(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 101677272 B
(45)授权公告日 2013.08.21

(21)申请号 200910149873.8

(22)申请日 2009.07.02

(30)优先权数据
2008-240196 2008.09.19 JP

(73)专利权人 日立汽车系统株式会社
地址 日本茨城县

(72)发明人 梅泽克之 柏山正守 青岛弘和

(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 许静

(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 1497485 A,2004.05.19,
CN 1940940 A,2007.04.04,
WO 2008017008 A3,2008.05.15,
KR 100749720 B1,2007.08.16,
WO 2007115209 A3,2008.01.10,
CN 1388931 A,2003.01.01,

审查员 王桂霞

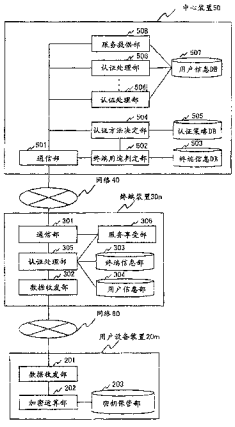
权利要求书3页 说明书6页 附图4页

(54)发明名称

中心装置、终端装置以及认证系统

(57)摘要

本发明提供一种中心装置、终端装置以及认证系统。在对个人进行认证的情况下，如果是自用车，则可以在汽车导航终端中登记家族成员数量的个人信息来使用，但是在租用车或者汽车共享使用等中，无法在共有的汽车的汽车导航终端中登记个人信息。即考虑到根据汽车的使用方式，在中心侧切换用户认证的方法是重要的，考虑能够不降低用户的便利性地安全地进行认证。本发明鉴于上述情况而做出，提供在认证了设备后切换用户认证的方法来利用的系统及其方法。具体来说，在经由终端装置进行用户认证时，在认证了终端装置后，根据其认证结果判别终端装置的使用用途，切换实施用户认证的方法使其适合该使用用途。



CN 101677272 B

1. 一种向终端装置提供服务的中心装置，其特征在于，

具有：

收发数据的通信部；

与终端装置的终端 ID 对应地存储其用途的终端信息 DB；

把所述终端装置的用途和认证方法的多种组合作为认证策略进行登记的认证策略 DB；

根据终端装置的用途和在所述认证策略 DB 中登记的所述认证策略来决定用户认证方法的认证方法决定部；

执行遵照所述认证方法决定部所决定的用户认证方法的认证处理的认证处理部；

在所述认证处理成功的情况下，向所述终端装置提供服务的服务提供部；

其中所述中心装置还包括：

具有根据从终端装置接收到的至少包含终端 ID、或者用服务器的私钥加密终端 ID 所得到的信息的终端信息、和所述终端信息 DB 判定所述终端装置的用途的终端用途判定部，

所述认证方法决定部，根据所述终端用途判定部判定的所述终端装置的用途、和在所述认证策略 DB 中登记的认证策略，决定用户认证方法。

2. 一种享受权利要求 1 所述的中心装置提供的服务的终端装置，其特征在于，具有：

和所述中心装置收发数据的通信部；

和用户设备装置收发数据的数据收发部；

保管该终端装置的终端信息的终端信息部；

执行与所述中心装置的认证请求对应的认证处理的认证处理部；和

在通过所述认证处理由所述中心装置认证了该终端的情况下，享受所述中心装置提供的服务的服务享受部；

其中，所述终端装置还具有存储一个或者多个用户的用户信息的用户信息部，

所述认证处理部根据所述中心装置的认证请求，从所述用户信息部取得所述用户信息，

所述通信部向所述中心装置发送所述用户信息。

3. 根据权利要求 2 所述的终端装置，其特征在于，

所述认证处理部根据所述中心装置的认证请求，从所述终端信息部取得所述终端信息，

所述通信部向所述中心装置发送所述终端信息。

4. 一种认证系统，其中的中心装置为提供服务，对使用终端装置的用户进行认证，所述认证系统的特征在于，

所述终端装置具有：

保管该终端装置的终端信息的终端信息部；和

享受所述中心装置提供的服务的服务享受部，

所述中心装置具有：

与终端装置的终端 ID 对应地存储其用途的终端信息 DB；

把所述终端装置的用途和认证方法的多种组合作为认证策略进行登记的认证策略 DB；

根据终端装置的用途和在所述认证策略 DB 中登记的所述认证策略来决定用户认证方法的认证方法决定部；

执行遵照所述认证方法决定部所决定的用户认证方法的认证处理的认证处理部；

在所述认证处理成功的情况下，向所述终端装置提供服务的服务提供部；

其中，所述中心装置具有，根据从所述终端装置接收到的至少包含终端 ID、或者用服务器的私钥加密终端 ID 所得到的信息的终端信息、和所述终端信息 DB，判定所述终端装置的用途的终端用途判定部，

所述中心装置的所述认证方法决定部，根据所述终端用途判定部判定的所述终端装置的用途、和在所述认证策略 DB 中登记的认证策略，决定用户认证方法。

5. 根据权利要求 4 所述的认证系统，其特征在于，

所述终端装置具有执行与所述中心装置的认证请求对应的认证处理的认证处理部，

所述中心装置具有存储与用户 ID 对应的信息的用户信息 DB，

在所述认证方法决定部决定的用户认证方法请求在所述终端装置中生成认证信息的情况下，

所述中心装置向所述终端装置发送包含随机数的认证请求，

所述终端装置的所述认证处理部生成基于所述随机数的认证信息，

所述终端装置，与该终端装置的用户信息部存储的用户信息一起，向所述中心装置发送该认证信息，

所述中心装置的所述认证处理部，根据从所述终端装置接收到的所述认证信息、所述用户信息、发送的所述随机数、和在所述用户信息 DB 中存储的所述与用户 ID 对应的信息，执行所述用户认证处理。

6. 根据权利要求 4 所述的认证系统，其特征在于，

所述终端装置具有和用户设备装置收发数据的数据收发部，

所述用户设备装置具有：

和所述终端装置收发数据的数据收发部；

保管秘密信息的密钥保管部；和

使用所述秘密信息进行加密处理的加密运算部，

所述中心装置的认证处理部，根据所述已决定的认证方法，向所述终端装置发送认证请求，

所述终端装置的认证处理部，遵照所述认证请求，向所述用户设备装置发送所述认证请求，

所述用户设备装置的所述加密运算部向所述用户设备装置发送基于所述认证请求的所述加密处理的处理结果，

所述终端装置的认证处理部向所述终端装置发送所述加密处理的处理结果，

所述中心装置的认证处理部，在所述已决定的认证方法中，执行基于所述加密处理的处理结果的处理。

7. 根据权利要求 4 所述的认证系统，其特征在于，

所述中心装置的所述认证处理部，

根据来自所述终端装置的访问请求进行所述终端认证的请求，

在请求所述终端认证时，发送服务器认证信息，

终端装置的认证处理部，

使用所述服务器认证信息进行所述中心装置的认证，

在认证了所述中心装置的情况下，对所述中心装置发送所述终端信息，

所述中心装置的所述认证处理部根据所述终端信息认证所述终端装置。

8. 根据权利要求 4 所述的认证系统，其特征在于，

请求的用户认证方法是 ID 口令方法、或者摘要认证方法、或者公开密钥认证方法。

中心装置、终端装置以及认证系统

技术领域

[0001] 本发明涉及进行用户认证、向正当的用户提供服务的系统。

背景技术

[0002] 已知基于用户、个人用终端、和服务器这三者模型的认证方法（例如特开2003-44436号（图6，段落0057～0068段），称为文献1）。另外，已知具有多个认证手段、阶段性地或者通过组合来进行认证的方法（例如特开2002-269043号（图8，段落0071～0077），称为文献2）。而且，已知根据终端的性能切换终端认证的方法（例如特开2007-305140号（图20，段落0073～0077），称为文献3）。

[0003] 作为近年来的汽车的利用形式，基于出租（lease）或者租用（rental）的租借使用、或者基于汽车共享（car-sharing）的共同使用等正在增加。在接受面向汽车的远程信息服务（Telematics）的情况下，如果汽车是个人的所有物，则只要认证作为个人所有物的车载设备（汽车导航终端）即已足够。但是，根据上述使用形式的变化，可以预想今后通过车载设备的认证不充分。即，可以预想在此时对正在驾驶汽车的个人进行认证会变得重要。

[0004] 在对个人进行认证的情况下，如果是自用车，则可以在汽车导航终端中登记个人信息在认证中使用，但是，在租用车或者汽车共享等中，无法在共有的汽车的汽车导航终端中登记个人信息，需要使用其他方法。即，考虑需要根据汽车的使用方式切换用户认证的方法。

[0005] 在文献1中揭示了基于用户、个人用终端和服务器三者的认证方法，但是不能根据个人用终端的使用状况来切换用户认证的方法。另外，在文献2中揭示了通过多种用户认证的组合，分阶段地认证用户的方法，但是无法根据终端的使用状况切换用户认证的方法。进而，在文献3中揭示了根据终端的性能切换终端认证的方法，但是无法切换经由该终端的用户认证。

发明内容

[0006] 本发明鉴于上述情况而做出，提供在认证了设备后切换用户认证的方法来利用的系统及其方法。

[0007] 具体来说，在经由终端装置进行用户认证时，在认证了终端装置后，根据其认证结果，判别终端装置的使用用途，切换实施用户认证的方法使适合其使用用途。

[0008] 即，本发明提供的终端以及用户认证系统，终端装置对中心装置进行访问请求，发送访问请求信息。接收到访问请求信息的中心装置对终端装置进行终端认证请求，发送服务器认证信息。终端装置使用所述服务器认证信息进行服务器认证，其结果，在确认是正当的用户的情况下，发送终端认证信息。接收到终端认证信息的中心装置，在终端用途判定部中，根据在所述终端信息DB中登记的终端信息、和从所述终端装置接收到的终端认证信息，判定为是正当的终端装置。其后，认证方法决定部根据终端判定结果、和在所述认证策略DB中登记的用户认证方法的决定规则，决定用户认证方法。在决定使用用户设备装置的

摘要 (digest) 认证的情况下，中心装置对终端装置发送摘要认证请求。终端装置对用户设备装置发送摘要认证请求。用户设备装置的加密运算部，使用接收到的摘要认证请求的信息、和预先在密钥保管部中保管的秘密信息进行加密运算，把作为结果的摘要认证信息向终端装置发送。终端装置向中心装置转发该摘要认证信息。中心装置的认证处理部，使用接收到的摘要认证信息、和在用户信息 DB 中登记的用户信息进行用户认证，在确认是正当的用户的情况下，服务提供部对所述终端装置提供服务。

[0009] 另外，在中心装置的用户认证方法决定部决定了使用 ID 和口令的认证的情况下，中心装置对终端装置发送 ID 口令认证请求。终端装置取得在用户信息部中登记的用户 ID 和口令。此时，也可以代替取得在终端装置的用户信息部中登记的 ID 和口令，而经由数据收发部取得在用户设备装置中登记的 ID 和口令。

[0010] 终端装置向中心装置发送所取得的 ID 和口令。中心装置的认证处理部，使用接收到的 ID 和口令、和在用户信息 DB 中登记的用户信息进行用户认证，在确认是正当的用户的情况下，服务提供部对所述终端装置提供服务。

[0011] 本发明的更具体的一种形式是中心装置为提供服务而对使用终端装置的用户进行认证的认证系统，其特征在于，终端装置具有保管该终端装置的终端信息的终端信息部、和享受中心装置提供的服务的服务享受部，中心装置具有 :存储每一终端装置的用途的终端信息 DB、把终端装置的用途和认证方法的多种组合作为认证策略来登记的认证策略 DB、根据在认证策略 DB 中登记的认证策略决定用户认证方法的认证方法决定部、执行遵照认证方法决定部所决定的用户认证方法的认证处理的认证处理部、和在认证处理成功的情况下向终端装置提供服务的服务提供部。

[0012] 而且，中心装置可以具有根据从终端装置接收到的终端信息、和终端信息 DB 来判定终端装置的用途的终端用途判定部，中心装置的认证方法决定部可以根据终端用途判定部判定的终端装置的用途、和在认证策略 DB 中登记的认证策略决定用户认证方法。

[0013] 进而，也可以是如下认证系统，其中，终端装置具有执行与中心装置的认证请求对应的认证处理的认证处理部，中心装置具有存储与用户 ID 对应的信息的用户信息 DB，在认证方法决定部所决定的用户认证方法请求生成终端装置中的认证信息的情况下，中心装置向终端装置发送包含随机数的认证请求，终端装置的认证处理部生成基于随机数的认证信息，终端装置，将其与该终端装置的用户信息部存储的用户信息一起，向中心装置发送，中心装置的认证处理部根据从终端装置接收到的认证信息、用户信息、发送的随机数、和在用户信息 DB 中存储的信息，执行用户认证处理。

[0014] 进而也可以是如下认证系统，其中，终端装置具有和用户设备装置收发数据的数据收发部，用户设备装置具有和终端装置收发数据的数据收发部、保管秘密信息的密钥保管部、使用秘密信息进行加密处理的加密运算部，中心装置的认证处理部，根据已决定的认证方法，向终端装置发送认证请求，终端装置的认证处理部遵照认证请求，向用户设备装置发送认证请求，用户设备装置的加密运算部向用户设备装置发送基于认证请求的加密处理的处理结果，终端装置的认证处理部向终端装置发送加密处理的处理结果，中心装置的认证处理部，在已决定的认证方法中执行基于加密处理的处理结果的处理。

[0015] 进而也可以是如下认证系统，其中，中心装置的认证处理部根据来自终端装置的访问请求进行终端认证的请求，在请求终端认证时，发送服务器认证信息，终端装置的认证

处理部使用服务器认证信息进行中心装置的认证，在认证了中心装置的情况下，对中心装置发送终端信息，中心装置的认证处理部根据终端信息认证终端装置。

[0016] 此外，请求的认证方法也可以是 ID 口令方法、摘要认证方法、或者公开密钥认证方法（基于 PKI(Public Key Infrastructure) 的认证方法）。

[0017] 另外，上述中心装置的特征在于，具有：收发数据的通信部、存储每一终端装置的用途的终端信息 DB、把终端装置的用途和认证方法的多种组合作为认证策略来登记的认证策略 DB、根据在认证策略 DB 中登记的认证策略决定用户认证方法的认证方法决定部、遵照认证方法决定部所决定的用户认证方法执行认证处理的认证处理部、在认证处理成功的情况下向终端装置提供服务的服务提供部。

[0018] 进而，中心装置可以具有根据从终端装置接收到的终端信息、和终端信息 DB，判定终端装置的用途的终端用途判定部，认证方法决定部可以根据终端用途判定部判定的终端装置的用途、和在认证策略 DB 中登记的认证策略，决定用户认证方法。

[0019] 另外，上述终端装置的特征在于，具有：和中心装置收发数据的通信部、和用户设备装置收发数据的数据收发部、保管该终端装置的终端信息的终端信息部、执行与中心装置的认证请求对应的认证处理的认证处理部、通过认证处理在该终端被中心装置认证的情况下享受中心装置提供的服务的服务享受部。

[0020] 进而，也可以是如下终端装置，其中，具有存储一个或者多个用户的用户信息的用户信息部，认证处理部根据中心装置的认证请求，从用户信息部取得用户信息，通信部向中心装置发送用户信息。

[0021] 进而，也可以是如下终端装置，其中，认证处理部根据中心装置的认证请求从终端信息部取得终端信息，通信部向中心装置发送终端信息。

[0022] 根据本发明，在中心对终端以及用户进行认证时，根据终端的使用形式切换用户认证的方法，能够执行更适当的认证处理。

附图说明

[0023] 图 1 是举例表示实施例的终端以及用户认证系统的结构的图。

[0024] 图 2 是举例表示实施例的终端装置的硬件结构的图。

[0025] 图 3 是举例表示实施例的用户设备装置的硬件结构的图。

[0026] 图 4 是举例表示进行实施例的认证处理时的处理流程的图。

[0027] 图 5 是举例表示实施例的终端信息 DB 的结构的图。

[0028] 图 6 是举例表示实施例的认证策略 DB 的结构的图。

[0029] 图 7 是举例表示实施例的用户信息 DB 的结构的图。

具体实施方式

[0030] 【实施例 1】

[0031] 图 1 是本实施例的终端以及用户认证系统的功能结构图。如图 1 所示，本实施例的终端以及用户认证系统，n 台（n 是 1 以上的整数）终端装置 30n 和中心装置 50 通过因特网或者移动电话网等一个或者多个网络 40 互相连接。进而，在一个终端装置 30n 上，m 台（m 是 1 以上的整数）用户设备装置 20m 通过非接触无线通信、或者车内有线网等一个或者

多个网络 60 互相连接。

[0032] 中心装置 50 经由网络 40 对终端装置 30n 进行认证，根据其认证结果决定用户认证方法，向所述终端装置 30n 通知所决定的用户认证方法。

[0033] 终端装置 30n 根据所通知的认证方法执行用户认证处理。在指定的用户认证处理是使用用户设备装置的方法的情况下，终端装置 30n 通过网络 60 向用户设备装置 20m 请求用户认证信息。终端装置 30n 通过所述网络 40 向所述中心装置 50 通知从用户设备装置 20m 取得的用户认证信息。中心装置 50 根据从所述终端装置 30n 发送的用户认证信息进行认证，如果合格（认证成功），则经由网络 40 向终端装置 30n 提供服务。如果认证失败，则经由网络 40 向终端装置 30n 发送认证失败通知。

[0034] 用户设备装置 20m 包含 :和终端装置 30n 收发数据的数据收发部 201、保管密钥或者口令等秘密信息的密钥保管部 203、以及使用所述秘密信息进行加密处理的加密运算部 202。

[0035] 终端装置 30n 包含 :通过网络 40 或者 60 和中心装置 50 收发数据的通信部 301、通过网络 60 和用户设备装置 20m 收发数据的数据收发部 302、保管终端装置 30 的终端信息的终端信息部 303、存储一个或者多个用户的用户信息的用户信息部 304、根据中心装置 50 的认证请求执行认证处理的认证处理部 305、和享受中心装置 50 提供的服务的服务享受部 306。作为终端信息部 303 保管的终端信息，例如有终端 ID。

[0036] 中心装置 50 包含 :通过网络 40 收发数据的通信部 501、存储终端信息的终端信息 DB 503、根据从终端装置 30n 接收到的终端信息和在终端信息 DB503 中登记的终端信息判定终端装置的用途的终端用途判定部 502、把终端装置的用途和认证方法的多种组合作为认证策略进行登记的认证策略 DB505、根据所述终端用途判定部 502 的判定结果和在所述认证策略 DB505 中登记的认证策略决定用户认证方法的认证方法决定部 504、根据所述认证方法决定部 504 的决定执行认证处理的多个认证处理部 506j、管理用户信息的用户信息 DB507、和提供服务的服务提供部 508。

[0037] 此外，在根据所述中心装置 50 的认证方法决定部 504 的决定所决定的认证方法是不使用用户设备装置 20m 的方法的情况下，不使用所述用户设备装置 20m 和所述终端装置 30n 的数据收发部 302。另外，在决定使用用户设备装置 20m 的方法的情况下，不使用所述终端装置 30n 的用户信息部 304。

[0038] 图 2 是中心装置 50 的硬件结构图。中心装置 50 是用总线等内部通信线 59 连接了 CPU51、主存储装置 52、辅助存储装置 54、通信装置 55、输入输出装置 56、存储介质 58 的读取装置 57 等的结构。

[0039] 尽管省略了图示，但虽然终端装置 30 在规模和性能上不同，却是与中心装置 50 同样的硬件结构。

[0040] 图 3 是用户设备装置 20m 的硬件结构图。用户设备装置 20m 是用总线等内部通信线 25 连接了 CPU22、输入输出装置 21、防篡改存储器 24、防篡改存储装置 23、通信装置 26 等的结构。

[0041] 通过把存储在各装置的辅助存储装置 54 中的处理程序加载到主存储装置 52 中并由 CPU51 执行，实现以下说明的本实施例的各处理。另外，各程序可预先存储在辅助存储装置 54 中，也可以在必要时通过其他存储介质或通信介质（网络 40 或者在网络 40 上传输的

载波或者数字信号）被加载。

[0042] 图 4 是中心装置 50 进行终端认证处理，其结果，进行使用了用户设备装置 20m 的认证处理时的处理流程图。

[0043] 首先，终端装置 30n 的服务享受部 306 对中心装置 50 进行访问请求 (S301)，发送访问请求信息 A301。接受到访问请求信息 A301 的中心装置 50 的服务提供部 508，对终端装置 30n 发送服务器认证信息 A501，进行终端认证请求 (S501)。

[0044] 终端装置 30 的认证处理部 305，使用上述服务器认证信息 A501 进行服务器的认证 (S302)。其结果，在确认了服务器的正当性的情况下，发送终端认证信息 A302。在终端认证信息 A302 中至少包含终端 ID、或者用服务器的私钥 (private-key) 等加密终端 ID 所得到的信息。接收到终端认证信息 A302 的中心装置 50 的终端用途判定部 502，根据在终端信息 DB 503 中登记的终端信息、和从终端装置 30n 接收到的终端认证信息 A302，认证是否是正当的终端装置 (S502)。在确认了终端的正当性的情况下，认证方法决定部 504 根据在终端认证信息 A302 中包含的终端 ID、和在图 5 中表示的终端信息 DB503，判定该终端的用途，根据该用途和在上述认证策略 DB 505 中登记的用户认证方法（认证策略）的决定规则，决定用户认证方法 (S503)。根据该用户认证方法的决定结果分配以下处理。首先说明决定了使用用户设备装置 20m 的摘要认证的例子。

[0045] 中心装置 50 的认证方法决定部 504 对终端装置 30 发送摘要认证请求 A503。终端装置 30 对用户设备装置 20 发送所接收到的摘要认证请求 A503。用户设备装置 20 的加密运算部 202 使用在接收到的摘要认证请求 A503 中包含的信息、和预先在密钥保管部 203 中保管的秘密信息，具体来说是与用户 ID 对应的秘密信息，进行加密运算 (S201)。例如，中心装置 50 的认证方法决定部 504 发送包含随机数的摘要认证信息 A503，加密运算部 202 把所述用户的秘密信息作为密钥，对在摘要认证信息 A503 中包含的随机数进行加密运算。

[0046] 加密运算部 202 向终端装置 30 发送作为运算结果的摘要认证信息 A201。终端装置 30 向中心装置 50 转发该摘要认证信息 A201。中心装置 50 的认证处理部 506j 使用接收到的摘要认证信息 A201、和在用户信息 DB507 中登记的用户信息（具体来说，是与用户 ID 对应的秘密信息）进行用户认证 (S506)。具体来说，例如使用与向终端装置 30 发送的相同的随机数、和与用户 ID 对应的秘密信息，调查是否得到相同的加密运算结果。

[0047] 在确认是正当的用户的情况下，服务提供部 508 对所述终端装置 30 提供服务，终端装置 30 的服务享受部 306 享受服务 (S505)。在判定为不是正当的用户的情况下 (S510)，不进行基于服务提供部 508 的服务提供，中心装置 50 的认证处理部 506j 发送认证失败通知，使其显示在终端装置 30 上。

[0048] 下面说明在所述用户认证方法决定处理 (S503) 中决定了 ID 口令认证方法的例子。

[0049] 中心装置 50 对终端装置 30n 发送 ID 口令认证请求 A502。终端装置 30n 的认证处理部 305 取得在用户信息部 304 中登记的用户 ID 和口令 (S303)。此时，也可以代替取得在终端装置 30n 的用户信息部中登记的 ID 和口令，而经由数据收发部 302 取得在用户设备装置 20m 中登记的 ID 和口令。另外，也可以使用终端装置 30n 的输入输出装置 56 使用户输入 ID 和口令。

[0050] 终端装置 30n 的通信部 301 向中心装置 50 发送认证处理部 305 取得的 ID 和口令

A303。中心装置50的认证处理部506j使用接收到的ID和口令A203、和在用户信息DB 507中登记的用户信息进行用户认证(S504)。

[0051] 在确认是正当的用户的情况下，服务提供部508对所述终端装置提供服务，终端装置30的服务享受部306享受服务(S505)。在判定为不是正当用户的情况下(S510)，不进行基于服务提供部508的服务提供，中心装置50的认证处理部发送认证失败通知，使其显示在终端装置30上。

[0052] 图5是在中心装置50的终端信息DB503中登记的终端信息的例子。与终端ID对应地登记其用途。通过在图4中从终端装置30n向中心装置50发送的终端认证信息A302中包含终端ID，中心装置50能够从图5中表示的终端信息DB 503确定该终端装置30n的用途。此外，也可以在上述终端认证信息A302中直接包含与终端装置的用途相关的信息。在这种情况下，在中心装置50的终端信息DB中不需要用途的信息。

[0053] 图6是在中心装置50的认证策略DB505中登记的认证策略的例子。与终端装置的用途对应地登记认证方法。在图4中的中心装置50的用户认证方法决定处理(S503)中，通过参照认证策略DB505能够决定对终端装置30n请求的用户认证方法。此外，在本例中，作为用途，以汽车的使用方式为例记述，但只要是能够决定认证方法的信息，则不管其种类。另外，作为认证方法举例表示了两种，但是也可以是3种以上。

[0054] 图7是在中心装置50的用户信息DB507中登记的用户信息的例子，将用户ID和秘密信息对应起来登记。秘密信息是在图4中的中心装置50的用户认证处理(S504以及S506)中，由中心装置的认证处理部506参照的信息。在本例中，秘密信息作为ID口令认证方法的口令、或者摘要认证方法的私钥来使用。根据中心装置50执行的用户认证处理的不同，需要的秘密信息不同，所以用户信息DB507也可以包含图7中表示的信息以外的信息。例如在基于公开密钥加密方法的用户认证方法的情况下，作为用户信息也可以包含用户的公开密钥证书。另外，也可以在用户认证的每一次，从终端装置30n取得未在用户信息DB507中存储的需要的秘密信息。

[0055] 图4中终端装置30进行了服务器认证处理(S302)，但是也可以设置仅可以访问特定的中心装置50这样的限制而省略服务器认证。

[0056] 另外，也可以加密中心装置50和终端装置30之间、终端装置30和用户设备装置20之间、以及中心装置50和用户设备装置20之间的通信来进行数据的收发。

[0057] 另外，中心装置50决定的用户认证方法不限于ID口令认证或者摘要认证，可以进行任意的用户认证。

[0058] 此外，本发明不限于上述实施形式，在其主旨的范围内可以进行各种变形。

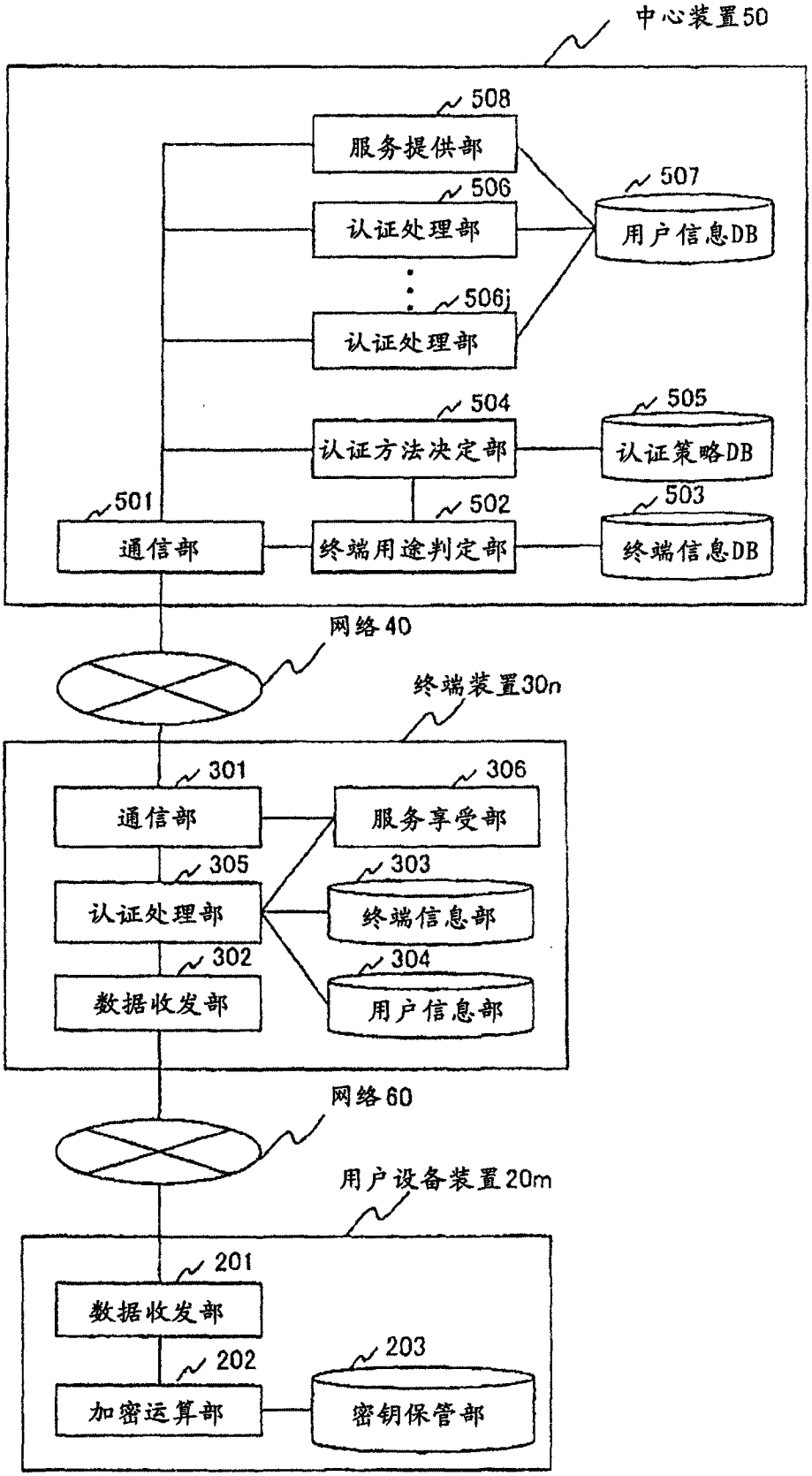

中心装置50
508
服务提供部
507
506
认证处理部
用户信息DB
506j
认证处理部
504
505
认证方法决定部
认证策略DB
501
502
503
通信部
终端用途判定部
终端信息DB
网络40
终端装置30n
301
306
通信部
服务享受部
305
303
认证处理部
终端信息部
302
304
数据收发部
用户信息部
网络60
用户设备装置20m
201
数据收发部
202
203
加密运算部
密钥保管部

图 1

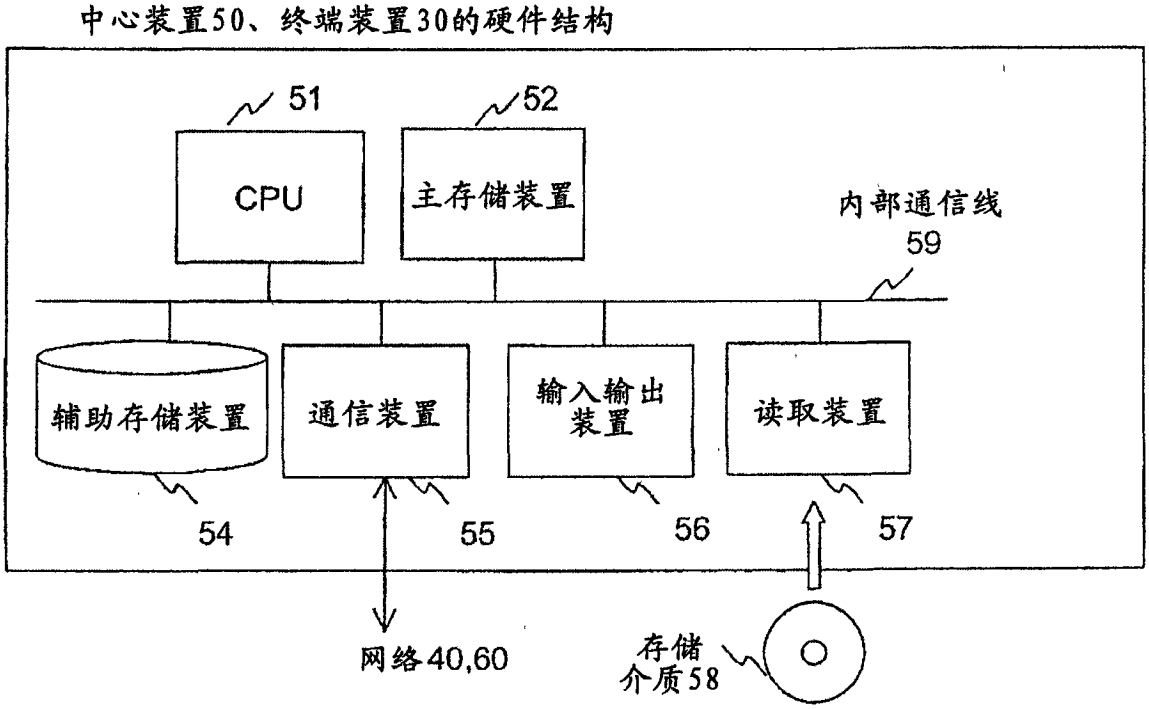

中心装置50、终端装置30的硬件结构
51
52
CPU
主存储装置
内部通信线
59
辅助存储装置
通信装置
输入输出装置
读取装置
54
55
56
57
网络40,60
存储介质58

图 2

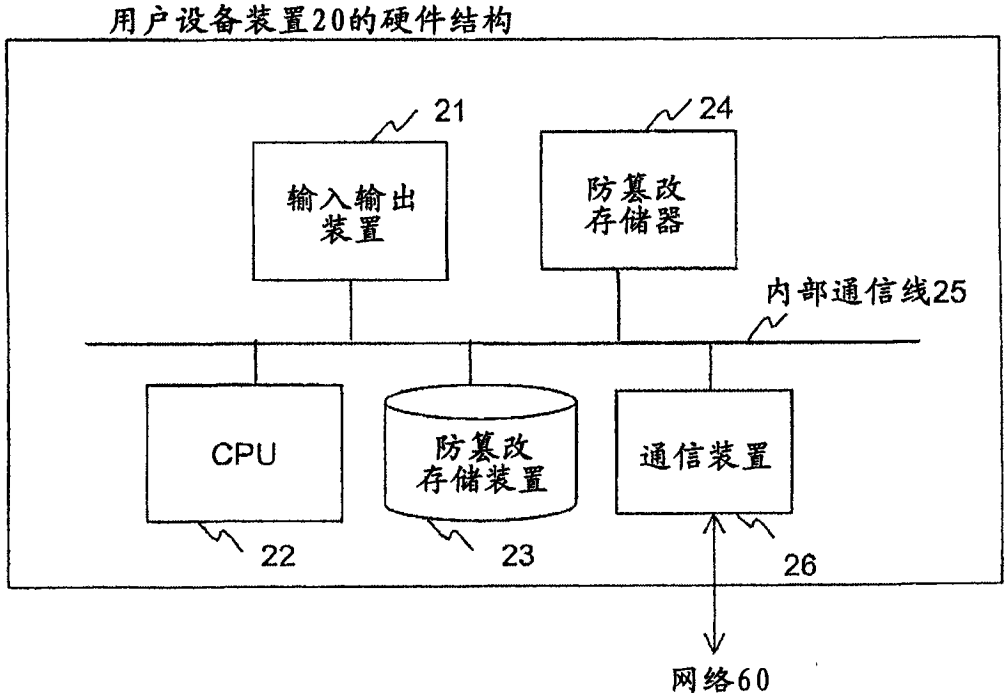

用户设备装置20的硬件结构
21
24
输入输出装置
防篡改存储器
内部通信线25
CPU
防篡改存储装置
通信装置
22
23
26
网络60

图 3

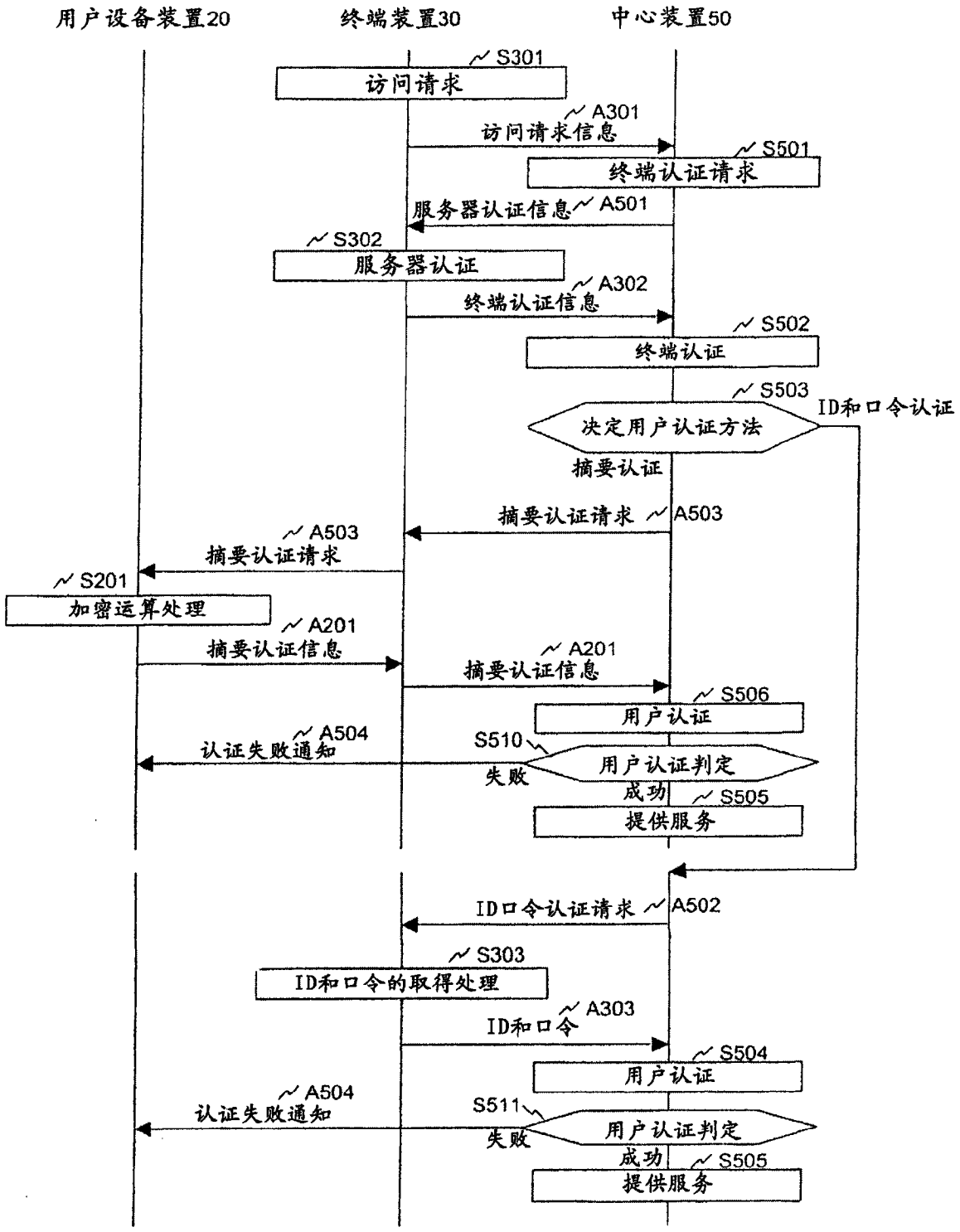

用户设备装置20
终端装置30
中心装置50
S301
访问请求
A301
访问请求信息
S501
终端认证请求
服务器认证信息
A501
S302
服务器认证
A302
终端认证信息
S502
终端认证
S503
ID和口令认证
决定用户认证方法
摘要认证
摘要认证请求
A503
A503
摘要认证请求
S201
加密运算处理
A201
摘要认证信息
A201
摘要认证信息
S506
用户认证
A504
认证失败通知
S510
用户认证判定
失败
成功
S505
提供服务
ID口令认证请求
A502
S303
ID和口令的取得处理
ID和口令
A303
S504
用户认证
A504
认证失败通知
S511
用户认证判定
失败
成功
S505
提供服务

图 4

终端信息DB 503的例子

终端ID	用途
00000001	自用
00000002	租用
…	
16467894	汽车共享使用

图 5

认证策略DB 505的例子

用途	认证方法
自用	ID和口令认证
租用	用户设备认证
汽车共享使用	用户设备认证

图 6

用户信息DB 507的例子

用户ID	秘密信息
00000000000001	2416597325315494
00000000000002	9786453154679524
…	…
45613547895123	5497685315467945

图 7