

权利要求书

1. 一种身份认证系统，其特征在于，包括：

第一设备，用于通过互联网获取加密信息，使用所述加密信息对登录第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至所述第二设备；

5 所述第二设备，与所述第一设备建立通信连接，用于基于验证信息来验证所述加密后的身份信息，得到验证结果，并将验证结果返回至所述第一设备；

其中，所述第一设备为允许访问互联网的设备，所述第二设备为不允许访问互联网的设备。

2. 根据权利要求 1 所述的系统，其特征在于，所述系统还包括：

10 服务器，与所述第一设备通信，用于接收所述第一设备发起的登录请求，并根据所述登录请求生成所述加密信息，其中，所述加密信息包括如下至少之一：密钥对和数字证书。

3. 一种身份认证方法，其特征在于，包括：

15 第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，所述第二设备为不允许访问互联网的设备；

所述第一设备使用所述加密信息对登录所述第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至所述第二设备；

所述第一设备接收所述第二设备返回的验证结果，其中，所述第二设备基于验证信息来验证所述加密后的身份信息。

20 4. 根据权利要求 3 所述的方法，其特征在于，所述第一设备使用所述加密信息对登录所述第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至所述第二设备，包括：

所述第一设备获取登录账号，并接收认证服务器返回的所述加密信息，其中，所述加密信息包括如下至少之一：密钥对和数字证书；

25 所述第一设备根据所述登录账号和所述加密信息，生成所述加密后的身份信息；

所述第一设备发送所述加密后的身份信息至所述第二设备。

5. 根据权利要求 4 所述的方法，其特征在于，所述第一设备根据所述登录账号和所述加密信息，生成所述加密后的身份信息包括：

30 所述第一设备使用所述密钥对中的私钥对所述登录账号和/或随机数进行加密，得到加密结果；

所述第一设备基于所述登录账号,以及如下至少之一的信息生成所述加密后的身份信息:所述加密结果和所述数字证书。

6. 根据权利要求 5 所述的方法,其特征在于,所述第一设备使用所述密钥对中的私钥对所述登录账号和/或随机数进行加密,得到加密结果,包括:

5 所述第一设备获取第一随机数;

所述第一设备使用所述密钥对中的私钥对所述登录账号和所述第一随机数进行加密,得到加密结果。

7. 根据权利要求 3 所述的方法,其特征在于,在所述第一设备使用所述加密信息对登录所述第二设备的账户的身份信息进行加密,并将加密后的身份信息发送至所述第二设备之前,所述方法还包括:

所述第一设备向认证服务器发起登录请求,其中,所述认证服务器根据所述登录请求生成所述加密信息,其中,所述加密信息包括如下至少之一:密钥对和数字证书。

8. 根据权利要求 3 所述的方法,其特征在于,所述第一设备通过如下任意一种通信方式与第二设备建立通信连接:传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、
15 WiFi。

9. 根据权利要求 6 所述的方法,其特征在于,所述第一设备发送所述加密后的身份信息至所述第二设备,包括:

所述第一设备将所述加密后的身份信息添加所述第一设备的数字签名;

所述第一设备将添加数字签名后的身份信息发送至所述第二设备。

10. 根据权利要求 9 所述的方法,其特征在于,在所述第一设备将添加数字签名后的身份信息发送至所述第二设备之后,所述方法还包括:

所述第二设备基于预先安装的根证书,判断所述添加数字签名后的身份信息中包含的数字证书是否可信;

在所述数字证书不可信的情况下,所述第一设备接收所述第二设备返回的身份验证失败的结果。

11. 根据权利要求 10 所述的方法,其特征在于,在所述数字证书可信的情况下,所述方法还包括:

在所述数字证书可信的情况下,所述第二设备提取所述数字证书中包含的公钥,并通过所述数字签名验证接收到的数据是否被篡改;

在所述接收到的数据被篡改的情况下,所述第一设备接收所述第二设备返回的身份

验证失败的结果。

12. 根据权利要求 11 所述的方法，其特征在于，在所述接收到的数据未被篡改的情况下，所述方法还包括：

所述第二设备利用所述公钥对所述加密结果进行解密，得到所述登录账号和/或所述
5 第一随机数；

所述第二设备判断所述登录账号是否存在于可信任列表中，其中，所述可信任列表包含允许登录所述第二设备的至少一个账户；

在所述登录账号不存在于所述可信任列表的情况下，所述第一设备接收所述第二设备返回的身份验证失败的结果。

10 13. 根据权利要求 12 所述的方法，其特征在于，在所述登录账号存在于所述可信任列表的情况下，所述方法还包括：

所述第一设备根据所述第一随机数和所述认证服务器返回的第二随机数，生成共享密钥，其中，所述第二随机数为所述第二设备在所述登录账号存在于所述可信任列表的情况下，所述第二设备生成的随机数；

15 其中，所述第二设备根据所述第一随机数和所述第二随机数，生成所述共享密钥。

14. 根据权利要求 12 所述的方法，其特征在于，所述方法包括：

所述第二设备判断所述可信任列表中是否存在登录账号；

在所述可信任列表中不存在登录账号的情况下，所述第二设备将解密得到的所述登录账号作为管理账号，并添加到所述可信任列表中，其中，所述管理账号用于管理所述
20 可信任列表中的至少一个登录账号。

15. 一种身份认证方法，其特征在于，包括：

第二设备与第一设备建立通信连接，并接收所述第一设备传输的待验证的身份信息，其中，所述第一设备为允许访问互联网的设备，所述第二设备为不允许访问互联网的设备；

25 所述第二设备基于验证信息来验证所述第一设备传输的待验证的身份信息，得到验证结果；

其中，所述待验证的身份信息为使用加密信息加密后的数据。

16. 一种身份认证方法，其特征在于，包括：

30 第二设备接收来自第一设备传输的待验证的身份信息，其中，所述第一设备为允许访问互联网的设备，所述第二设备为不允许访问互联网的设备；

所述第二设备根据验证信息验证所述待验证的身份信息，得到验证结果；

在所述验证结果为所述身份信息可信的情况下，生成用于加解密数据的共享密钥，其中，所述共享密钥用于保证所述第二设备和所述第一设备之间进行安全数据传输；

其中，所述待验证的身份信息为使用加密信息加密后的数据。

- 5 17. 根据权利要求 16 所述的方法，其特征在于，在第二设备接收来自第一设备传输的待验证的身份信息之前，所述方法还包括：

所述第一设备获取登录账号，并接收认证服务器返回的所述加密信息，其中，所述加密信息包括如下至少之一：密钥对和数字证书；

所述第一设备根据所述登录账号和所述加密信息，生成所述待验证的身份信息；

- 10 所述第一设备发送所述待验证的身份信息至所述第二设备。

18. 根据权利要求 17 所述的方法，其特征在于，所述第二设备通过如下任意一种通信方式接收所述第一设备发送的所述待验证的身份信息：传输控制协议 TCP、用户数据报协议 UDP、蓝牙、Zigbee、WiFi。

- 15 19. 根据权利要求 17 所述的方法，其特征在于，在所述第一设备获取登录账号，并接收服务器返回的认证服务器返回的所述加密信息之前，所述方法还包括：

所述第一设备向所述认证服务器发起登录请求，其中，所述认证服务器根据所述登录请求生成所述加密信息。

20. 根据权利要求 17 所述的方法，其特征在于，所述第一设备根据所述登录账号和所述加密信息，生成所述待验证的身份信息，包括：

- 20 所述第一设备使用所述密钥对中的私钥对所述登录账号和/或随机数进行加密，得到加密结果；

所述第一设备基于所述登录账号，以及如下至少之一的信息生成所述待验证的身份信息：所述加密结果和所述数字证书。

- 25 21. 根据权利要求 20 所述的方法，其特征在于，所述第一设备使用所述密钥对中的私钥对所述登录账号和/或随机数进行加密，得到加密结果，包括：

所述第一设备获取第一随机数；

所述第一设备使用所述密钥对中的私钥对所述登录账号和所述第一随机数进行加密，得到加密结果。

- 30 22. 根据权利要求 21 所述的方法，其特征在于，所述第一设备发送所述待验证的身份信息至所述第二设备，包括：

所述第一设备将所述待验证的身份信息添加所述第一设备的数字签名；

所述第一设备将添加数字签名后的身份信息发送至所述第二设备。

23. 根据权利要求 22 所述的方法，其特征在于，所述第二设备根据验证信息验证所述第一设备传输的待验证的身份信息，得到验证结果，包括：

5 所述第二设备基于预先安装的根证书，判断所述待验证的身份信息中包含的数字证书是否可信；

在所述数字证书不可信的情况下，所述第二设备向所述第一设备返回身份验证失败的结果。

24. 根据权利要求 23 所述的方法，其特征在于，在所述数字证书可信的情况下，所述方法还包括：

10 在所述数字证书可信的情况下，所述第二设备提取所述数字证书中包含的公钥，并通过所述数字签名验证接收到的数据是否被篡改；

在所述接收到的数据被篡改的情况下，所述第二设备向所述第一设备返回身份验证失败的结果。

15 25. 根据权利要求 24 所述的方法，其特征在于，在所述接收到的数据未被篡改的情况下，所述方法还包括：

所述第二设备利用所述公钥对所述加密结果进行解密，得到所述登录账号和/或所述第一随机数；

20 所述第二设备判断所述登录账号是否存在于可信任列表中，其中，所述可信任列表包含允许登录所述第二设备的至少一个账户；

在所述登录账号不存在于所述可信任列表的情况下，所述第二设备向所述第一设备返回身份验证失败的结果。

26. 根据权利要求 25 所述的方法，其特征在于，在所述登录账号存在于所述可信任列表的情况下，所述第二设备确定所述第一设备传输的身份信息为可信的验证结果。

25 27. 根据权利要求 26 所述的方法，其特征在于，在所述登录账号存在于所述可信任列表的情况下，所述第二设备确定所述第一设备传输的身份信息为可信的验证结果之后，所述方法还包括：

所述第二设备获取第二随机数，并根据所述第一随机数和所述第二随机数生成所述共享密钥；

30 其中，所述第一设备根据所述第一随机数和所述认证服务器返回的所述第二随机

数，生成所述共享密钥。

28. 根据权利要求 25 所述的方法，其特征在于，在所述第二设备利用所述公钥对所述加密结果进行解密，得到所述登录账号和/或所述第一随机数之后，所述方法包括：

所述第二设备判断所述可信任列表中是否存在登录账号；

- 5 在所述可信任列表中不存在登录账号的情况下，所述第二设备将解密得到的所述登录账号作为管理账号，并添加到所述可信任列表中，其中，所述管理账号用于管理所述可信任列表中的至少一个登录账号。

29. 一种计算设备，其特征在于，包括：

- 10 通信装置，与控制设备建立通信连接，用于接收来自控制设备传输的待验证的身份信息，其中，所述控制设备为允许访问互联网的设备；

处理器，与所述通信装置连接，用于根据验证信息，验证所述控制设备传输的待验证的身份信息，得到验证结果，并在所述验证结果为所述身份信息可信的情况下，生成用于加解密数据的共享密钥，其中，所述共享密钥用于保证所述通信装置和所述控制设备之间进行安全数据传输。

- 15 30. 一种存储介质，其特征在于，所述存储介质包括存储的程序，其中，在所述程序运行时控制所述存储介质所在设备执行权利要求 3 至 14 中任意一项所述的身份认证方法。

31. 一种计算终端，其特征在于，包括：处理器，所述处理器用于运行程序，其中，所述程序运行时执行权利要求 3 至 14 中任意一项所述的身份认证方法。

- 20 32. 一种身份认证系统，其特征在于，包括：

处理器；以及

存储器，与所述处理器连接，用于为所述处理器提供处理以下处理步骤的指令：

第一设备与第二设备建立通信连接，并通过互联网获取加密信息，其中，所述第一设备为允许访问互联网的设备，所述第二设备为不允许访问互联网的设备；

- 25 所述第一设备使用所述加密信息对登录所述第二设备的账户的身份信息进行加密，并将加密后的身份信息发送至所述第二设备；

所述第一设备接收所述第二设备返回的验证结果，其中，所述第二设备基于验证信息来验证所述加密后的身份信息。