(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 101282330 B
(45)授权公告日 2013.08.28

(21)申请号 200710091131.5
(22)申请日 2007.04.04
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
(72)发明人 黄成 许国军
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 1855832 A,2006.11.01, 说明书第3页第12-21行，第6页7行-第7页9行，第15页18-23行、附图1,7.
CN 1855832 A,2006.11.01, 说明书第3页第12-21行，第6页7行-第7页9行，第15页18-23行、附图1,7.
CN 1617507 A,2005.05.18, 说明书第3页第12-21行，说明书第4页第1-3行.
US 2006/0224735 A1,2006.10.05, 全文.

审查员 袁敏

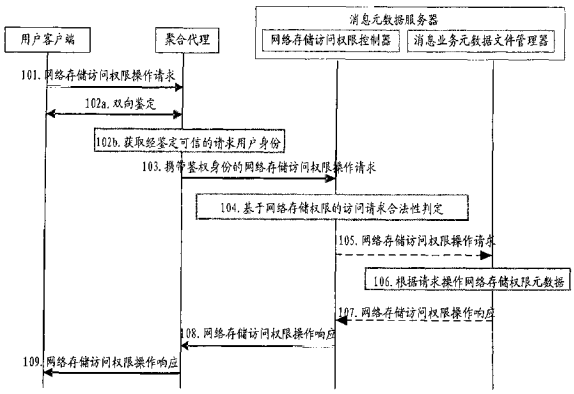
权利要求书9页 说明书23页 附图9页

(54)发明名称

网络存储访问权限管理方法及装置、网络存储访问控制方法

(57)摘要

本发明公开了一种网络存储访问权限管理方法及装置、网络存储访问控制方法，其通过在与所述授权用户对应的授权用户网络存储访问权限元数据中，根据授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限，从而允许被授权用户访问被授权用户的网络存储。



CN 101282330 B

1. 一种网络存储访问权限管理方法，其特征在于，包括：

获得授权用户的网络存储访问权限操作请求，所述请求中携带授权用户请求操作的存储访问权限信息，所述请求中携带授权用户请求操作的存储访问权限信息包括授权用户的身份标识，所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息，以及包括：至少一个被授予访问权限的被授权用户的身份标识，或者，至少一个不能被授予访问权限的访问用户的身份标识；

根据所述授权用户的身份标识，以及网络存储元数据目录或网络存储文件的相关信息，查找对应于授权用户的身份标识的消息业务网络存储访问权限管理元数据文件；

根据授权用户请求操作的存储访问权限信息，在授权用户的网络存储访问权限元数据中，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限；

所述根据授权用户请求操作的存储访问权限，操作存储访问权限的过程，具体包括：

在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求授予的存储访问权限信息，创建授权用户为被授权用户设置的存储访问权限元数据；

或者，

在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求更新的存储访问权限信息，更改授权用户为被授权用户设置的存储访问权限元数据；

或者，

在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求撤回的存储访问权限，删除授权用户为被授权用户设置的存储访问权限元数据。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

按照消息业务的属性，对同一应用下消息业务的元数据，进行分类；为每个类别的元数据建立网络存储目录，并建立所述网络存储目录与存储所述元数据的网络存储文件之间的关联关系。

3. 如权利要求 2 所述的方法，其特征在于，所述网络存储目录中还包括：

为每个类别的元数据的下一级元数据建立的下一级网络存储目录。

4. 如权利要求 1 所述的方法，其特征在于，所述请求操作的存储访问权限信息还包括如下信息中的至少一个：文件和目录的访问权限，权限的继承属性，权限的锁属性，权限过期时间，权限授予时间。

5. 如权利要求 4 所述的方法，其特征在于，所述文件和目录的访问权限包括如下属性信息中的至少一个：完全控制、修改、列出目录内容、读取、写入、文件和目录访问权限的优先级别。

6. 如权利要求 1 所述的方法，其特征在于，所述根据授权用户请求授予的存储访问权限，创建存储访问权限元数据的过程，具体包括：

检索授权用户的“存储授权策略”元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据；

或者，

检索授权用户的“存储授权策略”元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储

访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

7. 如权利要求 1 所述的方法，其特征在于，所述根据授权用户请求更新的存储访问权限，更改存储访问权限元数据的过程，具体包括：

检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与被授权用户身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

或者，

在所述授权用户对应的“用户访问策略”元数据文件中，检索与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，与所述被授权用户身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述被授权用户身份标识对应的存储访问权限元数据；

或者，

在所述授权用户对应的“用户访问策略”元数据文件中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，检索与不能被授予访问权限的访问用户的身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

8. 如权利要求 1 所述的方法，其特征在于，所述根据授权用户请求撤回的存储访问权限，删除存储访问权限元数据的过程，具体包括：

检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述网络存储目

录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述被授权用户身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；

或者，

检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述不能被授予访问权限的访问用户的身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

9. 如权利要求 1 所述的方法，其特征在于，还包括：

在授权用户的网络存储访问权限元数据中，授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的过期时间到达时，删除与所述被授权用户身份标识对应的存储访问权限元数据。

10. 如权利要求 9 所述的方法，其特征在于，所述权限过期时间到达时，删除与所述被授权用户身份标识对应的存储访问权限元数据的过程，具体包括：

在授权用户的“存储授权策略”元数据文件中，当某个被授权用户身份标识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；

或者，

在授权用户的网络存储元数据文件中，当某个被授权用户身份标识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；同时，在授权用户的“用户访问策略”元数据文件中，删除与所述被授权用户该存储访问权限对应的用户访问规则元数据。

11. 如权利要求 9 所述的方法，其特征在于，还包括：

当根据授权用户的网络存储访问权限操作请求，操作所述授权用户的网络存储目录或网络存储文件的存储访问权限后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权限元数据中对应的被授权用户；

或者，

当授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的权限过期时间到达后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权

限元数据中对应的被授权用户。

12. 如权利要求 11 所述的方法，其特征在于，在通知被授权用户变化后的存储访问权限元数据时，将能够采用的访问方式，通知给所述被授权用户。

13. 一种网络存储访问控制方法，其特征在于，包括：

获得被授权用户针对授权用户网络存储的访问请求，所述请求中携带需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识以及请求用户的身份标识；

根据授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，将授权用户网络存储元数据文件中被授权用户具有访问权限的元数据提供给所述被授权用户；

所述根据所述授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，将授权用户网络存储元数据文件中被授权用户具有访问权限的元数据提供给所述被授权用户的过程，具体包括：

检索授权用户的“存储授权策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的存储授权策略元数据，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据提供给所述被授权用户；

或者，

检索授权用户的“用户访问策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的用户访问规则元数据，获得与所述被授权用户身份标识对应的用户访问规则；根据所述用户访问规则，在对应的网络存储元数据文件中，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据提供给所述被授权用户。

14. 如权利要求 13 所述的方法，其特征在于，还包括：

获得被授权用户针对与所述元数据对应的网络存储消息内容的访问请求；

根据授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，对所述被授权用户的访问请求进行合法性验证；为通过验证的被授权用户建立与授权用户网络存储之间的数据传输通道，利用所述数据传输通道，进行所述被授权用户与授权用户网络存储之间的数据传输。

15. 如权利要求 14 所述的方法，其特征在于，还包括：

利用所述数据传输通道，获得被授权用户上传的消息内容；根据所述上传的消息内容，在所述授权用户所拥有的网络存储内容中，添加、更改或删除相应的信息，并根据变化后的信息，更新授权用户网络存储目录或网络存储文件中相应的元数据信息。

16. 如权利要求 15 所述的方法，其特征在于，还包括：

当根据被授权用户上传的消息内容在授权用户对应的网络存储文件中，或对应的网络存储目录所关联的网络存储文件中更新相应的元数据信息后，将变化后的元数据，通知给所述授权用户，和 / 或，具有该网络存储目录和 / 或网络存储文件访问权限的被授权用户。

17. 如权利要求 16 所述的方法，其特征在于，在通知被授权用户变化后的存储访问权限元数据时，将能够采用的访问方式，通知给所述被授权用户。

18. 一种网络存储访问权限管理装置，其特征在于，包括：

“网络存储权限访问控制器”和“消息业务元数据文件管理器”；

所述“网络存储权限访问控制器”，用于获得授权用户的网络存储访问权限操作请求，所述请求中携带授权用户请求操作的存储访问权限信息，所述请求中携带授权用户请求操作的存储访问权限信息包括授权用户的身份标识，所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息，以及包括：至少一个被授予访问权限的被授权用户的身份标识，或者，至少一个不能被授予访问权限的访问用户的身份标识；根据所述“消息业务元数据文件管理器”中的存储访问权限信息，对所述授权用户的网络存储访问权限操作请求，进行合法性验证；

所述“消息业务元数据文件管理器”，用于根据所述“网络存储权限访问控制器”通过验证的网络存储访问权限操作请求，查找对应于授权用户的身份标识的消息业务网络存储访问权限管理元数据文件，在授权用户的网络存储访问权限元数据中，根据所述授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限；

所述“消息业务元数据文件管理器”包括：

权限授予单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求授予的存储访问权限信息，创建授权用户为被授权用户设置的存储访问权限元数据；

或者，

权限更新单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户对应的网络存储访问权限元数据文件中，根据所述授权用户请求更新的存储访问权限信息，更改授权用户为被授权用户设置的存储访问权限元数据；

或者，

第一权限删除单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户对应的网络存储访问权限元数据文件中，根据所述授权用户请求撤回的存储访问权限，删除授权用户为被授权用户设置的存储访问权限元数据。

19. 如权利要求 18 所述的网络存储访问权限管理装置，其特征在于，所述权限授予单元包括：

第一权限授予子单元，用于检索与所述授权用户对应的“存储授权策略”元数据文件，并在其中的与授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据；或者，检索授权用户的“存储授权策略”元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；或者，

第二权限授予子单元，用于检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访

问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据，或者，检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

20. 如权利要求 18 所述的网络存储访问权限管理装置，其特征在于，所述权限更新单元包括：

第一权限更新子单元，用于检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户身份标识对应的存储授权策略元数据文件，并在其中的与被授权用户访问的授权用户网络存储目录或网络存储文件的所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

或者，

第二权限更新子单元，用于在所述授权用户对应的“用户访问策略”元数据文件中，检索与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，与所述被授权用户身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于在所述授权用户对应的“用户访问策略”元数据文件中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，检索与不能被授予访问权限的访问用户的身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

21. 如权利要求 18 所述的网络存储访问权限管理装置，其特征在于，所述第一权限删除单元包括：

第一权限删除子单元，用于检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户对应的存储授权策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予

访问权限的访问用户的身份标识对应的存储访问权限元数据；

或者，

第二权限删除子单元，用于检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述被授权用户身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述不能被授予访问权限的访问用户的身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

22. 如权利要求 18 至 21 任意一项所述的网络存储访问权限管理装置，其特征在于，所述“消息业务元数据文件管理器”还包括：

第二权限删除单元，用于在授权用户对应的网络存储访问权限元数据中，授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的过期时间到达时，删除与所述被授权用户身份标识对应的存储访问权限元数据。

23. 如权利要求 22 所述的网络存储访问权限管理装置，其特征在于，所述第二权限删除单元包括：

第三权限删除子单元，用于在授权用户的“存储授权策略”元数据文件中，当某个被授权用户身份标识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；

或者，

第四权限删除子单元，用于在授权用户的网络存储元数据文件中，当某个被授权用户身份标识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；同时，在授权用户的“用户访问策略”元数据文件中，删除与所述被授权用户该存储访问权限对应的用户访问规则元数据。

24. 如权利要求 22 所述的网络存储访问权限管理装置，其特征在于，还包括：

通知服务器，用于当根据授权用户的网络存储访问权限操作请求，操作所述授权用户的网络存储目录或网络存储文件的存储访问权限后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权限元数据中对应的被授权用户；或者，当授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的权限过期时间到达后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权限元数据中对应的被授权用户。

25. 如权利要求 24 所述的网络存储访问权限管理装置，其特征在于，所述通知服务器还用于：在通知被授权用户变化后的存储访问权限元数据时，将能够采用的访问方式，通知给所述被授权用户。

26. 一种网络存储访问权限管理装置，其特征在于，包括：

“网络存储权限访问控制器”和“消息业务元数据文件管理器”；

所述“网络存储权限访问控制器”，用于获得被授权用户针对授权用户网络存储的访问请求，所述请求中携带需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识以及请求用户的身份标识；根据所述“消息业务元数据文件管理器”中与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，对所述被授权用户的访问请求进行合法性验证；对通过验证的访问请求，向所述“消息业务元数据文件管理器”请求所述被授权用户具有访问权限的元数据，并将所述“消息业务元数据文件管理器”反馈的元数据提供给所述被授权用户；

所述“消息业务元数据文件管理器”，用于将与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，反馈给所述“网络存储权限访问控制器”。

27. 如权利要求 26 所述的网络存储访问权限管理装置，其特征在于，所述“消息业务元数据文件管理器”包括：

第一请求处理单元，用于检索授权用户的“存储授权策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的存储授权策略元数据，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据，反馈给所述“网络存储权限访问控制器”；

或者，

第二请求处理单元，用于检索授权用户的“用户访问策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的用户访问规则元数据，获得与所述被授权用户身份标识对应的用户访问规则；根据所述用户访问规则，在对应的网络存储元数据文件中，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据，反馈给所述“网络存储权限访问控制器”。

28. 如权利要求 26 所述的网络存储访问权限管理装置，其特征在于，所述“网络存储权限访问控制器”，还用于：

获得被授权用户针对所述元数据对应的网络存储消息内容的访问请求；根据所述“消息业务元数据文件管理器”中授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，对所述被授权用户的访问请求进行合法性验证；对通过验证的访问请求，将授权用户网络存储元数据文件中所述被授权用户具有访问权限的元数据，提供给“消息服务器”；获得“消息服务器”根据所述元数据向“消息内容存储器”请求的所述被授权用户具有访问权限的元数据对应的消息内容，并将其提供给被授权用户。

29. 如权利要求 28 所述的网络存储访问权限管理装置，其特征在于，所述“消息业务元数据文件管理器”还包括：

数据更新单元，用于获得“消息服务器”发送的请求，所述请求中携带：根据被授权用户上传的消息内容，在“消息内容存储器”中所述授权用户所拥有的网络存储内容中添加、更改或删除的信息；根据所述变化的信息，更新授权用户网络存储目录或网络存储文件中相应的元数据信息。

30. 如权利要求 28 所述的网络存储访问权限管理装置，其特征在于，还包括：

通知服务器，用于当根据被授权用户上传的消息内容在授权用户对应的网络存储文件中更新相应的元数据信息后，将变化后的元数据，通知给所述授权用户，和 / 或，具有该网络存储目录和 / 或网络存储文件访问权限的被授权用户。

31. 如权利要求 30 所述的网络存储访问权限管理装置，其特征在于，所述通知服务器还用于：在通知被授权用户变化后的存储访问权限元数据时，将能够采用的访问方式，通知给所述被授权用户。

网络存储访问权限管理方法及装置、网络存储访问控制方法

技术领域

[0001] 本发明涉及通信领域，尤其涉及网络存储访问权限管理技术。

背景技术

[0002] OMA(Open Mobile Alliance，开放移动联盟）是制定移动通信系统标准的国际组织，其提出了包括PoC(一键通）、IM(Instant Messaging，即时消息）、以及CPM(Call Protocol Message，融合消息）等基于SIP(Session Initiation Protocol，会话初始协议）的消息业务的规范。该规范通过部署在网络侧的OMA消息系统来实现对消息业务的存储功能。所述OMA消息系统的架构如图1所示，包括：“消息内容存储器”、“消息元数据服务器”、“消息服务器”，以及“聚合代理”、“搜索代理”和“核心网”。所述“消息元数据服务器”包括“网络存储权限访问控制器”和“消息业务元数据文件管理器”。

[0003] 所述“消息内容存储器”用于负责管理存储用户使用消息业务过程中实际收发的消息业务的消息文件，所述消息业务包括：消息、会话历史以及其中可能包含的多媒体数据等历史通信数据。

[0004] 所述“消息元数据服务器”，用于负责用户消息业务的配置信息和描述用户消息业务的元数据信息的存储和管理。所述用户消息业务的配置信息包括：消息业务设置信息，如联系列表、预定义群组、用户访问策略等；所述描述元数据信息包括：描离线消息和会话历史通信数据的元数据等，这些元数据一般通过“消息业务元数据文件”等媒体文件存储。

[0005] 所述“消息元数据服务器”中的“消息业务元数据文件管理器”，用于负责管理其内的“消息业务元数据文件”等媒体文件，所述“消息业务元数据文件”中存储着配置信息和消息业务的元数据信息等。

[0006] 所述“消息元数据服务器”中的“网络存储权限访问控制器”，用于根据所述“消息业务元数据文件管理器”中管理的媒体文件中的数据进行访问权限的控制。

[0007] 所述“消息服务器”用于负责消息业务逻辑控制，即控制所述“消息内容存储器”存储和管理消息业务，控制“消息元数据服务器”存储和管理用户消息业务的配置信息。

[0008] 所述“聚合代理”，是网络中为用户提供访问消息元数据的代理，主要执行对拥有管理消息元数据的权限的授权客户端的鉴权，以及路由网络存储访问请求至适当的网络实体，譬如消息元数据服务器、搜索代理。

[0009] 所述“搜索代理”，用于接收客户端经聚合代理转发来的消息元数据查询请求，并将该请求发送至适当的消息元数据存储实体，譬如“消息元数据服务器”。还用于将接收到查询响应中的搜索结果进行整合，并经聚合代理返回至用户客户端。

[0010] 当客户端访问所记录的消息业务时，首先通过所述“聚合代理”访问“消息元数据服务器”中记录的消息业务的元数据信息；然后根据所述元数据信息，经“核心网”与所述“消息服务器”交互，访问“消息内容存储器”中的消息业务内容。

[0011] 目前，“消息元数据服务器”在记录用户消息业务的元数据信息时，通常按照应

用语义对同一用户的所有元数据信息进行分类，将同一应用语义下的元数据归为一类，然后按照“XML 文件目录”(XML Documents Directory) 元数据文件中的目录结构来组织该用户的消息业务的所有元数据信息。其逻辑结构如图 2 所示，可以看出，其包括：<xcap-directory> 根节点、所述根节点下的子节点 <folder>、所述子节点 <folder> 下的 <entry> 子节点。

[0012] 其中所述 <xcap-directory> 根节点代表某用户的所有消息业务对应的元数据信息的根目录；其下的每个子节点 <folder>，分别对应所述用户在同一应用语义标识 (AUID) 下的某类特定消息业务的所有元数据信息；所述 <entry> 子节点则指向某个具体的消息业务元数据文件，如图中列举的“deferred-list”、“cpm-rules”、“history-list”和“index”四类消息业务元数据文件。

[0013] 当组织好某个用户所拥有的所有元数据信息后，将所述“XML 文件目录”存储到为所述用户预留的存储空间中，以便所述网络存储拥有用户根据网络存储的元数据信息访问相应的网络存储，包括网络存储元数据和 / 或网络存储消息业务。

[0014] 本发明的发明人发现，现有的消息系统是按照应用语义，将某个用户的所有消息业务的元数据信息进行分类的，这样无法分级组织某个应用语义下的元数据；

[0015] 另外，现有的消息系统中，网络存储拥有用户只能根据自己所拥有的“XML 文件目录”中的元数据信息访问自己的网络存储，还不允许其它用户访问自己的网络存储。

发明内容

[0016] 本发明的实施例提供一种网络存储访问权限管理方法及装置、网络存储访问控制方法，其能够允许其它用户访问网络存储拥有用户的网络存储。为描述方便，本发明的实施例中将网络存储拥有用户称为授权用户，将能够访问所述网络存储拥有用户的网络存储的用户称为被授权用户。

[0017] 本发明的实施例通过如下技术方案实现：

[0018] 本发明的实施例提供了一种网络存储访问权限管理方法，其包括：

[0019] 获得授权用户的网络存储访问权限操作请求，所述请求中携带授权用户请求操作的存储访问权限信息，所述请求中携带授权用户请求操作的存储访问权限信息包括授权用户的身份标识，所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息，以及包括：至少一个被授予访问权限的被授权用户的身份标识，或者，至少一个不能被授予访问权限的访问用户的身份标识；

[0020] 根据所述授权用户的身份标识，以及网络存储元数据目录或网络存储文件的相关信息，查找对应于授权用户的身份标识的消息业务网络存储访问权限管理元数据文件；

[0021] 根据授权用户请求操作的存储访问权限信息，在授权用户的网络存储访问权限元数据中，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限；

[0022] 所述根据授权用户请求操作的存储访问权限，操作存储访问权限的过程，具体包括：

[0023] 在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求授予的存储访问权限信息，创建授权用户为被授权用户设置的存储访问权限元数据；

[0024] 或者，

[0025] 在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求更新的存储访问权限信息，更改授权用户为被授权用户设置的存储访问权限元数据；

[0026] 或者，

[0027] 在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求撤回的存储访问权限，删除授权用户为被授权用户设置的存储访问权限元数据。

[0028] 本发明的实施例还提供了一种网络存储访问控制方法，其包括：

[0029] 获得被授权用户针对授权用户网络存储的访问请求，所述请求中携带需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识以及请求用户的身份标识；

[0030] 根据授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，将授权用户网络存储元数据文件中被授权用户具有访问权限的元数据提供给所述被授权用户；

[0031] 所述根据所述授权用户的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，将授权用户网络存储元数据文件中被授权用户具有访问权限的元数据提供给所述被授权用户的过程，具体包括：

[0032] 检索授权用户的“存储授权策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的存储授权策略元数据，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据提供给所述被授权用户；

[0033] 或者，

[0034] 检索授权用户的“用户访问策略”元数据文件中的与被授权用户访问的授权用户网络存储目录或网络存储文件的相关信息对应的用户访问规则元数据，获得与所述被授权用户身份标识对应的用户访问规则；根据所述用户访问规则，在对应的网络存储元数据文件中，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据提供给所述被授权用户。

[0035] 本发明的实施例还提供了一种网络存储访问权限管理装置，其包括：

[0036] “网络存储权限访问控制器”和“消息业务元数据文件管理器”；

[0037] 所述“网络存储权限访问控制器”，用于获得授权用户的网络存储访问权限操作请求，所述请求中携带授权用户请求操作的存储访问权限信息，所述请求中携带授权用户请求操作的存储访问权限信息包括授权用户的身份标识，所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息，以及包括：至少一个被授予访问权限的被授权用户的身份标识，或者，至少一个不能被授予访问权限的访问用户的身份标识；根据所述“消息业务元数据文件管理器”中的存储访问权限信息，对所述授权用户的网络存储访问权限操作请求，进行合法性验证；

[0038] 所述“消息业务元数据文件管理器”，用于根据所述“网络存储权限访问控制器”通过验证的网络存储访问权限操作请求，查找对应于授权用户的身份标识的消息业务网络存储访问权限管理元数据文件，在授权用户的网络存储访问权限元数据中，根据所述授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络

存储文件的存储访问权限；

[0039] 所述“消息业务元数据文件管理器”包括：

[0040] 权限授予单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在授权用户的网络存储访问权限元数据文件中，根据所述授权用户请求授予的存储访问权限信息，创建授权用户为被授权用户设置的存储访问权限元数据；

[0041] 或者，

[0042] 权限更新单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户对应的网络存储访问权限元数据文件中，根据所述授权用户请求更新的存储访问权限信息，更改授权用户为被授权用户设置的存储访问权限元数据；

[0043] 或者，

[0044] 第一权限删除单元，用于根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户对应的网络存储访问权限元数据文件中，根据所述授权用户请求撤回的存储访问权限，删除授权用户为被授权用户设置的存储访问权限元数据。

[0045] 本发明的实施例还提供了另一种网络存储访问权限管理装置，其包括：

[0046] “网络存储权限访问控制器”和“消息业务元数据文件管理器”；

[0047] 所述“网络存储权限访问控制器”，用于获得被授权用户针对授权用户网络存储的访问请求，所述请求中携带需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识以及请求用户的身份标识；根据所述“消息业务元数据文件管理器”中与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，对所述被授权用户的访问请求进行合法性验证；对通过验证的访问请求，向所述“消息业务元数据文件管理器”请求所述被授权用户具有访问权限的元数据，并将所述“消息业务元数据文件管理器”反馈的元数据提供给所述被授权用户；

[0048] 所述“消息业务元数据文件管理器”，用于将与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户对应的存储访问权限信息，反馈给所述“网络存储权限访问控制器”。

[0049] 由上述本发明的实施例提供的具体实施方案可以看出，其通过在与所述授权用户对应的授权用户网络存储访问权限元数据中，根据授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限，从而允许被授权用户访问被授权用户的网络存储。

附图说明

[0050] 图 1 为背景技术提供的 OMA 消息系统的架构图；

[0051] 图 2 为背景技术提供的“XML 文件目录”元数据文件中的目录结构的逻辑结构图；

[0052] 图 3 为本发明第一实施例提供的“XML 文件目录”元数据文件的目录结构的逻辑结构图；

[0053] 图 4 为本发明第一实施例提供的流程图；

[0054] 图 5 为本发明第一实施例提供的“存储授权策略”应用语义的消息业务元数据的目录结构的逻辑结构图；

[0055] 图 6 为本发明第一实施例提供的“用户访问策略”应用语义的用户访问控制信息的目录结构的逻辑结构图；

[0056] 图 7 为本发明第一实施例中，基于“存储授权策略”方案，实现授予、更改和撤回网络存储访问权限的流程图；

[0057] 图 8 为本发明第一实施例中，第一种通知变化的网络存储访问权限方案的流程；

[0058] 图 9 为本发明第一实施例中，第二种通知变化的网络存储访问权限方案的流程；

[0059] 图 10 为本发明第一实施例中，第三种通知变化的网络存储访问权限方案的流程图；

[0060] 图 11 为本发明第一实施例中，第四种通知变化的网络存储访问权限方案的流程图；

[0061] 图 12 为本发明第二实施例中提供的的流程图；

[0062] 图 13 为本发明第二实施例中授权用户对网络存储元数据访问请求的合法性进行鉴定的流程图；

[0063] 图 14 为对拥有“读 / 写”权限的被授权用户的访问，进行控制的流程图；

[0064] 图 15 为本发明第三实施例提供的结构原理图；

[0065] 图 16 为本发明第四实施例提供的结构原理图。

具体实施方式

[0066] 本发明的第一实施例提供了一种网络存储访问权限管理方法，在实施所述第一实施例时，需要按照消息业务的属性，对某一用户的同一应用语义下的消息业务的元数据信息进行分类；为每个类别的元数据建立网络存储目录；并建立所述网络存储目录与存储所述元数据的网络存储元数据文件（即媒体文件）之间的映射关系。

[0067] 所述消息业务的属性，包括同一应用下消息业务的主题″ subject″属性、消息业务执行时间“date”属性等。按照所述消息业务的属性，将同一用户同一应用语义下的所有消息业务的元数据进行分类，将属性相同的消息业务的元数据归到一类中，得到不同类别的元数据；为每个类别的元数据建立网络存储目录，并建立所述网络存储目录与存储所述元数据的网络存储元数据文件之间的映射关系。还可以将每个类别的元数据进一步细分，得到所述类别的下一级元数据，并为其建立下一级网络存储目录。

[0068] 可以按照“XML 文件目录”元数据文件中定义的网络存储目录结构来组织该用户的消息业务的所有元数据信息，其逻辑结构如图 3 所示：可以看出，其包括：<xcap-directory> 根节点、所述根节点下的 <folder> 子节点、所述根节点下的 <folder> 子节点下的 <folder> 子节点、<entry> 子节点。

[0069] 其中所述 <xcap-directory> 根节点代表某用户的所有消息业务对应的元数据信息的根目录；其下的 <folder> 子节点代表同一应用语义下不同消息业务属性对应的元数据的“网络存储目录”；所述根节点下的 <folder> 子节点下的 <folder> 子节点代表按照消息业务的属性，对其上一级的 <folder> 子节点所代表的元数据的“网络存储目录”对应的元数据更细分后，得到的元数据对应的“网络存储目录”；<entry> 节点代表具体存储所述元

数据的“网络存储元数据文件”。

[0070] 其中，每一个<folder>节点携带唯一标识″ id″和“网络存储目录”的属性信息，如主题″ subject″属性信息。每一个<folder>节点下代表具体存储所述元数据的文件的<entry>子节点也携带唯一标识″ id″属性，还可以携带URI属性，用于指向具体的消息业务元数据文件。

[0071] 为描述方便，本实施例中将存储具体元数据的网络存储元数据文件（也称为媒体文件）和存储消息业务内容的消息文件，统称为网络存储文件。

[0072] 为了允许其它被授权用户访问授权用户所拥有的网络存储，每个授权用户可以在“消息元数据服务器”中，为自己的网络存储目录或网络存储元数据文件所对应的元数据的网络存储权限进行管理，从而控制其它被授权用户的访问权限。本发明第一实施例的具体实施过程如图4所示，包括：

[0073] 步骤S101，请求用户发送网络存储访问权限操作请求，所述请求中携带授权用户请求操作的被授权用户的存储访问权限信息；

[0074] 其中，所述授权用户请求操作的被授权用户的存储访问权限信息包括：

[0075] 授权用户的身份标识，至少一个被授予访问权限的被授权用户的身份标识和所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息。其中所述网络存储目录或网络存储文件的相关信息可以是所述网络存储目录或网络存储文件的标识。

[0076] 或者，授权用户的身份标识，所述授权用户请求操作的被授权用户的存储访问权限信息包括至少一个不能被授予访问权限的访问用户的身份标识和所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息。其中所述网络存储目录或网络存储文件的相关信息可以是所述网络存储目录或网络存储文件的标识。

[0077] 所述至少一个被授予访问权限的被授权用户的身份标识，以及所述至少一个不能被授予访问权限的访问用户的身份标识，均可以通过存储的用户列表携带，分别对应白名单用户列表和黑名单用户列表。本实施例中仅以所述授权用户请求操作的被授权用户的存储访问权限信息包括至少一个被授予访问权限的被授权用户的身份标识为例进行说明。

[0078] 另外，所述授权用户请求操作的被授权用户的存储访问权限信息还可以包括如下信息中的至少一个：访问权限类别，权限过期时间，权限授予时间等。

[0079] 所述访问权限类别包括：文件和目录权限，权限的继承属性，权限的锁属性等。

[0080] 所述文件和目录访问权限可以包括Full Control“完全控制”、Modify“修改”、List Folder Content“列出目录内容”、Read“读取”、Write“写入”，以及文件和目录访问权限的优先级别。

[0081] 所述“完全控制”，表示权限只能由授权用户拥有，即只能由授权用户操作（授予、更改、撤回）文件和目录的权限；

[0082] 请求用户访问请求中所需的文件或目录访问权限的优先级别必须低于或等于请求用户所拥有的该文件或目录权限优先级别；请求用户同一文件或目录的高优先级权限将覆盖低优先级权限。

[0083] 所述权限的继承属性，将影响文件和目录权限，如果对目录设置该继承权限后，表示在该目录中创建的新文件和子文件夹默认将继承这些权限。

[0084] 所述权限的锁属性，将影响文件或目录权限是否允许请求用户查看，如果对文件

或目录某个权限的“锁”属性设置为真，表示文件或目录的该权限信息禁止请求用户查看。

[0085] 步骤 S102a ～ b，“聚合代理”和授权用户，根据所述请求中携带的请求用户的身份标识进行双向鉴定。鉴定通过后，获取经鉴定可信任的请求用户的身份标识。

[0086] “聚合代理”将施加本地安全策略，譬如利用 HTTP 数字摘要 (HTTP Digest) 对接收到的初始请求发出质询，并根据授权用户的反馈，或者返回未授权 (Unauthorized) 失败响应，或者鉴定通过后，获取经鉴定可信任的请求用户的身份标识。

[0087] 步骤 S103，“聚合代理”转发网络存储访问权限操作请求，给“消息元数据服务器”，所述请求中携带请求用户请求操作的被授权用户的存储访问权限信息。其中所述授权用户请求操作的被授权用户的存储访问权限信息包括：经过鉴定后的所述请求用户的身份标识，所述存储访问权限中涉及到的网络存储目录或网络存储文件的相关信息，如网络存储目录或网络存储文件的标识 ID；以及，被授权用户的身份标识。

[0088] 步骤 S104，所述网络存储访问权限操作请求到达“消息元数据服务器”后，所述“消息元数据服务器”通过其内的“网络存储访问权限控制器”，根据请求中携带的网络存储目录或网络存储文件的相关信息对应的资源访问路径上的授权用户身份标识，以及请求用户身份标识，判断请求用户是否为授权用户，若不是，则拒绝该请求；若是，则认为其是合法请求用户，接收其网络存储权限操作请求。

[0089] 该步骤中，“网络存储访问权限控制器”判断请求用户是否为授权用户时，比较请求用户身份标识与请求中携带的网络存储目录或网络存储文件的相关信息对应的资源访问路径上的授权用户身份标识是否一致，若一致，则认为请求用户是授权用户，为合法用户；若不一致，则认为请求用户不是授权用户，为非合法用户。

[0090] 步骤 S105，所述“网络存储访问权限控制器”将所述网络存储访问权限操作请求发送到“消息元数据服务器”中的“消息业务元数据文件管理器”。所述请求中携带请求用户请求操作的所述请求用户的存储访问权限信息。其中，所述请求用户请求操作的所述请求用户的存储访问权限信息中包括：请求用户的身份标识，所述访问权限中涉及到的网络存储目录或网络存储文件标识，被授权用户的身份标识。

[0091] 步骤 S106，所述“消息业务元数据文件管理器”接收到所述网络存储访问权限操作请求后，根据所述请求用户的身份标识，以及网络存储元数据目录或网络存储文件的相关信息，查找对应于请求用户身份标识的消息业务网络存储访问权限管理元数据文件；

[0092] 在所述网络存储访问权限管理元数据文件中，根据所述请求用户请求中携带的请求操作的所述请求用户的存储访问权限信息，操作与所述被授权用户标识对应的存储访问权限元数据。具体实现时，可以采用两种方法来实现，如下：

[0093] 第一种方法为基于“存储授权策略”的操作方法：该方法通过新定义的“存储授权策略”(Storage Authorization Policy) 应用语义的消息业务元数据，实现授权用户对其网络存储权限的管理，如权限的授予、更改和撤回。所述消息业务元数据包括一些访问控制信息和存储访问权限信息。其中，所述访问控制信息包括：请求用户的身份标识，以及网络存储访问权限中涉及到的消息业务元数据标识等。所述存储访问权限信息中的信息如步骤 S101 中所列，包括：访问权限类别、权限授予时间、权限过期时间等。

[0094] 新定义的“存储授权策略”(Storage Authorization Policy) 应用语义的消息业务元数据，可以采用如图 5 所示的目录结构存储，称作“存储授权策略”元数据文件。

[0095] 图 5 中，<authorization> 元素代表授权用户网络存储目录或网络存储文件的存储授权策略，并为它赋予一个与该网络存储目录或网络存储文件相关联的授权用户全局唯一的标识“ID”；所述 <authorization> 元素下的 <principal> 子元素，代表所述存储授权策略 <authorization> 中创建的一个与被授权用户对应的存储访问权限元数据，所述存储访问权限元数据 <principal> 元素包括：被授予请求用户 B 的标识“URI”，访问权限类别 <access> 子元素，权限授予时间 <date> 子元素，权限过期时间 <expiry> 子元素等。

[0096] 基于上述定义的“存储授权策略”元数据文件结构，操作所述请求用户标识对应的存储访问权限元数据时，根据所述请求用户请求中携带的请求操作的所述请求用户的存储访问权限信息，在对应于授权用户身份标识的“存储授权策略”元数据文件中创建与所述被授权用户标识对应的存储访问权限信息；或者，根据所述请求用户请求中携带的请求操作的所述请求用户的存储访问权限信息，在对应于授权用户身份标识的“存储授权策略”的元数据文件中更新与所述被授权用户标识对应的存储访问权限信息；或者，根据所述请求用户请求中携带的请求操作的所述请求用户的存储访问权限信息，在对应于授权用户身份标识的“存储授权策略”的元数据文件中删除与所述被授权用户标识对应的存储访问权限信息。

[0097] 第二种方法为基于“用户访问策略”的操作方法，该方法将访问控制信息和存储访问权限信息相分离，利用已被 OMA 标准采纳的用户访问策略 (User Access Policy) 应用语义元数据定义用户网络存储访问控制规则，实现基于授权用户自定义规则的网络存储访问控制；具体的存储访问权限信息则存储在与网络存储访问控制规则相关联的授权用户网络存储目录或网络存储文件元数据文件之中。

[0098] 图 6 为上述用户访问策略元数据文件结构定义逻辑视图，其中采用 <rule> 元素定义用户访问控制信息，或者施用于“XML 文件目录”元数据中一个 <folder> 元素所代表的整个网络存储目录的访问控制信息，或者仅针对一个 <entry> 元素代表的某网络存储目录中存储的消息、会话历史、多媒体数据文件的访问控制信息，本发明实施例根据授权用户请求的具体实现问题，通过比较 <rule> 元素与 <folder>、<entry> 元素在各自唯一标识″ id″ 属性之间关系来判断访问控制信息在 <folder> 元素还是在 <entry> 元素中。进一步，还可以在 <rule> 元素定义 <conditions> 和 <actions> 元素，分别对应 <folder> 元素或 <entry> 元素的访问条件和访问动作。

[0099] 基于“用户访问策略”元数据文件，操作所述请求用户标识对应的存储访问权限元数据时，在对应于授权用户身份标识的“用户访问策略”元数据文件中创建与所述被授权用户标识对应的网络存储访问控制规则，以及根据所述请求中携带的请求操作的存储访问权限信息，在与网络存储访问控制规则相关联的授权用户网络存储目录或网络存储文件元数据文件中创建与所述被授权用户标识对应的存储访问权限信息；或者，根据所述请求中携带的请求操作的存储访问权限信息，在与网络存储访问控制规则相关联的授权用户网络存储目录或网络存储文件元数据文件中更改与所述被授权用户标识对应的存储访问权限信息；或者，在对应于授权用户身份标识的“用户访问策略”元数据文件中删除与所述被授权用户标识对应的网络存储访问控制规则，以及根据所述请求中携带的请求操作的存储访问权限信息，在与网络存储访问控制规则相关联的授权用户网络存储目录或网络存储文件元数据文件中删除与所述被授权用户标识对应的存储访问权限信息。

[0100] 步骤 S107 ～步骤 S109，反馈网络存储权限操作响应。

[0101] 上述网络存储访问权限操作请求可以包括如下几种请求：网络存储访问权限授予请求、网络存储访问权限更改请求和网络存储访问权限撤回请求。

[0102] 下面结合第一实施例中的步骤 S106 中的“存储授权策略”为例，具体描述上述几种不同的网络存储访问权限操作请求的具体实施情况，如图 7 所示：

[0103] 步骤 S201 ～ S204，授权用户 A 经由“聚合代理”向“消息元数据服务器”发送获取网络存储目录结构的请求 (XCAP GET)；所述“消息元数据服务器”根据所述请求，将其存储的用户 A 的网络存储目录及其对应的网络存储元数据文件的元数据反馈给所述授权用户 A；

[0104] 步骤 S205 ～ S206，所述授权用户 A 获取到所述网络存储目录及其对应的网络存储目录元数据文件的元数据后，可以通过终端设备浏览其网络存储目录，并查看某目录下的消息业务元数据，从中选择出想要授权给用户 B 访问的网络存储目录对应的网络存储目录元数据文件的元数据，或网络存储目录元数据文件的元数据，并设置具体的访问权限；然后经由“聚合代理”发送网络存储访问权限授予请求 (XCAP PUT) 给“消息元数据服务器”，所述请求中携带授权用户 A 请求授予用户 B 的网络存储访问权限。其中所述网络存储访问权限包括：授权用户 A 的身份标识，所述访问权限中涉及到的网络存储目录或网络存储文件的标识，被授权用户 B 的身份标识。

[0105] 步骤 S207 ～ S209，“消息元数据服务器”中的“网络存储访问权限控制器”根据请求中授权用户 A 的身份标识向“消息业务元数据文件管理器”发送关于授权用户 A 的网络存储权限操作请求，其中携带请求授予的所述被授权用户 B 的存储访问权限信息，以及访问权限所涉及的网络存储目录或网络存储文件的标识；

[0106] 收到请求后“消息业务元数据文件管理器”将检索授权用户 A 的“存储授权策略”元数据文件（如图 5 所示），分析其中是否存在与所述请求中携带的网络存储目录或文件标识对应的存储授权策略元数据，即图 5 中的 <authorization> 元素。如果不存在，则新创建一个代表请求中网络存储目录或文件存储授权策略的 <authorization> 元素，并为它赋予一个与该网络存储目录或文件相关联的用户 A 全局唯一的标识“ID”；同时，为此新创建的存储授权策略 <authorization> 元数据创建一个与请求中授予用户 B 的网络存储访问权限相对应的存储访问权限元数据，即图中的 <principal> 元素，所述存储访问权限元数据 <principal> 元素包括：被授予用户 B 的标识“URI”，访问权限类别 <access> 子元素，权限授予时间 <date> 子元素，权限过期时间 <expiry> 子元素等。

[0107] 如果授权用户 A 的“存储授权策略”元数据文件中，已经存在与所述请求中携带的网络存储目录或网络存储元数据文件标识对应的存储授权策略 <authorization> 元数据，则“消息业务元数据文件管理器”直接为此存储授权策略元数据创建一个与请求中授予用户 B 的网络存储访问权限相对应的存储访问权限 <principal> 元数据。

[0108] “消息业务元数据文件管理器”只有全部完成上述步骤后，才会向“网络存储访问权限控制器”返回操作成功响应，否则返回失败响应。

[0109] “消息元数据服务器”经由聚合代理向用户 A 客户端返回响应。

[0110] 步骤 S210，当“消息元数据服务器”创建新的存储权限策略完毕后，请求用户 B 将收到网络存储访问权限通知，其中包含授权用户 A 所授权的网络存储目录标识及其权限信

息。下面给出网络存储访问权限发生变化后用户 B 接收通知的几种可选流程：

[0111] 第一种方式：“消息服务器”通过主动订阅“消息元数据服务器”中的网络存储访问权限通知，获得发生变化的网络存储访问权限元数据，并将其通知给所述网络存储访问权限元数据中对应的被授权用户，具体实现如图 8 所示，包括：

[0112] 步骤 S1 ～ 4，消息服务器发送 SIP SUBSCRIBE(SIP 订阅）请求订阅“消息元数据服务器”中存储的授权用户 A 对应的存储访问权限元数据的状态变化通知；

[0113] 步骤 S5 ～ 6，一旦授权用户 A 执行网络存储权限操作或者由于某网络存储权限因过期而被系统自动删除，导致“消息元数据服务器”中授权用户 A 对应的存储访问权限元数据中的用户 B 的授权信息状态发生改变，“消息元数据服务器”向“消息服务器”发送 SIP NOTIFY(SIP 通知）；所述通知中携带请求用户 B 改变后的网络存储权限；

[0114] 步骤 S7 ～ 8，“消息服务器”向用户 B 发送 SIP MESSAGE(SIP 消息），通知其所被授予的网络存储权限发生改变。

[0115] 第二种方式：“消息元数据服务器”发现网络存储访问权限发生变化后，将变化后的网络存储访问权限元数据通知给所述网络存储访问权限元数据中对应的被授权用户，具体实现如图 9 所示，包括：

[0116] 步骤 1，一旦授权用户 A 执行网络存储权限操作或者由于某网络存储权限因过期而被系统自动删除，导致“消息元数据服务器”中授权用户 A 对应的存储访问权限元数据中的用户 B 的授权信息状态发生改变，则“消息元数据服务器”向用户 B 发送 SIP MESSAGE 通知，所述通知中携带用户 B 变化后的网络存储权限；

[0117] 步骤 2，请求用户 B 向消息元数据服务器返回响应。

[0118] 第三种方式：授权用户在操作其网络存储访问权限后，经由“消息服务器”将变化后的网络存储访问权限，通知给所述网络存储访问权限元数据中对应的被授权用户。具体实现如图 10 所示，包括：

[0119] 步骤 1 ～ 2，一旦授权用户 A 执行网络存储权限操作，导致“消息元数据服务器”中的授权用户 A 对应的存储访问权限元数据中的针对用户 B 的授权信息状态发生改变，则授权用户 A 向“消息服务器”发送 SIP MESSAGE 通知消息，所述通知消息中携带用户 B 变化后的网络存储权限。

[0120] 步骤 3 ～ 4，“消息服务器”向用户 B 转发 SIP MESSAGE 通知。

[0121] 第四种方式：请求用户向“消息元数据服务器”订阅网络存储访问权限通知；网络存储访问权限发生变化后，“消息元数据服务器”将变化后的网络存储访问权限通知给所述网络存储访问权限元数据中对应的被授权用户。具体实现如图 11 所示，包括：

[0122] 步骤 1 ～ 4，请求用户 B 发送 SIP SUBSCRIBE 请求订阅“消息元数据服务器”中存储的授权用户 A 对应的存储访问权限元数据的状态变化通知；

[0123] 步骤 5 ～ 6，一旦由于授权用户 A 执行网络存储访问权限操作或者由于某网络存储权限因过期而被系统自动删除，导致“消息元数据服务器”中存储的授权用户 A 对应的存储访问权限元数据中涉及用户 B 的授权信息状态发生改变，则消息元数据服务器向用户 B 发送 SIP NOTIFY 通知消息，所述通知消息中携带用户 B 变化后的网络存储权限。

[0124] 上述是授予请求用户网络存储访问权限的流程。对于更新网络存储访问权限的流程，具体如下：

[0125] 步骤S211～S212，所述授权用户A还可以请求更新授予用户B的网络存储访问权限，为此，用户A浏览已经授予用户B的网络存储目录或网络存储文件的权限并重新设置新的访问权限；然后经由“聚合代理”发送网络存储访问权限更新请求（XCAP PUT）给“消息元数据服务器”，所述请求中携带用户A的身份标识；请求更新用户B的网络存储访问权限，以及，所述访问权限中涉及到的网络存储目录或网络存储文件的标识。

[0126] “消息元数据服务器”中的“网络存储访问权限控制器”根据请求中授权用户A的身份标识，向“消息业务元数据文件管理器”发送关于授权用户A的网络存储权限操作请求，其中携带请求更新操作的所述用户B的存储访问权限信息。其中所述存储访问权限信息包括：授权用户A的身份标识，访问权限所涉及的网络存储目录或网络存储文件的相关信息，以及用户B的身份标识。

[0127] 收到请求后“消息业务元数据文件管理器”将检索授权用户A的“存储授权策略”元数据文件中与所述请求中网络存储目录或网络存储元数据文件的相关信息对应的授权策略元数据<authorization>元素，并根据请求中携带的请求更新操作的所述请求用户B的存储访问权限信息，更改所述授权策略元数据<authorization>元素中代表所述被授权用户标识对应的存储访问权限元数据的<principal>元素。

[0128] 当“消息元数据服务器”更改存储权限策略元数据完毕后，用户B将收到网络存储访问权限变化通知，其中包含授权用户A所更改的网络存储目录或网络存储文件标识及其对应的网络存储权限信息。网络存储访问权限发生变化后，用户B接收通知的方式可以采取上述几种可选流程实现，这里不再详细描述。

[0129] 授权用户A想要撤回已经授权给请求用户B的网络存储访问权限时，其通过如下流程实现：

[0130] 步骤S213～S216，所述授权用户A还可以请求撤回授予用户B的网络存储访问权限，为此，用户A浏览已经授予用户B的网络存储目录或网络存储文件的权限并有选择地撤回访问权限；然后经由“聚合代理”发送网络存储访问权限撤回请求（XCAP DELETE）给“消息元数据服务器”，所述请求中携带请求撤回用户B的网络存储访问权限。其中所述网络存储访问权限包括用户A的身份标识，所述访问权限中涉及到的网络存储目录或网络存储文件的标识，以及用户B的身份标识。

[0131] “消息元数据服务器”中的“网络存储访问权限控制器”根据请求中授权用户A的身份标识向“消息业务元数据文件管理器”发送关于授权用户A的网络存储权限操作请求，其中携带请求撤回操作的所述用户B的存储访问权限信息。其中所述存储访问权限信息包括：用户A的身份标识，访问权限所涉及的网络存储目录或网络存储文件的相关信息，以及用户B的身份标识。

[0132] 收到请求后“消息业务元数据文件管理器”将检索授权用户A的“存储授权策略”元数据文件中与所述请求中网络存储目录或网络存储元数据文件的相关信息对应的授权策略元数据<authorization>元素，并根据请求中携带的请求撤回操作的所述用户B的存储访问权限信息，删除所述授权策略元数据<authorization>元素中代表所述被授权用户标识对应的存储访问权限元数据的<principal>元素。

[0133] 当“消息元数据服务器”删除存储权限策略完毕后，请求用户B将收到网络存储访问权限变化通知，其中包含授权用户A所撤回的网络存储目录标识及其权限信息。网络存

储访问权限发生变化后用户 B 接收通知的方式可以采取上述几种可选流程实现，这里不再详细描述。

[0134] 上述是结合第一实施例中的步骤 S106 中的“存储授权策略”来描述上述几种不同的网络存储访问权限操作请求的具体实施情况的，如果结合第一实施例中的步骤 S106 中的“用户访问策略”，则网络存储访问权限操作的情况如下：

[0135] 一、对于网络存储访问权限授予操作

[0136] “消息元数据服务器”中的“网络存储访问权限控制器”根据请求中携带授权用户 A 的身份标识，向“消息业务元数据文件管理器”发送有关授权用户 A 的网络存储权限授予请求，其中携带请求授予的所述请求用户 B 的存储访问权限信息。其中所述存储访问权限信息包括：授权用户 A 的身份标识，访问权限所涉及的网络存储目录或网络存储文件的相关信息，以及被授权用户 B 的身份标识；

[0137] “消息业务元数据文件管理器”收到请求后，首先，检索授权用户 A 的“用户访问策略”元数据文件（如图 6 所示），分析其中是否存在与所述请求中携带的网络存储目录或网络存储元数据文件标识相对应的访问规则元数据，即图 6 中的 <rule> 元素。如果不存在，则新创建一个代表请求中网络存储目录或网络存储元数据文件访问规则元数据的 <rule> 元素，并为它赋予一个与该网络存储目录或网络存储元数据文件相关联的授权用户 A 全局唯一的标识“ID”；同时作如下操作：将用户 B 的标识“URI”加入到 <rule> 元素中的代表访问控制条件的 <condition> 子元素中，并设置 <rule> 元素中代表访问控制动作 <action> 子元素中的 <allow-invite> 元素值为“accept”，以表示允许用户 B 访问该访问控制规则对应的用户 A 的网络存储目录或网络存储文件。

[0138] 如果授权用户 A 的“用户访问策略”元数据文件中，已经存在代表与所述请求中携带的网络存储目录或网络存储元数据文件标识对应的访问规则元数据的 <rule> 元素，则“消息业务元数据文件管理器”直接对此访问规则元数据施加同样的操作。

[0139] 其次，“消息业务元数据文件管理器”还将根据所述请求中携带的网络存储目录或网络存储元数据文件标识，定位与上述访问规则对应的授权用户 A 的网络存储元数据文件，譬如“会话历史”元数据文件。“消息业务元数据文件管理器”将在所述授权请求涉及到的网络存储元数据文件中，创建与请求中携带的授予用户 B 的网络存储访问权限相对应的存储访问权限元数据，其中包括：请求用户 B 的标识“URI”，代表访问权限类别的 <access> 子元素，代表权限授予时间的 <date> 子元素，代表权限过期时间的 <expiry> 子元素等。

[0140] “消息业务元数据文件管理器”只有全部完成上述步骤后，才会向“网络存储访问权限控制器”返回操作成功响应，否则返回失败响应。

[0141] 二、对于网络存储访问权限更新操作

[0142] “消息元数据服务器”中的“网络存储访问权限控制器”根据请求中携带授权用户 A 的身份标识，向“消息业务元数据文件管理器”发送有关授权用户 A 的网络存储权限更新请求，其中携带请求更新的所述请求用户 B 的存储访问权限信息。所述存储访问权限信息包括授权用户 A 的身份标识，访问权限所涉及的网络存储目录或网络存储文件的相关信息，以及被授权用户 B 的身份标识；

[0143] “消息业务元数据文件管理器”收到请求后，检索授权用户 A 的“用户访问策略”元数据文件中与所述请求中携带的网络存储目录或网络存储元数据文件标识相对应的访问

规则元数据，即图 6 中的 <rule> 元素，并根据所述请求中携带的网络存储目录或网络存储元数据文件标识，定位与上述访问规则对应的授权用户 A 的网络存储元数据文件，譬如“会话历史”元数据文件。“消息业务元数据文件管理器”将在所述更新请求涉及到的网络存储元数据文件中，根据请求更新的所述用户 B 的存储访问权限信息，更改与用户 B 身份标识对应的存储访问权限元数据。

[0144] 三、对于网络存储访问权限撤回操作

[0145] “消息元数据服务器”中的“网络存储访问权限控制器”根据请求中携带授权用户 A 的身份标识，向“消息业务元数据文件管理器”发送有关授权用户 A 的网络存储权限撤回请求，其中携带：请求撤回的所述用户 B 的存储访问权限信息。其中，所述存储访问权限信息包括授权用户 A 的身份标识，访问权限所涉及的网络存储目录或网络存储文件的相关信息，以及被授权用户 B 的身份标识；

[0146] “消息业务元数据文件管理器”，根据所述授权用户 A 的身份标识，检索所述授权用户 A 身份标识对应的“用户访问策略”元数据文件中与所述网络存储目录或网络存储文件的相关信息对应的访问规则元数据，即图 6 中的 <rule> 元素，并在所述 <rule> 元素下的 <condition> 子元素中，删除用户 B 的身份标识；同时，根据所述请求中携带的网络存储目录或网络存储元数据文件标识，定位与上述访问规则对应的授权用户 A 的网络存储元数据文件，譬如“会话历史”元数据文件。“消息业务元数据文件管理器”将在所述撤回请求涉及到的网络存储元数据文件中，根据请求撤回的所述用户 B 的存储访问权限信息，删除与用户 B 身份标识对应的存储访问权限元数据。

[0147] 经过上述具体实施方案，授权用户能够对其所拥有的网络存储，进行网络存储权限管理，从而可以利用其管理的网络存储访问权限，控制请求用户访问自己的网络存储。为此，本发明第二实施例提供了一种网络存储访问控制方法，其具体实施过程如图 12 所示，包括：

[0148] 步骤 S301，请求用户发送网络存储元数据访问请求；所述请求中携带所述请求用户需要访问的网络存储信息。其中所述请求用户需要访问的网络存储信息包括：需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识请求用户的身份标识；

[0149] 步骤 S302a ～ b，所述请求用户和“聚合代理”之间进行双向鉴定；鉴定通过后，聚合代理获取经鉴定可信的请求用户的身份标识。

[0150] 如果请求用户与被访问授权用户的网络存储分属不同网络域中，则所述“聚合代理”还可以支持请求用户跨域访问，即请求用户所在网络域中“聚合代理”将经过身份鉴别的请求路由到授权用户所在网络域中的“聚合代理”；

[0151] 步骤 S303，“聚合代理”向“消息元数据服务器”发送网络存储元数据访问请求，所述请求中携带：所述请求用户需要访问的网络存储信息。其中所述请求用户需要访问的网络存储信息包括：请求用户的身份标识，需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识。

[0152] 步骤 S304，所述“消息元数据服务器”中的“网络存储访问权限控制器”接收到所述网络存储元数据访问请求后，根据所述请求中携带的授权用户的身份标识、所述网络存储目录或网络存储元数据文件的相关信息，以及请求用户的身份标识，获得授权用户授予所

述请求用户的存储访问权限元数据；根据所获得的存储访问权限元数据，对请求用户发送的网络存储元数据访问请求进行合法性鉴定，如果鉴定为合法请求，则继续执行步骤 S305；如果鉴定为不合法请求，则拒绝所述网络存储元数据访问请求。

[0153] 具体对所述网络存储元数据访问请求进行合法性鉴定的流程如图 13 所示，包括：

[0154] 步骤 S3041，“消息元数据服务器”根据所述网络存储元数据访问请求中携带的请求用户的身份标识，以及请求中携带的网络存储目录或网络存储元数据文件的相关信息对应的授权用户身份标识，判断所述请求用户是否为授权用户，若是，则执行步骤 S3042，认为请求用户发送的网络存储元数据访问请求合法，转向步骤 S305；若所述请求用户不为授权用户，则执行步骤 S3043。

[0155] 步骤 S3041 和步骤 S3042 中，“消息元数据服务器”中的“网络存储访问权限控制器”可以根据请求中携带的网络存储目录或网络存储元数据文件的相关信息，找到对应的授权用户身份标识，然后将所述网络存储元数据访问请求中携带的请求用户的身份标识，与所找到的授权用户身份标识进行比较，如果一致，则认为所述请求用户为“授权用户”，否则，认为所述请求用户不为授权用户。

[0156] 步骤 S3043，所述“网络存储访问权限控制器”请求“消息业务元数据文件管理器”查询所述请求用户被授予的访问权限，所述请求中携带被访问授权用户的身份标识、所述网络存储目录或网络存储元数据文件的相关信息、请求用户的身份标识等。

[0157] “消息业务元数据文件管理器”根据所述请求中携带的信息，查找所述请求用户身份标识对应的存储访问权限元数据。具体可以采用两种方法实现：

[0158] 第一种方法是基于“存储授权策略”的实现方法

[0159] 检索与所述被访问授权用户的身份标识对应的“存储授权策略”元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，检索是否存在与请求用户身份标识对应的存储访问权限；

[0160] 第二种方法是基于“用户访问策略”的实现方法

[0161] 检索与所述被访问授权用户的身份标识对应的“用户访问策略”元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，检索是否存在与请求用户身份标识对应的用户访问规则；如果存在，则在与所述用户访问规则对应的网络存储元数据文件中检索与请求用户身份标识对应的存储访问权限。

[0162] 步骤 S3044，“网络存储访问权限控制器”根据所述“消息业务元数据文件管理器”的反馈结果，判断是否存在授予所述请求用户的访问权限，若存在，则执行步骤 S3045；否则，执行步骤 S3046。

[0163] 步骤 S3045，“网络存储访问权限控制器”根据所述授予所述请求用户的访问权限，判断所述网络存储访问请求中携带的网络存储目录或网络存储元数据文件的相关信息是否符合授权，即请求用户访问请求中所需的文件或目录的访问权限的优先级别必须低于或等于请求用户所拥有的该文件或目录权限优先级别。若符合，则执行步骤 S3042；否则，执行步骤 S3046。

[0164] 步骤 S3046，“网络存储访问权限控制器”拒绝所述网络存储元数据访问请求。

[0165] 步骤 S305，将判定为合法的网络存储元数据访问请求，发送给“消息业务元数据文件管理器”，所述请求中携带所述请求用户需要访问的网络存储信息。其中所述请求用户需

要访问的网络存储信息包括：请求用户的身份标识，需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识。

[0166] 步骤 S306 ～ 309，所述“消息业务元数据文件管理器”根据所述网络存储元数据访问请求中携带的网络存储目录或网络存储元数据文件的相关信息，获取网络存储元数据；对所述网络存储元数据访问请求进行响应，并在响应中携带所获取到的网络存储元数据。

[0167] 步骤 S310，所述请求用户根据所述响应，获得所述网络存储元数据；发送网络存储内容访问请求给“消息服务器”，其中携带所述网络存储元数据，以及所述请求用户的身份标识。

[0168] 步骤 S311，所述消息服务器请求消息元数据服务器对所述网络存储内容访问请求进行合法性鉴定，如果鉴定为合法请求，则继续执行步骤 S312；如果鉴定为不合法请求，则拒绝所述网络存储内容访问请求。

[0169] 具体的鉴定流程，与步骤 S304 中的实现流程类似，这里不再详细描述。

[0170] 步骤 S312，所述“消息服务器”发送网络存储访问请求给“消息内容存储器”；所述请求中携带所请求的消息业务网络存储对应的元数据；

[0171] 步骤 S313 ～ 314，所述“消息内容存储器”根据所述元数据，检索到相应的消息业务网络存储，并经过“消息服务器”反馈网络存储检索响应给所述用户客户端；

[0172] 步骤 S315，建立请求用户客户端与“消息内容存储器”之间的数据传输通道，通过所述数据传输通道，所述“消息内容存储器”将所检索到的消息业务网络存储内容发送给所述请求用户；

[0173] 或者，请求用户客户端将消息业务本地存储内容上传至“消息内容存储器”。

[0174] 下面，假设在授权用户 A 授予请求用户 B 拥有会话历史网络存储目录的“读 / 写”权限的情况下，以基于“存储授权策略”的操作方法为例，对上述网络存储访问流程进行详细说明，实现流程如图 14 所示，包括：

[0175] 步骤 S401 ～ 403，请求用户 B 希望访问授权用户 A 的网络存储，为此请求用户 B 首先要获取授权用户 A 授予请求用户 B 的网络存储权限，于是请求用户 B 经由聚合代理、搜索代理向“消息元数据服务器”发送存储权限查询 (HTTP POST) 请求消息，其中携带如下信息：所述请求用户需要访问的网络存储信息。其中所述请求用户需要访问的网络存储信息包括：请求用户的身份标识，需要访问的网络存储对应的网络存储目录或网络存储元数据文件的相关信息，需要访问的网络存储所对应的授权用户的身份标识。

[0176] 步骤 S404，“消息元数据服务器”检索请求用户“存储授权策略”元数据，并进行访问控制。具体如下：

[0177] “消息元数据服务器”中的“消息业务元数据文件管理器”，在“网络存储访问权限控制器”的控制下按照 HTTP POST 请求中携带的被访问授权用户的身份标识、所述网络存储目录或网络存储元数据文件的相关信息，检索授权用户 A 的身份标识对应的存储授权策略元数据文件中，是否存在所述网络存储目录或网络存储文件的相关信息对应的存储授权策略元数据；若存在，则根据所述请求用户的身份标识，在所述存储授权策略元数据中，查找所述请求用户 B 身份标识对应的存储访问权限元数据；如果所述存储访问权限元数据中存在相应的授权信息，则“网络存储访问权限控制器”接收该请求，然后执行步骤 S405；否则，

“网络存储访问权限控制器”拒绝该请求。

[0178] 步骤 S405 ～ 407,“网络存储访问权限控制器”通过网络存储权限查询响应,将“消息业务元数据文件管理器”返回的搜索结果,经由搜索代理、聚合代理,向请求用户 B 返回,其中携带授权用户 A 授予请求用户 B 的网络存储访问权限信息。

[0179] 步骤 S408 ～ 410,请求用户 B 在终端查看授权用户 A 授予其的网络存储目录或网络存储元数据文件的权限信息,发现自己拥有授权用户 A 的某会话历史网络存储目录的“读 / 写”权限,为了查看此目录中的会话历史内容,请求用户 B 发送网络存储元数据获取 (XCAP GET) 请求,并经由“聚合代理”到达“消息元数据服务器”。所述 XCAP GET 请求中携带如下信息 :所述请求用户需要访问的网络存储信息。其中所述请求用户需要访问的网络存储信息包括 :请求用户的身份标识,所述请求用户需要访问的某会话历史消息业务对应的网络存储目录或网络存储元数据文件的相关信息,需要访问的网络存储所对应的授权用户的身份标识。

[0180] 步骤 S411,“消息元数据服务器”收到 XCAP GET 请求后,检索所述请求用户 B “存储授权策略”元数据和“会话历史”元数据,并进行相应的控制。

[0181] 具体实现如下 :

[0182] 首先检索授权用户 A “存储授权策略”元数据文件中有关授权用户 A 授予请求用户 B 的网络存储访问权限信息,具体实现与步骤 S404 中的相关描述类似,这里不再详细描述。

[0183] 在判断请求用户 B 拥有网络存储拥有授权用户 A 的网络存储访问权限后,“网络存储访问权限控制器”将会结合“消息业务元数据文件管理器”检索到有关用户 B 的授权信息。

[0184] 按照如图 13 所示的对所述网络存储元数据访问请求进行合法性鉴定的流程,判断请求用户 B 的此次访问请求是否符合授权用户 A 对其所作的授权,“网络存储访问权限控制器”只会接收经过合法的网络存储访问请求。

[0185] 步骤 S412 ～ 413,“消息元数据服务器”通过网络存储元数据获取响应,返回授权用户 A 所授予的会话历史元数据信息,并经由聚合代理到达请求用户 B ;

[0186] 步骤 S414,请求用户 B 浏览授权用户 A 网络存储中授权的会话历史元数据信息,为了获取会话历史实际内容,请求用户 B 客户端向“消息服务器”发送网络存储内容获取请求,譬如 SIP INVITE,其中 :“Request-URI”指出消息网络存储 URl,如“history@hostname”,此外 MIME SDP 消息体中将 direction 属性设置为“a = recvonly”,并包含会话历史元数据信息,譬如网络存储目录中的消息标识 (msg-id) 构成的 URI List。

[0187] 步骤 S415 ～ 419,收到 SIP INVITE 请求后,“消息服务器”和“消息元数据服务器”协调执行用户访问策略控制,为合法的请求用户建立起“消息内容存储器”与请求用户 B 之间的会话历史内容传输通道,并通过所述传输通道,将“消息内容存储器”中的会话历史内容传输给所述请求用户 B。具体如下 :

[0188] “消息服务器”请求“消息元数据服务器”中的“网络存储访问权限控制器”执行与步骤 S404 类似的访问权限控制。如果接受请求用户 B 的请求,则“消息服务器”向请求用户 B 返回 SIP 200 OK 响应,并在收到请求用户 B 再次发送的 SIP ACK 应答后,建立起“消息内容存储器”与请求用户 B 之间的会话历史内容传输通道,譬如 MSRP 通道。至此,请求用户 B

通过所述传输通道，可以接收授权用户 A 网络存储中其所请求的并具有访问权限的会话历史信息。

[0189] 步骤 S420 ～ 425，请求用户 B 还拥有授权用户 A 授予的该会话历史网络存储目录的“写”权限，因此除了可以获取目录中授权用户 A 的会话历史外，还可以将本地数据上传至该目录，为此请求用户 B 向“消息服务器”发送网络存储内容上传请求，譬如 SIP INVITE，其中：“Request-URI”指出消息网络存储实体所在的 URI，如“history@hostname”，此外 MIME SDP 消息体将 direction 属性设置为“a = sendonly”，并包含上传数据所要存放的用户 A 网络存储，譬如网络存储目录标识“id”或会话历史文件名称“file-name”。

[0190] “消息服务器”将请求“消息元数据服务器”执行与步骤 S404 类似的访问策略控制，一旦接受请求用户 B 的请求，将建立起“消息内容存储器”与请求用户 B 之间的数据传输通道。至此，请求用户 B 可以通过建立的数据传输通道，譬如 MSRP 通道，将本地数据上传至其所具有写权限的授权用户 A 的网络存储之中。

[0191] 数据传输成功后，“消息服务器”还将请求“消息元数据服务器”更新授权用户 A 的消息业务元数据信息，以反映授权用户 A 网络存储中新增加的数据。

[0192] 与图 8 至图 11 中介绍的通知流程类似，当请求用户 B 成功完成向授权用户 A 的“消息内容存储器”中“写”数据后，授权用户 A 将收到网络存储变化通知。

[0193] 上述是以请求中携带的存储访问权限信息中包括至少一个被授予访问权限的授权用户的身份标识为例，进行说明的，当请求中携带的存储访问权限信息中包括至少一个不能被授予访问权限的授权用户的身份标识时，对不同的操作请求对应的操作如下：

[0194] 一、对于网络存储访问权限授予操作

[0195] 检索授权用户的“存储授权策略”元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0196] 或者，

[0197] 检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0198] 二、对于网络存储访问权限更新操作

[0199] 检索与所述授权用户身份标识对应的存储授权策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0200] 或者，

[0201] 在所述授权用户的身份标识对应的“用户访问策略”元数据文件中的与所述授权用户请求操作的存储访问权限信息涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，检索与不能被授予访问权限的访问用户的身份标识对应的用户访

问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0202] 三、对于网络存储访问权限删除操作

[0203] 检索与所述授权用户的身份标识对应的存储授权策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0204] 或者，

[0205] 检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述不能被授予访问权限的访问用户的身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0206] 本发明的第三实施例提供一种网络存储访问权限管理装置，其结构如图 15 所示，包括“网络存储权限访问控制器”和“消息业务元数据文件管理器”。所述“网络存储权限访问控制器”和“消息业务元数据文件管理器”包括：权限授予单元、权限更新单元和第一权限删除单元。所述权限授予单元包括：第一权限授予子单元和第二权限授予子单元。所述权限更新单元包括第一权限更新子单元和第二权限更新子单元。所述第一权限删除单元包括：第一权限删除子单元和第二权限删除子单元。

[0207] 所述“消息业务元数据文件管理器”还可以包括：第二权限删除单元。所述第二权限删除单元包括：第三权限删除子单元和第四权限删除子单元。

[0208] 所述“消息业务元数据文件管理器”还可以包括：通知服务器。

[0209] 所述网络存储访问权限管理装置中的各个元器件之间的交互关系如下：

[0210] 所述“网络存储权限访问控制器”，获得授权用户的网络存储访问权限操作请求，所述请求中携带授权用户请求操作的存储访问权限信息；所述存储访问权限信息包括授权用户的身份标识，所述存储访问权限信息涉及的网络存储目录或网络存储文件相关信息，至少一个被授权用户的身份标识或至少一个不能被授予访问权限的访问用户的身份标识；根据所述“消息业务元数据文件管理器”中存储访问权限信息，对所述授权用户的网络存储访问权限操作请求，进行合法性验证；

[0211] 所述“消息业务元数据文件管理器”，根据所述“网络存储权限访问控制器”通过验证的网络存储访问权限操作请求，在与所述授权用户的身份标识，以及网络存储目录或网络存储文件相关信息对应的授权用户网络存储访问权限元数据中，根据所述授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限。其根据不同网络存储访问权限操作请求，执行相应的处理，具体如下：

[0212] 通过权限授予单元，根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户的身份标识，以及网络存储目录或网络存储文件相关信息对应的网络存储访问权限元数据文件中，根据所述授权用户请求授予的存储访问权限信

息，将相应的存储访问权限元数据授予给相应的被授权用户。具体处理可以采用两种方案进行：

[0213] 第一种方案，通过第一权限授予子单元，检索与所述授权用户的身份标识对应的“存储授权策略”元数据文件，并在其中的与授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据；或者，检索授权用户的“存储授权策略”元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0214] 第二种方案，通过第二权限授予子单元，检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中根据所述请求中携带的请求授予的存储访问权限信息，创建与被授权用户身份标识对应的存储访问权限元数据，或者，检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述授权用户请求操作的存储访问权限信息所涉及的网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，创建与被授权用户身份标识对应的用户访问规则；同时，在与所述用户访问规则对应的网络存储元数据文件中，根据所述请求中携带的请求授予的存储访问权限信息，创建与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0215] 通过权限更新单元，根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户的身份标识，以及网络存储目录或网络存储文件相关信息对应的网络存储访问权限元数据文件中，根据所述授权用户请求更新的存储访问权限信息，更改授权用户为被授权用户设置的存储访问权限元数据；具体处理可以采用两种方案进行：

[0216] 第一种方案，通过第一权限更新子单元，检索与所述授权用户身份标识对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户身份标识对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求更新的存储访问权限信息，更改与不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0217] 第二种方案，通过第二权限更新子单元，在所述授权用户的身份标识对应的“用户访问策略”元数据文件中，检索与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，与所述被授权用户身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，或对应的“网络存储目录”所关联的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于在所述授权用户的身份标识对应的“用户

访问策略”元数据文件中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，检索与不能被授予访问权限的访问用户的身份标识对应的用户访问规则；并且在与所述用户访问规则对应的网络存储元数据文件中，或对应的“网络存储目录”所关联的网络存储元数据文件中，根据所述请求中携带的请求更新的存储访问权限信息，更改与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0218] 通过第一权限删除单元，根据所述“网络存储权限访问控制器”获得的网络存储访问权限操作请求，在与所述授权用户的身份标识，以及网络存储目录或网络存储文件相关信息对应的网络存储访问权限元数据文件中，根据所述授权用户请求撤回的存储访问权限，删除授权用户为被授权用户设置的存储访问权限元数据。具体处理可以采用两种方案进行：

[0219] 第一种方案，通过第一权限删除子单元，检索与所述授权用户的身份标识对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户的身份标识对应的存储授权策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据；

[0220] 第二种方案，通过第二权限删除子单元，检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述被授权用户身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，或对应的“网络存储目录”所关联的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述被授权用户身份标识对应的存储访问权限元数据；或者，用于检索与所述授权用户的身份标识对应的用户访问策略元数据文件，并在其中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据中，删除与所述不能被授予访问权限的访问用户的身份标识对应的用户访问规则；同时，在与所述被删除的用户访问规则对应的网络存储元数据文件中，或对应的网络存储目录所关联的网络存储元数据文件中，根据所述请求中携带的请求撤回的存储访问权限信息，删除与所述不能被授予访问权限的访问用户的身份标识对应的存储访问权限元数据。

[0221] 另外，所述“消息业务元数据文件管理器”还可以通过第二权限删除单元，用于在所述授权用户对应的网络存储访问权限元数据中，授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的过期时间到达时，删除该存储访问权限元数据。具体处理可以采用两种方案进行：

[0222] 第一种方案，通过第三权限删除子单元，在与所述授权用户身份标识对应的存储授权策略元数据文件中，当某个被授权用户身份标识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；

[0223] 第二种方案，通过第四权限删除子单元，在与所述授权用户身份标识对应的网络存储文件中，或对应的网络存储目录所关联的网络存储文件中，当某个被授权用户身份标

识对应的存储访问权限元数据中的权限过期时间到达时，则删除该存储访问权限元数据；同时，在与所述授权用户身份标识对应的“用户访问策略”元数据文件中，删除与该存储访问权限元数据对应的用户访问规则元数据。

[0224] 另外，一旦“消息业务元数据文件管理器”中的元数据发生变化，所述消息元数据服务器还能够通知变化后的元数据，具体实现如下：

[0225] 通过通知服务器，当根据授权用户的网络存储访问权限操作请求，操作所述授权用户的网络存储目录或网络存储文件的存储访问权限后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权限元数据中对应的被授权用户；或者，当授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限的权限过期时间到达后，将发生变化的网络存储访问权限元数据，通知给所述网络存储访问权限元数据中对应的被授权用户。

[0226] 所述通知服务器在通知被授权用户变化后的存储访问权限元数据时，还可以将能够采用的访问方式，通知给所述访问用户。

[0227] 本发明的第四实施例提供一种网络存储访问权限管理装置，其结构如图 16 所示，包括“网络存储权限访问控制器”和“消息业务元数据文件管理器”。

[0228] 其中所述“消息业务元数据文件管理器”包括：第一访问请求处理单元和第二访问请求处理单元。

[0229] 所述“消息业务元数据文件管理器”还可以包括：数据更新单元。

[0230] 所述“消息业务元数据文件管理器”还可以包括：通知服务器。

[0231] 所述网络存储访问权限管理装置中的各个元器件之间的交互关系如下：

[0232] 当被授权用户访问授权用户的网络存储时，所述“网络存储权限访问控制器”，获得被授权用户针对授权用户网络存储目录或网络存储文件的访问请求，所述访问请求中携带所述被授权用户的身份标识，授权用户身份标识，以及被授权用户请求访问的授权用户网络存储目录或网络存储文件的相关信息；向所述“消息业务元数据文件管理器”请求所述被授权用户身份标识对应的存储访问权限信息；

[0233] 此时，所述“消息业务元数据文件管理器”，将与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户身份标识对应的存储访问权限信息，提供给所述“网络存储权限访问控制器”；

[0234] 所述“网络存储权限访问控制器”根据所述“消息业务元数据文件管理器”返回的信息获得所述“消息业务元数据文件管理器”中与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户身份标识对应的存储访问权限信息；利用所述存储访问权限信息，对所述被授权用户的访问请求进行合法性验证；对通过验证的访问请求，向所述“消息业务元数据文件管理器”请求所述被授权用户具有访问权限的元数据；

[0235] 此时，所述“消息业务元数据文件管理器”将授权用户网络存储文件中，或网络存储目录所关联的网络存储文件中所述被授权用户具有访问权限的元数据，提供给所述“网络存储权限访问控制器”；具体处理时可以采取两种方案实现：

[0236] 第一种方案，通过第一请求处理单元，检索与所述授权用户身份标识对应的“存储授权策略”元数据文件中的与所述网络存储目录或网络存储文件相关信息对应的存储授权策略元数据，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储

访问权限元数据对应的网络存储目录或网络存储文件元数据，反馈给所述“网络存储权限访问控制器”；

[0237] 第二种方案，通过第二请求处理单元，检索与所述授权用户的身份标识对应的“用户访问策略”元数据文件中的与所述网络存储目录或网络存储文件相关信息对应的用户访问规则元数据，获得与所述被授权用户身份标识对应的用户访问规则；根据所述用户访问规则，在对应的网络存储元数据文件中，或对应的网络存储目录所关联的网络存储元数据文件中，获得与所述被授权用户身份标识对应的存储访问权限元数据；将与所述存储访问权限元数据对应的网络存储目录或网络存储文件元数据，反馈给所述“网络存储权限访问控制器”。

[0238] 所述“网络存储权限访问控制器”将所述“消息业务元数据文件管理器”返回的元数据提供给所述被授权用户；

[0239] 所述“网络存储权限访问控制器”获得被授权用户针对所述元数据对应的网络存储消息内容的访问请求，所述访问请求中携带所述被授权用户的身份标识，授权用户身份标识，以及被授权用户请求访问的授权用户网络存储消息内容对应的元数据；此时所述“网络存储权限访问控制器”同样向所述“消息业务元数据文件管理器”请求与所述授权用户对应的网络存储访问权限元数据中的与所述被授权用户身份标识对应的存储访问权限信息，以验证本次访问请求的合法性；验证通过后，对经过认为合法的访问请求，将授权用户网络存储元数据文件中，或网络存储目录所关联的网络存储元数据文件中所述被授权用户具有访问权限的元数据，提供给“消息服务器”，通过“消息服务器”向“消息内容存储器”请求所述被授权用户具有访问权限的元数据对应的消息内容。

[0240] 之后通过所述“消息服务器”与“核心网”的交互控制，建立“消息内容存储器”与所述被授权用户之间的数据传输通道。通过所述数据传输通道，所述被授权用户可以上传消息内容，或者读取消息内容。

[0241] 对于被授权用户上传的消息内容，经过“消息服务器”控制，在“消息内容存储器”中所述授权用户所拥有的网络存储消息内容中添加、更改或删除的信息，随后，所述“消息服务器”会发出请求，以控制所述“消息业务元数据文件管理器”根据所述变化的信息，更新授权用户网络存储目录或网络存储文件中相应的元数据信息。

[0242] 所述“消息业务元数据文件管理器”通过数据更新单元，获得“消息服务器”发送的请求，所述请求中携带：根据被授权用户上传的消息内容在“消息内容存储器”中所述授权用户所拥有的网络存储内容中添加、更改或删除操作后变化的信息；所述数据更新单元根据所述变化的信息，更新授权用户网络存储目录或网络存储文件中相应的元数据信息。

[0243] 另外，一旦“消息业务元数据文件管理器”中的元数据发生变化，所述消息元数据服务器还能够通知变化后的元数据，具体实现如下：

[0244] 通过通知服务器，当根据被授权用户上传的消息内容在授权用户对应的网络存储文件中，或对应的网络存储目录所关联的网络存储文件中更新相应的元数据信息后，将变化后的元数据，通知给所述授权用户，和／或，具有该网络存储目录和／或网络存储文件访问权限的被授权用户。

[0245] 所述通知服务器在通知被授权用户变化后的存储访问权限元数据时，还可以将能够采用的访问方式，通知给所述访问用户。

[0246] 由上述本发明实施例提供的具体实施方案可以看出，其通过在与所述授权用户对应的授权用户网络存储访问权限元数据中，根据授权用户请求操作的存储访问权限信息，操作授权用户为被授权用户设置的网络存储目录或网络存储文件的存储访问权限，从而允许被授权用户访问被授权用户的网络存储。

[0247] 显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

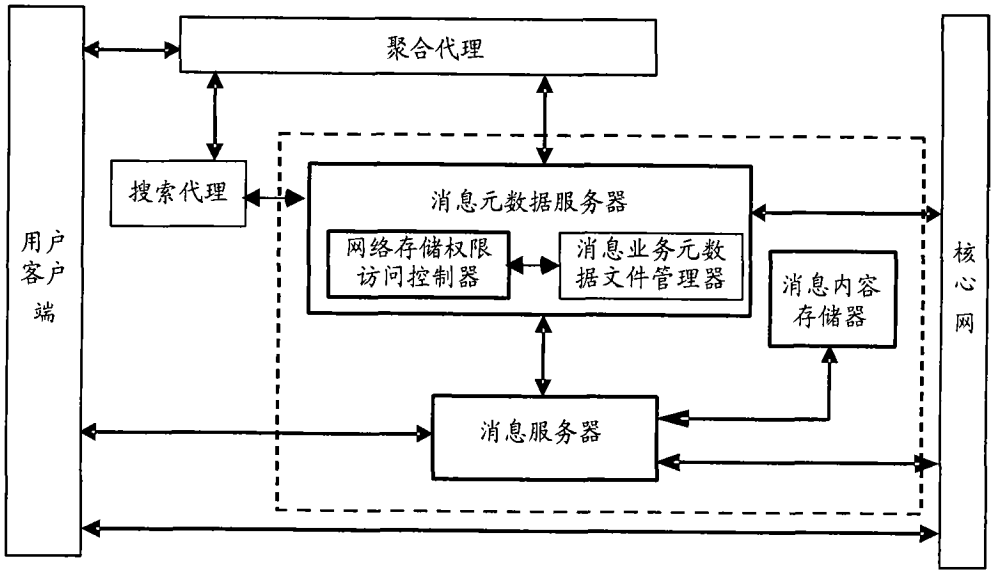

聚合代理
搜索代理
消息元数据服务器
网络存储权限访问控制器
消息业务元数据文件管理器
消息内容存储器
消息服务器
用户客户端
核心网

图 1

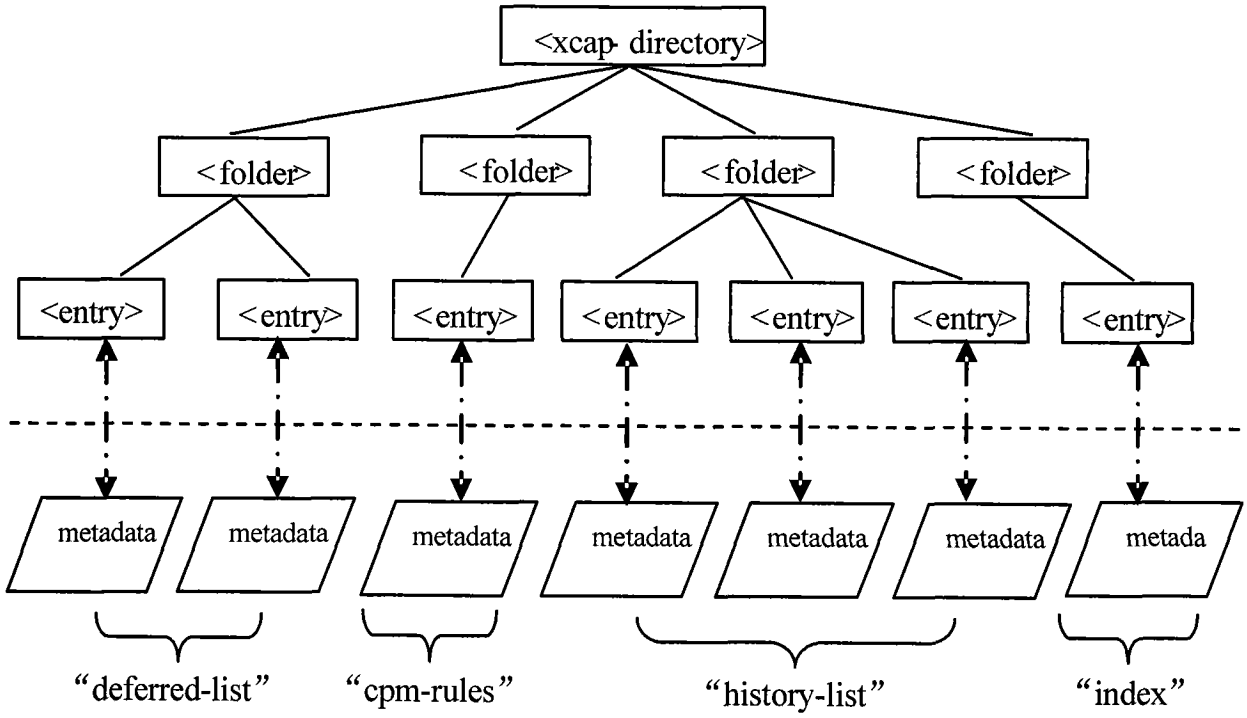

<xcap- directory>
<folder>
<folder>
<folder>
<folder>
<entry>
<entry>
<entry>
<entry>
<entry>
<entry>
<entry>
metadata
metadata
metadata
metadata
metadata
metadata
metada
“deferred-list”
“cpm-rules”
“history-list”
“index”

图 2

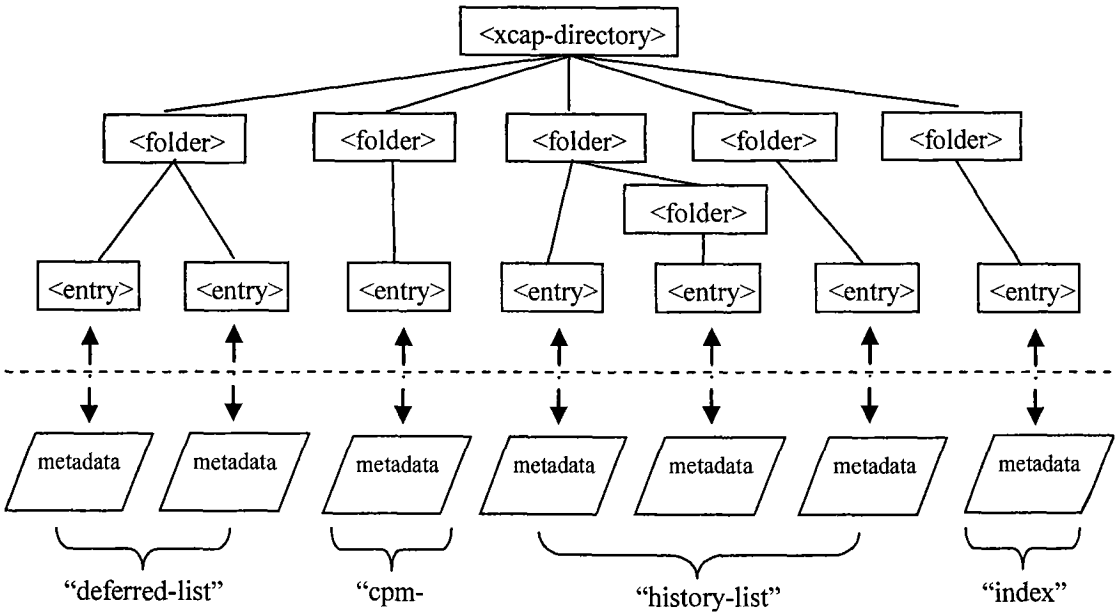

<xcap-directory>
<folder>
<folder>
<folder>
<folder>
<folder>
<folder>
<entry>
<entry>
<entry>
<entry>
<entry>
<entry>
<entry>
metadata
metadata
metadata
metadata
metadata
metadata
metadata
"deferred-list"
"cpm-
"history-list"
"index"

图 3

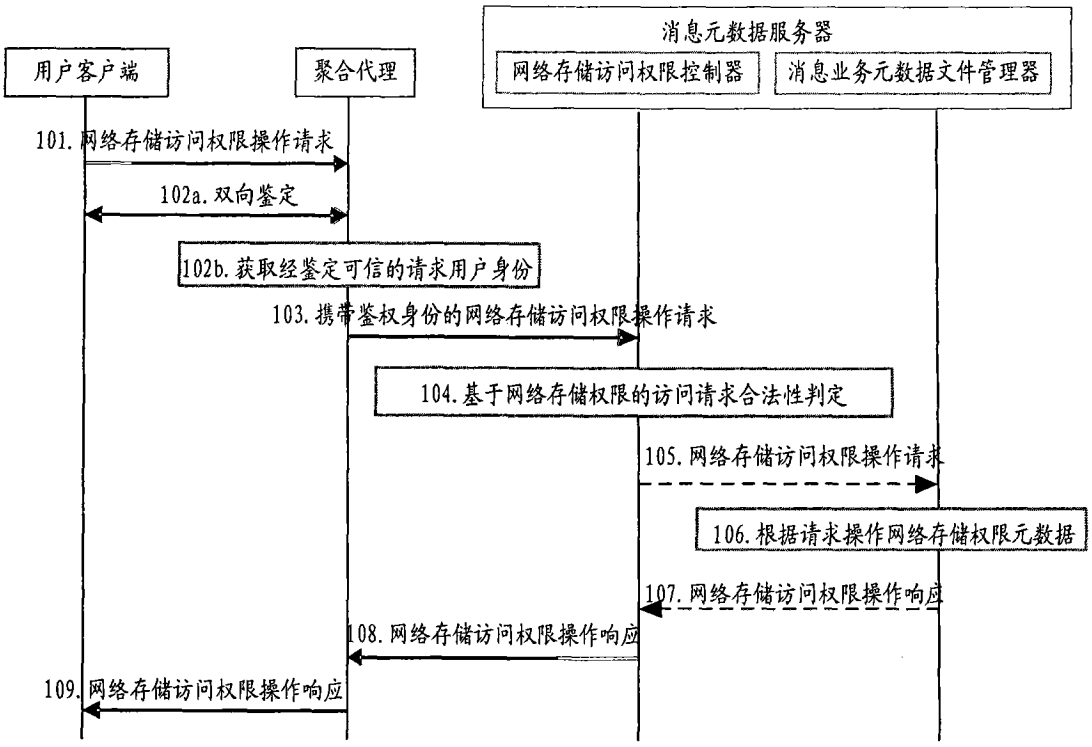

消息元数据服务器
网络存储访问权限控制器
消息业务元数据文件管理器
用户客户端
聚合代理
101. 网络存储访问权限操作请求
102a. 双向鉴定
102b. 获取经鉴定可信的请求用户身份
103. 携带鉴权身份的网络存储访问权限操作请求
104. 基于网络存储权限的访问请求合法性判定
105. 网络存储访问权限操作请求
106. 根据请求操作网络存储权限元数据
107. 网络存储访问权限操作响应
108. 网络存储访问权限操作响应
109. 网络存储访问权限操作响应

图 4

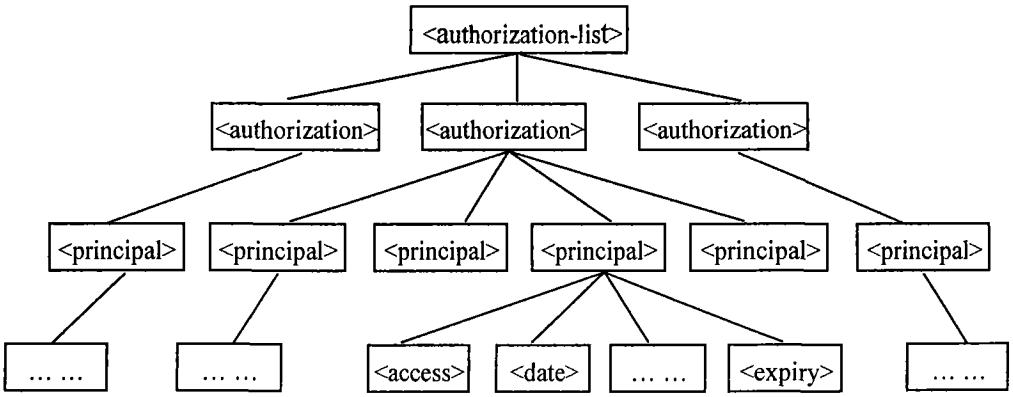

<authorization-list>
<authorization>
<authorization>
<authorization>
<principal>
<principal>
<principal>
<principal>
<principal>
<principal>
… …
… …
<access>
<date>
… …
<expiry>
… …

图 5

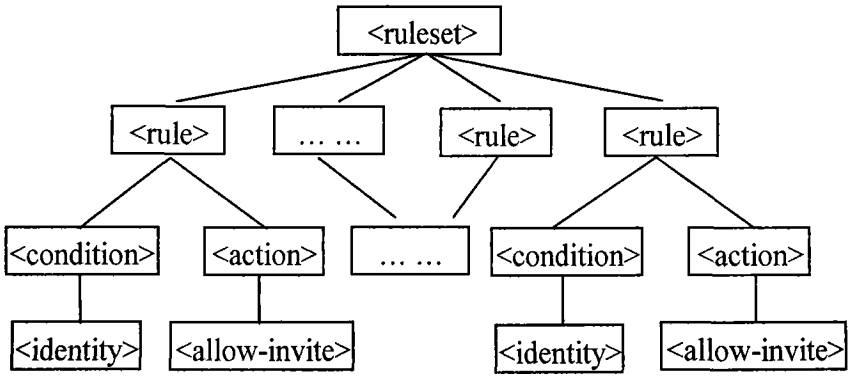

<ruleset>
<rule>
… …
<rule>
<rule>
<condition>
<action>
… …
<condition>
<action>
<identity>
<allow-invite>
<identity>
<allow-invite>

图 6

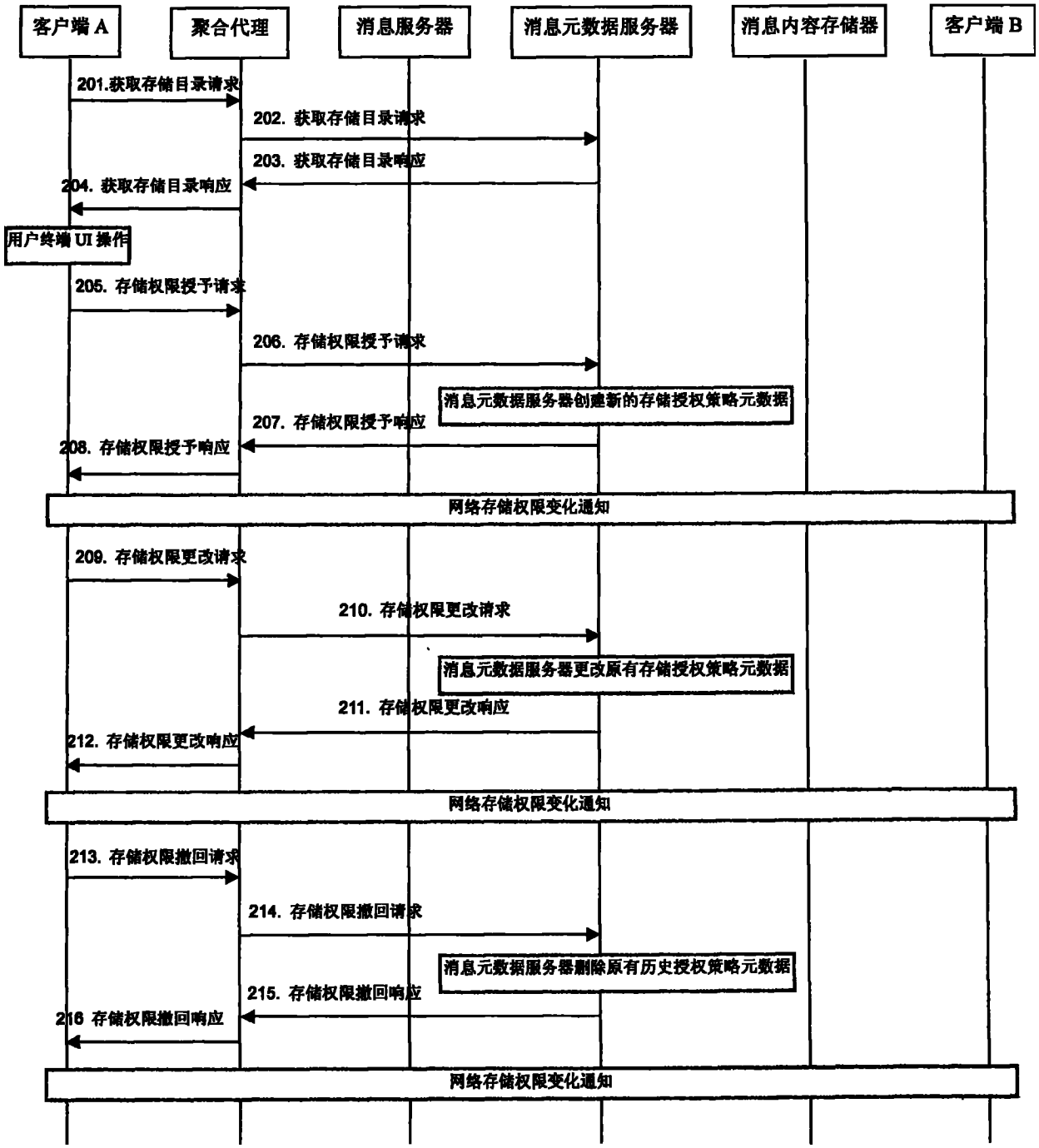

客户端 A
聚合代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
201.获取存储目录请求
202. 获取存储目录请求
203. 获取存储目录响应
204. 获取存储目录响应
用户终端 UI 操作
205. 存储权限授予请求
206. 存储权限授予请求
消息元数据服务器创建新的存储授权策略元数据
207. 存储权限授予响应
208. 存储权限授予响应
网络存储权限变化通知
209. 存储权限更改请求
210. 存储权限更改请求
消息元数据服务器更改原有存储授权策略元数据
211. 存储权限更改响应
212. 存储权限更改响应
网络存储权限变化通知
213. 存储权限撤回请求
214. 存储权限撤回请求
消息元数据服务器删除原有历史授权策略元数据
215. 存储权限撤回响应
216 存储权限撤回响应
网络存储权限变化通知

图 7

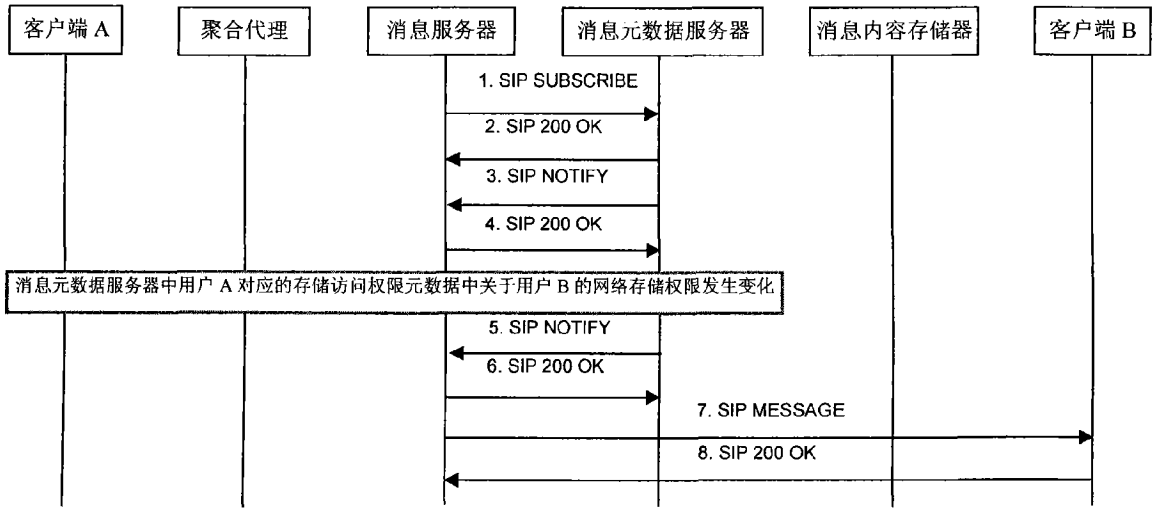

客户端 A
聚合代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
1. SIP SUBSCRIBE
2. SIP 200 OK
3. SIP NOTIFY
4. SIP 200 OK
消息元数据服务器中用户 A 对应的存储访问权限元数据中关于用户 B 的网络存储权限发生变化
5. SIP NOTIFY
6. SIP 200 OK
7. SIP MESSAGE
8. SIP 200 OK

图 8

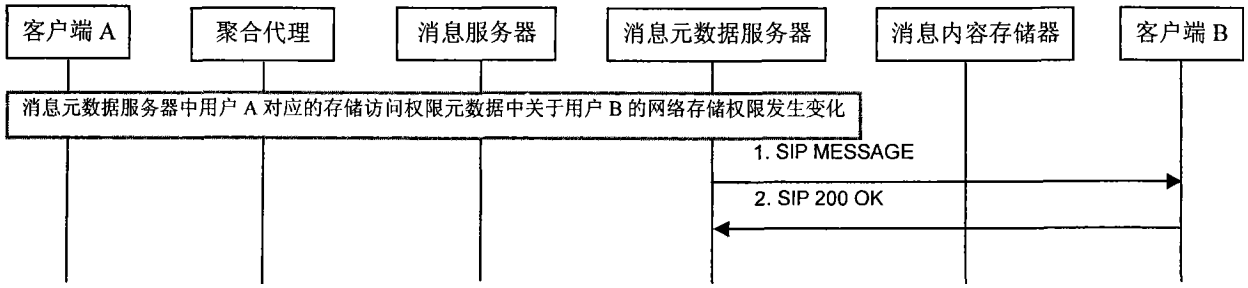

客户端 A
聚合代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
消息元数据服务器中用户 A 对应的存储访问权限元数据中关于用户 B 的网络存储权限发生变化
1. SIP MESSAGE
2. SIP 200 OK

图 9

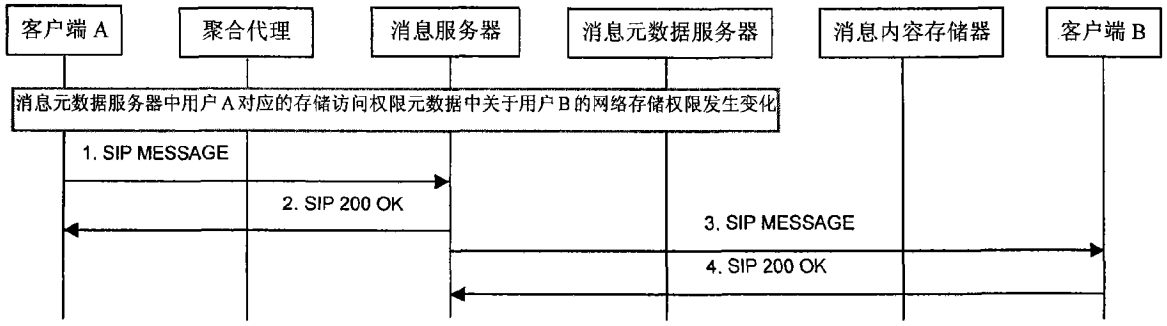

客户端 A
聚合代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
消息元数据服务器中用户 A 对应的存储访问权限元数据中关于用户 B 的网络存储权限发生变化
1. SIP MESSAGE
2. SIP 200 OK
3. SIP MESSAGE
4. SIP 200 OK

图 10

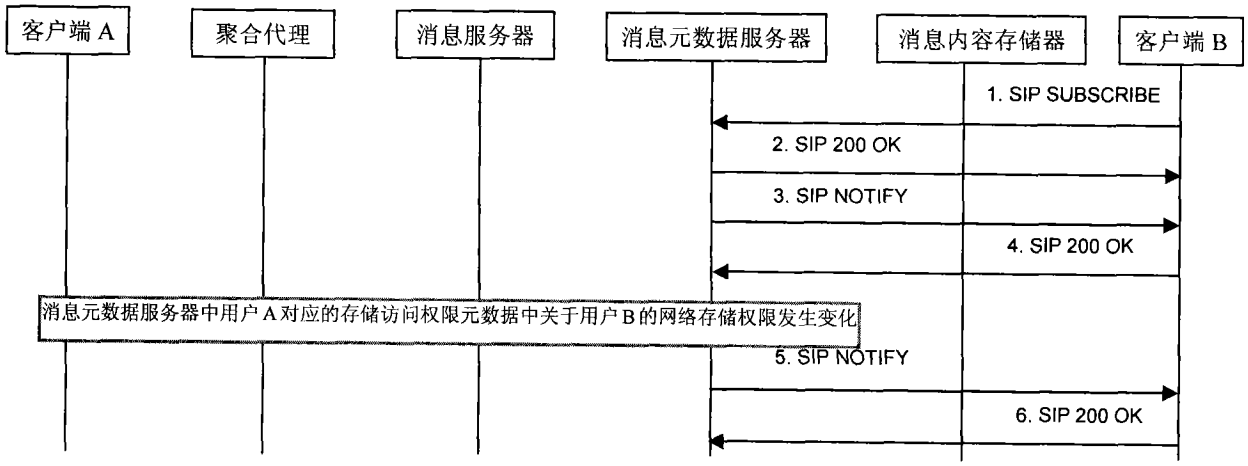

客户端 A
聚合代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
1. SIP SUBSCRIBE
2. SIP 200 OK
3. SIP NOTIFY
4. SIP 200 OK
消息元数据服务器中用户 A 对应的存储访问权限元数据中关于用户 B 的网络存储权限发生变化
5. SIP NOTIFY
6. SIP 200 OK

图 11

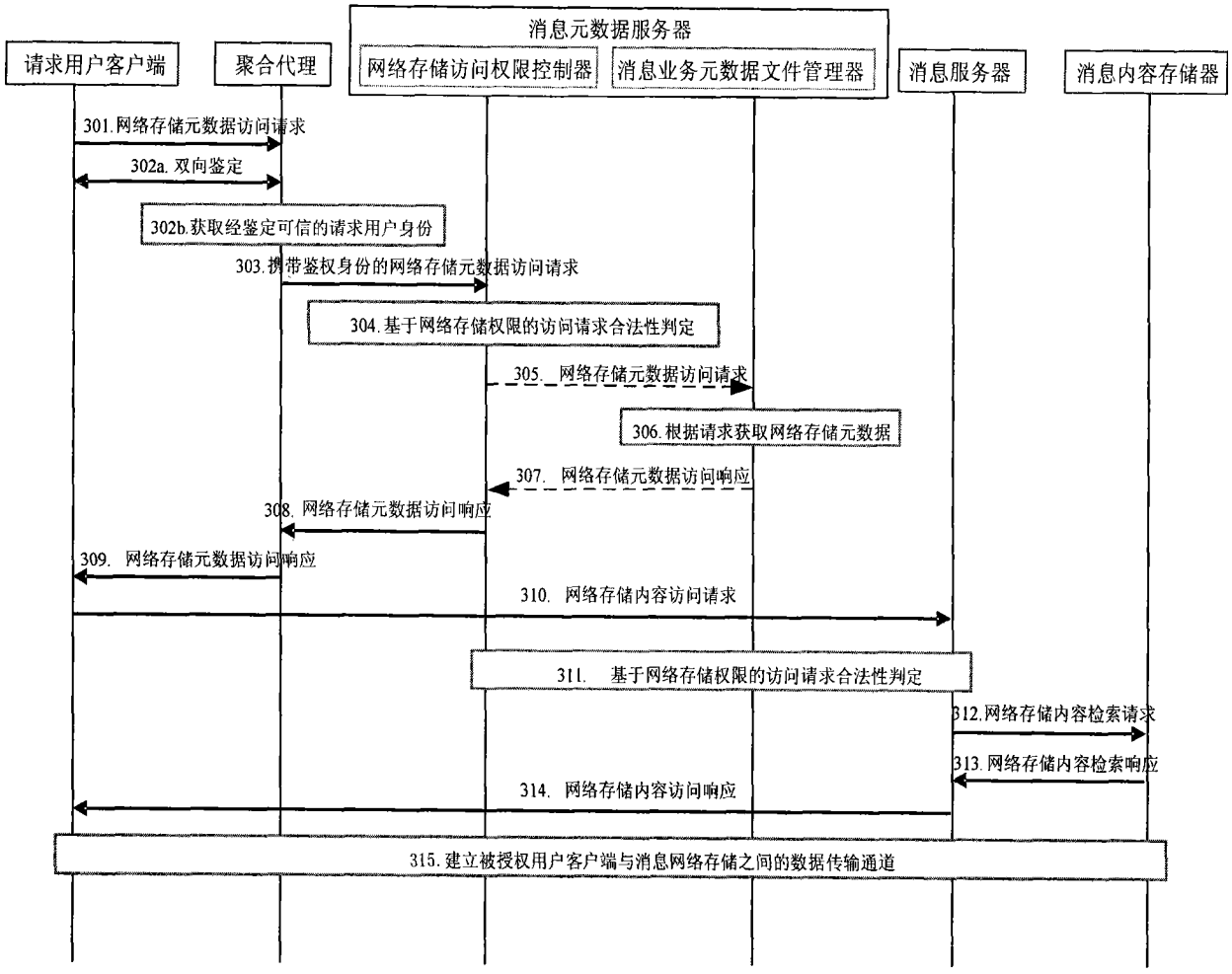

请求用户客户端
聚合代理
消息元数据服务器
网络存储访问权限控制器
消息业务元数据文件管理器
消息服务器
消息内容存储器
301. 网络存储元数据访问请求
302a. 双向鉴定
302b. 获取经鉴定可信的请求用户身份
303. 携带鉴权身份的网络存储元数据访问请求
304. 基于网络存储权限的访问请求合法性判定
305. 网络存储元数据访问请求
306. 根据请求获取网络存储元数据
307. 网络存储元数据访问响应
308. 网络存储元数据访问响应
309. 网络存储元数据访问响应
310. 网络存储内容访问请求
311. 基于网络存储权限的访问请求合法性判定
312. 网络存储内容检索请求
313. 网络存储内容检索响应
314. 网络存储内容访问响应
315. 建立被授权用户客户端与消息网络存储之间的数据传输通道

图 12

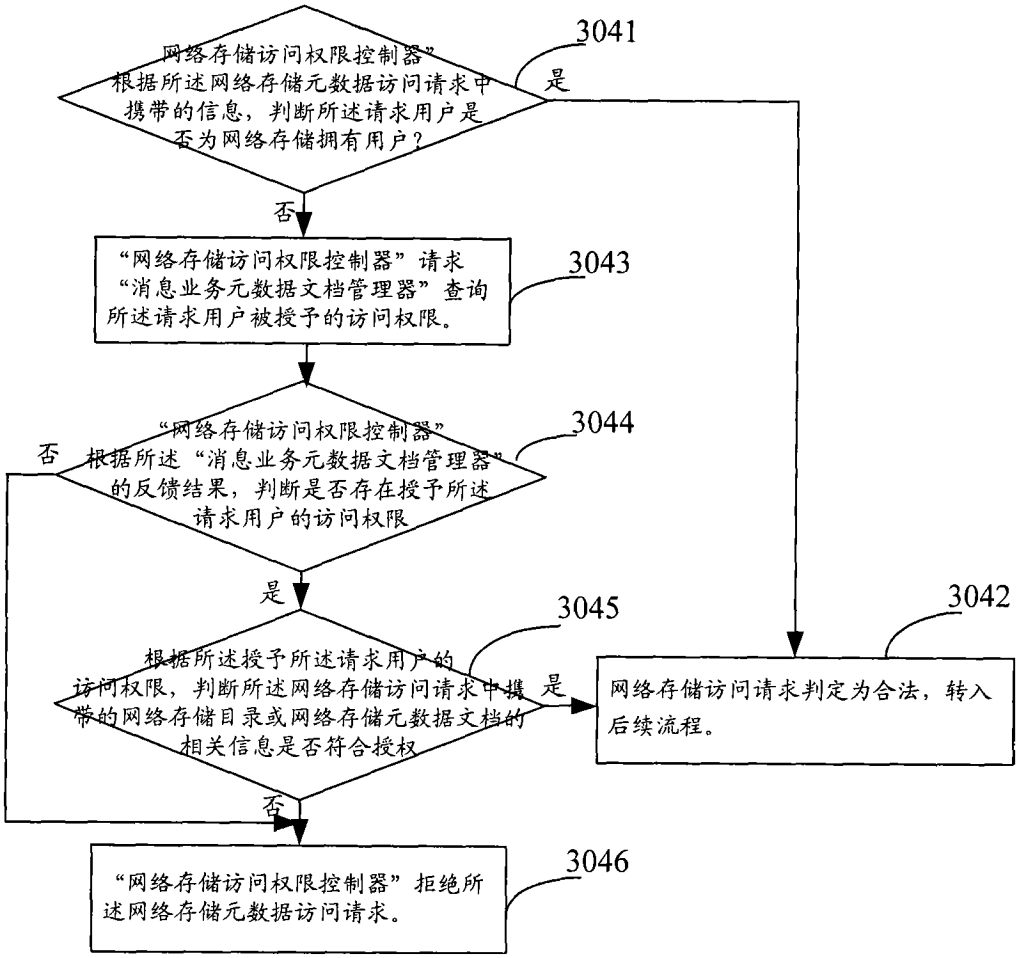

网络存储访问权限控制器”根据所述网络存储元数据访问请求中携带的信息，判断所述请求用户是否为网络存储拥有用户？
3041
是
否
“网络存储访问权限控制器”请求“消息业务元数据文档管理器”查询所述请求用户被授予的访问权限。
3043
“网络存储访问权限控制器”根据所述“消息业务元数据文档管理器”的反馈结果，判断是否存在授予所述请求用户的访问权限
3044
否
是
根据所述授予所述请求用户的访问权限，判断所述网络存储访问请求中携带的网络存储目录或网络存储元数据文档的相关信息是否符合授权
3045
是
网络存储访问请求判定为合法，转入后续流程。
3042
否
“网络存储访问权限控制器”拒绝所述网络存储元数据访问请求。
3046

图 13

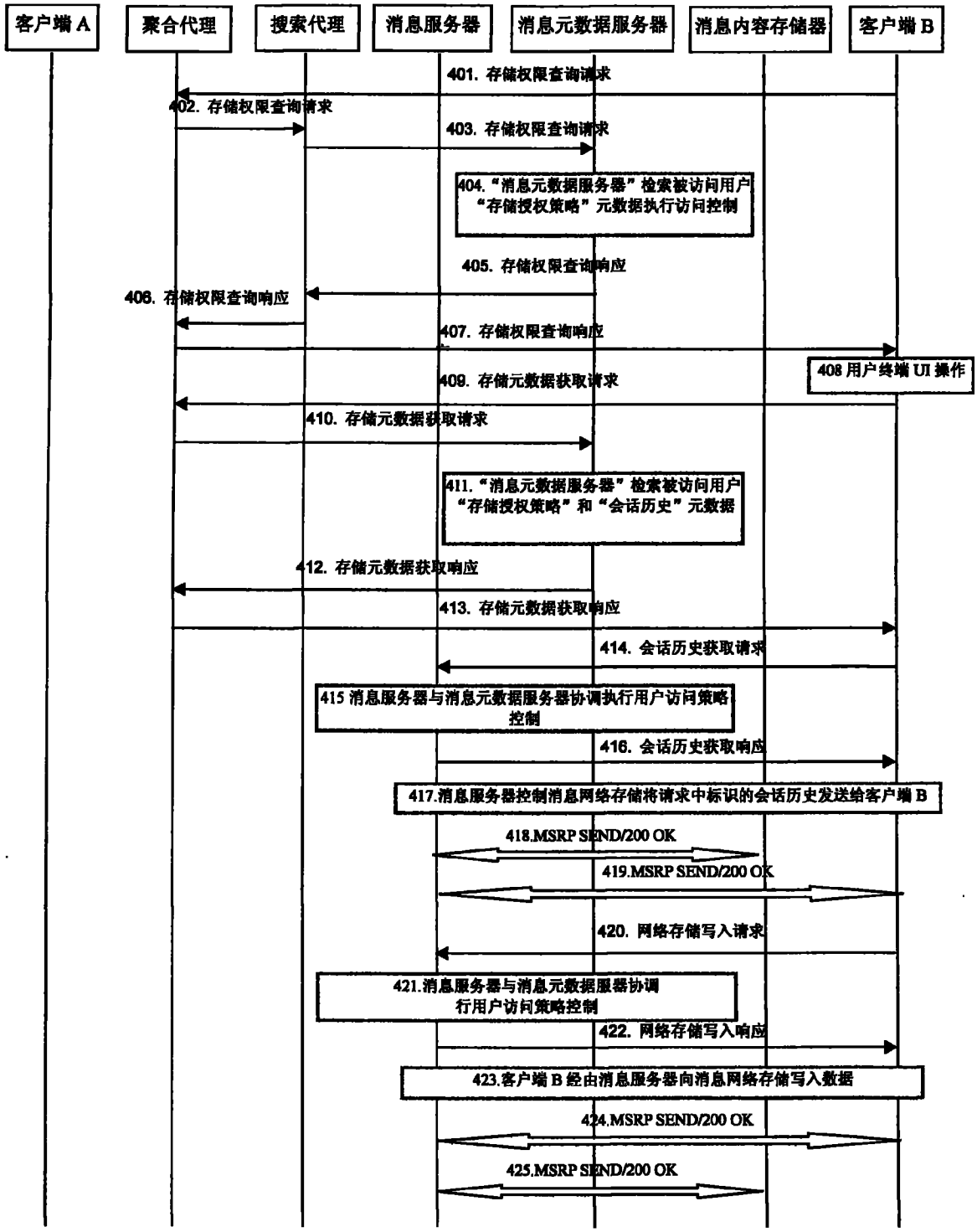

客户端 A
聚合代理
搜索代理
消息服务器
消息元数据服务器
消息内容存储器
客户端 B
401. 存储权限查询请求
402. 存储权限查询请求
403. 存储权限查询请求
404. “消息元数据服务器”检索被访问用户“存储授权策略”元数据执行访问控制
405. 存储权限查询响应
406. 存储权限查询响应
407. 存储权限查询响应
408 用户终端 UI 操作
409. 存储元数据获取请求
410. 存储元数据获取请求
411. “消息元数据服务器”检索被访问用户“存储授权策略”和“会话历史”元数据
412. 存储元数据获取响应
413. 存储元数据获取响应
414. 会话历史获取请求
415 消息服务器与消息元数据服务器协调执行用户访问策略控制
416. 会话历史获取响应
417.消息服务器控制消息网络存储将请求中标识的会话历史发送给客户端 B
418.MSRP SEND/200 OK
419.MSRP SEND/200 OK
420. 网络存储写入请求
421.消息服务器与消息元数据服务器协调行用户访问策略控制
422. 网络存储写入响应
423.客户端 B 经由消息服务器向消息网络存储写入数据
424.MSRP SEND/200 OK
425.MSRP SEND/200 OK

图 14

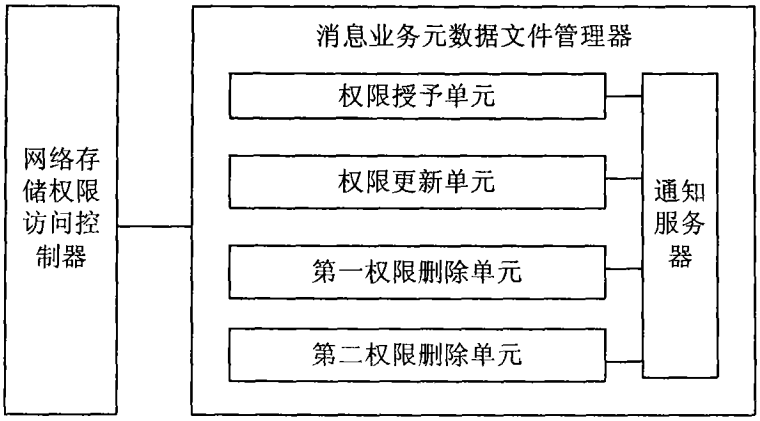

网络存储权限访问控制器
消息业务元数据文件管理器
权限授予单元
权限更新单元
第一权限删除单元
第二权限删除单元
通知服务器

图 15

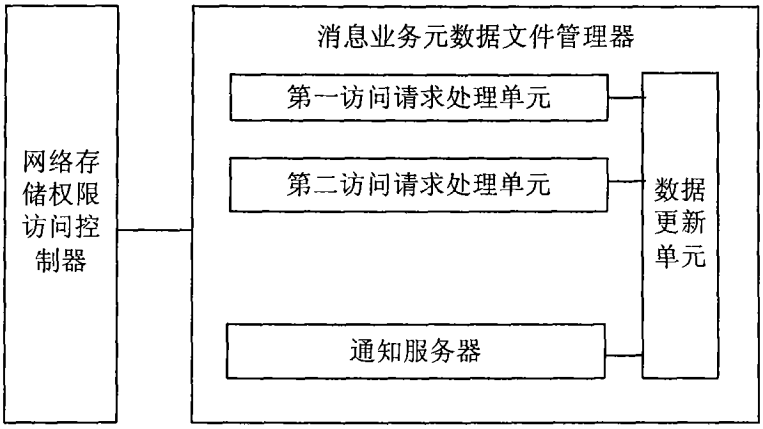

网络存储权限访问控制器
消息业务元数据文件管理器
第一访问请求处理单元
第二访问请求处理单元
通知服务器
数据更新单元

图 16