(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2025 年 5 月 22 日 (22.05.2025)

WIPO | PCT

(10) 国际公布号
WO 2025/102725 A1

(51) 国际专利分类号:
G06F 21/60 (2013.01) *G06F 21/62* (2013.01)

(21) 国际申请号: PCT/CN2024/099581

(22) 国际申请日: 2024 年 6 月 17 日 (17.06.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311534765.9 2023年11月16日 (16.11.2023) CN

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼 518129 (CN)。

(72) 发明人: 蒋武 (**JIANG, Wu**); 中国广东省深圳市龙岗区坂田华为总部办公楼 518129 (CN)。张钊 (**ZHANG, Zhao**); 中国广东省深圳市龙岗区坂田华为总部办公楼 518129 (CN)。杨辉 (**YANG, Hui**); 中国广东省深圳市龙岗区坂田华为总部办公楼 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所（普通合伙） (**SHENPAT INTELLECTUAL PROPERTY AGENCY**); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2 518001 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(54) **Title:** FILE ACCESS METHOD AND APPARATUS, FILE ACCESS PERMISSION DETERMINATION METHOD AND APPARATUS, AND RELATED DEVICES

(54) 发明名称: 文件访问方法、文件访问权限确定方法、装置及相关设备

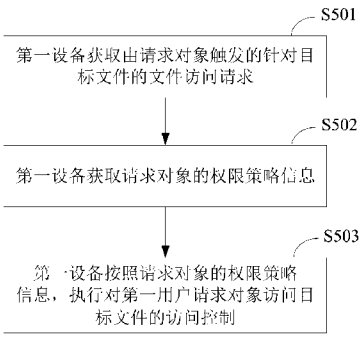

图 5

S501 A first device acquires a file access request which is triggered by a request object for a target file
S502 The first device acquires permission policy information of the request object
S503 The first device executes access control on the access of a first user request object to the target file according to the permission policy information of the request object

(57) **Abstract:** Provided in the embodiments of the present application are a file access method and apparatus, and a related device, which are applied in the technical field of data security. In the method, a first device acquires a file access request which is triggered by a request object for a target file, acquires permission policy information of the request object, and executes access control on the access of the request object to the target file according to the permission policy information of the request object. The permission policy information of the request object is determined on the basis of file label policy information of the target file and the file access request of the request object. In this way, a policy corresponding to a file label, i.e., file label policy information, can be used, so as to realize fine-grained data protection with a file as the granularity. Further provided in the present application are a file access permission determination method and apparatus, and a related device, which are applied to a second device. The second device decrypts the file label policy information, and determines the permission policy information, such that the degree of security of the file label policy information can be improved, thereby improving the degree of security of the target file.

WO 2025/102725 A1

[见续页]

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 本申请实施例提供应用于数据安全技术领域的文件访问方法、装置及相关设备。该方法中，第一设备获取由请求对象触发的针对目标文件的文件访问请求，获取请求对象的权限策略信息，按照请求对象的权限策略信息，执行对请求对象访问目标文件的访问控制。请求对象的权限策略信息基于目标文件的文件标签策略信息以及请求对象的所述文件访问请求确定。如此能够采用与文件标签对应的策略，也就是文件标签策略信息，实现以文件为粒度的细粒度的数据保护。本申请还提供了应用于第二设备的文件访问权限确定方法、装置及相关设备。由第二设备解密文件标签策略信息，并确定权限策略信息，能够提高文件标签策略信息的安全程度，进而提高目标文件的安全程度。

文件访问方法、文件访问权限确定方法、装置及相关设备

本申请要求于 2023 年 11 月 16 日提交国家知识产权局、申请号为 202311534765.9、发明名称为“文件访问方法、文件访问权限确定方法、装置及相关设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及数据安全技术领域，特别是涉及文件访问方法、文件访问权限确定方法、装置及相关设备。

背景技术

在数据的使用过程中经常出现泄露、篡改以及勒索等恶意的攻击，存在安全隐患。需要采用一定的安全防护方法保护数据，避免数据遭到攻击。

目前，通常是采用检测攻击的方式，及时发现并处理攻击，提高数据的安全程度。但是，攻击的种类较多，通过检测的方式难以发现各类攻击，防御攻击的效果难以满足数据安全的需要。

发明内容

本申请提供了一种文件访问方法以及文件访问权限确定方法，旨在实现在用户访问文件时，以文件为粒度的对于文件的数据保护。此外，本申请还提供了对应的装置、计算设备、计算机可读存储介质以及计算机程序产品。

第一方面，本申请提供了一种文件访问方法。该方法应用于第一设备。第一设备获取由请求对象触发的针对目标文件的文件访问请求。文件访问请求包括访问操作信息，访问操作信息用于描述请求对象需要对目标文件执行的访问操作。请求对象为请求访问目标文件的用户。请求对象为第一设备的操作系统程序的系统用户，或者为应用程序的应用用户。第一设备获取请求对象的权限策略信息。权限策略信息是基于目标文件的文件标签策略信息以及文件访问请求确定的，用于指示请求对象具有的操作目标文件的权限。文件标签策略信息与目标文件的文件标签对应，用于描述针对目标文件的访问操作的控制策略。文件标签包括一种或者多种安全维度的标签。文件标签由目标文件的管理者设置或者基于目标文件的文件属性生成。第一设备按照权限策略信息执行对请求对象访问目标文件的访问控制。基于文件标签，能够实现以文件为粒度的数据保护，提高文件访问的安全程度。以文件为中心的数据安全防护，能够在一定程度上减少文件被篡改以及泄露等安全问题，提高文件完整性和机密性的保护。

在一种可能的实现方式中，由第一设备生成请求对象的权限策略信息。第一设备根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息。

在一种可能的实现方式中，由第二设备生成请求对象的权限策略信息。第一设备向第二设备发送针对目标文件的权限请求。权限请求包括目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥。目标文件的文件标签策略信息由目标文件的公钥加密。第一设备获取第二设备反馈的权限信息。权限信息包括第一密文。第一密文包括利用请求对象的公钥对请求对象的权限策略信息加密得到的密文。请求对象的权限策略信息是第二设备利用目标文件的私钥、目标文件的文件标签策略信息以及访问操作信息处理得到的。第一设备利用请求对象的私钥对第一密文进行解密，得到请求对象的权限策略信息。由第二设备利用目标文件的私钥对目标文件的文件标签策略信息进行解密，并确定权限策略信息，无需第一设备具有目标文件的私钥，减少第一设备具有的目标文件的私钥泄露后所导致的文件标签策略信息被篡改的安全问题，提高文件标签策略信息的安全程度，进而提高目标文件的安全程度。并且，第一设备与第二设备交互的文件标签策略信息和权限策略信息均是加密后的信息，减少第一设备和第二设备在交互过程中信息泄露的风险。

在一种可能的实现方式中，目标文件利用文件加密密钥加密。文件加密密钥封装在目标文件的文件标签策略信息中。第一设备获取的权限信息还包括利用请求对象的公钥对文件加密密钥加密得到的第二密文。在按照请求对象的权限策略信息，执行对请求对象访问目标文件的访问控制之前，若基于权限策略信息，确定请求对象具有访问权限，第一设备利用文件加密密钥对目标文件进行解密。文件加密密钥为第一设备利用请求对象的私钥对第二密文进行解密得到的。如此针对每个文件进行加密，提高文件的

安全程度。利用文件独有的密钥，也能够有效减少利用统一的密钥进行加密所导致的密钥泄露后对多个文件的安全威胁。

在一种可能的实现方式中，第一设备还获取目标文件的文件标签，基于文件标签以及标签策略模板，生成目标文件的文件标签策略信息。如此能够根据目标文件的文件标签，利用标签策略模板，自动生成文件标签策略信息。

在一种可能的实现方式中，标签策略模板是从第二设备获取的。

在一种可能的实现方式中，设置文件标签策略信息的用户还能够对文件标签策略信息进行自定义更新。第一设备获取针对目标文件的自定义标签策略信息；并利用自定义标签策略信息更新目标文件的文件标签策略信息。如此能够实现文件标签策略信息的自定义调整，提高配置文件标签策略信息的灵活度，便于为文件配置符合文件保护需要的文件标签策略信息。

在一种可能的实现方式中，第一设备为主机。

在一种可能的实现方式中，方法应用于第一设备的应用层，或者应用于第一设备的系统层，或者应用于第一设备应用层和系统层。

在一种可能的实现方式中，第一设备为存储设备。请求对象通过与第一设备连接的第三设备触发文件访问请求。第一设备获取第三设备发送的由请求对象触发的针对目标文件的文件访问请求。文件访问请求由第三设备利用安全协议封装。第一设备利用安全协议解封文件访问请求。如此能够利用安全协议保护文件访问请求的安全，进而提高文件的安全性。

在一种可能的实现方式中，第一设备按照请求对象的权限策略信息以及请求对象的访问操作信息，生成反馈文件信息，向第三设备发送利用安全协议封装后的反馈文件信息。利用安全协议提高第一设备与第三设备之间传输的信息的安全程度。

在一种可能的实现方式中，方法应用于第一设备的系统层，应用程序为预设安全应用程序。

第二方面，本申请提供了一种文件访问权限确定方法。方法应用于第二设备。第二设备获取第一设备发送的针对目标文件的权限请求。权限请求包括目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，文件标签策略信息由目标文件的公钥加密，用于描述针对目标文件的访问操作的控制策略，文件标签策略信息与目标文件的文件标签对应。文件标签由目标文件的管理者设置或者基于目标文件的文件属性生成。文件标签包括一种或者多种安全维度的标签。请求对象为第一设备的操作系统程序的系统用户，或者为应用程序的应用用户。第二设备利用目标文件的私钥对文件标签策略信息解密，基于目标文件的文件标签策略信息和访问操作信息确定请求对象的权限策略信息。权限策略信息用于描述请求对象针对目标文件的访问操作的权限策略。第二设备利用请求对象的公钥对请求对象的权限策略信息加密，得到第一密文，向第一设备发送包括第一密文的权限信息。由第二设备利用目标文件的私钥对目标文件的文件标签策略信息进行解密，并确定权限策略信息，能够避免第一设备拥有目标文件的私钥，减少第一设备具有的目标文件的私钥泄露后所产生的安全问题，提高文件标签策略信息的安全性，进而提高目标文件的安全程度。并且，第一设备与第二设备交互的文件标签策略信息和权限策略信息均是加密后的信息，提高第一设备与第二设备交互过程中信息的安全程度，减少第一设备和第二设备在交互过程中信息泄露的风险。

在一种可能的实现方式中，目标文件利用文件加密密钥加密。文件加密密钥封装在目标文件的文件标签策略信息中。第二设备还利用请求对象的公钥对文件加密密钥加密得到第二密文。第二设备向第一设备发送的权限信息还包括第二密文。第二设备向第一设备发送加密后的文件加密密钥，便于第一设备基于文件加密密钥对目标文件进行解密，并且控制请求对象访问。利用针对目标文件独有的密钥，也能够有效避免利用统一的密钥进行加密所导致的密钥泄露后对多个文件的安全威胁，提高目标文件的数据安全。

在一种可能的实现方式中，第二设备还向第一设备提供标签策略模板。第二设备响应于获取第一设备发送的标签策略模板获取请求，向第一设备发送标签策略模板。

在一种可能的实现方式中，第二设备为服务器，或者管理设备。

第三方面，本申请提供了一种文件访问装置，装置应用于第一设备，装置包括：获取模块，用于获取由请求对象触发的针对目标文件的文件访问请求，文件访问请求包括访问操作信息，访问操作信息用

于描述请求对象需要对目标文件执行的访问操作；请求对象为第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；处理模块，用于获取请求对象的权限策略信息，权限策略信息是基于目标文件的文件标签策略信息以及文件访问请求确定的；文件标签策略信息与目标文件的文件标签对应，文件标签策略信息用于描述针对目标文件的访问操作的控制策略，权限策略信息用于指示请求对象具有的操作目标文件的权限；文件标签包括一种或者多种安全维度的标签，文件标签由目标文件的管理者设置或者基于目标文件的文件属性生成；控制模块，用于按照权限策略信息执行对请求对象访问目标文件的访问控制。

在一种可能的实现方式中，处理模块，具体用于根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息。

在一种可能的实现方式中，处理模块，具体用于向第二设备发送针对目标文件的权限请求，权限请求包括目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，目标文件的文件标签策略信息由目标文件的公钥加密；获取第二设备反馈的权限信息，权限信息包括第一密文，第一密文包括利用请求对象的公钥对请求对象的权限策略信息加密得到的密文，请求对象的权限策略信息是第二设备利用目标文件的私钥、目标文件的文件标签策略信息以及访问操作信息处理得到的；利用请求对象的私钥对第一密文进行解密，得到请求对象的权限策略信息。

在一种可能的实现方式中，目标文件利用文件加密密钥加密，文件加密密钥封装在目标文件的文件标签策略信息中，权限信息还包括利用请求对象的公钥对文件加密密钥加密得到的第二密文，处理模块还用于若基于权限策略信息，确定请求对象具有访问权限，利用文件加密密钥对目标文件进行解密，文件加密密钥为利用请求对象的私钥对第二密文进行解密得到的。

在一种可能的实现方式中，获取模块，还用于获取目标文件的文件标签；生成模块，用于基于文件标签以及标签策略模板，生成目标文件的文件标签策略信息。

在一种可能的实现方式中，标签策略模板是从第二设备获取的。

在一种可能的实现方式中，获取模块，还用于获取针对目标文件的自定义标签策略信息；生成模块，还用于利用自定义标签策略信息更新目标文件的文件标签策略信息。

在一种可能的实现方式中，第一设备为主机。

在一种可能的实现方式中，装置应用于第一设备的应用层。

在一种可能的实现方式中，装置应用于第一设备的系统层。

在一种可能的实现方式中，应用程序为预设安全应用程序。

在一种可能的实现方式中，第一设备为存储设备，获取模块，具体用于获取第三设备发送的由请求对象触发的针对目标文件的文件访问请求，文件访问请求由第三设备利用安全协议封装；利用安全协议解封文件访问请求。

在一种可能的实现方式中，控制模块，具体用于按照请求对象的权限策略信息以及请求对象的访问操作信息，生成反馈文件信息，向第三设备发送利用安全协议封装后的反馈文件信息。

第四方面，本申请提供了一种文件访问权限确定装置，装置应用于第二设备，装置包括：获取模块，用于获取第一设备发送的针对目标文件的权限请求，权限请求包括目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，文件标签策略信息由目标文件的公钥加密，文件标签策略信息与目标文件的文件标签对应，文件标签策略信息用于描述针对目标文件的访问操作的控制策略，文件标签包括一种或者多种安全维度的标签，文件标签由目标文件的管理者设置或者基于目标文件的文件属性生成，请求对象为第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；解密模块，用于利用目标文件的私钥对文件标签策略信息解密；确定模块，用于基于目标文件的文件标签策略信息和访问操作信息确定请求对象的权限策略信息，权限策略信息用于描述请求对象针对目标文件的访问操作的权限策略；加密模块，用于利用请求对象的公钥对请求对象的权限策略信息加密，得到第一密文；发送模块，用于向第一设备发送权限信息，权限信息包括第一密文。

在一种可能的实现方式中，目标文件利用文件加密密钥加密，文件加密密钥封装在目标文件的文件标签策略信息中，加密模块，还用于利用请求对象的公钥对文件加密密钥加密得到第二密文，权限信息还包括第二密文。

在一种可能的实现方式中，发送模块，还用于响应于获取第一设备发送的标签策略模板获取请求，向第一设备发送标签策略模板。

在一种可能的实现方式中，第二设备为服务器，或者管理设备。

第五方面，本申请提供一种计算设备集群，计算设备集群包括至少一个计算设备，每个计算设备包括处理器和存储器；该存储器用于存储指令，当该计算设备集群运行时，每个计算设备中的处理器执行存储器存储的指令，以使该计算设备集群执行上述第一方面或第一方面任一种可能实现方式中的文件访问方法，或者执行上述第二方面或第二方面任一种可能实现方式中的文件访问权限确定方法。需要说明的是，该存储器可以集成于处理器中，也可以是独立于处理器之外。每个计算设备还可以包括总线。其中，处理器通过总线连接存储器。其中，存储器可以包括可读存储器以及随机存取存储器。

第六方面，本申请提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当其在计算设备集群（该计算设备集群包括至少一个计算设备）上运行时，使得计算设备集群执行上述第一方面或第一方面任一种可能实现方式中的文件访问方法，或者执行上述第二方面或第二方面任一种可能实现方式中的文件访问权限确定方法。

第七方面，本申请提供了一种包含指令的计算机程序产品，当其在计算设备集群（该计算设备集群包括至少一个计算设备）上运行时，使得计算设备集群执行上述第一方面或第一方面任一种可能实现方式中的文件访问方法，或者执行上述第二方面或第二方面任一种可能实现方式中的文件访问权限确定方法。

本申请在上述各方面提供的实现方式的基础上，还可以进行进一步组合以提供更多实现方式。

附图说明

图 1a 为本申请实施例提供的一种场景示意图；

图 1b 为本申请实施例提供的另一种场景示意图；

图 1c 为本申请实施例提供的一种第一设备与第二设备交互的示意图；

图 2a 为本申请实施例提供的再一种场景示意图；

图 2b 为本申请实施例提供的又一种场景示意图；

图 2c 为本申请实施例提供的另一种第一设备与第二设备交互的示意图；

图 3a 为本申请实施例提供的一种场景示意图；

图 3b 为本申请实施例提供的另一种场景示意图；

图 3c 本申请实施例提供的又一种第一设备与第二设备交互的示意图；

图 4a 为本申请实施例提供的再一种场景示意图；

图 4b 为本申请实施例提供的又一种场景示意图；

图 4c 为本申请实施例提供的再一种第一设备与第二设备交互的示意图；

图 5 为本申请实施例提供的一种文件访问方法的流程示意图；

图 6 为本申请实施例提供的另一种文件访问方法的流程示意图；

图 7 为本申请实施例提供的一种生成目标文件的文件标签策略信息的流程示意图；

图 8 为本申请实施例提供的一种文件标签策略示意图；

图 9 为本申请实施例提供的另一种生成目标文件的文件标签策略信息的流程示意图；

图 10 为本申请实施例提供的一种文件访问装置的结构示意图；

图 11 为本申请实施例提供的一种文件访问权限确定装置的结构示意图；

图 12 为本申请实施例提供的一种计算设备的结构示意图；

图 13 为本申请实施例提供的一种计算设备集群的结构示意图；

图 14 为本申请实施例提供的另一种计算设备集群的结构示意图。

具体实施方式

下面将结合本申请中的附图，对本申请提供的实施例中的方案进行描述。

本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的术语在适当情况下可以互换，这仅仅是描述本申请的实施例中对相同属性的对象在描述时所采用的区分方式。

数据作为较为重要的资产，包含个人或者企业的重要信息。在使用数据的过程中，需要防止数据遭到攻击，避免出现数据泄露、数据被篡改或者数据不可用的问题。目前，通常在网络、主机以及存储等维度构建攻击的检测算法。利用检测算法及时发现攻击行为，并且对攻击行为进行处理，维护数据安全。但是，检测算法所能检测发现的攻击行为有限，仅能针对当前已知的攻击行为进行识别，难以发现未知的攻击，仍然存在安全隐患。并且，检测算法存在检测误差，可能会影响处理数据的业务的正常运行。利用检测算法检测攻击的方式难以满足数据安全的需求。

基于此，本申请实施例提供应用于第一设备的文件访问方法。第一设备获取由请求对象触发的针对目标文件的包括访问操作信息的文件访问请求。第一设备获取请求对象的权限策略信息。其中，请求对象的权限策略信息是基于目标文件的文件标签策略信息以及请求对象的文件访问请求确定的。文件标签策略信息与目标文件的文件标签对应。文件标签策略信息用于描述针对目标文件的访问操作的控制策略。第一设备按照权限策略信息执行对请求对象访问目标文件的访问控制。利用文件标签策略信息能够实现以文件为粒度的针对数据的安全保护。如此，实现以数据为中心的安全防护，在一定程度上能够减少文件面临的被篡改、泄露以及勒索的安全风险。并且，能够基于文件的安全保护需求配置文件标签，进而实现灵活的文件标签策略信息的配置，满足不同文件的安全需求。

本申请实施例不限定文件访问方法以及文件访问权限确定方法的部署方式。作为一些示例，参见图 1a-图 4c 所示，本申请实施例提供四种应用场景示意图。

作为一种示例，参见图 1a 所示，本申请实施例提供的文件访问方法能够应用于标签策略客户端或者标签策略软件开发工具包（Software Development Kit，SDK），部署在第一设备的应用程序中，也就是部署在第一设备的应用层中。第一设备例如为主机。请求访问目标文件的请求对象能够是第一设备的应用程序的应用用户，或者为第一设备的操作系统程序的系统用户。图 1a 所示的场景能例如为应用程序具有独立的用户体系的场景。第一设备的应用层实现对第一设备的应用程序的应用用户或者操作系统程序的系统用户，访问文件的控制。

在一种可能的实现方式中，第一设备的应用层包括的标签策略客户端或者标签策略软件开发工具包，获取由请求对象触发的针对目标文件的文件访问请求，根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息，按照权限策略信息执行对请求对象访问目标文件的访问控制。

在另一种可能的实现方式中，参见图 1b 所示，第一设备与第二设备交互实现对目标文件的访问控制。本申请实施例提供文件访问权限确定方法。文件访问权限确定方法能够应用于标签策略服务，或者标签策略管理组件，部署在第二设备。第二设备例如为服务器。参见图 1c 所示，该图为本申请实施例提供的一种第一设备与第二设备交互的示意图。第一设备的应用层包括的标签策略客户端或者标签策略软件开发工具包，包括初始化模块、文件标签生成模块、文件标签策略信息生成模块、访问请求处理模块以及访问操作控制模块。第二设备的标签策略服务，或者标签策略管理组件，包括初始化模块以及权限信息确定模块。第一设备的初始化模块与第二设备的初始化模块交互，以便实现初始化认证，也就是身份认证以及证书颁发。第一设备的文件标签生成模块用于基于用户触发生成文件标签，或者自动生成文件标签，并向第二设备发送标签策略模板获取请求，获取第二设备反馈的标签策略模板。第一设备的文件标签策略信息生成模块，基于文件标签和标签策略模板，生成目标文件的文件标签策略信息。第一设备的访问请求处理模块，用于基于获取的由请求对象触发的文件访问请求，向第二设备的权限信息确定模块发送权限请求。第二设备的权限信息确定模块基于权限请求，解析文件标签策略信息，确定请求对象的权限策略信息，并向第一设备发送包括利用请求对象的公钥加密的请求对象的权限策略信息的权限信息。第一设备的访问操作控制模块用于基于权限信息包括的请求对象的权限策略信息，控制请求对象的访问操作。

作为另一种示例，参见图 2a 所示，本申请实施例提供的文件访问方法能够应用于标签内核模块，部署在第一设备的操作系统程序（Operating System，OS）中，也就是部署在第一设备的系统层中。第一设备例如为主机。其中，请求访问目标文件的请求对象能够是第一设备的操作系统程序的系统用户，或者是应用程序的应用用户。图 2a 所示的场景例如为应用程序与 OS 具有统一的用户体系，或者应用程序的用户体系能够同步到 OS 的用户体系，或者应用程序不具有独立的用户体系的场景。第一设备的系

统层实现对应用程序的应用用户，或者操作系统程序的系统用户访问文件的控制。

在一种可能的实现方式中，第一设备的系统层包括的标签内核模块，获取由请求对象触发的针对目标文件的文件访问请求，根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息，按照权限策略信息执行对请求对象访问目标文件的访问控制。

在另一种可能的实现方式中，参见图 2b 所示，第一设备与第二设备交互实现对目标文件的访问控制。本申请实施例提供的文件访问权限确定方法能够应用于标签策略服务，或者标签策略管理组件，部署在第二设备。第二设备例如为服务器。参见图 2c 所示，该图为本申请实施例提供的另一种第一设备与第二设备交互的示意图。第一设备的系统层包括的标签策略客户端或者标签策略软件开发工具包，包括初始化模块、文件标签生成模块、文件标签策略信息生成模块、访问请求处理模块以及访问操作控制模块。第二设备的标签策略服务，或者标签策略管理组件，包括初始化模块以及权限信息确定模块。第一设备与第二设备之间的交互过程与上述图 1c 对应的示例类似，在此不再赘述。

作为再一种示例，参见图 3a 所示，本申请实施例提供的文件访问方法能够应用于标签内核模块，以及标签策略客户端或者标签策略 SDK 中，部署在第一设备的 OS 和应用程序中，也就是部署在第一设备的系统层和应用层中。第一设备例如为主机。其中，请求访问目标文件的请求对象能够是第一设备的操作系统程序的系统用户，或者是应用程序的应用用户。图 3a 所示的场景例如为安全性要求较高的业务场景。第一设备的系统层和应用层协同实现对应用程序的应用用户，或者操作系统程序的系统用户，访问文件的控制。

在一种可能的实现方式中，第一设备的标签内核模块，以及标签策略客户端或者标签策略 SDK，获取由请求对象触发的针对目标文件的文件访问请求，根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息，按照权限策略信息执行对请求对象访问目标文件的访问控制。

在另一种可能的实现方式中，参见图 3b 所示，第一设备与第二设备交互实现对目标文件的访问控制。本申请实施例提供的文件访问权限确定方法能够应用于标签策略服务，或者标签策略管理组件，部署在第二设备。第二设备例如为服务器。

参见图 3c 所示，该图为本申请实施例提供的又一种第一设备与第二设备交互的示意图。第一设备的系统层和应用层包括的标签策略客户端或者标签策略软件开发工具包，包括初始化模块、文件标签生成模块、文件标签策略信息生成模块、访问请求处理模块以及访问操作控制模块。第二设备的标签策略服务，或者标签策略管理组件，包括初始化模块以及权限信息确定模块。第一设备与第二设备之间的交互过程与上述图 1c 对应的示例类似，在此不再赘述。

作为又一种示例，参见图 4a 所示，图 4a 所示的场景适用于存储场景中。本申请实施例提供的文件访问方法能够应用于标签内核模块，部署在第一设备中。第一设备例如为存储设备。第一设备还与第三设备连接。第三设备例如为生产主机。请求访问目标文件的请求对象通过第三设备访问第一设备存储的目标文件。第一设备与第三设备之间通过安全协议通信。第一设备还包括安全协议服务端。第三设备包括安全协议客户端。安全协议服务端和安全协议客户端用于利用安全协议对传输信息进行封装或者解封，实现第一设备与第三设备之间的通信。如此请求对象能够在第三设备上完成对第一设备存储的目标文件的访问操作。

在一种可能的实现方式中，第一设备的标签内核模块，获取由请求对象触发的针对目标文件的文件访问请求，根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息，按照权限策略信息执行对请求对象访问目标文件的访问控制。

在另一种可能的实现方式中，参见图 4b 所示，第一设备与第二设备交互实现对目标文件的访问控制。本申请实施例提供的文件访问权限确定方法能够应用于标签策略服务，或者标签策略管理组件，部署在第二设备。第二设备例如为存储设备的管理设备。参见图 4c 所示，该图为本申请实施例提供的再一种第一设备与第二设备交互的示意图。第一设备包括的标签策略客户端或者标签策略软件开发工具包，包括初始化模块、文件标签生成模块、文件标签策略信息生成模块、访问请求处理模块以及访问操作控制模块。第一设备还包括安全协议服务端。第二设备的标签策略服务，或者标签策略管理组件，包括初始化模块以及权限信息确定模块。第三设备 A 和第三设备 B 包括安全协议客户端。第一设备与第二设

备之间的交互过程与上述图 1c 对应的示例类似，在此不再赘述。第三设备 A 的安全协议客户端用于获取用户选择的文件标签，并利用安全协议将文件标签封装后向第一设备发送。第一设备的安全协议服务端利用安全协议解封得到文件标签，并向文件标签生成模块发送文件标签。第三设备 A 的安全协议客户端用于获取请求对象触发的文件访问请求，并利用安全协议将文件访问请求封装后向第一设备发送。第一设备的安全协议服务端利用安全协议解封得到文件访问请求，并向访问请求处理模块发送文件访问请求。如此能够实现对请求对象，也就是第三设备的应用程序的应用用户，或者操作系统程序的系统用户访问文件的控制。

需要说明的是，以上图 1a-图 4c 所示的应用场景仅作为示例，本申请提供的文件访问方法以及文件访问权限确定方法的应用场景不受图 1a-图 4c 所示的应用场景的限制。

接下来，对本申请提供的文件访问方法以及文件访问权限确定方法的各种非限定性的具体实施方式进行详细描述。

参见图 5 所示，该图为本申请实施例提供的一种文件访问方法的流程示意图。该方法应用于第一设备，包括 S501-S503。

S501：第一设备获取由请求对象触发的针对目标文件的文件访问请求。

请求对象为通过第一设备，请求访问第一设备储存的目标文件的对象。本申请实施例不限定请求对象的身份。请求对象例如为用户。作为示例，用户为第一设备的应用程序的应用用户，或者为第一设备的操作系统程序的系统用户。另外，请求对象例如为用户和程序进程。程序进程为用户触发文件访问请求的进程。

需要说明的是，在一些可能的实现方式中，作为请求对象的用户需要通过安全认证。

在一种可能的实现方式中，第一设备与第二设备建立连接。第一设备在初始化阶段，与第二设备交互用户信息，完成对用户的认证。认证过程包括身份认证和第二设备向第一设备颁发证书两个过程。其中，身份认证过程中，第一设备发送涉及文件访问的对象的对象信息。作为一些示例，第一设备发送在该应用程序登录的用户的用户信息，或者在第一设备的操作系统程序登录的用户的用户信息。

第二设备基于获取的对象信息，对对象进行认证，并向第一设备发送认证结果。第一设备基于认证结果确定通过安全认证的对象。若请求对象已经为认证的对象，则第一设备基于认证结果能够确定请求对象是否通过安全认证。在请求对象为通过安全认证的情况下，第一设备处理请求对象触发的针对目标文件的文件访问请求。若请求对象未通过安全认证，则第一设备不处理请求对象触发的针对目标文件的文件访问请求。若请求对象为未认证的对象，例如首次在第一设备登录的用户，则第一设备向第二设备发送请求对象的用户信息。第二设备基于获取的请求对象的用户信息，对请求对象进行认证，并向第一设备发送请求对象的认证结果。第一设备基于请求对象的认证结果能够确定请求对象是否通过安全认证。在请求对象为通过安全认证的情况下，第一设备处理请求对象触发的针对目标文件的文件访问请求。若请求对象未通过安全认证，则第一设备不处理请求对象触发的针对目标文件的文件访问请求。

在另一种实现方式中，以图 2a 和图 3a 所示的应用场景为例，本申请实施例提供的文件访问方法应用于第一设备的系统层。也就是由第一设备的操作系统程序执行文件访问方法。请求对象能够是第一设备部署的应用程序的应用用户。第一设备的系统层在获取应用用户触发的文件访问请求后，先验证应用用户所属的应用程序是否为安全的应用程序。例如，基于预先建立的应用程序白名单。应用程序白名单包括安全的应用程序的信息。判断应用用户是否为应用程序白名单包括的应用程序的应用用户。如果应用用户是应用程序白名单包括的应用程序的应用用户，则第一设备处理应用用户触发的针对目标文件的文件访问请求。如果应用用户不是应用程序白名单包括的应用程序的应用用户，则第一设备不处理请求对象触发的针对目标文件的文件访问请求。如此够实现对应用用户所属的应用程序的安全认证，限制访问文件的应用程序，防止出现应用程序恶意处理文件，例如删除文件，提高文件的安全程度。

第一设备存储的目标文件是预先配置文件标签策略信息的文件。文件标签策略信息与目标文件的文件标签对应。文件标签能够基于文件的属性以及文件保护需要设置。文件标签策略信息用于描述针对目标文件的访问操作的控制策略。文件标签策略信息用于指示访问目标文件需要遵守的权限策略。目标文件受到文件标签策略信息的保护。

本申请实施例不限定目标文件的文件标签策略信息的配置方式。在一种可能的实现方式中，能够由

目标文件的所有者或者管理者直接进行配置。在另一种可能的实现方式中，由目标文件的所有者或者管理者编辑生成。本申请实施例提供一种生成目标文件的文件标签策略信息的具体实现方式，具体请参见下文。

文件访问请求包括访问操作信息。访问操作信息包括请求对象的对象信息以及请求对象请求对目标文件进行访问操作的操作信息。作为一种示例，请求对象的对象信息例如为请求对象的账号信息以及对象类型。例如，请求对象为用户，账号信息为用户的账号。对象类型比如为系统用户或者应用用户。区分不同的请求对象的类型，便于确定不同类型的请求对象的权限策略信息，实现对不同类型的请求对象的访问控制，提高数据的安全程度。在一些可能的实现方式中，请求对象的对象信息还包括触发文件访问请求的程序进程的进程信息，例如进程号。操作信息例如包括访问操作的类型。

S502：第一设备获取请求对象的权限策略信息。

请求对象的权限策略信息用于指示请求对象具有的操作目标文件的权限。请求对象的权限策略信息是基于目标文件的文件标签策略信息以及请求对象的文件访问请求确定的。

本申请实施例不限定第一设备获取权限策略信息的可能的实现方式。

在一种可能的实现方式中，第一设备根据目标文件的文件标签策略信息以及请求对象的文件访问请求，生成请求对象的权限策略信息。

第一设备基于获取的访问操作信息，从目标文件的文件标签策略信息中，确定与访问操作信息相关的权限策略信息，得到请求对象的权限策略信息。请求对象的权限策略信息用于指示请求对象具有的操作目标文件的权限。

作为一种示例，目标文件的文件标签策略信息包括针对不同的安全维度，所能够针对目标文件执行的操作。作为一种示例，目标文件的文件标签策略信息包括文件的敏感度、访问用户、访问进程以及文件所属的业务类型四个安全维度的策略信息。其中，文件的敏感度的策略信息包括绝密文件执行加密保护。访问用户的策略信息包括属于 U1 类型的用户具有所有操作权限，属于非 U1 类型的用户拒绝访问，属于 U2 类型的用户具有读取操作和写入操作的权限，属于 U3 类型的用户具有打印操作的权限。访问进程的策略信息包括 P1 类型的进程具有所有权限，非 P1 类型的进程拒绝访问。文件所属的业务类型的策略信息为包括财务数据的文件限制向非财务人员发送。

访问操作信息包括请求对象所属的用户类型为 U1 类型，以及访问操作的类型为读取操作。以上述目标文件的文件标签策略信息为例，第一设备基于访问操作信息和文件标签策略信息确定，U1 类型的请求对象具有所有操作权限。请求对象的权限策略信息为具有所有操作权限。作为另一种示例，访问操作信息包括请求对象所属的用户类型为 U3 类型，以及访问操作的类型为读取操作。以上述目标文件的文件标签策略信息为例，第一设备基于访问操作信息和文件标签策略信息确定，U3 类型的请求对象具有打印操作的权限。请求对象的权限策略信息为具有打印操作的权限。

在另一种可能的实现方式中，第一设备通过与第二设备进行交互，获取第二设备发送的请求对象的权限策略信息。参见图 6 所示，上述 S502 具体包括以下步骤：

S5021：第一设备向第二设备发送针对目标文件的权限请求，权限请求包括访问操作信息，请求对象的公钥，以及由目标文件的公钥加密的目标文件的文件标签策略信息。

第一设备在获取针对目标文件的文件访问请求后，向第二设备发送针对目标文件的权限请求。第二设备能够基于目标文件的文件标签策略信息和访问操作信息确定请求对象访问目标文件的权限信息。

权限请求包括目标文件的文件标签策略信息、文件访问请求包括的访问操作信息，以及请求对象的公钥。其中，目标文件的文件标签策略信息由目标文件的公钥加密。

目标文件的文件标签策略信息预先基于目标文件的数据保护需要确定。目标文件的文件标签策略信息由第一设备生成，并利用目标文件的公钥加密进行保护。第一设备不具有目标文件的公钥对应的私钥，避免在第一设备的本地实现对目标文件的文件标签策略信息的解密处理，防止第一设备被攻击后，攻击者利用目标文件的私钥解密得到文件标签策略信息，并进行篡改。如此能够提高文件标签策略信息的安全程度，进而提高目标文件的安全性。

目标文件的公钥能够是预先由目标文件的所有者设置，或者基于目标文件的所有者的信息生成的密钥。作为示例，目标文件的公钥例如为目标文件的所有者所属的组织，例如公司、团体，的公钥，实现

属于组织对文件的管理和访问。

另外，请求对象的公钥能够是请求对象预先设置的公钥。本申请实施例不限定请求对象的公钥的生成方式。作为示例，请求对象的公钥基于请求对象的相关信息生成。

S5022：第二设备获取第一设备发送的针对目标文件的权限请求，权限请求包括访问操作信息，请求对象的公钥，以及由第一公钥加密的目标文件的文件标签策略信息。

S5023：第二设备利用目标文件的私钥对文件标签策略信息解密。

目标文件的私钥为目标文件的公钥的解密密钥。目标文件的私钥，例如是预先由目标文件的所有者设置的密钥，或者例如为基于目标文件的所有者的信息生成的密钥。作为示例，目标文件的私钥例如为目标文件的所有者所属的组织或者机构的私钥。如此便于组织和机构对文件进行统一的管理。由第二设备利用目标文件的私钥对第一设备生成的文件标签策略信息解密，第一设备不具有解密密钥，能够避免第一设备被攻击所导致的解密密钥泄露的问题，提高文件标签策略信息的安全程度，进而提高目标文件的安全程度。

S5024：第二设备基于目标文件的文件标签策略信息和访问操作信息确定请求对象的权限策略信息。

第二设备基于获取的针对目标文件的权限请求，获取目标文件的文件标签策略信息以及访问操作信息。第二设备能够基于访问操作信息，从目标文件的文件标签策略信息中，确定与访问操作信息相关的权限策略信息，得到请求对象的权限策略信息。请求对象的权限策略信息用于指示请求对象具有的操作目标文件的权限。

S5025：第二设备利用请求对象的公钥对请求对象的权限策略信息加密，得到第一密文。

第二设备在确定请求对象的权限策略信息后，利用请求对象的公钥对请求对象的权限策略信息进行加密，得到第一密文。加密后的请求对象的权限策略信息的安全程度较高，能够在一定程度上防止在第二设备与第一设备交互过程中权限策略信息被恶意获取。

S5026：第二设备向第一设备发送包括第一密文的权限信息。

S5027：第一设备获取第二设备反馈的权限信息。

S5028：第一设备利用请求对象的私钥对第一密文进行解密，得到请求对象的权限策略信息。

本申请实施例不限定请求对象的公钥和请求对象的私钥的生成方式。第一设备在获取权限信息后，利用请求对象的私钥对权限信息包括的第一密文解密，得到请求对象的权限策略信息。请求对象的权限策略信息指示请求对象具有的操作目标文件的权限。

利用目标文件的公钥对文件标签策略信息进行加密，能够提高文件标签策略信息在第一设备内存储的安全程度。由第二设备对文件标签策略信息进行解密，并分析得到权限策略信息，无需由第一设备在本地对文件标签策略信息解密，能够避免攻击者利用从第一设备获取的解密密钥恶意篡改文件标签策略信息的风险，提高文件标签策略信息的安全程度，进而提高目标文件的安全性。

S503：第一设备按照请求对象的权限策略信息，执行对请求对象访问目标文件的访问控制。

第一设备基于请求对象的权限策略信息，能够确定请求对象访问目标文件的权限。第一设备按照请求对象的权限策略信息，执行对请求对象访问目标文件的访问控制。

基于上述 S501-S503 的相关内容可知，以文件为粒度的细粒度的文件标签策略信息以及权限策略信息，能够实现针对目标文件的保护，实现以数据为中心的安全防护，提高对数据完整性和机密性的保护，在一定程度上能够减少文件面临的被篡改、泄露以及勒索的安全风险。

在一些场景中，目标文件具有保密需求。目标文件的保密需求能够通过目标文件的文件标签策略信息配置。第一设备基于生成的目标文件的文件标签策略信息确定目标文件具有保密的需求。第一设备利用文件加密密钥对目标文件进行加密。本申请实施例不限定文件加密密钥的生成方式。作为一种示例，文件加密密钥是随机生成的对称密钥。文件加密密钥与需要加密的文件一一对应。如此能够提高各个需要加密的文件的安全程度，也能够保证在部分文件的文件加密秘钥被破解的情况下，其他文件的安全。在一种可能的实现方式中，文件加密密钥封装在目标文件的文件标签策略信息中，并利用目标文件的公钥对目标文件的文件标签策略信息进行加密，实现对文件加密密钥和文件标签策略信息的保护。

在由第二设备确定请求对象的权限策略信息的实现方式中，第二设备在获取利用目标文件的公钥加密的文件标签策略信息后，利用目标文件的私钥对文件标签策略信息解密，得到文件标签策略信息以及

文件加密密钥。第二设备还利用请求对象的公钥对文件加密密钥加密得到第二密文。第二设备向第一设备发送包括第一密文和第二密文的权限信息。第一设备基于获取的权限信息的第二密文，能够利用请求对象的私钥对第二密文解密得到文件加密密钥。如果第一设备基于权限策略信息，确定请求对象具有目标文件的访问权限，则利用对第二密文解密得到的文件加密密钥对目标文件进行解密，以便请求对象对目标文件进行操作。如此能够实现对目标文件的进一步加密处理，提高目标文件的数据安全程度。

以上为利用目标文件的文件标签策略信息实现目标文件访问的方法，下面提供一种可能的生成目标文件的文件标签策略信息的具体实现方式。

参见图 7 所示，该图为本申请实施例提供的一种生成目标文件的文件标签策略信息的流程示意图。该方法包括 S701-S703：

S701：第一设备获取目标文件的文件标签。

目标文件的文件标签为针对目标文件设置的标签。文件标签包括一种或者多种安全维度的标签。需要说明的是，目标文件的文件标签基于标签模板确定。标签模板为预先设置的配置文件标签的模板。作为一种示例，标签模板包括多个可选择的文件标签。从标签模板中选择目标文件的文件标签。

本申请实施例不限定生成目标文件的文件标签的方式。在一种可能的实现方式中，由目标文件的管理者触发生成目标文件的文件标签。目标文件的管理者为具有管理目标文件权限的用户。目标文件的管理者例如为目标文件的所有者。用户能够通过选择或者输入的方式生成文件标签。在另一种可能的实现方式中，第一设备基于目标文件的文件属性自动生成文件标签。文件属性例如为文件类型、文件生成时间以及文件优先级等属性。作为示例，根据预先设置的标签生成规则以及目标文件的文件属性，自动生成目标文件的文件标签。标签生成规则例如包括文件属性与文件标签之间的对应关系。

作为一种示例，参见图 8 所示，该图为本申请实施例提供的一种文件标签策略示意图。标签模板包括四个安全维度的标签，分别是敏感度标签、所属用户标签、访问进程标签以及外发权限标签。敏感度标签例如包括绝密、机密、内部、公开和个人。所属用户标签例如包括 U1 类型。访问进程标签包括 P1 类型。外发权限标签包括财务数据和销售数据。

基于用户对文件标签的选择指令，从标签模板包括的标签中确定文件标签，或者基于标签模板包括的标签自动生成文件标签。例如，参见图 8 所示，从标签模板中选择绝密标签、U1 类型标签、P1 类型标签以及财务数据标签。

S703：第一设备基于文件标签以及标签策略模板，生成目标文件的文件标签策略信息。

标签策略模板为标签策略管理用户预先配置的策略模板。本申请实施例不限定标签策略模板包括的具体内容。作为示例，标签策略模板包括敏感度、所属用户、访问进程以及外发权限四个安全维度的标签对应的策略。

标签策略模板与标签模板对应。标签策略模板包括标签模板包括的各个标签对应的标签策略信息。

参见图 8 为例，标签策略模板包括四个安全维度的标签策略信息，包括标签模板包括的各个标签对应的标签策略信息。敏感度策略信息包括：1、针对绝密文件或者机密文件加密；2、针对公开文件不做加密；3、绝密文件拒绝打印和复制；4、个人文件只有所属用户有权限使用。所属用户策略信息包括：1、U1 类型的用户具有所有权限；2、对于绝密文件和机密文件，其他类型的用户拒绝访问；对于公开文件，所有类型的用户具有所有全部权限。访问进程策略信息包括：1、P1 类型进程具有所有权限；2、对于绝密文件或者机密文件，其他进程拒绝访问；对于公开文件，所有类型的进程具有所有全部权限。外发权限策略信息包括：1、财务数据仅能在财务人员内部发送；2、公开数据不限制外发权限。

第一设备从标签策略模板中获取目标文件的文件标签的标签策略信息，整合文件标签的标签策略信息，得到目标文件的文件标签策略信息。

作为一种示例，将目标文件的文件标签与标签策略模板包括的标签模板匹配。将与目标文件的文件标签一致的标签模板的文件标签策略信息，作为目标文件的文件标签对应的文件标签策略信息。

参见图 8 所示，第一设备从标签策略模板中，能够确定目标文件的文件标签对应的文件标签策略信息，也就是目标文件的文件标签策略信息，包括：1、敏感度策略信息：绝密文件加密；2、访问用户策略信息：U1 类型的用户具有所有权限，其他类型的用户拒绝访问；3、访问进程策略信息：P1 类型进程具有所有权限，其他进程拒绝访问；4、外发权限策略信息：限制向非财务人员外发。

第一设备在得到目标文件的文件标签策略信息后，能够将目标文件的文件内容、目标文件的文件标签以及目标文件的文件标签策略信息封装为受保护的文件。本申请实施例不限定封装文件的实现方式。作为一种示例，将目标文件的文件内容、目标文件的文件标签以及目标文件的文件标签策略信息封装为一个文件。作为另一种示例，分别将目标文件的文件内容、目标文件的文件标签以及目标文件的文件标签策略信息封装为三个相互关联的文件。目标文件的文件标签策略信息能够由第一公钥加密。

基于上述 S701 和 S703 的相关内容可知，能够较为灵活地配置符合目标文件的数据安全需求的文件标签以及文件标签策略信息，实现对文件的细粒度的安全防护，满足不同文件，以及针对不同对象类型访问文件的安全需求。并且，利用文件标签以及标签策略模板配置文件标签策略信息，能够提高配置文件标签策略信息的效率。

本申请实施例不限定标签策略模板的来源。

在一种可能的实现方式中，标签策略模板预先配置在第一设备中。

在另一种可能的实现方式中，标签策略模板是第一设备从第二设备获取得到的。参见图 7 所示，该方法还能够包括 S7021-S7023。

S7021：第一设备向第二设备发送标签策略模板获取请求。

标签策略模板获取请求用于获取标签策略模板。标签策略模板为标签策略管理用户预先配置的策略模板。本申请实施例不限定标签策略模板包括的具体内容。作为示例，标签策略模板包括敏感度、访问用户、访问进程以及外发权限四个安全维度的标签对应的策略。

S7022：第二设备响应于获取第一设备发送的标签策略模板获取请求，向第一设备发送标签策略模板。

第二设备存储标签策略模板。

S7023：第一设备获取第二设备发送的标签策略模板。

进一步的，在基于标签策略模板生成的文件标签策略信息的基础上，还能够对文件标签策略信息进行自定义地调整。

参见图 9 所示，该图为本申请实施例提供的另一种生成目标文件的文件标签策略信息的流程示意图。该方法应用于第一设备和第二设备，除上述 S701-S703，还包括 S704 和 S705。

S704：第一设备获取针对目标文件的自定义标签策略信息。

在一种可能的实现方式中，第一设备显示用于编辑文件标签策略信息的编辑控件。用户能够通过编辑控件输入针对目标文件的自定义标签策略信息。自定义标签策略信息例如包括增加的附加标签策略信息。作为示例，以图 8 所示的目标文件的文件标签策略信息为例，附加标签策略信息包括新增的访问用户策略信息：U2 类型用户具有读取权限和写入权限，U3 类型用户具有读取权限、写入权限和打印权限，P2 类型进程具有只读权限，P3 类型进程具有读取权限和写入权限。自定义标签策略信息又例如包括修正标签策略信息。修正标签策略信息包括目标文件的文件标签策略信息需要修改的标签策略信息，以及包括修改后的标签策略信息。

S705：第一设备利用自定义标签策略信息更新目标文件的文件标签策略信息。

如此能够在快速配置目标文件的文件标签策略信息的基础上，实现对目标文件的灵活调整，使得生成的目标文件的文件标签策略信息更为符合目标文件的数据安全需求。

此外，在存储场景中，参见图 4a 所示，第一设备为存储设备。存储设备与第三设备连接。第三设备例如生产主机。生产主机为与存储设备连接的能够访问存储设备内存储的数据的主机。存储设备与生产主机之间通过安全协议交互。本申请实施例不限定安全协议的类型。作为一种示例，安全协议为网络附属存储（Network Attached Storage，NAS）协议，或者为对象存储服务（Object Storage Service，OBS）协议。

在一种可能的实现方式中，请求对象利用与第一设备连接的第三设备实现文件的访问。请求对象在第三设备触发针对目标文件的文件访问请求。第三设备利用安全协议封装文件访问请求。第三设备向第一设备发送封装后的文件访问请求。第一设备利用安全协议解封获取的文件访问请求。

此外，在按照请求对象的权限策略信息，执行对请求对象访问目标文件的访问控制时，第一设备按照请求对象的权限策略信息以及请求对象的访问操作信息，生成反馈文件信息。第一设备向第三设备发

送利用安全协议封装后的反馈文件信息。第三设备在获取反馈文件信息，利用安全协议解封反馈文件信息。

如此利用安全协议封装和解封第一设备与第三设备之间交互的信息，能够提高第一设备与第三设备之间交互的安全性，满足访问文件的安全需求。

在针对存储设备的文件配置目标文件的文件标签策略信息的过程中，能够由第三设备的用户或者，由第三设备自动触发生成目标文件的文件标签。第三设备利用安全协议，封装目标文件的文件标签，向第一设备发送封装后的目标文件的文件标签。第一设备获取利用安全协议封装的目标文件的文件标签。第一设备利用安全协议解封封装后的目标文件的文件标签，得到目标文件的文件标签。

本申请还提供一种文件访问装置 1000，该装置应用于第一设备，如图 10 所示，包括：

获取模块，用于获取由请求对象触发的针对目标文件的文件访问请求，所述文件访问请求包括访问操作信息，所述访问操作信息用于描述所述请求对象需要对所述目标文件执行的访问操作；所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

处理模块，用于获取所述请求对象的权限策略信息，所述权限策略信息是基于所述目标文件的文件标签策略信息以及所述文件访问请求确定的；所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述权限策略信息用于指示所述请求对象具有的操作目标文件的权限；所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成；

控制模块，用于按照所述权限策略信息执行对所述请求对象访问所述目标文件的访问控制。

在一种可能的实现方式中，所述处理模块，具体用于根据所述目标文件的文件标签策略信息以及所述请求对象的所述文件访问请求，生成所述请求对象的权限策略信息。

在一种可能的实现方式中，所述处理模块，具体用于向第二设备发送针对所述目标文件的权限请求，所述权限请求包括所述目标文件的文件标签策略信息、所述访问操作信息以及所述请求对象的公钥，所述目标文件的文件标签策略信息由所述目标文件的公钥加密；获取所述第二设备反馈的权限信息，所述权限信息包括第一密文，所述第一密文包括利用所述请求对象的公钥对请求对象的权限策略信息加密得到的密文，所述请求对象的权限策略信息是所述第二设备利用所述目标文件的私钥、所述目标文件的文件标签策略信息以及所述访问操作信息处理得到的；利用所述请求对象的私钥对所述第一密文进行解密，得到所述请求对象的权限策略信息。

在一种可能的实现方式中，所述目标文件利用文件加密密钥加密，所述文件加密密钥封装在所述目标文件的文件标签策略信息中，所述权限信息还包括利用所述请求对象的公钥对所述文件加密密钥加密得到的第二密文，所述处理模块还用于若基于所述权限策略信息，确定所述请求对象具有访问权限，利用所述文件加密密钥对所述目标文件进行解密，所述文件加密密钥为利用所述请求对象的私钥对所述第二密文进行解密得到的。

在一种可能的实现方式中，所述获取模块，还用于获取目标文件的文件标签；

生成模块，用于基于所述文件标签以及标签策略模板，生成所述目标文件的文件标签策略信息。

在一种可能的实现方式中，所述标签策略模板是从第二设备获取的。

在一种可能的实现方式中，所述获取模块，还用于获取针对所述目标文件的自定义标签策略信息；

所述生成模块，还用于利用所述自定义标签策略信息更新所述目标文件的文件标签策略信息。

在一种可能的实现方式中，所述第一设备为主机。

在一种可能的实现方式中，所述装置应用于所述第一设备的应用层。

在一种可能的实现方式中，所述装置应用于所述第一设备的系统层。

在一种可能的实现方式中，所述应用程序为预设安全应用程序。

在一种可能的实现方式中，所述第一设备为存储设备，所述获取模块，具体用于获取第三设备发送的由请求对象触发的针对目标文件的文件访问请求，所述文件访问请求由所述第三设备利用安全协议封装；利用所述安全协议解封所述文件访问请求。

在一种可能的实现方式中，所述控制模块，具体用于按照所述请求对象的权限策略信息以及所述请求对象的访问操作信息，生成反馈文件信息，向所述第三设备发送利用安全协议封装后的所述反馈文件

信息。

其中，获取模块、处理模块和控制模块均可以通过软件实现，或者可以通过硬件实现。示例性的，接下来以获取模块为例，介绍获取模块的实现方式。类似的，处理模块和控制模块的实现方式可以参考获取模块的实现方式。

模块作为软件功能单元的一种举例，获取模块可以包括运行在计算实例上的代码。其中，计算实例可以包括物理主机（计算设备）、虚拟机、容器中的至少一种。进一步地，上述计算实例可以是一台或者多台。例如，获取模块可以包括运行在多个主机/虚拟机/容器上的代码。需要说明的是，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的区域（region）中，也可以分布在不同的 region 中。进一步地，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的可用区（availability zone，AZ）中，也可以分布在不同的 AZ 中，每个 AZ 包括一个数据中心或多个地理位置相近的数据中心。其中，通常一个 region 可以包括多个 AZ。

同样，用于运行该代码的多个主机/虚拟机/容器可以分布在同一个虚拟私有云（virtual private cloud，VPC）中，也可以分布在多个 VPC 中。其中，通常一个 VPC 设置在一个 region 内，同一 region 内两个 VPC 之间，以及不同 region 的 VPC 之间跨区通信需在每个 VPC 内设置通信网关，经通信网关实现 VPC 之间的互连。

模块作为硬件功能单元的一种举例，获取模块可以包括至少一个计算设备，如服务器等。或者，获取模块也可以是利用专用集成电路（application-specific integrated circuit，ASIC）实现、或可编程逻辑器件（programmable logic device，PLD）实现的设备等。其中，上述 PLD 可以是复杂程序逻辑器件（complex programmable logical device，CPLD）、现场可编程门阵列（field-programmable gate array，FPGA）、通用阵列逻辑（generic array logic，GAL）或其任意组合实现。

获取模块包括的多个计算设备可以分布在相同的 region 中，也可以分布在不同的 region 中。获取模块包括的多个计算设备可以分布在相同的 AZ 中，也可以分布在不同的 AZ 中。同样，获取模块包括的多个计算设备可以分布在同一个 VPC 中，也可以分布在多个 VPC 中。其中，所述多个计算设备可以是服务器、ASIC、PLD、CPLD、FPGA 和 GAL 等计算设备的任意组合。

需要说明的是，在其他实施例中，获取模块可以用于执行文件访问方法中的任意步骤，处理模块可以用于执行文件访问方法中的任意步骤，控制模块可以用于执行文件访问方法中的任意步骤，获取模块、处理模块和控制模块负责实现的步骤可根据需要指定，通过获取模块、处理模块和控制模块分别实现文件访问方法中不同的步骤来实现文件访问装置的全部功能。

本申请还提供一种文件访问权限确定装置 1100，所述装置应用于第二设备，如图 11 所示，所述装置包括：

获取模块，用于获取第一设备发送的针对所述目标文件的权限请求，所述权限请求包括所述目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，所述文件标签策略信息由所述目标文件的公钥加密，所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成，所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

解密模块，用于利用所述目标文件的私钥对所述文件标签策略信息解密；

确定模块，用于基于所述目标文件的文件标签策略信息和所述访问操作信息确定请求对象的权限策略信息，所述权限策略信息用于描述所述请求对象针对所述目标文件的访问操作的权限策略；

加密模块，用于利用所述请求对象的公钥对所述请求对象的权限策略信息加密，得到第一密文；

发送模块，用于向所述第一设备发送权限信息，所述权限信息包括所述第一密文。

在一种可能的实现方式中，所述目标文件利用文件加密密钥加密，所述文件加密密钥封装在所述目标文件的文件标签策略信息中，所述加密模块，还用于利用所述请求对象的公钥对所述文件加密密钥加密得到第二密文，所述权限信息还包括所述第二密文。

在一种可能的实现方式中，所述发送模块，还用于响应于获取所述第一设备发送的标签策略模板获取请求，向所述第一设备发送标签策略模板。

在一种可能的实现方式中，第二设备为服务器，或者管理设备。

其中，获取模块、解密模块、确定模块、加密模块和发送模块均可以通过软件实现，或者可以通过硬件实现。示例性的，接下来以获取模块为例，介绍获取模块的实现方式。类似的，解密模块、确定模块、加密模块和发送模块的实现方式可以参考获取模块的实现方式。

模块作为软件功能单元的一种举例，获取模块可以包括运行在计算实例上的代码。其中，计算实例可以包括物理主机（计算设备）、虚拟机、容器中的至少一种。进一步地，上述计算实例可以是一台或者多台。例如，获取模块可以包括运行在多个主机/虚拟机/容器上的代码。需要说明的是，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的区域（region）中，也可以分布在不同的 region 中。进一步地，用于运行该代码的多个主机/虚拟机/容器可以分布在相同的可用区（availability zone，AZ）中，也可以分布在不同的 AZ 中，每个 AZ 包括一个数据中心或多个地理位置相近的数据中心。其中，通常一个 region 可以包括多个 AZ。

同样，用于运行该代码的多个主机/虚拟机/容器可以分布在同一个虚拟私有云（virtual private cloud，VPC）中，也可以分布在多个 VPC 中。其中，通常一个 VPC 设置在一个 region 内，同一 region 内两个 VPC 之间，以及不同 region 的 VPC 之间跨区通信需在每个 VPC 内设置通信网关，经通信网关实现 VPC 之间的互连。

模块作为硬件功能单元的一种举例，获取模块可以包括至少一个计算设备，如服务器等。或者，获取模块也可以是利用专用集成电路（application-specific integrated circuit，ASIC）实现、或可编程逻辑器件（programmable logic device，PLD）实现的设备等。其中，上述 PLD 可以是复杂程序逻辑器件（complex programmable logical device，CPLD）、现场可编程门阵列（field-programmable gate array，FPGA）、通用阵列逻辑（generic array logic，GAL）或其任意组合实现。

获取模块包括的多个计算设备可以分布在相同的 region 中，也可以分布在不同的 region 中。获取模块包括的多个计算设备可以分布在相同的 AZ 中，也可以分布在不同的 AZ 中。同样，获取模块包括的多个计算设备可以分布在同一个 VPC 中，也可以分布在多个 VPC 中。其中，所述多个计算设备可以是服务器、ASIC、PLD、CPLD、FPGA 和 GAL 等计算设备的任意组合。

需要说明的是，在其他实施例中，获取模块可以用于执行文件访问权限确定方法中的任意步骤，解密模块可以用于执行文件访问权限确定方法中的任意步骤，确定模块可以用于执行文件访问权限确定方法中的任意步骤，加密模块可以用于执行文件访问权限确定方法中的任意步骤，发送模块可以用于执行文件访问权限确定方法中的任意步骤，获取模块、解密模块、确定模块、加密模块和发送模块负责实现的步骤可根据需要指定，通过获取模块、解密模块、确定模块、加密模块和发送模块分别实现文件访问权限确定方法中不同的步骤来实现文件访问权限确定装置的全部功能。

本申请还提供一种计算设备 1200。如图 12 所示，计算设备 1200 包括：总线 1202、处理器 1204、存储器 1206 和通信接口 1208。处理器 1204、存储器 1206 和通信接口 1208 之间通过总线 1202 通信。计算设备 1200 可以是服务器或终端设备。应理解，本申请不限定计算设备 1200 中的处理器、存储器的个数。

总线 1202 可以是外设部件互连标准（peripheral component interconnect，PCI）总线或扩展工业标准结构（extended industry standard architecture，EISA）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 12 中仅用一条线表示，但并不表示仅有一根总线或一种类型的总线。总线 1202 可包括在计算设备 1200 各个部件（例如，存储器 1206、处理器 1204、通信接口 1208）之间传送信息的通路。

处理器 1204 可以包括中央处理器(central processing unit，CPU)、图形处理器（graphics processing unit，GPU）、微处理器（micro processor，MP）或者数字信号处理器（digital signal processor，DSP）等处理器中的任意一种或多种。

存储器 1206 可以包括易失性存储器(volatile memory)，例如随机存取存储器(random access memory，RAM)。处理器 1204 还可以包括非易失性存储器(non-volatile memory)，例如只读存储器(read-only memory，ROM)，快闪存储器，机械硬盘（hard disk drive，HDD）或固态硬盘（solid state drive，SSD）。

存储器 1206 中存储有可执行的程序代码，处理器 1204 执行该可执行的程序代码以分别实现前述获

取模块、处理模块和控制模块的功能，从而实现文件访问方法。也即，存储器 1206 上存有用于执行文件访问方法的指令。

或者，存储器 1206 中存储有可执行的代码，处理器 1204 执行该可执行的代码以分别实现前述获取模块、解密模块、确定模块、加密模块和发送模块的功能，从而实现文件访问方法。也即，存储器 1206 上存有用于执行文件访问权限确定方法的指令。

通信接口 1208 使用例如但不限于网络接口卡、收发器一类的收发模块，来实现计算设备 1200 与其他设备或通信网络之间的通信。

本申请实施例还提供了一种计算设备集群。该计算设备集群包括至少一台计算设备。该计算设备可以是服务器，例如是中心服务器、边缘服务器，或者是本地数据中心中的本地服务器。在一些实施例中，计算设备也可以是台式机、笔记本电脑或者智能手机等终端设备。

如图 13 所示，所述计算设备集群包括至少一个计算设备 1200。计算设备集群中的一个或多个计算设备 1200 中的存储器 1206 中可以存有相同的用于执行文件访问方法的指令。

在一些可能的实现方式中，该计算设备集群中的一个或多个计算设备 1200 的存储器 1206 中也可以分别存有用于执行文件访问方法的部分指令。换言之，一个或多个计算设备 1200 的组合可以共同执行用于执行文件访问方法的指令。

需要说明的是，计算设备集群中的不同的计算设备 1200 中的存储器 1206 可以存储不同的指令，分别用于执行文件访问装置的部分功能。也即，不同的计算设备 1200 中的存储器 1206 存储的指令可以实现获取模块、处理模块和控制模块中的一个或多个模块的功能。

在一些可能的实现方式中，计算设备集群中的一个或多个计算设备可以通过网络连接。其中，所述网络可以是广域网或局域网等等。图 14 示出了一种可能的实现方式。如图 14 所示，两个计算设备 1200A 和 1200B 之间通过网络进行连接。具体地，通过各个计算设备中的通信接口与所述网络进行连接。在这一类可能的实现方式中，计算设备 1200A 中的存储器 1206 中存有执行获取模块的功能的指令。同时，计算设备 1200B 中的存储器 1206 中存有执行处理模块和控制模块的功能的指令。

图 14 所示的计算设备集群之间的连接方式可以是考虑到本申请提供的文件访问方法需要例如处理大量数据，因此考虑将处理模块和控制模块实现的功能交由计算设备 1200B 执行。

应理解，图 14 中示出的计算设备 1200A 的功能也可以由多个计算设备 1200 完成。同样，计算设备 1200B 的功能也可以由多个计算设备 1200 完成。

本申请实施例还提供了另一种计算设备集群。该计算设备集群中各计算设备之间的连接关系可以类似的参考图 13 和图 14 所述计算设备集群的连接方式。不同的是，该计算设备集群中的一个或多个计算设备 1200 中的存储器 1206 中可以存有相同的用于执行文件访问权限确定方法的指令。

在一些可能的实现方式中，该计算设备集群中的一个或多个计算设备 1200 的存储器 1206 中也可以分别存有用于执行文件访问权限确定方法的部分指令。换言之，一个或多个计算设备 1200 的组合可以共同执行用于执行文件访问权限确定方法的指令。

需要说明的是，计算设备集群中的不同的计算设备 1200 中的存储器 1206 可以存储不同的指令，用于执行文件访问权限确定的部分功能。也即，不同的计算设备 1200 中的存储器 1206 存储的指令可以实现获取模块、解密模块、确定模块、加密模块和发送模块中的一个或多个装置的功能。

本申请实施例还提供了一种包含指令的计算机程序产品。所述计算机程序产品可以是包含指令的，能够运行在计算设备上或被储存在任何可用介质中的软件或程序产品。当所述计算机程序产品在至少一个计算设备上运行时，使得至少一个计算设备执行文件访问方法，或文件访问权限确定方法。

本申请实施例还提供了一种计算机可读存储介质。所述计算机可读存储介质可以是计算设备能够存储的任何可用介质或者是包含一个或多个可用介质的数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘）等。该计算机可读存储介质包括指令，所述指令指示计算设备执行文件访问方法，或指示计算设备执行文件访问权限确定方法。

最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技

术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的保护范围。

权 利 要 求 书

1.一种文件访问方法，其特征在于，所述方法应用于第一设备，所述方法包括：

获取由请求对象触发的针对目标文件的文件访问请求，所述文件访问请求包括访问操作信息，所述访问操作信息用于描述所述请求对象需要对所述目标文件执行的访问操作；所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

获取所述请求对象的权限策略信息，所述权限策略信息是基于所述目标文件的文件标签策略信息以及所述文件访问请求确定的；所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述权限策略信息用于指示所述请求对象具有的操作目标文件的权限；所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成；

按照所述权限策略信息执行对所述请求对象访问所述目标文件的访问控制。

2.根据权利要求 1 所述的方法，其特征在于，所述获取所述请求对象的权限策略信息，包括：

根据所述目标文件的文件标签策略信息以及所述请求对象的所述文件访问请求，生成所述请求对象的权限策略信息。

3.根据权利要求 1 所述的方法，其特征在于，所述获取所述请求对象的权限策略信息，包括：

向第二设备发送针对所述目标文件的权限请求，所述权限请求包括所述目标文件的文件标签策略信息、所述访问操作信息以及所述请求对象的公钥，所述目标文件的文件标签策略信息由所述目标文件的公钥加密；

获取所述第二设备反馈的权限信息，所述权限信息包括第一密文，所述第一密文包括利用所述请求对象的公钥对请求对象的权限策略信息加密得到的密文，所述请求对象的权限策略信息是所述第二设备利用所述目标文件的私钥、所述目标文件的文件标签策略信息以及所述访问操作信息处理得到的；

利用所述请求对象的私钥对所述第一密文进行解密，得到所述请求对象的权限策略信息。

4.根据权利要求 3 所述的方法，其特征在于，所述目标文件利用文件加密密钥加密，所述文件加密密钥封装在所述目标文件的文件标签策略信息中，所述权限信息还包括利用所述请求对象的公钥对所述文件加密密钥加密得到的第二密文，在所述按照所述请求对象的权限策略信息，执行对所述请求对象访问所述目标文件的访问控制之前，所述方法还包括：

若基于所述权限策略信息，确定所述请求对象具有访问权限，利用所述文件加密密钥对所述目标文件进行解密，所述文件加密密钥为利用所述请求对象的私钥对所述第二密文进行解密得到的。

5.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

获取目标文件的文件标签；

基于所述文件标签以及标签策略模板，生成所述目标文件的文件标签策略信息。

6.根据权利要求 5 所述的方法，其特征在于，所述标签策略模板是从第二设备获取的。

7.根据权利要求 5 所述的方法，其特征在于，所述方法还包括：

获取针对所述目标文件的自定义标签策略信息；

利用所述自定义标签策略信息更新所述目标文件的文件标签策略信息。

8.根据权利要求 1 所述的方法，其特征在于，所述第一设备为主机。

9.根据权利要求 8 所述的方法，其特征在于，所述方法应用于所述第一设备的应用层。

10.根据权利要求 8 或 9 所述的方法，其特征在于，所述方法应用于所述第一设备的系统层。

11.根据权利要求 10 所述的方法，其特征在于，所述应用程序为预设安全应用程序。

12.根据权利要求 1 所述的方法，其特征在于，所述第一设备为存储设备，所述获取由请求对象触发的针对目标文件的文件访问请求，包括：

获取第三设备发送的由请求对象触发的针对目标文件的文件访问请求，所述文件访问请求由所述第三设备利用安全协议封装；

利用所述安全协议解封所述文件访问请求。

13.根据权利要求 12 所述的方法，其特征在于，所述按照所述权限策略信息执行对所述请求对象访

问所述目标文件的访问控制，包括：

按照所述请求对象的权限策略信息以及所述请求对象的访问操作信息，生成反馈文件信息，向所述第三设备发送利用安全协议封装后的所述反馈文件信息。

14.一种文件访问权限确定方法，其特征在于，所述方法应用于第二设备，所述方法包括：

获取第一设备发送的针对所述目标文件的权限请求，所述权限请求包括所述目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，所述文件标签策略信息由所述目标文件的公钥加密，所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成，所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

利用所述目标文件的私钥对所述文件标签策略信息解密；

基于所述目标文件的文件标签策略信息和所述访问操作信息确定请求对象的权限策略信息，所述权限策略信息用于描述所述请求对象针对所述目标文件的访问操作的权限策略；

利用所述请求对象的公钥对所述请求对象的权限策略信息加密，得到第一密文；

向所述第一设备发送权限信息，所述权限信息包括所述第一密文。

15.根据权利要求 14 所述的方法，其特征在于，所述目标文件利用文件加密密钥加密，所述文件加密密钥封装在所述目标文件的文件标签策略信息中，所述方法还包括：

利用所述请求对象的公钥对所述文件加密密钥加密得到第二密文，所述权限信息还包括所述第二密文。

16.根据权利要求 14 所述的方法，其特征在于，所述方法还包括：

响应于获取所述第一设备发送的标签策略模板获取请求，向所述第一设备发送标签策略模板。

17.根据权利要求 14-16 任一项所述的方法，其特征在于，所述第二设备为服务器，或者管理设备。

18.一种文件访问装置，其特征在于，所述装置应用于第一设备，所述装置包括：

获取模块，用于获取由请求对象触发的针对目标文件的文件访问请求，所述文件访问请求包括访问操作信息，所述访问操作信息用于描述所述请求对象需要对所述目标文件执行的访问操作；所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

处理模块，用于获取所述请求对象的权限策略信息，所述权限策略信息是基于所述目标文件的文件标签策略信息以及所述文件访问请求确定的；所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述权限策略信息用于指示所述请求对象具有的操作目标文件的权限；所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成；

控制模块，用于按照所述权限策略信息执行对所述请求对象访问所述目标文件的访问控制。

19.一种文件访问权限确定装置，其特征在于，所述装置应用于第二设备，所述装置包括：

获取模块，用于获取第一设备发送的针对所述目标文件的权限请求，所述权限请求包括所述目标文件的文件标签策略信息、访问操作信息以及请求对象的公钥，所述文件标签策略信息由所述目标文件的公钥加密，所述文件标签策略信息与所述目标文件的文件标签对应，所述文件标签策略信息用于描述针对所述目标文件的访问操作的控制策略，所述文件标签包括一种或者多种安全维度的标签，所述文件标签由所述目标文件的管理者设置或者基于所述目标文件的文件属性生成，所述请求对象为所述第一设备的操作系统程序的系统用户，或者为应用程序的应用用户；

解密模块，用于利用所述目标文件的私钥对所述文件标签策略信息解密；

确定模块，用于基于所述目标文件的文件标签策略信息和所述访问操作信息确定请求对象的权限策略信息，所述权限策略信息用于描述所述请求对象针对所述目标文件的访问操作的权限策略；

加密模块，用于利用所述请求对象的公钥对所述请求对象的权限策略信息加密，得到第一密文；

发送模块，用于向所述第一设备发送权限信息，所述权限信息包括所述第一密文。

20.一种计算设备集群，其特征在于，包括至少一个计算设备，每个计算设备包括处理器和存储器；

所述至少一个计算设备的处理器用于执行所述至少一个计算设备的存储器中存储的指令，以使得所

述计算设备集群执行如权利要求1-13任一项所述的方法，或者执行如权利要求14-17任一项所述的方法。

21.一种包含指令的计算机程序产品，其特征在于，当所述指令被计算设备集群运行时，使得所述计算设备集群执行如权利要求的1-13任一项所述的方法，或者执行如权利要求14-17任一项所述的方法。

22.一种计算机可读存储介质，其特征在于，包括计算机程序指令，当所述计算机程序指令由计算设备集群执行时，所述计算设备集群执行如权利要求1-13任一项所述的方法，或者执行如权利要求14-17任一项所述的方法。


第一设备
应用程序
标签策略客户端，
或者标签策略软件开发工具包
操作系统程序

图 1a

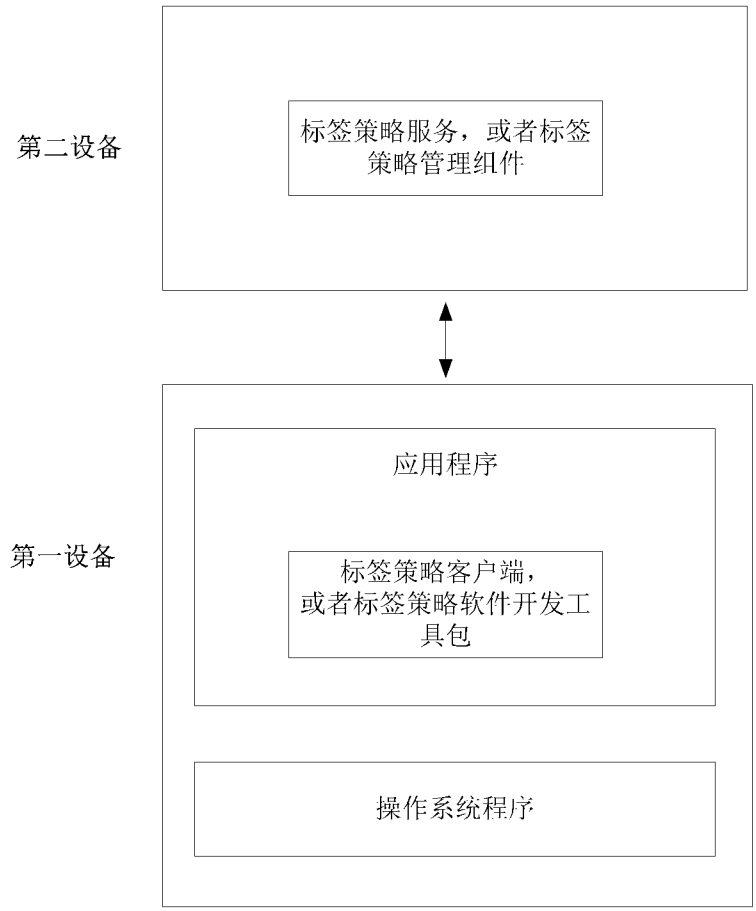
第二设备
标签策略服务，或者标签策略管理组件
第一设备
应用程序
标签策略客户端，
或者标签策略软件开发工具包
操作系统程序

图 1b

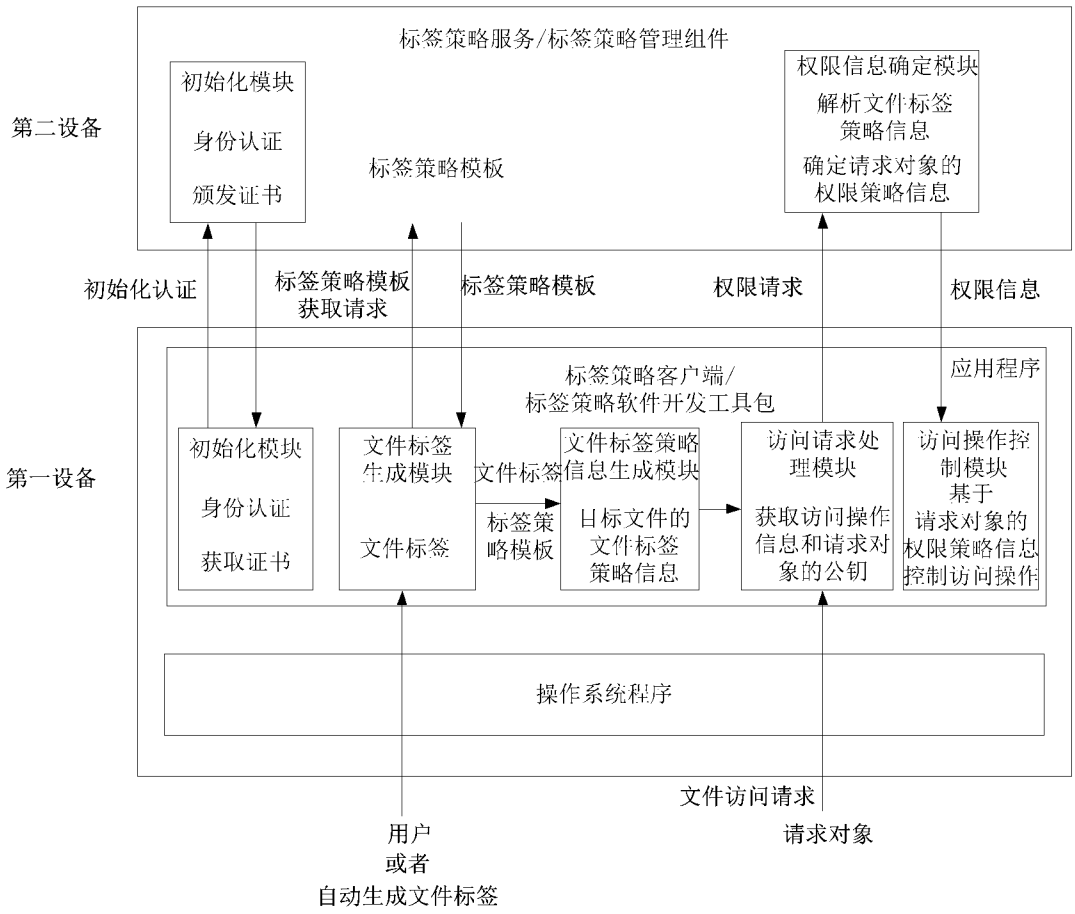
标签策略服务/标签策略管理组件
初始化模块
身份认证
颁发证书
标签策略模板
权限信息确定模块
解析文件标签策略信息
确定请求对象的权限策略信息
第二设备
初始化认证
标签策略模板获取请求
标签策略模板
权限请求
权限信息
标签策略客户端/标签策略软件开发工具包
应用程序
初始化模块
身份认证
获取证书
文件标签生成模块
文件标签
文件标签
标签策略模板
文件标签策略信息生成模块
目标文件的文件标签策略信息
访问请求处理模块
获取访问操作信息和请求对象的公钥
访问操作控制模块
基于请求对象的权限策略信息控制访问操作
第一设备
操作系统程序
文件访问请求
用户
或者
自动生成文件标签
请求对象

图 1c


第一设备
应用程序
操作系统程序
标签内核模块

图 2a

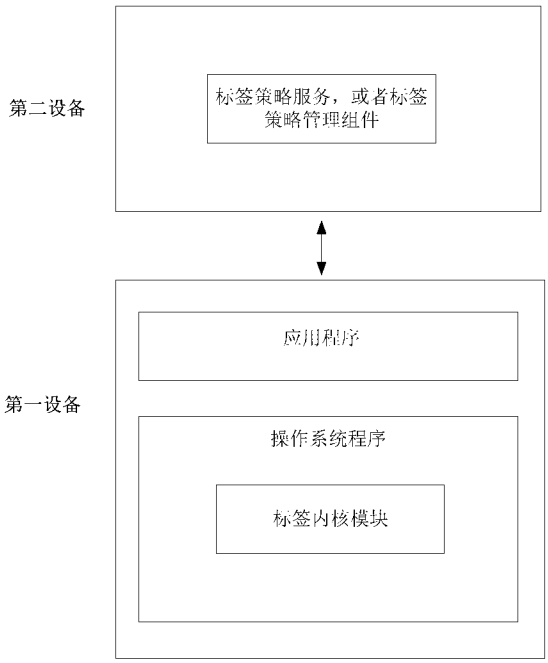
第二设备
标签策略服务，或者标签策略管理组件
第一设备
应用程序
操作系统程序
标签内核模块

图 2b

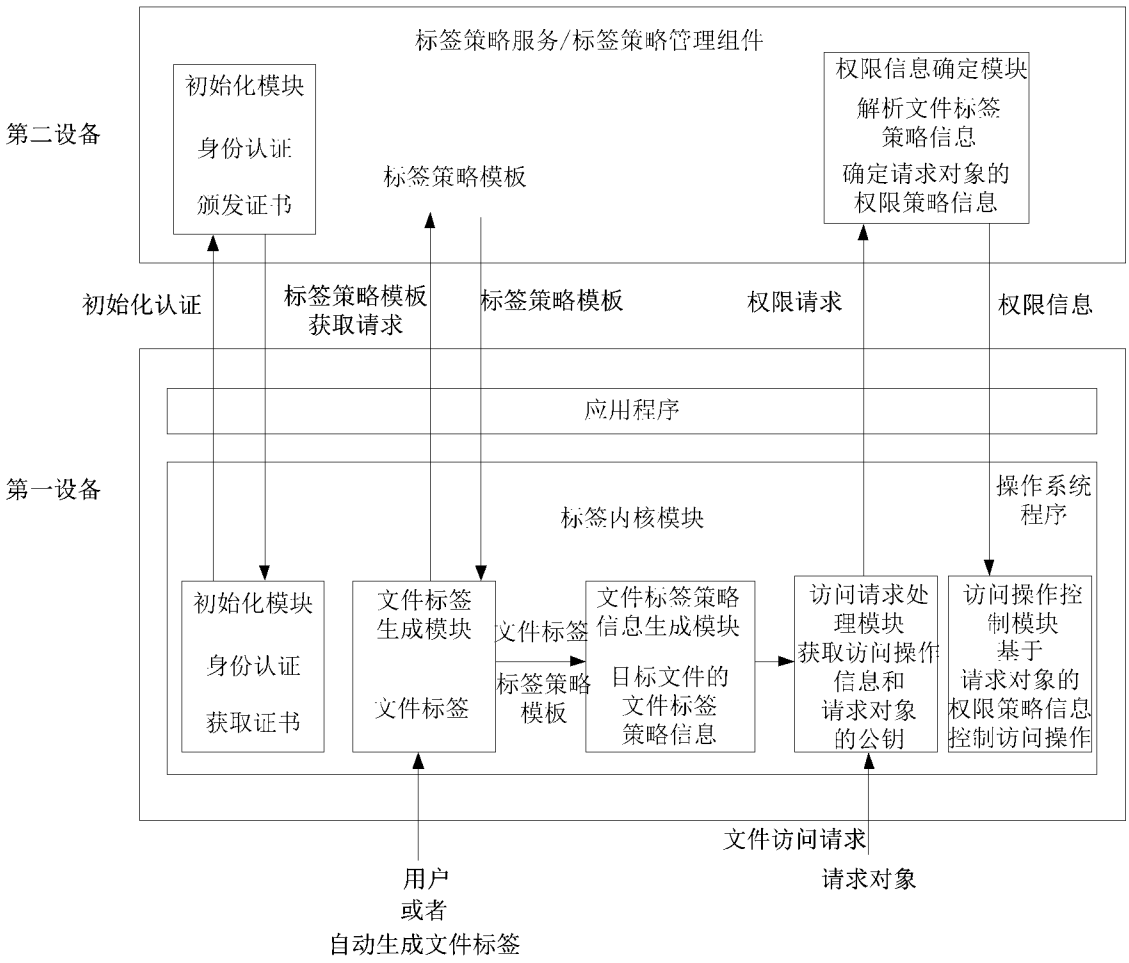
第二设备
标签策略服务/标签策略管理组件
初始化模块
身份认证
颁发证书
标签策略模板
权限信息确定模块
解析文件标签策略信息
确定请求对象的权限策略信息
初始化认证
标签策略模板获取请求
标签策略模板
权限请求
权限信息
第一设备
应用程序
标签内核模块
操作系统程序
初始化模块
身份认证
获取证书
文件标签生成模块
文件标签
文件标签
标签策略模板
文件标签策略信息生成模块
目标文件的文件标签策略信息
访问请求处理模块
获取访问操作信息和请求对象的公钥
访问操作控制模块
基于请求对象的权限策略信息控制访问操作
文件访问请求
用户
或者
自动生成文件标签
请求对象

图 2c

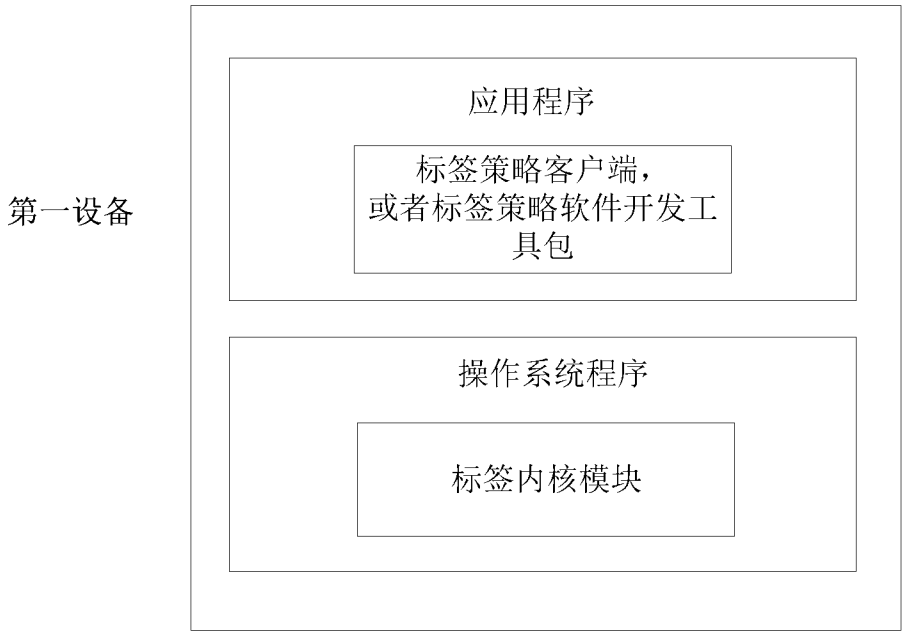
第一设备
应用程序
标签策略客户端，
或者标签策略软件开发工具包
操作系统程序
标签内核模块

图 3a

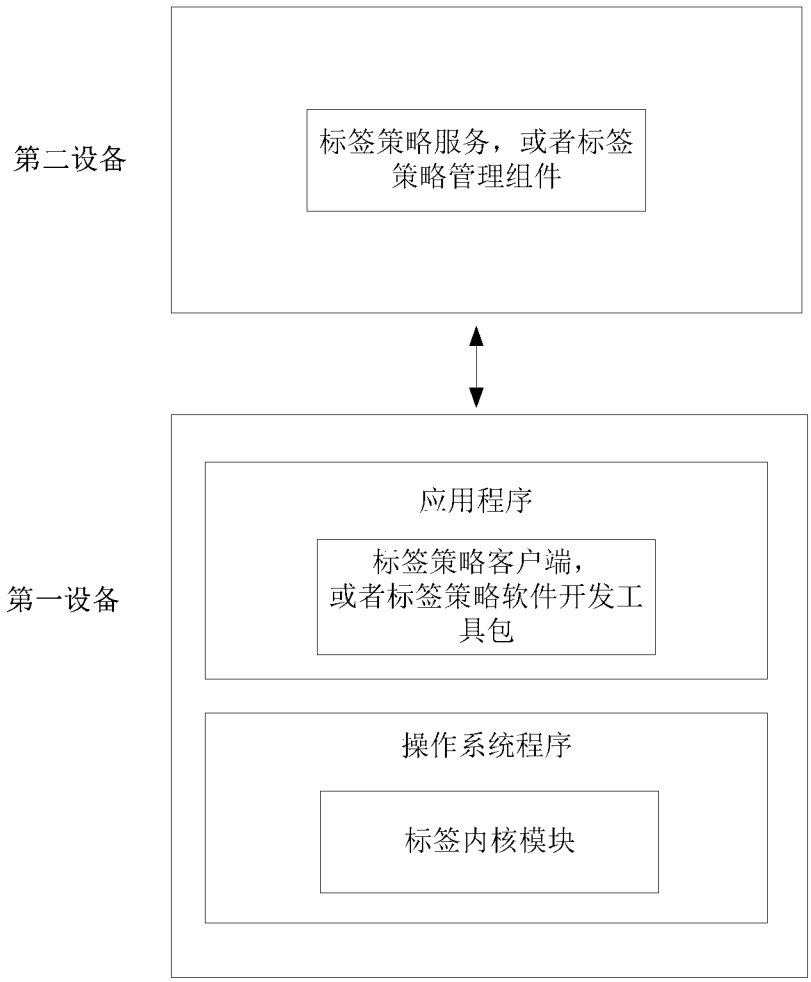
第二设备
标签策略服务，或者标签策略管理组件
第一设备
应用程序
标签策略客户端，
或者标签策略软件开发工具包
操作系统程序
标签内核模块

图 3b

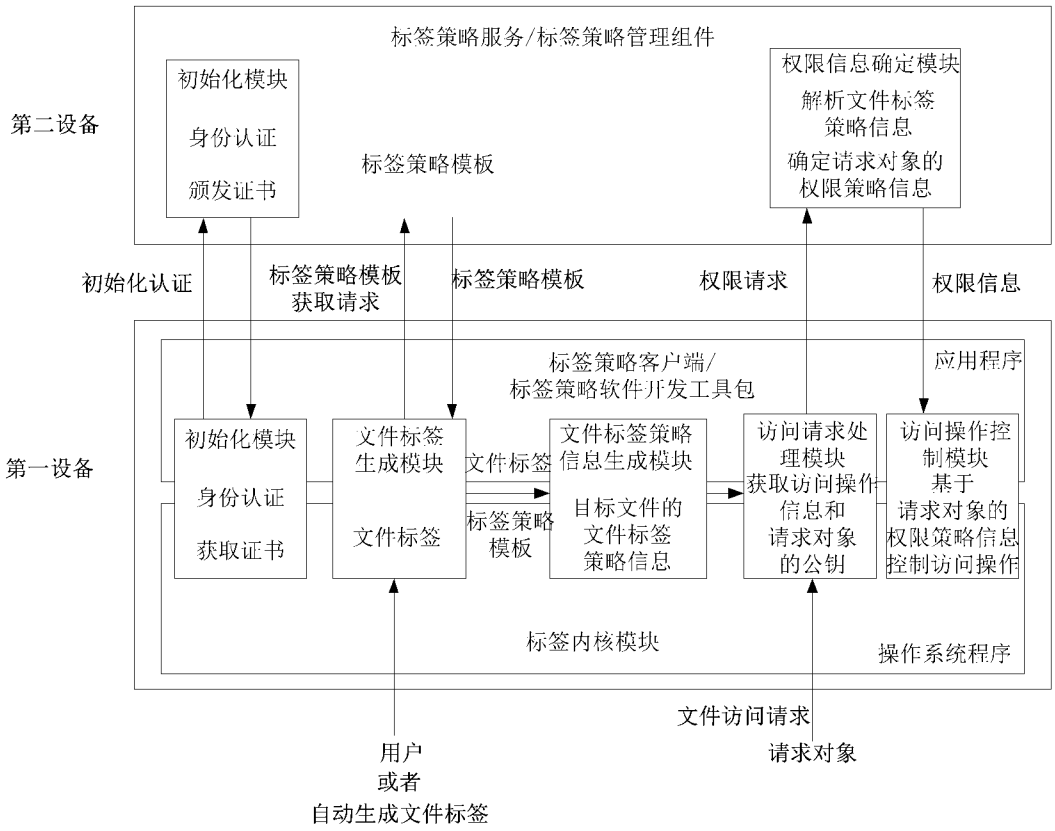
标签策略服务/标签策略管理组件
初始化模块
身份认证
颁发证书
标签策略模板
权限信息确定模块
解析文件标签策略信息
确定请求对象的权限策略信息
第二设备
初始化认证
标签策略模板获取请求
标签策略模板
权限请求
权限信息
标签策略客户端/标签策略软件开发工具包
应用程序
初始化模块
身份认证
获取证书
文件标签生成模块
文件标签
文件标签
标签策略模板
文件标签策略信息生成模块
目标文件的文件标签策略信息
访问请求处理模块
获取访问操作信息和请求对象的公钥
访问操作控制模块
基于请求对象的权限策略信息控制访问操作
第一设备
标签内核模块
操作系统程序
文件访问请求
请求对象
用户
或者
自动生成文件标签

图 3c

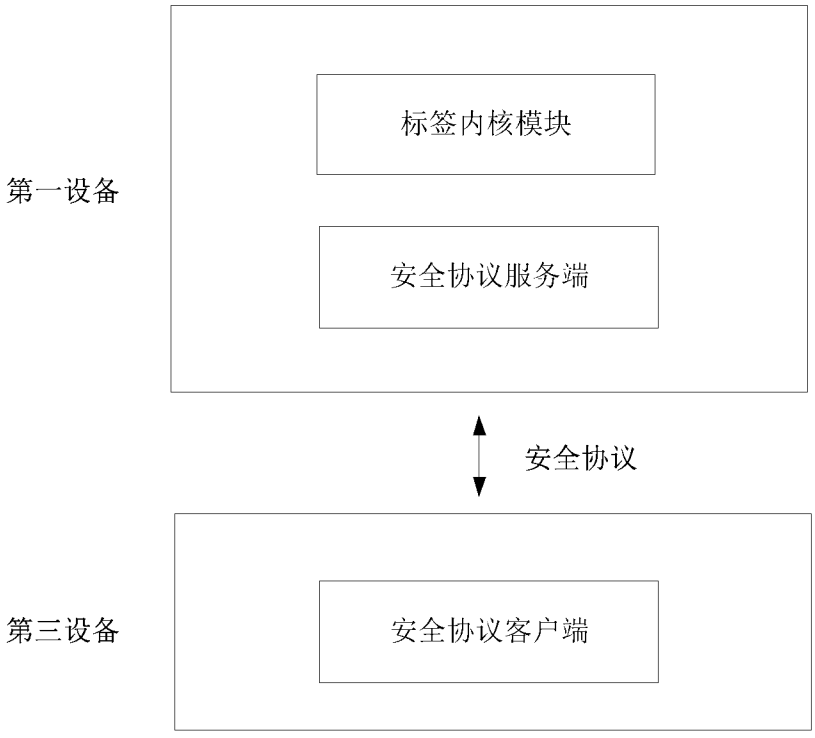
第一设备
标签内核模块
安全协议服务端
安全协议
第三设备
安全协议客户端

图 4a

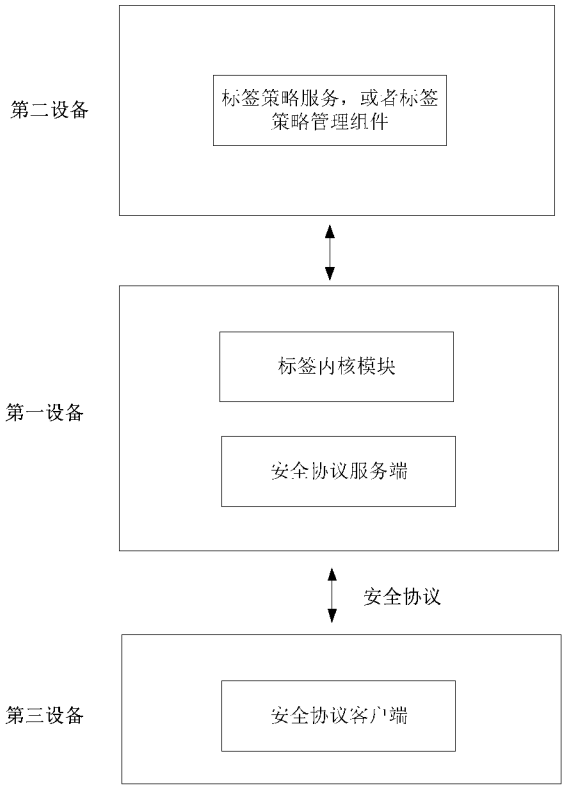
第二设备
标签策略服务，或者标签策略管理组件
第一设备
标签内核模块
安全协议服务端
安全协议
第三设备
安全协议客户端

图 4b

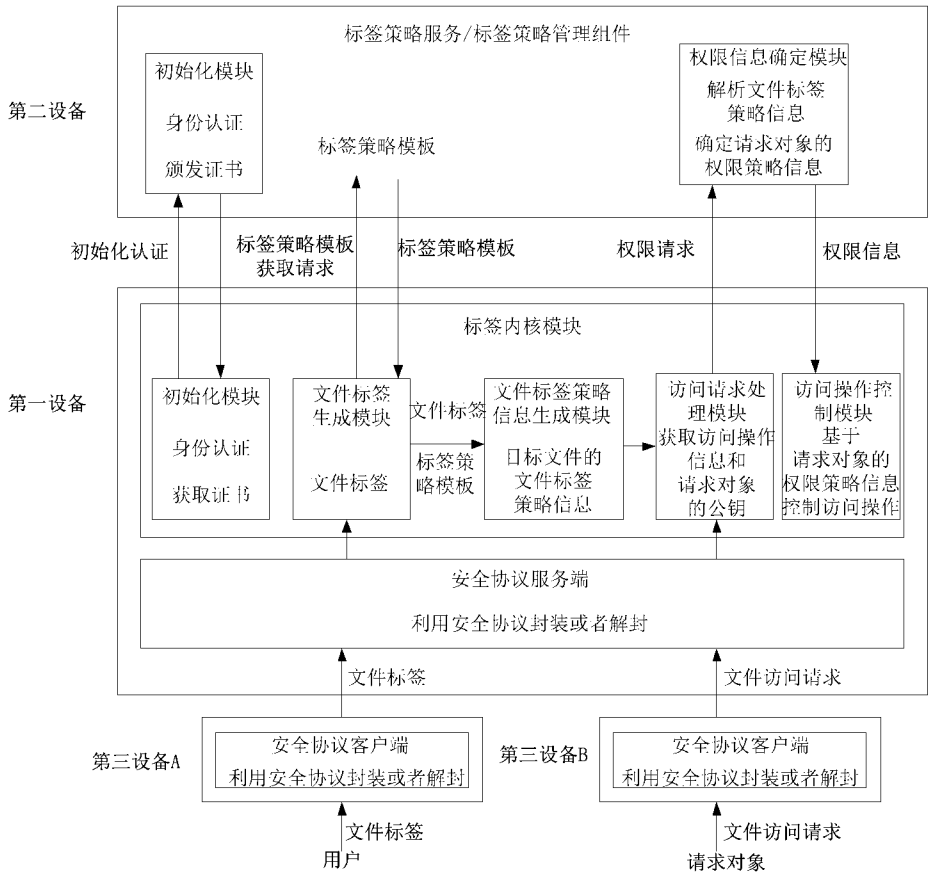
第二设备
标签策略服务/标签策略管理组件
初始化模块
身份认证
颁发证书
标签策略模板
权限信息确定模块
解析文件标签策略信息
确定请求对象的权限策略信息
初始化认证
标签策略模板获取请求
标签策略模板
权限请求
权限信息
第一设备
标签内核模块
初始化模块
身份认证
获取证书
文件标签生成模块
文件标签
文件标签
标签策略模板
文件标签策略信息生成模块
目标文件的文件标签策略信息
访问请求处理模块
获取访问操作信息和请求对象的公钥
访问操作控制模块
基于请求对象的权限策略信息控制访问操作
安全协议服务端
利用安全协议封装或者解封
文件标签
文件访问请求
第三设备A
安全协议客户端
利用安全协议封装或者解封
第三设备B
安全协议客户端
利用安全协议封装或者解封
文件标签
用户
文件访问请求
请求对象

图 4c

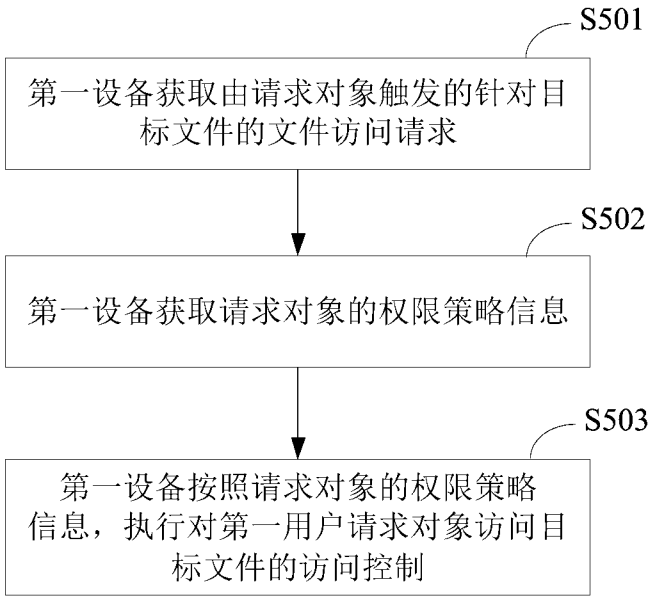
S501
第一设备获取由请求对象触发的针对目标文件的文件访问请求
S502
第一设备获取请求对象的权限策略信息
S503
第一设备按照请求对象的权限策略信息，执行对第一用户请求对象访问目标文件的访问控制

图 5

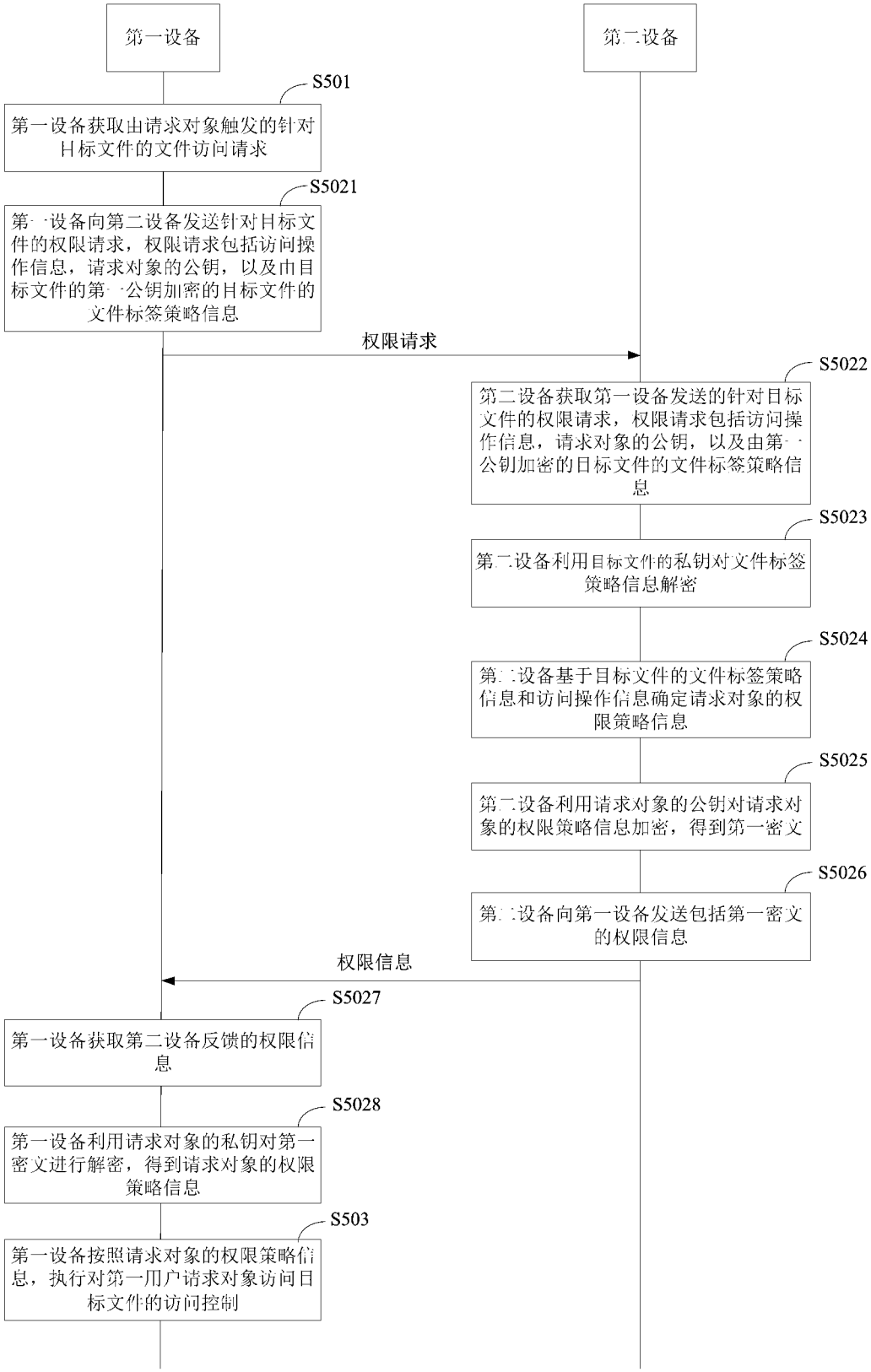
第一设备
第二设备
S501
第一设备获取由请求对象触发的针对目标文件的文件访问请求
S5021
第一设备向第二设备发送针对目标文件的权限请求，权限请求包括访问操作信息，请求对象的公钥，以及由目标文件的第一公钥加密的目标文件的文件标签策略信息
权限请求
S5022
第二设备获取第一设备发送的针对目标文件的权限请求，权限请求包括访问操作信息，请求对象的公钥，以及由第一公钥加密的目标文件的文件标签策略信息
S5023
第二设备利用目标文件的私钥对文件标签策略信息解密
S5024
第二设备基于目标文件的文件标签策略信息和访问操作信息确定请求对象的权限策略信息
S5025
第二设备利用请求对象的公钥对请求对象的权限策略信息加密，得到第一密文
S5026
第二设备向第一设备发送包括第一密文的权限信息
权限信息
S5027
第一设备获取第二设备反馈的权限信息
S5028
第一设备利用请求对象的私钥对第一密文进行解密，得到请求对象的权限策略信息
S503
第一设备按照请求对象的权限策略信息，执行对第一用户请求对象访问目标文件的访问控制

图 6

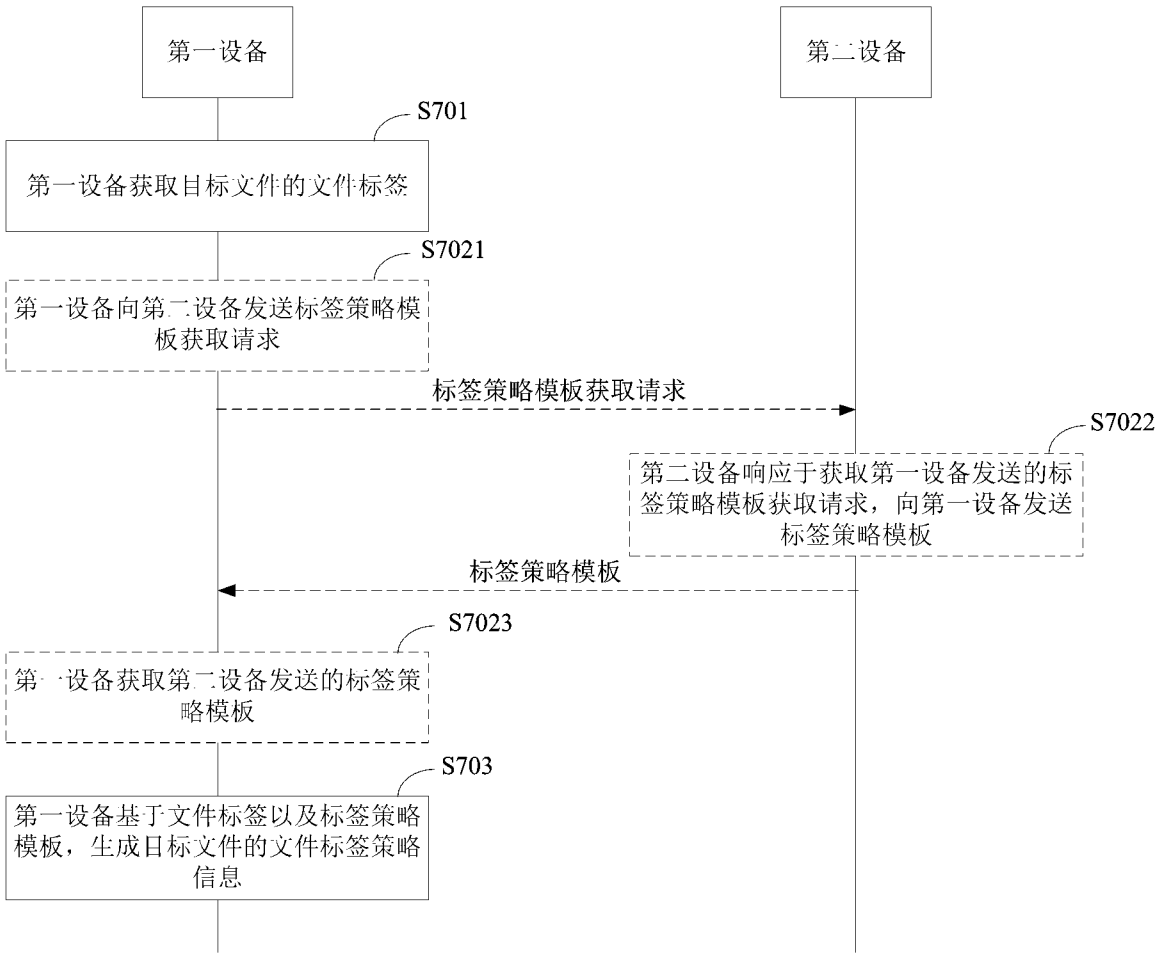
第一设备
第二设备
S701
第一设备获取目标文件的文件标签
S7021
第一设备向第二设备发送标签策略模板获取请求
标签策略模板获取请求
S7022
第二设备响应于获取第一设备发送的标签策略模板获取请求，向第一设备发送标签策略模板
标签策略模板
S7023
第一设备获取第二设备发送的标签策略模板
S703
第一设备基于文件标签以及标签策略模板，生成目标文件的文件标签策略信息

图 7

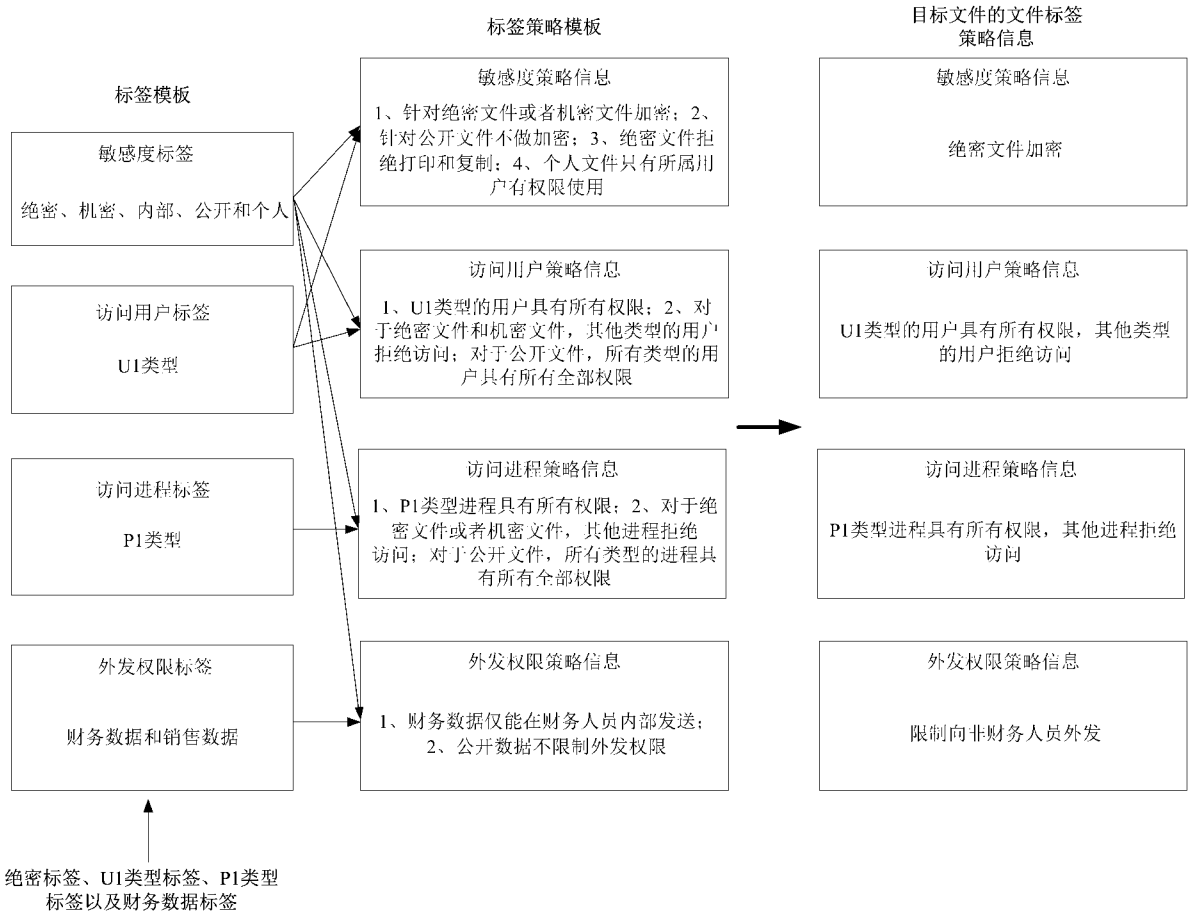
标签模板
敏感度标签
绝密、机密、内部、公开和个人
访问用户标签
U1类型
访问进程标签
P1类型
外发权限标签
财务数据和销售数据
绝密标签、U1类型标签、P1类型标签以及财务数据标签
标签策略模板
敏感度策略信息
1、针对绝密文件或者机密文件加密；2、针对公开文件不做加密；3、绝密文件拒绝打印和复制；4、个人文件只有所属用户有权限使用
访问用户策略信息
1、U1类型的用户具有所有权限；2、对于绝密文件和机密文件，其他类型的用户拒绝访问；对于公开文件，所有类型的用户具有所有全部权限
访问进程策略信息
1、P1类型进程具有所有权限；2、对于绝密文件或者机密文件，其他进程拒绝访问；对于公开文件，所有类型的进程具有所有全部权限
外发权限策略信息
1、财务数据仅能在财务人员内部发送；2、公开数据不限制外发权限
目标文件的文件标签策略信息
敏感度策略信息
绝密文件加密
访问用户策略信息
U1类型的用户具有所有权限，其他类型的用户拒绝访问
访问进程策略信息
P1类型进程具有所有权限，其他进程拒绝访问
外发权限策略信息
限制向非财务人员外发

图 8

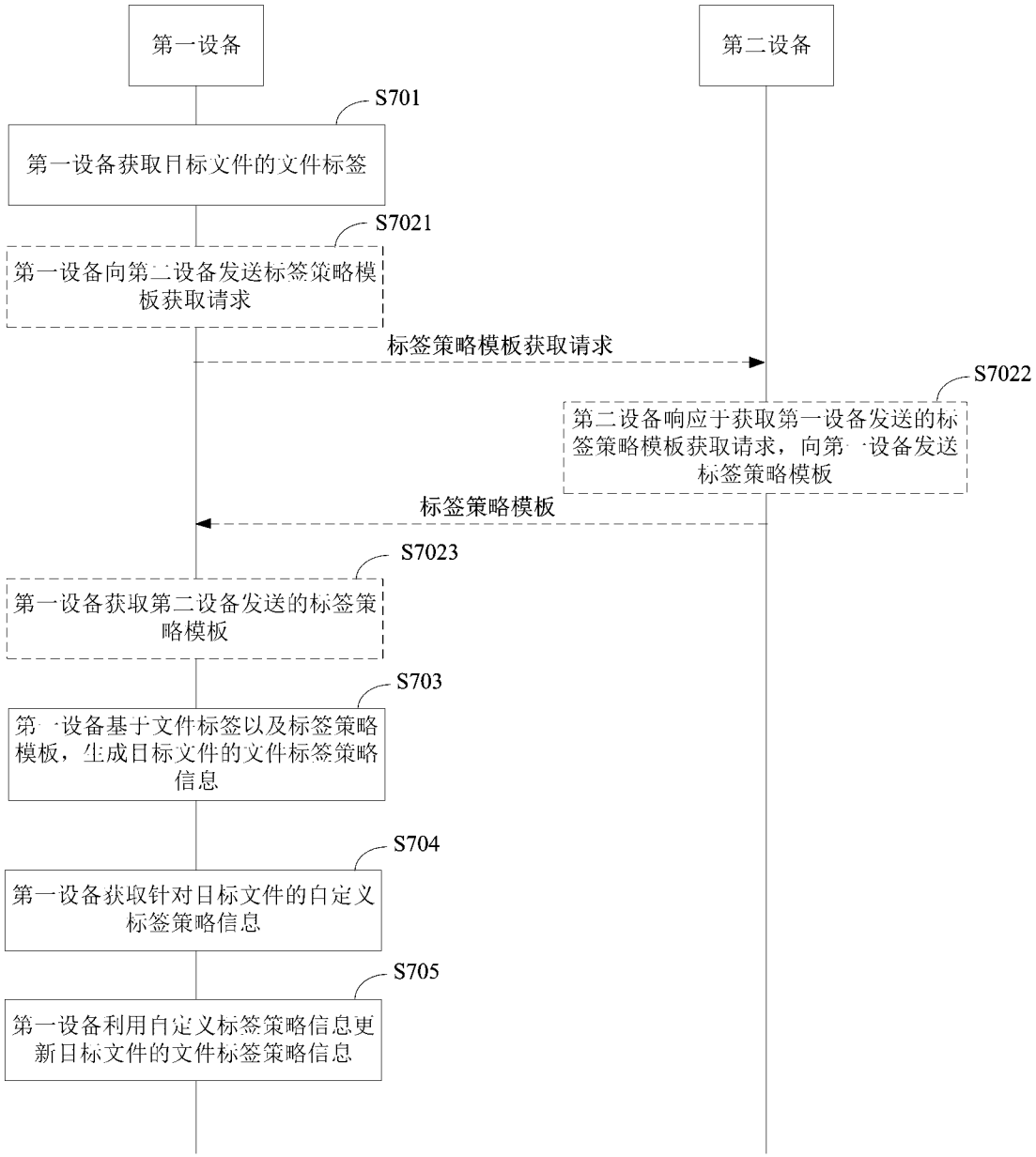
第一设备
第二设备
S701
第一设备获取目标文件的文件标签
S7021
第一设备向第二设备发送标签策略模板获取请求
标签策略模板获取请求
S7022
第二设备响应于获取第一设备发送的标签策略模板获取请求，向第一设备发送标签策略模板
标签策略模板
S7023
第一设备获取第二设备发送的标签策略模板
S703
第一设备基于文件标签以及标签策略模板，生成目标文件的文件标签策略信息
S704
第一设备获取针对目标文件的自定义标签策略信息
S705
第一设备利用自定义标签策略信息更新目标文件的文件标签策略信息

图 9

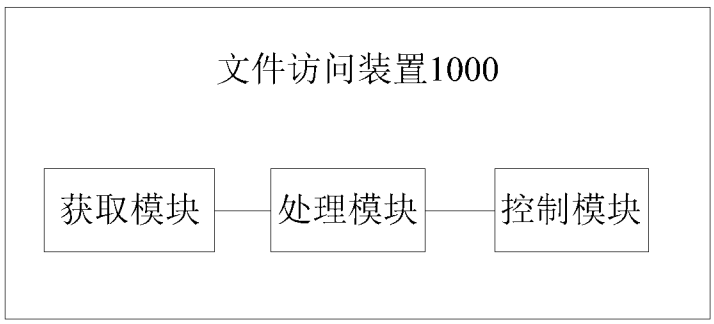
文件访问装置1000
获取模块
处理模块
控制模块

图 10

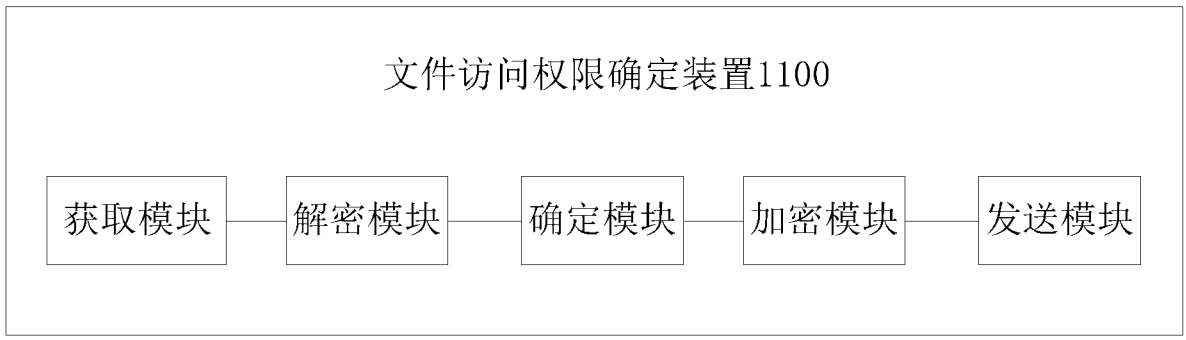
文件访问权限确定装置1100
获取模块
解密模块
确定模块
加密模块
发送模块

图 11

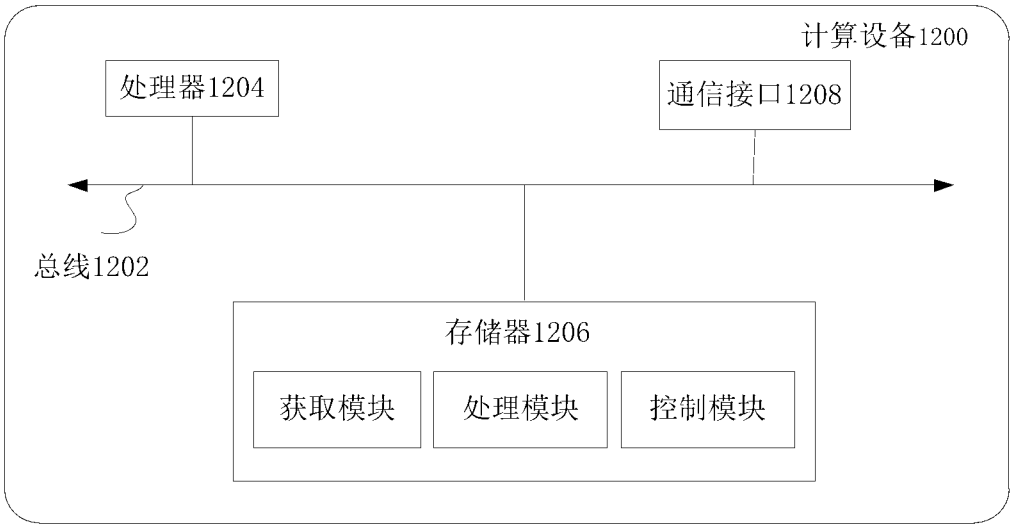
计算设备1200
处理器1204
通信接口1208
总线1202
存储器1206
获取模块
处理模块
控制模块

图 12

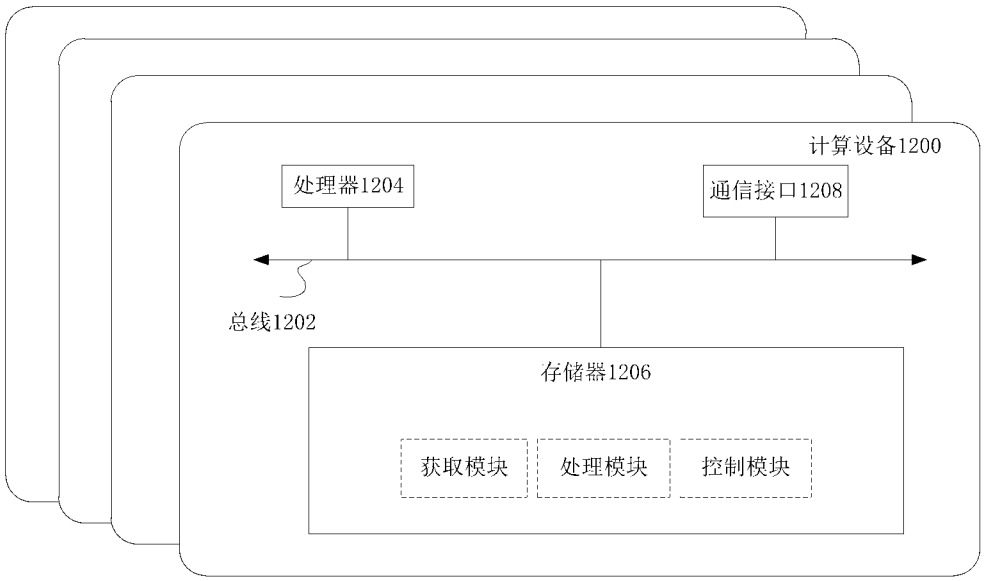
计算设备1200
处理器1204
通信接口1208
总线1202
存储器1206
获取模块
处理模块
控制模块

图 13

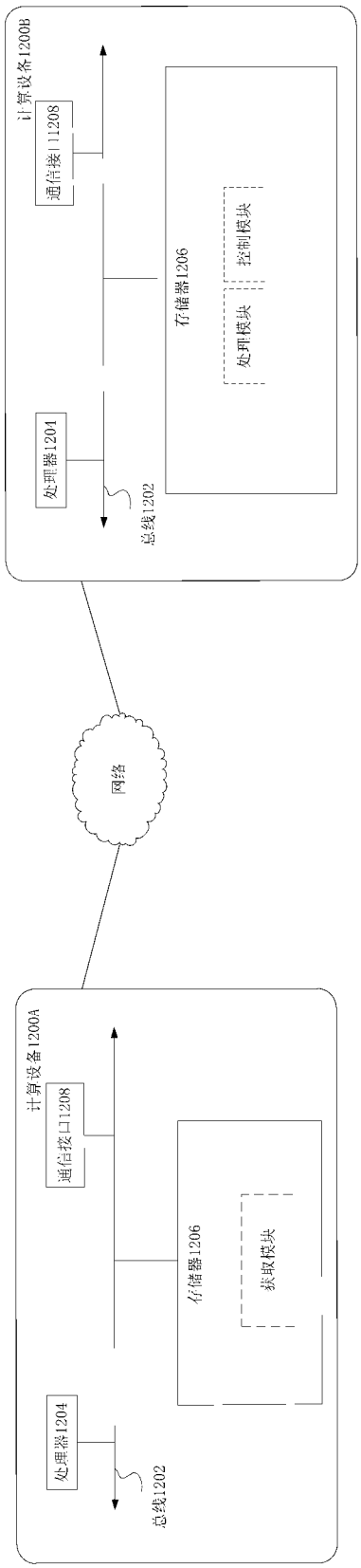
计算设备1200B
通信接口1208
处理器1201
总线1202
存储器1206
处理模块
控制模块
网络
计算设备1200A
通信接口1208
处理器1204
总线1202
存储器1206
获取模块

图 14

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/099581

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/60(2013.01)i; G06F 21/62(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

VEN, CNABS, CNTXT, WOTXT, USTXT, CNKI, IEEE: 文件访问, 权限策略, 标签, 安全, 公钥, 加密, 密文, 解密, file access, permission policy, labeling, security, public key, encryption, ciphertext, decryption

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 105512565 A (INSPUR ELECTRONIC INFORMATION INDUSTRY CO., LTD.) 20 April 2016 (2016-04-20) description, paragraphs [0061]-[0136], and figures 1-5	1-13, 18, 20-22
A	CN 115982778 A (BEIJING RENKE INTERACTIVE NETWORK TECHNOLOGY CO., LTD.) 18 April 2023 (2023-04-18) entire document	1-22
A	CN 111400269 A (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE et al.) 10 July 2020 (2020-07-10) entire document	1-22
A	CN 104318171 A (INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES) 28 January 2015 (2015-01-28) entire document	1-22
A	CN 109614812 A (BEIJING INSTITUTE OF COMPUTER TECHNOLOGY AND APPLICATION) 12 April 2019 (2019-04-12) entire document	1-22

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 August 2024	**21 August 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2024/099581

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 7992188 B2 (RICOH CO., LTD.) 02 August 2011 (2011-08-02) entire document	1-22

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2024/099581

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 105512565 A	20 April 2016	None	
CN 115982778 A	18 April 2023	None	
CN 111400269 A	10 July 2020	None	
CN 104318171 A	28 January 2015	None	
CN 109614812 A	12 April 2019	None	
US 7992188 B2	02 August 2011	EP 1821234 A2	22 August 2007
		EP 1821234 A3	12 November 2008
		JP 2007207171 A	16 August 2007
		JP 4843325 B2	21 December 2011
		US 2007198462 A1	23 August 2007

国际检索报告

国际申请号
PCT/CN2024/099581

A. 主题的分类

G06F 21/60(2013.01)i；G06F 21/62(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

VEN, CNABS, CNTXT, WOTXT, USTXT, CNKI, IEEE：文件访问, 权限策略, 标签, 安全, 公钥, 加密, 密文, 解密, file access, permission policy, labeling, security, public key, encryption, ciphertext, decryption

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 105512565 A (浪潮电子信息产业股份有限公司) 2016年4月20日 (2016 - 04 - 20) 说明书第[0061]-[0136]段、附图1-5	1-13,18,20-22
A	CN 115982778 A (北京仁科互动网络技术有限公司) 2023年4月18日 (2023 - 04 - 18) 全文	1-22
A	CN 111400269 A (中国移动通信有限公司研究院 等) 2020年7月10日 (2020 - 07 - 10) 全文	1-22
A	CN 104318171 A (中国科学院信息工程研究所) 2015年1月28日 (2015 - 01 - 28) 全文	1-22
A	CN 109614812 A (北京计算机技术及应用研究所) 2019年4月12日 (2019 - 04 - 12) 全文	1-22
A	US 7992188 B2 (RICOH COMPANY,LTD.) 2011年8月2日 (2011 - 08 - 02) 全文	1-22

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024年8月8日	2024年8月21日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 吴卿 电话号码 (+86) 010-53961436

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2024/099581

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	105512565	A	2016年4月20日	无			
CN	115982778	A	2023年4月18日	无			
CN	111400269	A	2020年7月10日	无			
CN	104318171	A	2015年1月28日	无			
CN	109614812	A	2019年4月12日	无			
US	7992188	B2	2011年8月2日	EP	1821234	A2	2007年8月22日
				EP	1821234	A3	2008年11月12日
				JP	2007207171	A	2007年8月16日
				JP	4843325	B2	2011年12月21日
				US	2007198462	A1	2007年8月23日