

SZSD

数 字 山 东 工 程 标 准

SZSD01 0016—2024

基于零信任的数字机关应用运行安全体系 建设与评估指南

Construction and evaluation guidelines for operation security system of digital
government agencies based on zero trust

2024 - 04 - 15 发布

2024 - 06 - 01 实施

济南市大数据局 发 布

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 安全体系建设 2

 4.1 参考框架 2

 4.2 建设过程及要求 3

5 安全评估指南 4

 5.1 评估原则 4

 5.2 评估实施流程 4

 5.3 评估指标体系 4

 5.4 评估指标分级 6

附 录 A（资料性） 南北向安全防护应用场景..... 8

附 录 B（资料性） 东西向安全防护应用场景..... 11

附 录 C（资料性） 数字机关信息系统零信任应用示例..... 14

参 考 文 献 16

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专利的责任。

本文件由济南市大数据局提出、归口并组织实施。

本文件起草单位：济南市大数据局、国家计算机网络与信息安全管理中心山东分中心、中孚安全技术有限公司、北京笛卡尔盾科技有限公司、山东方寸微电子科技有限公司、山东中创软件商用中间件股份有限公司。

本文件主要起草人：王越、李胜葆、陈晓光、刘德莉、杨文宏、陈长成、崔新安、张建彬、周春龙、何忠胜、刘静。

基于零信任的数字机关应用运行安全体系建设与评估指南

1 范围

本文件提供了济南市数字机关基于零信任理念构建应用运行安全体系的建设的总体框架、零信任安全评估体系以及典型应用场景等内容。

本文件适用于济南市市、县（区）数字机关零信任应用运行防护体系建设的参考，以及数字机关和测评单位对零信任应用运行安全体系的评估依据。

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 18794.3—2003 信息技术 开放系统互连 开放系统安全框架 第3部分：访问控制框架

GB/T 20984 信息安全技术 信息安全风险评估规范

GB/T 25069 信息安全技术 术语

3 术语和定义

GB/T 25069界定的术语和定义适用于本文件。

3.1

数字机关 digital government agencies

将数字化理念和数字技术应用到事务工作的全过程、全领域的机关单位。

3.2

零信任 zero Trust

一种以资源保护为核心的网络安全理念。认为对资源的访问，无论主体和资源是否可信，主体和资源之间的信任关系都需要从零开始，通过持续环境感知与动态信任评估进行构建，从而实施访问控制。

3.3

零信任技术 zero trust technology

以零信任安全理念，降低访问过程安全风险的持续动态安全访问控制技术。

3.4

零信任系统 zero trust system

基于零信任技术的相关产品和服务，或者是产品和服务的组合。

3.5

访问主体 access subject

发起资源访问请求的用户、设备、软件应用、系统等对象。

3.6

访问客体 access object
表示需要被保护和受到控制的系统或资源。

4 安全体系建设

4.1 参考框架

4.1.1 总体框架

构建零信任应用运行安全体系，需从零开始构建访问主体和资源之间的信任关系，并持续对访问主体进行安全风险监测，实现动态访问控制。参照GB/T 18794.3—2003定义的通用访问控制框架，数字机关的零信任安全体系参考框架如图1所示。

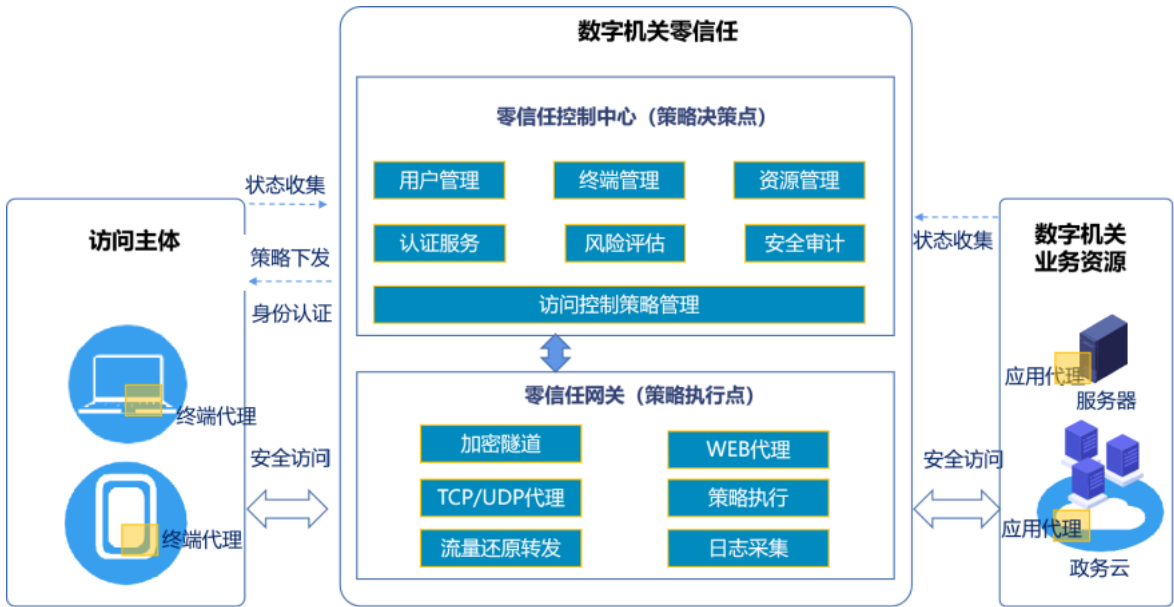


图1 数字机关零信任安全体系参考框架

4.1.2 零信任控制中心

零信任控制中心是零信任安全体系的大脑，主要功能包括但不限于：

- a) 能支持制定终端到业务资源、业务应用之间的访问控制策略；
- b) 能支持管理用户、终端、资源信息，对访问主体的统一身份认证；
- c) 能支持收集终端、业务资源的状态信息以及其他网络威胁情报，进行安全审计和整体风险评估，根据风险动态调整访问控制策略；
- d) 能支持收集终端的环境信息，进行环境分析，识别环境风险；
- e) 能支持收集用户的行为日志，进行用户行为分析，识别用户行为风险。

4.1.3 零信任网关

零信任网关是零信任安全体系中的策略执行组件，接收并执行零信任控制中心下发的策略。功能包括但不限于：

- a) 能支持与终端代理及应用代理建立加密隧道，保证数据的传输安全；
- b) 能支持对应用资源创建 WEB 代理、TCP/UDP 代理等反向代理，防止未授权的资源访问；
- c) 能支持根据策略对特定流量进行还原转发，以进一步识别风险；
- d) 能支持进行访问日志采集上报，便于综合的动态风险评估。

4.1.4 零信任访问主体

零信任访问主体包括终端代理和应用代理，主要功能包括但不限于：

- a) 能支持与零信任网关之间建立加密隧道，保证通信链路的传输安全；
- b) 能支持识别终端和应用的身份，便于终端访问业务资源以及应用之间互相访问资源时的身份认证以及权限控制；
- c) 能支持终端环境信息采集上报，便于对接入终端的执行环境进行风险评估；
- d) 能支持终端行为日志采集上报，便于对接入的终端用户的行为进行风险评估；
- e) 能支持接收零信任控制中心下发的安全策略，依据策略对终端进行相应的安全控制。

4.2 建设过程及要求

4.2.1 设计阶段

设计阶段应依据法律法规要求，基于零信任理念进行安全需求分析，确定安全设计原则和安全标准：

- a) 应梳理用户、设备、数据和应用清单并进行风险评估；
- b) 应梳理用户和应用之间，应用和应用之间的访问关系、访问权限等，并进行风险评估；
- c) 应依据风险评估报告，结合零信任理念和业务需求设计安全体系建设方案；
- d) 安全体系建设方案中应选用具有自主知识产权的零信任解决方案和相关产品；
- e) 安全体系建设方案应满足等保条例以及密改密评中对应的安全要求；
- f) 安全体系建设方案应通过安全专家组的评审。

4.2.2 建设阶段

建设阶段应按照建设方案实施，确保安全体系的建设合法合规且具备安全对抗能力：

- a) 应选择具有安全资质的集成商负责安全体系的建设；
- b) 应实现以身份为中心的访问控制机制，为用户、设备和应用设置统一的身份标识；
- c) 应采用细粒度访问控制策略对各个应用的访问权限进行设置；
- d) 应统一管理用户和应用之间，应用和应用之间的访问关系和访问权限；
- e) 应基于最小权限原则给访问主体分配所需的功能和接口权限；
- f) 应对访问主体的身份、行为、网络环境、终端环境等因素进行持续风险评估；
- g) 应基于持续的风险评估结果动态调整访问主体对资源的访问权限；
- h) 应满足网络、存储和计算等性能要求，确保安全体系的稳定运行；
- i) 应具备指导用户进行系统运行维护的相关文档；
- j) 应对运维等相关人员进行培训；
- k) 应在交付前对运行安全体系进行专门的安全测试。

4.2.3 运行阶段

运行阶段需保证安全体系的稳定运行，从而保障数字机关业务系统的安全运行：

- a) 应及时处置安全体系的告警和异常事件信息；
- b) 应定期对安全体系的各个组件进行巡检，及时发现并处理安全风险；

- c) 应及时对安全体系的各个组件升级和更新补丁；
- d) 应定期对安全体系防护的关键数据进行备份；
- e) 应定期对安全体系进行应急响应演练。

4.2.4 关停阶段

关停阶段应保障业务平稳过渡且谨防敏感信息泄露：

- a) 应在停用下线前提供满足客户使用的更新软件，制定下线方案与计划，确保数字机关业务的平滑过渡；
- b) 应妥善处理相关程序和数据信息，删除残留信息，确保数据留存符合最小化原则；
- c) 应进行安全检测和风险评估，确保除例外的要求和规则外，软件产品及其相关信息被完全清除。

5 安全评估指南

5.1 评估原则

安全评估原则包括：

- a) 以零信任安全理念为导向：基于零信任“永不信任，持续验证”的安全理念，对数字机关系统中身份、网络、应用、数据、基础设施进行评估；
- b) 采用静态与动态相结合：评估过程中既要收集系统的技术架构、系统部署等文档进行分析评估，又要在系统中采用模拟攻击、动态监控、日志分析等手段进行评估；
- c) 数据客观、注重实效原则：在保证数字机关系统正常运转下，采用定量与定性相结合的方法对数字机关系统中身份、网络、应用、数据、基础设施等方面进行评估，客观、实效地反映数字机关整体安全防护水平。

5.2 评估实施流程

评估实施流程如下：

- a) 评估发起：根据评估目标，选择评估对象和指标项，发起评估；
- b) 预评估：被评估对象根据评估要求，进行初步预评估及准备评估资料；
- c) 正式评估：由评估方采用现场进行评估；
- d) 发布评估结果：评估方计算评估分数，发布评估结果；
- e) 改进提升：被评估方根据评估结果反馈进行改进提升。

5.3 评估指标体系

5.3.1 身份

数字机关应建立统一的身份认证体系，各机构应确保用户和实体因正确的目的，在正确的时间访问正确的资源，且未授予他们过多的访问权限，相关技术要求如下：

- a) 身份认证，应持续对接入数字机关办公人员/运维人员使用 MFA 对身份进行验证，而不仅仅是在最初授权时进行验证；
- b) 身份库，应在整个数字机关环境中以及合作伙伴的环境中安全地整合身份库；
- c) 风险评估，应基于持续分析和动态规则，实时地确定办公人员/运维人员身份风险，以提供持续的保护；
- d) 访问管理，应使用自动化来实现即时授权和恰到好处的授权，以满足办公人员/运维人员的操作和资源需求。

5.3.2 设备

设备是指数字机关的硬件、软件、固件等资产。为确保所有设备的安全性，管理安全风险，并阻止未经授权设备访问资源，相关技术要求如下：

- a) 策略执行和合规监控，应在设备和虚拟资产的整个生命周期中，持续检查并执行合规策略；
- b) 应在数字机关的所有环境中对设备、软件、配置和漏洞管理进行整合，包括虚拟资产；
- c) 资产与供应链风险管理，应提供全面的、实时或接近实时的、跨供应商和服务提供商的资产视图，在合适情况下，自动化其供应链风险管理；
- d) 资源访问，应在资源访问时应对设备和虚拟资产进行实时风险分析；
- e) 设备威胁保护，应部署集中式的，具有先进功能的威胁保护安全解决方案，对所有设备和虚拟资产进行保护，并在设备威胁保护、策略实施和合规监控方面采用统一的方法；
- f) 终端安全隔离，终端设备如存在一机两用场景，应支持安全隔离，即将工作秘密区与非工作秘密区进行隔离，包括网络隔离、会话隔离和存储隔离。

5.3.3 网络

为保证整个数字机关网络的安全，相关技术要求如下：

- a) 网络微隔离，数字机关内相关应用之间要建立分布式的微隔离边界，当应用之间需要交互时，微隔离平台应提供即时的、适度的联通；
- b) 网络流量管理，应具备网络流量管理功能，依据不同应用的特性，构建动态的网络规则和配置，并持续进行评估，依据任务的关键性和风险，不断调整应用的优先级；
- c) 流量加密，应根据需要持续加密流量，密钥的管理采用最小权限原则，以保证密钥的安全，并采取了最佳实践来方便密码的使用；
- d) 网络弹性，应能及时感知所有工作负载的可用性变化，提供相应的弹性机制，在工作负载异常过大时，仍然能提供基本的服务，保持网络的可用性。

5.3.4 应用和工作负载

数字机关内部署有大量的系统、计算机程序和服务，包括内部应用和公共应用。为保护这些应用和工作负载的安全，相关技术要求如下：

- a) 应用访问控制，应对应用程序采取持续的访问授权机制，并结合实时的风险分析，以及行为或使用模式等因素的影响；
- b) 应用威胁防护，应将高级威胁保护集成到所有应用的工作流中，提供实时可见性和内容感知保护，以应对特定于应用程序的复杂攻击；
- c) 可访问的应用，应根据需要，把所有适用的应用通过开放的公共网络提供给授权用户和设备使用；
- d) 安全的应用开发和发布流程，在可行的情况下充分利用不可变工作负载，只能通过重新部署来更改工作负载，支持自动化的代码部署流程，并取消管理员对部署环境的访问权限；
- e) 应用安全测试，应将应用安全测试集成到从开发到部署的整个软件开发周期中，并实现日常、自动化测试。

5.3.5 数据

数据包括所有结构化和非结构化的文件和碎片，存在于系统、设备、网络、应用程序、数据库、基础设施和备份中，包括相关的元数据。基于零信任的数字机关安全防护体系，在数据防护方面的相关技术要求如下：

- a) 应确保数字机关数据的识别和清点，能自动检测到数据环境的任何更改；

- b) 能对数据环境进行审查，以确定与数据丢失、攻击或任何其他未经授权的更改或访问相关的潜在风险；
- c) 应持续维护数字机关所有使用数据的清单，并采用强大的数据防泄漏策略，动态阻止可疑的数据泄露；
- d) 能实现用细粒度、结构化格式自动对所有数字机关数据执行分类并标记；
- e) 能根据用户和实体需求动态调整优化数字机关数据的可用性；
- f) 能在整个数字机关范围内实现自动化数据访问控制，并持续审查权限；
- g) 能实现必要的数据加密，执行最小授权原则以进行安全密钥管理；
- h) 能使用最新的安全标准和密码敏捷性应用加密技术。

5.3.6 可视化与分析

可视化是指从数字机关的事件特征中产生的可观测指标。对与数字机关安全相关的数据进行分析有助于提供策略决策依据、促进应急响应活动，并采取有效的安全措施。基于零信任的数字机关体系，在可视化与分析方面，相关技术要求如下：

- a) 能组织收集和处理所有日志，包括网络、数据、应用程序、设备和用户日志，日志和事件遵循标准化格式，并根据需要开发规则或分析；
- b) 能对用户活动日志进行自动化分析，维护数字机关范围内的全面可见性和态势感知；
- c) 能自动化采集所有设备和虚拟资产的状态，并与身份关联、执行端点监控和异常检测，为资源授权提供信息；
- d) 能跟踪虚拟资产的供应和销毁模式以监测异常；
- e) 能维持对整个数字机关的通信可见性，并自动对所有检测源的检测信息进行关联；
- f) 能在所有应用程序上执行持续、动态的监控，以保持全面可见性；
- g) 能实现全面跟踪数据生命周期，并具备强大的分析能力，支持全面的数据视图和持续的安全状况评估；
- h) 能实现对日志和事件的集中、动态监控和高级分析，以达到数字机关范围内的全面可见性。

5.3.7 自动化与编排

基于零信任的数字机关安全防护体系，采用自动化工具和 workflows。在自动化与编排方面，相关技术要求如下：

- a) 应能在整个数字机关实现完全集成的所有身份自动编排；
- b) 应能通过全自动流程，实现连接数字机关的设备及虚拟资产的供应、注册、监控、隔离、修复和销毁；
- c) 应能由基础设施定义网络和环境，并实现自动化的变更管理方法，包括自动的初始化和过期失效；
- d) 应能自动处理数字机关应用程序配置，实现安全性和性能的持续优化；
- e) 应能最大程度地自动化实施数字机关所有数据的生命周期管理和安全策略；
- f) 应能动态响应整个数字机关范围内的需求变化和环境变化。

5.4 评估指标分级

零信任应用运营安全体系的建设是一个持续的过程，数字机关单位在建设过程中可按步骤实施，首先实现基本级，保证合法合规要求，并具备一定的对抗性；增强级是在符合基本级要求基础上，依据业务需求提升对抗能力。具体指标分级如表 1 所示。

表1 评估指标分级表

评估指标	基本级	增强级
身份	a, b	c, d
网络	a, b, c	d
应用和工作负载	a, b, c	d, e
数据	a, b, c	d, e, f
设备	a, b, c	d, e
可视化与分析	a, b, c, d	e, f, g, h
自动化与编排	a, b	c, d, e, f

附 录 A
(资料性)
南北向安全防护应用场景

A. 1 场景描述

数字机关南北向资源访问控制主要通过零信任控制中心、安全协同系统、零信任网关以及零信任终端完成，数字机关南北向资源访问控制场景见图2。具体组成包括：

- a) 终端用户（访问主体）为资源访问发起方；
- b) 零信任网关提供对来访请求的转发和拦截功能；
- c) 零信任控制中心提供对来访请求的认证和持续访问控制功能；
- d) 安全协同系统通过接口为控制中心提供证书类、分析类以及防护类安全支撑，辅助零信任控制中心决策数字机关业务系统（访问客）体提供被访问的资源服务。

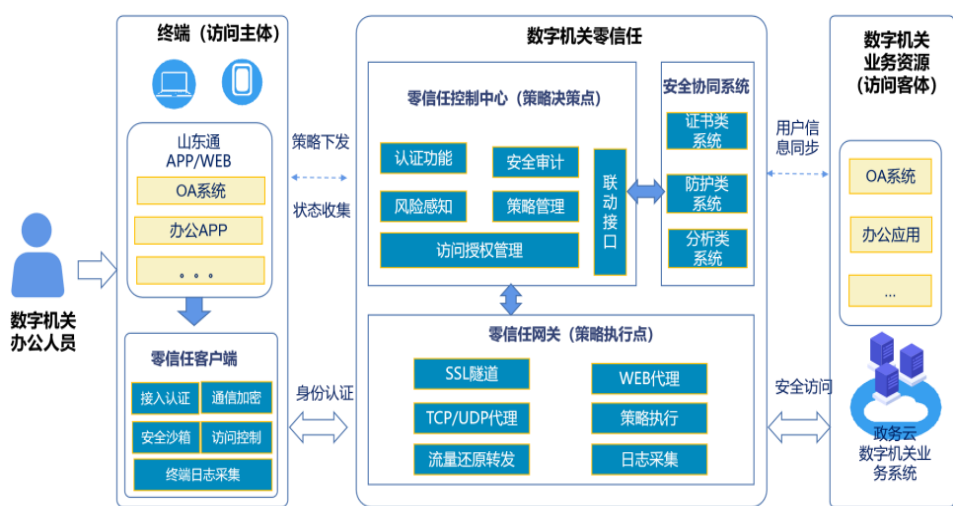


图 A. 1 数字机关南北向安全防护场景

A. 2 关键功能要求

A. 2. 1 通信安全

通信传输安全功能应符合以下要求：

- a) 控制通信传输加密功能应支持客户端 agent 与控制中心通信应采用双向加密，相互验证，防止伪造的服务器或者终端。如双向加密传输等；
- b) 数据通道传输加密功能应支持客户端代理可以把任意流量加密，再转发到网关再鉴权解密到目的系统，防止终端到网关的网络存在中间人劫持，如 https 等。

A. 2. 2 安全认证

安全认证功能应符合以下要求：

- a) 应支持统一身份认证以及对接用户的认证信息；
- b) 应能够提供本地账户的创建、批量导入、批量导出（加密导出/明文导出）、修改、删除；
- c) 应支持与第三方认证体系对接，能够同步第三方对应的账户、组织架构信息等；
- d) 多因素认证功能应支持数字证书、动态令牌、短信、扫码、token、人脸识别等；
- e) 单点登录授权功能应支持 SAML2.0、Oauth2 协议。

A. 2.3 策略管理

零信任策略管理功能应符合以下要求：

- a) 零信任策略服务接收零信任客户端的鉴权请求并转发给零信任授权管理模块；
- b) 支持与零信任授权管理模块对接，根据权限服务的鉴权结果下发应用访问控制策略至相应的零信任代理客户端；
- c) 接收零信任权限服务下发的用户权限变更结果，并将变更结果下发给应用控制代理、可信接入代理、可信 API 代理；
- d) 需具备基于用户可信评分的应用控制策略管理能力，根据可信评分阈值制定不同的应用访问控制策略，支持自定义评分阈值、自定义策略关联的策略执行点、自定义策略执行点处置动作、自定义策略生效的用户组。

A. 2.4 访问授权

访问授权管理功能应符合以下要求：

- a) 支持存储用户安全等级、应用安全等级、API 安全等级，用于判断用户是否有权限访问应用或 API；
- b) 够接收零信任策略引擎发送的用户可信评分并根据评分调整用户安全等级；
- c) 支持自定义零信任用户组；
- d) 支持服务资源目录定义管理；
- e) 支持基于零信任用户组设置访问控制策略，访问指定的服务资源；
- f) 支持基于用户业务需求自定义应用访问控制策略；
- g) 支持基于终端应用沙箱或应用容器，授权可信的沙箱或容器应用访问后端资源。

A. 2.5 风险感知

风险感知功能应支持用户行为、终端环境、网络环境三种风险感知，相关感知能力要求如下：

- a) 包含终端暴力破解检测、账号异地登录检测、用户截屏/录屏检测、用户使用第三方分享功能检测等用户行为风险感知能力；
- b) 包含终端 ROOT/越狱检测、终端无锁屏密码检测、高风险应用安装检测、终端病毒感染检测、操作系统漏洞检测等终端风险检测能力；
- c) 包含连接风险 WIFI 检测、命令注入攻击检测、SQL 注入攻击检测、恶意加密 C&C 流检测、DGA 域名请求等网络风险感知能力。

A. 2.6 安全审计

安全审计日志功能要求如下：

- a) 对于访问行为日志，应支持如下访问连接行为信息的采集：用户身份、设备身份、终端应用进程、IP、目的 IP、源端口、目的端口、协议、域名、uri、时间、状态；
- b) 对于终端认证日志，应支持如下信息收集：认证时间、认证身份、来源设备信息、网络信息、认证结果；
- c) 对于审计日志，应支持收集后台管理系统管理员操作行为。

A. 2.7 开放接口

开放接口对接要求功能如下：

- a) 应支持通过常见认证协议，如 LDAP, OAuth2.0、RADIUS、OIDC、SAML 等对接第三方认证系统；

- b) 应支持提供给第三方安全协同系统调用的接口，出现安全风险的时候，支持阻断身份、应用、终端设备标识对应的所有访问连接；
- c) 应支持安全状态信息收集接口，接收第三方安全协同系统状态信息，用于角色判断用户访问策略，提供安全状态信息接收接口；
- d) 应支持访问行为日志对外输出，可以提供给第三方安全分析系统针对本系统获取到的日志，如认证、访问日志等。

A. 2. 8 部署要求

A. 2. 8. 1 控制中心部署

控制中心部署功能要求如下：

- a) 应支持单机、集群、多级部署模式，集群模式具备扩展性，实现服务的弹性伸缩，集群内避免异构部署模式；多级模式下，控制中心独立部署、互相隔离，仅通过服务总线实现跨控制中心服务调用；
- b) 应支持高并发机制，确保单节点并发处理能力满足并发处理要求，对高频访问数据采用高速分布式缓存，确保服务达到响应时间要求；
- c) 应支持数据库的分布式部署，建设分布式数据库集群，隶属于控制中心的数据库仅支持本控制中心垂直访问；
- d) 应支持可运维性，统计和展示服务调用量、异常量、最高并发量等运行情况，支持系统的安装、配置、部署、升级操作；
- e) 应支持授权、保护等策略管理，包括制定、修改、删除、审核与发布等。

A. 2. 8. 2 网关部署

网关部署功能要求如下：

- a) 宜支持集群部署，集群架构具备扩展性，实现服务的弹性伸缩，集群内避免异构部署模式；
- b) 宜支持加速和动态分发，采用负载均衡技术，实现接入的均衡分布。

A. 2. 8. 3 客户端部署

零信客户端功能要求如下：

- a) 能支持有代理模式，支持的客户端操作系统类型应包括且不限于麒麟、统信等；
- b) 能支持无代理模式，支持各类标准浏览器访问。

附录 B
(资料性)
东西向安全防护应用场景

B.1 场景描述

数字机关东西向资源访问控制主要是通过零信任控制中心、零信任网关以及零信任应用代理三部分。数字机关东西向资源控制场景如图3所示：

- a) 零信任控制中心提供认证、访问授权、策略统一管理、策略动态调整、安全管理能力和第三方联动管理；
- b) 零信任网关负责在网络层接受并执行控制中心下发的策略，对应用进行访问授权，记录应用访问日志并加密上传至控制中心，根据需要扩充安全监测、安全防护能力；
- c) 零信任代理负责对业务应用进行认证，接受并执行控制中心下发的策略，对应用及接口进行访问授权，记录工作负载访问日志并加密上传至控制中心。

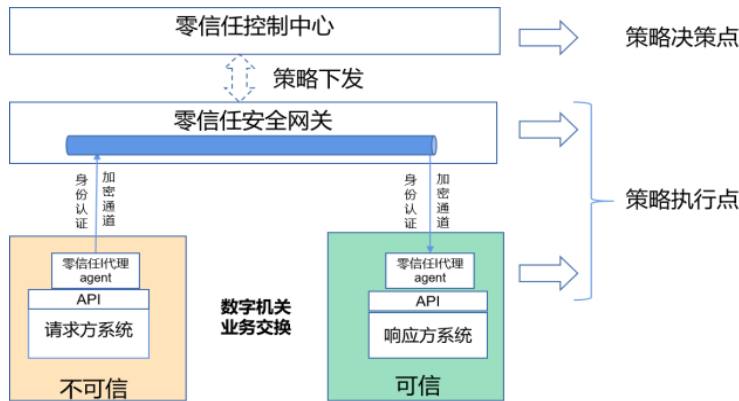


图 B.1 数字机关东西向资源访问控制

B.2 关键功能要求

B.2.1 认证功能要求

认证功能要求应符合：

- a) 应支持自身具备或可从外部获取工作负载基本信息的功能，基本信息包括操作系统版本、网卡信息、服务信息、监听端口信息等；
- b) 应能够为每一台工作负载确定唯一标识的身份信息；
- c) 应支持当主机信息发生变化时，可上传至管理端；
- d) 应支持认证组件在控制中心组件中负责主体的身份认证。认证组件可以自己完成，或提供与第三方认证对接的接口。实现对工作负载的认证。

B.2.2 访问控制功能

零信任客户端/网关组件要具备访问控制能力，具体要求如下：

- a) 应支持客户端组件使用最小安全原则，即除非明确允许，否则阻断；
- b) 应能实现基于源 IP 地址、目的 IP 地址和端口的访问控制；
- c) 应支持实现出站和入站的双向访问控制；
- d) 应支持接收并执行控制中心组件下发的动态访问控制策略；
- e) 应支持记录违反策略规则的阻断日志，并上传至控制中心组件。

- f) 宜支持组件对 ipv6 网络流量进行访问控制；
- g) 宜支持组件进行容器之间的访问控制；
- h) 宜支持通过建立服务之间的加密隧道来实现访问控制。

B.2.3 策略管理要求

策略管理要求应符合如下要求：

- a) 应支持通过集中安全管理界面对分布式部署的安全服务组件的统一策略下发；
- b) 应支持配置任意两个工作负载之间的安全策略；
- c) 应支持接收策略控制点组件上传的工作负载策略状态变化信息；
- d) 宜支持基于识别到的流量自动或半自动的方式生成安全策略；
- e) 宜支持基于业务角色、主机属性等进行安全策略配置；
- f) 宜支持应具备防护及非防护状态，尽可能减少策略配置对业务的影响。

B.2.4 动态授权要求

动态授权功能要求如下：

- a) 宜支持在业务系统发生变化时，如虚拟机下线、IP 地址变化或虚拟机迁移时，动态调整访问控制策略；
- b) 宜支持在业务系统认证信息发生变化时，动态调整访问控制策略。

B.2.5 可信 API 代理

可信API代理功能应符合以下要求：

- a) 可信 API 代理向零信任策略管理发送鉴权请求；
- b) 根据零信任控制中心返回的鉴权结果判断用户是否具备对 API、数据的访问权限；针对有权限的用户则将相关请求转发至数字机关业务应用（后置），否则拒绝该请求；
- c) 提供给第三方安全系统调用的接口，出现安全风险的时候，支持阻断身份、应用、终端设备标识对应的所有访问连接；
- d) 提供给第三方安全分析系统针对本系统获取到的日志，如认证、访问日志等。

B.2.6 流量识别分析

应用间流量识别功能要求如下：

- a) 应能识别出站及入站的网络流量，包括流量的来源 IP，目的 IP，端口及服务信息等；
- b) 应支持管理中心将学习到的流量信息统一进行呈现及搜索；
- c) 应支持以报表形式输出流量统计分析结果；
- d) 应支持记录异常访问日志，并支持输出到第三方平台；
- e) 应支持通过组件上传的流量，展示实时业务应用间流量关系拓扑，并标识流量与安全策略的匹配情况，包括匹配策略的流量和不匹配策略的流量；
- f) 应支持对组件上传的阻断日志进行统一的查看，并支持基于时间、来源、目的、端口等维度的分析；
- g) 可支持识别 IPv6 的出站及入站的流量。

B.2.7 部署要求

部署功能要求如下：

- a) 零信任控制中心应支持集群化部署，具备高可用性；

- b) 零信任客户端/网关组件应能支持自动化部署。

附录 C
(资料性)
数字机关信息系统零信任应用示例

C.1 项目背景

济南市业务协同交换系统是该市数字机关建设的关键基础设施，旨在建设全市各级机关应用之间进行协同互联的数字高速公路网，支撑全市各级机关办公、办事、办会、督办等各类业务之间的高效协同任务，一旦接入非法或不可控应用与用户，将带来严重损失，安全问题迫在眉睫。

C.2 现状分析

业务协同交换系统整体架构如下图所示：

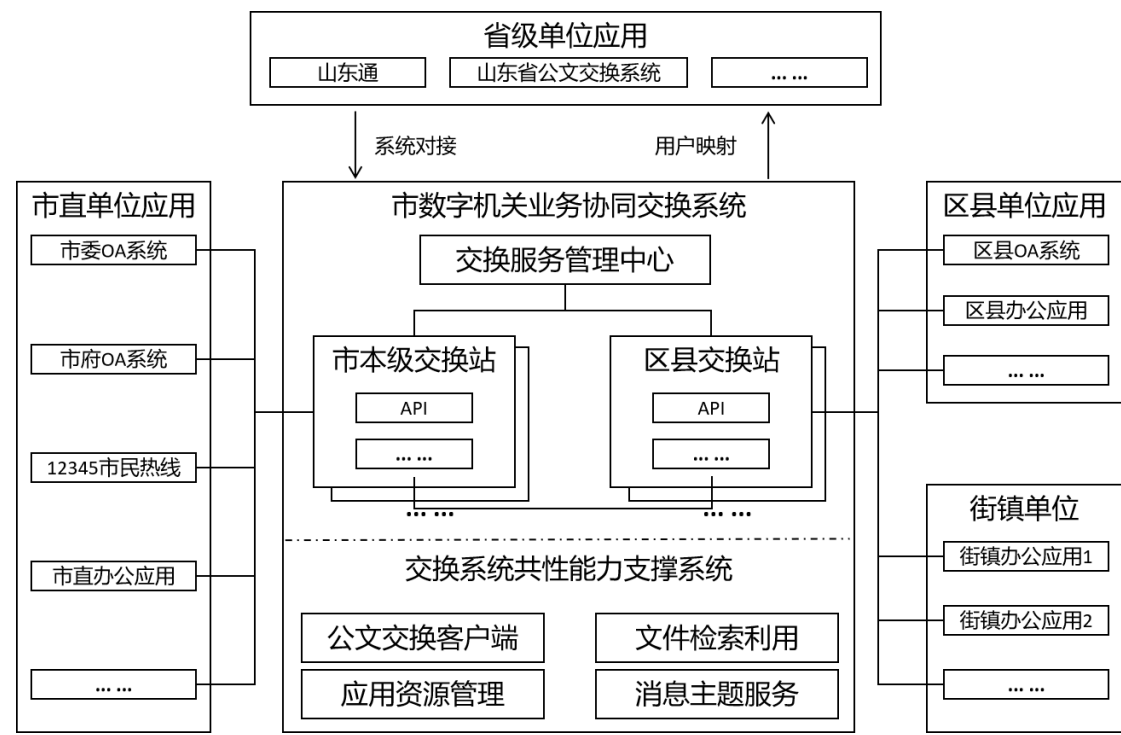


图 C.1 数字机关业务协同交换系统架构图

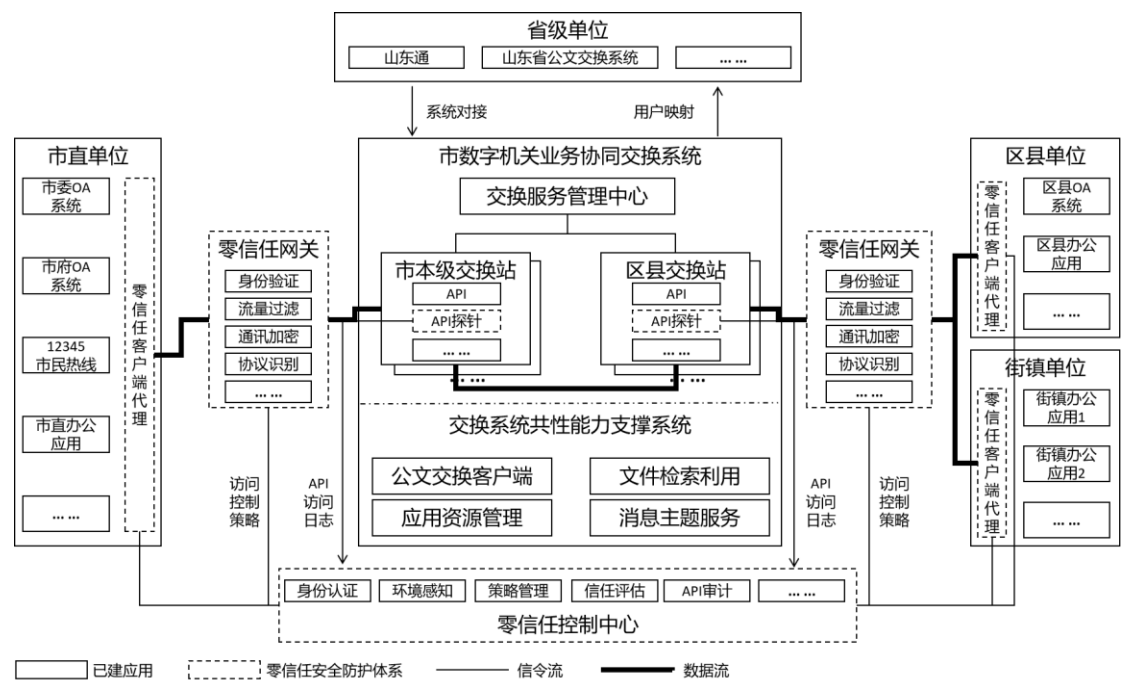
业务协同交换系统的主要功能是提供跨部门之间的业务数据交换，在方便各部门业务之间协同交换的同时，引入了新的安全风险。比如各业务系统在协同交换过程中，应用身份鉴别、访问权限控制和API接口审计等关键环节都缺乏有效的安全管控手段，存在非法访问、越权访问、API接口二次封装/转发等安全风险。

C.3 需求分析

为保证业务协同交换系统的安全稳定运行，基于零信任理念构建安全防护体系，需在以下几个方面加强安全防护：一是强化应用身份鉴别。每个合法应用都需要设置唯一的身份标识，并对身份进行鉴别，只有具有合法身份的应用才能访问业务协同交换系统；二是精细化动态访问控制。业务协同交换系统需采用白名单策略，默认最小授权原则，给各个应用分配相应的访问权限。并依据环境的变化对访问权限进行动态调整；三是增加API接口安全审计。所有访问API接口的行为都需要记录日志，并提供审计服务，及时发现数据违规导出、越权调用、数据泄露、API接口滥用、转发等风险。

C.4 解决方案

基于零信任理念和零信任参考架构，安全防护体系的总体框架图如下所示：



C.4.1 零信任控制中心

零信任控制中心相当于整个安全防护体系的大脑，主要负责对合法应用进行身份认证并授权；收集各个应用的环境信息和行为信息，通过大数据平台进行用户行为分析和信用评估，依据分析和评估结果动态调整各个应用的访问策略；收集交换站侧的API访问日志，分析识别API访问相关风险。

C.4.2 零信任网关

零信任网关部署在应用和业务协同交换系统之间，对业务协同交换系统进行安全防护，具备身份和授权验证、流量过滤、通讯加密以及协议识别等核心能力，为应用和业务协同交换系统之间提供便捷、安全的通信环境和访问控制机制，防止非法应用、非法设备访问等风险。

C.4.3 零信任客户端代理

零信任客户端代理部署在应用侧，一是负责与零信任控制中心进行交互，进行身份认证，采集并上报环境信息和用户操作访问日志等，并接收和执行控制中心下发的安全策略；二是负责与零信任网关之间建立安全隧道，进行加密通信。

C.4.4 API探针

API探针部署在业务协同交换系统内部，对各个交换站的API接口进行监听，采集、解析API访问日志，并上报给零信任控制中心进行分析。

参 考 文 献

- [1] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
 - [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 34678-2017 智慧城市 技术参考模型
 - [4] GB/T 37971-2019 信息安全技术 智慧城市安全体系框架
 - [5] GB/Z 38649-2020 信息安全技术 智慧城市建设信息安全保障指南
 - [6] GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
 - [7] GM/T 0094-2020 公钥密码应用技术体系框架规范
 - [8] DB37/T 4550-2022 智慧城市网络安全建设和评估指南
-