



中华人民共和国国家标准

GB/T 47697—2026

网络安全技术 鉴别与授权 基于属性的 访问控制模型与管理规范

Cybersecurity technology—Authentication and authorization—
Specification for attribute-based access control model and management

2026-05-25 发布

2026-12-01 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 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 2

5 模型概述 2

6 属性 3

 6.1 概述 3

 6.2 属性分类 3

 6.3 属性的元数据 3

7 策略 4

 7.1 策略制定 4

 7.2 策略表达 4

8 ABAC 引擎 5

9 ABAC 的管理要求 5

 9.1 属性管理 5

 9.2 策略管理 6

 9.3 ABAC 引擎管理 6

10 测试方法 7

 10.1 属性管理测试方法 7

 10.2 策略测试方法 9

 10.3 ABAC 引擎测试方法 9

附录 A (资料性) ABAC 系统 11

 A.1 概述 11

 A.2 授权组件 11

 A.3 属性提供组件 11

 A.4 策略管理组件 12

 A.5 安全性设计 12

参考文献 13

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：北京中关村实验室、中国科学院大学、奇安信网神信息技术(北京)股份有限公司、华北电力大学、中国科学院软件研究所、北京邮电大学、中金金融认证中心有限公司、中国长江三峡集团有限公司、中国电子技术标准化研究院、北京理工大学、联通在线信息科技有限公司、陕西省信息化工程研究院、湖北省数字证书认证管理中心有限公司、中国电子科技集团公司第十五研究所、中科信息安全共性技术国家工程研究中心有限公司、北京山石网科信息技术有限公司、北京天融信网络安全技术有限公司、中电信量子信息科技集团有限公司、启明星辰信息技术集团股份有限公司、杭州安恒信息技术股份有限公司、数盾信息科技股份有限公司、北京万里红科技有限公司、兴唐通信科技有限公司、天翼安全科技有限公司、中兴通讯股份有限公司、四川大学、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(重庆)有限公司、国家信息技术安全研究中心、公安部第三研究所、上海东航数字科技有限公司、国能数智科技开发(北京)有限公司、中国科学院信息工程研究所、北京芯盾时代科技有限公司、北京持安科技有限公司、蚂蚁科技集团股份有限公司、中国信息通信研究院、国家计算机网络应急技术处理协调中心、四川省商投信息技术有限责任公司、格尔软件股份有限公司、长春吉大正元信息技术股份有限公司。

本文件主要起草人：刘勇、荆继武、李建彬、张立武、张勇、安锦程、孔坚、王跃武、马梦娜、吴思宇、李小勇、张严、范煊茁、谢亮、李彦峰、王惠莅、张子剑、程福兴、赵晓荣、陈诚、金达、刘栋、刘丽敏、崔宝江、徐洁、高雅丽、胡建勋、黄亮、刘浩、马思源、付巍、刘治平、刘勇、周瑞群、张凯歌、朱云、江海昇、王辉、方宇、曹鲲鹏、徐蕾、李贝贝、张爱雯、秦益飞、李俊、李海玲、陈妍、东明、曹慧、李敏、孙悦、何艺、白晓媛、穆域博、崔牧凡、孙涌潮、郑强、李武璐。

网络安全技术 鉴别与授权 基于属性的访问控制模型与管理规范

1 范围

本文件确立了基于属性的访问控制的模型,规定了基于属性的访问控制的管理要求,描述了对应的测试方法。

本文件适用于网络应用机构、网络安全产品和服务提供商规划、设计、开发和建设基于属性访问控制系统,也可为基于属性访问控制系统实施测评、监管提供参考。

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 信息安全技术 术语

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

基于属性的访问控制 attribute-based access control

根据分配给主体、客体的属性,环境属性以及基于这些属性制定的一组策略,来判定主体对客体执行操作的请求是否允许的访问控制方法。

3.2

属性 attribute

可被策略调用,用于控制客体访问权限的特征信息。

注 1: 属性包括主体属性、客体属性、环境属性以及策略中用于控制访问的其他属性。

注 2: 属性信息以名称-值对的形式定义。

3.3

属性授权机构 attribute authority

负责授权属性信息的创建、发布与管理的机构。

3.4

策略 policy

执行访问控制决策所遵循的规则。

注 1: 策略由一组规则、一种规则组合算法标识和(可选的)一组义务组成,是策略集的组成部分。

注 2: 在给定主体属性、客体属性及环境属性的属性值的前提下,策略用于判定所请求的访问是否被允许。

3.5

数字策略 digital policy

直接编码成机器可执行的代码的访问控制规则。

注: 主体属性、客体属性、环境属性和操作是数字策略的基本元素,数字策略规则的编译结果由访问控制机制执行。

3.6

元策略 metapolicy

用于定义、管理和约束访问控制策略的策略。

3.7

自然语言策略 natural language policy

用自然语言描述的访问控制策略。

4 缩略语

下列缩略语适用于本文件。

ABAC: 基于属性的访问控制(attribute-based access control)

5 模型概述

ABAC 是一种访问控制方法,其核心思想是将属性与权限相关联,以实现基于属性的动态访问控制。该方法通过组织间统一的主体属性、客体属性和环境属性来定义访问策略,避免了将访问权限直接授予某个主体。

ABAC 通过 ABAC 引擎对主体属性、客体属性和环境属性的当前值进行评估,并根据这些属性所生成的策略执行授权决策。ABAC 模型由主体属性、客体属性、环境属性、策略、操作(主体访问请求)和 ABAC 引擎等组件构成,见图 1。

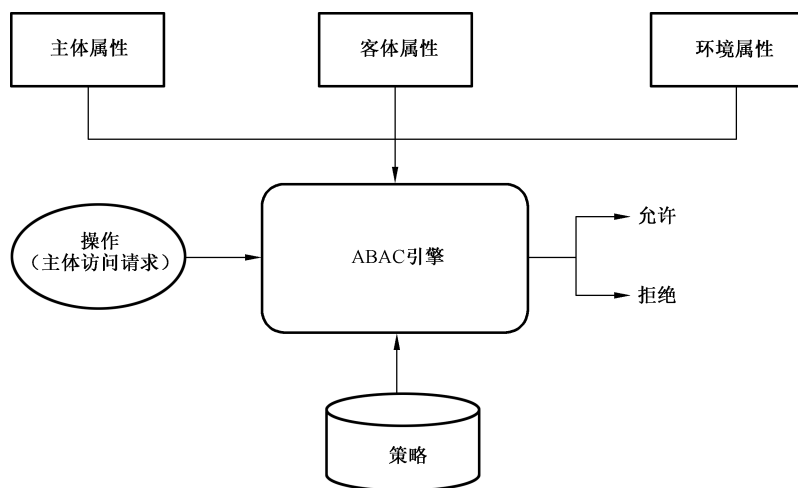


图 1 ABAC 模型

ABAC 在实施访问控制(见图 1)时,包括以下三个阶段。

- a) 主体发出访问客体的操作请求。
- b) ABAC 引擎评估主体属性、客体属性、环境属性和策略,以得出允许或拒绝主体访问操作请求的授权。
- c) 如果被授权,允许主体访问客体;如果未被授权,客体拒绝主体访问。

在任何系统中,ABAC 的实施都依赖于主体和客体的属性分配,以及包含访问规则的策略制定。

6 属性

6.1 概述

ABAC 基于属性定义访问控制策略,并实施访问控制。ABAC 属性反映主体身份、客体特征、操作类型、环境状态等的信息,都作为属性参与访问控制决策。

ABAC 通过使用属性,在访问控制决策过程中引入更多的离散输入变量,定义丰富、明确的策略表达。

6.2 属性分类

6.2.1 主体属性

主体是指访问控制行为的发起者,是自然人或非自然人实体。每个主体均被分配一组主体属性。

主体属性是描述与主体相关的特征信息的集合,可划分为自然主体属性和授权主体属性两类。

- a) 自然主体属性:描述主体所固有的、不随访问控制操作上下文的不同而变化的属性。例如个人身份信息、个人生物识别信息等。
- b) 授权主体属性:描述在给定的访问控制操作上下文中分配给主体访问权限的一组属性,随着给定上下文的不同而动态变化。例如分配给主体的角色、工作职能、工号、域名、网址等。授权主体属性反映了主体在特定访问控制环境下的角色、权限级别及临时状态,随着主体特征、访问环境态势及业务需求等的变化而动态调整。

6.2.2 客体属性

客体是访问控制行为的对象,每个客体均被分配一组客体属性。

客体属性是描述与客体相关的特征信息的集合,可划分为自然客体属性和授权客体属性两类。

- a) 自然客体属性:描述客体创建后,固有的、不随给定访问控制操作上下文变化或变化不频繁的属性,通常描述客体的基本信息或物理特性。例如数据库主键、时间戳、文件扩展名、编码方式及数字指纹等。
- b) 授权客体属性:描述在给定访问控制上下文中分配给客体被访问的一组属性,随着给定上下文的不同而动态变化。例如分配给客体的编号、所有者、创建和删除的日期和时间、授权级别等。这些属性反映了客体在不同访问控制环境下的状态、权限设置以及临时特性,通常基于管理制度、业务需求而设定。

6.2.3 环境属性

环境属性是指独立于任何特定的主体或客体,参与判定访问控制操作的访问环境态势信息。例如当前日期、时间、位置、威胁种类和系统状态等。环境属性不是被动创建和管理的,而是内在的且能被 ABAC 系统检测。在授权访问请求时,根据当前匹配的环境变量评估环境属性,环境属性为访问控制策略中指定特殊或动态规则的定义提供依据。

注:当使用环境属性组成访问控制规则时,环境属性变量和它们的值是防篡改的。

6.3 属性的元数据

ABAC 在实施访问控制前,确定、定义和描述一组标准化的元数据。属性的元数据是每个属性的基本信息元素,主要包括属性值信息、属性创建信息以及属性来源信息等。

- a) 属性值信息:例如更新频率、有效期等。

- b) 属性创建信息:例如属性是自断言的,还是从属性授权系统检索而来的。
- c) 属性来源信息:例如属性来源的标识等。

在访问控制判定过程中,标准化的属性的元数据用于评估属性的可信度,通过评估属性来源的权威性、属性信息的时效性以及属性信息验证频率的准确性等属性的元数据来为属性的可信度打分,定义属性的真实性、安全性和时效性。属性可信度的评估结果可作为访问控制判定输入的一部分,以实现细粒度访问控制。

在属性管理过程中,属性的元数据用于对属性进行分组和划分等级,避免为每个主体或客体分配相同的属性,以提高访问控制的灵活性和属性管理的便捷性。例如,根据系统中主体或客体的共同特征,将主体或客体划入不同的分组,每个“组”即为属性的元数据。

7 策略

7.1 策略制定

在 ABAC 中,策略是基于属性来制定的,来判定访问控制是否授权的规则或其集合。策略制定的原则如下:

- a) 策略的制定符合条件-结果逻辑,即在某种属性组合条件下,允许或拒绝某个主体对某个客体执行何种操作;
- b) 在定义策略过程中,预先确定主体属性、客体属性和环境属性;
- c) 在定义策略过程中,策略描述的访问控制操作来源于组织内部的业务流程、管理制度等。

7.2 策略表达

7.2.1 策略表达形式

策略表达是从人可理解的业务和管理视角的自然语言向机器可执行的形式化语言转化的过程,表达形式包括自然语言策略和数字策略两种。

- a) 自然语言策略是访问控制策略的自然语言表达,应符合策略定义的原则。例如按条件-结果逻辑描述访问控制策略,但不可被机器直接执行。
- b) 数字策略是能直接编码成机器可读、可执行的代码的访问控制策略表达形式。数字策略语句由主体和客体属性以及满足允许访问控制操作的环境属性组成。

自然语言策略向数字策略的转换过程经历两个阶段。

- a) 阶段一:将自然语言策略转换成一组仍由自然语言描述和可部署执行的访问控制规则。在该阶段,应确定策略中的主体属性、客体属性的组合和允许的操作。
- b) 阶段二:通过技术手段,将访问控制规则转换为机器可执行的数字策略。

7.2.2 策略表达语言

策略表达语言是用于描述访问控制策略的编程语言。ABAC 对策略表达语言的基本需求主要包括:

- a) 提供一种方法来基于主体、客体的属性进行授权决策;
- b) 提供一组逻辑和数学操作符来处理主体、客体 and 环境的属性;
- c) 提供一种方法将单独的规则和策略组合成一个策略集,以便使其适用于某次决策请求;
- d) 提供一种方法来定义策略和规则的组合过程;
- e) 提供一种方法来处理多值属性。

8 ABAC 引擎

ABAC 引擎是 ABAC 模型的核心组件。ABAC 引擎将策略、主体属性、客体属性和环境属性组合在一起,然后进行策略匹配与逻辑计算以执行策略判定。

ABAC 引擎一般包括策略判定、策略执行、策略管理和属性提供四个功能,该引擎的系统组件参考架构见附录 A。

ABAC 引擎应能管理策略的决策与执行流程,包括对检索的策略、获取不同类型属性的先后顺序,以及属性来源等的确定。

9 ABAC 的管理要求

9.1 属性管理

9.1.1 总体要求

属性管理总体要求包括以下内容:

- a) 授权属性应由属性授权机构提供,在多个属性授权机构并存的场景下,每个机构应对其提供的主体属性或客体属性分别具有权威性;
- b) 属性授权机构应识别所有属性信息并整理成属性列表,以使在定义每一条访问控制策略时,均有对应的属性;
- c) 属性授权机构应按照数字策略的要求对属性进行命名、定义、赋予一组允许值,规定属性命名、定义及赋予允许值的数据模式,并向所有参与者公开;

注:属性命名、定义及赋予允许值的模式是指定义属性信息的内容、结构和约束的描述。

- d) 在属性被命名、定义、赋予一组允许值后,属性授权机构应为主体和客体建立属性和适当属性值的分配方法;
- e) 属性授权机构应对属性的存储机制、防护机制进行评估,评估内容包含但不限于以下因素:属性完整性校验,用于属性更新、复制、撤销等操作的安全策略,属性存储环境的防御手段,属性变更和审核日志等。

9.1.2 主体属性管理

主体属性管理要求包括以下内容:

- a) 属性授权机构应采用技术措施,使得主体属性的完整性、准确性和更改记录等可被验证;
- b) 检查属性授权机构是否提供了组织内部使用的属性列表,并标识了属性来源。

9.1.3 客体属性管理

客体属性管理要求包括以下内容:

- a) 属性授权机构应采用技术措施,使得客体属性只能以合规的流程来进行分配或验证;
- b) 属性授权机构应采用技术措施,使得客体属性的完整性、准确性以及更改记录等可被验证,并集成于客体属性管理的机制或框架中;
- c) 在计算策略决策时,属性授权机构应使得客体属性可被检索。

9.1.4 环境属性管理

环境属性管理要求包括以下内容:

- a) 环境属性采集系统应采用技术措施,使环境属性变量及其取值是可信的;
- b) 环境属性采集系统应采用技术措施,使环境属性变量及其取值能被 ABAC 中的所有相关组件获取;
- c) 环境属性采集系统应使环境属性变量及其取值与当前所请求的访问控制操作所处的环境相关联。

9.1.5 属性管理机制

属性管理机制管理要求包括以下内容:

- a) 属性授权机构应采取技术措施,使主体属性、客体属性的定义和取值在 ABAC 范围内保持有效性和一致性,例如属性的元数据、属性分组的层次结构等,以使得 ABAC 引擎能基于全局一致的属性值计算访问控制判定;
- b) 属性授权机构应遵循属性来源最小化原则;
- c) 属性授权机构应根据 ABAC 引擎策略判定点的请求,由权威的属性来源提供属性信息;
- d) 属性授权机构应确定、定义和描述一组标准化的属性的元数据;
- e) 属性授权机构应采取技术措施,防止属性值及其元数据遭到篡改或破坏。

9.2 策略管理

策略管理是指对访问控制规则、数字策略和元策略的管理。管理要求包括以下内容。

- a) 访问控制规则应由组织内的权威部门制定、应用、维护、共享和断言。
注:断言是提供给规则被共享方的相关规则被验证的可信声明。
- b) 访问控制规则应准确和完整地反映自然语言策略。
- c) 系统中的每个客体都应在自然语言策略中记录对应的访问控制规则。
- d) 策略管理机构应采用技术措施实现信息共享和隐私保护的平衡。例如,当支持多个访问控制规则时,应限制某些规则对特定主体的可见范围,以降低未授权主体通过篡改属性非法访问客体的风险。
- e) 数字策略应由具备自然语言策略解读能力且拥有定义权限的机构进行定义或修改。
- f) 策略管理机构定义的每个数字策略都应满足自然语言策略的要求。
- g) 策略管理机构应采用技术措施保护数字策略的安全性。
- h) 元策略是管理策略的策略,当某个数字策略存储、更新,或多个数字策略出现优先级分配或冲突时,策略管理机构应通过元策略进行策略管理。
- i) 策略管理机构负责管理数字策略和元策略,当出现多个策略管理机构时,数字策略和元策略的管理规则应由最高权威机构制定。

9.3 ABAC 引擎管理

ABAC 引擎管理要求主要包括以下内容:

- a) ABAC 引擎的管理应仅限于专门负责维护的人员、相关机构;
- b) 维护的人员、机构应建立规范的流程文档,以验证对主体分配的客体访问授权要求的满足情况;
- c) 维护的人员、机构应开发 ABAC 引擎功能组件所应用的接口和程序,以根据相关权威机构定义和授权的权限,对访问信息的妥善维护;
- d) 维护的人员、机构应对 ABAC 引擎的功能组件定期开展评估或审计;
- e) 维护的人员、机构应定期维护 ABAC 引擎的功能组件。

10 测试方法

10.1 属性管理测试方法

10.1.1 总体要求

总体要求包括以下内容。

a) 测试方法：

- 1) 检查所有的属性信息是否被属性授权机构识别并整理成属性列表；
- 2) 检查属性授权机构是否按照数字策略的要求对属性进行命名、定义、赋予一组允许值，是否规定了属性的数据模式，并向所有参与者公开；
- 3) 检查属性授权机构是否为主体和客体建立了属性和适当属性值的分配方法；
- 4) 检查主体属性、客体属性是否由属性授权机构提供，在多个属性授权机构并存的场景下，每个机构是否对不同主体属性和客体属性分别具有权威性；
- 5) 检查属性授权机构是否对属性的存储机制、防护机制进行了评估，检查内容包括是否采用了加密方法，是否采用了用于属性更新、复制、撤销等操作的安全策略、属性存储环境的防御手段以及属性变更和审核日志等。

b) 预期结果：

- 1) 所有的属性信息均被属性授权机构识别并整理成属性列表；
- 2) 属性授权机构按照数字策略的要求对属性进行了命名、定义、赋予一组允许值，规定了属性的数据模式，并向所有参与者公开；
- 3) 主体属性、客体属性由属性授权机构提供，在多个属性授权机构并存的场景下，每个机构对不同主体属性和客体属性分别具有权威性；
- 4) 属性授权机构为主体和客体建立了属性和适当属性值的分配方法；
- 5) 属性授权机构对属性的存储机制、防护机制进行了评估，评估内容涵盖了采用了加密方法，用于属性更新、复制、撤销等操作的安全策略、属性存储环境的防御手段以及属性变更和审核日志等。

c) 结果判定：上述预期结果均满足判定为符合，否则为不符合或部分符合。

10.1.2 主体属性管理

主体属性管理测试要求包括以下内容。

a) 测试方法：

- 1) 检查属性授权机构是否采用技术措施保障了主体属性的完整性、准确性、可用性和隐私保护；
- 2) 检查属性授权机构是否提供了组织内部使用的属性列表，并标识了属性来源。

b) 预期结果：

- 1) 属性授权机构采用了相关技术措施对主体属性的完整性、准确性、可用性和隐私进行了保护；
- 2) 存在组织内部使用的属性列表，对属性来源进行了标识。

c) 结果判定：上述预期结果均满足判定为符合，否则为不符合或部分符合。

10.1.3 客体属性管理

客体属性管理测试要求包括以下内容。

- a) 测试方法：
 - 1) 检查属性授权机构是否采用了技术措施,使得客体属性以合规的流程来进行分配或验证;
 - 2) 检查属性授权机构是否采用了技术措施,对客体属性的完整性、准确性以及更改记录等进行了验证,是否将相关技术措施集成于客体属性管理的机制或框架中;
 - 3) 检查在计算策略决策时,客体属性是否可被检索。
- b) 预期结果：
 - 1) 属性授权机构采用了技术措施,客体属性以合规的流程来进行分配或验证;
 - 2) 属性授权机构采用了技术措施,客体属性的完整性、准确性以及更改记录得到验证,客体属性管理的机制或框架中集成了相关技术措施;
 - 3) 计算策略决策时,客体属性可被检索并展示检索结果。
- c) 结果判定:上述预期结果均满足判定为符合,否则为不符合或部分符合。

10.1.4 环境属性管理

环境属性管理测试要求包括以下内容。

- a) 测试方法：
 - 1) 检查 ABAC 中的所有相关组件是否能获取属性授权机构提供的环境属性变量及其取值;
 - 2) 检查属性授权机构是否采用了技术措施,对环境属性变量及其取值的可信性进行保障;
 - 3) 检查属性授权机构提供的环境属性变量及其取值,是否与当前判定的访问控制操作所处的环境相关联。
- b) 预期结果：
 - 1) ABAC 中的所有相关组件能获取属性授权机构提供的环境属性变量及其取值;
 - 2) 属性授权机构采用了技术措施,对环境属性变量及其取值的可信性进行保障;
 - 3) 属性授权机构提供的环境属性变量及其取值与当前判定的访问控制操作所处的环境相关联;
- c) 结果判定:上述预期结果均满足判定为符合,否则为不符合或部分符合。

10.1.5 属性管理机制

属性管理机制测试要求包括以下内容。

- a) 测试方法：
 - 1) 在 ABAC 范围内,检查主体属性、客体属性的定义和取值是否保持有效性和一致性;
 - 2) 检查访问控制授权决策过程中,属性授权机构是否遵循了属性来源最小化原则;
 - 3) 检查 ABAC 引擎发出属性检索请求后,是否由权威的属性来源向 ABAC 引擎提供属性信息;
 - 4) 检查属性授权机构是否确定、定义和描述了一组标准化的属性的元数据;
 - 5) 检查属性授权机构是否采用了技术措施保障属性值及其元数据的安全性。
- b) 预期结果：
 - 1) 主体属性、客体属性的定义和取值保持了有效性和一致性;
 - 2) 访问控制授权决策过程中,属性授权机构遵循了属性来源最小化原则;
 - 3) 权威的属性来源按照 ABAC 引擎发出属性检索请求,属性授权机构提供了属性信息;
 - 4) 属性授权机构确定、定义和描述了一组标准化的属性的元数据;
 - 5) 属性授权机构采用了技术措施,对属性值及其元数据的安全性进行保障。
- c) 结果判定:上述预期结果均满足判定为符合,否则为不符合或部分符合。

10.2 策略测试方法

策略测试要求包括以下内容。

a) 测试方法：

- 1) 检查访问控制规则是否由组织内的权威部门定义、应用、维护、共享和断言；
- 2) 检查访问控制规则是否能准确、完整地反映自然语言策略；
- 3) 检查自然语言策略是否记录了每个客体对应的访问控制规则；
- 4) 检查策略管理机构是否采用了技术措施保障信息共享和隐私保护的平衡；
- 5) 检查数字策略是否由具备自然语言策略解读能力且拥有定义权限的机构进行定义或修改；
- 6) 检查策略管理机构定义的每个数字策略是否满足自然语言策略的要求；
- 7) 检查策略管理机构是否采用了技术措施保护数字策略的隐私性；
- 8) 检查当数字策略存储、更新,或多个数字策略出现优先级分配或冲突时,策略管理机构是否通过元策略进行策略管理；
- 9) 检查是否由策略管理部门负责管理数字策略和元策略。

b) 预期结果：

- 1) 访问控制规则是由组织内的权威部门定义、应用、维护、共享和断言；
- 2) 访问控制规则能准确、完整地反映自然语言策略；
- 3) 自然语言策略记录了每个客体对应的访问控制规则；
- 4) 策略管理机构采用了技术措施保障信息共享和隐私保护的平衡；
- 5) 数字策略是由具备自然语言策略解读能力且拥有定义权限的机构进行定义或修改的；
- 6) 策略管理机构定义的每个数字策略都能满足自然语言策略的要求；
- 7) 策略管理机构采用了技术措施保护了数字策略的隐私性；
- 8) 当数字策略存储、更新,或多个数字策略出现优先级分配或冲突时,元策略对数字策略进行了策略管理；
- 9) 存在策略管理部门,并由该部门负责管理数字策略和元策略。

c) 结果判定:上述预期结果均满足判定为符合,否则为不符合或部分符合。

10.3 ABAC 引擎测试方法

ABAC 引擎测试要求包括以下内容。

a) 测试方法：

- 1) 检查 ABAC 引擎的管理是否仅限于专门负责维护的人员、相关机构；
- 2) 检查维护的人员、机构是否制定规范化的流程文档,以此确认授权定义中对主体所分配的客体访问权限要求的落实情况；
- 3) 检查 ABAC 引擎功能组件是否开发了所应用的接口和程序,以根据相关权威机构定义和授权的权限,对访问信息的妥善维护；
- 4) 检查维护的人员、机构是否对 ABAC 引擎的功能组件定期开展了评估或审计；
- 5) 检查维护的人员、机构是否定期维护 ABAC 引擎的功能组件。

b) 预期结果：

- 1) ABAC 引擎仅由专门的负责人员、相关机构进行管理维护；
- 2) 维护的人员、机构制定了规范化的流程文档,以此确认授权定义中对主体所分配的客体访

问权限要求是否已落实；

- 3) ABAC 引擎功能组件开发了所应用的接口和程序；
 - 4) 维护的人员、机构对 ABAC 引擎的功能组件定期开展了评估或审计；
 - 5) 维护的人员、机构定期对 ABAC 引擎的功能组件进行了维护。
- c) 结果判定：上述预期结果均满足判定为符合，否则为不符合或部分符合。

附录 A
(资料性)
ABAC 系统

A.1 概述

ABAC 系统通过引入主体、客体、环境等属性,实现访问控制机制。
ABAC 系统由授权组件、属性提供组件和策略管理组件组成,见图 A.1。

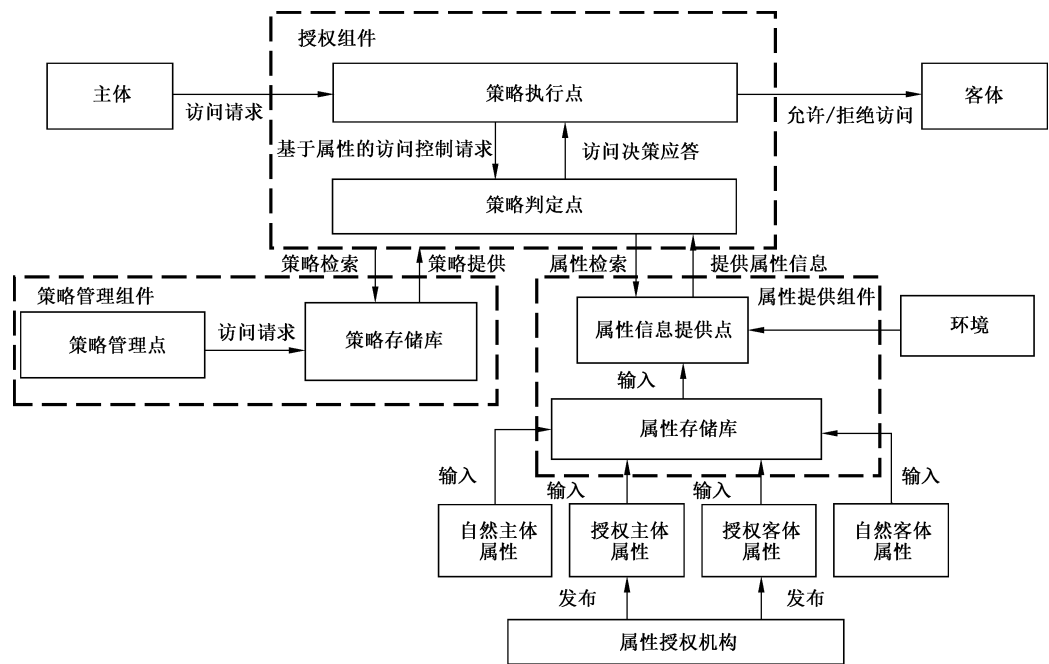


图 A.1 ABAC 系统

授权组件包括策略判定点和策略执行点,属性提供组件包括属性信息提供点和属性存储库,策略管理组件包括策略管理点和策略存储库。

当主体访问资源时,授权组件中的策略执行点将访问请求发送给策略判定点,由策略判定点根据属性提供组件的属性信息提供点提供的属性信息做出策略判定,并经策略管理组件的策略管理点验证和评估后,策略执行点强制执行策略判定。

A.2 授权组件

授权组件对数字策略进行评估,结合 ABAC 模型中的各种要素,产生访问控制策略并执行。授权组件由策略判定点和策略执行点组成,主要功能如下。

- a) 策略判定点:负责评估使用的数字策略并对策略冲突进行调解,生成访问控制决策。策略判定点可支持向多个策略执行点下发策略。
- b) 策略执行点:负责执行策略判定点的决策,响应操作受保护客体的主体访问请求。策略执行点的部署位置与应用紧密结合(如:部署在软件应用中、部署在网关位置)。

A.3 属性提供组件

属性提供组件由属性信息提供点和属性存储库组成,主要功能如下。

- a) 属性信息提供点:产生并提供属性值的系统实体,负责向数字策略提供判定所需的信息,是属性或策略评估所应用数据的检索源。
- b) 属性存储库:负责存储主体、客体属性集合。通过属性存储库,确定工作流过程中一组执行访问请求的主体和被访问的客体。

A.4 策略管理组件

策略管理组件负责提供数字策略的管理、存储、验证、更新、优先级排序、冲突解决、共享、策略下线和执行等能力。策略管理组件由策略管理点和策略存储库组成,主要功能如下:

- a) 策略管理点:是创建策略或策略集的系统实体,负责创建、管理、测试和调试数字策略和元策略,并将这些策略存储在适当的策略存储库中;
- b) 策略存储库:负责存储 ABAC 规则、策略和策略集。

A.5 安全性设计

使用密码服务保障 ABAC 访问控制系统的实体属性的真实性、数据的机密性和完整性、操作行为的不可否认性,为主体、客体、访问控制系统提供密码相关的网络和通信安全服务,设备和计算安全服务、应用和数据安全服务。

参 考 文 献

- [1] GB/T 11457—2006 信息技术 软件工程术语
 - [2] GB/T 18336.1—2024 网络安全技术 信息技术安全评估准则 第1部分:简介和一般模型
 - [3] 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
 - [4] 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
 - [5] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
 - [6] GB/T 43696—2024 网络安全技术 零信任参考体系架构
 - [7] NIST SP 800-162 Guide to Attribute Based Access Control (ABAC) Definition and Considerations
 - [8] NIST SP 800-205 Attribute Considerations for Access Control Systems
-