

权利要求书

- 1、一种生物支付设备的认证方法，所述方法包括：
- 获取设备的密钥，其中，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；
- 根据所述密钥和设备信息生成签名；及
- 5 基于所述设备信息和所述签名向支付认证服务器发送认证请求，所述认证请求指示所述支付认证服务器根据所述设备信息对所述签名进行验证，并根据验证结果生成对所述生物支付设备的认证结果；
- 接收所述支付认证服务器返回认证结果，所述认证结果使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物支付。
- 10 2、根据权利要求1所述的方法，其特征在于，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：
- 根据密钥生产指令生成公钥和私钥；及
- 导出所述公钥至生产商设备，由所述生产商设备上传所述公钥至所述支付认证服务器。
- 15 3、根据权利要求1所述的方法，其特征在于，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：
- 将多因子设备信息导出至生产商设备，通过所述生产商设备将所述多因子设备信息发送至支付认证服务器，由支付认证服务器根据所述多因子信息生成存储所述生物支付设备的密钥的动态链接库文件；及
- 20 响应所述生产商设备的烧录指令，将所述支付认证服务器返回的动态链接库文件烧录至本地。
- 4、根据权利要求2所述的方法，其特征在于，所述根据密钥生产指令生成公钥和私钥，包括：根据密钥生产指令控制生物支付设备的安全芯片生成公钥和私钥；
- 25 所述根据所述密钥和设备信息生成签名，包括：控制所述安全芯片根据所述私钥和所述设备信息生成签名。

5、根据权利要求2所述的方法，其特征在于，所述根据密钥生产指令生成公钥和私钥，包括：根据密钥生产指令，基于可执行环境生成公钥和私钥；

所述根据所述密钥和设备信息生成签名，包括：基于所述可执行环境根据所述私钥和所述设备信息生成签名。

5 6、根据权利要求3所述的方法，其特征在于，所述动态链接库文件为混淆和加固的动态链接库文件，所述根据所述密钥和设备信息生成签名，包括：根据混淆和加固的动态链接库文件所存储的密钥对所述设备信息进行加密生成签名。

10 7、一种生物支付设备的认证方法，包括：

接收生物支付设备基于签名和设备信息发送的认证请求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

根据所述设备信息对所述签名进行验证；

15 根据验证结果生成对所述生物支付设备的认证结果；及

向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

8、根据权利要求7所述的方法，其特征在于，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：

20 获取所述生产商设备上传的所述生物支付设备的公钥，其中，所述公钥以及所述公钥对应的私钥根据密钥生产指令生成，所述公钥被导出至生产商设备。

9、根据权利要求7所述的方法，其特征在于，生产阶段通过生产商设备与支付认证服务器通信而获得被支付认证服务器认可的密钥的方式，包括：

25 获取所述生产商设备上传的所述生物支付设备的多因子信息；

根据所述多因子信息生成存储所述生物支付设备的密钥的动态链接库文件；及

将所述动态链接库文件发送至生产商设备，所述动态链接库文件指示所述生产商设备将所述动态链接库文件烧录至所述生物支付设备。

10、根据权利要求 8 所述的方法，其特征在于，所述根据所述设备信息对所述签名进行验证，包括：获取对应的公钥，根据所述设备信息和所述公
5 钥对所述签名进行验证。

11、根据权利要求 9 所述的方法，其特征在于，所述方法还包括：
对存储有所述密钥的所述动态链接库文件进行混淆和加固处理。

12、一种生物支付设备的认证装置，其特征在于，所述装置包括：
10 密钥获取模块，用于获取设备的密钥，其中，所述密钥是生产阶段通过
生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；
签名模块，用于根据所述密钥和设备信息生成签名；
认证模块，用于基于所述设备信息和所述签名向支付认证服务器发送认
证请求，所述认证请求指示所述支付认证服务器根据所述设备信息对所述签
15 名进行验证，并根据验证结果生成对所述生物支付设备的认证结果；
接收模块，用于接收所述支付认证服务器返回认证结果，所述认证结果
使所述支付认证服务器基于已认证的生物支付设备发送的生物数据实现生物
支付。

13、根据权利要求 12 所述的装置，其特征在于，所述密钥获取模块，包
20 括：

密钥生成模块，用于根据密钥生产指令生成公钥和私钥；

密钥导出模块，用于导出所述公钥至生产商设备，由所述生产商设备上
传所述公钥至所述支付认证服务器。

14、根据权利要求 12 所述的装置，其特征在于，所述密钥获取模块，包
25 括：

设备信息导出模块，用于将多因子设备信息导出至生产商设备，通过所
述生产商设备将所述多因子设备信息发送至支付认证服务器，由支付认证服

务器根据所述多因子信息生成存储所述生物支付设备的密钥的动态链接库文件；

密钥导入模块，用于响应所述生产商设备的烧录指令，将所述支付认证服务器返回的动态链接库文件烧录至本地。

- 5 15、根据权利要求 13 所述的装置，其特征在于，所述密钥生成模块，用于根据密钥生产指令控制生物支付设备的安全芯片生成公钥和私钥；

所述签名模块，用于控制所述安全芯片根据所述私钥和所述设备信息生成签名。

- 10 16、根据权利要求 13 所述的装置，其特征在于，所述密钥生成模块，用于根据密钥生产指令，基于可执行环境生成公钥和私钥；

所述签名模块，用于基于所述可执行环境根据所述私钥和所述设备信息生成签名。

- 15 17、根据权利要求 14 所述的装置，其特征在于，所述签名模块，用于根据混淆和加固的动态链接库文件所存储的密钥对所述设备信息进行加密生成签名。

18、一种生物支付设备的认证装置，包括：

- 20 认证获取模块，用于接收生物支付设备基于签名设备信息发送的认证请求，其中，所述签名由所述生物支付设备根据密钥和设备信息生成，所述密钥是生产阶段通过生产商设备与支付认证服务器通信而获得的被支付认证服务器认可的密钥；

验证模块，用于根据所述设备信息对所述签名进行验证；

认证模块，用于根据验证结果生成对所述生物支付设备的认证结果；

- 25 发送模块，用于向所述生物支付设备返回认证结果，以基于已认证的生物支付设备发送的生物数据实现生物支付。

19、根据权利要求 18 所述的装置，其特征在于，还包括：

密钥获取模块，用于获取所述生产商设备上传的所述生物支付设备的公

钥，其中，所述公钥以及所述公钥对应的私钥根据密钥生产指令生成，所述公钥被导出至生产商设备。

20、根据权利要求 18 所述的装置，其特征在于，还包括：

设备信息获取模块，用于获取所述生产商设备上传的所述生物支付设备
5 的多因子信息；

密钥生成模块，用于根据所述多因子信息生成存储所述生物支付设备的
密钥的动态链接库文件；

密钥发送模块，用于将所述动态链接库文件发送至生产商设备，所述动
态链接库文件指示所述生产商设备将所述动态链接库文件烧录至所述生物支
10 付设备。

21、根据权利要求 19 所述的装置，其特征在于，所述验证模块，用于获
取对应的公钥，根据所述设备信息和所述公钥对所述签名进行验证。

22、根据权利要求 20 所述的装置，其特征在于，还包括密钥处理模块，
用于对存储有所述密钥的所述动态链接库文件进行混淆和加固处理。

15

23、一种计算机设备，包括存储器和处理器，所述存储器存储有计算机
程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求 1 至 11
中任一项所述方法的步骤。

24、一种计算机可读存储介质，存储有计算机程序，其特征在于，所述
20 计算机程序被处理器执行时实现权利要求 1 至 11 中任一项所述的方法的步
骤。

25、一种计算机程序，所述计算机程序包括计算机指令，所述计算机指
令存储在计算机可读存储介质中，其特征在于，计算机设备的处理器从所述
计算机可读存储介质读取所述计算机指令，所述处理器执行所述计算机指令，
25 使得所述计算机设备执行上述权利要求 1 至 11 中任一项所述的方法的步骤。