ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 零信任参考体系架构

Information security technology—Zero trust reference architecture

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本稿完成时间：2022 年 6 月 1 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　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专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：奇安信网神信息技术（北京）股份有限公司、中国信息通信研究院、中国科学院软件研究所、中国科学院大学、国家计算机网络应急技术处理协调中心、中国科学技术大学、飞天诚信科技股份有限公司、国家信息技术安全研究中心、中国科学院信息工程研究所、北京天融信网络安全技术有限公司、公安部第三研究所、北京数字认证股份有限公司、江苏易安联网络技术有限公司、国民认证科技（北京）有限公司、启明星辰信息技术集团股份有限公司、深圳竹云科技股份有限公司、格尔软件股份有限公司、海信集团控股股份有限公司、大唐高鸿信安（浙江）信息科技有限公司、北京奇虎科技有限公司、上海派拉软件股份有限公司、杭州安恒信息技术股份有限公司、上海观安信息技术股份有限公司、国网区块链科技（北京）有限公司、兴唐通信科技有限公司、厦门市美亚柏科信息股份有限公司、北京百度网讯科技有限公司、北京远鉴信息技术有限公司、国家工业信息安全发展研究中心、中国信息安全测评中心、国家信息中心、公安部第一研究所、成都卫士通信息产业股份有限公司、中能融合智慧科技有限公司、北京信安世纪科技股份有限公司、长春吉大正元信息技术股份有限公司、中国科学院数据与通信保护研究教育中心、中国移动通信集团公司、深圳市腾讯计算机系统有限公司、北京协和医院、新华三技术有限公司、北京芯盾时代科技有限公司、北京神州绿盟科技有限公司、杭州海康威视数字技术股份有限公司、华为技术有限公司、云从科技集团股份有限公司、深信服科技股份有限公司、北京安博通科技股份有限公司。

本文件主要起草人：齐向东、吴云坤、张彬、刘勇、张泽洲、安锦程、荆继武、詹榜华、李新友、张立武、左晓栋、邬怡、韩永刚、孟楠、赵泰、张严、刘丽敏、郭莉、陈亮、朱鹏飞、陆舟、王哲麟、李海玲、姚叶鹏、韩冬旭、刘治平、王龑、陈妍、刘占斌、夏冰冰、秦益飞、杨正权、李俊、韩少波、蒋蓉生、王文路、戴立伟、郑强、高雪松、何晨迪、郑驰、梅宗林，张睿、茆正华、黄铭恺、谢江、杨珂、蔡子凡、许雪姣、程长高、朱红星、郑榕、孙岩、孙明亮、国强、黄卉、苏智睿、汪仕兵、周开宇、李海宁、焦靖伟、索瑞军、李敏、于乐、赵蓓、蔡东赟、孟晓阳、万晓兰、尹晓东、鲁暄、陈加栋、王雨晨、李军、訾然、种竹。

信息安全技术 零信任参考体系架构

1 范围

本文件给出了零信任参考体系架构，包括组件及组件之间的关系。

本文件适用于采用零信任参考体系架构的信息系统的规划、设计、开发、应用。

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 25069—2022 信息安全技术 术语

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

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

零信任 zero trust；ZT

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。

3.2

零信任参考体系架构 zero trust reference architecture

依据零信任建立的参考体系架构，遵守最小权限原则，采用多属性动态访问策略，实现主体对资源的端到端访问控制。

3.3

资源 resource

系统中可供访问的客体，例如：应用、系统、接口、服务、数据等。

3.4

控制层 control layer

控制和管理在主体到资源之间建立、维持或阻断数据访问信道的抽象层。

注：零信任参考体系架构采用分层架构，隔离控制策略和数据。

3.5

数据层 data layer

在控制层的控制下，实施主体和资源之间数据传输的抽象层。

4 缩略语

下列缩略语适用于本文件。

PKI：公钥基础设施（Public Key Infrastructure）

URL：统一资源定位符（Uniform Resource Locator）

5 概述

零信任访问模型描述零信任参考体系架构下的主体访问资源过程，见图1。通过持续环境感知、动态信任评估、最小权限访问的循环过程，进行零信任策略决定与执行，实现对资源的访问保护；同时，主体和资源之间的传输需要加密。

图1 零信任访问模型

零信任访问模型具有以下基本构成。

a) 持续环境感知：

持续对主体环境、资源环境、网络环境等进行数据采集，感知安全威胁、脆弱性等安全态势。

注1：尽可能多地采集主体对资源访问过程中所有参与对象的信息，例如：通过设备管理系统采集和感知主体运行环境的硬件、操作系统、软件配置、安全配置等信息；通过态势感知系统采集和感知网络环境和资源环境的安全态势信息等；通过采集身份管理、资源管理等组件的系统运行日志，感知主体对资源的访问行为信息等。

注2：在零信任策略执行过程产生的运行数据，通过身份管理系统/设备、设备管理系统/设备、资源管理系统/设备、态势感知系统/设备等最终汇集到零信任策略决定过程中。

b) 动态信任评估：

在主体访问资源之前，根据主体属性、资源属性、环境属性等进行信任评估，在访问过程中，根据属性变化进行动态信任评估，维持或改变策略决定。

注3：主体属性包括主体自然属性（例如：用户自然属性包括用户身份识别码、岗位、职务等）、主体身份权威属性（例如：属性权威机构颁发的属性证书、权威身份源等）、主体身份鉴别属性（包括身份鉴别方式、私有密钥、口令等鉴别相关数据）、主体访问行为属性（包括账户状态、历史访问行为等）等；资源属性包括资源分级分类属性（例如：数据敏感等级、资源归属分类等）、资源访问属性（包括资源共享、资源远程访问、资源访问接口、资源访问策略等）、资源存储属性（包括资源存储位置，例如云存储、本地存储等，资源存储模式，如直接存储、网络存储、集中存储等）等；环境属性包括主体环境属性（例如：主体地理位置、主体网络环境、主体计算环境、主体代码签名等）、资源环境属性（例如：资源物理位置、资源网络环境、资源计算环境、资源代码签名等）、安全态势（例如：终端安全态势、网络安全态势、资源安全态势等）、威胁情报（主体威胁情报、网络威胁情报、资源威胁情报等）等。

c) 最小权限访问：

根据业务需求和风险容忍度动态调整策略，对每次允许的访问请求主体授予最小权限，并保证及时执行调整后的最小权限。

注4：授予主体的最小权限包括完成访问请求任务所需最小范围、最低权限的资源。

注5：按照完成主体访问任务所需的最小范围，精准组合被访问资源。

注6：最低权限是指资源具有的可授予主体完成访问任务所需的最低权限级别。例如：数据资源具有分配给访问主体

的可见、可读取、可写入、可删除等从低到高的权限分级，应用服务资源具有分配给访问主体的可见、可执行等从低到高的权限分级。

注7：尽量缩短策略决定和执行的时间间隔。例如：在建立主体到应用系统资源访问连接的执行策略，缩短策略决定和执行的时间间隔。

d) 加密传输：

主体访问资源的通信都需要采用安全加密传输。

6 参考体系架构

6.1 组成

按照GB/T 18794.3—2003定义的通用访问控制框架，主体作为发起者、资源作为目标，由主体、资源、核心组件和支撑组件组成零信任参考体系架构，见图2。

核心组件由策略决定点和策略执行点组成，执行主体对资源的策略决定。

支撑组件由密码服务和应用、身份管理、设备管理、资源管理、态势感知组件组成，提供多来源信息、以及支撑主体、资源和核心组件运行的多种服务。

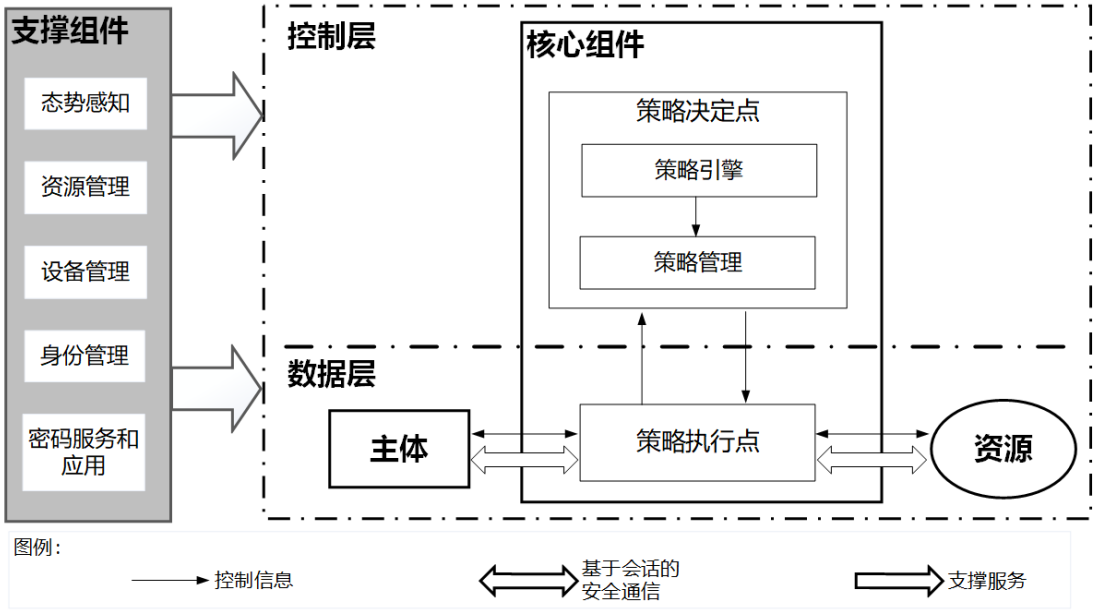


图2 零信任参考体系架构图

不确定数据传输所在网络环境的安全性，所有实现主体到资源之间数据传输的组件共同组成数据层，包括主体到资源之间的信道、网络设备、密码系统/设备等，在控制层的管理和控制下，采用密码技术建立、维持或阻断主体到资源的数据访问信道。

6.2 主体

主体是发起资源访问请求的用户、设备、软件应用、系统等对象。

主体可以是单一的用户、设备、软件应用、系统等，也可以是用户、设备、软件应用、系统等的组合。在进行主体属性评估和身份鉴别时，组合主体共同作为主体对象。

主体使用数字身份作为标识，关联主体的属性信息。

主体的属性包括：主体自然属性、主体身份权威属性、主体身份鉴别属性、主体访问行为属性、主体环境属性、主体安全状态、主体威胁情报等。

注1：典型的组合主体示例：用户、用户使用的设备和发起访问的软件应用（该软件应用安装在设备计算环境中）共同作为主体。

注2：主体数字身份是主体在网络中的虚拟身份标识，通过具有唯一性标识标记，关联主体相关的属性信息。数字身份定义参考[GB/T 31504-2015，定义3.6]。

注3：收集、获取、存储、共享主体信息遵守《GB/T 35273-2020 信息安全技术　个人信息安全规范》相关规定。

6.3　资源

资源是系统中可供访问的客体，包括：应用、系统、接口、服务、数据等。

基于资源属性，划分资源最小集合为同一资源单元，遵从共同安全策略并予以标识。例如：一个URL标识的应用系统是一个资源单元、一个URL标识的功能单元是一个资源单元、一个组件接口或者一个数据字段，都是一个资源单元。

资源单元具有与事先定义的访问对应的权限。例如，数据字段具有可用于分配给主体的读取、写入、执行和删除权限。

资源的属性包括：资源分级分类属性、资源访问属性、资源存储属性、资源环境属性、资源安全态势、资源威胁情报等。

注1：采用隔离、标识等技术手段进行资源单元划分，典型技术手段包括统一资源标识(URI)、数据标识、软件定义边界、微隔离等。

注2：举例说明划分最小资源集合，标识资源单元：应用系统的资源单元为可被访问的最小应用系统集，采用应用系统访问地址或URL予以标识，如一个应用系统；功能单元的资源单元为可被访问的最小功能单元集，采用URL标识，如可标识的直接访问功能单元；接口的资源单元为可被访问的最小组件接口集、移动开发接口集、应用编程接口集等，采用相应接口标识；数据资源单元为可被访问的最小数据库、数据表、数据记录、数据字段等。

6.4　核心组件

6.4.1　组成

核心组件由策略决定点和策略执行点组成，执行主体对资源的策略决定。

核心组件之间信息传递分为控制信息传递和基于会话的安全通信。

主体发起对资源的访问请求，策略执行点将访问请求信息传递到策略决定点，在支撑组件辅助下，策略决定点创建、更新、调整策略决定，并将策略决定实时传递到策略执行点。控制层传递访问请求信息、策略创建、策略更新、策略调整、策略执行等管理控制信息。

策略执行点在策略决定点的管理下，建立、维持或阻断主体到资源的数据访问信道，在数据层基于会话进行加密传输。

注：假设数据传输网络环境的安全性不确定，核心组件采用密码技术建立、维持或阻断主体到资源的数据访问信道。

6.4.2　策略决定点

6.4.2.1　组成

策略决定点由策略引擎子组件和策略管理子组件组成，基于控制层进行信息传递。

策略决定点接收支撑组件提供的多来源信息，持续进行环境感知。在接收到策略执行点转发的访问请求后，进行动态信任评估并控制执行策略决定。

策略决定点与其他组件的关系如下：

a)　策略决定点接收支撑组件提供的多来源信息，识别、提取、归纳主体属性信息、资源属性信息、环境属性信息、以及策略基准、策略规则等；

b)　策略决定点接收策略执行点转发的主体访问请求，控制策略执行点执行策略决定；

c） 策略决定点在支撑组件服务支撑下，对主体持续进行身份鉴别和身份鉴别动态调整，精细管理资源。

注：策略基准、策略规则可以由策略引擎接收支撑组件提供的多来源信息后生成，或者通过管理界面输入策略引擎。策略基准定义参考[GB/T 25069—2010，定义2.108]，策略规则定义参考[GB/T 25069—2010，定义2.107]。

6.4.2.2 策略引擎子组件

策略引擎子组件和策略管理子组件搭配使用，策略引擎子组件做出策略决定，并将策略决定发送到策略管理子组件。

策略引擎子组件应用信任算法，最终决定是否授予或拒绝特定主体对资源的访问权限。

策略引擎子组件在支撑组件提供的多来源信息支持下，持续进行环境感知，在收到访问请求后，进行信任评估、策略决定，确定拒绝或授予对被访问资源的访问权限。在授权主体对被访问资源访问期间，策略引擎子组件持续进行环境感知、信任评估以及策略决定，决定继续授予或撤销对被访问资源的访问权限。

策略引擎子组件进行策略创建、存储、更新、撤销，对策略全生命周期进行监控，负责策略评估审核和一致性检查，依据策略基准和策略规则，处理冲突策略和错误策略。

注1：策略是执行访问控制决策遵循的规则，由一组规则、一个规则组合算法标识和一组义务（可选）组成，是策略集的组成部分。策略定义参考[GB/T 25069—2010，定义2.104]。

注2：信任算法支撑策略引擎同意或拒绝主体对资源的访问。信任算法的输入包括访问请求、主体属性、资源属性、访问过程环境属性、威胁情报信息等，基于条件、分值或者上下文等因素，输出策略决定，并结合策略实施效果进行持续优化。

注3：策略引擎子组件自行判断支撑组件所提供信息的准确性和可靠性，包括但不限于采用数据安全处理技术，进行数据来源判别、数据清洗、数据汇聚、数据源标识等。

6.4.2.3 策略管理子组件

策略管理子组件和策略引擎子组件和搭配使用，按照策略引擎子组件发送的策略决定，采用动态会话管理，控制策略执行点执行策略决定。

策略管理子组件实时接收策略决定和策略调整。

策略管理子组件控制策略执行点建立、或阻断主体和资源之间的数据访问信道。

注：零信任策略管理组件不同于策略管理点（策略管理点定义参考[GB/T 30280—2013，定义3.20]），不能创建策略或策略集。

6.4.3 策略执行点

策略执行点在策略决定点管理下，实施身份鉴别，启动、监控和终止主体与资源之间的数据访问信道。

策略执行点对应于不同业务场景，形态和部署方式不同。

策略执行点与其他组件的关系如下：

a） 策略执行点接收来自主体的访问请求、并转发到策略决定点；

b） 策略执行点配合策略决定点，在辅助组件支撑下对主体实施身份鉴别；

c） 策略执行点配合策略决定点，在辅助组件支撑下管理被访问资源；

d） 策略执行点接收策略决定点输出策略和动态调整策略，按照策略决定，建立、维持或阻断主体和被授权资源的数据访问信道。

注：策略执行点作为一个逻辑组件，有多种实现方式，即可以分成两个组件：客户端组件（例如：客户端访问代理）和资源端组件（例如：资源侧的访问控制网关），也可以是单个门户组件。

6.5 支撑组件

6.5.1 组成

支撑组件由密码服务和应用、身份管理、设备管理、资源管理、态势感知子组件组成。

支撑组件提供多来源信息、以及支撑主体、资源和核心组件运行的多种服务。

身份管理子组件、设备管理子组件、资源管理子组件对主体和资源提供相应管理服务，配合核心组件作出策略决定，执行策略决定。支撑组件有多种组成和实现形式，密码服务和应用子组件、身份管理子组件、态势感知子组件所提供服务不可缺少。

支撑组件子组件各自遵循相关规范进行信息采集、提供对应服务，本标准不再对重复内容进行描述。

注1：支撑组件对于多来源信息的搜集和完善是持续的，信息的多来源、广覆盖影响策略决定的准确性。对于支撑组件提供信息的准确性和可靠性，需要核心组件在使用时进行甄别。

注2：支撑组件有多种实现形式。即可以由单个系统/设备提供单个子组件服务能力，例如：PKI系统/设备作为一个密码服务和应用子组件；也可以由单个系统/设备提供多个子组件服务能力，例如：云计算业务管理系统提供身份管理子组件、资源管理子组件和态势感知子组件服务能力；还可以由多个系统/设备提供单个子组件服务能力，例如：安全管理平台、终端管理系统等提供态势感知子组件服务能力。

6.5.2 密码服务和应用

密码服务和应用子组件提供身份权威属性信息。

密码服务和应用子组件提供密码相关服务，包括身份鉴别服务、标识管理服务、及其他密码相关服务，例如：感知信息传输安全保护，策略配置完整性保护，重要数据存储安全保护、应用软件来源真实性和完整性保护等。

注：PKI系统/设备、密码服务系统/设备作为密码服务和应用支撑组件。PKI系统或/设备可为人员、应用、系统等发布证书，作为标识权威机构，提供标识管理以及身份鉴别相关服务；密码服务系统/设备提供密码相关服务。

6.5.3 身份管理

身份管理子组件提供数字身份信息。包括主体自然属性信息、主体身份鉴别属性信息、主体访问行为属性信息等。

身份管理子组件提供数字身份信息服务等。

注1：数字身份信息是数字身份关联的主体相关属性信息，描述了该主体的各种特征、偏好或历史行为。参考[GB/T 31504—2015，7.1 数字身份信息服务]。

注2：数字身份信息服务是由管理主体数字身份的数字身份提供方向主体和其他网络实体提供的主体数字身份信息访问服务，包括各种数字身份信息的创建，删除，查询和修改服务。参考[GB/T 31504—2015，7.1 数字身份信息服务]。

6.5.4 设备管理

设备管理子组件提供设备的硬件配置信息、操作系统环境信息、设备运行状态信息等。

设备管理子组件提供设备监控服务、设备唯一性身份验证服务、设备绑定关系服务等。

注1：网络中提供服务、可被访问的设备也被视为资源，例如：网络共享打印机。

注2：核心组件在设备管理子组件服务支撑下，进行资产完整性和安全态势监控，包括探测漏洞、设备身份验证等。

6.5.5 资源管理

资源管理子组件提供资源分级分类属性信息、资源访问属性、资源存储属性、资源环境属性信息等。

资源管理子组件提供数据管理服务、网络管理服务、应用系统管理服务，包括数据目录、数据标识、网络地址标识、应用系统唯一性身份验证等。

注1：网络管理服务和应用系统管理服务共同实施应用分级管理，包括：对不同等级的应用进行分级隔离、对符合同一安全策略的应用或数据进行分域隔离等；辅助实施多种计算环境下应用之间的通信，例如：云计算环境下容器间通信等。

注2：应用系统通过验证应用系统的唯一性信息实施应用系统身份鉴别，应用系统的唯一性信息根据实际情况设置，例如：软件代码签名/验签等。

6.5.6 态势感知

态势感知子组件提供环境属性信息、安全态势信息、威胁情报信息等。

态势感知子组件提供计算环境监控、网络环境监控、风险和威胁感知服务、威胁情报预警等服务。

注1：态势感知子组件通过感知、监测等方式收集事件数据，分析、预测安全风险和威胁，为核心组件提供动态化多来源信息。

注2：态势感知子组件持续监控主体、资源和核心组件运行状态。

6.6 组件间关系

6.6.1 主体与核心组件、支撑组件关系

核心组件对主体进行持续环境感知和持续属性评估，实时执行策略决定，进行身份鉴别、建立/维持/阻断主体到被访问资源的授权访问；

支撑组件为主体提供数字身份管理、身份鉴别、设备管理、风险和威胁感知服务等。

6.6.2 资源与核心组件、支撑组件关系

核心组件对资源进行持续威胁感知和持续属性评估，控制资源实时响应策略决定，建立/维持/阻断主体到被访问资源的授权访问；

支撑组件为资源提供资源信息管理、网络连接服务、风险和威胁感知服务等。

6.6.3 支撑组件与核心组件关系

支撑组件为核心组件提供支持开展持续威胁感知、持续信任评估、动态细粒度调整的多来源信息。

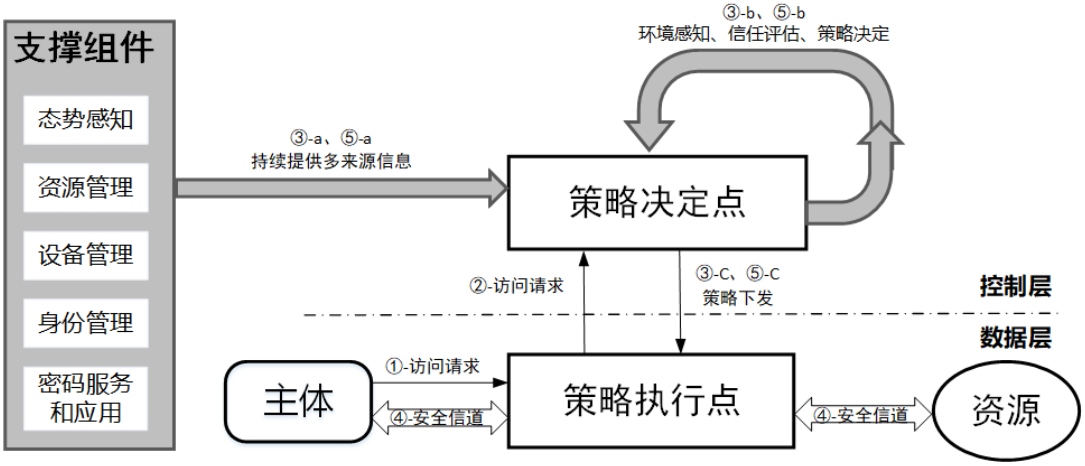
支撑组件对主体、资源、和核心组件实施安全监控和运行环境感知，为核心组件实时提供采集的主体、资源、和核心组件运行信息，例如：系统日志等。

支撑组件为核心组件提供包括密码服务、身份鉴别服务、资源管理服务、设备服务等多种服务支撑。

附 录 A
（资料性）
典型工作流程

A.1 主体访问资源

主体访问资源典型工作流程见图A.1。



图A.1 主体访问资源典型工作流程图

步骤如下：

①主体发起访问请求；

②策略执行点接收访问请求，转发访问请求相关信息至策略决定点；

③策略决定点根据多来源信息，采用信任评估等方法进行策略决定，向策略执行点发送允许或拒绝指令，并进行会话管理；

③-a 支撑组件向策略决定点提供多来源信息；

③-b 策略决定点根据多来源信息，进行环境感知、信任评估，直至策略决定；

③-b 策略决定点向策略执行点下发策略决定，进行会话管理，控制在数据层建立主体到资源的安全信道。

④策略执行点按照策略决定结果，在收到允许指令时建立主体到资源的安全通信，在收到拒绝指令时，终止访问；

⑤持续监控访问过程，持续信任评估，根据终端环境感知、用户行为分析、威胁情报等信息进行动态细粒度调整，在策略决定点控制下，维持或终止访问。

⑤-a 支撑组件持续向策略决定点提供多来源信息；

⑤-b 策略决定点根据多来源信息，持续进行环境感知、信任评估，直至策略决定；

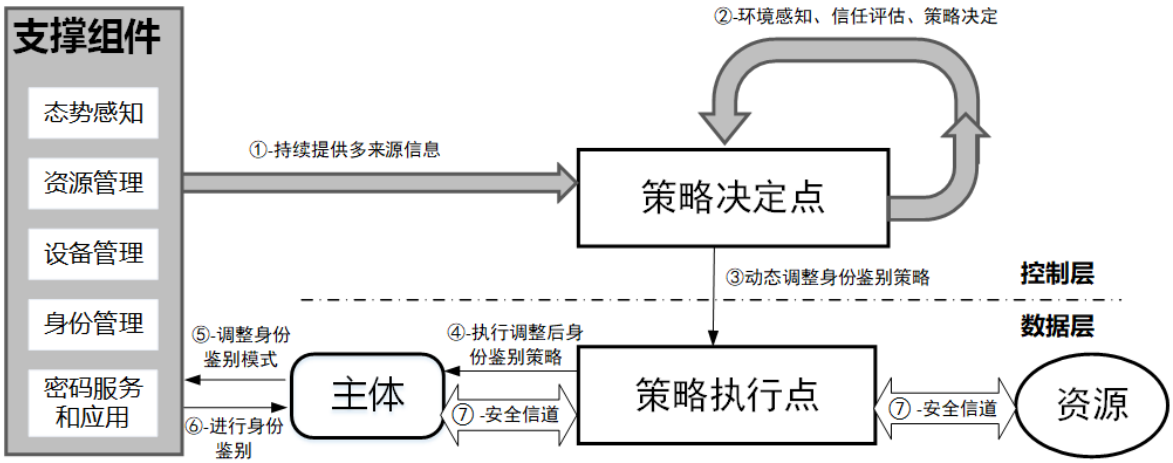
⑤-b 策略决定点向策略执行点下发策略决定，通过会话管理，控制在数据层维持或终止主体到资源的安全信道。

注1：支撑组件提供的多来源信息包括主体信息、资源信息、访问日志、感知信息、监控信息、安全事件等。

注2：策略执行点接收访问请求并转发的时间窗口内，保持访问请求其他信息，等待策略决策，若终止访问，则释放该访问请求相关信息。

A.2 动态调整访问策略

以身份鉴别策略调整为例，动态调整访问策略工作流程见图A.2。



图A.2 身份鉴别策略调整工作流程图

步骤如下：

①持续监控访问过程，获取支撑组件提供的多来源信息；

②策略决定点感知主体属性、资源属性和环境属性变化，发现影响身份鉴别的因素，进行信任评估、策略决定，产生身份鉴别调整策略；

③策略决定点向策略执行点下发身份鉴别调整策略；

④策略执行点向主体下发身份鉴别调整策略，控制执行调整后的身份鉴别策略；

⑤主体向支撑组件申请调整身份鉴别服务，示例为调整身份鉴别模式；

⑥支撑组件对主体进行调整鉴别模式后的身份鉴别，向策略执行点反馈执行情况；

⑦策略执行点根据身份鉴别结果，执行身份鉴别调整策略，在数据层维持或终止主体到资源的安全信道。

注1：在主体访问资源的过程中，属性的变化直接影响策略的变化。

注2：影响身份鉴别策略动态调整因素包括时间窗口到期、运行环境风险变化等，策略决定点持续分析支撑组件所提供的多来源信息后感知发现。

参 考 文 献

[1] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

[2] GB/T 35273—2020 信息安全技术 个人信息安全规范

[3] GB/T 31504—2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范

[4] GB/T 36960—2018 信息安全技术 鉴别与授权 访问控制中间件框架与接口

[5] GB/T 29242—2012 信息安全技术 鉴别与授权 安全断言标记语言

[6] GB/T 30281—2013 信息安全技术 鉴别与授权 可扩展访问控制标记语言

[7] GB/T 34990—2017 信息安全技术 信息系统安全管理平台技术要求和测试评价方法

[8] ISO/IEC 24760-1:2011 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts

[9] ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements

[10] ISO/IEC 24760-3:2016 Information technology — Security techniques — A framework for identity management — Part 3: Practice

[11] Scott W. Rose and Oliver Borchert et al., Zero Trust Architecture, National Institute of Standards and Technology (NIST) Special Publication 800-207, Gaithersburg, Md., August 2020. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf