



(12) 发明专利申请

(10) 申请公布号 CN 117062075 A

(43) 申请公布日 2023. 11. 14

(21) 申请号 202311113791.4

H04W 8/18 (2009.01)

(22) 申请日 2023.08.30

H04W 4/14 (2009.01)

(71) 申请人 中移互联网有限公司

地址 510640 广东省广州市天河区高唐路
333号自编1.1栋

申请人 中国移动通信集团有限公司

(72) 发明人 庄严 蒋周良 张燕平 熊中芝

童安璐 吴锦涛 陈澎聪 李卫

毋挺 林翔 马晓凯 柯晓程

(74) 专利代理机构 北京清亦华知识产权代理事

务所(普通合伙) 11201

专利代理师 白雪静

(51) Int. Cl.

H04W 12/06 (2021.01)

H04W 12/08 (2021.01)

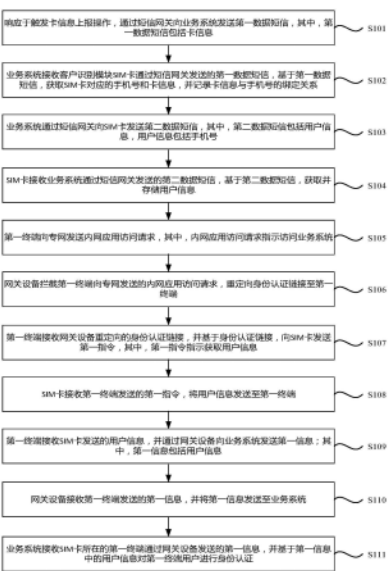
权利要求书3页 说明书17页 附图6页

(54) 发明名称

专网安全认证方法、装置及系统

(57) 摘要

本申请提供了一种专网安全认证方法、装置及系统。其中方法包括：SIM卡将卡信息通过短信网关发送至业务系统，业务系统向SIM卡返回用户信息，第一终端向专网发送内网应用访问请求，网关设备拦截内网应用访问请求，重定向身份认证链接至第一终端；第一终端获取SIM卡的用户信息并通过网关设备发送至业务系统。业务系统基于用户信息对第一终端用户进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限，实现了专网企业侧的身份认证管控。



1. 一种专网安全认证方法,其特征在于,所述方法应用于客户识别模块SIM卡,包括:
响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,所述第一数据短信包括卡信息;

接收所述业务系统通过所述短信网关发送的第二数据短信,基于所述第二数据短信,获取并存储用户信息;其中,所述用户信息包括手机号;

接收所述SIM卡所在的第一终端发送的第一指令,将所述用户信息发送至所述第一终端,其中,所述第一指令指示获取所述用户信息,所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

2. 根据权利要求1所述的方法,其特征在于,所述响应于触发卡信息上报操作之前,包括:

向所述第一终端注册监听入网事件;

监听到所述第一终端首次入网鉴权通过事件,触发卡信息上报操作。

3. 根据权利要求1所述的方法,其特征在于,所述通过短信网关向业务系统发送第一数据短信,包括:

读取卡信息,并将所述卡信息组装于所述第一数据短信的响应数据包中;

通过所述短信网关向所述业务系统发送所述第一数据短信。

4. 根据权利要求1所述的方法,其特征在于,所述接收所述业务系统通过所述短信网关发送的第二数据短信,基于所述第二数据短信,获取并存储用户信息,包括:

接收所述短信网关转发的所述业务系统发送的第二数据短信;其中,所述第二数据短信包括应用命令报文,所述应用命令报文包括所述用户信息;

解密所述第二数据短信,获取所述应用命令报文中的短信内容;

解析所述短信内容,获取并存储所述用户信息。

5. 根据权利要求1所述的方法,其特征在于,所述将所述用户信息发送至所述第一终端,包括:

建立与所述第一终端之间的安全访问通道;

读取用户信息;并加密所述用户信息,得到用户信息密文;

将所述用户信息密文通过所述安全访问通道发送至所述第一终端。

6. 根据权利要求3所述的方法,其特征在于,所述响应数据包包括卡应用主版本号、安全参数标识定义、应用响应数据包和MAC,所述应用响应数据包包括所述卡信息,所述安全参数标识包括加密标识和环境标识。

7. 根据权利要求3所述的方法,其特征在于,所述存储所述用户信息,包括:

将所述用户信息存储于所述SIM卡的安全存储空间。

8. 一种专网安全认证方法,其特征在于,所述方法应用于第一终端,所述第一终端包括客户识别模块SIM卡;所述方法包括:

向专网发送内网应用访问请求,其中,所述内网应用访问请求指示访问所述业务系统;

接收网关设备重定向的身份认证链接,并基于所述身份认证链接,向所述SIM卡发送第一指令,其中,所述第一指令指示获取所述用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号;

接收所述SIM卡发送的所述用户信息,并通过所述网关设备向业务系统发送第一信息;

其中,所述第一信息包括用户信息,所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

9.根据权利要求8所述的方法,其特征在于,所述第一终端向所述专网发送内网应用访问请求之前,包括:

所述第一终端向专网发送接入请求,所述接入请求指示所述专网验证所述第一终端的权限。

10.根据权利要求8所述的方法,其特征在于,所述方法还包括:

接收所述SIM卡发送的监听入网事件注册请求。

11.一种专网安全认证方法,其特征在于,所述方法应用于网关设备,包括:

拦截所述第一终端向专网发送的内网应用访问请求,重定向身份认证链接至所述第一终端;其中,所述第一终端包括客户识别模块SIM卡,所述内网应用访问请求指示访问业务系统;

接收所述第一终端发送的第一信息,并将所述第一信息发送至所述业务系统,其中,所述第一信息包括用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号,所述第一终端基于所述用户信息请求所述业务系统对第一终端用户进行身份认证。

12.一种专网安全认证方法,其特征在于,所述方法应用于专网内的业务系统,包括:

接收所述客户识别模块SIM卡通过所述短信网关发送的第一数据短信,其中,所述第一数据短信包括卡信息;

基于所述第一数据短信,获取所述SIM卡对应的手机号和所述卡信息,并记录所述卡信息与所述手机号的绑定关系;

通过所述短信网关向所述SIM卡发送第二数据短信,其中,所述第二数据短信包括用户信息,所述用户信息包括所述手机号;

接收所述SIM卡所在的第一终端通过网关设备发送的第一信息,并基于所述第一信息中的用户信息对所述第一终端用户进行身份认证。

13.一种专网安全认证系统,其特征在于,包括客户识别模块SIM卡,所述SIM卡所在的第一终端、短信网关、网关设备和业务系统,

所述SIM卡,被配置为执行如权利要求1—7中任一项所述的专网安全认证方法;

所述SIM卡所在的第一终端,被配置为执行如权利要求8—10中任一项所述的专网安全认证方法;

所述网关设备,被配置为执行如权利要求11所述的专网安全认证方法;

所述业务系统,被配置为执行如权利要求12所述的专网安全认证方法。

14.一种专网安全认证装置,其特征在于,所述装置配置于客户识别模块SIM卡,包括:

卡信息上报模块,用于响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,所述第一数据短信包括卡信息;

所述卡信息上报模块,还用于接收所述业务系统通过所述短信网关发送的第二数据短信,基于所述第二数据短信,获取并存储用户信息;其中,所述用户信息包括手机号;

收发模块,用于接收所述SIM卡所在的第一终端发送的第一指令,将所述用户信息发送至所述第一终端,其中,所述第一指令指示获取所述用户信息,所述第一终端基于所述用户

信息请求所述业务系统对所述第一终端用户进行身份认证。

15. 一种专网安全认证装置, 其特征在于, 所述装置配置于第一终端, 所述第一终端包括SIM卡, 包括:

收发模块, 用于向所述专网发送内网应用访问请求, 其中, 所述内网应用访问请求指示访问所述业务系统;

所述收发模块, 还用于接收网关设备重定向的身份认证链接, 并基于所述身份认证链接, 向所述客户识别模块SIM卡发送第一指令, 其中, 所述第一指令指示获取所述用户信息, 所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的, 所述用户信息包括手机号;

所述收发模块, 还用于接收所述SIM卡发送的所述用户信息, 并通过所述网关设备向业务系统发送第一信息; 其中, 所述第一信息包括用户信息, 所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

16. 一种专网安全认证装置, 其特征在于, 所述装置配置于网关设备, 包括:

接入网关模块, 用于拦截所述第一终端向专网发送的内网应用访问请求, 重定向身份认证链接至所述第一终端; 其中, 所述第一终端包括客户识别模块SIM卡, 所述内网应用访问请求指示访问业务系统;

控制中心模块, 用于接收所述第一终端发送的第一信息, 并将所述第一信息发送至所述业务系统, 其中, 所述第一信息包括用户信息, 所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的, 所述用户信息包括手机号, 所述第一终端基于所述用户信息请求所述业务系统对第一终端用户进行身份认证。

17. 一种专网安全认证装置, 其特征在于, 所述装置配置于专网内的业务系统, 包括:

收发模块, 用于接收所述客户识别模块SIM卡通过所述短信网关发送的第一数据短信, 其中, 所述第一数据短信包括卡信息;

处理模块, 用于基于所述第一数据短信, 获取所述SIM卡对应的手机号和所述卡信息, 并记录所述卡信息与所述手机号的绑定关系;

所述收发模块, 还用于通过所述短信网关向所述SIM卡发送第二数据短信, 其中, 所述第二数据短信包括用户信息, 所述用户信息包括所述手机号;

身份认证模块, 用于接收所述SIM卡所在的第一终端通过网关设备发送的第一信息, 并基于所述第一信息中的用户信息对所述第一终端用户进行身份认证。

18. 一种电子设备, 其特征在于, 包括:

至少一个处理器; 以及

与所述至少一个处理器通信连接的存储器; 其中,

所述存储器存储有可被所述至少一个处理器执行的指令, 所述指令被所述至少一个处理器执行, 以使所述至少一个处理器能够执行权利要求1至12中任一项所述的专网安全认证方法。

19. 一种存储有计算机指令的非瞬时计算机可读存储介质, 其特征在于, 所述计算机指令用于使所述计算机执行权利要求1至12中任一项所述的专网安全认证方法。

专网安全认证方法、装置及系统

技术领域

[0001] 本申请涉及通信技术领域,尤其涉及一种专网安全认证方法、装置及系统。

背景技术

[0002] 目前,运营商为行业用户建设5G专网普遍采用核心网用户面功能 (UPF) 下沉模式,该模式依赖于运营商的核心网和基站,终端准入由运营商进行业务开通,但对于行业用户而言,建设完成的5G专网等同于企业内网,仅依赖于运营商在5G核心网的一次鉴权不足以满足行业用户的接入安全需求,尤其是党政军、公检法、金融等高安全级别面向个人用户接入的场景,仅依赖运营商做安全准入管理,远不能满足行业用户的需求。

[0003] 目前5G专网建设方案,依赖于运营商的核心网和基站,终端准入由运营商进行业务开通,数据签约在运营商侧配置,对于行业用户而言,无法自主管理用户通过5G专网访问业务系统的准入权限。

发明内容

[0004] 本申请提供了一种专网安全认证方法、装置及系统,以实现自主管理用户通过专网访问业务系统的准入权限。本申请的技术方案如下:

[0005] 第一方面,本申请实施例提供了一种专网安全认证方法,所述方法应用于SIM卡,包括:

[0006] 响应于触发卡信息上报操作,

[0007] 响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,所述第一数据短信包括卡信息;

[0008] 接收所述业务系统通过所述短信网关发送的第二数据短信,基于所述第二数据短信,获取并存储用户信息;其中,所述用户信息包括手机号;

[0009] 接收所述SIM卡所在的第一终端发送的第一指令,将所述用户信息发送至所述第一终端,其中,所述第一指令指示获取所述用户信息,所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

[0010] 在一些实现方式中,所述响应于触发卡信息上报操作之前,包括:

[0011] 向所述第一终端注册监听入网事件;

[0012] 监听到所述第一终端首次入网鉴权通过事件,触发卡信息上报操作。

[0013] 在一些实现方式中,所述通过短信网关向业务系统发送第一数据短信,其中,所述第一数据短信包括卡信息;包括:

[0014] 读取卡信息,并将所述卡信息组装于所述第一数据短信的响应数据包中;

[0015] 通过所述短信网关向所述业务系统发送所述第一数据短信。

[0016] 在一些实现方式中,所述接收所述业务系统通过所述短信网关发送的第二数据短信,基于所述第二数据短信,获取并存储用户信息,包括:

[0017] 接收所述短信网关转发的所述业务系统发送的第二数据短信;其中,所述第二数

据短信包括应用命令报文,所述应用命令报文包括所述用户信息;

[0018] 解密所述第二数据短信,获取所述应用命令报文中的短信内容;

[0019] 解析所述短信内容,获取并存储所述用户信息。

[0020] 在一些实现方式中,所述将所述用户信息发送至所述第一终端,包括:

[0021] 建立与所述第一终端之间的安全访问通道;

[0022] 读取用户信息;并加密所述用户信息,得到用户信息密文;

[0023] 将所述用户信息密文通过所述安全访问通道发送至所述第一终端。

[0024] 在一些实现方式中,所述响应数据包包括卡应用主版本号、安全参数标识定义、应用响应数据包和MAC,所述应用响应数据包包括所述卡信息,所述安全参数标识包括加密标识和环境标识。

[0025] 在一些实现方式中,所述存储所述用户信息,包括:

[0026] 将所述用户信息存储于所述SIM卡的安全存储空间。

[0027] 第二方面,本申请实施例提供了一种专网安全认证方法,所述方法应用于第一终端,所述第一终端包括SIM卡;所述方法包括:

[0028] 向专网发送内网应用访问请求,其中,所述内网应用访问请求指示访问所述业务系统;

[0029] 接收网关设备重定向的身份认证链接,并基于所述身份认证链接,向所述SIM卡发送第一指令,其中,所述第一指令指示获取所述用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号;

[0030] 接收所述SIM卡发送的所述用户信息,并通过所述网关设备向业务系统发送第一信息;其中,所述第一信息包括用户信息,所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

[0031] 在一些实现方式中,所述第一终端向所述专网发送内网应用访问请求之前,包括:

[0032] 所述第一终端向专网发送接入请求,所述接入请求指示所述专网验证所述第一终端的权限。

[0033] 在一些实现方式中,所述方法还包括:

[0034] 接收所述SIM卡发送的监听入网事件注册请求。

[0035] 第三方面,本申请实施例提供了一种专网安全认证方法,所述方法应用于网关设备,包括:

[0036] 拦截所述第一终端向专网发送的内网应用访问请求,重定向身份认证链接至所述第一终端;其中,所述第一终端包括客户识别模块SIM卡,所述内网应用访问请求指示访问业务系统;

[0037] 接收所述第一终端发送的第一信息,并将所述第一信息发送至所述业务系统,其中,所述第一信息包括用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号,所述第一终端基于所述用户信息请求所述业务系统对第一终端用户进行身份认证。

[0038] 第四方面,本申请实施例提供了一种专网安全认证方法,所述方法应用于专网内的业务系统,包括:

[0039] 接收所述客户识别模块SIM卡通过所述短信网关发送的第一数据短信,其中,所述

第一数据短信包括卡信息；

[0040] 基于所述第一数据短信，获取所述SIM卡对应的手机号和所述卡信息，并记录所述卡信息与所述手机号的绑定关系；

[0041] 通过所述短信网关向所述SIM卡发送第二数据短信，其中，所述第二数据短信包括用户信息，所述用户信息包括所述手机号；

[0042] 接收所述SIM卡所在的第一终端通过网关设备发送的第一信息，并基于所述第一信息中的用户信息对所述第一终端用户进行身份认证。

[0043] 第五方面，本申请实施例提供了一种专网安全认证系统，包括SIM卡，所述SIM卡所在的第一终端、短信网关、网关设备和业务系统，

[0044] 所述SIM卡，被配置为执行第一方面所述的专网安全认证方法；

[0045] 所述SIM卡所在的第一终端，被配置为执行第二方面所述的专网安全认证方法；

[0046] 所述网关设备，被配置为执行第三方面所述的专网安全认证方法；

[0047] 所述业务系统，被配置为执行第四方面所述的专网安全认证方法。

[0048] 第六方面，本申请实施例提供了一种专网安全认证装置，所述装置配置于SIM卡，包括：

[0049] 卡信息上报模块，用于响应于触发卡信息上报操作，通过短信网关向业务系统发送第一数据短信，其中，所述第一数据短信包括卡信息；

[0050] 所述卡信息上报模块，还用于接收所述业务系统通过所述短信网关发送的第二数据短信，基于所述第二数据短信，获取并存储用户信息；其中，所述用户信息包括手机号；

[0051] 收发模块，用于接收所述SIM卡所在的第一终端发送的第一指令，将所述用户信息发送至所述第一终端，其中，所述第一指令指示获取所述用户信息，所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

[0052] 在一些实现方式中，所述卡信息上报模块，还用于：

[0053] 向所述第一终端注册监听入网事件；

[0054] 监听到所述第一终端首次入网鉴权通过事件，触发卡信息上报操作。

[0055] 在一些实现方式中，所述卡信息上报模块，具体用于：

[0056] 读取卡信息，并将所述卡信息组装于所述第一数据短信的响应数据包中；

[0057] 通过所述短信网关向所述业务系统发送所述第一数据短信。

[0058] 在一些实现方式中，所述卡信息上报模块，具体用于：

[0059] 接收所述短信网关转发的所述业务系统发送的第二数据短信；其中，所述第二数据短信包括应用命令报文，所述应用命令报文包括所述用户信息；

[0060] 解密所述第二数据短信，获取所述应用命令报文中的短信内容；

[0061] 解析所述短信内容，获取并存储所述用户信息。

[0062] 在一些实现方式中，所述收发模块，具体用于：

[0063] 建立与所述第一终端之间的安全访问通道；

[0064] 读取用户信息；并加密所述用户信息，得到用户信息密文；

[0065] 将所述用户信息密文通过所述安全访问通道发送至所述第一终端。

[0066] 在一些实现方式中，所述响应数据包包括卡应用主版本号、安全参数标识定义、应用响应数据包和MAC，所述应用响应数据包包括所述卡信息，所述安全参数标识包括加密标

识和环境标识。

[0067] 在一些实现方式中,所述卡信息上报模块,具体用于:

[0068] 将所述用户信息存储于所述SIM卡的安全存储空间。

[0069] 第七方面,本申请实施例提供了一种专网安全认证装置,所述装置配置于第一终端,所述第一终端包括SIM卡,包括:

[0070] 收发模块,用于向所述专网发送内网应用访问请求,其中,所述内网应用访问请求指示访问所述业务系统;

[0071] 所述收发模块,还用于接收网关设备重定向的身份认证链接,并基于所述身份认证链接,向所述客户识别模块SIM卡发送第一指令,其中,所述第一指令指示获取所述用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号;

[0072] 所述收发模块,还用于接收所述SIM卡发送的所述用户信息,并通过所述网关设备向业务系统发送第一信息;其中,所述第一信息包括用户信息,所述第一终端基于所述用户信息请求所述业务系统对所述第一终端用户进行身份认证。

[0073] 在一些实现方式中,所述收发模块,还用于:

[0074] 所述第一终端向专网发送接入请求,所述接入请求指示所述专网验证所述第一终端的权限。

[0075] 在一些实现方式中,所述收发模块,还用于:

[0076] 接收所述SIM卡发送的监听入网事件注册请求。

[0077] 第八方面,本申请实施例提供了一种专网安全认证装置,所述装置配置于网关设备,包括:

[0078] 接入网关模块,用于拦截所述第一终端向专网发送的内网应用访问请求,重定向身份认证链接至所述第一终端;其中,所述第一终端包括客户识别模块SIM卡,所述内网应用访问请求指示访问业务系统;

[0079] 控制中心模块,用于接收所述第一终端发送的第一信息,并将所述第一信息发送至所述业务系统,其中,所述第一信息包括用户信息,所述用户信息为所述业务系统基于所述SIM卡上报的卡信息发送至所述SIM卡的,所述用户信息包括手机号,所述第一终端基于所述用户信息请求所述业务系统对第一终端用户进行身份认证。

[0080] 第九方面,本申请实施例提供了一种专网安全认证装置,所述装置配置于专网内的业务系统,包括:

[0081] 收发模块,用于接收所述客户识别模块SIM卡通过所述短信网关发送的第一数据短信,其中,所述第一数据短信包括卡信息;

[0082] 处理模块,用于基于所述第一数据短信,获取所述SIM卡对应的手机号和所述卡信息,并记录所述卡信息与所述手机号的绑定关系;

[0083] 所述收发模块,还用于通过所述短信网关向所述SIM卡发送第二数据短信,其中,所述第二数据短信包括用户信息,所述用户信息包括所述手机号;

[0084] 身份认证模块,用于接收所述SIM卡所在的第一终端通过网关设备发送的第一信息,并基于所述第一信息中的用户信息对所述第一终端用户进行身份认证。

[0085] 第十方面,本申请实施例提供了一种电子设备,包括:至少一个处理器;以及与所

述至少一个处理器通信连接的存储器;其中,所述存储器存储有可被所述至少一个处理器执行的指令,所述指令被所述至少一个处理器执行,以使所述至少一个处理器能够执行本申请第一方面至第四方面中任一项实施例所述的专网安全认证方法。

[0086] 第十一方面,本申请实施例提供了一种存储有计算机指令的非瞬时计算机可读存储介质,所述计算机指令用于使所述计算机执行本申请第一方面至第四方面中任一项实施例所述的专网安全认证方法。

[0087] 第十二方面,本申请实施例提供了一种计算机程序产品,包括计算机指令,该计算机指令被处理器执行时实现本申请第一方面至第四方面中任一项实施例所述的专网安全认证方法的步骤。

[0088] 本申请实施例提供的技术方案至少带来以下有益效果:

[0089] 通过SIM卡上报卡信息至专网内的业务系统,将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。

[0090] 应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本申请。

附图说明

[0091] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本申请的实施例,并与说明书一起用于解释本申请的原理,并不构成对本申请的不当限定。

[0092] 图1是根据一示例性实施例示出的一种专网安全认证方法的流程图。

[0093] 图2是根据一示例示出的第一数据短信的结构示意图。

[0094] 图3是根据一示例示出的响应数据包的结构示意图。

[0095] 图4是根据一示例示出的第二数据短信的结构示意图。

[0096] 图5是根据一示例示出的应用命令报文的结构示意图。

[0097] 图6是根据另一示例性实施例示出的一种专网安全认证方法的流程图。

[0098] 图7是根据又一示例性实施例示出的一种专网安全认证方法的流程图。

[0099] 图8是根据又一示例性实施例示出的一种专网安全认证方法的流程图。

[0100] 图9是根据又一示例性实施例示出的一种专网安全认证方法的流程图。

[0101] 图10是根据一示例性实施例示出的一种专网安全认证装置的框图。

[0102] 图11是根据另一示例性实施例示出的一种专网安全认证装置的框图。

[0103] 图12是根据又一示例性实施例示出的一种专网安全认证装置的框图。

[0104] 图13是根据又一示例性实施例示出的一种专网安全认证装置的框图。

[0105] 图14是根据又一示例性实施例示出的一种专网安全认证系统的框图。

[0106] 图15是根据一示例性实施例示出的一种电子设备的框图。

具体实施方式

[0107] 为了使本领域普通人员更好地理解本申请的技术方案,下面将结合附图,对本申请实施例中的技术方案进行清楚、完整地描述。

[0108] 需要说明的是,本申请中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本申请实施例能够以除了在这里图示或描述的那些以外的顺序实施。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0109] 5G(5th Generation Mobile Communication Technology,第五代移动通信技术)网络自正式商用以来,已快速实现民用阶段的普及,商用领域以中国移动为首的运营商5G专网的建设也迅猛发展,借助于专网的低时延、高带宽、高容载等特点,高度契合数字化转型需求,是OT(Operation Technology,操作技术)+IT(Internet Technology,互联网技术)+CT(Communication Technology,通讯技术)的全面融合与提升,可快速助力于传统行业、垂直公安、轨道交通、社会部门等实现数字化转型。

[0110] 5G专网是一种局域网(LAN),依托于5G网络切片技术,能为目标客户和企业创建具有统一连接性、优化服务功能和在特定区域内保障通信安全的专属的网络连接体系,作为专属服务,网络的稳定性、服务性和安全性都具备更好的保障。

[0111] 目前,运营商为行业用户建设5G专网普遍采用核心网用户面功能(UPF)下沉模式,该模式依赖于运营商的核心网和基站,终端准入由运营商进行业务开通,数据签约在运营商侧配置。但对于行业用户而言,建设完成的5G专网等同于企业内网,仅依赖于运营商在5G核心网的一次鉴权不足以满足行业用户的接入安全需求,尤其是高安全级别面向个人用户接入的场景,仅依赖运营商做安全准入管理,远不能满足行业用户的需求,无法自主管理用户通过5G专网访问业务系统的准入权限。

[0112] 为了解决上述问题,本申请实施例提供了一种专网安全认证方法、装置及系统,通过引入SIM(Subscriber Identity Module,客户识别模块)卡和网关设备作为基础设施和IT支撑,实现5G专网在CT层的安全身份认证,解决5G专网企业侧无法认证管控,二次用户身份管控鉴权需要频繁登录、安全等级低等问题。

[0113] 图1是根据本申请一个实施例的专网安全认证方法的流程图。该方法应用于专网安全认证系统,专网安全认证系统包括SIM卡,SIM卡所在的第一终端、短信网关、网关设备和专网内的业务系统,短信网关和网关设备为专网的网关。如图1所示,该专网安全认证方法可以包括如下步骤。

[0114] 步骤S101,响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,第一数据短信包括卡信息。

[0115] 首先需要说明的是,本申请实施例的SIM卡为支持ISO/IEC 7816-4规范及3GPPTS 31.111规范的智能卡,具体表现形式为支持APDU(Application Protocol Data Unit,应用协议数据单元)指令,支持面向连接的承载独立传输协议BIP(Bearer Independent Protocol,承载独立协议)。

[0116] 在一些实施例中,SIM卡向该SIM卡所在的第一终端注册监听入网事件;监听到第一终端首次入网鉴权通过事件后,触发卡信息上报操作。

[0117] 示例性的,SIM卡通过向第一终端注册STATUS入网事件监听,当第一终端接入专网入网鉴权通过后,SIM卡检测到SIM卡首次入网成功,自动触发一次卡信息上报,即触发SIM卡上报卡信息至短信网关。

[0118] 作为一种实现方式, SIM卡的卡信息上报模块向该SIM卡所在的第一终端注册监听入网事件。

[0119] 作为一种实现方式, SIM卡读取卡信息, 并将卡信息组装于第一数据短信的响应数据包中, 通过短信网关向业务系统发送第一数据短信。

[0120] SIM卡向短信网关发送第一数据短信, 第一数据短信包括响应数据包, 响应数据包包括卡信息, 短信网关将卡信息和手机号透传至业务系统。

[0121] 需要说明的是, 数据短信是一段数字标识, 可以理解为APDU指令, 在SIM卡通过短信网关将第一数据短信发送至业务系统时, 由于SIM卡需要通过手机号向短信网关发送短信, 短信网关的网关端口则可以获取SIM卡的手机号。即SIM卡入网的时候, 需要通过手机号接入移动网络, 业务系统在接收到该第一数据短信之后, 则可以获取该SIM卡对应的手机号, 手机号是与终端用户绑定的, 由此, 业务系统能够基于手机号对终端用户进行身份认证。

[0122] 可选的, SIM卡将空卡序列号、ICCID(Integrate circuit card identity, 集成电路卡识别码, 即SIM卡卡号)、IMSI(International Mobile Subscriber Identity, 国际移动用户识别码)、SEID(Security Element Identifier, 安全元素标识符)等卡信息组装在响应数据包中作为第一数据短信的一部分发送至短信网关, 第一数据短信为上行短信。

[0123] 短信网关接收第一数据短信, 即卡信息上报短信, 短信网关将卡信息及该手机号透传至业务系统。

[0124] 示例性的, 图2所示为第一数据短信的结构, 图3所示为第一数据短信的响应数据包的结构。响应数据包包括卡应用主版本号、安全参数标识定义、应用响应数据包和MAC(Media Access Control Address, 媒体存取控制位址, 又称物理地址), 应用响应数据包包括卡信息, 安全参数标识包括加密标识和环境标识。

[0125] 表1: 上行短信响应数据包字段定义

[0126]	参数	长度(字节)	值(Hex)	说明
	Ver	1	0x02	卡应用主版本号
	Flag	1		表 2 安全参数标识定义
	APP-Data	XX		应用响应数据包
	MAC	4		对 Ver ~APP-Data 使用 SM4-CBC 计算 MAC, 使用固定追加一字节 0x80 方式填充, 初始向量为全“00”。注意如果 APP-DATA 需要加密, 则待计算数据是加密后的 APP-DATA

[0127] 表2: 安全参数标识定义

	b8	b7	b6	b5	b4	b3	b2	b1	说明
[0128]	0	0	0	0	0	0	-	X	加密标识 0: 不加密 1: 加密
[0129]	0	0	0	0	0	0	X	-	环境标识 0: 测试环境 1: 生产环境

[0130] 步骤S102,业务系统接收客户识别模块SIM卡通过短信网关发送的第一数据短信,基于第一数据短信,获取SIM卡对应的手机号和卡信息,并记录卡信息与手机号的绑定关系。

[0131] 可以理解为,业务系统在接收到第一数据短信之后,则可以获取该SIM卡对应的手机号,业务系统便可以将接收到的卡信息与手机号进行绑定,记录卡信息与手机号的绑定关系。也就是说,由于卡信息中的空卡序列号、ICCID、IMSI等均是唯一的,手机号与这些唯一的卡信息是一一绑定的,通过SIM卡实现将卡信息与手机号关联起来,SIM卡则作为终端用户的身份标识。

[0132] 步骤S103,业务系统通过短信网关向SIM卡发送第二数据短信,其中,第二数据短信包括用户信息,用户信息包括手机号。

[0133] 可以理解为,业务系统组装携带手机号的第二数据短信;请求短信网关将第二数据短信发送至SIM卡。短信网关下发第二数据短信至该手机号对应的SIM卡,第二数据短信为下行短信。

[0134] 在一些实施例中,第二数据短信包括应用命令报文,应用命令报文包括手机号。

[0135] 示例性的,图4所示为第二数据短信的结构,图5所示为第二数据短信的应用命令报文的结构。

[0136] 表3:下行短信应用数据APP-DATA字段定义

[0137]	参数	长度(字节)	值	说明
	Tag	1	0x2D	命令类型
	长度	1	XX	命令长度
	手机号长度	1	XX	最大支持20字节
	手机号	0-20	XX	

[0138] 步骤S104,SIM卡接收业务系统通过短信网关发送的第二数据短信,基于第二数据短信,获取并存储用户信息。

[0139] 作为一种实现方式,SIM卡接收短信网关转发的业务系统发送的第二数据短信;解密第二数据短信,获取应用命令报文中的短信内容;解析短信内容,获取并存储用户信息。

[0140] 可以理解为,SIM卡接收短信网关转发的业务系统发送的第二数据短信,对第二数据短信进行消息验证码校验,校验通过后解密第二数据短信,获取第二数据短信的内容,并

解析该内容,提取手机号等用户信息,并将用户信息写入存储。

[0141] 可选的,SIM卡将用户信息存储于SIM卡的安全存储空间。

[0142] 步骤S105,第一终端向专网发送内网应用访问请求,其中,内网应用访问请求指示访问业务系统。

[0143] 需要说明的是,终端与专网对应,例如,在业务系统属于5G专网的内网应用时,第一终端为5G终端。

[0144] 在一些实施例中,第一终端向专网发送内网应用访问请求之前,还包括:第一终端向专网发送接入请求,接入请求指示专网验证第一终端的权限。

[0145] 可以理解为,终端用户通过第一终端接入专网,运营商的核心网通过分配专网IP地址,实现专网的一次鉴权。鉴权通过后,第一终端向专网发送内网应用访问请求,在请求访问企业内网应用时则会触发终端用户的身份认证核验。

[0146] 在一些实施例中,第一终端接收SIM卡发送的监听入网事件注册请求,以便SIM卡监听到第一终端针对专网首次入网鉴权通过事件后,触发卡信息上报操作。

[0147] 步骤S106,网关设备拦截第一终端向专网发送的内网应用访问请求,重定向身份认证链接至第一终端。

[0148] 可以理解为,网关设备拦截专网流量发起重定向请求。可选的,网关设备的接入网关模块拦截专网流量发起重定向请求。

[0149] 示例性的,第一终端发送的内网应用访问请求的网络流量经交换机/路由器镜像到网关设备的接入网关模块,接入网关模块,接收到交换机/路由器的镜像内网应用访问请求,发送TCP RESET阻断包至交换机/路由器,并重定向身份认证链接(接入网关8081端口URL)至第一终端。

[0150] 步骤S107,第一终端接收网关设备重定向的身份认证链接,并基于身份认证链接,向SIM卡发送第一指令,其中,第一指令指示获取用户信息。

[0151] 可以理解为,第一终端向专网发送内网应用访问请求时,网关设备拦截第一终端向专网发送的内网应用访问请求,重定向身份认证链接至第一终端。

[0152] 可以理解为,第一终端接收到身份认证链接之后,向SIM卡获取用户信息密文。

[0153] 可选的,第一指令为APDU指令,即第一终端向SIM卡发送APDU指令,APDU指令指示获取用户信息。

[0154] 步骤S108,SIM卡接收第一终端发送的第一指令,将用户信息发送至第一终端。

[0155] 可以理解为,用户通过第一终端接入专网,请求企业内网应用,则会触发用户身份核验。第一终端则向其内配置的SIM卡发送的第一指令请求获取之前SIM卡存储的用户信息。

[0156] 作为一种实现方式,SIM卡建立与第一终端之间的安全访问通道;读取存储的用户信息,并加密用户信息,得到用户信息密文;将用户信息密文通过安全访问通道发送至第一终端。

[0157] 可选地,SIM卡接收第一指令之后,读取保存在安全存储空间中的用户信息,通过卡内预置密钥对用户信息进行加密,得到用户信息密文。

[0158] 可选的,该密钥为SIM卡制卡过程预置,仅与业务系统共享,以保证数据安全性。

[0159] 步骤S109,第一终端接收SIM卡发送的用户信息,并通过网关设备向业务系统发送

第一信息;其中,第一信息包括用户信息。

[0160] 在本实施例中,第一信息中的“信息”也可以是消息、信令、指令等名称。

[0161] 需要说明的是,第一信息中的用户信息为用户信息密文。

[0162] 作为一种实现方式,第一终端接收SIM卡发送的用户信息密文,拼接包括用户信息密文的代理身份认证请求,通过访问身份认证链接接入网关设备,将代理身份认证请求发送至网关设备的控制中心;其中,代理身份认证请求指示网关设备将用户信息透传至业务系统。

[0163] 可以理解为,第一终端接收用户信息密文之后,通过网关设备将用户信息密文透传给业务系统。

[0164] 步骤S110,网关设备接收第一终端发送的第一信息,并将第一信息发送至业务系统。

[0165] 作为一种实现方式,网关设备接收第一终端发送的代理身份认证请求,将用户信息发送至业务系统;其中,代理身份认证请求指示网关设备将用户信息发送至业务系统,代理身份认证请求包括第一信息。

[0166] 在一些实施例中,网关设备的控制中心接收第一终端通过身份认证链接发送的代理身份认证请求,将用户信息透传至业务系统。

[0167] 需要说明的是,第一信息包括用户信息密文。

[0168] 作为一种实现方式,控制中心接收代理身份认证请求,并将用户信息密文封装成通用认证接口协议报文;将通用认证接口协议报文发送至企业内网的业务系统的身份认证平台。由于传输过程中,全程为密文,保障了用户信息的安全传输。

[0169] 步骤S111,业务系统接收SIM卡所在的第一终端通过网关设备发送的第一信息,并基于第一信息中的用户信息对第一终端用户进行身份认证。

[0170] 也就是说,业务系统接收用户信息,并基于用户信息对第一终端用户进行身份认证。

[0171] 作为一种实现方式,业务系统的身份认证平台解析接收到的通用认证接口协议报文,获取用户信息密文;通过本地私钥解密,获取用户信息;将用户信息与本地管理员配置的用户信息白名单进行比对,校验通过,方通访问,即授权该第一终端用户访问业务系统。

[0172] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定,无需界面搜集用户信息,体验佳。通过SIM卡硬介质层面对用户信息进行加密,全程密文传输,实现安全认证。通过网关设备重定向进行用户身份信息校验,可覆盖全终端,易于推广。

[0173] 在上述实施例的基础上,图6是根据本申请一个实施例的专网安全认证方法的流程图。该方法应用于SIM卡。如图6所示,该专网安全认证方法可以包括如下步骤。

[0174] 步骤S601,响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,第一数据短信包括卡信息。

[0175] 步骤S602,接收业务系统通过短信网关发送的第二数据短信,基于第二数据短信,

获取并存储用户信息;其中,用户信息包括手机号。

[0176] 步骤S603,接收SIM卡所在的第一终端发送的第一指令,将用户信息发送至第一终端,其中,第一指令指示获取用户信息,第一终端基于用户信息请求业务系统对第一终端用户进行身份认证。

[0177] 将用户信息发送至第一终端,以便第一终端通过网关设备将用户信息发送至业务系统,以请求业务系统对第一终端用户进行身份认证。

[0178] 需要说明的是,在本申请的实施例中,步骤S601—步骤S603的实现过程可参见本申请图1所示的实施例中对应步骤的实现过程的描述,在此不再赘述。

[0179] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,并将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定,无需界面搜集用户信息,体验佳。通过SIM卡硬介质层面对用户信息进行加密,全程密文传输,实现安全认证。

[0180] 在上述任一实施例的基础上,图7是根据本申请另一个实施例的专网安全认证方法的流程图。该方法应用于第一终端,第一终端包括SIM卡;如图7所示,该专网安全认证方法可以包括如下步骤。

[0181] 步骤S701,向专网发送内网应用访问请求,其中,内网应用访问请求指示访问业务系统。

[0182] 第一终端向专网发送内网应用访问请求,其中,内网应用访问请求指示访问业务系统。

[0183] 步骤S702,接收网关设备重定向的身份认证链接,并基于身份认证链接,向SIM卡发送第一指令。

[0184] 其中,第一指令指示获取用户信息,用户信息为业务系统基于SIM卡上报的卡信息发送至SIM卡的,用户信息包括手机号。

[0185] 步骤S703,接收SIM卡发送的用户信息,并通过网关设备向业务系统发送第一信息;其中,第一信息包括用户信息。

[0186] 向业务系统发送第一信息,以请求业务系统对第一终端用户进行身份认证。

[0187] 需要说明的是,在本申请的实施例中,步骤S701—步骤S703的实现过程可参见本申请图1所示的实施例中对应步骤的实现过程的描述,在此不再赘述。

[0188] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。

[0189] 在上述任一实施例的基础上,图8是根据本申请又一个实施例的专网安全认证方法的流程图。该方法应用于网关设备;如图8所示,该专网安全认证方法可以包括如下步骤。

[0190] 步骤S801,拦截第一终端向专网发送的内网应用访问请求,重定向身份认证链接至第一终端;其中,第一终端包括SIM卡,内网应用访问请求指示访问业务系统。

[0191] 步骤S802,接收第一终端发送的第一信息,并将第一信息发送至业务系统,其中,第一信息包括用户信息,用户信息为业务系统基于SIM卡上报的卡信息发送至SIM卡的,用户信息包括手机号,第一终端基于用户信息请求业务系统对第一终端用户进行身份认证。

[0192] 需要说明的是,在本申请的实施例中,步骤S801—步骤S802的实现过程可参见本申请图1所示的实施例中对应步骤的实现过程的描述,在此不再赘述。

[0193] 通过实施本实施例,当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的业务系统基于SIM卡上报的卡信息返回的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。通过网关设备重定向进行用户身份信息校验,可覆盖全终端,易于推广。

[0194] 在上述任一实施例的基础上,图9是根据本申请又一个实施例的专网安全认证方法的流程图。该方法应用于专网内的业务系统;如图9所示,该专网安全认证方法可以包括如下步骤。

[0195] 步骤S901,接收客户识别模块SIM卡通过短信网关发送的第一数据短信,其中,第一数据短信包括卡信息。

[0196] 步骤S902,基于第一数据短信,获取SIM卡对应的手机号和卡信息,并记录卡信息与手机号的绑定关系。

[0197] 步骤S903,通过短信网关向SIM卡发送第二数据短信,其中,第二数据短信包括用户信息,用户信息包括手机号。

[0198] 步骤S904,接收SIM卡所在的第一终端通过网关设备发送的第一信息,并基于第一信息中的用户信息对第一终端用户进行身份认证。

[0199] 需要说明的是,在本申请的实施例中,步骤S901—步骤S904的实现过程可参见本申请图1所示的实施例中对应步骤的实现过程的描述,在此不再赘述。

[0200] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,业务系统返回用户信息至SIM卡。当SIM卡所在的第一终端请求访问业务系统时,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定,无需界面搜集用户信息,体验佳。

[0201] 在上述任一实施例的基础上,图10是根据一示例性实施例示出的一种专网安全认证装置的框图,该装置配置于SIM卡。参照图10,该专网安全认证装置可以包括:卡信息上报模块1001和收发模块1002。

[0202] 具体地,卡信息上报模块1001,用于响应于触发卡信息上报操作,通过短信网关向业务系统发送第一数据短信,其中,第一数据短信包括卡信息;

[0203] 卡信息上报模块,还用于接收业务系统通过短信网关发送的第二数据短信,基于第二数据短信,获取并存储用户信息;其中,用户信息包括手机号;

[0204] 收发模块1002,用于接收SIM卡所在的第一终端发送的第一指令,将用户信息发送至第一终端,其中,第一指令指示获取用户信息,第一终端基于用户信息请求业务系统对第一终端用户进行身份认证。

[0205] 在一些实现方式中,卡信息上报模块1001,还用于:

- [0206] 向第一终端注册监听入网事件；
- [0207] 监听到第一终端首次入网鉴权通过事件，触发卡信息上报操作。
- [0208] 在一些实现方式中，卡信息上报模块1001，具体用于：
- [0209] 读取卡信息，并将卡信息组装于第一数据短信的响应数据包中；通过短信网关向业务系统发送第一数据短信。
- [0210] 在一些实现方式中，卡信息上报模块1001，具体用于：
- [0211] 接收短信网关转发的业务系统发送的第二数据短信；其中，第二数据短信包括应用命令报文，应用命令报文包括用户信息；
- [0212] 解密第二数据短信，获取应用命令报文中的短信内容；
- [0213] 解析短信内容，获取并存储用户信息。
- [0214] 在一些实现方式中，收发模块1002，具体用于：
- [0215] 建立与第一终端之间的安全访问通道；
- [0216] 读取用户信息；并加密用户信息，得到用户信息密文；
- [0217] 将用户信息密文通过安全访问通道发送至第一终端。
- [0218] 在一些实现方式中，响应数据包包括卡应用主版本号、安全参数标识定义、应用响应数据包和MAC，应用响应数据包包括卡信息，安全参数标识包括加密标识和环境标识。
- [0219] 在一些实现方式中，卡信息上报模块1001，具体用于：
- [0220] 将用户信息存储于SIM卡的安全存储空间。
- [0221] 关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。
- [0222] 通过实施本实施例，通过SIM卡上报卡信息至专网内的业务系统，并将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时，第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限，实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定，无需界面搜集用户信息，体验佳。通过SIM卡硬介质层面对用户信息进行加密，全程密文传输，实现安全认证。
- [0223] 在上述任一实施例的基础上，图11是根据一示例性实施例示出的一种专网安全认证装置的框图，该装置配置于第一终端，第一终端包括SIM卡。参照图11，该专网安全认证装置可以包括：收发模块1101。
- [0224] 具体地，收发模块1101，用于向专网发送内网应用访问请求，其中，内网应用访问请求指示访问业务系统；
- [0225] 收发模块1101，还用于接收网关设备重定向的身份认证链接，并基于身份认证链接，向客户识别模块SIM卡发送第一指令，其中，第一指令指示获取用户信息，用户信息为业务系统基于SIM卡上报的卡信息发送至SIM卡的，用户信息包括手机号；
- [0226] 收发模块1101，还用于接收SIM卡发送的用户信息，并通过网关设备向业务系统发送第一信息；其中，第一信息包括用户信息，第一终端基于用户信息请求业务系统对第一终端用户进行身份认证。
- [0227] 在一些实现方式中，收发模块1101，还用于：
- [0228] 第一终端向专网发送接入请求，接入请求指示专网验证第一终端的权限。

[0229] 在一些实现方式中,收发模块1101,还用于:

[0230] 接收SIM卡发送的监听入网事件注册请求。

[0231] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0232] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,将业务系统返回的用户信息存储于SIM卡。当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。

[0233] 在上述任一实施例的基础上,图12是根据又一示例性实施例示出的一种专网安全认证装置的框图,该装置配置于网关设备,第一终端包括SIM卡。参照图12,该专网安全认证装置可以包括:接入网关模块1201和控制中心模块1202。

[0234] 具体地,接入网关模块1201,用于拦截第一终端向专网发送的内网应用访问请求,重定向身份认证链接至第一终端;其中,第一终端包括SIM卡,内网应用访问请求指示访问业务系统;

[0235] 控制中心模块1202,用于接收第一终端发送的第一信息,并将第一信息发送至业务系统,其中,第一信息包括用户信息,用户信息为业务系统基于SIM卡上报的卡信息发送至SIM卡的,用户信息包括手机号,第一终端基于用户信息请求业务系统对第一终端用户进行身份认证。

[0236] 其中,代理身份认证请求指示网关设备将用户信息发送至业务系统,用户信息为业务系统基于SIM卡上报的卡信息发送至SIM卡的,用户信息包括手机号。

[0237] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0238] 通过实施本实施例,当SIM卡所在的第一终端请求访问业务系统时,网关设备重定向身份认证,第一终端则将存储于SIM卡的业务系统基于SIM卡上报的卡信息返回的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。通过网关设备重定向进行用户身份信息校验,可覆盖全终端,易于推广。

[0239] 在上述任一实施例的基础上,图13是根据又一示例性实施例示出的一种专网安全认证装置的框图,该装置配置于专网内的业务系统,第一终端包括SIM卡。参照图13,该专网安全认证装置可以包括:收发模块1301、处理模块1302和身份认证模块1303。

[0240] 具体地,收发模块1301,用于接收客户识别模块SIM卡通过短信网关发送的第一数据短信,其中,第一数据短信包括卡信息。

[0241] 处理模块1302,用于基于第一数据短信,获取SIM卡对应的手机号和卡信息,并记录卡信息与手机号的绑定关系。

[0242] 收发模块1301,还用于通过短信网关向SIM卡发送第二数据短信,其中,第二数据短信包括用户信息,用户信息包括手机号。

[0243] 身份认证模块1303,用于接收SIM卡所在的第一终端通过网关设备发送的第一信息,并基于第一信息中的用户信息对第一终端用户进行身份认证。

[0244] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0245] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,业务系统返回用户信息至SIM卡。当SIM卡所在的第一终端请求访问业务系统时,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定,无需界面搜集用户信息,体验佳。

[0246] 在上述任一实施例的基础上,图14是根据一示例性实施例示出的一种专网安全认证系统的框图,参照图14,该专网安全认证系统可以包括:SIM卡1401,SIM卡所在的第一终端1402、短信网关1403、网关设备1404和业务系统1405。

[0247] 具体地,SIM卡1401,被配置为执行图6所示的专网安全认证方法;

[0248] SIM卡所在的第一终端1402,被配置为执行图7所示的专网安全认证方法;

[0249] 网关设备1404,被配置为执行图8所示的专网安全认证方法;

[0250] 业务系统1405,被配置为执行图9所示的专网安全认证方法。

[0251] 通过实施本实施例,通过SIM卡上报卡信息至专网内的业务系统,业务系统返回用户信息至SIM卡。当SIM卡所在的第一终端请求访问业务系统时,第一终端则将存储于SIM卡的用户信息发送至业务系统进行身份认证。实现了专网用户侧自主管理用户通过专网访问业务系统的准入权限,实现了专网企业侧的身份认证管控。业务系统通过SIM卡和短信网关实现用户信息的采集及绑定,无需界面搜集用户信息,体验佳。

[0252] 根据本申请的实施例,本申请还提供了一种电子设备和一种可读存储介质。

[0253] 如图15所示,是根据本申请实施例的用于实现专网安全认证的方法的电子设备的框图。电子设备旨在表示各种形式的数字计算机,诸如,膝上型计算机、台式计算机、工作台、个人数字助理、服务器、刀片式服务器、大型计算机、和其它适合的计算机。电子设备还可以表示各种形式的移动装置,诸如,个人数字处理、蜂窝电话、智能电话、可穿戴设备和其它类似的计算装置。本文所示的部件、它们的连接和关系、以及它们的功能仅作为示例,并且不意在限制本文中描述的和/或者要求的本申请的实现。

[0254] 如图15所示,该电子设备包括:一个或多个处理器1501、存储器1502,以及用于连接各部件的接口,包括高速接口和低速接口。各个部件利用不同的总线互相连接,并且可以被安装在公共主板上或者根据需要以其它方式安装。处理器可以对在电子设备内执行的指令进行处理,包括存储在存储器中或者存储器上以在外部输入/输出装置(诸如,耦合至接口的显示设备)上显示GUI的图形信息的指令。在其它实施方式中,若需要,可以将多个处理器和/或多条总线与多个存储器和多个存储器一起使用。同样,可以连接多个电子设备,各个设备提供部分必要的操作(例如,作为服务器阵列、一组刀片式服务器、或者多处理器系统)。图15中以一个处理器1501为例。

[0255] 存储器1502即为本申请所提供的非瞬时计算机可读存储介质。其中,所述存储器存储有可由至少一个处理器执行的指令,以使所述至少一个处理器执行本申请所提供的专网安全认证的方法。本申请的非瞬时计算机可读存储介质存储计算机指令,该计算机指令用于使计算机执行本申请所提供的专网安全认证的方法。

[0256] 存储器1502作为一种非瞬时计算机可读存储介质,可用于存储非瞬时软件程序、

非瞬时计算机可执行程序以及模块,如本申请实施例中的专网安全认证的方法对应的程序指令/模块(例如,附图12所示的接入网关模块1201和控制中心模块1202)。处理器1501通过运行存储在存储器1502中的非瞬时软件程序、指令以及模块,从而执行服务器的各种功能应用以及数据处理,即实现上述方法实施例中的专网安全认证的方法。

[0257] 存储器1502可以包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需要的应用程序;存储数据区可存储根据专网安全认证的电子设备的使用所创建的数据等。此外,存储器1502可以包括高速随机存取存储器,还可以包括非瞬时存储器,例如至少一个磁盘存储器件、闪存器件、或其他非瞬时固态存储器件。在一些实施例中,存储器1502可选包括相对于处理器1501远程设置的存储器,这些远程存储器可以通过网络连接至专网安全认证的电子设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0258] 专网安全认证的方法的电子设备还可以包括:输入装置1503和输出装置1504。处理器1501、存储器1502、输入装置1503和输出装置1504可以通过总线或者其他方式连接,图15中以通过总线连接为例。

[0259] 输入装置1503可接收输入的数字或字符信息,以及产生与专网安全认证的电子设备的用户设置以及功能控制有关的键信号输入,例如触摸屏、小键盘、鼠标、轨迹板、触摸板、指示杆、一个或者多个鼠标按钮、轨迹球、操纵杆等输入装置。输出装置1504可以包括显示设备、辅助照明装置(例如,LED)和触觉反馈装置(例如,振动电机)等。该显示设备可以包括但不限于,液晶显示器(LCD)、发光二极管(LED)显示器和等离子体显示器。在一些实施方式中,显示设备可以是触摸屏。

[0260] 此处描述的系统和技术各种实施方式可以在数字电子电路系统、集成电路系统、专用ASIC(专用集成电路)、计算机硬件、固件、软件、和/或它们的组合中实现。这些各种实施方式可以包括:实施在一个或者多个计算机程序中,该一个或者多个计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释,该可编程处理器可以是专用或者通用可编程处理器,可以从存储系统、至少一个输入装置、和至少一个输出装置接收数据和指令,并且将数据和指令传输至该存储系统、该至少一个输入装置、和该至少一个输出装置。

[0261] 这些计算程序(也称作程序、软件、软件应用、或者代码)包括可编程处理器的机器指令,并且可以利用高级过程和/或面向对象的编程语言、和/或汇编/机器语言来实施这些计算程序。如本文使用的,术语“机器可读介质”和“计算机可读介质”指的是用于将机器指令和/或数据提供给可编程处理器的任何计算机程序产品、设备、和/或装置(例如,磁盘、光盘、存储器、可编程逻辑装置(PLD)),包括,接收作为机器可读信号的机器指令的机器可读介质。术语“机器可读信号”指的是用于将机器指令和/或数据提供给可编程处理器的任何信号。

[0262] 为了提供与用户的交互,可以在计算机上实施此处描述的系统和技术,该计算机具有:用于向用户显示信息的显示装置(例如,CRT(阴极射线管)或者LCD(液晶显示器)监视器);以及键盘和指向装置(例如,鼠标或者轨迹球),用户可以通过该键盘和该指向装置来将输入提供给计算机。其它种类的装置还可以用于提供与用户的交互;例如,提供给用户的反馈可以是任何形式的传感反馈(例如,视觉反馈、听觉反馈、或者触觉反馈);并且可以用

任何形式(包括声输入、语音输入或者、触觉输入)来接收来自用户的输入。

[0263] 可以将此处描述的系统和技术实施在包括后台部件的计算系统(例如,作为数据服务器)、或者包括中间件部件的计算系统(例如,应用服务器)、或者包括前端部件的计算系统(例如,具有图形用户界面或者网络浏览器的用户计算机,用户可以通过该图形用户界面或者该网络浏览器来与此处描述的系统和技术实施方式交互)、或者包括这种后台部件、中间件部件、或者前端部件的任何组合的计算系统中。可以通过任何形式或者介质的数字数据通信(例如,通信网络)来将系统的部件相互连接。通信网络的示例包括:局域网(LAN)、广域网(WAN)和互联网。

[0264] 计算机系统可以包括客户端和服务器。客户端和服务器一般远离彼此并且通常通过通信网络进行交互。通过在相应的计算机上运行并且彼此具有客户端-服务器关系的计算机程序来产生客户端和服务器的关系。

[0265] 在示例性实施例中,还提供了一种计算机程序产品,当计算机程序产品中的指令由电子设备的处理器执行时,使得电子设备能够执行上述方法。

[0266] 还需要说明的是,本发明中提及的示例性实施例,基于一系列的步骤或者装置描述一些方法或系统。但是,本发明不局限于上述步骤的顺序,也就是说,可以按照实施例中提及的顺序执行步骤,也可以不同于实施例中的顺序,或者若干步骤同时执行。

[0267] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的。

[0268] 应当理解的是,本申请并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

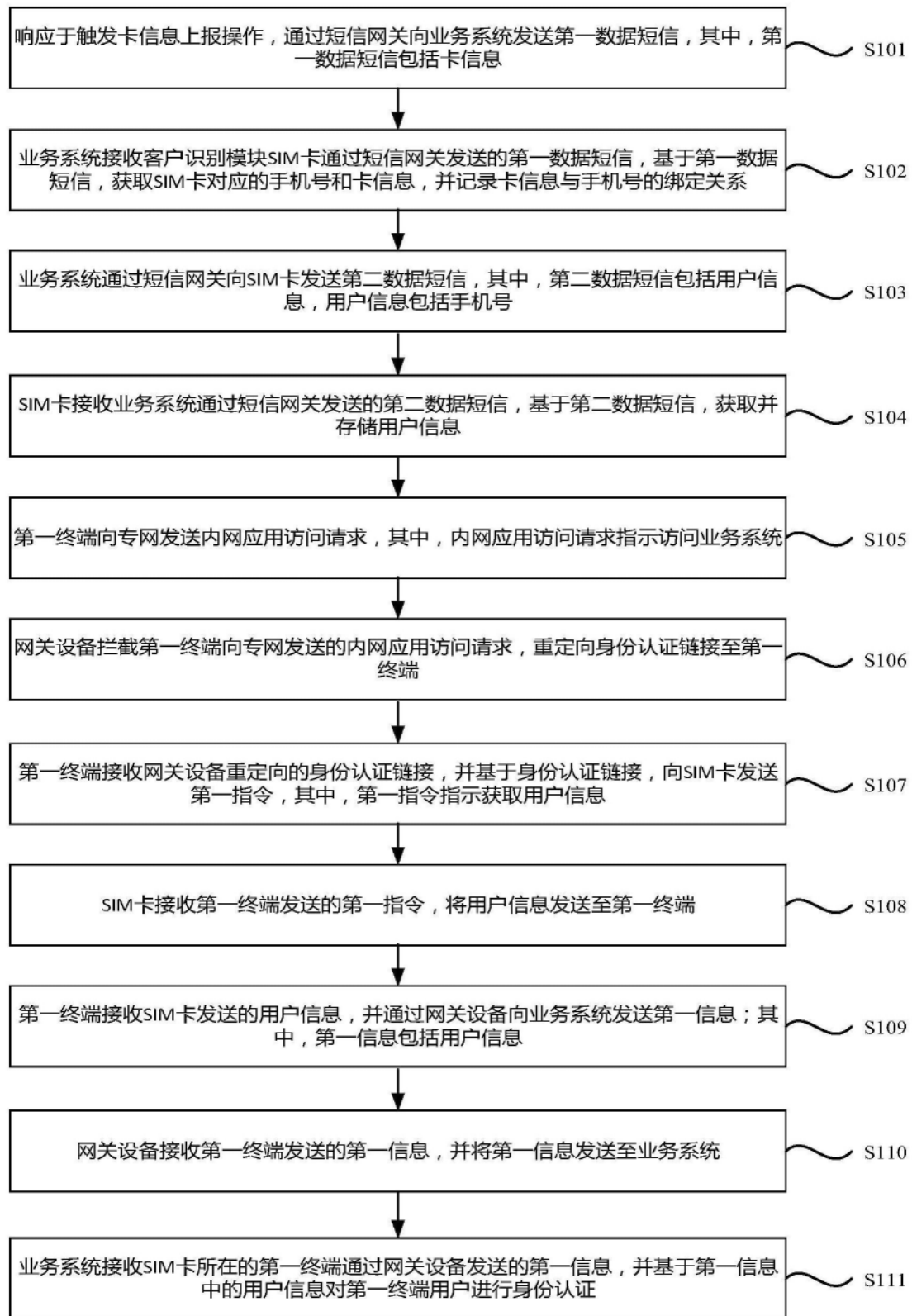


图1



图2

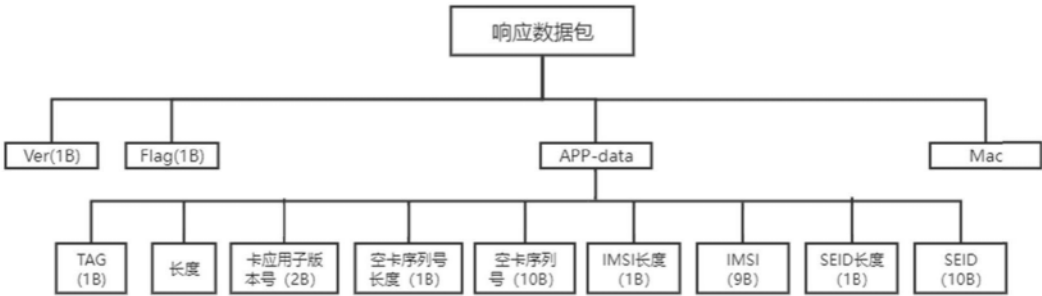


图3



图4

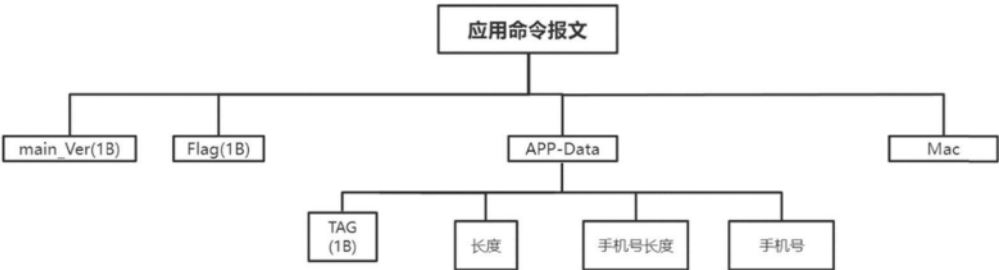


图5

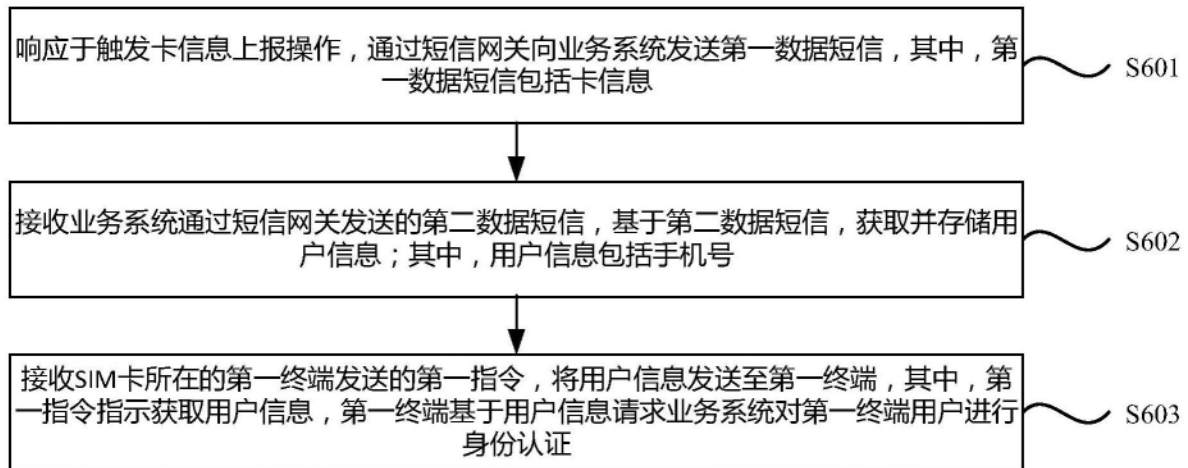


图6

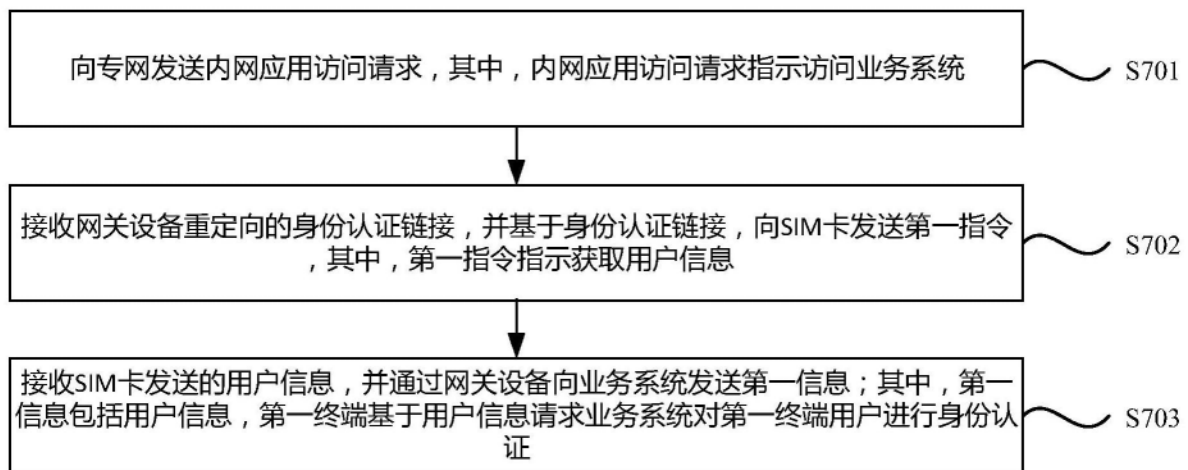


图7

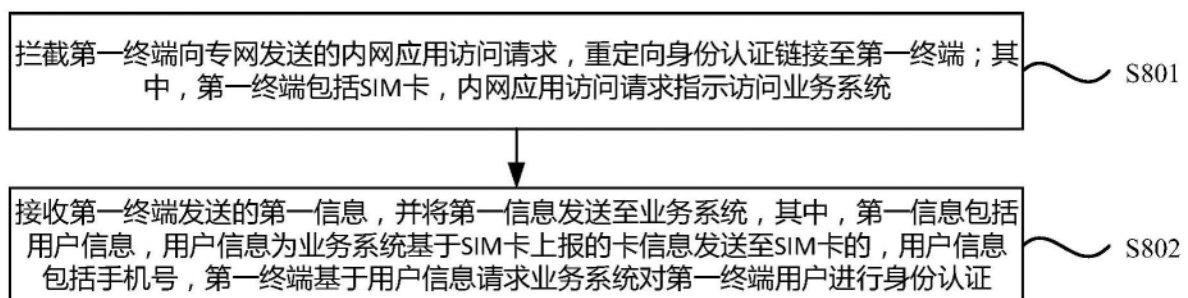


图8

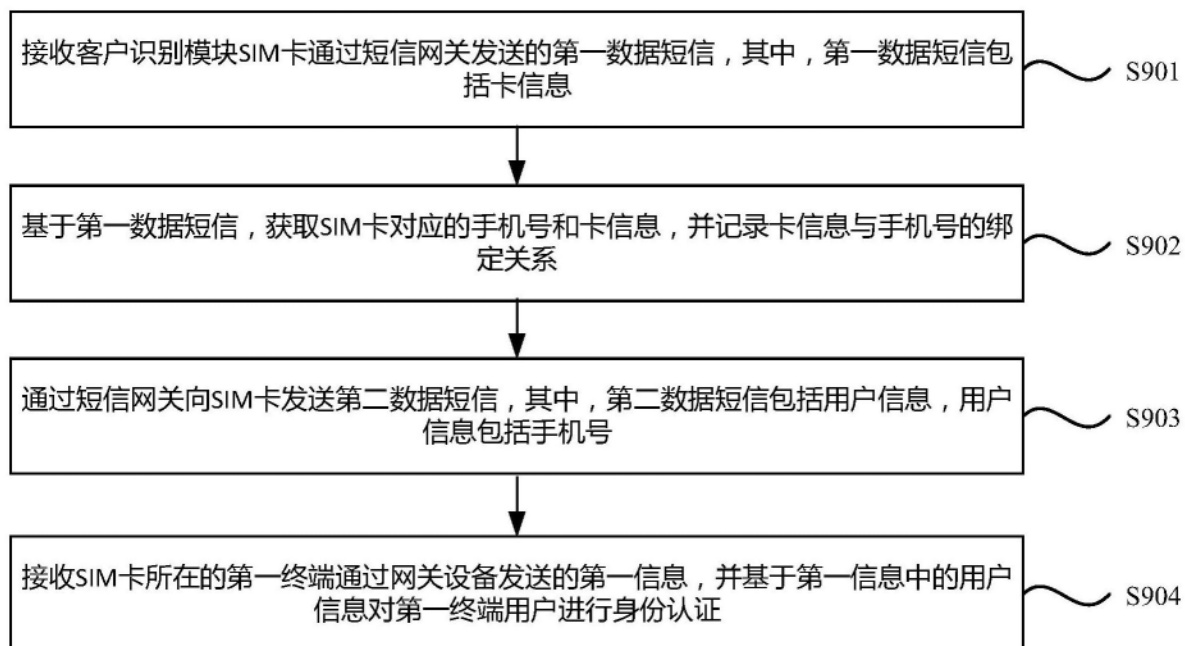


图9

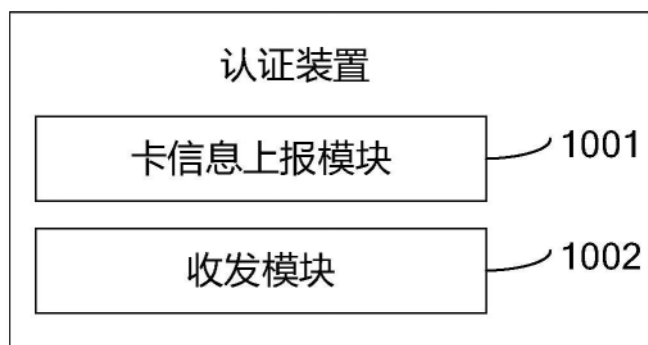


图10

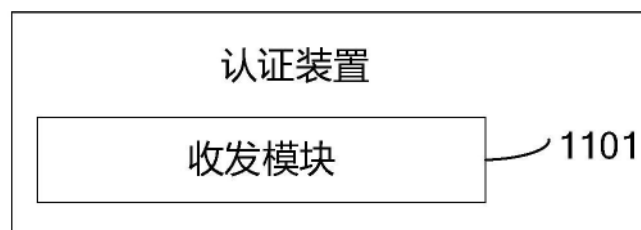


图11

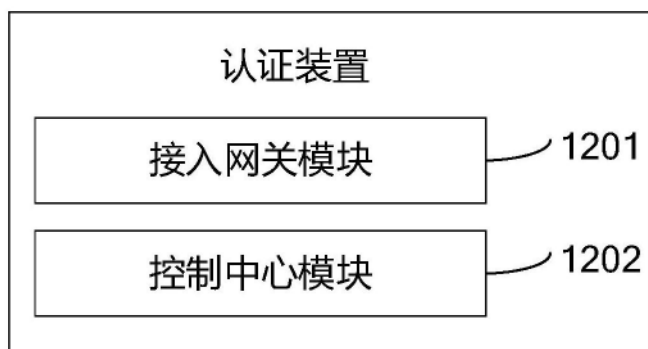


图12

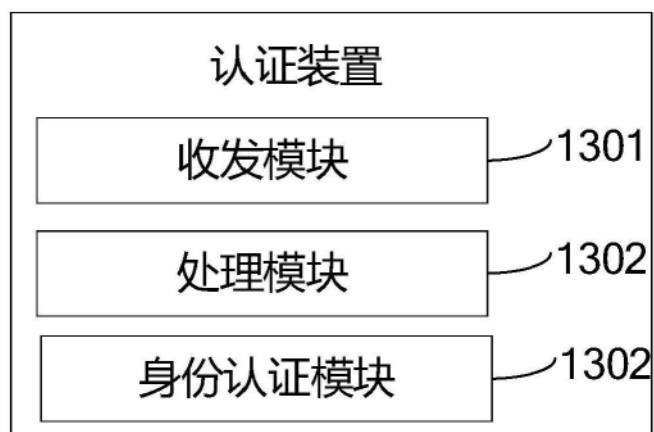


图13

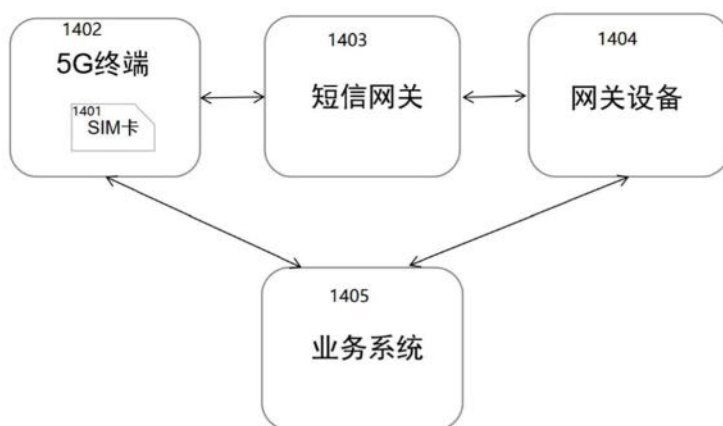


图14

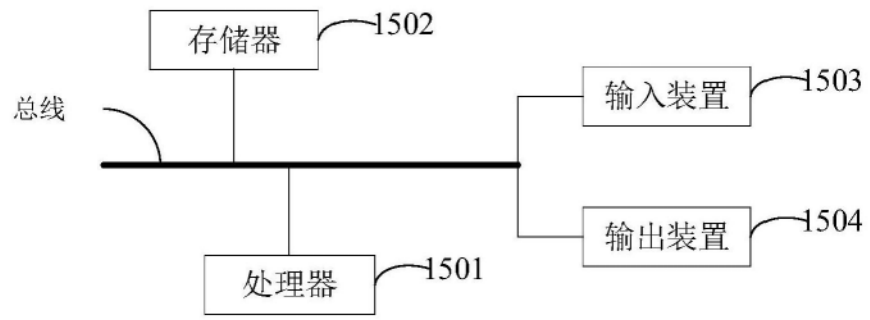


图15