实性，重要业务数据的完整性以及关键操作的不可否认性等。                                                                                                                                              |           |
|  |  | 提供数据传输加解密通道服务，支持 SSL/TLS、IPSec 等协议，支持国密算法。吞吐率 $\geq 100\text{Mbps}$ ，SSL 并发连接数 $\geq 1900$ ，IPSec 并发隧道数 $\geq 100$ 。                                                       | 数据传输加解密   |
|  |  | 云密钥管理服务，具备对称密钥、非对称密钥管理，支持密钥的生成、存储、归档、恢复、销毁等生命周期管理操作，通过管理控制台集中管理密钥整个生命周期。密钥数量 $\geq 10000$ 。                                                                                | 密钥管理服务    |
|  |  | SM4 对称加解密能力 $\geq 250\text{Mbps}$ ，SM3 完整性校验能力 $\geq 120\text{Mbps}$ ，SM4 完整性校验能力 $\geq 250\text{Mbps}$                                                                    | 虚拟服务器密码机  |
|  |  | 提供可靠的时间服务，具体包括业务系统对接、密码系统对接、密码模块对接。并发连接数：300，守时精度： $< 0.5\text{ms}$ （72 小时），产生时间戳速度 300 次/秒，时间戳签发：200 次/秒，时间戳验证：120 次/秒；                                                   | 时间戳服务     |
|  |  | 1 个数据库实例。提供数据库机密性和完整性保障。存量（300W）数据加/解密：1.5 万条/秒，加密表插入速率：6000 条/秒，加密表查询速率：4000 条/秒。                                                                                         | 数据库加密服务   |
|  |  | 只对云服务端提供服务。提供支持国产商用密码算法的安全浏览器，包括 SM2/SM3/SM4 国密算法以及国密的 SSL 协议。                                                                                                             | 国密浏览器     |
|  |  | 只对云服务端提供服务。提供终端密码模块运算、密钥安全管理能力。SM4 加/解密速率 $\geq 1\text{Mbps}$ ，SM2 加/解密速率 $\geq 0.6\text{Mbps}$ ，SM2 签名速率 $\geq 50.96$ 次/秒，SM2 验签速率为 70 次/秒，SM3 运算速率 $\geq 1\text{Mbps}$ 。 | USBKey    |
|  |  | 针对系统提供基于密钥分割的协同数字签名和加解密功能；包括 CA 对接、系统对接等工作，针对移动端提供终端密码模块能力，提供客户端设备和用户认证、协同密钥生成、存储、加密和签名运算以及数字证书存储功能。服务并发速率 $\geq 1000$ ，身份认证 $\geq 1000$ 次/秒，数字签名 $\geq 2000$ 次/秒。         | 手机盾签名验签   |
|  |  | SM2、SM3 签名验签能力 $\geq 280\text{Mbps}$                                                                                                                                       | 虚拟签名验签服务器 |

## 参 考 文 献

- [1] DB37/T 3521.1 政务信息资源目录 第1部分：编码规则
  - [2] DB37/T 4394.1—2021 政务云平台 第1部分：基本服务目录
  - [3] DB37/T 4394.2—2023 政务云平台 第2部分：服务资源编码规范
  - [4] DB37/T 4785—2024 政务云平台监管指标体系
-