[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 9/00 (2006.01)
H04L 12/22 (2006.01)

[12] 发明专利说明书

专利号 ZL 02145981.9

[45] 授权公告日 2006 年 9 月 27 日

[11] 授权公告号 CN 1277366C

[22] 申请日 2002.10.31 [21] 申请号 02145981.9

[71] 专利权人 华为技术有限公司
地址 518057 广东省深圳市科技园科发路华为用服大厦
[72] 发明人 段小琴
审查员 李婷婷

[74] 专利代理机构 北京德琦知识产权代理有限公司
代理人 张颖玲

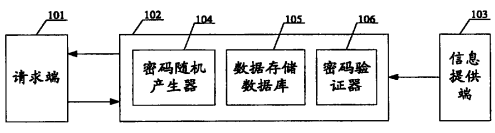
权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称

一种信息提供端数据保护的方法

[57] 摘要

本发明公开了一种信息提供端数据保护的方法，涉及数据安全领域，采用数据管理服务器完成对请求端访问密码的管理：数据管理服务器为信息提供端授权的每个请求端分配访问密码，数据管理服务器依据请求端提供的访问密码进行身份验证；数据管理服务器还可以按照信息提供端的指示对请求端的访问密码进行注销和修改。在授权过程中，信息提供端只需在数据管理服务器上对请求端进行授权，由数据管理服务器完成对请求端访问密码的分配，而信息提供端无需自行为请求端分配访问密码，以实现对授权机制的改进；在验证过程中，当请求端向信息提供端发访问请求时，由数据管理服务器完成请求端访问密码的核对和验证，以提高请求端对信息提供端数据的访问效率。



1、一种信息提供端数据保护的方法，其特征在于该方法包括:

A、预先在请求端和信息提供端之间设置数据管理服务器，信息提供端通知数据管理服务器其授权的请求端信息，由该数据管理服务器为信息提供端授权的每个请求端分配一个访问密码，并将该访问密码通知相应的请求端;

B、当请求端访问信息提供端时，由步骤 A 所设置的数据管理服务器根据请求端提供的访问密码对其身份进行验证。

2、根据权利要求 1 所述的方法，其特征在于步骤 A 进一步包括:

A1、信息提供端向数据管理服务器提供其授权的请求端标识名单;

A2、数据管理服务器为每个请求端分配一个访问密码，并将该访问密码通知相应的请求端；同时，数据管理服务器存储信息提供端标识、请求端标识和访问密码及三者之间的对应关系。

3、根据权利要求 1 所述的方法，其特征在于步骤 B 进一步包括:

B1、请求端请求访问信息提供端数据时，向数据管理服务器提供被访问信息提供端的标识、请求端标识及该请求端的访问密码;

B2、数据管理服务器在自身存储的信息中搜索到与信息提供端相对应的请求端的访问密码，将其与当前请求端所提供的访问密码进行比较核对，如果一致，则通过密码验证，数据管理服务器通知该请求端接受其访问请求；否则，数据管理服务器通知该请求端拒绝其访问请求。

4、根据权利要求 1 所述的方法，其特征在于该方法进一步包括：信息提供端注销请求端的访问密码时，信息提供端向数据管理服务器提供需要注销的请求端标识名单，数据管理服务器根据该注销请求端标识名单注销相应请求端原来的访问密码，并通知该请求端。

5、根据权利要求 1 所述的方法，其特征在于该方法进一步包括：信息提供端修改请求端的访问密码时，信息提供端向数据管理服务器提供需要修改的请求端标识名单，数据管理服务器根据该修改请求端标识名单为相应请求端重新

分配访问密码，同时注销该请求端原来的访问密码，并将修改后的访问密码通知该请求端。

6、根据权利要求 1 所述的方法，其特征在于步骤 A 进一步包括：在请求端和信息提供端之间预先设置包括密码随机产生器、数据存储数据库和密码验证器的数据管理服务器。

一种信息提供端数据保护的方法

技术领域

本发明涉及数据安全领域，特别是一种信息提供端数据保护的方法。

背景技术

在通信领域中，对于信息提供端信息、资源等数据的安全保护方式通常采用密码验证的方式。对每个需要访问信息数据的请求端都分配有一个访问密码，该请求端在访问信息提供端数据之前要先进行访问密码的验证，访问密码验证通过后请求端才能被接入访问，访问密码验证不通过则拒绝请求端的访问，即通过访问密码保护来控制请求端对信息提供端数据的访问，防止非法访问和非法接入。这里，信息提供端是指提供一定信息和资源的被访问者，请求端是指向信息提供端请求访问其信息、资源等数据的访问端。

具体到移动通信网络的位置业务（LCS，Location Service）中，请求端在获取信息提供端地理位置的过程中，信息提供端需要请求端提供访问密码（cordword）来验证请求端是否已被授权。在第三代伙伴计划（3GPP ，Third Generation Partnership Project）的 Rel 6 TS2071-610 规范中提出两种对访问密码的验证方式：一种方式是信息提供端为每个请求端分配访问密码，且在位置请求时，请求端向移动通信网络提供访问密码，移动通信网络将访问密码随同请求信息一起提供给信息提供端，由信息提供端进行访问密码的验证，该验证方式通常称为信息提供端全权管理方式。另一种方式是信息提供端提前在移动通信网络上对每一个请求端的访问密码进行注册，由移动通信网络对请求端提供的访问密码进行验证，该验证方式通常称为密码验证服务器管理方式。

目前，在信息提供端全权管理方式下，当信息提供端对请求端 A 进行

授权、验证时，信息提供端为请求端 A 分配一个访问密码，并将与请求端 A 相对应的访问密码通知请求端 A；请求端 A 请求访问信息提供端数据时，向信息提供端提供自己的访问密码；信息提供端在进行访问密码验证时，是将请求端 A 提供的访问密码与自己分配给请求端 A 的访问密码进行比较、核对，如果一致，则访问密码验证通过，接受访问请求；否则，拒绝访问请求。

信息提供端全权管理方式下，访问密码的分配、比较、核对和管理全部由信息提供端完成。这样，对于大量的请求端，信息提供端需要为请求端分配大量的不同的访问密码，并且需要记忆每个访问密码和请求端之间的对应关系。对于访问密码的修改和注销工作，也需要由信息提供端进行相应的访问密码分配和管理，工作量较大且需要占用信息提供端的存储资源。

在密码验证服务器管理方式下，信息提供端为请求端 B 分配一个访问密码，并将该访问密码提前注册于密码验证服务器上，然后信息提供端或密码验证服务器将请求端 B 的访问密码通知请求端 B；请求端 B 请求访问信息提供端数据时，向密码验证服务器提供自己的访问密码。密码验证服务器在进行访问密码验证时，密码验证服务器将请求端 B 提供的访问密码与信息提供端提前注册的与请求端 B 对应的访问密码进行比较、核对，如果一致，则访问密码验证通过，接受访问请求；否则，拒绝访问请求。

上面所述的密码验证服务器是一种能够存储信息提供端对不同请求端分配的不同访问密码，并能够根据请求端提供的访问密码进行验证的服务器。该密码验证服务器可以独立成一个物理实体，也可以作为一个功能模块集成在其他实体中。

密码验证服务器管理方式较信息提供端全权管理方式简化了信息提供端的访问密码验证部分，将访问密码验证部分通过密码验证服务器来完成。但访问密码的分配和管理工作同样由信息提供端来完成，信息提供端同样需要记忆已分配了的每个访问密码与请求端之间的对应关系，以避免造成误用。对于访问密码的修改和注销工作，也需要由信息提供端进行相应的访问

密码分配和管理，同样存在信息提供端工作量大的问题。

发明内容

有鉴于此，本发明的目的在于提供一种信息提供端数据保护的方法，将访问密码的分配、管理和安全性验证全部集中在数据管理服务器中完成，实现了对授权验证机制的改进。

为了达到上述目的，本发明提供了一种信息提供端数据保护的方法，其特征在于该方法包括:

A、预先在请求端和信息提供端之间设置数据管理服务器，信息提供端通知数据管理服务器其授权的请求端信息，由该数据管理服务器为信息提供端授权的每个请求端分配一个访问密码，并将该访问密码通知相应的请求端;

B、当请求端访问信息提供端时，由步骤 A 所设置的数据管理服务器根据请求端提供的访问密码对其身份进行验证。

步骤 A 进一步包括:

A1、信息提供端向数据管理服务器提供其授权的请求端标识名单;

A2、数据管理服务器为每个请求端分配一个访问密码，并将该访问密码通知相应的请求端；同时，数据管理服务器存储信息提供端标识、请求端标识和访问密码及三者之间的对应关系。

步骤 B 进一步包括:

B1、请求端请求访问信息提供端数据时，向数据管理服务器提供被访问信息提供端的标识、请求端标识及该请求端的访问密码;

B2、数据管理服务器在自身存储的信息中搜索到与信息提供端相对应的请求端的访问密码，将其与当前请求端所提供的访问密码进行比较核对，如果一致，则通过密码验证，数据管理服务器通知该请求端接受其访问请求；否则，数据管理服务器通知该请求端拒绝其访问请求。

较佳地，该方法进一步包括：信息提供端注销请求端的访问密码时，信息提供端向数据管理服务器提供需要注销的请求端标识名单，数据管理服务器根

据该注销请求端标识名单注销相应请求端原来的访问密码，并通知该请求端。

该方法进一步包括：信息提供端修改请求端的访问密码时，信息提供端向数据管理服务器提供需要修改的请求端标识名单，数据管理服务器根据该修改请求端标识名单为相应请求端重新分配访问密码，同时注销该请求端原来的访问密码，并将修改后的访问密码通知该请求端。

步骤 A 进一步包括：在请求端和信息提供端预先设置包括密码随机产生器、数据存储数据库和密码验证器的数据管理服务器。

本发明通过数据管理服务器集中完成了对请求端访问密码的分配、验证和管理操作。在整个过程中，信息提供端只需在数据管理服务器上对请求端进行授权，数据管理服务器自动对每个请求端分配访问密码，并完成对请求端身份的鉴别和对访问密码的管理。因此，访问密码对信息提供端来说完全是透明的，信息提供端不需要为请求端自行分配访问密码，甚至信息提供端不需要知道访问密码的内容便完成了整个授权过程，大大简化了信息提供端的授权机制。当请求端向信息提供端发出访问请求时，由数据管理服务器完成请求端访问密码的核对和验证工作，提高了请求端对信息提供端数据的访问效率。

附图说明

图 1 为本发明授权验证系统结构示意图；

图 2 为本发明数据管理服务器授权验证实现的流程图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图对本发明作进一步地详细描述。

本发明是通过访问密码的分配、验证和管理全部由数据管理服务器完成的方法来改进授权验证机制。

图 1 为本发明授权验证系统结构示意图，如图 1 所示：本发明的授权验

证系统主要由请求端 101、数据管理服务器 102 和信息提供端 103 组成。

其中，数据管理服务器 102 是指一种能够根据信息提供端授权的不同请求端标识来分配不同的访问密码、并且对访问密码进行管理和验证的服务器。该数据管理服务器 102 可以独立成一个物理实体，也可以作为一个功能模块集成在其他实体中。

数据管理服务器 102 从功能上可进一步划分为三个部分：密码随机产生器 104、数据存储数据库 105 和密码验证器 106。密码随机产生器 104 用于随机产生密码，要求使用一定的标准算法使得产生的密码各不相同且无规律性。此处所采用的密码产生算法可以随意选择，如根据请求端的标识加随机后缀等等。数据存储数据库 105 用于保存各信息提供端 103 标识、与其对应的请求端 101 标识和密码随机产生器为请求端 101 分配的访问密码，以及三者相互之间的对应关系。密码验证器 106 用于从数据存储数据库 105 中搜索出与当前某信息提供端的请求端相对应的访问密码，并将其与当前请求端 101 提供的访问密码进行比较核对。由此可见，数据管理服务器可以是授权验证机制中新设置的一个功能实体，也可以是在现有技术中的密码验证服务器上增加密码随机产生器部分，如此，即可实现数据管理服务器的全部功能。

在本发明中，信息提供端向数据管理服务器提供需要授权的请求端标识名单，该请求端标识可以是请求端名称等能够唯一标识请求端的信息，用以区分该信息提供端各个不同的请求端。数据管理服务器中的密码随机产生器依据事先设定的标准算法为每个请求端随机分配一个访问密码，如采用依据请求端的标识加上随机后缀生成密码的算法，以保证每个请求端的密码各不相同且无规律性。数据管理服务器将访问密码通知相应的请求端。该信息提供端的标识、该信息提供端的每个请求端标识和分配的密码以及三者相互之间的对应关系存储于数据管理服务器中的数据存储数据库中。请求端请求访问信息提供端数据时，请求端向数据管理服务器提供被访问信息提供端的标识、请求端标识及该请求端的访问密码。数据管理服务器中的密码验证器从

数据存储数据库中搜索到与该信息提供端相对应的该请求端的访问密码，将其与该信息提供端的请求端提供的访问密码进行比较核对，如果一致，则通过密码验证，数据管理服务器通知该请求端接受其访问请求；如果不一致，则数据管理服务器通知该请求端拒绝其访问请求。

当信息提供端需要注销一些请求端的访问密码时，只需向数据管理服务器提供需要注销的请求端标识名单，数据管理服务器根据该注销请求端标识名单自动注销该请求端原来的访问密码，并通知该请求端。该请求端使用原来的访问密码将无法通过密码验证，无法访问信息提供端。

当信息提供端需要修改一些请求端的访问密码时，只需向数据管理服务器提供需要修改的请求端标识名单，数据管理服务器根据该修改请求端标识名单自动为该请求端重新分配访问密码，同时将该请求端原来的访问密码注销。数据管理服务器会将修改后的访问密码通知该请求端。该请求端使用原来的访问密码将无法通过密码验证，无法访问信息提供端，该请求端只有使用新分配的访问密码才能通过密码验证，访问信息提供端。

以移动通信网络中的位置业务为例，预先在移动通信网络中设置数据管理服务器，那么，请求端在获取信息提供端地理位置时的数据管理服务器授权验证过程如图 2 所示，包括以下的步骤：

步骤 201~步骤 203：授权过程。信息提供端向移动通信网络的数据管理服务器提供其授权的请求端标识名单；数据管理服务器中的密码随机产生器为该信息提供端的每个请求端分配一个访问密码，数据管理服务器中的数据存储数据库存储该信息提供端的标识、该信息提供端的每个请求端标识和分配的访问密码以及三者相互之间对应的关系；数据管理服务器将分配的访问密码通知相应的请求端。

步骤 204~步骤 208：验证过程。请求端向移动通信网络的数据管理服务器发出访问信息提供端位置的请求，请求端向数据管理服务器提供被访问信息提供端的标识、请求端标识及该请求端的访问密码；数据管理服务器中的

密码验证器从数据存储数据库中搜索到与该信息提供端相对应的该请求端的访问密码，将其与该信息提供端的请求端提供的访问密码进行比较核对，如果一致，则通过密码验证，数据管理服务器通知该请求端接受其访问请求；否则，数据管理服务器通知该请求端拒绝其访问请求。

在本实施例中，当信息提供端需要注销一些请求端的访问密码时，只需向移动通信网络的数据管理服务器提供需要注销的请求端标识名单，数据管理服务器根据该注销请求端标识名单自动注销该请求端原来的访问密码，并通知该请求端。该请求端使用原来的访问密码将无法通过密码验证，无法访问信息提供端。

在本实施例中，当信息提供端需要修改一些请求端的访问密码时，只需向移动通信网络的数据管理服务器提供需要修改的请求端标识名单，数据管理服务器根据该修改请求端标识名单自动为该请求端重新分配访问密码，并将该请求端原来的访问密码注销。数据管理服务器会将修改后的访问密码通知该请求端。该请求端使用原来的访问密码将无法通过密码验证，无法访问信息提供端，该请求端只有使用新分配的访问密码才能通过密码验证，访问信息提供端。

当然，在实际应用中，本发明提出的有关信息提供端数据安全的授权验证机制还可以应用于其他多种通信系统中。

总之，以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

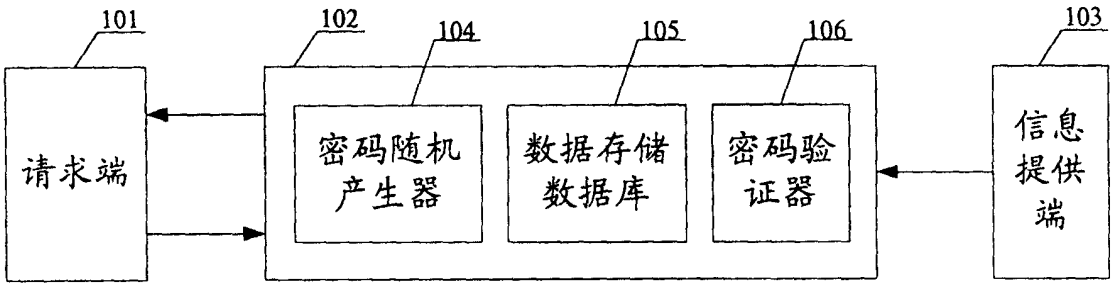


图 1

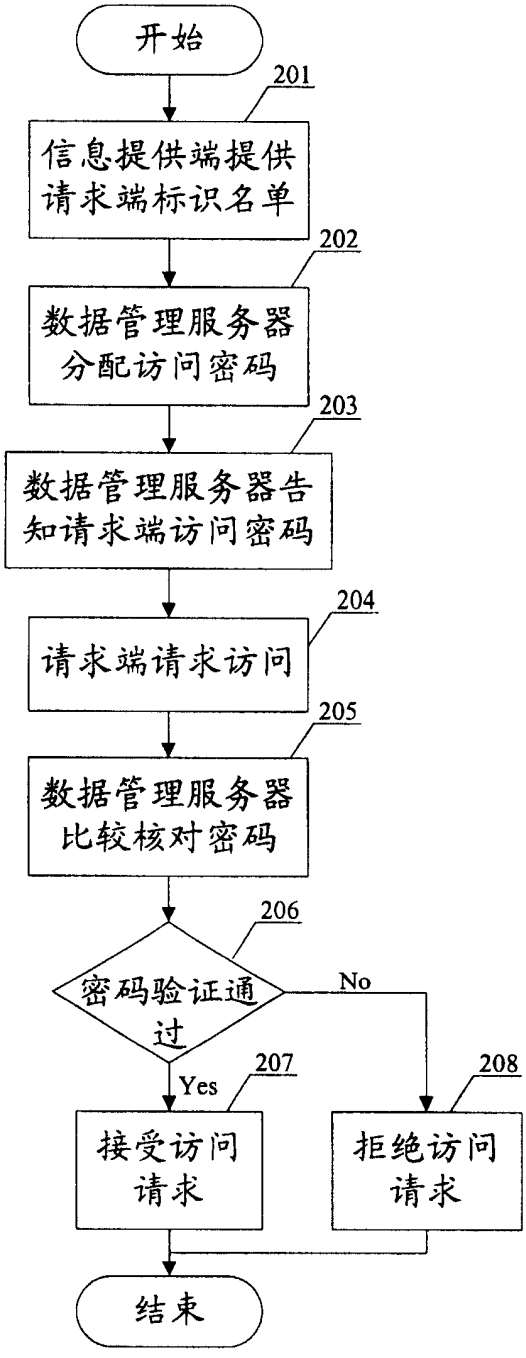

开始
201
信息提供端提供请求端标识名单
202
数据管理服务器分配访问密码
203
数据管理服务器告知请求端访问密码
204
请求端请求访问
205
数据管理服务器比较核对密码
206
密码验证通过
No
Yes
207
208
接受访问请求
拒绝访问请求
结束

图 2