

SZSD

数 字 山 东 工 程 标 准

SZSD01 0010—2024

政务信息系统 零信任网络安全应用要求

Government information system—Application requirements of cybersecurity for 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

引言 III

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 总体原则 2

6 零信任网络安全应用要求 2

 6.1 已建政务信息系统 2

 6.2 新建政务信息系统 3

7 网络安全应用管理要求 4

附录 A（资料性） 已建政务信息系统零信任网络安全应用示例 5

附录 B（资料性） 新建政务信息系统零信任网络安全应用示例 9

附录 C（资料性） 政务信息系统零信任网络安全体系参考架构 14

参考文献 18

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、山东省标准化研究院、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、深信服科技股份有限公司、中孚安全技术有限公司、山东正中信息技术股份有限公司、道普信息技术有限公司、杭州安恒信息技术股份有限公司、亚信科技（成都）有限公司、国家网络软件产品质量监督检验中心（济南）、浪潮云信息技术股份公司、北京网猿科技有限公司。

本文件主要起草人：王玮、李振、彭栋栋、党斌、王曙光、公伟、黄飞、刘振国、赵治刚、杨文宏、任强、于志波、李文昌、路坤、张燕、李广贝、徐猛、赵彬琦、刘鹏博、刘德莉、王明玺、魏丽丽、李玉婷、宋红涛、孟宪勇、张光坦、陈福康。

引 言

2022年6月，国务院下发《关于加强数字政府建设的指导意见》（国发〔2022〕14号），提出构建数字政府全方位安全保障体系，其中包括提升安全保障能力、建立健全动态监控、主动防御、协同响应的数字政府安全技术保障体系。

为更好保障济南市政务信息系统网络安全，有必要在各部门、各区（县）政务信息系统建设运营中借鉴零信任技术，加强政务信息系统零信任网络安全体系建设。本文件主要为济南市各部门、各区（县）在政务信息系统网络安全建设及运营过程中应用零信任提供规范和指导。

政务信息系统 零信任网络安全应用要求

1 范围

本文件规定了政务信息系统零信任网络安全应用总体原则、应用要求和管理要求。
本文件适用于政务信息系统零信任网络安全建设和运维管理。

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 22239 信息安全技术 网络安全等级保护基本要求
GB/T 25069 信息安全技术 术语
GB/T 28827.1 信息技术服务 运行维护 第1部分：通用要求
GB/T 35282 信息安全技术 电子政务移动办公系统安全技术规范
GB/T 36626 信息安全技术 信息系统安全运维管理指南
GB/T 40692 政务信息系统定义和范围

3 术语和定义

GB/T 25069、GB/T 40692界定的术语和定义适用于本文件。

4 缩略语

以下缩略语适用于本文件。

API：应用程序接口（Application Program Interface）
DDos：分布式拒绝服务（Distributed Denial of Service）
DGA：域名生成算法（Domain Generate Algorithm）
H5：第5代超文本标记语言（Fifth Hyper Text Markup Language）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
HTTPS：基于安全嵌套层的超文本传输协议（Hyper Text Transfer Protocol over Secure Socket Layer）
PHP：超文本预处理器（Hypertext Preprocessor）
SDK：软件开发工具包（Software Development Kit）
SDP：软件定义边界（Software Defined Perimeter）
SLB：服务器负载均衡（Server Load Balancing）
SQL：结构化查询语言（Structured Query Language）
SSL：安全嵌套层（Secure Sockets Layer）
TCP：传输控制协议（Transmission Control Protocol）
UDP：用户数据报协议（User Datagram Protocol）

WIFI：无线网络（Wireless Fidelity）

5 总体原则

政务信息系统零信任网络安全应用应遵循以下原则：

- a) 最小特权原则：用户和设备仅能获得必要的访问权限，以最大程度地减少攻击面，提高网络安全的可靠性；
- b) 动态访问控制原则：建立基于环境评估的动态访问控制策略，结合网络环境、用户行为、终端环境等因素持续评估访问主体，根据评估结果对访问主体进行动态授权；
- c) 实时监控和响应原则：对网络流量和安全事件进行实时监控和响应，发现问题立即处理，防止恶意攻击扩散；
- d) 多层次验证和审批原则：主体访问时，应进行多重身份验证和授权审批，以保证访问的合法性和安全性；
- e) 应用与数据分离原则：对政务信息系统前端应用和后端数据进行分层解耦，实现政务信息系统分层授权和可信访问控制；
- f) 日志留存原则：记录并保存零信任网络安全应用的行为，如访问主体和访问客体对应的访问、策略下发、策略执行，以及涉及的敏感行为等。

6 零信任网络安全应用要求

6.1 已建政务信息系统

6.1.1 工作流程

已建政务信息系统零信任网络安全应用应包括网络安全能力梳理、政务信息系统改造和网络安全应用验证测试等环节，工作流程如图1所示。已建政务信息系统零信任网络安全应用示例见附录A。

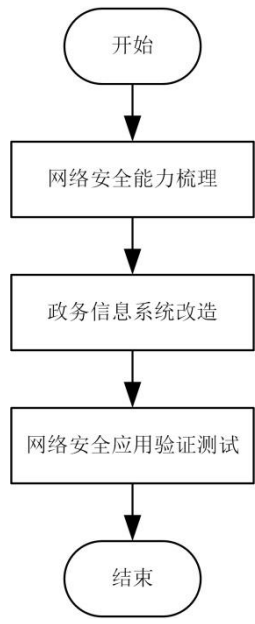


图1 已建政务信息系统零信任网络安全应用工作流程

6.1.2 网络安全能力梳理

应对政务信息系统当前的网络安全能力进行梳理，包括但不限于以下内容：

- a) 用户、设备、数据和应用清单；
- b) 用户和政务信息系统及不同政务信息系统间的访问关系；
- c) 用户和政务信息系统及不同政务信息系统间的访问权限。

6.1.3 政务信息系统改造

政务信息系统改造应遵循以下内容：

- a) 对用户和政务信息系统及不同政务信息系统间的访问关系进行统一管理；
- b) 对用户和政务信息系统及不同政务信息系统间的访问权限进行统一管理；
- c) 政务信息系统中的每项服务具备认证、授权和鉴权能力；
- d) 可将政务信息系统与身份管理系统进行集成，并建立多种认证机制。

6.1.4 网络安全应用验证测试

政务信息系统零信任网络安全应用验证测试应遵循以下内容：

- a) 制定验证测试方案和测试用例，详细记录测试数据，形成测试报告；
- b) 指定或授权专门的部门负责验收；
- c) 组织相关部门和人员对验证测试报告进行复核。

6.1.5 应用要求

政务信息系统零信任网络安全应用要求包括但不限于：

- a) 根据网络安全能力梳理情况，制定零信任网络安全建设方案，并通过专家评审；
- b) 系统验证测试通过后，进行系统上线运行，开展相关人员的培训，提交系统建设过程文档及系统运行维护文档；
- c) 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，动态调整访问主体对资源的访问权限，确保访问主体可信；
- d) 对不满足改造条件的政务信息系统，按照 GB/T 22239 要求进行安全加固。

6.2 新建政务信息系统

6.2.1 工作流程

新建政务信息系统零信任网络安全应用应包括政务信息系统设计开发、政务信息系统验证测试和政务信息系统上线等环节，工作流程如图2所示。新建政务信息系统零信任网络安全应用示例见附录B。

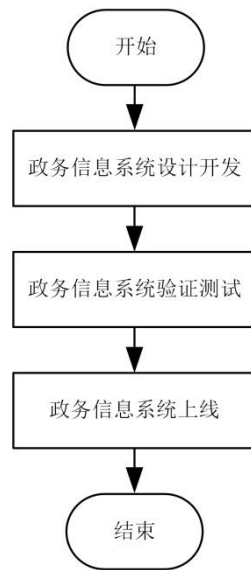


图2 新建政务信息系统零信任网络安全应用工作流程

6.2.2 政务信息系统设计开发

政务信息系统设计开发应遵循以下内容：

- a) 根据零信任网络安全体系参考架构（见附录 C），进行政务信息系统设计开发；
- b) 宜使用云资源提供的零信任网络安全服务。

6.2.3 政务信息系统验证测试

见6.1.4。

6.2.4 应用要求

政务信息系统零信任网络安全应用要求如下：

- a) 零信任网络安全应用与政务信息系统同步规划、同步建设、同步使用；
- b) 系统验证测试通过后，进行系统上线运行，开展相关人员的培训，提交系统建设过程文档及系统运行维护文档；
- c) 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，动态调整访问主体对资源的访问权限，确保访问主体可信。

7 网络安全应用管理要求

政务信息系统网络安全应用管理应满足以下要求：

- a) 符合 GB/T 36626、GB/T 28827.1 的相关规定；
- b) 制定政务信息系统运维策略，并定期评估；
- c) 为政务信息系统运维定义和分配相关角色和职责；
- d) 对运维人员身份进行认证，定期检查运维人员访问权限；
- e) 采用运维服务外包的，明确外包运维范围、工作职责等内容；
- f) 加强安全风险管控，制定突发事件应急预案，规范处置流程，定期组织应急培训及应急演练。

附 录 A

(资料性)

已建政务信息系统零信任网络安全应用示例

A.1 项目背景

为贯彻《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号），某市公积金管理中心（以下简称管理中心）在信创云的基础上，全面推进住房公积金数字化转型，将数字技术广泛应用于住房公积金管理服务，助推经济社会快速发展。住房公积金系统属于关键基础设施且涉及大量敏感信息，为保障数字化转型的顺利实施，需要推动网络安全与信息化一体化规划、一体化建设、一体化使用，全方位筑牢网络安全工作体系。

A.1.1 现状分析

管理中心整体业务架构见图A.1。

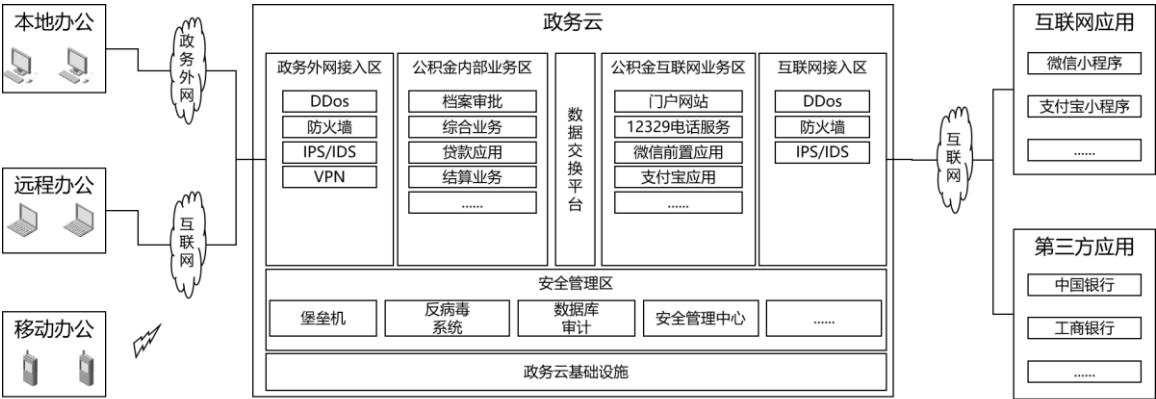


图 A.1 业务架构

管理中心的所有业务均部署在信创政务云上，核心业务包括内部业务和互联网业务，分别部署在政务云的内部业务区和互联网业务区。两个区之间逻辑隔离，通过数据交换平台进行数据交换。内部办公人员可以访问内部业务区的业务，在本地办公时可以通过政务外网直接访问，远程办公或移动办公时，需要通过政务外网接入区的VPN进行访问。第三方（主要是银行等金融机构）和互联网应用（比如微信和支付宝）只能访问互联网区的业务，通过互联网接入区进行访问。

管理中心在安全防护方面还是采用传统的基于网络的防护手段，已无法满足日益复杂的安全环境，面临的主要风险包括：一是对于内部人员窃密以及单点突破后的横向攻击缺乏有效的防护手段；二是互联网业务暴露在公网，针对DDos攻击、权限控制以及越权访问等难以防范；三是办公终端和移动终端普遍存在一机两用现象，既能访问互联网又能访问政务外网，导致失泄密安全风险。

A.1.2 需求分析

为保证管理中心内外部业务的安全稳定运行，基于零信任构建网络安全体系，需在以下几个方面加强安全防护：

- 强化应用身份鉴别。每个合法用户或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人或应用才能访问中心业务；
- 业务隐身。通过代理网关将互联网业务进行隐藏，只对具有合法身份的人或应用可见；
- 精细化动态访问控制。采用白名单策略，默认最小授权原则，给各个用户或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；
- 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；
- 部署终端安全沙箱。终端安全沙箱将终端隔离成不同的工作区，其中只有工作区才能访问政务外网业务，有效规避终端一机两用带来的数据失泄密风险。

A.2 解决方案

A.2.1 总体架构

基于零信任参考架构，整个管理中心的网络安全体系总体框架见图A.2所示。

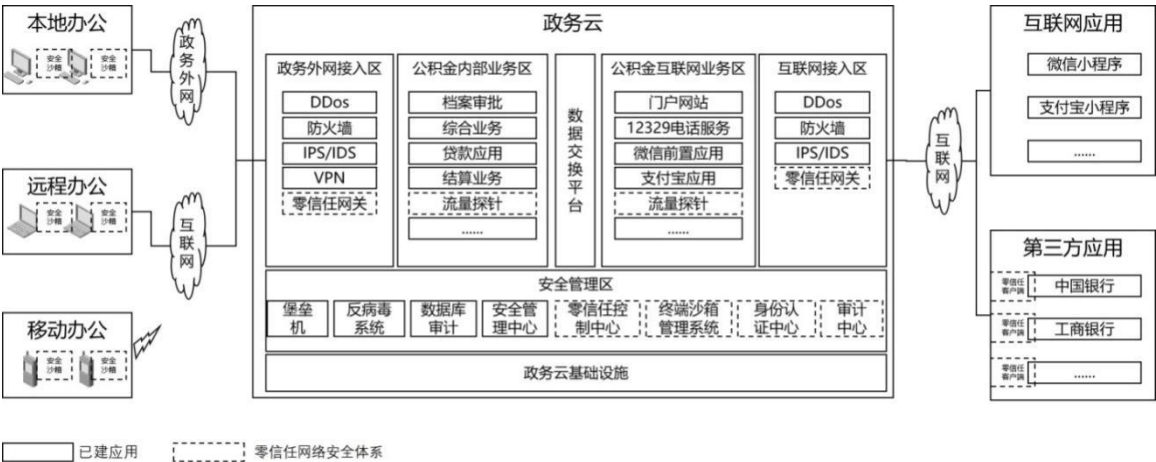


图 A.2 零信任网络安全体系总体框架

零信任网络安全体系包括身份认证中心、零信任控制中心、零信任网关、流量探针、终端安全沙箱和零信任客户端。

- 身份认证中心。身份认证中心是整个零信任网络安全体系的基石，通过为所有用户和应用建立了统一的身份认证机制，既强化了身份认证的安全性，又方便了认证过程。
- 零信任控制中心。零信任控制中心是整个网络安全体系的大脑，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。
- 零信任网关。零信任网关分别部署在内部业务和互联网业务前面，对业务系统进行安全防护，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，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。其中互联网业务区的网关还具备业务隐身功能，可有效避免 DDos 攻击和各种非法入侵。
- 流量探针。流量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。

- e) 终端安全沙箱。终端安全沙箱部署在每个需要访问内部业务的办公终端上，将办公终端隔离成两个工作区，一个是办公区，用于访问政务外网相关业务，一个是生活区，可以访问互联网。两个区之间实现了存储隔离、网络隔离和会话隔离，很好地规避了终端的失泄密风险。
- f) 零信任客户端。零信任客户端部署在应用侧，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。

A.2.2 总体部署

整个管理中心的零信任网络安全体系部署情况见图A.3所示。

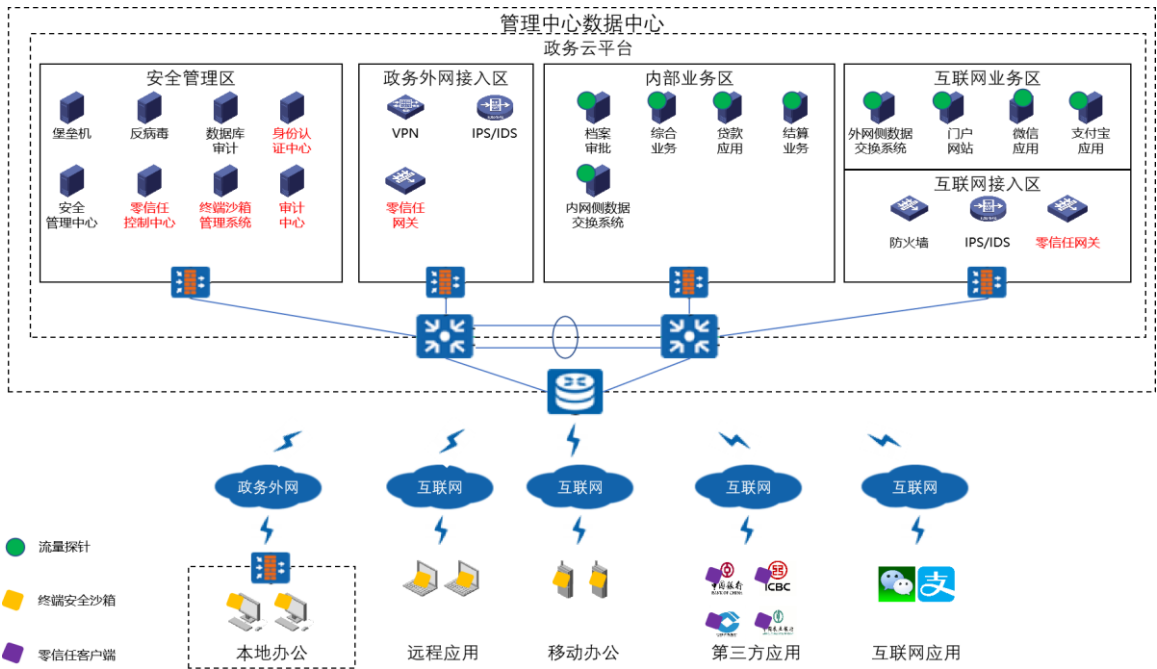


图 A.3 零信任网络安全体系部署

身份认证中心、零信任控制中心、审计中心以及终端沙箱管理系统部署在安全管理区，零信任网关分别部署在内部业务区和互联网业务区对各个关键业务进行隐身和安全防护。每个核心业务服务端都部署有流量探针，实时采集用户或应用的访问行为并上报审计中心。各类终端要想访问内部业务都需要安装终端安全沙箱，否则无法访问。第三方应用需要安装零信任客户端代理，才能访问互联网业务。用户使用互联网应用经过身份认证后可直接访问互联网业务。

A.3 效益分析

通过构建零信任网络安全体系，对管理中心业务系统进行安全加固，收到如下效果：

- 提高了管理中心整体安全性。基于零信任构建的网络安全体系，通过对所有用户和应用实施身份认证和鉴权，有效避免了非法侵入。通过终端安全沙箱有效规避了终端失泄密的风险。通过应用隐藏，规避了遭受DDoS攻击和非法入侵等风险。通过实时的用户行为分析和动态信用评估，及时发现和应对非法入侵、勒索等安全风险。总的来说，从端、网、云各个层次强化了整个管理中心的安全性。
- 提升了管理中心的整体运行效率。基于零信任构建的网络安全体系，以身份认证为基石，在强化安全认证的同时方便了认证流程，从而提升了业务访问效率。此外，通过提高整体安全

性，减少了安全事件对管理中心各类业务运行的影响，减少了因安全问题而导致的业务中断或数据丢失，保障整个管理中心办公流程顺畅、高效地运行。

附 录 B
(资料性)
新建政务信息系统零信任网络安全应用示例

B.1 概述

“山东通”安全接入平台（见图B.1）是全省推出的一套解决智能终端办公的安全解决方案，旨在解决全省在移动信息化建设过程中，面临的多样化终端设备、多样化移动应用接入所带来的信息、数据安全问题，如图I.1所示。

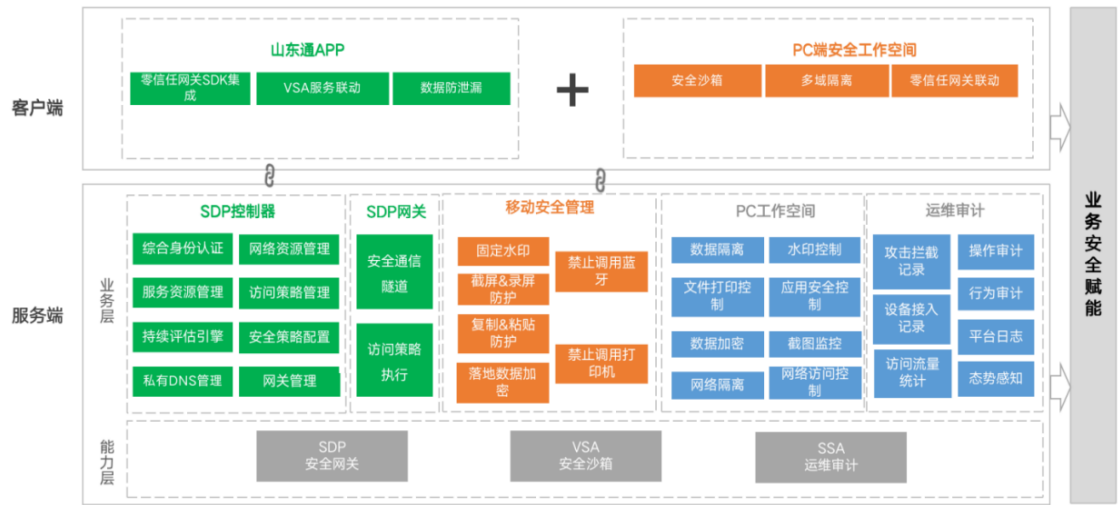


图 B.1 “山东通”安全接入平台架构

“山东通”安全接入平台提供了端、网、云一体化安全防护能力，构建起统一的应用安全保障平台。平台由三大核心赋能功能组成，包括业务应用安全赋能、网络传输安全赋能和“安全沙箱”技术赋能。

B.2 整体架构设计

“山东通”安全接入平台整体架构设计主要包括：

- a) 业务应用安全赋能。业务应用安全赋能是通过安全沙箱技术手段，与安全沙箱服务联动对移动应用进行重新封装并赋予其额外能力的过程。其实现原理是移动端使用 HOOK 技术，基于服务端的安全设置对可能造成数据泄密的操作进行拦截，防止敏感数据的泄漏。可赋能能力包括防截屏、防录屏、防复制粘贴、应用水印、数据加密等。
- b) 网络传输安全赋能。“山东通”安全接入平台赋能应用准入能力，减少自身互联网暴露面，通过与 SDP-SDK 集成赋能安全接入能力（如信道加密、应用准入、应用校验）。该平台是一种基于零信任模型、以基于身份的细粒度访问代替广泛的安全接入平台，为用户提供安全可靠的访问业务系统方案。
- c) “安全沙箱”技术赋能。PC 安全工作空间通过领先的“安全沙箱”技术为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台计算机上，同时建立多个逻辑隔离空间（如互联网安全空间、普通业务区安全空间、涉密区安全空间）。在每个安全空间中可进行不同

的网络访问，安全空间内的操作通过应用的安全策略得到控制，安全空间中数据在个人桌面无法访问和读取。

“山东通”安全接入平台以零信任终端为边界，结合零信任代理网关建立起一块逻辑安全域，同时结合零信任代理网关基于端口动态授权的网络隐身技术构建起一张隐形的网络，即网络应用只对“特定的用户+特定的设备”可见，对其他人完全不可见，并且该用户访问应用的行为可以进行严格控制和记录。这种模式很好地解决了移动办公、上云带来的系统暴露面过多的问题，同时也可增强现有政务外网办公的安全性。应用接入“山东通”安全接入平台的流程（见图B.2）如下：

- a) 零信任终端登录鉴权并上报设备环境信息；
- b) 零信任控制中心判断接入身份合法性。身份非法无响应；身份合法回应零信任终端；
- c) 零信任控制中心下发访问策略和安全策略；
- d) 零信任终端和零信任代理网关建立加密隧道；
- e) 零信任终端定时上报设备、网络等环境信息，零信任控制中心动态评估，调整信任等级，变更访问策略。

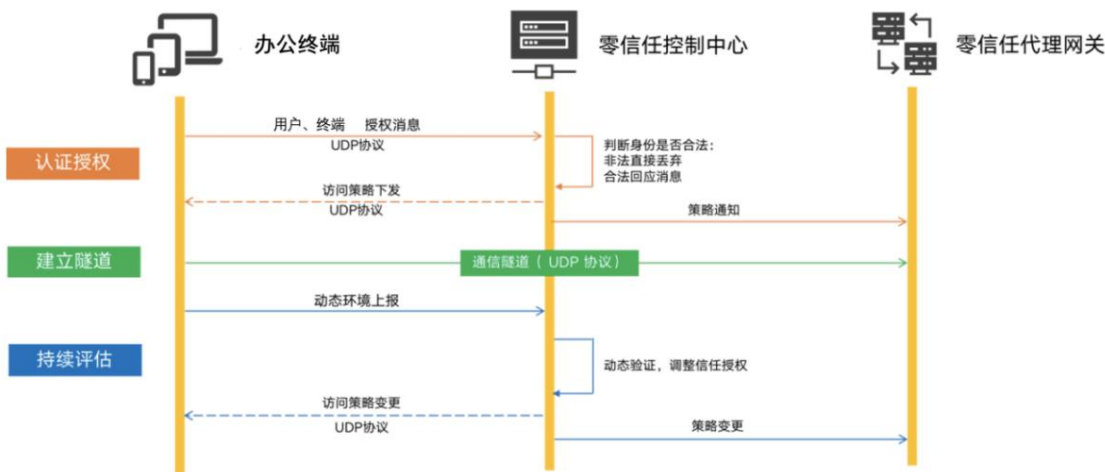


图 B.2 应用接入流程

B.3 业务安全设计

可信认证根据“零信任”的安全框架，零信任应用数据安全及接入代理服务网关控制中心对包括用户、设备、网络、时间、位置等多因素的身份信息进行验证，确认身份的可信度和可靠性。在默认不可信的前提下，只有全部身份信息符合安全要求，才能认证通过，客户端才能与安全网关建立加密的隧道连接，由安全网关代理可访问的服务。针对异地登录、新设备登录的等风险行为，系统将追加二次验证，防止账号信息泄露而导致的内网入侵。

B.4 应用安全设计

B.4.1 应用安全封装与发布

“山东通”安全接入平台建设，除了主应用“山东通”的搭建外，还包含大量政务办公或部门业务的H5应用。平台以“山东通”为统一入口，H5应用通过进入“山东通”后进行跳转。

为了对主应用以及其余大量H5应用进行统一加固与防护，确保相关应用均需要通过严格身份评估才可接入访问，同时受到APP沙箱或桌面沙箱保护，故需要对所有应用分别进行安全加固改造。

考虑应用更新频率、业务上线要求以及应用二次开发难易程度，此次规划将主应用使用SDK进行代码封装，H5应用通过零信任控制平台建立SDP隧道进行访问。

零信任安全厂商提供SDK代码包，由软件开发将代码集成到“山东通”APP中，集成后软件的更新、大版本的迭代均不会影响零信任接入能力，实现“一次SDK代码封装，业务应用始终体验零信任能力”的安全接入。

B.4.2 H5应用对接安全

基于代理网关提供的“山东通”服务端的全生命周期管理服务，为H5应用提供身份鉴权、过载保护、异常响应等能力。

B.4.3 支持HTTPS

移动端和PC端接入服务端的协议宜支持HTTP与HTTPS协议。

B.4.4 访问鉴权流程

所有从客户端发起的请求，代理网关会将流量截获，自动进入身份认证过程，认证后将请求转发至站点的服务端。

B.5 最小化授权

当用户行为或环境发生变化时，零信任代理网关会持续监视上下文，基于位置、时间、安全状态和一些自定义属性实施访问控制管理。通过用户身份、终端类型、设备属性、接入方式、接入位置、接入时间来感知用户的访问上下文行为，并动态调整用户信任级别。

对用户需要设定其最小业务集及最大业务集，对于每次访问，基于用户属性、职务、业务组、操作系统安全等进行安全等级评估，按照其安全等级，动态调整开放对应的业务系统访问权限。

B.6 业务服务隐身

SDP零信任应用数据安全及接入安全服务认证采用基于UDP协议的认证机制，默认“拒绝一切”请求，仅在接收到合法认证数据包的情况下，对用户身份进行认证。认证通过后，接入终端和网关之间建立基于UDP协议的加密隧道。UDP协议和加密隧道协议技术实现对外关闭所有的TCP端口，保证了潜在的网络攻击者嗅探不到SDP零信任应用安全接入平台的端口，无法对网关进行扫描，预防网络攻击行为，有效地减少互联网暴露面。

B.7 WEB 服务防护

WEB应用作为政务业务系统重要的实现方式，让其逐渐成为互联网攻击中的主要目标，安全事件频繁发生。该平台提供应用层的安全防护，执行一系列HTTP、HTTPS的安全策略，针对来自WEB应用程序客户端的各类请求进行内容检测和验证，有效防御应用层的XSS攻击、PHP攻击、远程命令执行、SQL注入、本地/远程文件注入、SESSION攻击等7层网络攻击，确保其安全性与合法性，对非法的请求予以实时阻断/记录，从而对政务各类WEB应用进行有效安全防护。

B.8 应用数据安全设计

B.8.1 概述

PC安全工作空间通过领先的“安全沙箱”技术为不同区域的网络访问提供了安全的逻辑隔离方法，使用户能够在一台计算机上，同时建立多个逻辑隔离空间（如互联网安全空间、普通业务区安全空间、

涉密区安全空间），在每个安全空间中可进行不同的网络访问，安全空间内的操作通过应用的安全策略得到控制，安全空间中数据全程在个人桌面无法访问和读取。

工作空间解决方案可有效阻止病毒、木马对政务外网的攻击，防止政府机密数据有意泄漏（如外接设备、截录屏、URL二次跳转、文件打印）和无意的泄漏（如病毒侵入、木马攻击、未锁屏）。

B.8.2 数据隔离

用户在日常使用电脑时产生的数据是最敏感的资源，也是需要重点保护的對象。数据隔离最主要的目标就是空间内的数据文件。工作空间和基于虚拟机的重量级的方案不同，不需要为不同的空间安装操作系统和应用二进制文件，而是在运行过程中尽量利用系统已有的文件，同时把用户实际产生的数据，按照“写时拷贝”的原则，由重定向引擎将数据文件重定向到安全加密的虚拟磁盘中，实现了数据文件的隔离。

安全空间可通过挂钩剪贴板操作，在发生粘贴相关的API调用时，判断数据的来源，根据安全策略判断是否允许操作，从而返回不同的结果，这样就实现了对于拷贝粘贴的数据隔离和流动控制。

更进一步，重定向引擎可支持多实例化机制，保证不同空间内操作的数据保存在不同的工作空间中，达到了更深层次的数据隔离目的。

B.8.3 数据加密

文件在沙箱内落地后，如何防止被泄露，加密是有效的手段。PC安全工作空间针对磁盘使用透明加解密技术，可支持AES等多种加密算法。

B.8.4 应用控制

应用控制可实现对于工作空间内运行应用的精确控制，工作空间的控制程序在工作空间启动或者活动过程中，可设置指定的工作空间内允许运行的应用以及时间范围。

工作空间管理驱动注册了系统进程创建的回调函数，在回调函数里，判断相关的应用是否可在沙箱里运行，从而实现了进程控制的功能。

当应用特征匹配时，允许应用运行，这样在保证安全性的同时，也提高了应用程序运行的平滑，保证用户使用过程不会被打断。

B.8.5 网络拦截

传统的系统防火墙可实现基于进程名或者基于包特征的过滤，而工作空间则希望空间内的应用可访问政务外网系统或拦截互联网访问动作，而对于空间外的应用，则不允许访问政务外网系统。

B.8.6 水印技术

根据工作空间的策略，策略控制模块会截获工作空间应用窗口的创建过程，按需给工作空间应用窗口建立对应的透明窗口并添加水印，并屏幕上显示。

通过添加水印的方式保护沙箱内应用窗口数据安全，防止信息泄露。

B.8.7 截图监控

相对于文件和网络等方式，通过截图造成的信息泄露虽然较弱，但在政务外网环境下，仍然希望对其进行一定的控制和审计。策略控制模块通过挂钩实现截图功能的关键API，结合发起应用程序的其他特征，有效地判断截图行为。在截图数据返回给截图应用的时候，根据配置的策略，可将应用窗口涂黑或添加水印，并主动上报服务端进行审计。

B.8.8 文档安全设计

终端用户使用沙箱办公，有跨空间拷贝文本的诉求，在剪切板以及文件导入导出的过程中需要相应的技术手段实现权限控制或者全面的审计回溯手段。

剪切板拷贝审计，用户在文档或网页复制文本内容，此时拷贝工具会自动捕获用户复制的文本内容（纯文本格式，保留换行、段落信息），当用户在拷贝工具中点击“复制”按钮时，客户端将剪切板拷贝行为日志及拷贝内容上报到代理网关（代理网关转发给外置日志中心），在审计日志上报成功后，用户可切换至个人空间拷贝剪切板内容，而上报至外置数据中心的剪切板拷贝行为日志则形成日志列表供管理员审计追溯。

文件导入导出审计，用户在进行文件导入导出时，客户端将文件导入或导出行为日志上报到代理网关（代理网关转发给外置数据中心），在上报成功后才允许用户进行下一步的文件导入导出操作，而上报至外置数据中心的文件导入导出行为日志则形成日志列表供管理员审计追溯。

附 录 C
(资料性)

政务信息系统零信任网络安全体系参考架构

C.1 参考架构

政务信息系统零信任网络安全体系参考架构（如图C.1所示）主要包括访问主体、零信任控制中心和政务云上的访问客体。其中零信任控制中心包括环境感知、信任评估、策略管理、策略执行等4个模块。

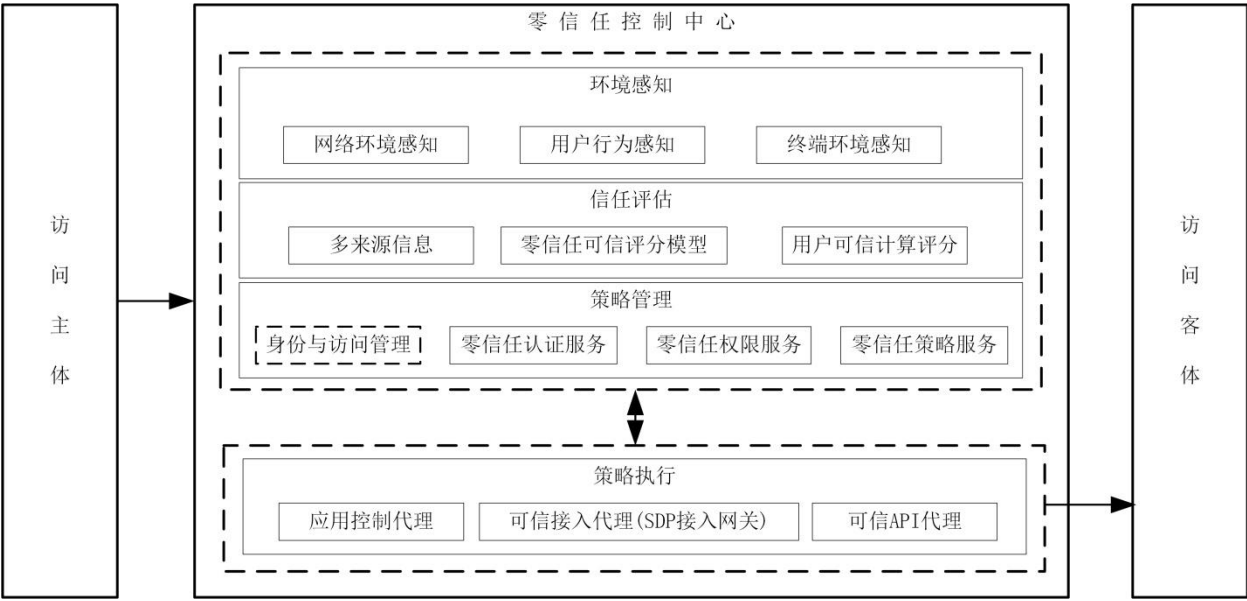


图 C.1 政务信息系统零信任网络安全体系参考架构

C.2 环境感知

环境感知包括网络环境感知、用户行为感知、终端环境感知，其由环境感知终端及环境感知代理两部分组成，环境感知代理负责接收环境感知终端采集的网络、用户行为、终端等事件，并实时上报信任评估模块。

环境感知宜实现以下功能及要求：

- a) 环境感知终端实时上报终端各类事件；
- b) 向访问终端实时动态下发环境感知策略，当终端触发相关策略时，终端上报对应事件；
- c) 获取到访问终端上报的各类事件后，形成日志上报给信任评估模块进行用户可信评分；
- d) 环境感知模块支持用户行为、终端环境、网络环境等 3 种环境感知，相关感知能力可包括：
 - 1) 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感知能力；
 - 2) 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环境检测能力；
 - 3) 连接风险 WIFI 检测、命令注入攻击检测、SQL 注入攻击检测、恶意加密流量检测、DGA 域名请求等网络环境感知能力。

C.3 信任评估

信任评估根据风险感知上报的环境感知信息以及日志服务器收集的鉴权日志、认证日志等基于零信任可信评分模型为用户计算可信评分，并将评分结果上报零信任权限服务。

信任评估宜实现以下功能及要求：

- a) 具备可信评分计算能力，接收上报的各类事件、认证服务发送的认证日志及零信任权限服务发送的鉴权日志，基于零信任可信评分模型计算用户可信分，对用户进行安全评级；
- b) 信任评估与零信任权限服务联动，当用户的安全等级变更时，向零信任权限服务下发变更信息；
- c) 支持日志检索与审计；
- d) 记录用户的历史评分以及资产信息。

C.4 策略管理

C.4.1 概述

策略管理主要包括零信任认证服务、零信任权限服务和零信任策略服务。

C.4.2 零信任认证服务

零信任认证服务用于用户零信任身份与用户业务身份之间的映射转换，当用户通过身份管理与访问控制的统一身份认证后，将通过认证的令牌发送至零信任认证服务，并以该令牌交换零信任专属令牌，作为访问业务的用户在零信任中的鉴权标识。

零信任认证服务宜实现以下功能及要求：

- a) 对接用户的统一身份认证信息；
- b) 建立统一身份认证令牌与零信任令牌的映射关系，维护零信任令牌表；
- c) 向信任评估模块发送用户认证日志。

C.4.3 零信任权限服务

零信任权限服务在零信任架构中实现鉴权功能，零信任权限服务定义策略执行点的动作、零信任用户的授权组、应用访问控制策略与用户可信评分的关联。零信任权限服务对接信任评估与零信任策略服务，下发应用访问控制策略至各策略执行点。

零信任权限服务宜实现以下功能及要求：

- a) 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访问应用或 API；
- b) 接收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) 支持基于零信任用户组设置访问控制策略；
- e) 支持基于用户业务需求自定义应用访问控制策略。

C.4.4 零信任策略服务

零信任策略服务与零信任权限服务、可信API代理、可信接入代理和应用控制代理对接，零信任策略服务接收可信接入代理的鉴权请求后，与零信任权限服务核对用户的鉴权信息，将对应的访问控制策略下发至相应的可信接入代理、应用控制代理、可信API代理。

零信任策略服务宜实现以下功能及要求：

- a) 接收可信接入代理和可信 API 代理的鉴权请求并转发给零信任权限服务；

- b) 支持与零信任权限服务对接，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可信接入代理、应用控制代理、可信 API 代理；
- 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) 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。

C.5 策略执行

C.5.1 概述

策略执行包括应用控制代理、可信接入代理、可信API代理三类策略执行点。

C.5.2 应用控制代理

应用控制代理负责在政务信息系统访问终端对应用功能进行访问控制，在零信任策略管理中定义应用控制代理的访问控制策略。当用户评分触发阈值时，由零信任策略管理下发相关策略至应用控制代理，对政务信息系统访问终端的功能进行限制。

应用控制代理功能宜符合以下要求：

- a) 支持接收零信任策略管理下发的应用访问控制策略；
- b) 支持根据访问控制策略限制政务信息系统访问终端的相关功能；
- c) 支持根据政务信息系统访问终端自定义限制动作；
- d) 支持对政务信息系统访问终端上小程序的入口限制；
- e) 支持对政务信息系统访问终端的功能入口限制。

C.5.3 可信接入代理

可信接入代理负责代理政务信息系统访问终端到服务端的访问，并向零信任策略管理查询每一个访问用户的鉴权信息。

可信接入代理功能宜符合以下要求：

- a) 可信接入代理支持上传证书及 SLB 负载均衡，对接零信任策略管理；
- b) 对接零信任策略管理并对用户进行认证和鉴权。用户首次访问应用，请求报文转发至可信接入代理，如果可信接入代理检查到请求报文中没有用户令牌，则将请求报文重定向到认证页面；
- c) 提供 SSL 卸载，用户使用 HTTPS 方式访问应用前端时，配置 SSL 卸载配置文件用于解密 HTTPS 报文；
- d) 提供虚拟服务，用户通过可信接入代理的虚拟服务访问政务信息系统和认证页面。

C.5.4 可信API代理

可信API代理实现政务信息系统前后置分离的访问控制功能，当政务信息系统（前置）调用政务信息系统（后置）的API接口及数据时，需通过可信API代理对政务信息系统（后置）的访问再次鉴权，以保障政务信息系统（后置）数据、API接口等的安全性。

可信API代理功能宜符合以下要求：

- a) 可信 API 代理向零信任策略管理发送鉴权请求；
- b) 根据零信任策略管理返回的鉴权结果判断用户是否具备对 API、数据的访问权限；

- c) 针对有权限的用户则将相关请求转发至政务信息系统（后置），否则拒绝该请求。

参 考 文 献

- [1] 《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）
 - [2] GA/DSJ 351—2020 公安大数据安全 零信任体系技术设计要求
-