[19] Patents Registry
The Hong Kong Special Administrative Region
香港特別行政區
專利註冊處

[11] 40037726 B
CN 111683103 B

[12] **STANDARD PATENT (R) SPECIFICATION**
轉錄標準專利說明書

[21] Application no. 申請編號
42021027155.7

[22] Date of filing 提交日期
14.03.2021

[51] Int. Cl.
H04L 9/40 (2022.01)

[54] INFORMATION INTERACTION METHOD AND DEVICE
信息交互方法及裝置

[43] Date of publication of application 申請發表日期
18.06.2021

[45] Date of publication of grant of patent 批予專利的發表日期
16.12.2022

CN Application no. & date 中國專利申請編號及日期
CN 202010690618.0 21.12.2016

CN Publication no. & date 中國專利申請發表編號及日期
CN 111683103 18.09.2020

Date of grant in designated patent office 指定專利當局批予專利日期
30.08.2022

[73] Proprietor 專利所有人
Advanced New Technologies Co., Ltd.
创新先进技术有限公司
開曼群島
大开曼岛
乔治镇医院路 27 号开曼企业中心

[72] Inventor 發明人
孙元博

[74] Agent and / or address for service 代理人及/或送達地址
博思佳知識產權代理有限公司
香港
火炭禾寮坑路 2-16 號
安盛工業大廈 6 樓 C(22)室

(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111683103 B
(45)授权公告日 2022.08.30

(21)申请号 202010690618.0
(22)申请日 2016.12.21
(65)同一申请的已公布的文献号
申请公布号 CN 111683103 A
(43)申请公布日 2020.09.18
(62)分案原申请数据
201611190037.0 2016.12.21
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心邮编KY1-9008
(72)发明人 孙元博
(74)专利代理机构 北京晋德允升知识产权代理有限公司 11623
专利代理师 王戈
(51)Int.Cl.
H04L 9/40(2022.01)
(56)对比文件
CN 104079581 A,2014.10.01
CN 103856485 A,2014.06.11
CN 104113551 A,2014.10.22
CN 104243157 A,2014.12.24
US 2013318591 A1,2013.11.28
审查员 齐雅男

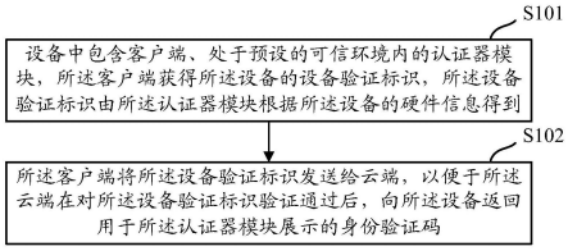
权利要求书6页 说明书15页 附图4页

(54)发明名称

信息交互方法及装置

(57)摘要

本申请实施例公开了信息交互方法及装置。设备中包含客户端、处于预设的可信环境内的认证器模块，所述方法包括：所述客户端获得所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；所述客户端将所述设备验证标识发送给云端，以便于所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。利用本申请实施例，可以提高身份验证码的安全性，降低身份验证码泄露的可能性。



CN 111683103 B

1.一种信息交互方法,设备中包含客户端、处于预设的可信环境内的认证器模块,所述方法包括:

所述客户端获得所述设备的设备验证标识,所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到;

所述客户端基于互联网络将所述设备验证标识发送给云端,所述设备验证标识用于被所述云端对所述设备验证标识进行验证,若验证通过,则表示所述设备为可信设备;

接收所述云端基于互联网络返回的身份验证码。

2.如权利要求1所述的方法,还包括:

获取所述云端对所述设备验证标识验证通过后,向所述设备返回的用于所述认证器模块展示的身份验证码。

3.如权利要求1或2所述的方法,所述客户端将所述设备验证标识发送给云端,具体包括:

所述客户端基于互联网将所述设备验证标识发送给云端。

4.如权利要求2所述的方法,所述获取所述云端对所述设备验证标识验证通过后,向所述设备返回的用于所述认证器模块展示的身份验证码,具体包括:

获取所述云端对所述设备验证标识验证通过后,基于互联网向所述设备返回的用于所述认证器模块展示的身份验证码。

5.如权利要求2所述的方法,所述云端包括消息分发服务器、所述客户端对应的服务端;

所述客户端将所述设备验证标识发送给云端,具体包括:

所述客户端将所述设备验证标识发送给所述服务端;

所述获取所述云端在对所述设备验证标识验证通过后,向所述设备返回的用于所述认证器模块展示的身份验证码,具体包括:

获取所述服务端通过调用所述消息分发服务器,使所述消息分发服务器在对所述设备验证标识验证通过后,向所述设备返回的用于所述认证器模块展示的身份验证码。

6.如权利要求5所述的方法,所述客户端获得的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的;和/或,

所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

7.如权利要求1所述的方法,所述设备验证标识由所述认证器模块根据所述设备的硬件信息和所述客户端的业务信息得到。

8.如权利要求5所述的方法,所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的,所述第一安全通道由所述设备上预定的安全服务实现;和/或,

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的,所述第二安全通道由所述设备上预定的安全服务实现。

9.如权利要求1所述的方法,所述设备包括用户终端。

10.一种信息交互方法,设备中包含客户端、处于预设的可信环境内的认证器模块,所述方法包括:

所述认证器模块接收到所述客户端的标识获取请求;

所述认证器模块向所述客户端返回所述设备的设备验证标识,所述设备验证标识由所

述认证器模块根据所述设备的硬件信息得到;所述设备验证标识用于被云端对所述设备验证标识进行验证,若验证通过,则表示所述设备为可信设备;其中,所述云端验证的所述设备验证标识是由所述客户端基于互联网络发送给所述云端的;

所述认证器模块展示所述云端在对所述设备验证标识验证通过后,基于互联网络返回的身份验证码。

11.如权利要求10所述的方法,所述云端验证的所述设备验证标识是由所述客户端基于互联网发送给所述云端的。

12.如权利要求10所述的方法,所述云端包括消息分发服务器、所述客户端对应的服务端;

所述认证器模块展示的所述身份验证码是所述消息分发服务器对所述设备验证标识验证通过后,向所述设备返回的,其中,所述消息分发服务器验证的所述设备验证标识是通过所述客户端将所述设备验证标识发送给所述服务端,以及所述服务端调用所述消息分发服务器而获得的。

13.如权利要求12所述的方法,所述认证器模块向所述客户端返回所述设备的设备验证标识,具体包括:

所述认证器模块根据所述设备的硬件信息,得到所述设备的设备验证标识;

所述认证器模块对得到的设备验证标识进行加密处理和/或签名处理;

所述认证器模块向所述客户端返回加密处理和/或签名处理过的设备验证标识。

14.如权利要求10所述的方法,所述认证器模块根据所述设备的硬件信息,得到所述设备的设备验证标识,具体包括:

所述认证器模块获得所述客户端的业务信息;

所述认证器模块根据所述设备的硬件信息和所述业务信息,得到所述设备的设备验证标识。

15.如权利要求12所述的方法,所述认证器模块展示所述云端在对所述设备验证标识验证通过后,向所述设备返回的身份验证码,具体包括:

所述认证器模块获得所述消息分发服务器在对所述设备验证标识验证通过后,向所述设备返回的身份验证码;

所述认证器模块生成可信界面,所述可信界面处于所述可信环境内;

所述认证器模块在所述可信界面中展示所述身份验证码。

16.如权利要求15所述的方法,所述认证器模块获得的所述身份验证码是所述消息分发服务器进行加密处理和/或签名处理过的;

所述认证器模块在所述可信界面中展示所述身份验证码前,所述方法还包括:

所述认证器模块对加密处理和/或签名处理过的身份验证码进行解密处理和/或签名验证处理。

17.如权利要求12所述的方法,所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的,所述第一安全通道由所述设备上预定的安全服务实现;和/或,

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的,所述第二安全通道由所述设备上预定的安全服务实现。

18.如权利要求10～17任一项所述的方法,所述设备包括用户终端。

19.一种信息交互方法，设备中包含客户端、处于预设的可信环境内的认证器模块，所述方法包括：

云端获得所述客户端基于互联网络发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

所述云端对所述设备验证标识进行验证，若验证通过，则表示所述设备为可信设备；

所述云端在对所述设备验证标识验证通过后，基于互联网络向所述设备返回用于所述认证器模块展示的身份验证码。

20.如权利要求19所述的方法，所述云端包括消息分发服务器、所述客户端对应的服务端；

云端获得所述客户端发送的所述设备的设备验证标识，具体包括：

所述服务端获得所述客户端发送的所述设备的设备验证标识；

所述云端对所述设备验证标识进行验证，具体包括：

所述服务端通过调用所述消息分发服务器，将所述设备验证标识发送给所述消息分发服务器；

所述消息分发服务器对接收到的所述设备验证标识进行验证；

所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码，具体包括：

所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

21.如权利要求20所述的方法，所述客户端发送的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；和/或，

所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

22.如权利要求20所述的方法，所述服务端通过调用消息分发服务器，将所述设备验证标识发送给所述消息分发服务器后，所述方法还包括：

所述服务端在所述消息分发服务器在对所述设备验证标识验证通过后，生成所述身份验证码；

所述服务端将所述身份验证码发送给所述消息分发服务器。

23.如权利要求20所述的方法，所述消息分发服务器接收到的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；

所述消息分发服务器对所述设备验证标识进行验证前，所述方法还包括：

所述消息分发服务器对加密处理和/或签名处理过的设备验证标识进行解密处理和/或签名验证处理。

24.如权利要求20所述的方法，所述消息分发服务器向所述设备返回用于所述认证器模块展示的身份验证码，具体包括：

所述消息分发服务器向所述服务端发送表明对所述设备验证标识验证通过的通知消息；

所述消息分发服务器接收所述服务端生成并返回的身份验证码；

所述消息分发服务器向所述设备返回所述身份验证码。

25.如权利要求20所述的方法，所述消息分发服务器向所述设备返回所述身份验证码，

具体包括：

所述消息分发服务器对所述身份验证码进行加密处理和/或签名处理；

所述消息分发服务器向所述设备返回加密处理和/或签名处理过的身份验证码。

26.如权利要求20所述的方法，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

27.如权利要求19～26任一项所述的方法，所述设备包括用户终端。

28.一种信息交互装置，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于所述客户端，包括：

获得模块，获得所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

发送模块，基于互联网络将所述设备验证标识发送给云端，所述设备验证标识用于被所述云端对所述设备验证标识验证，若验证通过，则表示所述设备为可信设备；

接收模块，接收所述云端基于互联网络返回的身份验证码。

29.如权利要求28所述的装置，所述获得模块，还用于：获取所述云端对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

30.如权利要求29所述的装置，所述云端包括消息分发服务器、所述客户端对应的服务端；

所述发送模块将所述设备验证标识发送给云端，具体包括：

所述发送模块将所述设备验证标识发送给所述服务端；

所述获取所述云端在对所述设备验证标识验证通过后，向所述设备返回的用于所述认证器模块展示的身份验证码，具体包括：

获取所述服务端通过调用所述消息分发服务器，使所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回的用于所述认证器模块展示的身份验证码。

31.如权利要求30所述的装置，所述客户端获得的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；和/或，

所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

32.如权利要求29所述的装置，所述设备验证标识由所述认证器模块根据所述设备的硬件信息和所述客户端的业务信息得到。

33.如权利要求30所述的装置，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

34.如权利要求28～33任一项所述的装置，所述设备包括用户终端。

35.一种信息交互装置，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于所述认证器模块，包括：

接收模块，接收到所述客户端的标识获取请求；

返回模块，向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认

证器模块根据所述设备的硬件信息得到;所述设备验证标识用于被云端对所述设备验证标识进行验证,若验证通过,则表示所述设备为可信设备;其中,所述云端验证的所述设备验证标识是由所述客户端基于互联网发送给所述云端的;

展示模块,展示所述云端在对所述设备验证标识验证通过后,基于互联网络返回的身份验证码。

36.如权利要求35所述的装置,所述云端包括消息分发服务器、所述客户端对应的服务端;

所述认证器模块展示的身份验证码是所述消息分发服务器对所述设备验证标识验证通过后,向所述设备返回的,其中,所述消息分发服务器验证的所述设备验证标识是通过所述客户端将所述设备验证标识发送给所述服务端,以及所述服务端调用所述消息分发服务器而获得的。

37.如权利要求35所述的装置,所述返回模块向所述客户端返回所述设备的设备验证标识,具体包括:

所述返回模块根据所述设备的硬件信息,得到所述设备的设备验证标识,对得到的设备验证标识进行加密处理和/或签名处理,向所述客户端返回加密处理和/或签名处理过的设备验证标识。

38.如权利要求35所述的装置,所述返回模块根据所述设备的硬件信息,得到所述设备的设备验证标识,具体包括:

所述返回模块获得所述客户端的业务信息,根据所述设备的硬件信息和所述业务信息,得到所述设备的设备验证标识。

39.如权利要求36所述的装置,所述展示模块展示所述云端在对所述设备验证标识验证通过后,向所述设备返回的身份验证码,具体包括:

所述展示模块获得所述消息分发服务器在对所述设备验证标识验证通过后,向所述设备返回的身份验证码,生成可信界面,所述可信界面处于所述可信环境内,在所述可信界面中展示所述身份验证码。

40.如权利要求39所述的装置,所述认证器模块获得的所述身份验证码是所述消息分发服务器进行加密处理和/或签名处理过的;

所述展示模块在所述可信界面中展示所述身份验证码前,对加密处理和/或签名处理过的身份验证码进行解密处理和/或签名验证处理。

41.如权利要求36所述的装置,所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的,所述第一安全通道由所述设备上预定的安全服务实现;和/或,

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的,所述第二安全通道由所述设备上预定的安全服务实现。

42.如权利要求35～41任一项所述的装置,所述设备包括用户终端。

43.一种信息交互装置,设备中包含客户端、处于预设的可信环境内的认证器模块,所述装置位于云端,包括:

获得模块,获得所述客户端基于互联网络发送的所述设备的设备验证标识,所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到;

验证模块,对所述设备验证标识进行验证,若验证通过,则表示所述设备为可信设备;

返回模块，在所述验证模块对所述设备验证标识验证通过后，基于互联网络向所述设备返回用于所述认证器模块展示的身份验证码。

44.如权利要求43所述的装置，所述装置包括：消息分发服务器、所述客户端对应的服务端；所述获得模块位于所述服务端，所述验证模块、所述返回模块位于所述消息分发服务器；

所述获得模块获得所述客户端发送的所述设备的设备验证标识，具体包括：

所述服务端获得所述客户端发送的所述设备的设备验证标识；

所述验证模块对所述设备验证标识进行验证，具体包括：

所述服务端通过调用所述消息分发服务器，将所述设备验证标识发送给所述消息分发服务器；

所述消息分发服务器对接收到的所述设备验证标识进行验证；

所述返回模块在所述验证模块对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码，具体包括：

所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

45.如权利要求44所述的装置，所述客户端发送的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；和/或，

所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

46.如权利要求44所述的装置，所述服务端通过调用消息分发服务器，将所述设备验证标识发送给所述消息分发服务器后，在所述消息分发服务器在对所述设备验证标识验证通过后，生成所述身份验证码，将所述身份验证码发送给所述消息分发服务器。

47.如权利要求44所述的装置，所述消息分发服务器接收到的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；

所述消息分发服务器对所述设备验证标识进行验证前，对加密处理和/或签名处理过的设备验证标识进行解密处理和/或签名验证处理。

48.如权利要求44所述的装置，所述消息分发服务器向所述设备返回所述身份验证码，具体包括：

所述消息分发服务器向所述服务端发送表明对所述设备验证标识验证通过的通知消息，接收所述服务端生成并返回的身份验证码，向所述设备返回所述身份验证码。

49.如权利要求44所述的装置，所述消息分发服务器向所述设备返回所述身份验证码，具体包括：

所述消息分发服务器对所述身份验证码进行加密处理和/或签名处理，向所述设备返回加密处理和/或签名处理过的身份验证码。

50.如权利要求44所述的装置，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

51.如权利要求43～50任一项所述的装置，所述设备包括用户终端。

信息交互方法及装置

技术领域

[0001] 本申请涉及计算机软件技术领域，尤其涉及信息交互方法及装置。

背景技术

[0002] 随着移动互联网的发展，通过手机短信下发身份验证码作为一种辅助的身份认证方式得到了广泛的应用。

[0003] 但是，不法者有针对性的一些攻击手段给身份验证码的安全带来了较大威胁，比如，短信木马、复制手机卡、伪基站、钓鱼程序等。

[0004] 例如，攻击者可以预先将短信木马种植于某用户的手机中，当该用户手机接收到短信时，短信木马自动将短信隐秘地发送给攻击者，则短信中包含的身份验证码会泄露。

[0005] 又例如，攻击者可以通过非法手段复制一张与用户的手机卡，并可以利用复制的手机卡同步接收该用户的短信，则短信中包含的身份验证码也会泄露。

[0006] 由此可知，不法者的上述攻击手段对现有技术中通过手机短信下发的身份验证码的安全带来了较大威胁，导致身份验证码容易泄露。

发明内容

[0007] 本申请实施例提供信息交互方法及装置，用以解决如下技术问题：现有技术中通过手机短信下发的身份验证码容易泄露的问题。

[0008] 为解决上述技术问题，本申请实施例是这样实现的：

[0009] 本申请实施例提供的第一种信息交互方法，设备中包含客户端、处于预设的可信环境内的认证器模块，所述方法包括：

[0010] 所述客户端获得所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0011] 所述客户端将所述设备验证标识发送给云端，以便于所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0012] 本申请实施例提供的第一种信息交互装置，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于所述客户端，包括：

[0013] 获得模块，获得所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0014] 发送模块，将所述设备验证标识发送给云端，以便于所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0015] 本申请实施例提供的第二种信息交互方法，设备中包含客户端、处于预设的可信环境内的认证器模块，所述方法包括：

[0016] 所述认证器模块接收到所述客户端的标识获取请求；

[0017] 所述认证器模块向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0018] 所述认证器模块展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，其中，所述云端验证的所述设备验证标识是由所述客户端发送给所述云端的。

[0019] 本申请实施例提供的第二种信息交互装置，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于所述认证器模块，包括：

[0020] 接收模块，接收到所述客户端的标识获取请求；

[0021] 返回模块，向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0022] 展示模块，展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，其中，所述云端验证的所述设备验证标识是由所述客户端发送给所述云端的。

[0023] 本申请实施例提供的第三种信息交互方法，设备中包含客户端、处于预设的可信环境内的认证器模块，所述方法包括：

[0024] 云端获得所述客户端发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0025] 所述云端对所述设备验证标识进行验证；

[0026] 所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0027] 本申请实施例提供的第三种信息交互装置，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于云端，包括：

[0028] 获得模块，获得所述客户端发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0029] 验证模块，对所述设备验证标识进行验证；

[0030] 返回模块，在所述验证模块对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0031] 本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：所述设备可以是诸如手机等用户终端，可以基于对根据设备的硬件信息得到的设备验证标识的验证通过，确定该设备确实为可信设备，再向设备下发身份验证码，因此可以抵御复制手机卡、伪基站等攻击，不仅如此，由于设备验证标识的生成以及后续身份验证码的展示都是在设备中的可信环境内进行的，因此可以抵御短信木马、钓鱼程序等攻击。综上所述，本申请的方案可以提高身份验证码的安全性，降低身份验证码泄露的可能性，可以部分或全部地解决现有技术中的问题。

附图说明

[0032] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0033] 图1为本申请实施例提供的第一种信息交互方法的流程示意图；

[0034] 图2为本申请实施例提供的第二种信息交互方法的流程示意图；

[0035] 图3为本申请实施例提供的第三种信息交互方法的流程示意图；

[0036] 图4为本申请实施例提供的一种实际应用场景下，上述信息交互方法的一种业务架构示意图；

[0037] 图5为本申请实施例提供的一种实际应用场景下，上述信息交互方法的一种技术架构示意图；

[0038] 图6为本申请实施例提供的一种实际应用场景下，上述信息交互方法的一种交互流程示意图；

[0039] 图7为本申请实施例提供的对应于图1的一种信息交互装置的结构示意图；

[0040] 图8为本申请实施例提供的对应于图2的一种信息交互装置的结构示意图；

[0041] 图9为本申请实施例提供的对应于图3的一种信息交互装置的结构示意图。

具体实施方式

[0042] 本申请实施例提供信息交互方法及装置。

[0043] 为了使本技术领域的人员更好地理解本申请中的技术方案，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本申请保护的范围。

[0044] 本申请的方案的具体实施可以涉及客户端、认证器模块、云端的动作，云端具体可以只包括一端(比如，消息分发服务器)，也可以包括至少两端(比如，消息分发服务器、该客户端对应的服务端等)。

[0045] 客户端、认证器模块可以处于同一设备。客户端、认证器模块所处设备一般是手机、平板电脑、智能可穿戴设备、车机等用户终端。

[0046] 服务端、消息分发服务器可以处于不同设备，也可以处于同一设备。服务端、消息分发服务器所处设备一般是用作服务器的计算机、计算机集群等。

[0047] 如无特殊说明，以下提到的“设备”均是指客户端与认证器模块所处设备。

[0048] 本申请实施例提供了一共三种信息交互方法及装置，这三种信息交互方法及装置基于同一发明思路并相互对应，是分别以客户端、认证器模块、云端中的每一端作为执行主体进行描述的，通过上述任一种信息交互方法或装置可以实现身份验证码的获取、下发及展示，可以提高身份验证码的安全性，降低身份验证码泄露的可能性。

[0049] 下面对本申请的方案进行详细说明。

[0050] 图1为本申请实施例提供的第一种信息交互方法的流程示意图，下述设备中包含客户端、处于预设的可信环境(Trusted Execution Environment，TEE)内的认证器模块。图1中的流程可以是在需要获取身份验证码时，按照指定方式触发执行的。比如，在客户端的业务第一次在设备上使用，需激活设备时，或者，用户以同一账号在移动设备的客户端与非移动设备的对应客户端上切换操作时，等等。

[0051] 在本申请实施例中，可信环境是依托其所在设备的硬件的，其通常可以基于微内核的操作系统提供可信服务，可以有多种具体实现方式，本申请并不做限定。列举其中三种实现方式作为示例：

[0052] 第一种，利用intel TXT或AMD的SVM均可提供可信环境，即基于处理器CPU的特殊

指令,提供动态信任根DRTM服务,实现可信环境;

[0053] 第二种,利用ARM TrustZone或TI M-Shield机制,直接在中央处理器硬件上提供的安全区域/非安全区域隔离机制,实现可信环境;

[0054] 第三种,利用hypervisor/VMM虚拟化机制,提供安全应用/非安全应用之间的隔离,实现可信环境。

[0055] 对图1中的信息交互方法的说明也适用于本申请实施例提供的另几种信息交互方法,后面不再赘述。

[0056] 图1中的流程的执行主体为客户端,该流程可以包括以下步骤:

[0057] S101:所述客户端获得所述设备的设备验证标识,所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到。

[0058] 在本申请实施例中,客户端可以是用户终端上任意需要使用身份验证码的客户端,比如,第三方支付应用的客户端、即时通讯应用的客户端、电子银行应用的客户端等。

[0059] 在本申请实施例中,可以根据设备的硬件信息将该设备与其他设备进行区分。以手机为例,硬件信息可以是国际移动设备身份码(International Mobile Equipment Identity,IMEI)、物理地址等。

[0060] 一般地,设备验证标识可以在一定的范围(比如,网络范围、设备范围、地域范围等)唯一标识其对应的设备,范围具体多大本申请不做限定,取决于具体实施情况。比如,若在某个国家内实施本申请的方案,则对于该国家内的设备,其设备验证标识只要在该国家内具有唯一性即可。

[0061] 在本申请实施例中,设备验证标识可以是认证器模块通过对设备的硬件信息进行一定的逻辑运算生成的,所述逻辑运算可以有多种具体实施方法,本申请并不作限定,列举一种作为示例。

[0062] 例如,可以通过执行base64(Hash(HardID+random))生成设备验证标识,其中,base64为一种密码算法,Hash表示哈希函数,HardID表示所使用的硬件信息,random表示随机数。由于生成过程是在设备的可信环境内进行的,因此,这种方式有利于提高设备验证标识的安全性,而且也有利于防止硬件信息泄露。

[0063] 当然,认证器模块也可以将设备的硬件信息直接作为设备验证标识。

[0064] 在本申请实施例中,客户端可以是通过直接或间接地向认证器模块发送标识获取请求,而获得认证器模块返回的设备验证标识。

[0065] S102:所述客户端将所述设备验证标识发送给云端,以便于所述云端在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码。

[0066] 在本申请实施例中,云端通过对设备验证标识进行验证,可以确定客户端所处设备是否为客户端所提供业务的可信设备,若是,则验证通过。

[0067] 在本申请实施例中,云端与设备是通过互联网(IP网络)进行交互的。

[0068] 在本申请实施例中,身份验证码的形式可以有多种。列举几种作为示例,比如,身份验证码可以是一串数字(6位数字、4位数字等等),一串字符等(比如,中文字符、英文字符或者其他语言的字符),一个任务(比如,将九宫格中的第1个字符和和最后一个字符交换顺序,将第2个字符和第5个字符交换顺序,将第3个字符和第8个字符用直线连接;九宫格是需要用户进行身份验证时展示在界面上,用户接到上述所述任务时,按照任务内容执行便可

通过身份验证)，等等。

[0069] 通过图1的方法，所述设备可以是诸如手机等用户终端，可以基于对根据设备的硬件信息得到的设备验证标识的验证通过，确定该设备确实为可信设备，再向设备下发身份验证码，因此可以抵御复制手机卡、伪基站等攻击，不仅如此，由于设备验证标识的生成以及后续身份验证码的展示都是在设备中的可信环境内进行的，因此可以抵御短信木马、钓鱼程序等攻击。综上所述，本申请的方案可以提高身份验证码的安全性，降低身份验证码泄露的可能性，可以部分或全部地解决现有技术中的问题。

[0070] 基于图1的方法，本申请实施例还提供了该方法的一些具体实施方案，以及扩展方案，下面进行说明。

[0071] 在本申请实施例中，如前所述，云端可以包括两端，消息分发服务器、该客户端对应的服务端。以下实施例主要基于这种情况进行说明。

[0072] 在这种情况下，对于步骤S102，所述云端包括消息分发服务器、所述客户端对应的服务端；

[0073] 所述客户端将所述设备验证标识发送给云端，具体可以包括：所述客户端将所述设备验证标识发送给所述服务端；

[0074] 所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码，具体可以包括：所述服务端通过调用所述消息分发服务器，使所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0075] 在本申请实施例中，所述服务端是客户端对应的服务端，比如，支付应用的客户端对应的服务端即为该支付应用的服务端。

[0076] 消息分发服务器可以是一个公用平台，在这种情况下，多个不同的服务端可以调用同一个消息分发服务器。当然，不同的服务端也可以有自己独享的消息分发服务器。需要说明的是，消息分发服务器并非移动运营商的短信服务器，因此，本申请的方案可以不像现有技术那样依赖于短信来发送和接收身份验证码，而是可以基于互联网传递身份验证码。

[0077] 在本申请实施例中，服务端通过调用消息分发服务器，可以将接收到的客户端发送的设备验证标识发送给消息分发服务器，以请求消息分发服务器对设备验证标识进行验证。消息分发服务器通过对设备验证标识验证，可以确定客户端所处设备是否为可信设备，若是，则验证通过。

[0078] 具体地，可以按照指定方式(比如，出厂预设、用户实名认证等、将该设备与另一可信设备进行绑定等)，预先将设备的设备验证标识在消息分发服务器注册，注册过的设备为可信设备。在这种情况下，消息分发服务器可以通过将步骤S102中的设备验证标识与注册的设备验证标识进行比较，对S102中的设备验证标识进行验证。

[0079] 例如，对于出厂预设的方式，无需用户干预，可以由厂家注册设备验证标识，以确定设备的硬件本身是可信的。这种方式主要强调“硬件层面上可信”。

[0080] 又例如，对于用户实名认证方式，可以由用户预先针对任意客户端的业务，通过与对应的服务端以及消息分发服务器进行交互，注册用户的实名等相关身份信息(比如，身份证号码等)和设备验证标识，以确定设备对于该业务和该用户而言是可信的。这种方式主要强调“业务层面上可信”。

[0081] 在本申请实施例中，身份验证码可以由服务端和/或消息分发服务器生成。一般地，身份验证码是与客户端或服务端的业务相关的(比如，进行该业务所需基于该身份验证码进行认证，或者，该身份验证码需要基于该业务相关信息生成，等等)，在这种情况下，身份验证码优选地可以由服务端生成，如此有利于减少消息分发服务器对该业务的干涉。

[0082] 在本申请实施例中，对于步骤S101，所述客户端获得的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的，进行加密处理的目的是可以防止设备验证标识被明文传输，降低泄露风险，进行签名处理的目的是防止设备验证标识被非法篡改。在这种情况下，消息分发服务器后续需要相应地进行解密处理和/或签名验证处理后，才能对设备验证标识进行验证，解密处理和/或签名验证所需的密钥可以由设备与消息分发服务器预先协商。

[0083] 类似地，所述消息分发服务器返回的所述身份验证码也可以是进行加密处理和/或签名处理过的。

[0084] 在本申请实施例中，设备验证标识还可以由认证器模块根据设备的硬件信息和客户端的业务信息得到，不同的客户端还可以预先指定不同的逻辑运算算法，以用于生成设备验证标识。如此，可以实现不同客户端的设备验证标识差异化，而且设备验证标识还可以随着同一个客户端业务信息的变化而变化，有利于提高设备验证标识的安全性。

[0085] 在本申请实施例中，对于以上信息交互流程，所述客户端与所述认证器模块之间的交互，和/或所述消息分发服务器与所述设备(包括但不限于认证器模块)之间的交互可以是基于所述设备上预定的安全服务所实现的安全通道进行的，比如，消息分发服务器与所述设备之间的交互基于第一安全通道进行，所述客户端与所述认证器模块之间的交互基于第二安全通道进行，等等。

[0086] 原因在于，虽然认证器模块处于可信环境中，但是客户端、消息分发服务器未必处于可信环境中，所述安全服务以其实现的安全通道有利于降低这几端之间的交互风险。

[0087] 所述安全服务可以由独立于上述几端的功能模块提供，也可以由上述几端自身提供，所述安全服务可以包括但不限于连接管理、访问控制、会话协商、连接心跳维护、安全隧道、密码控制等。

[0088] 需要说明的是，上述的安全通道可以是针对开放式系统互联(Open System Interconnection，OSI)模型中的某一层或多层实现的，不同层对应的安全通道具体实现方式不同。比如，对于应用层，可以基于加密和/或签名实现安全通道；对于传输层，可以基于TLS实现安全通道；对于网络层，可以基于IPSec实现安全通道；对于链路层，可以基于L2TP实现安全通道；等等。

[0089] 图2为本申请实施例提供的第二种信息交互方法的流程示意图。图2中的流程的执行主体为认证器模块，该流程可以包括以下步骤：

[0090] S201：所述认证器模块接收到所述客户端的标识获取请求。

[0091] S202：所述认证器模块向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到。

[0092] S203：所述认证器模块展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，其中，所述云端验证的所述设备验证标识是由所述客户端发送给所述云端的。

[0093] 由于图2与图1的方法是对应的，因此，图2的方法也具有图1的方法的技术效果，基于图2的方法，本申请实施例还提供了该方法的一些具体实施方案，以及扩展方案，对于在上面已经说明过的部分，下面不再赘述或只进行简单说明。后面的几种信息交互方法也是如此，不再赘述。

[0094] 在本申请实施例中，所述云端可以包括消息分发服务器、所述客户端对应的服务端；

[0095] 所述认证器模块展示的所述身份验证码是所述消息分发服务器对所述设备验证标识验证通过后，向所述设备返回的，其中，所述消息分发服务器验证的所述设备验证标识是通过所述客户端将所述设备验证标识发送给所述服务端，以及所述服务端调用所述消息分发服务器而获得的。

[0096] 在本申请实施例中，对于步骤S202，所述认证器模块向所述客户端返回所述设备的设备验证标识，具体可以包括：所述认证器模块根据所述设备的硬件信息，得到所述设备的设备验证标识；所述认证器模块对得到的设备验证标识进行加密处理和/或签名处理；所述认证器模块向所述客户端返回加密处理和/或签名处理过的设备验证标识，以便所述客户端将加密处理和/或签名处理过的设备验证标识发送给所述服务端。

[0097] 进一步地，所述认证器模块根据所述设备的硬件信息，得到所述设备的设备验证标识，具体可以包括：所述认证器模块获得所述客户端的业务信息；所述认证器模块根据所述设备的硬件信息和所述业务信息，得到所述设备的设备验证标识。

[0098] 在本申请实施例中，所述认证器模块展示消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，具体可以包括：所述认证器模块获得所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回的身份验证码；所述认证器模块生成可信界面，所述可信界面处于所述可信环境内；所述认证器模块在所述可信界面中展示所述身份验证码。

[0099] 在可信界面展示的条件下，由于可信环境的隔离性和安全特性可以不允许其他进程运行，或者只允许指定进程运行，因此可以防止短信木马、钓鱼程序等恶意程序窃取在可信界面中展示的消息。

[0100] 在本申请实施例中，所述认证器模块获得的所述身份验证码可以是所述消息分发服务器进行加密处理和/或签名处理过的；类似地，所述认证器模块在所述可信界面中展示所述身份验证码前，还可以执行：所述认证器模块对加密处理和/或签名处理过的身份验证码进行解密处理和/或签名验证处理。

[0101] 在本申请实施例中，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

[0102] 在本申请实施例中，所述设备可以包括用户终端。

[0103] 图3为本申请实施例提供的第三种信息交互方法的流程示意图。图3中的流程的执行主体为云端，该流程可以包括以下步骤：

[0104] S301：云端获得所述客户端发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到。

[0105] S302:所述云端对所述设备验证标识进行验证。

[0106] S303:所述云端在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码。

[0107] 在本申请实施例中,所述云端可以包括消息分发服务器、所述客户端对应的服务端;在这种情况下,对于步骤S301,云端获得所述客户端发送的所述设备的设备验证标识,具体可以包括:所述服务端获得所述客户端发送的所述设备的设备验证标识;

[0108] 对于步骤S302,所述云端对所述设备验证标识进行验证,具体可以包括:所述服务端通过调用消息分发服务器,将所述设备验证标识发送给所述消息分发服务器,所述消息分发服务器对接收到的所述设备验证标识进行验证;

[0109] 对于步骤S303,所述云端在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码,具体可以包括:所述消息分发服务器在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码。

[0110] 在本申请实施例中,所述客户端发送的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的;和/或,所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

[0111] 在本申请实施例中,前面已经提到,消息优选地可以由服务端生成。在这种情况下,所述将所述设备验证标识发送给所述消息分发服务器后,还可以执行:所述服务端在所述消息分发服务器在对所述设备验证标识验证通过后,生成所述身份验证码;所述服务端将所述身份验证码发送给所述消息分发服务器,以便于所述消息分发服务器向所述设备返回所述身份验证码。

[0112] 在本申请实施例中,所述消息分发服务器接收到的所述设备验证标识可以是所述认证器模块进行加密处理和/或签名处理过的;在这种情况下,所述消息分发服务器对所述设备验证标识进行验证前,还可以执行:所述消息分发服务器对加密处理和/或签名处理过的设备验证标识进行解密处理和/或签名验证处理。

[0113] 在本申请实施例中,所述消息分发服务器向所述设备返回用于所述认证器模块展示的身份验证码,具体可以包括:所述消息分发服务器向所述服务端发送表明对所述设备验证标识验证通过的通知消息;所述消息分发服务器接收所述服务端生成并返回的身份验证码;所述消息分发服务器向所述设备返回所述身份验证码,以用于所述认证器模块展示。

[0114] 在本申请实施例中,所述消息分发服务器向所述设备返回所述身份验证码,具体可以包括:所述消息分发服务器对所述身份验证码进行加密处理和/或签名处理;所述消息分发服务器向所述设备返回加密处理和/或签名处理过的身份验证码,以用于所述认证器模块进行解密处理和/或签名验证处理后展示。

[0115] 在本申请实施例中,所述消息分发服务器与所述设备之间的交互可以是基于第一安全通道进行的,所述第一安全通道由所述设备上预定的安全服务实现;和/或,所述客户端与所述认证器模块之间的交互可以是基于第二安全通道进行的,所述第二安全通道由所述设备上预定的安全服务实现。

[0116] 在本申请实施例中,所述设备可以包括用户终端。

[0117] 上面分别以各端为执行主体对本申请实施例提供的信息交互方法进行了说明。为了便于理解,本申请实施例还提供了一种实际应用场景下,上述信息交互方法的一种具体

实施方案，下面结合图4、图5、图6进行说明。

[0118] 图4为本申请实施例提供的一种实际应用场景下，上述信息交互方法的一种业务架构示意图。

[0119] 在图4中，“可信界面+设备认证标识”是客户端所处设备中涉及本申请的方案的关键部分之一，安全通道可以是基于上述的安全服务所实现的。每个服务提供商分别有其对应于服务端与对应的客户端，各服务提供商可以通过消息分发服务器向客户端下发诸如身份验证码等消息，前提是消息分发服务器对客户端所处设备的设备认证标识验证通过。其中，图4中三方之间的交互都是基于互联网的，无需依赖移动运营商的网络以及短信平台，有利于灵活地使用各种安全策略以提高业务架构的安全性，而且，业务架构中的可信界面相比于现有技术中的短信界面也更加安全。

[0120] 图5为本申请实施例提供的一种实际应用场景下，上述信息交互方法的一种技术架构示意图。

[0121] 在图5中，对于客户端所在设备，主要可以实现以下功能(可以对应于相应的功能模块)。

[0122] 连接管理：负责网络socket连接的创建、管理和维护；

[0123] 会话协商：基于socket连接建立时和消息分发服务器协商，获取本次会话的密钥；

[0124] 心跳维护：保持长连接(比如，安全服务与消息分发服务器之间可以建立的长连接)的维护；

[0125] 可信界面：安全界面，根据后台运营中心的要求绘制界面，可以是六位密码展示界面也可以是其他的；

[0126] 协议组装：根据业务要求组装数据并安全加解密及签名，网络层的包组装；

[0127] 协议解析：网路层的包解析及业务数据包的解析；

[0128] 设备数据采集：采集：客户端所在设备的可信数据；

[0129] 设备密钥：客户端所在设备出厂的时候内置，提供签名接口；

[0130] 设备ID：设备模块以硬件ID为基础生成业务的唯一ID(比如，上述的设备验证标识)并返回；

[0131] 加解密：密钥算法模块。

[0132] 在图5中，对于云端示出了消息分发服务器，消息分发服务器主要可以实现以下功能(可以对应于相应的功能模块)。

[0133] 连接管理：负责消息分发服务器连接的管理和维护；

[0134] 会话协商：根据与客户端所在设备的协商生成和管理会话密钥，同时保证会话和连接的维护；

[0135] 心跳维护：保证长连接；

[0136] 协议组装：组装网络层的数据包并封装业务；

[0137] 协议解析：组装网络层的数据包并解析业务；

[0138] 设备ID管理：设备ID的查询，废弃及增加；

[0139] 设备密钥管理：设备密钥的查询，废弃及增加；

[0140] 设备风险管理：根据设备采集的数据形成设备风险管理；

[0141] 访问控制：对服务端调用的访问控制。

[0142] 模板中心:形成消息内容及展示方式

[0143] 运营中心:对消息的管理及运营。

[0144] 图6为本申请实施例提供的一种实际应用场景下,上述信息交互方法的一种交互流程示意图。

[0145] 在图6中,非可信环境与可信环境处于设备上,安全服务由一个指定的功能模块实现,认证器模块处于可信环境中,认证器模块至少包含“可信逻辑处理”和“可信界面展示”两个子模块。安全服务与消息分发服务器通过心跳保持长连接。

[0146] 客户端所提供的业务第一次在设备上使用时,通过激活设备的操作触发后续流程的执行。客户端通过安全服务获得设备验证标识,其中,设备验证标识是由可信逻辑处理模块根据设备的硬件信息通过执行“执行base64(Hash(HardID+random))”生成,并采用设备的私钥签名后通过安全服务返回给客户端的。

[0147] 客户端将获得的签名过的设备验证标识发送给服务端请求验证,服务端调用消息分发服务器,以请求消息分发服务器对从客户端收到的签名过的设备验证标识进行验证。

[0148] 消息分发服务器利用预先获得的设备的数据(比如,公钥、硬件信息、设备验证标识等)验证当前得到的设备验证标识的签名是否合法,以及确定设备是否为可信设备。

[0149] 消息分发服务器对设备验证标识验证通过后,下发签名过的消息到安全服务,安全服务透传该消息到可信逻辑处理模块。

[0150] 可信逻辑处理模块验证该消息的签名,确保该消息可信,验证通过后,调用可信界面展示模块生成可信界面以展示该消息。

[0151] 上面对本申请实施例提供的信息交互方法进行了说明,基于同样的发明思路,本申请实施例还提供了对应的装置,如图7、图8、图9所示。

[0152] 图7为本申请实施例提供的对应于图1的一种信息交互装置的结构示意图,设备中包含客户端、处于预设的可信环境内的认证器模块,所述装置位于所述客户端,包括:

[0153] 获得模块701,获得所述设备的设备验证标识,所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到;

[0154] 发送模块702,将所述设备验证标识发送给云端,以便于所述云端在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码。

[0155] 可选地,所述云端包括消息分发服务器、所述客户端对应的服务端;

[0156] 所述发送模块702将所述设备验证标识发送给云端,具体包括:

[0157] 所述发送模块702将所述设备验证标识发送给所述服务端;

[0158] 所述云端在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码,具体包括:

[0159] 所述服务端通过调用所述消息分发服务器,使所述消息分发服务器在对所述设备验证标识验证通过后,向所述设备返回用于所述认证器模块展示的身份验证码。

[0160] 可选地,所述客户端获得的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的;和/或,

[0161] 所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

[0162] 可选地,所述设备验证标识由所述认证器模块根据所述设备的硬件信息和所述客

户端的业务信息得到。

[0163] 可选地，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

[0164] 所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

[0165] 可选地，所述设备包括用户终端。

[0166] 图8为本申请实施例提供的对应于图2的一种信息交互装置的结构示意图，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于所述认证器模块，包括：

[0167] 接收模块801，接收到所述客户端的标识获取请求；

[0168] 返回模块802，向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0169] 展示模块803，展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，其中，所述云端验证的所述设备验证标识是由所述客户端发送给所述云端的。

[0170] 可选地，所述云端包括消息分发服务器、所述客户端对应的服务端；

[0171] 所述认证器模块展示的所述身份验证码是所述消息分发服务器对所述设备验证标识验证通过后，向所述设备返回的，其中，所述消息分发服务器验证的所述设备验证标识是通过所述客户端将所述设备验证标识发送给所述服务端，以及所述服务端调用所述消息分发服务器而获得的。

[0172] 可选地，所述返回模块802向所述客户端返回所述设备的设备验证标识，具体包括：

[0173] 所述返回模块802根据所述设备的硬件信息，得到所述设备的设备验证标识，对得到的设备验证标识进行加密处理和/或签名处理，向所述客户端返回加密处理和/或签名处理过的设备验证标识，以便所述客户端将加密处理和/或签名处理过的设备验证标识发送给所述服务端。

[0174] 可选地，所述返回模块802根据所述设备的硬件信息，得到所述设备的设备验证标识，具体包括：

[0175] 所述返回模块802获得所述客户端的业务信息，根据所述设备的硬件信息和所述业务信息，得到所述设备的设备验证标识。

[0176] 可选地，所述展示模块803展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，具体包括：

[0177] 所述展示模块803获得所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，生成可信界面，所述可信界面处于所述可信环境内，在所述可信界面中展示所述身份验证码。

[0178] 可选地，所述认证器模块获得的所述身份验证码是所述消息分发服务器进行加密处理和/或签名处理过的；

[0179] 所述展示模块803在所述可信界面中展示所述身份验证码前，对加密处理和/或签名处理过的身份验证码进行解密处理和/或签名验证处理。

[0180] 可选地，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

[0181] 所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

[0182] 可选地，所述设备包括用户终端。

[0183] 图9为本申请实施例提供的对应于图3的一种信息交互装置的结构示意图，设备中包含客户端、处于预设的可信环境内的认证器模块，所述装置位于云端，包括：

[0184] 获得模块901，获得所述客户端发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到；

[0185] 验证模块902，对所述设备验证标识进行验证；

[0186] 返回模块903，在所述验证模块902对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0187] 可选地，所述装置包括：消息分发服务器、所述客户端对应的服务端；所述获得模块901位于所述服务端，所述验证模块902、所述返回模块903位于所述消息分发服务器；

[0188] 所述获得模块901获得所述客户端发送的所述设备的设备验证标识，具体包括：

[0189] 所述服务端获得所述客户端发送的所述设备的设备验证标识；

[0190] 所述验证模块902对所述设备验证标识进行验证，具体包括：

[0191] 所述服务端通过调用所述消息分发服务器，将所述设备验证标识发送给所述消息分发服务器；

[0192] 所述消息分发服务器对接收到的所述设备验证标识进行验证；

[0193] 所述返回模块903在所述验证模块902对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码，具体包括：

[0194] 所述消息分发服务器在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码。

[0195] 可选地，所述客户端发送的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；和/或，

[0196] 所述消息分发服务器返回的所述身份验证码是进行加密处理和/或签名处理过的。

[0197] 可选地，所述服务端通过调用消息分发服务器，将所述设备验证标识发送给所述消息分发服务器后，在所述消息分发服务器在对所述设备验证标识验证通过后，生成所述身份验证码，将所述消息发送给所述消息分发服务器，以便于所述消息分发服务器向所述设备返回所述身份验证码。

[0198] 可选地，所述消息分发服务器接收到的所述设备验证标识是所述认证器模块进行加密处理和/或签名处理过的；

[0199] 所述消息分发服务器对所述设备验证标识进行验证前，对加密处理和/或签名处理过的设备验证标识进行解密处理和/或签名验证处理。

[0200] 可选地，所述消息分发服务器向所述设备返回所述身份验证码，具体包括：

[0201] 所述消息分发服务器向所述服务端发送表明对所述设备验证标识验证通过的通知消息，接收所述服务端生成并返回的身份验证码，向所述设备返回所述身份验证码，以用于所述认证器模块展示。

[0202] 可选地，所述消息分发服务器向所述设备返回所述身份验证码，具体包括：

[0203] 所述消息分发服务器对所述身份验证码进行加密处理和/或签名处理，向所述设备返回加密处理和/或签名处理过的身份验证码，以用于所述认证器模块进行解密处理和/或签名验证处理后展示。

[0204] 可选地，所述消息分发服务器与所述设备之间的交互是基于第一安全通道进行的，所述第一安全通道由所述设备上预定的安全服务实现；和/或，

[0205] 所述客户端与所述认证器模块之间的交互是基于第二安全通道进行的，所述第二安全通道由所述设备上预定的安全服务实现。

[0206] 可选地，所述设备包括用户终端。

[0207] 本申请实施例提供的装置与方法是一一对应的，因此，装置也具有与其对应的方法类似的有益技术效果，由于上面已经对方法的有益技术效果进行了详细说明，因此，这里不再赘述对应装置的有益技术效果。

[0208] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device,PLD)(例如现场可编程门阵列(Field Programmable Gate Array,FPGA))就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言(Hardware Description Language,HDL)，而HDL也并非仅有一种，而是有许多种，如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等，目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[0209] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种

功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0210] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0211] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0212] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0213] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0214] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0215] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0216] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0217] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0218] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备

或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0219] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0220] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0221] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0222] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于装置实施例或系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0223] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

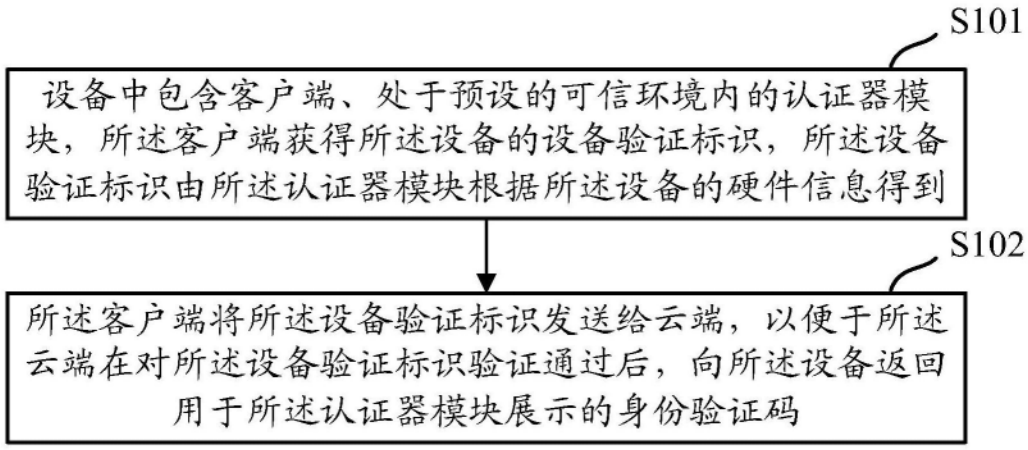

S101
设备中包含客户端、处于预设的可信环境内的认证器模块，所述客户端获得所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到
S102
所述客户端将所述设备验证标识发送给云端，以便于所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码

图1

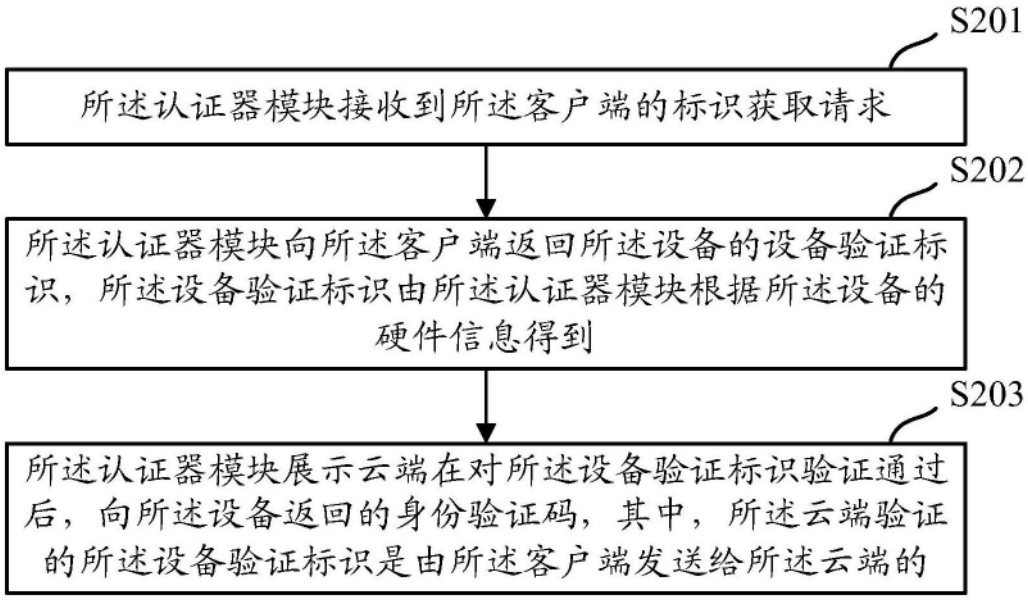

S201
所述认证器模块接收到所述客户端的标识获取请求
S202
所述认证器模块向所述客户端返回所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到
S203
所述认证器模块展示云端在对所述设备验证标识验证通过后，向所述设备返回的身份验证码，其中，所述云端验证的所述设备验证标识是由所述客户端发送给所述云端的

图2

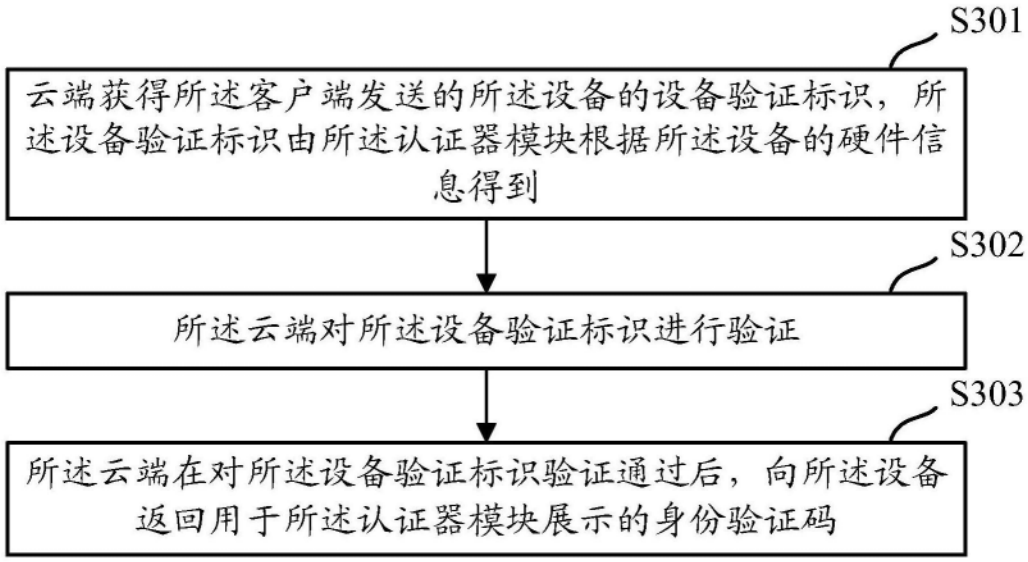

S301
云端获得所述客户端发送的所述设备的设备验证标识，所述设备验证标识由所述认证器模块根据所述设备的硬件信息得到
S302
所述云端对所述设备验证标识进行验证
S303
所述云端在对所述设备验证标识验证通过后，向所述设备返回用于所述认证器模块展示的身份验证码

图3

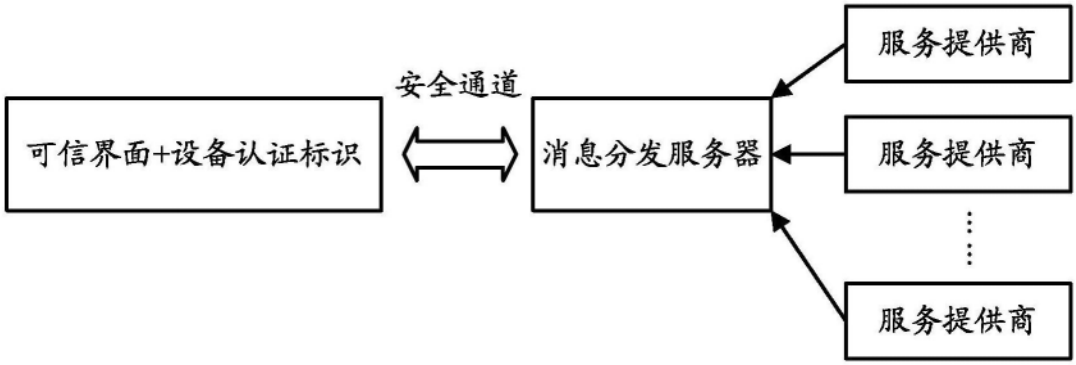

安全通道
可信界面+设备认证标识
消息分发服务器
服务提供商
服务提供商
服务提供商

图4

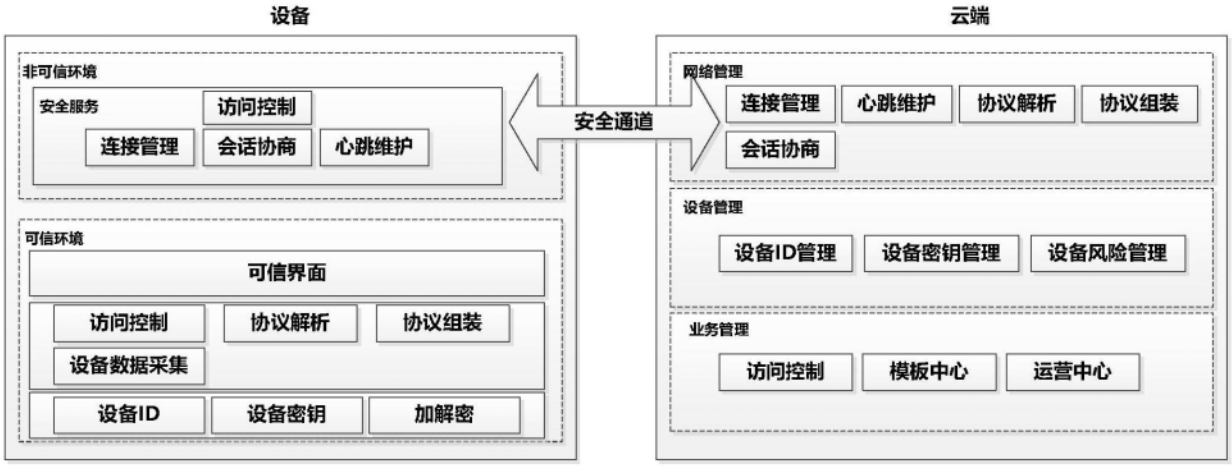

设备
云端
非可信环境
安全服务
访问控制
连接管理
会话协商
心跳维护
安全通道
网络管理
连接管理
心跳维护
协议解析
协议组装
会话协商
可信环境
可信界面
访问控制
协议解析
协议组装
设备数据采集
设备ID
设备密钥
加解密
设备管理
设备ID管理
设备密钥管理
设备风险管理
业务管理
访问控制
模板中心
运营中心

图5

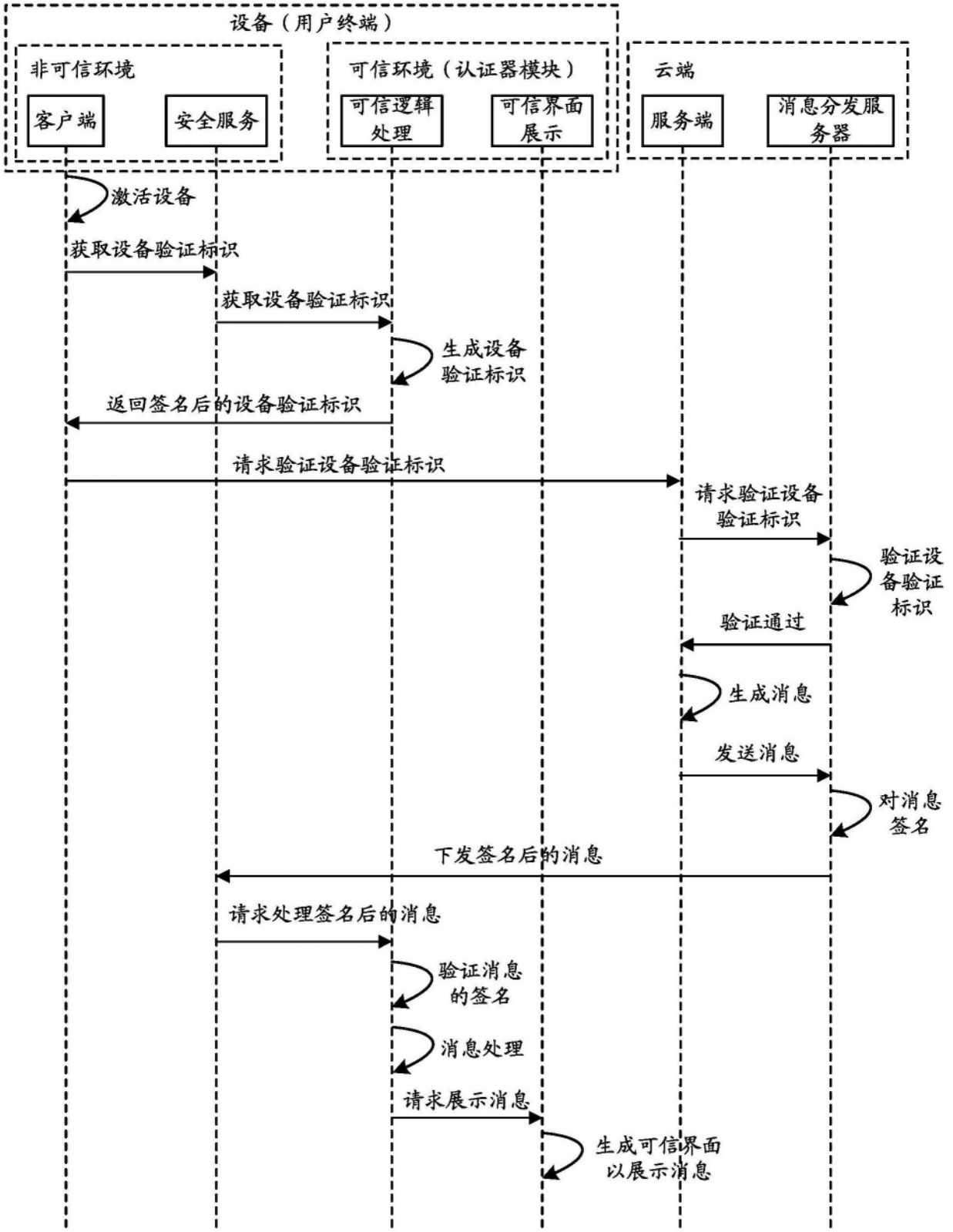

设备（用户终端）
非可信环境
客户端
安全服务
可信环境（认证器模块）
可信逻辑处理
可信界面展示
云端
服务端
消息分发服务器
激活设备
获取设备验证标识
获取设备验证标识
生成设备验证标识
返回签名后的设备验证标识
请求验证设备验证标识
请求验证设备验证标识
验证设备验证标识
验证通过
生成消息
发送消息
对消息签名
下发签名后的消息
请求处理签名后的消息
验证消息的签名
消息处理
请求展示消息
生成可信界面以展示消息

图6

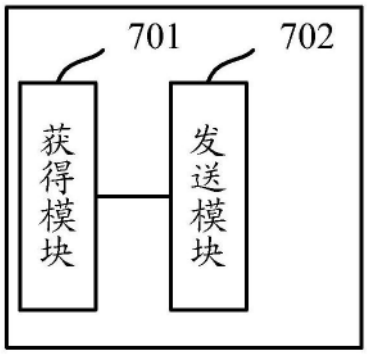

701
702
获得模块
发送模块

图7

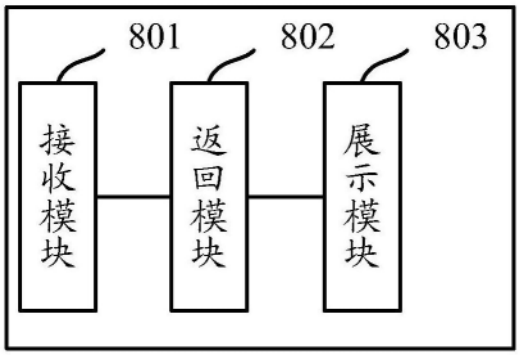

801
802
803
接收模块
返回模块
展示模块

图8

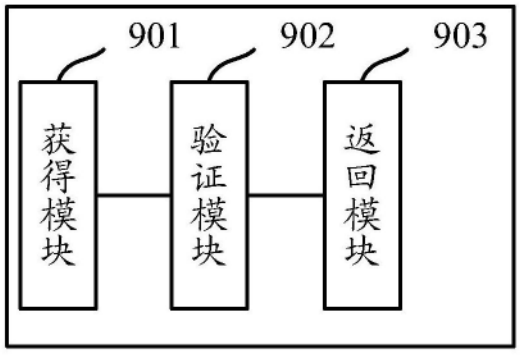

901
902
903
获得模块
验证模块
返回模块

图9