(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102176226 B
(45)授权公告日 2013.02.13

(21)申请号 201110162110.4
(22)申请日 2007.09.05
(30)优先权数据
11/530,438 2006.09.08 US
(62)分案原申请数据
200780033322.4 2007.09.05
(73)专利权人 微软公司
地址 美国华盛顿州
(72)发明人 B·B·迪拉韦 M·Y·贝克
A·D·戈登 C·富尔内
(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 顾嘉运
(51)Int.Cl.
G06F 21/62(2013.01)
(56)对比文件
US 2001018675 A1,2001.08.30,
US 2006106856 A1,2006.05.18,
US 2005132220 A1,2005.06.16,
US 2004123154 A1,2004.06.24,
US 2003225697 A1,2003.12.04,
审查员 吴广平

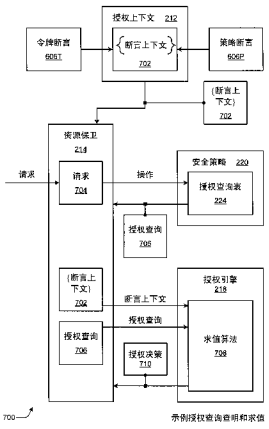
权利要求书 1 页 说明书 14 页 附图 10 页

(54)发明名称

安全授权查询

(57)摘要

在一示例实现中，一分支安全方案具有不允许使用否定的第一层和允许使用否定的第二层。在另一示例实现中，一授权查询表将各个资源专用操作映射到相应的相关联授权查询。在又一示例实现中，允许授权查询具有否定，但不允许个别断言具有否定。



CN 102176226 B

1. 一种通过具有第一层和第二层的分支安全方案来实现安全授权查询的方法，其中所述第一层不允许使用否定，所述第二层许可使用否定，所述第一层包括断言层，而所述第二层包括查询层，所述方法包括：

由令牌断言和策略断言来填充所述断言层；

由至少从所断言的事实和逻辑运算符形成的授权查询来填充所述查询层；

所述分支安全方案通过试图将来自所述断言层的有效断言匹配到特定的授权查询的一个或多个所断言的事实而对所述特定的授权查询求值以作出授权决策。

2. 如权利要求 1 所述的方法，其特征在于，所述分支安全方案包括不允许包含否定的任何断言的句法确认器。

3. 如权利要求 1 所述的方法，其特征在于，所述逻辑运算符包括与、或和非；且其中每一授权查询与一资源专用操作相关联。

安全授权查询

[0001] 本申请是申请人于 2007 年 9 月 5 日提交的、申请号为“200780033322.4”(国际申请号为“PCT/US2007/077641”) 的、发明名称为“安全授权查询”的发明专利申请的分案申请。

[0002] 背景

[0003] 计算机和其他电子设备遍布人们的职业和个人生活。在职业设置中,人们在项目协作期间交换和共享机密信息。在个人设置中,人们参与电子商务以及个人信息的传输。在这些和其他众多情况中,电子安全措施被认为是重要的。

[0004] 电子安全措施范例可令职业信息保持机密以及个人信息保持私密。电子安全措施范例可涉及某种水平的加密和 / 或针对诸如病毒、蠕虫和间谍软件等恶意软件的保护。信息的加密以及针对恶意软件的保护历来受到极大的关注,尤其是近几年来。

[0005] 然而,控制对信息的访问是保护电子信息安全性同等重要的方面。对于其中受益于电子信息的共享和 / 或传送的情形尤其如此。在这样的情形中,某些人被准许访问,而其他人要被排除在外。

[0006] 访问控制自早期的共享系统以来就是共享计算机和应用程序服务器的共同特征。存在用于控制对信息的访问的多种不同的方法。它们在组合对请求对某一资源的访问的实体的认证以及授权所允许的访问的机制方面享有共同的基础。认证机制包括口令、Kerberos、以及 x.509 证书。其目的在于允许进行资源控制的实体肯定地标识进行请求的实体或它所需的关于实体的信息。

[0007] 授权示例包括访问控制列表 (ACL) 以及基于策略的机制,诸如可扩展访问控制标记语言 (XACML) 或特权和角色管理基础架构 (PERMIS)。这些机制定义哪些实体可访问给定的资源,诸如文件系统中的文件、硬件设备、数据库信息等。它们通过提供关于请求者的认证信息以及所允许的对资源的访问之间的映射来执行这种授权。

[0008] 随着计算机系统越来越普遍地连接到诸如因特网等大型网络上,这些机制被证实在处理日益发展的访问控制要求方面稍有限制和不灵活。地理上散布的用户和计算机资源的系统,包括横跨多个行政区域的那些系统尤其提出了当前部署的技术解决不好的多个挑战。

[0009] 概述

[0010] 在一示例实现中,一分支安全方案具有不允许使用否定的第一层和允许使用否定的第二层。在另一示例实现中,一授权查询表将各个资源专用操作映射到相应的相关联授权查询。在又一示例实现中,允许授权查询具有否定,但不允许个别断言具有否定。

[0011] 提供本概述以便以简化的形式介绍将在以下详细描述中进一步描述的一些概念。该概述不旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用于帮助确定所要求保护的主题的范围。而且,其它方法、系统、方案、装置、设备、介质、过程、API、安排、协议等的实现也在此得到描述。

[0012] 附图简述

[0013] 在各图中使用相同的数字来引用相同和 / 或对应的方面、特征和组件。

[0014] 图 1 是示出其中可以实现示例安全方案的示例一般环境的框图。

[0015] 图 2 是示出具有两个设备以及多个示例安全相关组件的示例安全环境的框图。

[0016] 图 3 是示出其中在安全相关组件之间交换示例安全相关数据的图 2 的示例安全环境的框图。

[0017] 图 4 是可用于本文所述的安全相关实现的示例设备的框图。

[0018] 图 5 是示出用于一般安全方案的示例断言格式的框图。

[0019] 图 6 是示出具有第一层和第二层的示例分支安全方案的框图。

[0020] 图 7 是示出示例授权查询查明和示例授权查询求值的一般框图。

[0021] 图 8 是示出响应于资源访问请求的示例授权查询查明的更具体的框图。

[0022] 图 9 是示出给定断言上下文情况下的示例授权查询求值的更具体的框图。

[0023] 图 10 是示出用于查明授权查询并对其求值的方法的示例的流程图。

[0024] 详细描述

[0025] 示例安全环境

[0026] 图 1 是示出其中可以实现示例安全方案 100 的示例一般环境的框图。安全方案 100 表示进行保护的集成方法。如图所示，安全方案 100 包括多个安全概念：安全令牌 100(A)、安全策略 100(B)、以及求值引擎 100(C)。一般，安全令牌 100(A)、安全策略 100(B) 共同提供对求值引擎 100(C) 的输入。求值引擎 100(C) 接受输入，并产生指示应许可还是拒绝对某一资源的访问的授权输出。

[0027] 在所述实现中，安全方案 100 可由一个或多个设备 102 覆盖和 / 或与其集成，这些设备由硬件、软件、固件、其某种组合等组成。如图所示，“d”个设备在一个或多个网络 104 上互连，“d”是某一整数。更具体地，设备 102(1)、设备 102(2)、设备 102(3)... 设备 102(d) 能够经由网络 104 通信。

[0028] 每一设备 102 可以是能够实现安全方案 100 的至少一部分的任何设备。这样的设备的示例包括但不限于：计算机（例如，客户机计算机、服务器计算机、个人计算机、工作站、台式机、膝上型计算机、掌上型计算机等）、游戏机（例如，控制台、便携式游戏设备等）、机顶盒、电视机、消费电子产品（例如，DVD 播放器 / 记录器、摄录像一体机、数码录像机 (DVR) 等）、个人数字助理 (PDA)、移动电话、便携式媒体播放器、其某种组合等。一个示例电子设备在以下具体参考图 4 描述。

[0029] 网络 104 可由链接在一起和 / 或覆盖在彼此之上的任何一个或多个网络形成。网络 104 的示例包括但不限于：因特网、电话网络、以太网、局域网 (LAN)、广域网 (WAN)、有线电视网络、光纤网络、数字用户线 (DSL) 网络、蜂窝网络、Wi-Fi®网络、WiMAX®网络、虚拟专用网 (VPN)、其某种组合等。网络 104 可包括多个域、一个或多个网格网络等。这些网络或网络组合中的每一个可根据任何联网标准操作。

[0030] 如图所示，设备 102(1) 对应于正与之交互的用户 106。设备 102(2) 对应于正在其上执行的服务 108。设备 102(3) 与资源 110 相关联。资源 110 可以是设备 102(3) 的一部分，或与设备 102(3) 分开。

[0031] 用户 106、服务 108 以及诸如任何给定设备 102 等机器形成非穷举的示例实体列表。实体随时可能希望访问资源 110。安全方案 100 确保被正确认证和授权的实体被许可访问资源 110，而阻止其他实体访问资源 110。

[0032] 图 2 是示出具有两个设备 102(A) 和 102(B) 以及多个示例安全相关组件的示例安全环境 200 的框图。安全环境 200 还包括授权机构 202，诸如安全令牌服务 (STS) 授权机构。设备 102(A) 对应于实体 208。设备 102(B) 与资源 110 相关联。尽管安全方案 100 可在更复杂的环境中实现，但使用该相对简单的两个设备的安全环境 200 来描述示例安全相关组件。

[0033] 如图所示，设备 102(A) 包括两个安全相关组件 :安全令牌 204 和应用程序 210。安全令牌 204 包括一个或多个断言 206。设备 102(B) 包括五个安全相关组件 :授权上下文 212、资源保卫 214、审计日志 216、授权引擎 218 和安全策略 220。安全策略 220 包括信任和授权策略 222、授权查询表 224 和审计策略 226。

[0034] 每一设备 102 可被不同地配置，且仍能够实现安全方案 100 的全部或一部分。例如，设备 102(A) 可具有多个安全令牌 204 和 / 或应用程序 210。作为另一示例，设备 102(B) 可不包括审计日志 216 或审计策略 226。其它配置也是可能的。

[0035] 在所述实现中，授权机构 202 向实体 208 发放具有断言 206 的安全令牌 204。断言 206 在以下描述，包括在题为“安全策略断言语言示例特征”一节中。实体 208 从而与安全令牌 204 相关联。在操作中，实体 208 希望依靠安全令牌 204 使用应用程序 210 来访问资源 110。

[0036] 资源保卫 214 接收访问资源 110 的请求，并有效地管理与设备 102(B) 的其他安全相关组件的认证和授权过程。如其名所指示，信任和授权策略 222 包括针对在安全环境 200 内信任实体和授权动作的策略。信任和授权策略 222 可例如包括安全策略断言 (未在图 2 明确示出)。授权查询表 224 将诸如访问请求等所请求的动作映射到适当的授权查询。审计策略 226 描绘与在安全环境 200 中实现安全方案 100 有关的审计责任和审计任务。

[0037] 授权上下文 212 从安全令牌 204 收集断言 206，它用于认证进行请求的实体，授权上下文 212 还从信任和授权策略 222 收集安全策略断言。这些收集的断言在授权上下文 212 中形成断言上下文。因此，授权上下文 212 可包括除各种断言以外的其他信息。

[0038] 来自授权上下文 212 的断言上下文和来自授权查询表 224 的授权查询被提供给授权引擎 218。使用断言上下文和授权查询，授权引擎 218 作出授权决策。资源保卫 214 基于授权决策而响应访问请求。审计日志 216 包含审计信息，诸如所请求的资源 110 的标识和 / 或由授权引擎 218 执行的算法求值逻辑。

[0039] 图 3 是示出其中在安全相关组件之间交换示例安全相关数据的示例安全环境 200 的框图。交换安全相关数据以支持示例访问请求操作。在此示例访问请求操作中，实体 208 希望使用应用程序 210 访问资源 110，并用安全令牌 204 指示其这样做的授权。因此，应用程序 210 向资源保卫 214 发送访问请求 *。在图 3 的该描述中，星号 (即“*”) 指示所述安全相关数据在图 3 中明确示出。

[0040] 在所述实现中，实体 208 用令牌 *——安全令牌 204 向资源保卫 214 认证 * 它自己。资源保卫 214 将该令牌断言 * 转发到授权上下文 212。这些令牌断言是安全令牌 204 的断言 206(图 2)。安全策略 220 向资源保卫 214 提供授权查询表 *。授权查询表是从授权查询表模块 224 得到的。发送到资源保卫 214 的授权查询表可被限于与当前访问请求直接相关的一个或多个部分。

[0041] 策略断言是由安全策略 220 从信任和授权策略 222 提取的。策略断言可包括信任

相关断言和授权相关断言两者。安全策略 220 将策略断言 * 转发到授权上下文 212。授权上下文 212 将令牌断言和策略断言组合成断言上下文。如由带圈的“A”所示，从授权上下文 212 向授权引擎 218 提供断言上下文 *。

[0042] 根据授权查询表查明授权查询。资源保卫 214 向授权引擎 218 提供授权查询（授权查询 *）。授权引擎 218 在求值算法中使用授权查询和断言上下文来产生授权决策。授权决策（授权决策 *）被返回给资源保卫 214。实体 208 是否被资源保卫 214 准许访问 * 资源 110 取决于该授权决策。如果授权决策是肯定的，则访问被准许。另一方面，如果由授权引擎 218 发出的授权决策是否定的，则资源保卫 214 不准许实体 208 访问资源 110。

[0043] 授权过程还可使用补充授权过程的语义来审计。审计可能需要监视授权过程和 / 或存储如授权引擎 218 逻辑地执行的求值算法等任何中间和 / 或最终产品。为此，安全策略 220 向授权引擎 218 提供来自审计策略 226 的审计策略 *。至少当请求审计时，可从授权引擎 218 向审计日志 216 转发含有审计信息的审计记录 *。或者，审计信息可经由资源保卫 214 例如作为授权决策的一部分或单独地路由到审计日志 216。

[0044] 图 4 是可用于本文所述的安全相关实现的示例设备 102 的框图。多个设备 102 能够跨一个或多个网络 104 通信。如图所示，两个设备 102(A/B) 和 102(d) 能够经由网络 104 参与通信交换。尽管具体示出两个设备 102，但是也可以取决于实现利用一个或多于两个设备 102。

[0045] 一般而言，设备 102 可标识任何计算机或能够进行处理的设备，诸如客户机或服务器设备；工作站或其他通用计算机设备；PDA；移动电话；游戏平台；娱乐设备；以上参考图 1 列出的设备之一；其某种组合等。如图所示，设备 102 包括一个或多个输入 / 输出 (I/O) 接口 404、至少一个处理器 406 以及一个或多个介质 408。介质 408 包含处理器可执行指令 410。

[0046] 在所述设备 102 的实现中，I/O 接口 404 可包括 (i) 用于跨网络 104 通信的网络接口，(ii) 用于在显示屏上显示信息的显示设备接口，(iii) 一个或多个人机接口等。(i) 网络接口的示例包括网卡、调制解调器、一个或多个端口等。(ii) 显示设备接口的示例包括图形驱动器、显卡、屏幕或监视器的硬件或软件驱动器等。打印设备接口可类似地作为 I/O 接口 404 的一部分被包括。(iii) 人机接口的示例包括那些以有线或无线方式与人机接口设备 402（例如，键盘、遥控器、鼠标或其他图形定点设备等）通信的接口。

[0047] 通常，处理器 406 能够执行、运行、和 / 或以其它方式实现诸如处理器可执行指令 410 等处理器可执行指令。介质 408 由一个或多个处理器可访问介质组成。换言之，介质 408 可包括可由处理器 406 执行以由设备 102 实现功能的执行的处理器可执行指令 410。

[0048] 因此，安全相关实现的实行可以在处理器可执行指令的通用上下文中描述。一般而言，处理器可执行指令包括例程、程序、应用程序、代码、模块、协议、对象、组件、元数据及其定义、数据结构、应用程序编程接口 (API)、模式等，它们执行和 / 或完成特定的任务，和 / 或实现特定的抽象数据类型。处理器可执行指令可以位于单独的存储介质中，由不同的处理器执行，和 / 或通过各种传输介质传播或存在于各种传输介质上。

[0049] 处理器 406 可以使用任何适用的能进行处理的技术来实现。介质 408 可以是作为设备 102 的一部分被包括的和 / 或能被设备 102 访问的任何可用介质。其包括易失性和非易失性介质、可移动和不可移动介质以及存储和传输介质（例如，无线或有线通信信道）。

例如，介质408可以包括用于处理器可执行指令410的长期大容量存储的磁盘/闪存/光介质阵列，用于当前正在执行的指令的短期存储的随机存取存储器(RAM)，用于传输通信（例如，安全相关数据）的网络104上的链路等。

[0050] 如具体示出的，介质408至少包括处理器可执行指令410。一般而言，处理器可执行指令410在由处理器406执行时使设备102能执行本文所述的各种功能，包括在各个流程图中所示的那些动作。仅作为示例，处理器可执行指令410可包括安全令牌204、其断言206的至少其中之一、授权上下文模块212、资源保卫214、审计日志216、授权引擎218、安全策略220（例如，信任和授权策略222、授权查询表224和/或审计策略226等），其某种组合等。尽管未在图4中明确示出，但处理器可执行指令410还可包括应用程序210和/或资源110。

[0051] 安全策略断言语言示例特征

[0052] 本节描述了安全策略断言语言(SecPAL)的实现的示例特征。本节的SecPAL实现是以相对非正式的方式描述的，且仅作为示例。它具有解决创建端对端解决方案时所涉及的大量安全策略和安全令牌职责的能力。作为示例而非限制，这些安全策略和安全令牌职责包括：描述显式信任关系；表达安全令牌发放策略；提供包含身份、属性、能力和/或委托策略的安全令牌；表达资源授权和委托策略等。

[0053] 在所述实现中，SecPAL是用于以灵活且易处理的方式表达安全措施的声明性的基于逻辑的语言。它可以是综合的，且它可提供用于表达信任关系、授权策略、委托策略、身份和属性断言、能力断言、撤销、审计要求等的统一机制。该统一性在使安全方案可理解且可分析方面提供切实的好处。该统一机制还通过允许避免、至少显著减少不同安全技术之间的语义转换和调停的需求而提高安全保证。

[0054] SecPAL实现可包括以下示例特征的任何一个：[1]SecPAL可相对容易地理解。它可使用允许其断言作为英语语句阅读的定义句法。而且，其语法可以是限制性的，使其仅要求用户理解少数具有清楚定义的语义的主语-动词-宾语（例如，主语-动词短语）构造。最后，用于基于断言的集合对可推断事实求值的算法可依赖于少数相对简单的规则。

[0055] [2]SecPAL可在其实现中利用行业标准基础架构以便于其在现有系统中的采用和集成。例如，可使用可扩展标记语言(XML)句法，这是来自形式模型的直接映射。这允许使用标准语法分析器和句法正确性确认工具。它也允许对完整性、来源证明和机密性使用W3C XML数字签名和加密标准。

[0056] [3]SecPAL可通过支持分布式策略授权和合成而允许分布式策略管理。这允许灵活地适应不同的操作模型管控，其中基于所分派的管理责任来创作策略或策略的部分。使用标准方法来数字地签署和加密策略对象使其能够安全分发。[4]SecPAL允许高效且安全的求值。对输入的简单的句法检查足以确保求值将会终止并产生正确的答案。

[0057] [5]SecPAL可提供用于支持所要求的策略、授权决策、审计和用于身份管理的公钥基础架构(PKI)的访问控制要求的完整解决方案。相反，大多数其他方法仅能关注和解决这些安全问题范围内的一个子集。[6]SecPAL出于多个目的可以具有充分的表达力，这些目的包括但不限于：处理网格环境和其他类型的分布式系统的安全问题。以维护语言语义和求值性质同时允许适应特定系统的需求的方式来启用可扩展性。

[0058] 图5是示出用于一般安全方案的示例断言格式500的框图。在本文其他部分描述

的实现中使用的安全方案断言可以不同于示例断言格式500。然而，断言格式500是安全方案断言的一个示例格式的基本图示，且它提供理解一般安全方案的各个方面的所述示例实现的基础。

[0059] 如在断言格式500的最上行所示，概况层的示例断言包括：主体(principal)部分502、说(say)部分504以及主张(claim)部分506。文字上，概括层的断言格式500可被表示为：主体说主张。

[0060] 在断言格式500的下一行，主张部分506被分成示例组成部分。因此，示例主张部分506包括：事实(fact)部分508，如果(if)部分510，“n”个条件事实$_{1...n}$部分508(1...n)以及c部分512。下标“n”表示某一整数值。如图例524所示，c部分512表示约束部分。尽管仅示出单个约束，但c部分512实际上可表示多个约束(例如，c_1，...，c_m)。如果部分510右侧的条件事实部分508(1...n)和约束512(1...m)的集合可被称为前提。

[0061] 文字上，主张部分506可表示为：事实如果事实$_1$，... 事实$_n$，c。因此，整个断言格式500在文字上可如下表示：主体说如果事实$_1$，... 事实$_n$，c，则事实。然而，断言可被简化为：主体说事实。在断言的这一缩写的三部分形式中，略去了以如果部分510开始并延及c部分512的条件部分。

[0062] 每一事实部分508还可被细分成其各个组成部分。示例组成部分有：e部分514和动词短语部分516。如图例524所示，e部分514表示表达式部分。文字上，事实部分508可表示为：e动词短语。

[0063] 每一e即表达式部分514可采用两个示例选择之一。这两个示例表达式选择是：常量514(c)和变量514(v)。主体可归入常量514(c)和/或变量514(v)。

[0064] 每一动词短语部分516也可采用三个示例选择之一。这三个示例动词短语选择是：谓词部分518继之以一个或多个$e_{1...n}$部分514(1...n)、能够断言(can assert)部分520继之以事实部分508、以及别名部分522继之以表达式部分514。文字上，这三个动词短语选择分别可被表示为：谓词$e_1...e_n$、能够断言事实、以及别名e。整数“n”可对事实508(1...n)和表达式514(1...n)取不同的值。

[0065] 一般，SecPAL语句是安全主体作出的断言形式的。安全主体一般由密钥标识，以使其可跨系统边界认证。在其最简单的形式中，断言陈述，主体相信事实是有效的(例如，如由包括事实部分508的主张506所表示)。他们也陈述，如果一个或多个其他事实有效且满足某组条件，则一事实有效(例如，如由从事实部分508延及如果部分510以及条件事实部分508(1...n)到c部分512的主张506所表示)。也可能存在没有任何约束512的条件事实508(1...n)和/或没有任何条件事实508(1...n)的约束512。

[0066] 在所述实现中，事实是关于主体的陈述。在本节中此处描述了四种示例类型的事实陈述。首先，事实可陈述，主体具有用“动作动词”对资源行使动作的权利。示例动作动词包括但不限于：调用、发送、读取、列表、执行、写入、修改、追加、删除、安装、拥有等。资源可由统一资源指示符(URI)或任何其他方法标识。

[0067] 其次，事实可使用“拥有”动词来表达主体标识符与一个或多个属性之间的绑定。示例属性包括但不限于：电子邮件名、通用名、组名、角色头衔、帐户名、域名服务器/服务(DNS)名、网际协议(IP)地址、设备名、应用程序名、组织名、服务名、帐户标识/标识符(ID)等。第三种示例类型的事实是可使用“别名”动词定义两个主体标识符来表示同一主

体。

[0068] “限定词”或事实限定词可作为以上三种事实类型的任一种的一部分而被包括。限定词使得断言者能指示如果认为事实有效则它相信应成立的环境参数（例如，时间、主体位置等）。这样的陈述可基于这些限定词的值在断言者和依赖方的有效性检查之间清楚地分开。

[0069] 第四种示例类型的事实由“能够断言”动词定义。这种“能够断言”动词提供用于表达信任关系和委托的灵活且强大的机制。例如，它允许一个主体 (A) 陈述其相信第二主体 (B) 断言的某些类型的事实的意愿。例如，给定断言“A 说 B 能够断言事实 ()”以及“B 说事实 ()”，可得到 A 相信事实 () 有效的结论从而可推断“A 说事实 ()”。

[0070] 这样的信任和委托断言可以是 (i) 无边界的且是传递的以许可下游委托，或者 (ii) 有边界的以阻止下游委托。尽管可对“能够断言”类型事实应用限定词，但对这些“能够断言”类型事实省略对限定词的支持可显著地简化给定安全方案的语义和求值安全性质。

[0071] 在所述实现中，可陈述具体的事实，或可使用变量写出策略表达式。变量是类型化的，且可以是无限制的（例如，允许匹配正确类型的任何具体值）或有限制的（例如，要求基于指定的模式匹配具体值的子集）。

[0072] 安全授权决策基于针对来自适用的安全策略（例如，安全策略 220）和安全令牌（例如，一个或多个安全令牌 204）的断言集合（例如，断言上下文）的授权查询的求值算法（例如，可在授权引擎 218 处进行的那些算法）。授权查询是组合事实和 / 或条件的逻辑表达式，其可能会变得相当复杂。这些逻辑表达式例如包括对事实的与、或和 / 或非逻辑运算，带有或不带有伴随的条件和 / 或约束。

[0073] 该对授权查询的方法提供用于定义在对给定动作授权之前什么是必须已知且有效的灵活机制。查询模板（例如来自授权查询表 224）形成总的安全方案的一部分，且允许对不同类型的访问请求和其他操作 / 动作声明性地陈述适当的授权查询。

[0074] 安全授权查询的示例实现

[0075] 现有的安全策略语言遵循两种方法之一。某些阻止以任何方式在任何时间使用否定。该方法的确减少了可能因否定而引起的伴随的不一致性和不确定性。然而，它由于呈现了众多太难以处理的安全情形且某些安全情形根本无法处理而也有局限性。另一方法对否定的使用没有施加限制。尽管该方法更为灵活，但它呈现了建立难解甚至非确定性的安全策略的可能性。

[0076] 相比，所述实现创建了具有多层的安全方案。在一分支安全方案实现中，例如有两层。第一层禁止使用否定。这可例如使用对句法的确认来实施。第二层允许使用否定。该分支安全方案将确保安全断言易处理且可确定的安全性和确定性与处理排他安全规则的灵活性组合在一起。

[0077] 图 6 是示出具有第一层和第二层的示例分支安全方案 600 的框图。如图所示，第一层包括断言层 602，第二层包括查询层 604。断言层 602 包括多个断言 606 和句法确认器 614。查询层 604 包括具有多个部分的示例授权查询 616。这多个部分的示例包括但不限于：所断言的事实 608 以及逻辑运算符 610 和 612。

[0078] 在所述实现中，断言层 602 以断言 606 填充。断言 606 可以是断言层处任何类型的声明性安全陈述。断言 606 的示例包括但不限于：令牌断言和策略断言。（这两个断言

类型在图 7 中分开且明确地示出。）在安全断言 606 内不允许否定。句法确认器 614 分析每一断言 606 以检查是否存在否定。如果在给定断言 606 内存在否定，则拒绝或不允许给定断言 606。

[0079] 查询层 604 以诸如示例授权查询 616 等授权查询填充。查询层 606 的授权查询被允许包括否定，诸如非运算符 612。授权查询可按照任何方式结构化。尽管未在图 6 中明确示出，但授权查询一般可包括一个或多个逻辑约束。

[0080] 在示例授权查询 616 中，查询被结构化成布尔逻辑运算。这样的布尔逻辑运算可包括任何数目的所断言的事实 608、任何数目的逻辑运算符等。这些所断言的事实、逻辑运算符等可按照任何方式组合。示例逻辑运算符包括但不限于 ：与、或、非等。如图所示，示例授权查询 616 包括 ：三个所断言的事实 608、两个与运算符 610、一个非运算符 612。

[0081] 所断言的事实 608 是否为真取决于是否可推断出有效的匹配断言 606。当该匹配判断过程完成之后，即对得到的逻辑布尔运算求值。在示例授权查询 616 的情况中，在应用与运算符 610 之前，对最右端的所断言的事实 608 的真 / 假判定应用非运算符 612。如果整个布尔运算求值为真，则授权决策是肯定的。如果布尔运算的总的求值为假，则授权决策是否定的。

[0082] 断言 606 和授权查询（例如，示例授权查询 616）之间的示例相互关系以下在图 7-10 的描述中呈现。响应于请求来查明授权查询，该请求可包括一个或多个断言 606 或以其他方式与这些断言相关联。然后结合包括断言 606 在内的总的断言上下文对授权查询求值。断言上下文一般包括令牌断言和策略断言。

[0083] 图 7 是示出示例授权查询查明和示例授权查询求值的一般框图 700。框图 700 包括来自图 2 和 3 的多个安全相关组件。如图所示，它包括授权上下文 212、资源保卫 214、授权引擎 218 以及安全策略 220。安全策略 220 包含授权查询表 224。授权引擎 218 包括求值算法 708。

[0084] 在所述实现中，授权上下文 212 包括断言上下文 702。断言上下文 702 是断言 606 的集合。具体地，断言上下文 702 包括令牌断言 606T 和策略断言 606P。令牌断言 606T 从安全令牌（例如，图 2 和 3 的安全令牌 204）得到。安全令牌可作为资源访问请求的一部分和 / 或随之一起传递。策略断言 606P 从信任和授权策略（例如，安全策略 220（图 2）的信任和授权策略 222 模块）得到。

[0085] 断言上下文 702 被转发到资源保卫 214。向资源保卫 214 呈现请求 704。请求 704 是访问某一资源的请求。资源保卫 214 将请求转换成操作。该操作被提供给授权查询表 224。授权查询表 224 将资源专用操作映射到授权查询。在一示例实现中，每一操作与单个授权查询相关联。响应于所提供的操作，安全策略 220 查明相关联的授权查询 706，并将授权查询 706 返回到资源保卫 214。使用授权查询表 224 查明授权查询 706 在本文中以下具体参考图 8 进一步描述。

[0086] 因此，资源保卫 214 包括断言上下文 702 和授权查询 706 两者。资源保卫 214 将断言上下文 702 和授权查询 706 转发到授权引擎 218 的求值算法 708。求值算法 708 包括能够结合断言上下文 702 对授权查询 706 求值的逻辑。该逻辑可用硬件、软件、固件、其某种组合等实现。

[0087] 因此，断言上下文 702 在求值算法 708 中应用于授权查询 706。在逻辑分析之后，

求值算法 708 产生授权决策 710。结合断言上下文 702 对授权查询 706 求值在本文中以下具体参考图 9 进一步描述。

[0088] 一般而言，具有如本文所述的特征的安全语言使得复杂的访问控制准则能以声明性的方式编写起来相对简单且理解起来相对简单。它与展示基于输入策略和经认证的请求者数据推断的有效事实集的任何授权算法兼容。如本文中进一步描述的，它基于结合断言上下文与授权决策算法组合的授权查询的概念。

[0089] 在所述实现中，一般，授权查询包括所断言的事实集以及约束。所断言的事实是“A 说事实”形式的。它们表达可以（例如，从断言上下文）推断匹配的有效断言的要求。如果这一匹配的有效断言已知，则所断言的事实得到满足，且求值为布尔值真；否则，它求值为假。（在某些实现中，事实的断言者可基于求值上下文隐含地已知。在这些情况中，它可被略去。）约束是返回布尔值的表达式。它可包括在所断言的事实以及对环境值（例如，时间、位置等）的引用中使用的变量。约束一般用于表达变量等同性和不等同性。

[0090] 每一查询中存在至少一个所断言的事实。如果存在多个所断言的事实，则它们可使用诸如与、或和非等逻辑运算符组合。可任选的约束与所断言的事实进行逻辑与。

[0091] 该方法的结果是基本访问控制策略可按照关于每一主体被授权的访问的肯定陈述来写出，而不顾及较高层的结构要求。因此，在多主体策略中，可编写陈述每一主体对资源应潜在具有何种权限的每一策略。这样的安全策略就添加新策略陈述不会移除任何现有的访问权限而言是单调的。而且，可编写指示主体对资源集具有何种权限的肯定访问策略而不必顾虑潜在的冲突或不一致性。授权查询提供用于组合这些访问控制规则的较高层语义。

[0092] 例如，如果为对“Foo”准许读访问而要求 (i) 用户具有电子邮件地址“fabrikam.com”，以及 (ii) 应用程序具有代码摘要值“ABC”，则访问控制规则可写为如下：

[0093] A 说如果 p 拥有 r{(电子邮件名，*@fabrikam.com)} 则 p 读 Foo

[0094] A 说如果 p 拥有 r{摘要，ABC} 则 p 读 Foo

[0095] 为确保用户和应用程序均是经认证的请求者，一个示例授权查询为：

[0096] A 说 v1 读 Foo 与 A 说 v1 拥有 r{(电子邮件名，*)} 与 A 说 v2 读 Foo 与 A 说 v2 拥有 (摘要，*)}

[0097] 类似地，为要求具有电子邮件地址“fabrikam.com”的两个授权的主体请求访问“Foo”，可写出以下安全策略：

[0098] A 说如果 p 拥有 r{(电子邮件名，*@fabrikam.com)} 则 p 读 Foo，

[0099] 且它可与以下授权查询组合：

[0100] A 说 p1 读 Foo 与 A 说 p2 读 Foo 与 (p1 ！ ＝ p2)。

[0101] 在以上授权查询中，指示“p1”变量不等于“p2”变量的部分是约束。

[0102] 拒绝或排除可使用该方法来适当处理。例如，如果给定组 A 的成员能读访问 Foo，且组 B 的成员能读访问 Bar，但不允许同时访问。可用带有如下的两个策略断言的安全策略启用所需访问：

[0103] A 说如果 p 拥有 r{组，A} 则 p 读 Foo

[0104] A 说如果 p 拥有 r{组，B} 则 p 读 Bar。

[0105] 然后可使用以下授权查询实施排除：

[0106] (A 说 v 读 Foo 或 A 说 v 读 BAR) 与非 (A 说 v 读 Foo 与 A 说 v 读 BAR)。

[0107] 以类似方式，可排除同时承担两个角色、同时对给定资源具有多个访问权（例如，读和删除）等。

[0108] 图 8 是示出响应于资源访问请求 704 的示例授权查询查明 800 的更具体的框图。如图所示，授权查询查明 800 包括具有所标识的资源 802 的请求 704、转换功能 804、操作 806、授权查询表 224 和授权查询 706。授权查询查明 800 涉及接收请求 704 作为输入，以及产生相关联的授权查询 706 作为输出。

[0109] 在所述实现中，请求 704 是访问某一所标识的资源 802 的请求。请求 704 经由转换功能 804 被转换成资源专用操作 806。该转换功能 804 例如可由资源保卫 214（图 7）执行。资源专用操作的示例作为示例而非限制包括：(i) 对文件读和 / 或写，(ii) 通过通信端口发送数据，(iii) 利用处理器，(iv) 执行应用程序等。

[0110] 一般而言，操作 806 被提供给授权查询表 224。例如，安全策略 220 可负责将操作 806 应用于授权查询表 224 并检索相关联的授权查询 706。作为结果产生授权查询 706，并将其返回给资源保卫 214。

[0111] 更具体地，授权查询表 224 包括多个字段 808。每一字段 808 将资源专用操作映射到相关联的授权查询模板。如图所示，在授权查询表 224 中有“f”个字段 808(1)、808(2)...808(f)，f 是某一整数。检索到的授权查询模板被返回给资源保卫 214。资源保卫 214 然后执行代入过程以产生授权查询 706。换言之，为创建授权查询 706，资源保卫 214 将实际进行请求的主体、实际所请求的资源等代入相关联授权查询模板的预定的相应槽中。

[0112] 图 9 是示出给定断言上下文 702^* 情况下的示例授权查询求值 708^* 的更具体的框图。如以上参考图 7 概括描述，求值算法 708 接收授权查询 706 和断言上下文 702。在图 9 的具体示例授权求值 708^* 中，结合具体示例断言上下文 702^* 对具体示例授权查询 706^* 求值。实际断言上下文 702、授权查询 706 和求值算法 708 可与这些示例不同。

[0113] 如图所示，示例授权查询求值 708^* 包括示例断言上下文 702^*、示例授权查询 706^*、得到的布尔运算 910 和答案 912。断言上下文 702^* 包括 (i) 三个令牌断言 606T-1、606T-2 和 606T-3，以及 (ii) 两个策略断言 606P-1 和 606P-2。示例授权查询 706^* 包括三个所断言的事实 608-1、608-2 和 608-3；两个与运算符 610；一个非运算符 612；以及一个约束 902。

[0114] 在求值期间，授权引擎 218（图 7）试图确定是否可对授权查询 706^* 的每一所断言的事实 608 推断有效的匹配断言 606。该匹配判定过程可以是迭代的、递归的、和 / 或在一个有效断言导致另一可能有效的断言时为分叉的。在某一预定时间段之后，匹配判断过程收敛。

[0115] 图 9 的示例授权查询求值 708^* 示出了便于大体理解对授权查询求值的概念基础的简化的求值算法。更具体且技术上准确的说明以下在图 9 的描述之后呈现。而且，一个示例实现的相对严格的逻辑描述在本文中以下在图 10 的描述之后呈现。

[0116] 在示例授权查询求值 708^* 中，授权引擎 208 确定令牌断言 606T-2 是有效的且匹配 904 所断言的事实 608-1。还确定策略断言 606P-2 是有效的且匹配 906 所断言的事实 608-2，令牌断言 606T-3 是有效的且匹配 908 所断言的事实 608-3。尽管令牌断言 606T-1 和策略断言 606P-1 未明确匹配特定的所断言的事实 608，但它们可能已在匹配判定过程中使用了。另外，关于约束 902 作出真 / 假判断。

[0117] 在匹配判断过程之后和 / 或期间，执行真 / 假替换过程以创建布尔运算 910。如果特定的所断言的事实 608 具有匹配的有效断言 606，则用“真”替换特定的所断言的事实 608。如果不是，则用“假”替换该特定的所断言的事实 608。同样地，用其确定的“真”或“假”状态替换任何约束 902。尽管未对授权查询 706* 明确示出，但约束 902 与授权查询的其余部分进行逻辑与。

[0118] 例如，授权查询求值 708*、授权查询 706* 在文字上可如下表示 :所断言的事实 608-1，与运算符 610，所断言的事实 608-2，与运算符 610，非运算符 612，所断言的事实 608-3，以及约束 902。在替换过程之后，得到的布尔运算在文字上可如下表示 :真与真与非真与真。这可缩减成 :真与真与假与真，这是逻辑假。

[0119] 结果，布尔运算 910 的答案 912 为“假”。因此，授权决策 710 是拒绝请求。另一方面，如果例如对所断言的事实 608-3 没有匹配 908 断言 606，则布尔运算 910 将被缩减成 :真与真与真与真，这是逻辑真。在这种情况中，答案 912 将为“真”，且授权决策 710 将是允许请求。尽管未明确示出或描述，但存在布尔运算 910 将求值为逻辑假的其他排列 (例如，如果确定对所断言的事实 608-2 没有有效且匹配 906 的断言 606)。

[0120] 此处描述用于对授权查询求值的技术上更为准确的示例实现。首先，一次一个地对授权查询内的所断言的事实求值，而不必在完整的替换过程之前一次对所有事实进行。其次，授权查询内单个所断言的事实的求值返回使该所断言的事实为真的变量代入集。因此，一般而言，所返回的值不是立即为真 / 假状态，因为事实实际上被表示具有关于给定变量代入的真 / 假状态。

[0121] 如果授权查询内的两个所断言的事实之间的连接词为与 (如图 9 的示例中的情况)，则左边事实所返回的值 (即，该代入集) 被应用于右边的事实。之后，按需对右边的事实求值。得到的代入集然后通过代入合成来组合。对整个授权查询求值的结果是代入集，代入集的每一代入能够使授权查询为真。

[0122] 图 10 是示出用于查明授权查询并对其求值的方法的示例的流程图 1000。流程图 1000 包括十一 (11) 个框 1002-1022。尽管可在其他环境中以及采用各种硬件 / 软件 / 固件组合来执行流程图 1000 的动作，但使用图 1-9 的某些特征、组件和方面来示出该方法的示例。例如，资源保卫 214、授权查询表 224 和 / 或授权引擎 218 可单独或共同实现流程图 1000 的动作。

[0123] 在所述实现中，在框 1002，接收访问资源的请求。例如，可接收标识资源 802 的请求 704。在框 1004，将请求转换成对资源的操作。例如，资源保卫 214 可将请求 704 转换 804 成资源专用操作 806。

[0124] 在框 1006，操作被提供给授权查询表。例如，资源专用操作 806 可被提供给授权查询表 224。在框 1008，查明与该操作相关联的授权查询。例如，可定位包括资源专用操作 806 的字段 808。然后可从所定位的字段 806 检索相关联的授权查询。

[0125] 更具体地，检索到的授权查询可包括授权查询模板。基于由请求者提供的安全令牌，相关联的授权查询模板通过将实际的主体、资源等代入到授权查询模板的预定相应槽中而被转化成授权查询。在一示例实现中，了解来自请求 704 的实际变量信息的资源保卫 214 通过代入执行该转化。

[0126] 在框 1010，在求值算法中组合断言上下文和授权查询。例如，断言上下文 702 和授

权查询 706 可被共同提交给求值算法 708。

[0127] 在框 1012，在匹配判定过程中，断言上下文的有效断言被匹配到授权查询的所断言的事实。例如，在匹配判定过程中，被发现为有效的、可从断言上下文 702 推断（即，原始存在于其中和 / 或以其他方式从其得到）的一个或多个令牌断言 606T 和 / 或策略断言 606P 可试图匹配 904/906/908 到所断言的事实 608。还分析授权查询 706 的任何约束部分 902 以确定它们是真还是假。如以上在技术描述中所述，可单独和 / 或顺序分析每一断言。

[0128] 在框 1014，响应于匹配判定过程执行对授权查询的真 / 假替换。例如，在布尔运算 910 中，被确定为具有有效匹配断言 606 的所断言的事实 608 可用真替换，而未被确定为具有有效匹配断言 606 的所断言的事实 608 可用假替换。应理解，框 1014 的动作可按照与框 1012 的动作的执行全部或部分重叠的方式执行。

[0129] 在框 1016，对授权查询逻辑求值。例如，可作为求值算法 708 的一部分对布尔运算 910 逻辑求值，以确定其答案为真还是假。应理解，布尔运算 910 的结果无需用真或假状态替换每一所断言的事实 608 和 / 或约束 902 就可被确定，而且确实被确定。

[0130] 在框 1018，确定授权查询逻辑求值是否为“真”。如果是，则框 1020 处的授权决策是该请求被准许。另一方面，如果确定授权查询逻辑求值为“假”，则框 1022 处的授权决策是请求被拒绝。应理解，可能具有“真”状态的授权查询的算法求值可返回使授权查询为“真”的一组变量。

[0131] 也可从相对严格的逻辑观点描述安全授权查询。在安全授权查询的所述逻辑实现中，通过查询包含本地以及导入的断言的断言上下文来决定授权请求。在一示例实现中，授权可包括 A 说事实形式的原子查询和约束 c 的集合。这些原子查询和约束由包括否定在内的逻辑连接词组合。示例逻辑连接词包括以下：

[0132] q:: = e 说事实

[0133] $|q_1, q_2$

[0134] $|q_1$ 或 q_2

[0135] | 非 (q)

[0136] |c

[0137] 得到的查询语言比其中仅考虑原子查询的其他基于逻辑的语言表达力更强。例如，可通过将原子查询与否定和约束组合来表达责任的分离、阈值和拒绝策略。在语言的断言层不允许否定，因为将否定和递归语言耦合会导致语义的歧义，且通常导致计算更为复杂甚至不可判定。通过将否定的使用限于授权查询层（而非将这些特征添加到断言语言本身），将否定与递归有效地分开，从而绕开了与否定通常相关联的问题。

[0138] 查询的语义由关系$AC,\theta \vdash q$限定。以下，令 AC 为断言上下文。而且，令 θ 为代入，令 ε 为空代入。令 Dom(θ) 为代入 θ 的域。如果 X 是句法短语，则令 Vars(X) 为 X 中出现的变量集。授权查询的示例形式语义如下：

[0139] $AC,\theta \vdash e$ 说事实　　如果 e θ 说事实 θ 可从 AC 推断，

[0140] 且$Dom(\theta) \subseteq Vars(e \text{ 说事实})$

[0141] $AC,\theta_1\theta_2 \vdash q_1, q_2$　　如果$AC,\theta_1 \vdash q_1$且$AC,\theta_2 \vdash q_2\theta_1$

[0142] $AC,\theta \vdash q_1$ 或 q_2　　如果$AC,\theta \vdash q_1$或$AC,\theta \vdash q_2$

[0143] $AC,\varepsilon \vdash$非(q) 如果$AC,\varepsilon \vdash q$不成立且$Vars(q) = \emptyset$

[0144] $AC,\varepsilon \vdash c$ 如果$Vars(c) = \emptyset$且 c 是有效的。

[0145] 给定查询 q 和授权上下文 AC，授权算法返回代入 θ 的集合，使得$AC,\theta \vdash q$。如果查询不包含变量 (ground)，则答案集或者为空（意味着“不”，请求被拒绝）或包含空代入 ε 的单元素集（意味着“是”，请求被准许）。如果查询包含变量，则答案集中的代入是使查询为真的变量赋值。

[0146] 关于授权查询表，它们可以是本地安全策略的一部分，且可与命令性代码保持分开。该表通过将参数化的方法名映射到查询而提供对授权查询的接口。在请求时，资源保卫调用由该表映射到授权查询的方法（例如，代替直接发出查询），该查询然后用于查询断言上下文。

[0147] 例如，授权查询表可包含以下示例映射：

[0148] canAuthorizePayment（请求者，支付）：

[0149] 管理员说请求者拥有 BankManagerID id，

[0150] 非（管理员说请求者已启动支付）。

[0151] 如果 Alice 试图对支付 Payment47 授权，则资源保卫调用 canAuthorizePayment(Alice，Payment47)，这触发以下查询：

[0152] 管理员说 Alice 拥有 BankManagerID id，

[0153] 非（管理员说 Alice 已启动 Payment47)。

[0154] 得到的答案集（例如，或者是请求应被拒绝的情况下的空集，或者是 id 的变量赋值）被返回给资源保卫，后者然后可实施策略。

[0155] 也可从相对严格的逻辑观点描述安全授权查询的形式求值。以下描述假定存在另一算法，该算法返回对其从授权上下文 AC 可推断出“e 说事实”形式的给定陈述的代入集。这样的算法例如可依赖于将 AC 转换成诸如 Datalog 等另一逻辑语言。对授权查询定义函数 $AuthAns_{AC}$，如下：

[0156]

$$AuthAns_{AC}(e\ 说\ fact) = \{\theta \mid e\theta\ 说事实\theta\ 可从\ AC\ 推断$$
$$且\ Dom(\theta) \subseteq Vars(e\ 说事实)\}$$

[0157] $AuthAns_{AC}(q_1, q_2) = \{\theta_1\theta_2 \mid \theta_1 \in AuthAns_{AC}(q_1)\ 且\ \theta_2 \in AuthAns_{AC}(q_2\theta_1)\}$
$AuthAns_{AC}(q_1\ 或\ q_2) = AuthAns_{AC}(q_2) \cup AuthAns_{AC}(q_2)$

[0158]

$$AuthAns_{AC}(非(q)) = \{\varepsilon\} \quad 如果\ Vars(q) = \emptyset\ 且\ AuthAns_{AC}(q) = \emptyset$$

[0159]

$$= \emptyset \quad 如果\ Vars(q) = \emptyset\ 且\ AuthAns_{AC}(q) \neq \emptyset$$

[0160]

$$= 未定义，其他$$

[0161]

$$AuthAns_{AC}(c) = \{\varepsilon\} \quad 如果\ Vars(c) = \emptyset\ 且\ c\ 有效$$

[0162]

$= \emptyset$ 如果 $Vars(c) = \emptyset$ 且 c 不是有效的

[0163]

= 未定义，其他

[0164] 以下定理示出 $AuthAns_{AC}$ 是用于对安全授权查询求值的算法。该定理表示授权查询求值的有限性、可靠性和完全性：对所有安全断言上下文 AC 和安全授权查询 q，

[0165] 1. $AuthAns_{AC}(q)$ 被定义且是有限的，且

[0166] 2. $AC, \theta \vdash q$ 当且仅当 $\theta \in AuthAns_{AC}(q)$。

[0167] 图 1-10 中的设备、动作、方面、特征、功能、过程、模块、数据结构、协议、组件等都在分为多个框的示意图中得到阐明。然而，描述和 / 或示出图 1-10 的次序、互连、相互关系、布局等不旨在被解释为限制，任何数目的这些框可按照任何方式被修改、组合、重新排列、增加、省略等，以实现用于安全授权查询的一个或多个系统、方法、设备、过程、介质、装置、API、协议、安排等。

[0168] 尽管系统、介质、设备、方法、过程、装置、机制、方案、途径、进程、安排、以及其它实现都用专用于结构、逻辑、算法、以及功能特征和 / 或示意图的语言加以描述，但是应该理解在所附权利要求中定义的本发明不必限于以上描述的具体特征或动作。相反，上述具体特征和动作是作为实现权利要求的示例形式公开的。

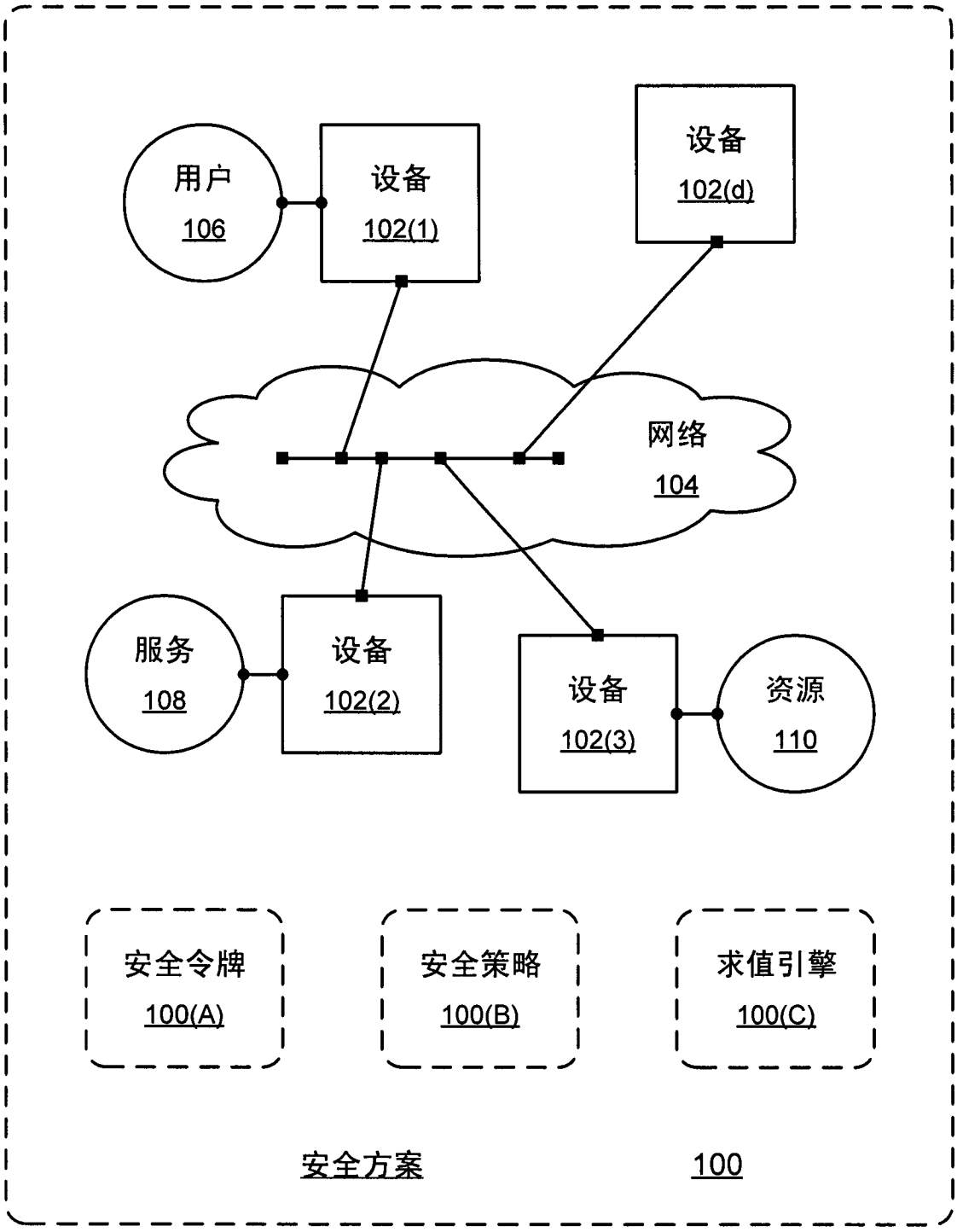

用户
106
设备
102(1)
设备
102(d)
网络
104
服务
108
设备
102(2)
设备
102(3)
资源
110
安全令牌
100(A)
安全策略
100(B)
求值引擎
100(C)
安全方案
100

图 1

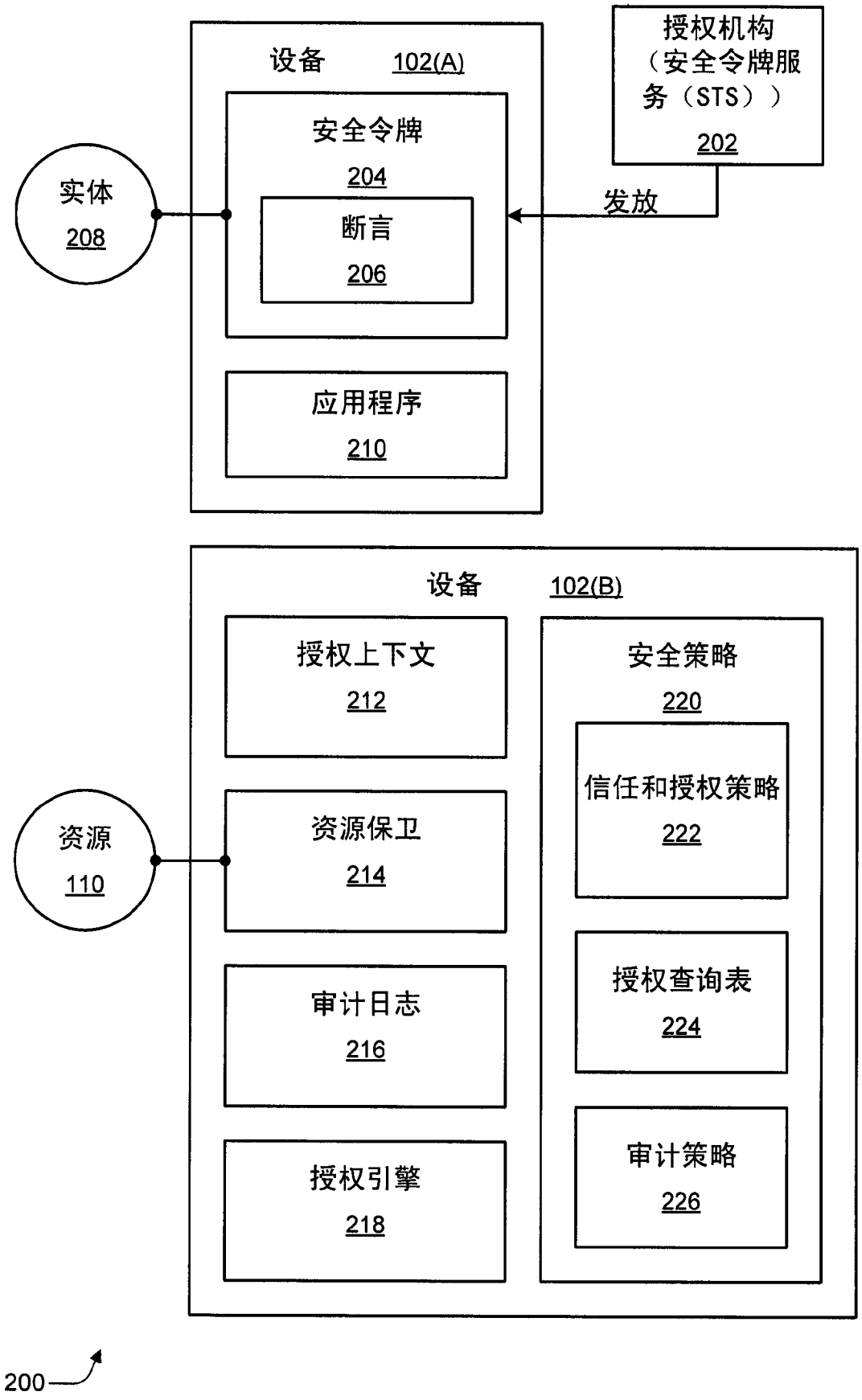

设备 102(A)
安全令牌
204
断言
206
应用程序
210
实体
208
授权机构
（安全令牌服务（STS））
202
发放
设备 102(B)
授权上下文
212
资源保卫
214
审计日志
216
授权引擎
218
安全策略
220
信任和授权策略
222
授权查询表
224
审计策略
226
资源
110
200

图 2

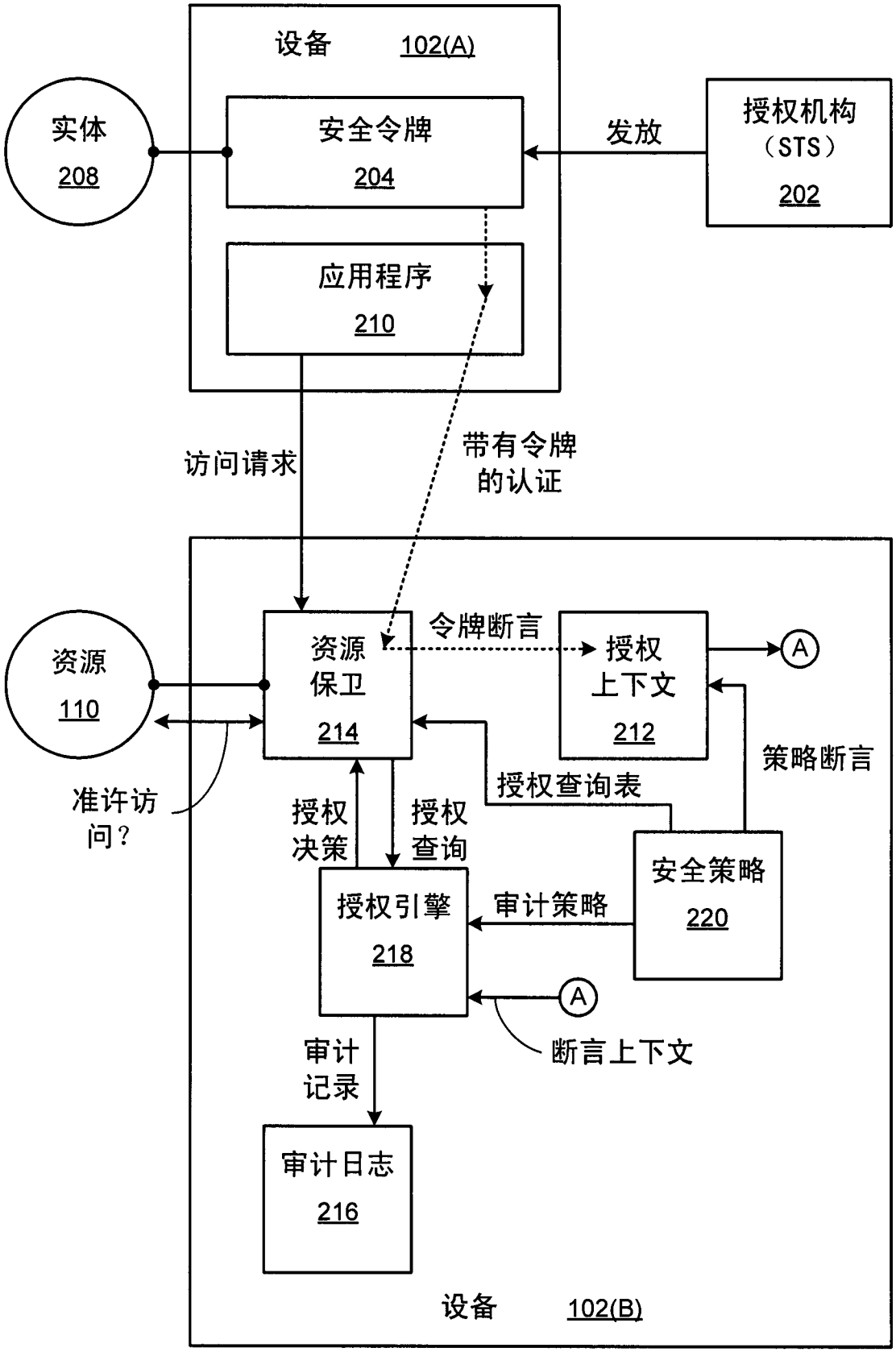

设备 102(A)
实体 208
安全令牌 204
发放
授权机构 (STS) 202
应用程序 210
访问请求
带有令牌的认证
资源 110
资源保卫 214
令牌断言
授权上下文 212
A
策略断言
授权查询表
准许访问？
授权决策
授权查询
安全策略 220
授权引擎 218
审计策略
A
断言上下文
审计记录
审计日志 216
设备 102(B)

图 3

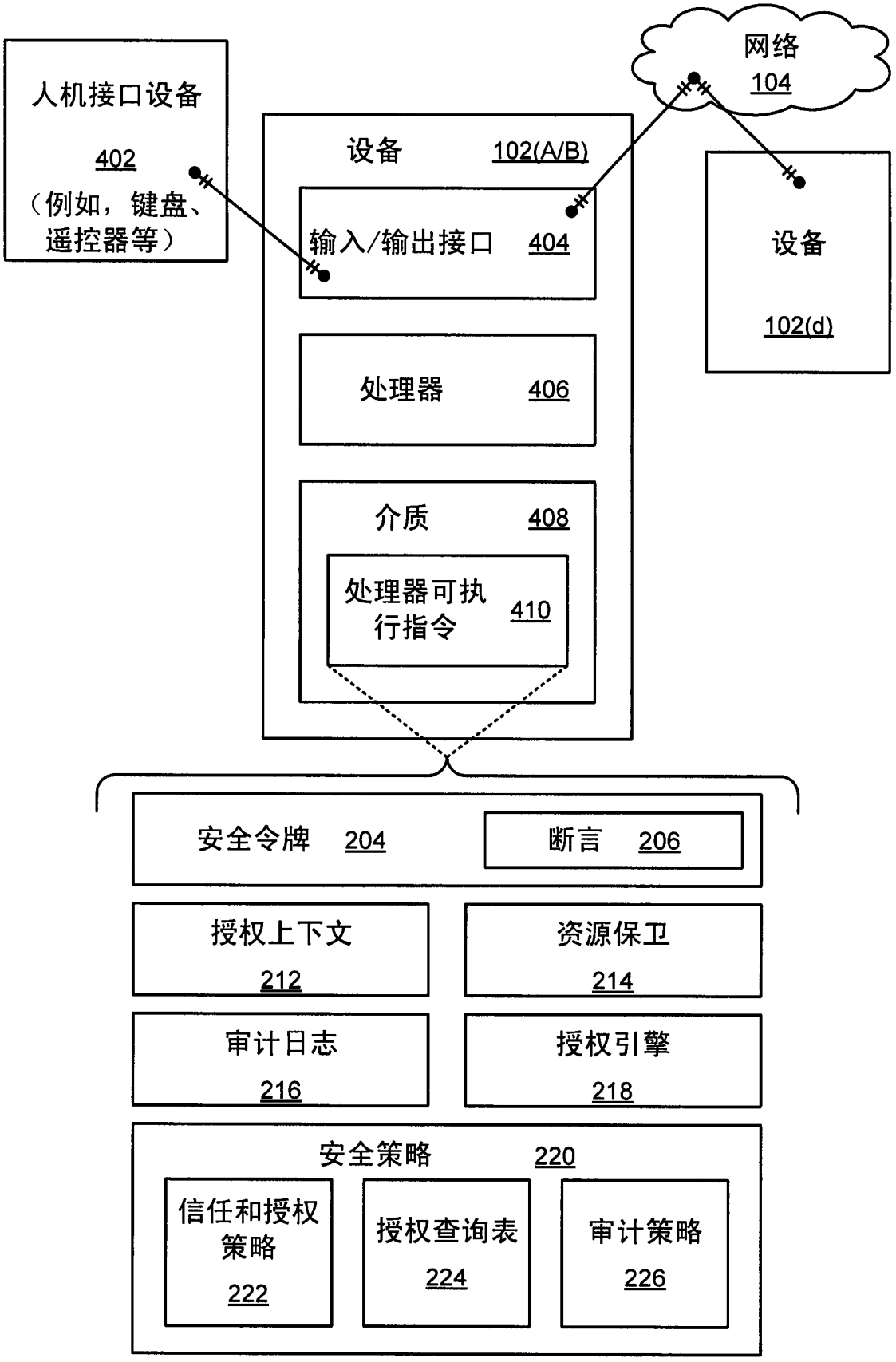
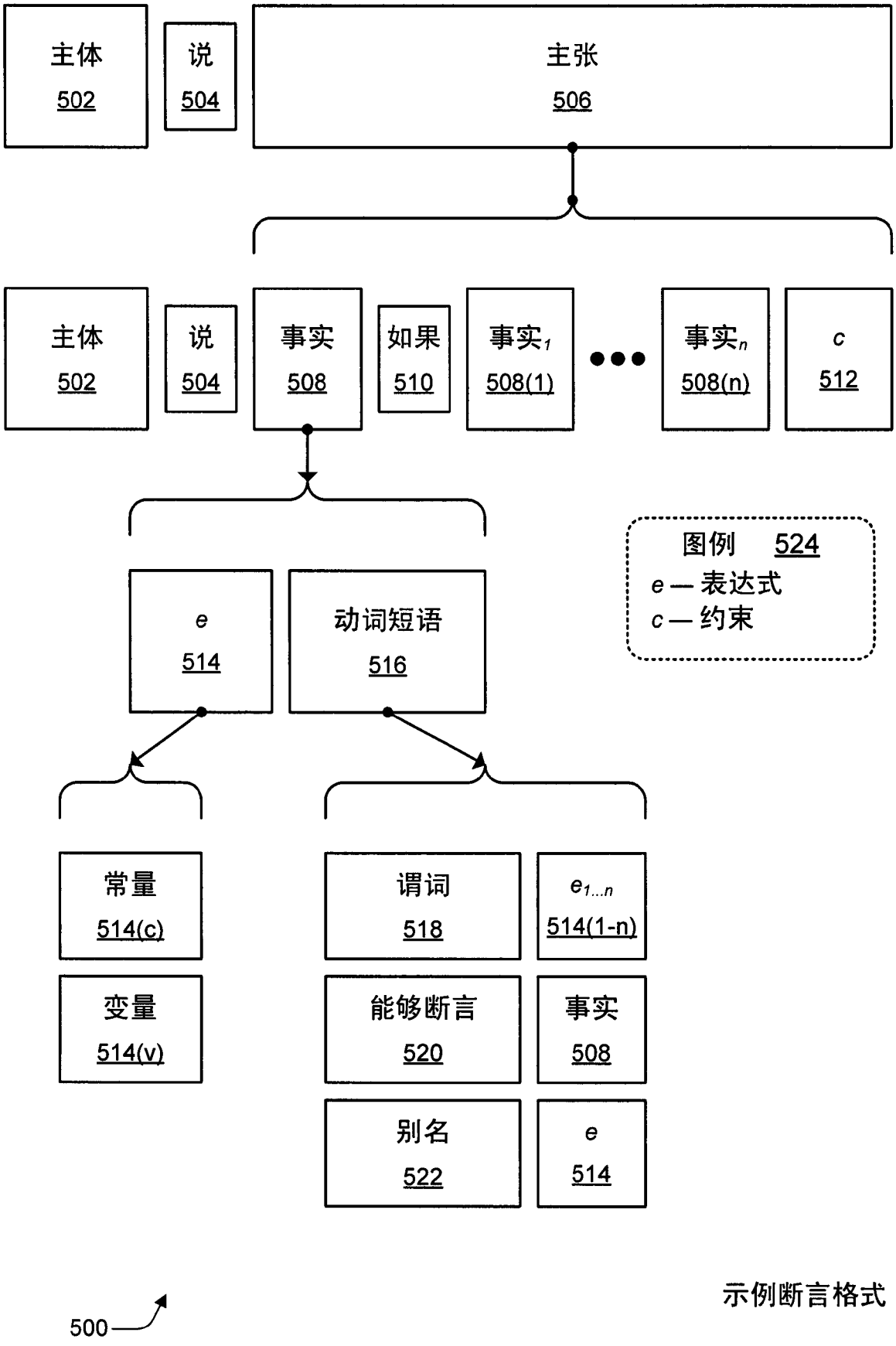

网络
104
人机接口设备
402
（例如，键盘、遥控器等）
设备 102(A/B)
输入/输出接口 404
设备
102(d)
处理器 406
介质 408
处理器可执行指令 410
安全令牌 204
断言 206
授权上下文
212
资源保卫
214
审计日志
216
授权引擎
218
安全策略 220
信任和授权策略
222
授权查询表
224
审计策略
226

图 4


主体
502
说
504
主张
506
主体
502
说
504
事实
508
如果
510
事实1
508(1)
事实n
508(n)
c
512
图例 524
e — 表达式
c — 约束
e
514
动词短语
516
常量
514(c)
变量
514(v)
谓词
518
e1...n
514(1-n)
能够断言
520
事实
508
别名
522
e
514
500

示例断言格式

图 5

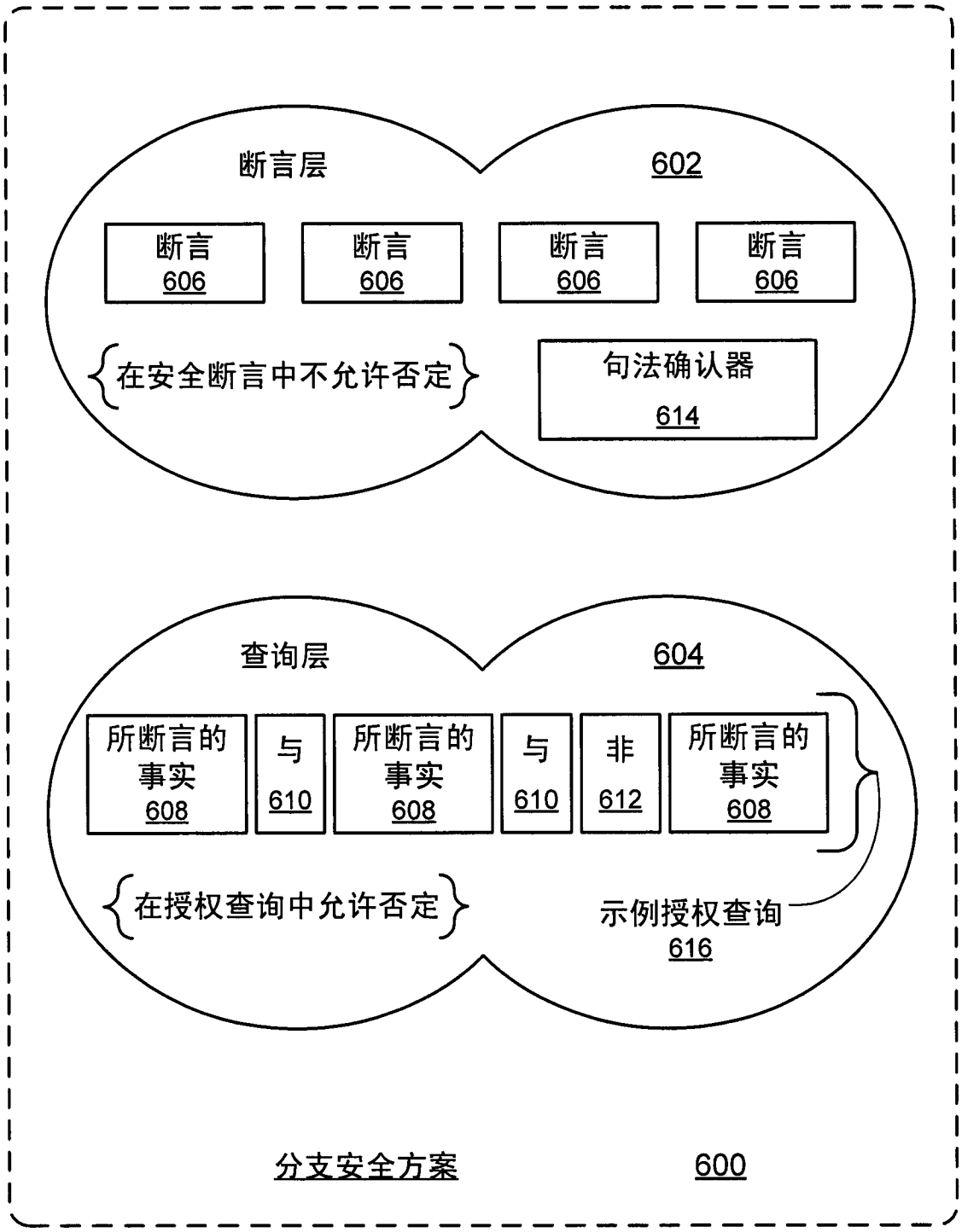
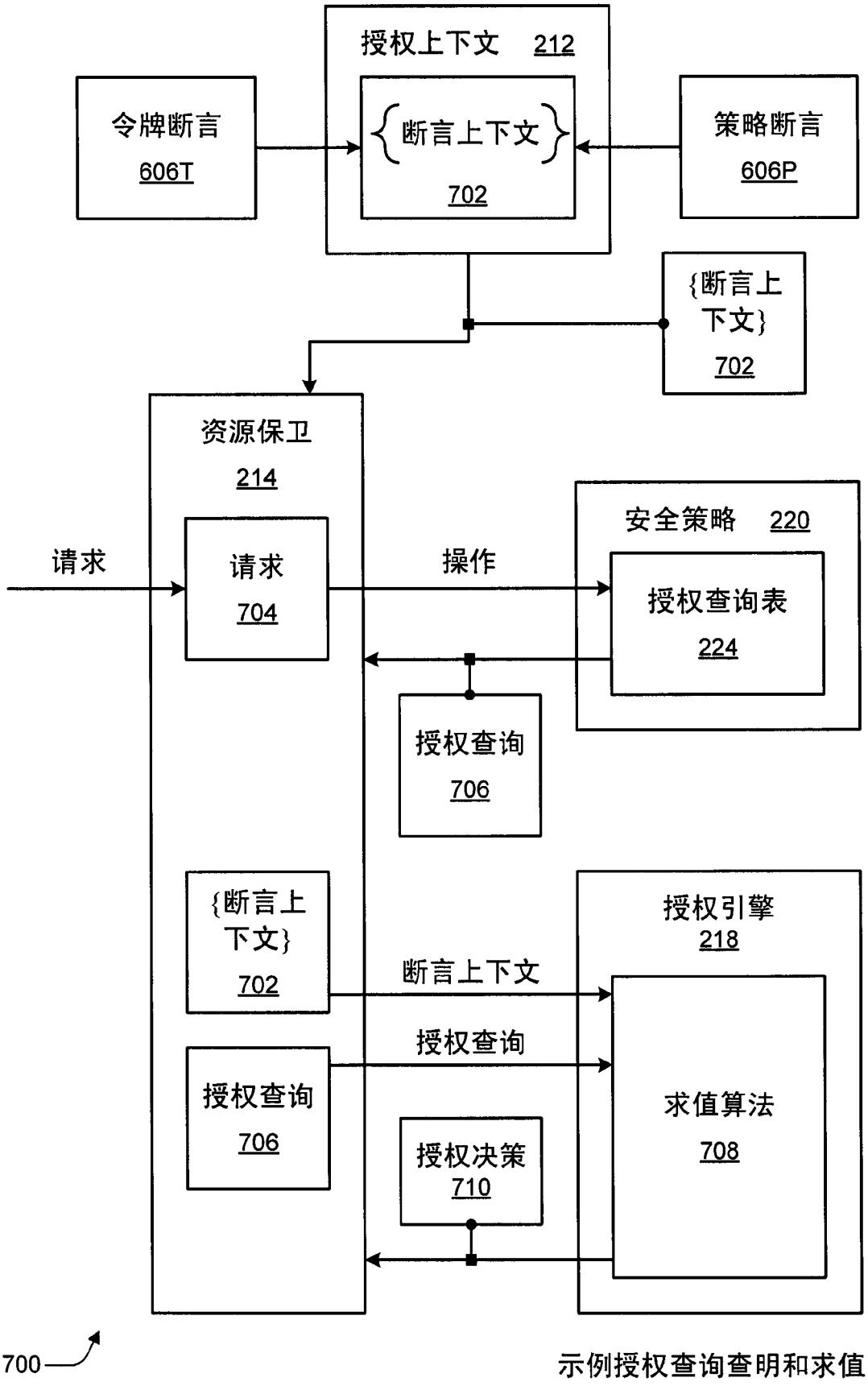

断言层
602
断言
606
断言
606
断言
606
断言
606
在安全断言中不允许否定
句法确认器
614
查询层
604
所断言的
事实
608
与
610
所断言的
事实
608
与
610
非
612
所断言的
事实
608
在授权查询中允许否定
示例授权查询
616
分支安全方案
600

图 6



示例授权查询查明和求值

图 7

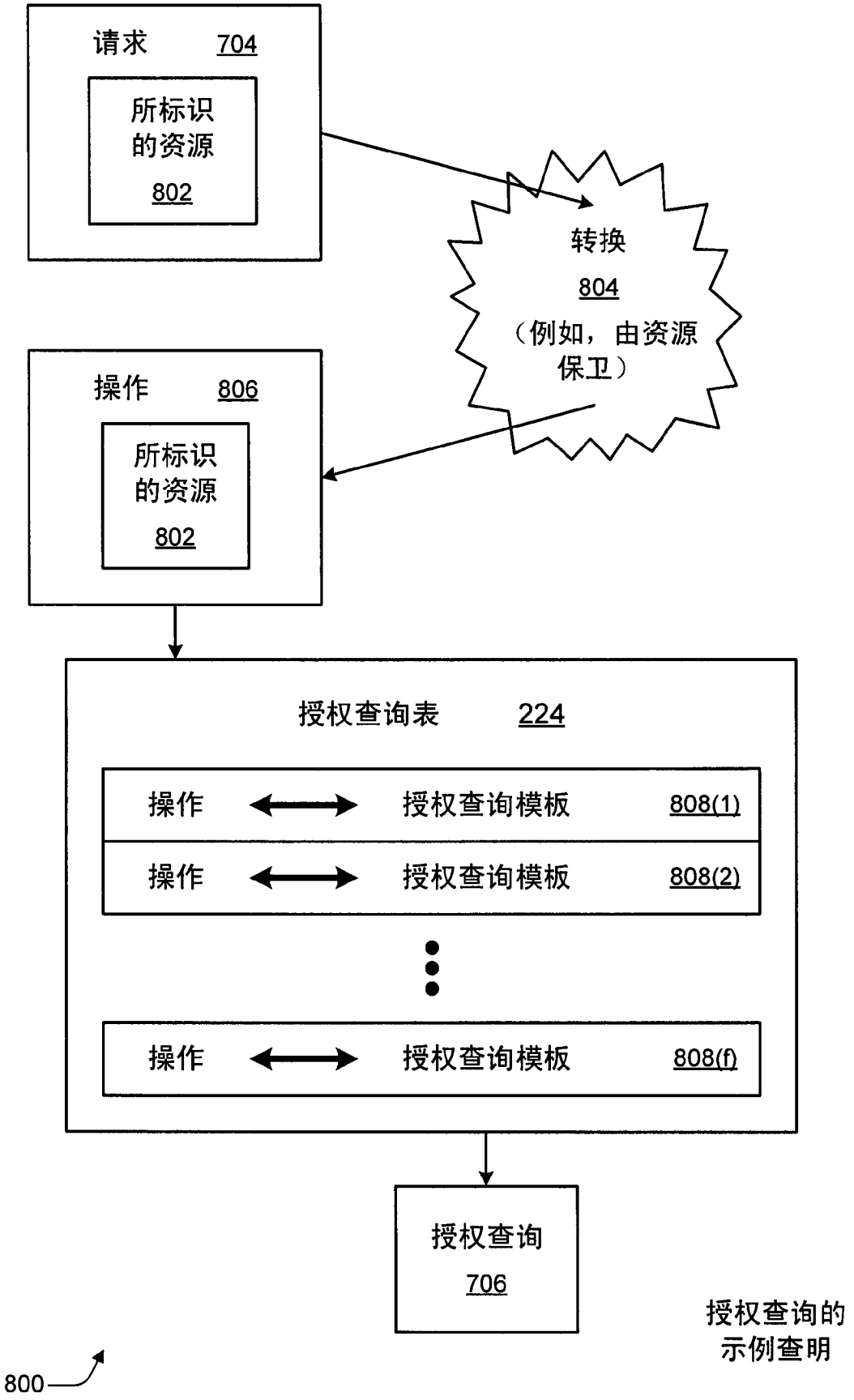

请求 704
所标识的资源 802
转换 804 （例如，由资源保卫）
操作 806
所标识的资源 802
授权查询表 224
操作 授权查询模板 808(1)
操作 授权查询模板 808(2)
操作 授权查询模板 808(f)
授权查询 706
800
授权查询的示例查明

图 8

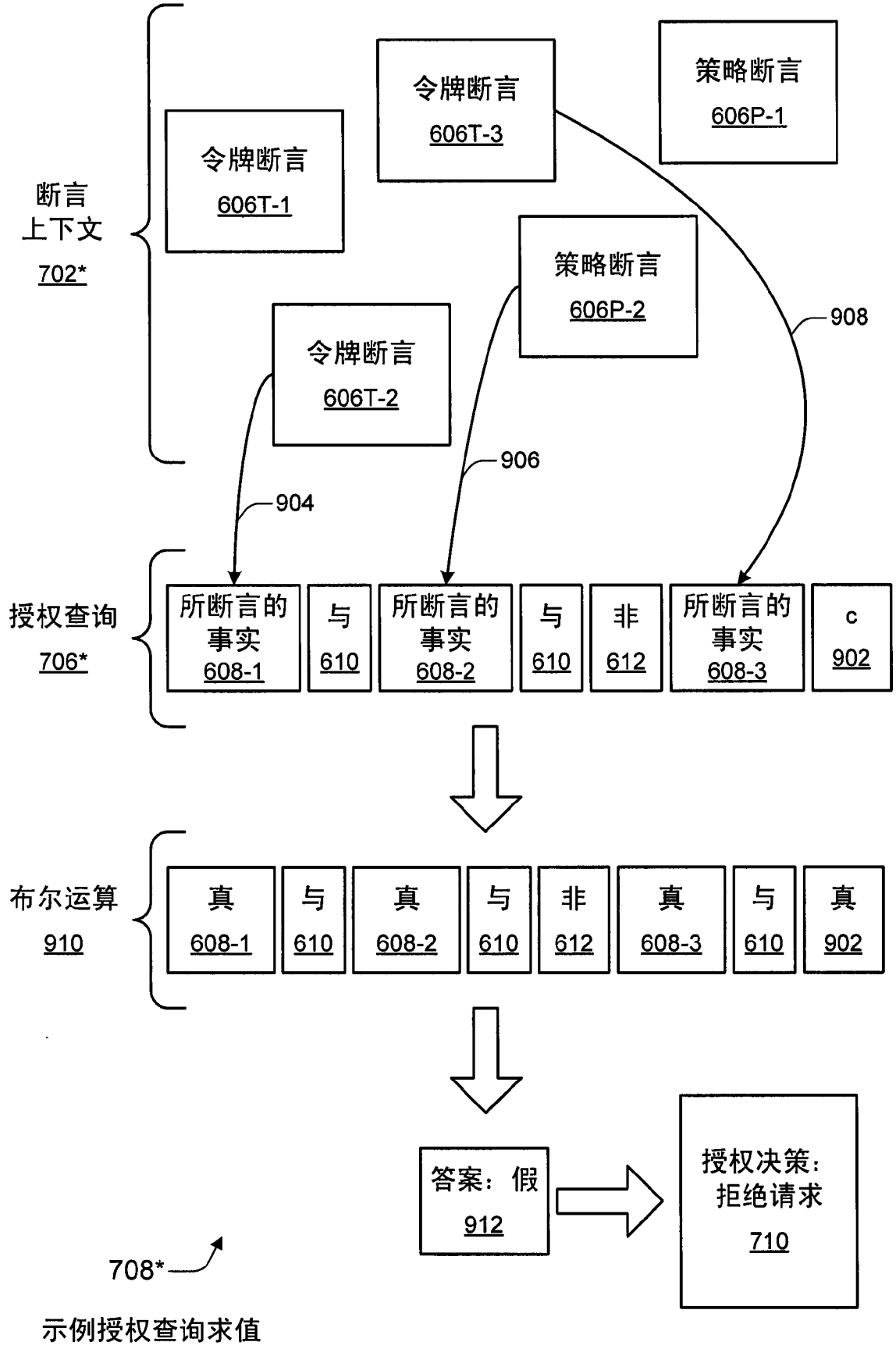
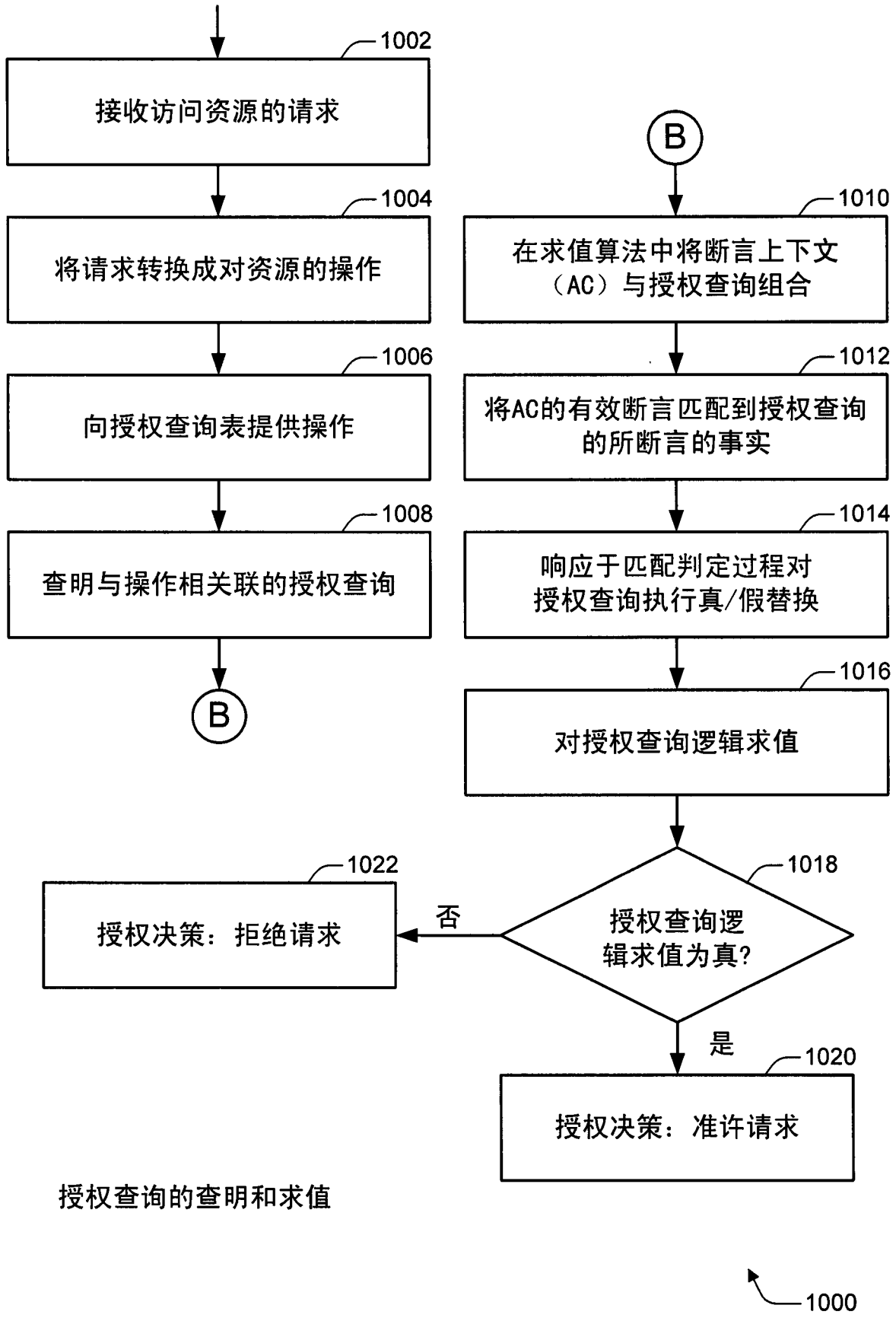

断言
上下文
702*
令牌断言
606T-1
令牌断言
606T-3
策略断言
606P-1
策略断言
606P-2
令牌断言
606T-2
908
906
904
授权查询
706*
所断言的
事实
608-1
与
610
所断言的
事实
608-2
与
610
非
612
所断言的
事实
608-3
c
902
布尔运算
910
真
608-1
与
610
真
608-2
与
610
非
612
真
608-3
与
610
真
902
答案：假
912
授权决策：
拒绝请求
710
708*
示例授权查询求值

图 9



授权查询的查明和求值

图 10