CSA 云安全联盟标准

CSA GCR XXXX—XXXX

云应用安全技术标准

英文名称

Cloud Application Security Technology Standard

（征求意见稿）

2022－XX－XX 发布　　2022－XX－XX 实施

云安全联盟大中华区　　发 布

目　　次

前　言

本标准按照 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。

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这些专利的责任。

本标准由云安全联盟大中华区归口。

本标准主要起草单位：北森云计算有限公司、公安部第三研究所、北京华为数字技术有限公司、中国信息通信研究院、北京江南天安科技有限公司、北京金山云网络技术有限公司、北京奇虎科技有限公司、北京神州数码云计算有限公司、北京数字认证股份有限公司、北京天融信网络安全技术有限公司、广州赛宝认证中心服务有限公司、杭州安恒信息技术股份有限公司、杭州迪普科技股份有限公司、杭州默安科技有限公司、江苏保旺达软件技术有限公司、启明星辰信息技术集团股份有限公司、融联易云金融信息服务（北京）有限公司、上海安几科技有限公司、上海派拉软件股份有限公司、深信服科技股份有限公司、深圳国家金融科技测评中心有限公司、深圳市联软科技股份有限公司、顺丰科技有限公司、腾讯云计算（北京）有限责任公司、网宿科技股份有限公司、浙江大华技术股份有限公司、浙江瀛云科技有限公司。

本标准主要起草人：郭鹏程、陈妍、李强、罗斌、柴瑶琳、王冬冬、于丽芳、王玉常、陈强、李向锋、王龑、刘克松、毛润华、仇俊杰、孟瑾、杜有为、杨天识、于跃、容晓琳、茆正华、雷若琦、吴祖顺、侯俊、马超、王永霞、朱梦婷、尚玉红、王方军。

1 范围

本标准确立云应用产品应该具备的安全相关的技术或能力要求。云应用包括但不限于SaaS云应用、PaaS和IaaS云的应用程序部分。云应用提供服务的形式可以是web应用、移动APP、API接口等。

本标准为云应用厂商或甲方构建安全的云应用产品提供参考和指导，为云客户选择安全的云应用产品提供参考和指南。

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标准必不可少的条款。其中，标注日期的引用文件，仅该日期所对应的版本适用于本标准；不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

[1] GB/T 25069-2010 信息安全技术 术语

[2] GB/T 35273-2020 信息安全技术 个人信息安全规范

[3] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[4] CSA云计算安全技术要求 SaaS安全技术要求

[5] ISO/IEC 27001 信息安全管理

3 术语和定义

云应用：云应用是以云的形式提供服务的应用，包括但不限于SaaS云应用、PaaS和IaaS云的应用程序部分。云应用提供服务的形式可以是web应用、移动APP、API接口等。

云应用厂商：是指为客户提供云应用及相关服务的厂商，又称云应用提供商。

云应用租户：是指云应用的购买方或使用方，可以是企业也可以是个人。

互操作性：互操作性（Interoperability ）又称互用性，是指不同的计算机系统或应用程序一起工作并共享信息的能力。比较常见的实现互操作性的方式是不同系统通过API接口进行集成和对接，以实现功能或数据的集成。

可移植性：可移植性（Portability）是指应用程序或数据在不同的平台、环境或服务商之间进行迁移的能力。

不可变基础设施：是一种基础设施变更管理的方式，主要是指不直接对运行中的云主机或容器等基础设施实例执行任何变更，而是统一基于标准镜像模板进行变更，再用变更以后的最新镜像创建新实例，然后用新实例替换运行中的实例。利用不可变基础设施可以减少攻击面，同时最大限度的保障环境配置的一致性。

4 缩略语

下列缩略语适用于本文件。

APP	Application	应用程序
API	Application Programming Interface	应用程序接口
SQL	Structured Query Language	结构化查询语音
CI/CD	Continuous Integration/ Continuous Delivery	持续集成/持续部署
SaaS	Software-as-a-Service	软件即服务
PaaS	Platform-as-a-Service	平台即服务
IaaS	Infrastructure-as-a-Service	基础设施即服务
SDK	Software Development Kit	软件开发工具包
RBAC	Role Based Access Control	基于角色的访问控制
ABAC	Attribute Based Access Control	基于属性的访问控制
IAM	Identity and Access Management	身份与访问管理
IDaaS	Identity-as-a-Service	身份验证即服务
SSO	SingleSignOn	单点登录
PII	Personally Identifiable Information	个人身份信息
SLA	Service Level Agreement	服务等级协议
GUID	Globally Unique Identifier	全局唯一标识符
APaaS.	Application Platform-as-a-Service.	应用级平台即服务
ISV	Independent Software Vendors	独立软件开发商
TEE	Trusted Execution Environment	可信执行环境
SE	Secure Element	安全元件
RASP	Runtime Application Self-protect	应用运行时自我保护

5 云应用安全技术或能力要求

本标准对云应用应该具备的安全技术或能力要求进行了说明，主要包括云应用架构设计要求、云应用运行环境安全要求、云应用程序安全要求、访问控制安全要求、租户级安全自助能力要求、云实施/交付/服务安全要求、云数据安全要求、云安全管理能力要求共8个控制域。各控制域对应的控制项见5.1-5.8。

5.1 云应用架构设计要求

云资源的弹性无法保障云应用整体的弹性能力，因此在云应用的设计阶段要充分考虑架构问题，通过架构设计来保证云应用层面的弹性，从而提升云应用的稳定性。此外还应在架构设计阶段充分考虑云应用的性能和安全问题。本标准涉及的云应用架构设计要求主要包括高可用、高性能、高安全三个方面。

5.1.1 高可用架构设计

云应用的架构设计应能够保障应用持续稳定运行，提升云应用的整体可用性，确保云应用满足 SLA 的要求。相关要求如下：

【基础要求】

a） 应支持从基础设施到应用程序各层级的负载均衡；

b） 应支持水平扩展集群或分布式集群部署；

c） 应支持异地灾备；

d） 应支持租户级策略路由；
e） 应支持微服务架构，实现不同业务功能解耦；
f） 应具备故障检测和处理能力。

【增强要求】

a） 数据存储应支持多副本架构；
b） 应支持双活或多活架构；
c） 应具备故障隔离、熔断或降级机制；
d） 应具备容错或故障自愈能力。

5.1.2 高性能架构设计

云应用架构设计应能够保障应用高效运行，能够承载高并发或业务峰值。相关要求如下：

【基础要求】

a） 应使用分库分表、读写分离或数据分片机制；
b） 应使用缓存技术并具备防缓存穿透或雪崩的能力；
c） 应使用索引技术；
d） 应使用消息队列技术；
e） 应具备全业务流程性能监测与预警能力；
f） 应支持冷热数据分离；
g） 应具备弹性能力。

【增强要求】

a） 应具备应用全链路的弹性能力。

5.1.3 高安全架构设计

云应用架构设计阶段应该充分考虑整体安全性，遵循必要的安全架构设计原则，本标准关注的安全设计要求如下：

【基础要求】

a） 租户间资源/数据应具备充分的隔离机制；
b） 应遵循默认安全原则，如默认白名单；
c） 应遵循纵深防御/立体防御原则；

【增强要求】

a） 应具备云原生安全能力。

5.2 应用运行环境安全要求

运行环境是云应用依赖的操作系统、中间件、数据库等，是云应用正常运行的基础。相关要求如下：

5.2.1 操作系统安全要求

【基础要求】

a） 应具备安全加固的能力；
b） 应具备主机安全监测和防御的能力；
c） 应具备访问控制的能力；
d） 应具备漏洞管理和补丁管理的能力；
e） 应具备系统变更管理和监测的能力；

f） 应保证操作系统镜像和快照的安全性与完整性；

【增强要求】

a） 支持不可变基础设施。

5.2.2 容器安全要求

【基础要求】

a） 应具备对容器相关的配置、运行状态及资源使用进行管理和监测的能力；
b） 应具备对容器的访问控制能力；
c） 应具备容器镜像的机密性和完整性保护的能力；
d） 应保证进程只能执行在允许列表中明确定义的函数；
e） 应具备对容器进程隔离的能力。

5.2.3 容器编排管理平台安全要求

【基础要求】

a） 应保证以非 root 身份构建容器；
b） 应能够用可变的文件系统运行容器；
c） 应能够支持对容器编排管理平台的访问控制；
d） 应将凭证和敏感信息放在安全函数文件系统中并加密；
e） 应具备漏洞管理和补丁管理的能力；
f） 应禁用匿名登录并具备登录审计的能力。

5.2.4 数据库安全

【基础要求】

a） 应能够支持对数据的加密保护；
b） 应具备控制管理员访问数据库及用户数据的能力；
c） 应具备访问控制的能力；
d） 应具备漏洞管理和补丁管理的能力；
e） 应具备审计的能力；

5.2.5 中间件安全

【基础要求】

a） 应具备安全加固的能力；
b） 应具备访问控制的能力；
c） 应具备漏洞管理和补丁管理的能力。

5.2.6 熔断与环境隔离

【基础要求】

a） 应支持租户间资源/数据的隔离；
b） 应支持对资源异常访问请求的熔断处理；
c） 应支持资源隔离失效时的访问熔断处理。

5.3 云应用程序安全要求

云应用程序包含多种形式，如web、移动APP、API接口、小程序等，相关的要求如下：

5.3.1 Web 安全要求

Web是云应用呈现给最终用户最常见的业务形态，本标准对web安全的相关要求如下：

【基础要求】

a） 应具备 Web 攻击检测和防御能力，如对 Owasp top 10 漏洞的检测与防御；
b） 应具备输入信息过滤和校验能力；
c） 使用参数化查询，禁止动态拼接 SQL；
d） 应具备对攻击 IP 或恶意请求阻断的能力；
e） 应具备数据包防重放能力；
f） 应使用 GUID 代替自增数字 ID；
g） 应具备参数防篡改的能力，如对参数进行签名和验签；
h） 应避免敏感信息回显，如避免将服务器版本信息或其它敏感信息回显到浏览器；
i） 应具备控制上传文件类型的能力；
j） 应防止租户间越权；
k） 应防止租户内平行越权或垂直越权；
l） 应采用白名单策略，如针对 url 跳转、跨域、iframe 嵌套等场景需要设置域名白名单；
m） 敏感信息应从配置文件或数据库读取，禁止硬编码；
n） 应具备代码审计的能力。

【增强要求】

a） 应该具备框架层面的全局安全防御能力；
b） 应具备通过语义分析、机器学习等技术执行安全检测的能力；
c） 应具备数据防泄漏检测的能力；
d） 应具备防止业务逻辑漏洞的能力；
e） 应具备对攻击请求自动阻断的能力；
f） 应具备基于 CI/CD 管线的自动化代码审计能力；
g） 应采用 RASP 运行时自我保护防御能力。

5.3.2 移动 APP 安全

移动APP安全除了技术层面的安全要求以外，还包括安全合规监管要求，本标准涉及的移动APP安全要求主要侧重于技术安全，移动APP的监管合规建议参考《个人信息保护法》、《数据安全法》和GB/T35273等相关法律法规和标准的要求：

【基础要求】

a） 应具备防反编译或破解的能力，如代码混淆、设置 debugable=false,allowbackup=false 等；
b） 发布前必须执行安全加固；
c） 应支持 APP 安装包的完整性较验；
d） 应该支持多种身份认证机制，如账号密码、生物识别、短信验证等；
e） 应加密用户提交的凭证信息；
f） 应仅支持安装在内部存储，不应将文件设置为全局可读或可写权限；
g） APP 客户端不应存储个人敏感信息；
h） 应限制导出关键组件，如 Service、Provider、Receiver 等；
i） 应具备检查设备是否被 root 或被越狱的能力；

j） 移动 APP 的功能设计应该符合应用商店审核要求。

【增强要求】

a） 应支持 APP 界面上个人信息默认脱敏显示；

b） APP 界面应支持水印；

c） 应支持登录设备管理和会话强制退出；

d） 移动 APP 的功能设计应符合监管合规要求；

e） 对移动 APP 采用基于可信执行环境+安全元件（TEE+SE）的安全保护方案。

5.3.3 API 接口安全要求

【基础要求】

a) 应具备API资产发现及管理的能力；

b) 应提供标准的API接口文档；

a) 非公开接口调用前应进行充分的身份认证；

b) 接口调用的身份凭证应支持租户自助获取；

c) 应遵循最小权限原则；

a) 对外开放的API应使用安全的通信协议；

b) 应具备参数防篡改的能力；

c) 应具备输入数据校验和过滤能力；

d) 应避免API调用时的回显信息里包含敏感数据；

a) 应具备API漏洞检测及修复能力；

b) 应具备API攻击检测与防御能力；

c) 应具备对非法调用的阻断能力；

d) 应具备接口防重放能力。

【增强要求】

a) 应支持使用接口网关对接口进行注册、鉴权、限频管理；

b) 应具备细粒度的授权机制，如使用Oauth3.0协议；

c) 应支持租户级接口调用的IP白名单。

5.3.4 小程序安全

【基础要求】

a) 应具备通过AppID监控代码泄露或敏感信息泄露的能力；

b) 应具备防止代码被逆向分析的能力，如对代码进行混淆处理；

c) 应具备防篡改防二次打包的能力；

d) 应具备检测程序调试状态的能力；

e) 应加密存储的数据，防止敏感信息泄露。

5.3.5 后台应用程序安全

后台应用程序主要是指与云应用紧密相关但是不直接与云租户或最终用户交互的应用程序。后台应用程序租户或者最终用户感知不到，但在云应用运行过程中不可或缺。相关的安全要求如下：

【基础要求】

a) 应具备租户身份鉴别的能力；

b) 应具备按租户路由的能力；

c） 应具备业务流程上下文监测和路径追踪的能力；
d） 应具备高可用和弹性能力；
e） 应具备对后台应用程序本身的安全保障能力。

5.3.6 第三方 SDK/类库安全

【基础要求】
a） 应具备集中管控第三方SDK和类库的能力，如SDK识别、安全评估等；
b） 应确保使用的第三方SDK和类库是从官方渠道获取，并且未被篡改；
c） 应确保使用的第三方SDK的许可证真实有效，许可证类型符合设计规范要求。

5.3.7 云应用代码防泄露

【基础要求】
a） 应具备源代码泄露监测和及时预警的能力；
b） 应具备从源代码中发现敏感信息硬编码的能力。

5.4 访问控制安全要求

本标准涉及的访问控制包括通信安全、安全区域、身份与访问管理IAM、会话安全及终端安全识别等方面。相关要求如下：

5.4.1 通信安全

【基础要求】
a） 在允许远程连接云应用前，应进行身份验证和授权；
b） 应具备阻止非授权远程连接的能力；
c） 应保证通信过程中数据的完整性和机密性，如使用TLS加密；
d） 应该具备防御DoS或DDoS等针对连接或流量攻击的能力；
e） 应该具备保障通信链路稳定高效的能力；
f） 云应用服务端应该具备带宽弹性扩容的能力。

5.4.2 安全访问区域

【基础要求】
a） 如果不同租户使用独立的资源，则应实现租户间的资源/网络访问区域隔离；
b） 应实现不同租户之间的数据隔离；
c） 应在不同等级的网络区域边界执行访问控制策略；
d） 应支持租户级的防火墙，如租户级的IP白名单；
e） 云应用厂商应具备限制其管理员访问租户资源/数据的能力；

5.4.3 会话安全

【基础要求】
a） 应具备控制账号并发会话数的能力；
b） 应具备控制会话凭证有效期的能力；
c） 应具备会话锁定/解锁的能力；
d） 应具备异常登录提醒能力。

5.4.4 身份与访问管理 IAM

【基础要求】

a) 应采用RBAC授权机制并满足最小权限原则；
b) 应支持多种身份认证方式；
c) 应具备对账号申请人进行实名/实人认证的能力；
d) 应具备租户级账号和口令策略定制的能力；
e) 应具备租户级账号分级授权管理的能力；
f) 应具备租户级的权限清单；
g) 应支持登录日志审计；

【增强要求】

a) 应采用ABAC或动态授权机制；
b) 应支持与主流IAM厂商或IDaaS厂商的集成；
c) 租户管理员也应该和普通用户一样遵循最小权限原则，如默认只有租户配置权限，没有数据权限。

5.4.5 识别访问终端安全

【基础要求】

a) 应该具备辨识访问终端身份的能力，如判断是人工访问还是机器访问；
b) 应具备辨识终端异常访问行为和阻断的能力，如识别并屏蔽扫描器或爬虫。

5.5 租户级安全自助能力要求

租户级安全是指云应用厂商提供的可由租户管理员自行操作的安全配置能力，通常作为云应用的安全功能存在，每个租户可以设置不同的安全策略。

5.5.1 租户级 IAM 自助服务

【基础要求】

a) 应支持租户管理员自助创建账号和授权；
b) 应支持租户管理员自助定制口令策略，如口令复杂度、有效期等；
c) 应支持租户管理员自助选择认证方式以及是否开启二次认证或双因素认证；
d) 应具备租户管理员自助设置防攻击策略的能力，如防暴力破解、撞库等；
e) 应支持租户管理员自助设置会话有效期的能力；
f) 如果云应用对租户开放API接口，则应支持租户自助管理接口调用凭证，如自助获取或轮换凭证；
g) 应提供完整的接口文档，支持租户级SSO自助集成。

5.5.2 租户级自助审计

【基础要求】

a) 应支持租户管理员自助审计用户的登录日志和操作日志；
b) 租户级的审计日志应支持通过接口调用或由租户自助导出。

5.6 云应用实施/交付/服务安全要求

云应用交付分两种方式，一种是私有化部署交付，另一种是SaaS公有云交付。SaaS公有云模式由云应用厂商履行应用程序及以下各层（甚至包含数据层）的安全和运维职责，而私有化部署模式的安全和运维职责需要双方协商约定。本标准只介绍云应用本身的实施/交付安全要求，不涉及基础设施安全。

5.6.1 云应用实施/交付/服务安全控制要求

云应用实施/交付/服务安全主要是指云应用程序在交付过程中涉及到的实施配置和初始化过程中的安全。相关要求如下：

【基础要求】

a) 云应用实施配置相关的权限应由租户管理员控制，如给实施人员授权和撤销权限；
b) 应具备对实施/交付/服务相关操作的审计能力；
c) 对实施过程中要用到的初始化数据，应具备租户自助导入的能力；
d) 实施工具的操作界面应该具备水印功能；
e) 应具备租户级的灰度交付能力；
f) 应具备用于云应用实施/交付的沙箱环境；
g) 应具备差异化/定制化交付的能力；
h) 应针对云应用制定并执行SLA协议。

5.6.2 互操作与可移植性要求

互操作性是指云应用的接口开放能力以及与其它应用进行集成的能力。可移植性主要是指云应用租约到期后迁移应用或数据的能力。相关要求如下：

【基础要求】

a) 应具备与常见的IAM或IDaaS产品集成的能力；
b) 应提供完善的接口文档以实现不同云应用间的集成和对接；
c) 集成对接过程应具备安全的身份认证和授权机制；
d) 接口调用过程传输的数据应遵循最小权限原则；
e) 接口调用日志应可审计；
f) 接口升级需要考虑安全和兼容；
g) 应具备迁移或导出云应用数据的能力；
h) 应保证系统集成或数据迁移过程中数据的机密性和完整性。

5.6.3 安全即服务要求

【基础要求】

a) 云应用自身应具备原生的安全配置功能模块；
b) 云应用所使用的安全服务应具备与云应用同等的弹性能力和安全保障；
c) 安全即服务本身不得引入新的安全风险。

5.6.4 云应用功能扩展与定制化交付能力

云应用应该具备灵活的功能扩展与定制化能力，相关要求如下：

【基础要求】

a) 应具备应用功能定制和扩展的能力；

【增强要求】

a) 应具备零代码能力，即通过字段或表单的拖拽即可实现功能的定制；
b) 应具备通过低代码low code扩展开发的能力；
c) 应具备APaaS平台并对租户开放ISV。

5.7 数据安全要求

数据安全是云应用安全最终保护的目标，数据安全涉及的面很广，本标准主要是基于云应用场景下的数据安全提出如下要求：

5.7.1 租户间数据隔离

【基础要求】

a) 租户间的数据应充分隔离，确保每个租户只能操作属于自己的数据；
b) 云应用的所有操作均应先进行租户信息鉴别和校验；
c) 私有化部署的云应用必须采用独立的数据库实例或对数据进行物理隔离。

5.7.2 数据机密性

【基础要求】

a) 应保障敏感数据传输的机密性，如采用通道加密或内容加密；
b) 应保障敏感数据存储的机密性，如加密存储；
c) 应保障加密机制本身的安全性，如使用安全的加密算法；
d) 应保障密钥生命周期的安全性；
e) 应遵循最小权限原则，避免租户间及租户内的数据越权。

【增强要求】

a) 敏感数据采用数据分片或分布式存储；
b) 敏感数据应采用密文检索技术；
c) 应保证敏感数据在分享给第三方的处理过程中始终以密文形式出现。

5.7.3 数据可用性

【基础要求】

a) 应执行完善的数据备份策略和恢复测试策略；
b) 应执行完善的容灾机制；
c) 分布式存储应设置多个副本。

【基础要求】

a) 应支持租户自助备份数据。

5.7.4 数据完整性

【基础要求】

a) 应具备数据完整性校验的能力；
b) 应具备数据防篡改的能力；
c) 分布式存储应具备保障各节点数据一致性的能力；

【增强要求】

a) 访问存储PII数据库时，应做完整性校验，如开启数据库TLS，进行多表交叉校验等；
b) 针对高敏感数据，采用数据分片和分布式存储技术，并确保各数据分片的完整性。

5.7.5 隐私保护

隐私保护建议参考《个人信息保护法》及GB/T 35273的要求，本标准只针对云应用的隐私保护功能提如下要求：

【基础要求】

a） 应在注册、登录等关键位置及云应用内部便捷的呈现隐私政策文件；
b） 应具备“同意”和“单独同意”相关的功能；
c） 应具备账号注销功能；
d） 应具备撤销同意的路径或功能；
e） 应具备删除个人信息的路径或功能。

5.7.6 数据位置与跨境

【基础要求】
a） 数据存储位置应遵守当地法律法规，如向境内用户提供服务的数据应存储于中国境内；
b） 数据跨境传输应遵循发出方、接收方甚至中转方当地的法律法规和监管要求。

5.8 安全管理能力要求

云应用厂商通常会承担绝大部分安全管理的职责，云应用需要为云租户提供安全管理相关的功能，云租户需要合理使用或设置云应用厂商提供的安全功能，进行租户级的应用安全加固。具体要求如下

5.8.1 云应用厂商安全管理能力要求

安全管理相关要求参见ISO27001标准的要求。本标准仅将安全管理相关要求概述如下：
【基础要求】
a） 应具备针对云应用相关资源执行访问控制的能力；
b） 应具备配置管理的能力；
c） 应具备变更管理的能力；
d） 应具备漏洞管理和补丁管理的能力；
e） 应具备安全事件管理和应急响应相关的能力和预案；
f） 应具备业务连续性方案或灾备方案并进行演练；
g） 应具备安全监控、态势感知和防御的能力；
h） 应执行有效的安全审计策略；
i） 应具备物理与环境安全保障能力；
j） 应具备供应链安全保障能力；
k） 应具备资源容量管理能力；
l） 应具备云应用生命周期安全管控能力，如执行SDL等。

5.8.2 云应用租户安全管理能力要求

【基础要求】
a） 应合理使用云应用厂商提供的安全功能，合理配置租户级的云应用安全策略；
b） 应使用统一的身份与访问管理系统IAM与云应用集成；
c） 应对云应用的安全合规性执行评估或审查，如渗透测试或其它方式的评估。