[19] 中华人民共和国国家知识产权局

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

[12] 发明专利申请公布说明书

[21] 申请号 200910112498.X

[43] 公开日 2010 年 2 月 17 日

[11] 公开号 CN 101651546A

[22] 申请日 2009.9.11

[21] 申请号 200910112498.X

[71] 申请人 福建天晴在线互动科技有限公司

地址 350001 福建省福州市马尾区星发路 8 号火炬创新大厦 206 室

[72] 发明人 曾家润 王 润 郑 晟 林 锋

[74] 专利代理机构 福州君诚知识产权代理有限公司

代理人 戴雨君

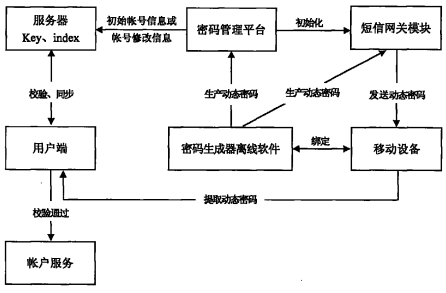
权利要求书 2 页 说明书 4 页 附图 1 页

[54] 发明名称

一种离线生成动态密码与服务器进行登陆认证和同步的方法

[57] 摘要

本发明公开了一种离线生成动态密码与服务器进行登陆认证和同步的方法，其通过密码管理平台，对动态密码的初始化信息进行申请、取得、重置、取消的相关操作，密码管理平台与服务器连接，密码生成器保存一个服务器随机生成并加密的初始随机数参数 key 和序号参数 index，每次使用时，利用两个参数生成一个新的动态密码，用户端在使用帐户时，输入其帐号或用户名称和该动态密码，与服务器端存储的同样随机数参数 key 和序号参数 index 进行计算并认证是否通过，并同步进行继续登陆或出错的反馈，其中密码生成器的离线软件安装在一个具备运行软件、存储、计算能力的安全环境的设备上，并对每个帐号名称绑定一个移动设备号码，通过短信网关模块接收验证、给绑定的移动设备号码发送短信，提供绑定凭据以及生成、并发送动态密码。



1、一种离线生成动态密码与服务器进行登陆认证和同步的方法，其通过密码管理平台，对动态密码的初始化信息进行申请、取得、重置、取消的相关操作，密码管理平台与服务器连接，密码生成器保存一个服务器随机生成并加密的初始随机数参数 key 和序号参数 index，每次使用时，利用两个参数生成一个新的动态密码，用户端在使用帐户时，输入其帐号或用户名称和该动态密码，与服务器端存储的同样随机数参数 key 和序号参数 index 进行计算并认证是否通过，并同步进行继续登陆或出错的反馈，其特征在于：密码生成器的离线软件安装在一个具备运行软件、存储、计算能力的安全环境的设备上，并对每个帐号名称绑定一个移动设备号码，通过短信网关模块接收验证、给绑定的移动设备号码发送短信，提供绑定凭据以及生成、并发送动态密码。

2、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的随机数参数 key 和序号参数 index 中，key 参数在初始化的时候服务器存档的记录与通过短信网关模块提供给用户的一致，除非重新生成，否则不会发生变化；index 参数是密码生成器每次生成动态密码时，无论是否有实际进行使用，默认每次都会做一次增量，直到与服务器同步时，才与服务器的增量同步，但不支持反向同步，即允许服务器 index 参数小于或等于服务器 index 参数，不然就判定为认证失败或过期。

3、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的通过短信网关模块向移动设备发送相关的短信，需要输入移动设备号码，或通过移动设备向服务器端提交申请，返回验证消息，在帐号信息进行绑定、取得、重置、取消等操作时，都要求对移动设备号码进行验证，并支持用动态密码对帐号信息进行解绑，无论是移动设备号码重置的操作还是取消操作，都会对服务器端的初始随机数参数 key 和序号参数 index 进行刷新。

4、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的密码生成器离线软件只提供最终生成的动态密码，不提供相关生成前的随机数参数 key 和序号参数 index，动态密码只与对应帐号存储的随机数参数 key 和序号参数 index 匹配，独立起作用或者与其他验证方法作配合。

5、根据权利要求 1 或 4 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的密码生成器离线软件除了提供基本的显示和操作，并支持配置数据的访问与存储、修改、加密。

6、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的动态密码采用验证密码、二级密码、反向验证，用过的密码不能再用。

7、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的服务器连接帐号管理平台，帐号管理平台存储和验证帐号的基本信息。

8、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的密码管理平台通过对帐号信息以及高安全级别的验证，可对动态密码、序号、激活信息进行申请绑

定、取得、重置、取消的进行操作。

9、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的移动设备具备接收短信的功能，如手机。

10、根据权利要求 1 或 9 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：如果上述的移动设备丢失，可通过移动设备的管理机构取回移动设备号码，或者是通过之前已安装的密码生成器离线软件生成动态密码，对帐号信息中的移动设备号码进行解绑。

11、根据权利要求 1 所述的一种离线生成动态密码与服务器进行登陆认证和同步的方法，其特征在于：上述的用户端在使用帐户时，输入的其帐号或用户名称和静态密码或图形验证码以及该动态密码，与服务器端存储的同样初始随机数参数和序号参数进行计算并认证是否通过。

一种离线生成动态密码与服务器进行登陆认证和同步的方法

技术领域 本发明涉及一种动态密码与服务器进行登陆认证的方法，尤其涉及通过服务器预先生成初始密码和序号，再通过客户端软件根据该密码和持续增量的序号，生成动态密码并与服务器端进行登陆认证，特别是保证服务器与客户端序号保持同步的方法。

背景技术 动态密码是一种会根据各种技术方法变化的密码，其实现方法目前有很多种。动态密码可以在使用前或使用过程中发生变化，通常在使用后会自动失效。因此，用户必须在使用时获得最新的动态密码才能进行有效的登陆。

随着网络游戏、网银、以及其他网络应用程序、网络页面的普及，用户越来越注重自身帐号的安全性，特别是如今的盗号工具和木马病毒屡禁不止，密码被盗取的问题越来越严重。很多厂商推出了密宝卡、硬件密宝、网络密宝等技术解决方案。与盗号软件、木马病毒完全绝缘，以达到保护帐号的目的。大多数密宝软件使用时，需要购买相关的硬件设备，这样除了增加额外的成本，使用时更换也麻烦，特别是目前的大多数网络应用、网络服务已慢慢向“所见即所得”、“即时体验”等高速化方向发展。如果是仅仅是远程定购的形式，即使满足了跨地域性需求，也满足不了时间同步的需求。更重要的是如果这些硬件设备一旦遗失，可能使帐号信息完全暴露在他人面前，即使没有造成损失，重新申请和费用也会给用户造成较大的不便。

通过软件实现动态密码的方法可以解决如上提到的大多数问题，但是不同类型的软件产品也略有不同。比如有的通过在移动设备上安装密码生成器软件的方法，通过互联网络获取密码。因为涉及手机必须连接互联网络的问题，除了在无网络的环境下无法使用，同其他网络软件一样，带来流量、费用、丢失、手机木马病毒等其他问题；或者采用直接与设备识别号相结合的方法，如果在手机上安装密码生成器软件，那么想换手机则没办法继续使用;还有的方法，是通过时间的方法进行算法的计算，但不一定能很好的实现同步。

发明内容 本发明的目的在于根据现有技术的不足之处，提供一种不带任何互联网络操作，可以实现快速获得高质量动态密码，还完全保证用户帐户安全性，不用担心遗失和被盗用问题的离线生成动态密码与服务器进行登陆认证和保证服务器与客户端序号保持同步的方法。

本发明是通过以下技术方案来实现的：动态密码与服务器进行登陆认证和同步的方法是通过密码管理平台，对动态密码的初始化信息进行申请、取得、重置、取消的相关操作，密码管理平台与服务器连接，密码生成器保存一个服务器随机生成并加密的初始随机数参数 key 和序号参数 index，每次使用时，利用两个参数生成一个新的动态密码，用户端在使用帐户时，输入其帐号或用户名称和该动态密码，与服务器端存储的同样随机数参数 key 和序号参数 index 进行计算并认证是否通过，并同步进行继续登陆或出错的

反馈，其中密码生成器的离线软件安装在一个具备运行软件、存储、计算能力的安全环境的设备上，并对每个帐号名称绑定一个移动设备号码，通过短信网关模块接收验证、给绑定的移动设备号码发送短信，提供绑定凭据以及生成、并发送动态密码。

上述的随机数参数 key 和序号参数 index 中，key 参数在初始化的时候服务器存档的记录与通过短信网关模块提供给用户的一致，除非重新生成，否则不会发生变化；index 参数是密码生成器每次生成动态密码时，无论是否有实际进行使用，默认每次都会做一次增量，直到与服务器同步时，才与服务器的增量同步，但不支持反向同步，即允许服务器 index 参数小于或等于服务器 index 参数，不然就判定为认证失败或过期。

上述的通过短信网关模块向移动设备发送相关的短信，需要输入移动设备号码，或通过移动设备向服务器端提交申请，返回验证消息，在帐号信息进行绑定、取得、重置、取消等操作时，都要求对移动设备号码进行验证，并支持用动态密码对帐号信息进行解绑，无论是移动设备号码重置的操作还是取消操作，都会对服务器端的初始随机数参数 key 和序号参数 index 进行刷新。

上述的密码生成器离线软件只提供最终生成的动态密码，不提供相关生成前的随机数参数 key 和序号参数 index，动态密码只与对应帐号存储的随机数参数 key 和序号参数 index 匹配，独立起作用或者与其他验证方法作配合。

上述的密码生成器离线软件除了提供基本的显示和操作，并支持配置数据的访问与存储、修改、加密。

上述的动态密码采用验证密码、二级密码、反向验证，用过的密码不能再用。

上述的服务器连接帐号管理平台，帐号管理平台存储和验证帐号的基本信息。

上述的移动设备具备接收短信的功能，如手机。

上述的密码管理平台通过对帐号信息以及高安全级别的验证，可对动态密码、序号、激活信息进行申请绑定、取得、重置、取消的进行操作。

如果上述的移动设备丢失，可通过移动设备的管理机构取回移动设备号码，或者是通过之前已安装的密码生成器离线软件生成动态密码，对帐号信息中的移动设备号码进行解绑。

上述的用户端在使用帐户时，输入的其帐号或用户名称和静态密码或图形验证码以及该动态密码，与服务器端存储的同样初始随机数参数和序号参数进行计算并认证是否通过。

本发明采用以上方法，通过生成器离线软件，利用随机数参数 key 和序号参数 index 生成一个新的动态密码，并对每个帐号名称绑定一个移动设备号码，通过短信网关模块接收验证、给绑定的移动设备号码发送短信，提供绑定凭据以及生成、并发送动态密码。这样用户端在使用帐户时，其帐号或用户名称和该动态密码，与服务器端存储的同样 key 和 index 进行计算并认证是否通过，并同步进行继续登陆或出错的反馈，登陆后即可使用帐户服务。应用该方法，即使移动设备丢失，也不会造成密码被盗取的问题，同时用过的动态密码不能再用，如此不使用实物密码、无需互联网、无需等待、不怕丢失等，具有安全性高的

优点。

附图说明 现结合附图对本发明做进一步阐述：

图 1 是本发明动态密码与服务器进行登陆认证和同步的方法的流程示意图之一；

图 2 是本发明用户登陆帐户的流程示意图。

具体实施方式 本发明通过密码管理平台，对动态密码的初始化信息进行申请、取得、重置、取消的相关操作，密码管理平台与服务器连接，密码管理平台通过对帐号信息以及高安全级别的验证，可以对动态密码、序号、激活信息进行申请绑定、取得、重置、取消的进行操作。或者服务器还可以连接帐号管理平台，帐号管理平台存储和验证帐号的基本信息。密码生成器保存一个服务器随机生成并加密的初始随机数参数 key 和序号参数 index，每次使用时，利用两个参数生成一个新的动态密码，动态密码可以采用验证密码、二级密码、反向验证等，用过的密码不能再用。随机数参数 key 和序号参数 index 中，key 参数在初始化的时候服务器存档的记录与通过短信网关模块提供给用户的一致，除非重新生成，否则不会发生变化；index 参数是密码生成器每次生成动态密码时，无论是否有实际进行使用，默认每次都会做一次增量，直到与服务器同步时，才与服务器的增量同步，但不支持反向同步，即允许服务器 index 参数小于或等于服务器 index 参数，不然就判定为认证失败或过期。

用户端在使用帐户时，输入其帐号或用户名称和上述的动态密码，还可以输入静态密码或图形验证码提高用户帐户安全性，与服务器端存储的同样随机数参数 key 和序号参数 index 进行计算并认证是否通过，并同步进行继续登陆或出错的反馈。

上述的密码生成器的离线软件除了提供基本的显示和操作，并支持配置数据的访问与存储、修改、加密，其安装在一个具备运行软件、存储、计算能力的安全环境的设备上，密码生成器离线软件只提供最终生成的动态密码，不提供相关生成前的随机数参数 key 和序号参数 index，动态密码只与对应帐号存储的随机数参数 key 和序号参数 index 匹配，独立起作用或者与其他验证方法作配合。密码生成器离线软件对每个帐号名称绑定一个移动设备号码，移动设备可以采用手机等，应具备接收短信的功能。通过短信网关模块接收验证、给绑定的移动设备号码发送短信，提供绑定凭据以及生成、并发送动态密码。通过短信网关模块向移动设备发送相关的短信，需要输入移动设备号码，或通过移动设备向服务器端提交申请，返回验证消息，在帐号信息进行绑定、取得、重置、取消等操作时，都要求对移动设备号码进行验证，并支持用动态密码对帐号信息进行解绑，无论是移动设备号码重置的操作还是取消操作，都会对服务器端的初始随机数参数 key 和序号参数 index 进行刷新。如果移动设备丢失，可通过移动设备的管理机构取回移动设备号码，或者是通过之前已安装的密码生成器离线软件生成动态密码，对帐号信息中的移动设备号码进行解绑。

请参阅图 1 所示，密码管理平台与服务器连接，将采集的初始帐号信息或帐号信息修改等相关信息传给服务器。根据用户端在使用帐户时，密码生成器离线软件只根据随机数参数 key 和序号参数 index 生产

动态密码，动态密码可以反馈给密码管理平台或者直接通过短信网关模块发送到与密码生成器离线软件绑定的移动设备上，再从移动设备上提取动态密码，输入用户端与其帐号一起提交给服务器，由服务器端存储的同样随机数参数 key 和序号参数 index 进行计算并认证是否通过，并同步进行继续登陆或出错的反馈，登陆后即可使用帐户服务。

再请参阅图 2 所示，本发明用户登陆帐户的步骤如下：先申请帐户的帐号，同时绑定一个移动设备号码（多个帐号可以绑定同一个移动设备号码），再输入帐号，由密码生成器离线软件生成动态密码，并将动态密码传送至移动设备，用户端用帐号和动态密码共同通过认证登陆，而后使用帐户服务。

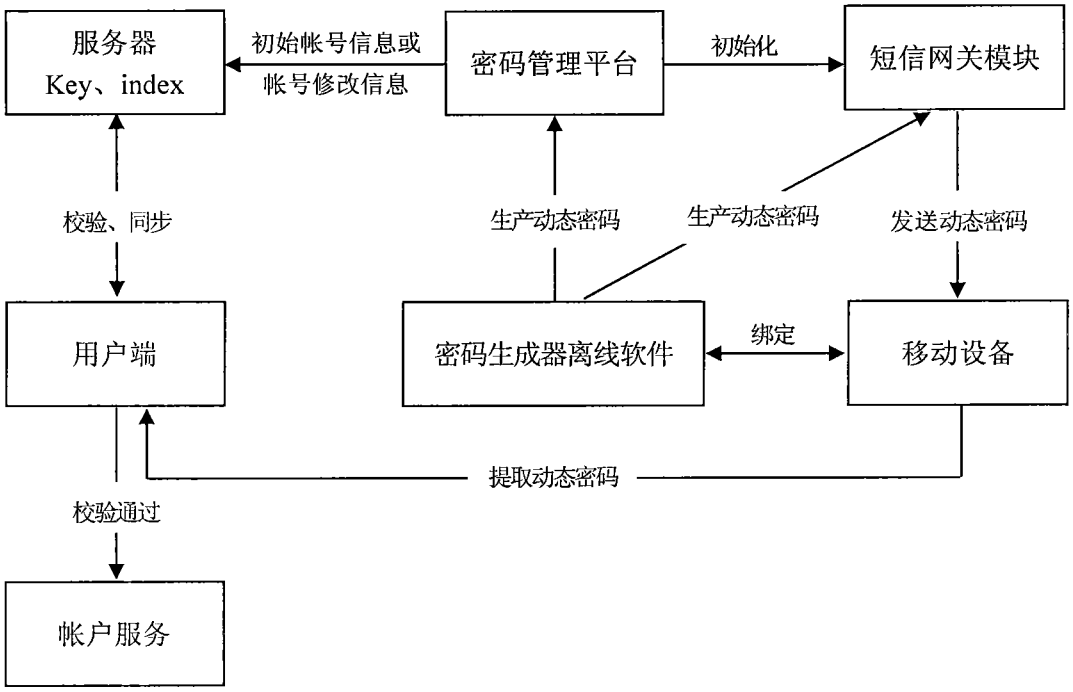

服务器
Key、index
初始帐号信息或
帐号修改信息
密码管理平台
初始化
短信网关模块
校验、同步
生产动态密码
生产动态密码
发送动态密码
用户端
密码生成器离线软件
绑定
移动设备
提取动态密码
校验通过
帐户服务

图 1

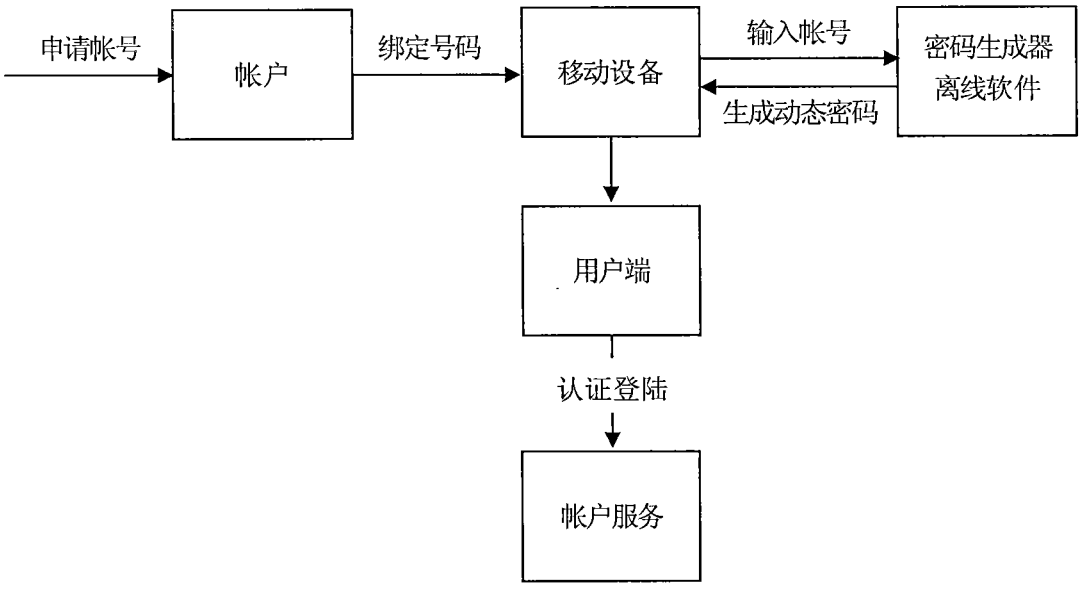

申请帐号
帐户
绑定号码
移动设备
输入帐号
生成动态密码
密码生成器
离线软件
用户端
认证登陆
帐户服务

图 2