CSA 云安全联盟标准

CSA GCR C0xx—20xx

零信任可信接口规范

Zero Trust Trusted Interface Specification

（征求意见稿）

20xx－xx－xx 发布

云安全联盟大中华区　　发 布

目 次

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。

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。

本文件由云安全联盟大中华区归口。

本文件起草单位：

本文件主要起草人：

1 范围

本标准规定了应用安全领域内，应用系统与零信任安全网关、零信任代理、零信任控制中心之间的通信协议要求、数据传输要求及数据接口规范。本标准适用于但不限于以下场景：

企业级应用系统与零信任系统的集成。

本标准旨在确保在应用系统与零信任系统之间的数据交换过程中，实现以下目标：

- 保障数据在传输过程中的安全性，防止数据泄露或被未授权访问。
- 确保数据传输的完整性，防止数据在传输过程中被篡改。
- 验证数据交换双方的身份，实施动态的访问控制和授权。
- 支持 IPv6 协议，满足新一代网络协议的安全需求。
- 适应 HTTPS 和国密算法等加密技术，增强数据传输的安全性。

本标准适用于应用系统的开发者、零信任解决方案提供商以及网络安全评估和监管机构。

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，标注日期的引用文件，仅该日期所对应的版本适用于本文件；不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2022　信息安全技术　术语

GB/T 29242—2012　信息安全技术　鉴别与授权安全断言标记语言

T/CESA 1165—2021　零信任系统技术规范

3 术语和定义

为了本标准的目的，以下术语和定义适用：

- **主体 (Subject)**：发起访问请求的实体。
- **资源 (Resource)**：可供主体访问的对象。

- **零信任技术 (Zero Trust Technology)**：一种基于持续动态安全访问控制的技术，旨在降低访问过程中的安全风险，通过身份认证和授权，确保只有经过验证和授权的主体才能访问资源。
- **零信任架构(Zero Trust Architecture)**：基于零信任建立的信息系统体系架构，包括构成架构的系统组件，以及组件间关系。
- **安全网关 (Security Gateway)**：在零信任系统中，用于管理和控制网络访问的组件，执行安全策略，如身份验证、加密通信等。
- **零信任代理 (Agent)**：在零信任系统中，用于客户端设备上的软件，负责与安全网关进行通信，实现身份认证和数据加密。
- **控制中心 (Control Center)**：在零信任系统中，负责制定和分发安全策略，以及收集和分析安全数据的中心组件。
- **国密算法 (Guomi Algorithm)**：中国国家标准规定的加密算法，用于确保数据传输的安全性。
- **幂等性 (Idempotence)**：在接口设计中，同一请求无论执行多少次，其结果都相同的特性。该特性用于保证系统的可靠性和数据一致性。

4 缩略语

下列缩略语适用于本文件：

- **API**：应用程序编程接口（Application Programming Interface）
- **TLS/SSL**：传输层安全性协议/安全套接层协议（Transport Layer Security/Secure Sockets Layer）
- **JSON**：JavaScript 对象表示法（JavaScript Object Notation）
- **OIDC**：开放 ID 连接（OpenID Connect）
- **HTTPS**：超文本传输安全协议（Hypertext Transfer Protocol Secure）
- **IP**：互联网协议（Internet Protocol）
- **CPU**：中央处理器（Central Processing Unit）
- **RAM**：随机存取存储器（Random Access Memory）
- **ID**：标识（Identification）
- **TLS**：传输层安全协议（Transport Layer Security）
- **AI**：人工智能（Artificial Intelligence）
- **IoT**：物联网（Internet of Things）
- **GUI**：图形用户界面（Graphical User Interface）

5 概述

5.1 理念

零信任是一种网络安全防护理念，核心思想是“永不信任，始终验证”，无论主体位于网络的哪个位置，都需要经过身份认证和授权。本标准采用零信任理念，以确保应用系统的安全性和对数据的保护。

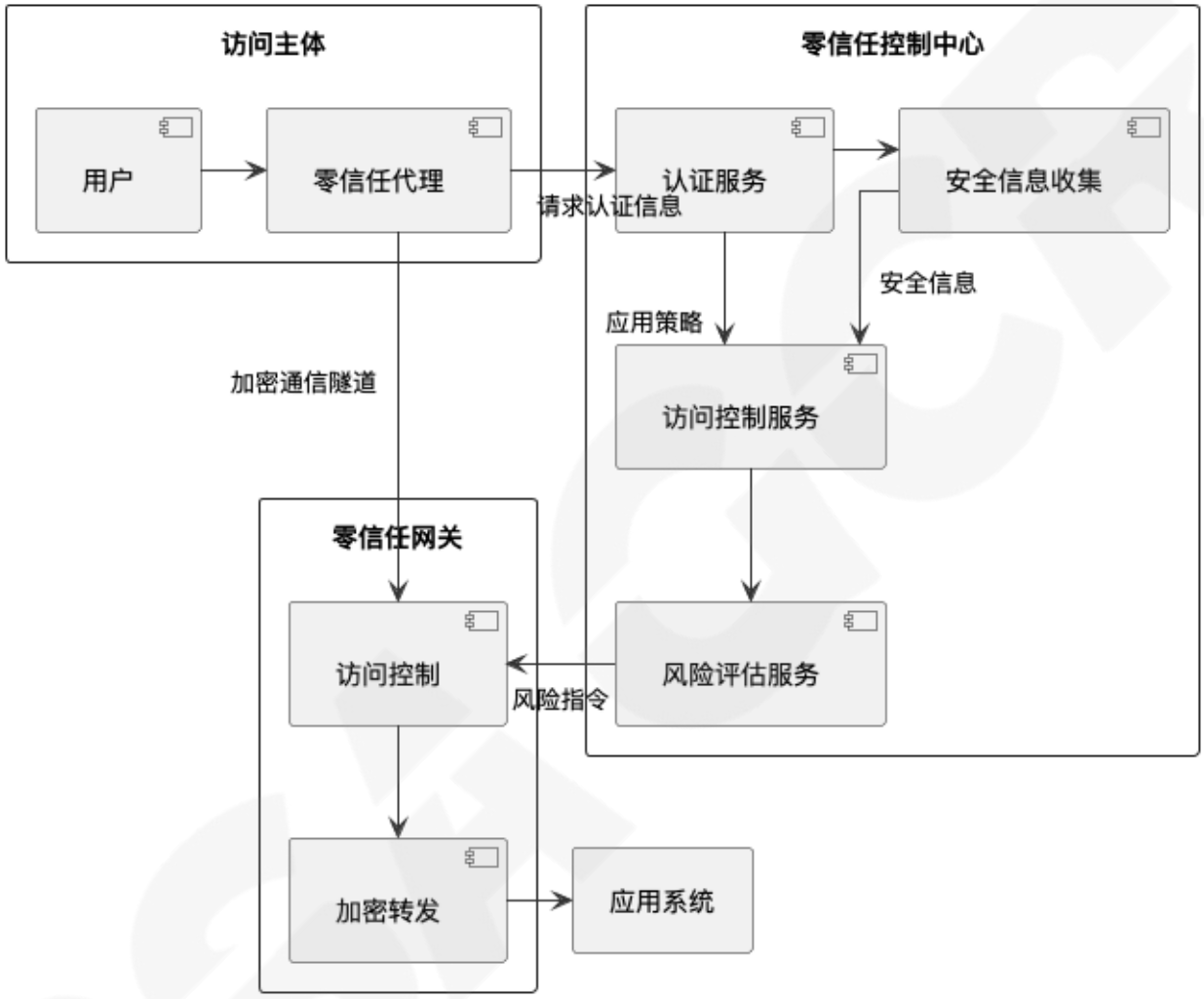
5.2 基本假设

- 网络位置不是信任的决定因素。
- 所有主体，包括用户和设备，都需要经过验证。
- 身份认证是多维度和持续性的。
- 授权是基于动态和细粒度的信任评估。

5.3 基本原则

- 最小权限原则：主体仅获得完成所需任务的最小权限集。
- 动态授权：基于实时的安全评估和信任级别执行访问授权。
- 持续监测：对所有访问活动持续执行的安全监测和评估。

5.4 基本架构



本架构图展示了应用系统与零信任安全网关、零信任代理和零信任控制中心之间的交互关系，以及数据流向。

6 应用系统与零信任安全网关的数据接口要求

6.1 通信协议要求

- 网络传输应采用 TLS 1.2 或更高版本的安全协议确保数据传输安全。

- 报文内容应采用可扩展标记语言（XML）或 JSON 格式，具体格式应根据应用场景的需求选择，以保证数据的可读性和易处理性。
- 报文结构应至少包含报文头、报文体和报文签名等字段。报文头应包含必要的元数据，如协议版本、消息类型、时间戳等；报文体加密应使用国密算法或等效国际标准加密算法；报文签名用于确保报文的完整性和身份认证。
- 身份验证和授权访问应采用 OIDC（OpenID Connect）或 SAML（Security Assertion Markup Language）。
- 接口请求应实现幂等性，确保重复请求不会导致数据不一致。

6.2 数据传输要求

应用系统与零信任安全网关之间的数据通信应满足以下基本要求：

- 数据传输的频率应不低于每 60 秒一次，以确保数据的实时性。
- 数据传输的延迟应控制在 3 秒以内，确保系统的实时性。
- 在通信中断的情况下，应暂存身份鉴别数据，并在通信恢复后及时补报。
- 支持对接口上的重要数据（如所有的密钥和私钥、身份验证和其他安全配置）和重要业务数据实施机密性保护。
- 应提供重要数据的本地备份与重传功能。
- 支持对终端上的重要数据（如所有的密钥和私钥、身份验证和其他安全配置）和重要业务数据实施完整性保护。

6.3 数据接口

6.3.1 应用系统身份鉴别接口

应用系统与安全网关间，需进行身份鉴别，其参数应符合表 1 的要求。

表 1 应用系统身份鉴别接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	应用系统标识	appId	字符型	字母、数字与符号的组合，11 位	必填项
2	应用系统名称	appName	字符型	汉字、字母、数字与符号的组合，40 位	必填项

3	系统状态	state	整型	数字，1 位	必填项 1：代表在线 0：代表离线
4	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
5	IP	ip	字符型	数字与点号的组合	必填项
6	端口	port	整型	数字，0~65535	必填项
7	认证方式	authMethod	字符型	字母、数字与符号的组合，10 位	可选项
8	会话令牌	sessionToken	字符型	字母、数字与符号的组合	可选项
9	一次性随机数	nonce	字符型	字母、数字与符号的组合	可选项

应用系统的身份鉴别响应参数应符合表 2 的要求。

表 2　鉴别响应参数

序号	字段名称	字段代码	数据类型	格式	说明
1	返回代码	code	整型	数字，3 位	必填项 200：代表成功 400：代表失败
2	返回信息	result	字符型	字母、数字与符号的组合	必填项 code 返回 400 时，返回失败原因说明
3	接入零信任网络授权 Key	authKey	字符串	字母、数字与符号的组合	返回代码 200 时，必填项 该授权 Key 可以让节点加入零信任网络。
4	认证过期时间	expiry	字符串	字母、数字与符号的组合	返回代码 200 时，必填项 节点认证过期时间，如果节点过期需要重新认证。
5	签名	signature	字符串	字母、数字与符号的组合	返回代码 200 时，必填项 对信息进行签名
6	签名类型	signatureType	字符串	字母、数字与符号的组合	返回代码 200 时，必填项 信息的签名类型

6.3.2 应用系统业务相关接口

零信任安全网关应通过 appId，向对应的应用系统发送业务请求，以获得响应业务信息的推送，请求使用 HTTPS 协议。

业务请求参数应符合表 3 的要求。

表 3 业务请求参数

序号	字段名称	字段代码	数据类型	格式	说明
1	应用系统标识	appId	字符型	字母、数字与符号的组合，11 位	必填项
2	密钥类型	keyType	字符型	字母、数字与符号的组合，10 位	必填项
3	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
4	数据内容	data	数组	JSON 数组	选填项
5	数据完整性哈希	dataHash	字符型	SHA-256 哈希值	选填项
6	备注	remark	字符型	汉字、字母、数字与符号的组合	选填项

表 3 中数据内容（data）格式，应根据应用系统的业务接口要求保持一致。

6.4 接口日志要求

- 应支持对主要接口操作的审计。
- 日志要至少包括主体、客体、操作时间、操作结果、IP 等字段信息。
- 审计日志要设定增删改查权限限制能力。

7 零信任安全网关与零信任控制中心的数据接口要求

7.1 通信协议要求

- 网络传输必须使用 TLS 1.2 或更高版本的协议，确保数据的安全性和隐私性。
- 请求 body 参数及响应报文内容应采用 JSON 格式，以便于解析和交互。
- 敏感信息报文应使用国密算法（非对称）加密，确保数据在传输过程中的安全性。

- 身份验证和授权访问应遵循 OIDC、OAuth2.X、SAML2.0、CAS 等 SSO 协议，确保接口请求的安全性和幂等性。

7.2 数据传输要求

零信任安全网关与零信任控制中心之间的数据通信应满足以下基本要求：

- 零信任安全网关向零信任控制中心报送身份鉴别信息的频率应不低于每 60 秒一次。
- 数据传输的延迟应控制在 3 秒以内，确保系统的实时性。
- 在通信中断的情况下，网关应暂存身份鉴别数据，并在通信恢复后及时补报。

7.3 数据接口

7.3.1 设备身份验证接口

零信任安全网关的设备身份验证接口参数应符合表 4 的要求。

表 4 设备身份验证接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备名称	deviceName	字符型	汉字、字母、数字与符号的组合，40 位	必填项
4	设备型号	deviceType	字符型	字母、数字与符号的组合，20 位	必填项
5	系统型号	systemType	字符型	字母、数字与符号的组合，30 位	必填项
6	IP	ip	字符型	数字与点号的组合	必填项
7	端口	port	整型	数字，0~65535	必填项
8	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项

零信任安全网关的设备身份验证接口响应参数应符合表 5 的要求。

表 5　设备身份验证接口响应参数

序号	字段名称	字段代码	数据类型	格式	说明
1	返回代码	code	整型	数字，3 位	必填项 200：代表成功 400：代表失败
2	返回信息	result	字符型	字母、数字与符号的组合	必填项 code 返回 400 时，返回失败原因说明

7.3.2　访问授权清单接口

零信任安全网关通过认证后，获得的访问授权清单接口的参数应符合表 6 的要求。

表 6　访问授权清单接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	密钥类型	keyType	字符型	字母、数字与符号的组合，10 位	必填项
4	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
5	数据内容	data	数组	JSON 数组	选填项
6	备注	remark	字符型	汉字、字母、数字与符号的组合	选填项

表 6 中数据内容（data）格式，应符合表 7 的要求。

表 7　访问授权清单接口参数数据内容（data）格式

序号	字段名称	字段代码	数据类型	格式	说明
1	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	身份认证 Token	authentication Token	字符型	字母、数字与符号的组合，11 位	必填项
4	有效期	expirationDate	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
5	应用系统标识列表	appIdList	数组	JSON 数组	选填项

7.3.3 安全策略接口

零信任安全网关通过认证后，获得的安全策略接口的参数应符合表 8 的要求。

表 8　安全策略接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
4	策略列表	policyList	数组	JSON 数组	选填项
5	备注	remark	字符型	汉字、字母、数字与符号的组合	选填项

表 8 中策略列表（policyList）格式，应符合表 9 的要求。

表 9　安全策略接口参数策略列表（policyList）格式

序号	字段名称	字段代码	数据类型	格式	说明
1	策略标识	policyId	字符型	字母、数字与符号的组合，11 位	必填项
2	策略名称	policyName	字符型	汉字、字母、数字与符号的组合，40 位	必填项
3	策略类型	policyType	字符型	字母、数字与符号的组合，10 位	必填项
4	策略内容	policyData	字符型	字母、数字与符号的组合，40 位	必填项

7.3.4 状态推送接口

零信任安全网关需周期性推送自身状态信息给控制中心，状态推送接口参数应符合表 10 的要求。

表 10　状态推送接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
4	CPU 使用率	cpuUsage	字符型	数字与符号，7 位	选填项
5	内存使用率	memoryUsage	字符型	数字与符号，7 位	选填项
6	磁盘使用率	diskUsage	字符型	数字与符号，7 位	选填项

7.3.5 异常告警接口

零信任安全网关在发现异常后，需实时报告异常，异常告警接口参数应符合表 11 的要求。

表 11　异常告警接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	异常告警发生时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
4	异常告警类型	exceptionAlertType	字符型	数字与符号，20 位	必填项
5	异常告警级别	exceptionAlertLevel	整型	数字，1 位	必填项 1：代表一般； 2：代表警告； 3：代表严重
6	异常告警内容	exceptionAlertContent	字符型	汉字、字母、数字与符号的组合	必填项

7.4 异常告警机制

- 明确异常告警的触发条件，包括但不限于安全策略违反、系统异常、异常访问流量等。
- 告警级别应分为一般、警告和严重三个等级，以便控制中心采取相应的响应措施。
- 告警内容应包括告警设备信息、告警发生时间、告警类型、级别、描述以及可能的解决方案或建议。

8 零信任安全网关与零信任代理的数据接口要求

8.1 通信协议要求

- 网络传输必须使用 TLS 1.2 或更高版本的协议，确保数据传输的安全性和隐私性。
- 报文内容应采用 JSON 格式，以便于系统的解析和数据交换。
- 报文结构应遵循报文头加报文体的格式，消息体应使用国密算法加密。

8.2 数据传输要求

零信任安全网关与零信任代理之间的数据通信应满足以下基本要求：

- 身份鉴别信息的报送频率不低于每 60 秒一次。
- 数据传输的延迟应控制在 3 秒以内，确保数据的实时性。
- 在通信中断的情况下，应暂存身份鉴别数据，并在通信恢复后及时补报。

8.3 数据接口

8.3.1 访问请求接口

零信任代理向零信任安全网关的访问请求接口参数应符合表 12 的要求。

表 12　访问请求接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	代理标识	agentId	字符型	字母、数字与符号的组合，11 位	必填项

2	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
4	身份认证 Token	authToken	字符型	字母、数字与符号的组合，11 位	必填项
5	应用系统标识	appId	字符型	字母、数字与符号的组合，11 位	必填项
6	应用系统名称	appName	字符型	汉字、字母、数字与符号的组合，40 位	必填项
7	IP	ip	字符型	数字与点号的组合	必填项
8	端口	port	整型	数字，0~65535	必填项

访问请求响应参数应符合表 13 的要求。

表 13　访问请求响应参数

序号	字段名称	字段代码	数据类型	格式	说明
1	返回码	code	整型	数字，3 位	必填项 200：代表成功 400：代表失败
2	返回信息	result	字符型	字母、数字与符号的组合	必填项 code 返回 400 时，返回失败原因说明

8.3.2 持续认证接口

零信任代理获得最新身份认证 Token 后，需持续进行认证，确保通信隧道不被关闭，持续认证接口参数应符合表 14 的要求。

表 14　持续认证接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	身份认证 Token	authToken	字符型	字母、数字与符号的组合，11 位	必填项

2	更新时间	updateTime	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项

8.3.3 异常告警接口

零信任网关在发现异常后，需实时报告异常，异常告警接口参数应符合表 15 的要求。

表 15　异常告警接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	网关标识	gatewayId	字符型	字母、数字与符号的组合，11 位	必填项
2	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
3	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
4	异常告警类型	exceptionAlertType	字符型	数字与符号，20 位	必填项
5	异常告警级别	exceptionAlertLevel	整型	数字，1 位	必填项 1：代表一般； 2：代表警告； 3：代表严重
6	异常告警内容	exceptionAlertContent	字符型	汉字、字母、数字与符号的组合	必填项

8.4 异常告警机制

- 零信任安全网关在检测到异常情况时，必须通过异常告警接口实时上报给零信任代理。
- 告警信息应包括告警类型、级别、时间戳、告警内容等关键信息，以便于代理进一步处理。

9 零信任代理与零信任控制中心的数据接口要求

9.1 通信协议要求

- 网络传输应使用 TLS 1.2 或更高版本的协议，保证数据传输的安全性和隐私性。
- 报文内容应采用或兼容 JSON 格式，以便系统解析和数据交换。

- 所有报文应使用国密算法进行加密，确保数据在传输过程中的安全性。
- 身份验证和授权访问应遵循 OIDC 协议，确保接口请求的安全性和幂等性。

9.2 数据传输要求

零信任代理与零信任控制中心的数据接口之间的数据通信应满足以下基本要求：

- 零信任代理应至少每 60 秒向零信任控制中心报送一次身份鉴别信息。
- 数据传输的延迟应低于 3 秒，确保系统的实时性。
- 在通信中断的情况下，代理应暂存身份鉴别数据，并在通信恢复后即时补报。

9.3 数据接口

9.3.1 身份认证接口

零信任代理的身份认证接口参数应符合表 16 的要求。

表 16　身份认证接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	代理标识	agentId	字符型	字母、数字与符号的组合，11 位	必填项
2	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
4	用户认证方式	userAuthentication Method	整型	数字，1 位	必填项 1：代表本地认证； 2：代表第三方认证；
5	用户认证列表	userAuthentication List	数组	JSON 数组	选填项
6	设备型号	deviceType	字符型	字母、数字与符号的组合，20 位	必填项
7	系统型号	systemType	字符型	字母、数字与符号的组合，30 位	必填项
8	位置经度	longitude	浮点型	ISO 6709:2022[+/-	必填项

				DD.DDDD]，其中第一个“+/-”表示经度正负	单位：度（°） 精确到小数点后 7 位，乘 10 的 7 次方后传输
9	位置纬度	latitude	浮点型	ISO 6709:2022[+/-DD.DDDD]，其中第一个“+/-”表示纬度正负	必填项 单位：度（°） 精确到小数点后 7 位，乘 10 的 7 次方后传输
10	IP	ip	字符型	数字与点号的组合	必填项
11	端口	port	整型	数字，0~65535	必填项
12	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项

表 16 中用户认证列表（userAuthenticationList）格式，应符合表 17 的要求。

表 17　身份认证接口参数用户认证列表（userAuthenticationList）格式

序号	字段名称	字段代码	数据类型	格式	说明
1	认证类型	authenticationType	整型	数字，2 位	必填项 1：代表静态密码； 2：代表短信码； 3：代表邮箱码； 4：代表动态令牌； 5：代表指纹； 6：代表人脸； 7：代表虹膜；
2	认证值	authenticationContent	字符型	字母、数字与符号的组合,500 位	必填项

身份认证响应参数应符合表 18 的要求。

表 18　身份认证响应参数

序号	字段名称	字段代码	数据类型	格式	说明
1	返回代码	code	整型	数字，3 位	必填项 200：代表成功

					400：代表失败
2	返回信息	result	字符型	字母、数字与符号的组合	必填项 code 返回 400 时，返回失败原因说明
3	身份认证 Token	authToken	字符型	字母、数字与符号的组合，11 位	返回代码为 200 时，必填
4	有效期	expirationDate	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	返回代码为 200 时，必填

9.3.2 资源访问清单接口

零信任代理通过认证后，获得的资源访问清单接口的参数应符合表 19 的要求。

表 19　资源访问清单接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	代理标识	agentId	字符型	字母、数字与符号的组合，11 位	必填项
2	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
4	密钥类型	keyType	字符型	字母、数字与符号的组合，10 位	必填项
5	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
6	资源列表	resourceList	数组	JSON 数组	选填项
7	备注	remark	字符型	汉字、字母、数字与符号的组合	选填项

表 19 中资源列表（resourceList）格式，应符合表 20 的要求。

表 20　资源访问清单接口参数资源列表（resourceList）格式

序号	字段名称	字段代码	数据类型	格式	说明

1	应用系统标识	appId	字符型	字母、数字与符号的组合，11 位	必填项
2	应用系统名称	appName	字符型	汉字、字母、数字与符号的组合，40 位	必填项
3	IP	ip	字符型	数字与点号的组合	必填项
4	端口	port	整型	数字，0~65535	必填项

9.3.3 状态推送接口

零信任代理需周期性推送状态信息给控制中心，状态推送接口参数应符合表 21 的要求。

表 21　状态推送接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	代理标识	agentId	字符型	字母、数字与符号的组合，11 位	必填项
2	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
4	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
5	IP	ip	字符型	数字与点号的组合	必填项
6	端口	port	整型	数字，0~65535	必填项
7	CPU 使用率	cpuUsage	字符型	数字与符号，7 位	选填项
8	内存使用率	memoryUsage	字符型	数字与符号，7 位	选填项
9	磁盘使用率	diskUsage	字符型	数字与符号，7 位	选填项

9.3.4 异常告警接口

零信任代理在发现异常后，需实时报告异常，异常告警接口参数应符合表 22 的要求。

表 22　异常告警接口参数

序号	字段名称	字段代码	数据类型	格式	说明
1	代理标识	agentId	字符型	字母、数字与符号的组合，11 位	必填项
2	用户标识	userId	字符型	字母、数字与符号的组合，11 位	必填项
3	设备标识	deviceId	字符型	字母、数字与符号的组合，11 位	必填项
4	当前时间	timestamp	字符型	ISO 8601[YYYY-MM-DDTHH:MM:SSZ]	必填项
5	异常告警类型	exceptionAlertType	字符型	数字与符号，20 位	必填项
6	异常告警级别	exceptionAlertLevel	整型	数字，1 位	必填项 1：代表一般 2：代表警告 3：代表严重
7	异常告警内容	exceptionAlertContent	字符型	汉字、字母、数字与符号的组合	必填项

9.4 异常告警机制

- 零信任代理在检测到异常情况时，应通过异常告警接口实时上报给零信任控制中心。
- 告警信息应包括告警类型、级别、时间戳、告警内容等关键信息，以便于控制中心进一步处理。