(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105227537 A
(43)申请公布日 2016.01.06

(21)申请号 201410723599.1

(22)申请日 2014.12.02

(66)本国优先权数据
201410268505.6 2014.06.16 CN

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 方成方 朱成康

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)

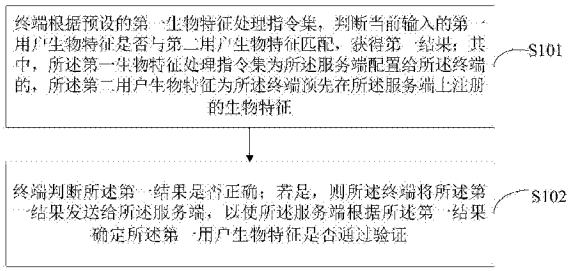
权利要求书5页 说明书22页 附图9页

(54)发明名称

用户身份认证方法、终端和服务端

(57)摘要

本发明实施例提供一种用户身份认证方法、终端和服务端。该方法包括：终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为所述服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；所述终端判断所述第一结果是否正确；若是，则所述终端将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。本发明实施例提供的方法，不仅提高了服务端进行用户身份验证时的安全性，而且避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私。



CN 105227537 A

1. 一种用户身份认证方法，其特征在于，包括：

终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

所述终端判断所述第一结果是否正确，其中，所述终端判断所述第一结果是否正确具体包括当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；

若是，则所述终端将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

2. 根据权利要求 1 所述的方法，其特征在于，所述终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果，具体包括：

所述终端接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文；

所述终端根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥；

所述终端根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

3. 根据权利要求 2 所述的方法，其特征在于，所述终端判断所述第一结果是否正确，具体包括：

所述终端根据预设的第二用户公钥判断所述第一签名是否正确；

若是，所述终端将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

4. 根据权利要求 2 所述的方法，其特征在于，所述终端根据当前输入的第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥，具体包括：

所述终端根据所述第二用户生物特征安全梗概和所述第一用户生物特征，获取第一生物特征编码；

所述终端根据所述第一生物特征编码的哈希值解密所述第二用户密钥密文，获得所述第一用户密钥。

5. 根据权利要求 3 所述的方法，其特征在于，所述终端根据预设的第二用户公钥判断所述第一签名是否正确，具体包括：

所述终端根据所述第二用户公钥判断所述第一签名是否与第三签名相同；所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

6. 根据权利要求 1-5 任一项所述的方法，其特征在于，所述终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果之前，还包括：

所述终端根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上；其中，所述第二生物特征处理指令集为所述服务端配置给所述终端的。

7. 根据权利要求 6 所述的方法，其特征在于，所述终端根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上，包括：

所述终端产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥；

所述终端接收用户输入的第二用户生物特征；

所述终端根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概；

所述终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

8. 根据权利要求 7 所述的方法，其特征在于，所述终端产生用户公钥密钥对之前，所述方法还包括：

所述终端向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

所述终端接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥；

所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

9. 根据权利要求 8 所述的方法，其特征在于，所述终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概之后，所述方法还包括：

所述终端根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

所述终端根据所述装置公钥判断所述第二签名是否正确；

若正确，则所述终端将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

10. 一种用户身份认证方法，其特征在于，包括：

服务端预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

所述服务端接收所述终端发送的所述第一结果；

所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

11. 根据权利要求 10 所述的方法，其特征在于，所述服务端接收所述终端发送的所述第一结果之前，还包括：

所述服务端向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

12. 根据权利要求 11 所述的方法，其特征在于，所述服务端接收所述终端发送的所述第一结果，具体包括：

所述服务端接收所述终端发送的所述第一签名和所述第二用户公钥；

则所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证，具体包

括：

所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

13. 根据权利要求 12 所述的方法，其特征在于，所述服务端预先将第一生物特征处理指令集配置给终端之前，所述方法还包括：

所述服务端将第二生物特征处理指令集配置给所述终端；

所述服务端接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

所述服务端将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

所述服务端接收所述终端发送的第二签名；

所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

14. 根据权利要求 13 所述的方法，其特征在于，所述服务端将装置密钥密文和装置公钥发送给所述终端，具体包括：

所述服务端产生装置公钥密钥对；其中，所述装置公钥密钥对包括所述装置公钥和所述装置密钥；

所述服务端根据所述用户账户口令的哈希值加密所述装置密钥，生成装置密钥密文；

所述服务端将所述装置密钥密文和所述装置公钥发送给所述终端。

15. 根据权利要求 12 所述的方法，其特征在于，所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证，具体包括：

所述服务端根据所述第二用户公钥判断所述第一签名是否与第三签名相同；其中，所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

16. 一种终端，其特征在于，包括：

获取模块，用于根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

判断模块，用于判断所述第一结果是否正确，其中，所述第一结果正确包括当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；

发送模块，用于在所述判断模块判断所述第一结果正确时，将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

17. 根据权利要求 16 所述的终端，其特征在于，所述获取模块，包括：

第一接收单元，用于接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文；

第一获取单元，用于根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二

用户密钥；

第二获取单元，用于根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

18. 根据权利要求 17 所述的终端，其特征在于，所述判断模块，具体用于根据预设的第二用户公钥判断所述第一签名是否正确；

则所述发送模块，具体用于若所述判断模块判断所述第一签名正确时，将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

19. 根据权利要求 17 所述的终端，其特征在于，所述第一获取单元，具体用于根据所述第二用户生物特征安全梗概和所述第一用户生物特征，获取第一生物特征编码；并根据所述第一生物特征编码的哈希值解密所述第二用户密钥密文，获得所述第一用户密钥。

20. 根据权利要求 18 所述的终端，其特征在于，所述判断模块，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

21. 根据权利要求 16-20 任一项所述的终端，其特征在于，所述终端还包括：

注册模块，用于在所述获取模块根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果之前，根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上；其中，所述第二生物特征处理指令集为所述服务端配置给所述终端的。

22. 根据权利要求 21 所述的终端，其特征在于，所述注册模块，包括：

生成单元，用于产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥；

第二接收单元，用于接收用户输入的第二用户生物特征；

第三获取单元，用于根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概；

保存单元，用于保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

23. 根据权利要求 22 所述的终端，其特征在于，所述注册模块，还包括：

发送单元，用于在所述生成单元产生用户公钥密钥对之前，向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

第三接收单元，用于接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥；

解密单元，用于根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

24. 根据权利要求 23 所述的终端，其特征在于，所述注册模块，还包括：

第四获取单元，用于在所述保存单元保存所述第二用户密钥密文和所述第二用户生物特征安全梗概之后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

判断单元，用于根据所述装置公钥判断所述第二签名是否正确；

则所述发送单元，还用于在所述判断单元判断所述第二签名正确时，将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户

生物特征是否注册成功。

25. 一种服务端，其特征在于，包括：

第一配置模块，用于预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

第一接收模块，用于接收所述终端发送的所述第一结果；

第一确定模块，用于根据所述第一结果确定所述第一用户生物特征是否通过验证。

26. 根据权利要求 25 所述的服务端，其特征在于，所述服务端，还包括：

第一发送模块，用于向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

27. 根据权利要求 26 所述的服务端，其特征在于，所述第一接收模块，具体用于接收所述终端发送的所述第一签名和所述第二用户公钥；

则所述第一确定模块，具体用于根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

28. 根据权利要求 27 所述的服务端，其特征在于，所述服务端，还包括：

第二配置模块，用于在所述第一配置模块将第一生物特征处理指令集配置给终端之前，将第二生物特征处理指令集配置给所述终端；

第二接收模块，用于接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

第二发送模块，用于将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

第三接收模块，用于接收所述终端发送的第二签名；

第二确定模块，用于根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

29. 根据权利要求 28 所述的服务端，其特征在于，所述第二发送模块，包括：

第一生成单元，用于产生装置公钥密钥对；其中，所述装置公钥密钥对包括所述装置公钥和所述装置密钥；

第二生成单元，用于根据所述用户账户口令的哈希值加密所述装置密钥，生成装置密钥密文；

发送单元，用于将所述装置密钥密文和所述装置公钥发送给所述终端。

30. 根据权利要求 27 所述的服务端，其特征在于，所述第一确定模块，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；其中，所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

用户身份认证方法、终端和服务端

技术领域

[0001] 本发明实施例涉及通信技术，尤其涉及一种用户身份认证方法、终端和服务端。

背景技术

[0002] 现今智能终端越来越普及，其中一个很重要的原因就是大量应用软件可提供用户下载，可以扩充终端的功能。然而，如此也造成终端安全问题日益严重，各种恶意软件都可能对终端造成严重威胁。例如，以最敏感的移动支付来说，用户输入的密码有可能被恶意软件窃取，支付的金额也有可能被篡改，这些都是很难单纯透过软件来保护的。因此，通过可信任区（TrustZone）的硬件切换隔离架构，在Trustzone的监控器之上，利用硬件将软件的安全模式和普通模式完全隔离，并且只通过Trustzone监控器切换。其中，安全模式下只运行最敏感的关键部分（例如，与支付相关的程序代码），尽可能减少可信计算基。具体的，将需要高度安全保护的程序部份置于安全模式运行，例如，用户输入密码的界面或是确认支付的界面等。当应用程序（例如支付程序）需要用到这些界面时，便送出调用请求，以切换至安全模式，待相关支付动作运行完毕后，再将运算结果送回至普通模式的原程序。由于在安全模式操作时，独享了许多硬件资源，因此可保障这些关键操作不受恶意软件攻击或窃取。

[0003] 传统的口令认证方式虽然也秉承了安全模式和普通模式分离的架构，但是口令泄露的风险太大，安全性依然不高。生物特征认证方式是目前终端认证的一个趋势。现有技术中，在远端的指纹认证方面，一般是通过将用户的指纹保存在终端的安全存储区，当有需要对用户身份进行认证时（例如，网上购物需要支付时），则终端通过录入用户指纹，并与安全存储区中的指纹进行比对，最后将比对结果发送给服务端（例如，支付宝平台）。

[0004] 但是，现有技术中，服务端太过依赖终端的比对结果，若终端被恶意软件攻击，恶意软件会代替终端向服务端发送“已支付“的比对结果，实际上并未支付，这样的“身份假冒”会导致服务端在支付方面具有很大的风险；另外，若服务端为了避免身份假冒带来的风险而选择自己验证指纹，则需要终端将用户的指纹信息发送给服务端，由服务端自己去比对，但是会造成用户隐私泄露。

发明内容

[0005] 本发明实施例提供一种用户身份认证方法、终端和服务端，用以解决现有技术在指纹验证过程中，由于终端被恶意软件攻击时造成的身份假冒以及用户隐私泄露的技术问题。

[0006] 第一方面，本发明实施例提供一种用户身份认证方法，包括：

[0007] 终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

[0008] 所述终端判断所述第一结果是否正确，其中，所述终端判断所述第一结果是否正确具体包括当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；

[0009] 若是，则所述终端将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0010] 结合第一方面，在第一方面的第一种可能的实施方式中，所述终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果，具体包括：

[0011] 所述终端接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文；

[0012] 所述终端根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥；

[0013] 所述终端根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

[0014] 结合第一方面的第一种可能的实施方式，在第一方面的第二种可能的实施方式中，所述终端判断所述第一结果是否正确，具体包括：

[0015] 所述终端根据预设的第二用户公钥判断所述第一签名是否正确；

[0016] 若是，所述终端将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0017] 结合第一方面的第一种可能的实施方式，在第一方面的第三种可能的实施方式中，所述终端根据当前输入的第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥，具体包括：

[0018] 所述终端根据所述第二用户生物特征安全梗概和所述第一用户生物特征，获取第一生物特征编码；

[0019] 所述终端根据所述第一生物特征编码的哈希值解密所述第二用户密钥密文，获得所述第一用户密钥。

[0020] 结合第一方面的第二种可能的实施方式，在第一方面的第四种可能的实施方式中，所述终端根据预设的第二用户公钥判断所述第一签名是否正确，具体包括：

[0021] 所述终端根据所述第二用户公钥判断所述第一签名是否与第三签名相同；所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0022] 结合第一方面至第一方面的第四种可能的实施方式中的任一项，在第一方面的第五种可能的实施方式中，所述终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果之前，还包括：

[0023] 所述终端根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上；其中，所述第二生物特征处理指令集为所述服务端配置给所述终端的。

[0024] 结合第一方面的第五种可能的实施方式，在第一方面的第六种可能的实施方式中，所述终端根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二

用户生物特征注册在所述服务端上，包括：

[0025] 所述终端产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥；

[0026] 所述终端接收用户输入的第二用户生物特征；

[0027] 所述终端根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概；

[0028] 所述终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0029] 结合第一方面的第六种可能的实施方式，在第一方面的第七种可能的实施方式中，所述终端产生用户公钥密钥对之前，所述方法还包括：

[0030] 所述终端向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

[0031] 所述终端接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥；

[0032] 所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

[0033] 结合第一方面的第七种可能的实施方式，在第一方面的第八种可能的实施方式中，所述终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概之后，所述方法还包括：

[0034] 所述终端根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

[0035] 所述终端根据所述装置公钥判断所述第二签名是否正确；

[0036] 若正确，则所述终端将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0037] 第二方面，本发明实施例提供一种用户身份认证方法，包括：

[0038] 服务端预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

[0039] 所述服务端接收所述终端发送的所述第一结果；

[0040] 所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0041] 结合第二方面，在第二方面的第一种可能的实施方式中，所述服务端接收所述终端发送的所述第一结果之前，还包括：

[0042] 所述服务端向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0043] 结合第二方面的第一种可能的实施方式，在第二方面的第二种可能的实施方式中，所述服务端接收所述终端发送的所述第一结果，具体包括：

[0044] 所述服务端接收所述终端发送的所述第一签名和所述第二用户公钥；

[0045] 则所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证，具体

包括：

[0046] 所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0047] 结合第二方面的第二种可能的实施方式，在第二方面的第三种可能的实施方式中，所述服务端预先将第一生物特征处理指令集配置给终端之前，所述方法还包括：

[0048] 所述服务端将第二生物特征处理指令集配置给所述终端；

[0049] 所述服务端接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

[0050] 所述服务端将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

[0051] 所述服务端接收所述终端发送的第二签名；

[0052] 所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0053] 结合第二方面的第三种可能的实施方式，在第二方面的第四种可能的实施方式中，所述服务端将装置密钥密文和装置公钥发送给所述终端，具体包括：

[0054] 所述服务端产生装置公钥密钥对；其中，所述装置公钥密钥对包括所述装置公钥和所述装置密钥；

[0055] 所述服务端根据所述用户账户口令的哈希值加密所述装置密钥，生成装置密钥密文；

[0056] 所述服务端将所述装置密钥密文和所述装置公钥发送给所述终端。

[0057] 结合第二方面的第二种可能的实施方式，在第二方面的第五种可能的实施方式中，所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证，具体包括：

[0058] 所述服务端根据所述第二用户公钥判断所述第一签名是否与第三签名相同；其中，所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0059] 第三方面，本发明实施例提供一种终端，包括：

[0060] 获取模块，用于根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

[0061] 判断模块，用于判断所述第一结果是否正确，其中，所述终端判断所述第一结果是否正确具体包括当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；

[0062] 发送模块，用于在所述判断模块判断所述第一结果正确时，将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0063] 结合第三方面，在第三方面的第一种可能的实施方式中，所述获取模块，包括：

[0064] 第一接收单元，用于接收所述服务端发送的生物特征认证请求；其中，所述生物特

征认证请求中包括所述服务端随机生成的挑战文；

[0065] 第一获取单元，用于根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥；

[0066] 第二获取单元，用于根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

[0067] 结合第三方面的第一种可能的实施方式，在第三方面的第二种可能的实施方式中，所述判断模块，具体用于根据预设的第二用户公钥判断所述第一签名是否正确；

[0068] 则所述发送模块，具体用于若所述判断模块判断所述第一签名正确时，将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0069] 结合第三方面的第一种可能的实施方式，在第三方面的第三种可能的实施方式中，所述第一获取单元，具体用于根据所述第二用户生物特征安全梗概和所述第一用户生物特征，获取第一生物特征编码；并根据所述第一生物特征编码的哈希值解密所述第二用户密钥密文，获得所述第一用户密钥。

[0070] 结合第三方面的第二种可能的实施方式，在第三方面的第四种可能的实施方式中，所述判断模块，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0071] 结合第三方面至第三方面的第四种可能的实施方式中的任一项，在第三方面的第五种可能的实施方式中，所述终端还包括：

[0072] 注册模块，用于在所述获取模块根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果之前，根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上；其中，所述第二生物特征处理指令集为所述服务端配置给所述终端的。

[0073] 结合第三方面的第五种可能的实施方式，在第三方面的第六种可能的实施方式中，所述注册模块，包括：

[0074] 生成单元，用于产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥；

[0075] 第二接收单元，用于接收用户输入的第二用户生物特征；

[0076] 第三获取单元，用于根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概；

[0077] 保存单元，用于保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0078] 结合第三方面的第六种可能的实施方式，在第三方面的第七种可能的实施方式中，所述注册模块，还包括：

[0079] 发送单元，用于在所述生成单元产生用户公钥密钥对之前，向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

[0080] 第三接收单元，用于接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥；

[0081] 解密单元，用于根据用户输入的用户账户口令解密所述装置密钥密文，获取装置

密钥。

[0082] 结合第三方面的第七种可能的实施方式，在第三方面的第八种可能的实施方式中，所述注册模块，还包括：

[0083] 第四获取单元，用于在所述保存单元保存所述第二用户密钥密文和所述第二用户生物特征安全梗概之后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

[0084] 判断单元，用于根据所述装置公钥判断所述第二签名是否正确；

[0085] 则所述发送单元，还用于在所述判断单元判断所述第二签名正确时，将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0086] 第四方面，本发明实施例提供一种服务端，包括：

[0087] 第一配置模块，用于预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；

[0088] 第一接收模块，用于接收所述终端发送的所述第一结果；

[0089] 第一确定模块，用于根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0090] 结合第四方面，在第四方面的第一种可能的实施方式中，所述服务端，还包括：

[0091] 第一发送模块，用于在所述第一接收模块接收所述终端发送的所述第一结果之前，向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0092] 结合第四方面的第一种可能的实施方式，在第四方面的第二种可能的实施方式中，所述第一接收模块，具体用于接收所述终端发送的所述第一签名和所述第二用户公钥；

[0093] 则所述第一确定模块，具体用于根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0094] 结合第四方面的第二种可能的实施方式，在第四方面的第三种可能的实施方式中，所述服务端，还包括：

[0095] 第二配置模块，用于在所述第一配置模块将第一生物特征处理指令集配置给终端之前，将第二生物特征处理指令集配置给所述终端；

[0096] 第二接收模块，用于接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；

[0097] 第二发送模块，用于将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；

[0098] 第三接收模块，用于接收所述终端发送的第二签名；

[0099] 第二确定模块，用于根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0100] 结合第四方面的第三种可能的实施方式，在第四方面的第四种可能的实施方式中，所述第二发送模块，包括：

[0101] 第一生成单元，用于产生装置公钥密钥对；其中，所述装置公钥密钥对包括所述装置公钥和所述装置密钥；

[0102] 第二生成单元，用于根据所述用户账户口令的哈希值加密所述装置密钥，生成装置密钥密文；

[0103] 发送单元，用于将所述装置密钥密文和所述装置公钥发送给所述终端。

[0104] 结合第四方面的第二种可能的实施方式，在第四方面的第五种可能的实施方式中，所述第一确定模块，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；其中，所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0105] 本发明实施例提供的用户身份认证方法、终端和服务端，通过终端根据服务端预设在终端内部的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果后，并判断该第一结果是否正确，并在第一结果正确时，将所述第一结果发送给服务端，以使服务端根据第一结果确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私。

附图说明

[0106] 为了更清楚地说明本发明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一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，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。

[0107] 图 1 为本发明提供的用户身份认证方法实施例一的流程示意图；

[0108] 图 2 为本发明提供的用户身份认证方法实施例二的流程示意图；

[0109] 图 3 为本发明提供的用户身份认证方法实施例三的流程示意图；

[0110] 图 4 为本发明提供的用户身份认证方法实施例四的流程示意图；

[0111] 图 5 为本发明提供的用户身份认证方法实施例五的流程示意图；

[0112] 图 6 为本发明提供的用户身份认证方法实施例六的流程示意图；

[0113] 图 7 为本发明提供的用户身份认证方法实施例七的信令流程图；

[0114] 图 8 为本发明提供的终端实施例一的结构示意图；

[0115] 图 9 为本发明提供的终端实施例二的结构示意图；

[0116] 图 10 为本发明提供的终端实施例三的结构示意图；

[0117] 图 11 为本发明提供的终端实施例四的结构示意图；

[0118] 图 12 为本发明提供的服务端实施例一的结构示意图；

[0119] 图 13 为本发明提供的服务端实施例二的结构示意图；

[0120] 图 14 为本发明提供的服务端实施例三的结构示意图；

[0121] 图 15 为本发明提供的服务端实施例四的结构示意图。

具体实施方式

[0122] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，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，都属于本发明保护的范围。

[0123] 本发明实施例中涉及的终端，可以是用户设备，可以是无线终端也可以是有线终端，无线终端可以是指向用户提供语音和 / 或数据连通性的设备，具有无线连接功能的手持式设备、或连接到无线调制解调器的其他处理设备。无线终端可以经无线接入网（例如，RAN，Radio Access Network）与一个或多个核心网进行通信，无线终端可以是移动终端，如移动电话（或称为“蜂窝”电话）和具有移动终端的计算机，例如，可以是便携式、袖珍式、手持式、计算机内置的或者车载的移动装置，它们与无线接入网交换语言和 / 或数据。例如，个人通信业务（PCS，Personal Communication Service）电话、无绳电话、会话发起协议（SIP）话机、无线本地环路（WLL，Wireless Local Loop）站、个人数字助理（PDA，Personal Digital Assistant）等设备。

[0124] 另外，本发明涉及的终端，还可以提供一在安全世界的可信执行环境（TEE），以保证下述方法实施例可以在安全的环境下运行。

[0125] 图 1 为本发明提供的用户身份认证方法实施例一的流程示意图。如图 1 所示，该方法包括如下步骤：

[0126] S101：终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征。

[0127] 具体的，终端在进行用户身份验证之前，会先将该用户的生物特征注册在服务端上，即 S101 中终端预先在服务端上注册第二用户生物特征。可选的，终端可以通过执行服务端预先设置在终端的生物特征注册指令第二用户生物特征注册在服务端上，以使服务端获知用户自身的生物特征，方便后期的用户身份验证。这里的服务端为提供终端相关服务的服务器平台，例如当用户通过终端进行网购时，这里的服务端就可以为支付宝平台。当用户需要进行移动支付时，则就需要通过终端和服务端对该用户的身份验证。

[0128] 当用户需要进行身份验证时，用户会在终端上输入第一用户生物特征。需要说明的是，这里的第一用户生物特征需要和第二用户生物特征是同类型的生物特征，即若用户在服务端注册的第二用户生物特征是指纹，则这里输入的第一用户生物特征也应该是指纹，而不能是瞳孔等其他的生物特征。终端在收到用户当前输入的第一用户生物特征之后，执行服务端预设在终端内部的第一生物特征处理指令集，以判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果。上述第一生物特征处理指令集主要用于终端对用户的身份进行验证。

[0129] S102：终端判断所述第一结果是否正确；若是，则所述终端将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0130] 具体的，终端判断上述第一结果是否正确，可选的，当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；可选的，当终端判断第一用户生物特征与第二用户生物特征匹配，但是第一结果中携带了第二用户生物特征，则说明该第一结果不正确；可选的，当终端判断第一用户生物特征与第二用户生物特征不匹配，那第一结果中不管有没有携带第二用户生物特征，该第一结果都是不正确。

[0131] 当终端判断该第一结果正确时，终端将该第一结果发送给服务端，服务端根据该第一结果确定上述第一用户生物特征是否通过验证。可选的，服务端可以通过自己的判断机制判断该第一结果是不是终端执行预设的第一生物特征处理指令集获得的，并且判断该第一结果是不是与服务端预知的正确结果相匹配，若是，则表明该用户通过验证。

[0132] 传统的用户身份认证过程中（例如指纹认证），包括两个极端：第一种，服务端完全依赖终端的指纹比对结果，即用户的指纹信息不离开手机，所以不会造成用户隐私泄露，但是服务端在支付上存在风险（例如恶意软件攻击指纹验证或身份假冒）；另一个为了确保服务端在支付时的安全性及指纹验证时的应用弹性，终端将用户的指纹信息发送给服务端，由服务端自己去比对，从而避免身份假冒等风险，但是会造成用户隐私泄露。

[0133] 但是，在本申请中，由于终端在验证用户身份时，所使用的第一生物特征处理指令集由于是服务端配置给终端的，因此终端通过执行该第一生物特征处理指令集得到的第一结果对于服务端来说是可信的，也就是说服务端没有完全依赖终端的比对结果，确保了服务端在身份验证时的安全性；同时，由于终端会判断第一结果是否正确，即判断该第一结果中是否携带了之前注册的用户的第二用户生物特征，以确保终端不会将用户注册的第二用户生物特征发送出去，即保证了第二用户生物特征不会离开终端，从而避免用户隐私的泄露。

[0134] 本发明实施例提供的用户身份认证方法，通过终端根据服务端预设在终端内部的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果后，并判断该第一结果是否正确，并在第一结果正确时，将所述第一结果发送给服务端，以使服务端根据第一结果确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私。

[0135] 图 2 为本发明提供的用户身份认证方法实施例二的流程示意图。本实施例涉及的是终端执行预设的第一生物特征处理指令集获取第一结果以及终端判断第一结果是否正确的具体过程，也就是终端对用户身份进行验证的具体过程。如图 2 所示：

[0136] S201：终端接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文。

[0137] 具体的，服务端在用户需要进行指纹验证时（例如，用户需要进行支付时），服务

端会向终端发送生物特征认证请求，该生物特征认证请求可以包括服务端随机生成的挑战文，还可以进一步包括用户的身份标识（Identifier，以下简称 ID）和终端的 ID，这里的用户 ID 可以为用户在支付网站上注册的用户账户。

[0138] S202：终端根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0139] 具体的，用户在终端上输入第一用户生物特征，终端在获取到第一用户生物特征之后，结合预先存储的第二用户生物特征安全梗概，推算出第一生物特征编码（在终端中生物特征实际上都是以编码形式存在的）。然后，终端根据该第一生物特征编码的哈希值对预先存储的第二用户密钥密文进行解密，以获得与第一用户生物特征对应的第一用户密钥。

[0140] S203：终端根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

[0141] 需要说明的是，这里的终端根据第一用户密钥对挑战文进行签名处理，实际上是利用第一用户密钥对挑战文进行计算，从而产生第一签名。

[0142] S204：终端根据预设的第二用户公钥判断所述第一签名是否正确；若是，所述终端将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0143] 具体的，终端根据预设的第二用户公钥判断上述第一签名是否正确。可选的，终端根据预设的第二用户公钥判断第一签名是否与第三签名相同，该第三签名为终端预先根据第二用户密钥对挑战文进行签名处理得到的，也就是说，该第三签名是终端利用所注册的第二用户生物特征对应的正确的第二用户密钥对挑战文进行签名处理得到的，而这里的第一用户密钥是与用户输入的第一用户生物特征对应的，其正确性无法保证（若输入的第一用户生物特征是正确的，即用户输入的第一用户生物特征与注册的第二用户生物特征一致，则这个第一用户密钥就是正确的密钥；但是，若输入的第一用户生物特征本身就是错误的生物特征，例如是另外一个用户输入的生物特征或者是同一个用户输入的其他的生物特征，则这里的第一用户密钥就是错误的），故利用第一用户密钥对同一挑战文进行签名处理得到的第一签名的正确性也无法保证。因此，终端可以利用与第二用户密钥对应的第二用户公钥判断该第一签名是否和第三签名相同，来判断该第一签名是否正确。当然，该第三签名中没有携带第二用户生物特征。

[0144] 若终端判断第一签名和第三签名相同，则说明第一签名正确。也就是说，该第一签名中没有携带第二用户生物特征。之后，终端就将该第一签名和第二用户公钥发送给服务端；服务端在接收到这两者之后，也根据第二用户公钥判断该第一签名是不是利用第二用户密钥对挑战文做签名处理后得到的，若是，则服务端确认该第一签名是正确的，即服务端确定用户当前输入的第一用户生物特征是正确的。

[0145] 本发明实施例提供的用户身份认证方法，通过终端执行服务端预设在终端内部的第一生物特征处理指令集，即根据用户输入的第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥，并在根据该第一用户密钥对服务端发送的挑战文进行签名处理获取第一签名之后，判断该第一签名是否准确，从而在第一签名正确后，将第一签名发送给服务端。本发明实施例提供的方法，由于第一生物特征

处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性和应用弹性（即服务端可以适当的调整终端执行第一生物特征处理指令集比对生物特征时的比对阈值）；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私；同时，本发明提供的方法，终端无需保存用户完整的生物特征，因此不需要额外的安全存储硬件，节省了硬件设计的成本。

[0146] 图 3 为本发明提供的用户身份认证方法实施例三的流程示意图。本实施例涉及的是在用户进行身份认证之前（即在上述 S101 之前），终端根据预设的第二生物特征处理指令集和第二用户生物特征，将第二用户生物特征注册在服务端上的具体过程。其中，该第二生物特征处理指令集为服务端配置给终端的，该第二生物特征处理指令集用于终端在服务端上注册第二用户生物特征。如图 3 所示，在 S101 之前，该方法还包括：

[0147] S301：终端向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户 ID 和终端 ID。

[0148] 具体的，终端在进行用户的第二用户生物特征注册之前，服务端会先通过其它如用户账户口令、密码、短信或语音等方式来认证用户，即用户需要先登录服务端，在用户身份首次被确认之后，才进行生物特征的注册。即，终端向服务端发送携带用户 ID 和终端 ID 的生物特征注册请求，以在服务端上注册第二用户生物特征。

[0149] S302：终端接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥。

[0150] 具体的，服务端在收到终端发送的生物特征注册请求之后，会产生装置公钥密钥对，该装置公钥密钥对包括一个装置密钥和一个装置公钥；之后，服务端利用用户输入的用户账户口令或密码的哈希值对装置密钥进行加密（服务端本身就知晓对应该用户账户的用户账户口令或密码或者这两者的哈希值），生成装置密钥密文之后，将装置密钥密文和装置公钥发送给终端。

[0151] S303：终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

[0152] S304：终端产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥。

[0153] S305：终端接收用户输入的第二用户生物特征。

[0154] S306：终端根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0155] S307：终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0156] 具体的，终端将第二用户密钥密文和第二用户生物特征安全梗概进行保存，是为了方便后面验证用户身份。可以结合上述图 2 所示的实施例，在此不再赘述。

[0157] S308：终端根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名。

[0158] 具体的，终端根据之前获取的装置密钥对第二用户公钥和用户 ID 进行签名处理，即对第二用户公钥和用户 ID 进行签名计算（可以参照现有技术），获取第二签名。

[0159] S309：终端根据所述装置公钥判断所述第二签名是否正确；若正确，则所述终端将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确

定所述第二用户生物特征是否注册成功。

[0160] 具体的，由于装置公钥与装置密钥相对应，因此，利用装置公钥可以准确的判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，并且，判断该第二签名中有没有包括第二用户生物特征；若没有，则说明该第二签名正确。

[0161] 之后，终端将该第二签名发送给服务端，该第二签名是终端通过执行服务端预设在终端内部的第二生物特征处理指令集得到的（即上述 S301-S308 均是终端执行第二生物特征处理指令集的过程），因此，对于服务端来说，其知道该第二签名是终端执行自己配置给终端的第二生物特征处理指令集得到的。服务端在收到该第二签名之后，利用装置公钥同样对该第二签名进行判断，即判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，若是，则说明该第二签名正确，用户的第二用户生物特征注册成功。

[0162] 本发明实施例提供的用户身份认证方法，终端通过执行服务端预设在终端内部的第二生物特征处理指令集，在服务端上注册用户的第二用户生物特征；之后，终端执行第一生物特征处理指令集，即根据用户输入的第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥，并在根据该第一用户密钥对服务端发送的挑战文进行签名处理获取第一签名之后，判断该第一签名是否准确，从而在第一签名正确后，将第一签名发送给服务端。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性和应用弹性（即服务端可以适当的调整终端执行第一生物特征处理指令集比对生物特征时的比对阈值）；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私；同时，本发明提供的方法，终端无需保存用户完整的生物特征，因此不需要额外的安全存储硬件，节省了硬件设计的成本。

[0163] 图 4 为本发明提供的用户身份认证方法实施例四的流程示意图。如图 4 所示，该方法包括：

[0164] S401：服务端预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征。

[0165] 具体的，服务端预先将第一生物特征处理指令集配置给终端，使得终端可以通过执行该第一生物特征处理指令集认证用户身份。可选的，终端在进行用户身份验证之前，会先将该用户的生物特征注册在服务端上，即终端预先在服务端上注册第二用户生物特征。可选的，终端可以通过执行服务端预先设置在终端的生物特征注册指令第二用户生物特征注册在服务端上，以使服务端获知用户自身的生物特征，方便后期的用户身份验证。这里的服务端为提供终端相关服务的服务器平台，例如当用户通过终端进行网购时，这里的服务端就可以为支付宝平台。当用户需要进行移动支付时，则就需要通过终端和服务端对该用户的身份验证。

[0166] 当用户需要进行身份验证时，用户会在终端上输入第一用户生物特征。需要说明的是，这里的第一用户生物特征需要和第二用户生物特征是同类型的生物特征，即若用

户在服务端注册的第二用户生物特征是指纹，则这里输入的第一用户生物特征也应该是指纹，而不能是瞳孔等其他的生物特征。终端在收到用户当前输入的第一用户生物特征之后，执行服务端预设在终端内部的第一生物特征处理指令集，以判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果。上述第一生物特征处理指令集主要用于终端对用户的身份进行验证。

[0167] 进一步地，终端在获得第一结果后，会判断该第一结果是否正确。可选的，当终端判断第一用户生物特征与第二用户生物特征匹配，且第一结果中没有携带第二用户生物特征，则说明该第一结果正确；可选的，当终端判断第一用户生物特征与第二用户生物特征匹配，但是第一结果中携带了第二用户生物特征，则说明该第一结果不正确；可选的，当终端判断第一用户生物特征与第二用户生物特征不匹配，那第一结果中不管有没有携带第二用户生物特征，该第一结果都是不正确。

[0168] 当终端判断该第一结果正确时，终端将该第一结果发送给服务端。

[0169] S402：服务端接收所述终端发送的所述第一结果。

[0170] S403：服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0171] 具体的，服务端根据该第一结果确定上述第一用户生物特征是否通过验证。可选的，服务端可以通过自己的判断机制判断该第一结果是不是终端执行预设的第一生物特征处理指令集获得的，并且判断该第一结果是不是与服务端预知的正确结果相匹配，若是，则表明该用户通过验证。

[0172] 传统的用户身份认证过程中（例如指纹认证），包括两个极端：第一种，服务端完全依赖终端的指纹比对结果，即用户的指纹信息不离开手机，所以不会造成用户隐私泄露，但是服务端在支付上存在风险（例如恶意软件攻击指纹验证或身份假冒）；另一个为了确保服务端在支付时的安全性及指纹验证时的应用弹性，终端将用户的指纹信息发送给服务端，由服务端自己去比对，从而避免身份假冒等风险，但是会造成用户隐私泄露。

[0173] 但是，在本申请中，由于终端在验证用户身份时，所使用的第一生物特征处理指令集由于是服务端配置给终端的，因此终端通过执行该第一生物特征处理指令集得到的第一结果对于服务端来说是可信的，也就是说服务端没有完全依赖终端的比对结果，确保了服务端在身份验证时的安全性；同时，由于终端会判断第一结果是否正确，即判断该第一结果中是否携带了之前注册的用户的第二用户生物特征，以确保终端不会将用户注册的第二用户生物特征发送出去，即保证了第二用户生物特征不会离开终端，从而避免用户隐私的泄露。

[0174] 本发明实施例提供的用户身份认证方法，通过服务端预先将第一生物特征处理指令集配置给终端，终端根据服务端预设在终端内部的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果后，并判断该第一结果是否正确，并在第一结果正确时，将所述第一结果发送给服务端，使得服务端根据第一结果确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私。

[0175] 图5为本发明提供的用户身份认证方法实施例五的流程示意图。本实施例涉及的

是服务端判断第一用户生物特征是否正确的具体过程。如图 5 所示，该方法包括：

[0176] S501：服务端预先将第一生物特征处理指令集配置给终端。

[0177] 具体的，服务端预先将第一生物特征处理指令集配置给终端，使得终端可以通过执行该第一生物特征处理指令集认证用户身份。可选的，终端在进行用户身份验证之前，会先将该用户的生物特征注册在服务端上，即终端预先在服务端上注册第二用户生物特征。可选的，终端可以通过执行服务端预先设置在终端的生物特征注册指令第二用户生物特征注册在服务端上，以使服务端获知用户自身的生物特征，方便后期的用户身份验证。这里的服务端为提供终端相关服务的服务器平台，例如当用户通过终端进行网购时，这里的服务端就可以为支付宝平台。当用户需要进行移动支付时，则就需要通过终端和服务端对该用户的身份验证。

[0178] S502：服务端向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0179] 具体的，当终端接收到服务端发送的生物特征认证请求之后，用户会在终端上输入第一用户生物特征。需要说明的是，这里的第一用户生物特征需要和第二用户生物特征是同类型的生物特征，即若用户在服务端注册的第二用户生物特征是指纹，则这里输入的第一用户生物特征也应该是指纹，而不能是瞳孔等其他的生物特征。

[0180] 终端在收到用户当前输入的第一用户生物特征之后，执行服务端预设在终端内部的第一生物特征处理指令集，即终端结合预先存储的第二用户生物特征安全梗概，推算出第一生物特征编码（在终端中生物特征实际上都是以编码形式存在的）。然后，终端根据该第一生物特征编码的哈希值对预先存储的第二用户密钥密文进行解密，以获得与第一用户生物特征对应的第一用户密钥。之后，终端根据该第一用户密钥对生物特征认证请求中的挑战文进行签名处理（实际上是利用第一用户密钥对挑战文进行计算），产生第一签名。

[0181] 进一步地，终端根据预设的第二用户公钥判断上述第一签名是否正确。可选的，终端根据预设的第二用户公钥判断第一签名是否与第三签名相同，该第三签名为终端预先根据第二用户密钥对挑战文进行签名处理得到的，也就是说，该第三签名是终端利用所注册的第二用户生物特征对应的正确的第二用户密钥对挑战文进行签名处理得到的，而这里的第一用户密钥是与用户输入的第一用户生物特征对应的，其正确性无法保证（若输入的第一用户生物特征是正确的，即用户输入的第一用户生物特征与注册的第二用户生物特征一致，则这个第一用户密钥就是正确的密钥；但是，若输入的第一用户生物特征本身就是错误的生物特征，则这里的第一用户密钥就是错误的），故利用第一用户密钥对同一挑战文进行签名处理得到的第一签名的正确性也无法保证。因此，终端可以利用与第二用户密钥对应的第二用户公钥判断该第一签名是否和第三签名相同，来判断该第一签名是否正确。当然，该第三签名中没有携带第二用户生物特征。

[0182] 若终端判断第一签名和第三签名相同，则说明第一签名正确。也就是说，该第一签名中没有携带第二用户生物特征。之后，终端就将该第一签名和第二用户公钥发送给服务端。

[0183] S503：服务端接收所述终端发送的所述第一签名和所述第二用户公钥。

[0184] S504：服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0185] 具体的，服务端在接收到第二用户公钥和第一签名之后，也根据第二用户公钥判断该第一签名是不是利用第二用户密钥对挑战文做签名处理后得到的，即服务端也需要判断第一签名是否和第三签名相同。若是，则服务端确认该第一签名是正确的，即服务端确定用户当前输入的第一用户生物特征是正确的，用户身份通过认证。

[0186] 本发明实施例提供的用户身份认证方法，通过服务端预先给终端配置第一生物特征处理指令集，终端执行该第一生物特征处理指令集，即终端根据用户输入的第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；并在根据该第一用户密钥对服务端发送的挑战文进行签名处理获取第一签名之后，判断该第一签名是否准确，从而在第一签名正确后，将第一签名发送给服务端，使得服务端根据第二用户公钥和第一签名确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性和应用弹性（即服务端可以适当的调整终端执行第一生物特征处理指令集比对生物特征时的比对阈值）；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私；同时，本发明提供的方法，终端无需保存用户完整的生物特征，因此不需要额外的安全存储硬件，节省了硬件设计的成本。

[0187] 图 6 为本发明提供的用户身份认证方法实施例六的流程示意图。本实施例涉及的是在用户进行身份认证之前（即在上述 S501 之前），终端根据服务端配置的第二生物特征处理指令集和第二用户生物特征，将第二用户生物特征注册在服务端上的具体过程。如图 6 所示，在 S501 之前，该方法还包括：

[0188] S601：服务端将第二生物特征处理指令集配置给所述终端。

[0189] 具体的，服务端预先将第二生物特征处理指令集配置给终端，使得终端能够根据该第二生物特征处理指令集在服务端上注册第二用户生物特征。需要说明的是，终端在进行用户的第二用户生物特征注册之前，服务端会先通过其它如用户账户口令、密码、短信或语音等方式来认证用户，即用户需要先登录服务端，在用户身份首次被确认之后，才进行生物特征的注册。

[0190] S602：服务端接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户 ID 和终端 ID。

[0191] S603：服务端将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名。

[0192] 具体的，服务端接收到终端发送的携带用户 ID 和终端 ID 的生物特征注册请求后，会产生装置公钥密钥对，该装置公钥密钥对包括一个装置密钥和一个装置公钥；之后，服务端利用用户输入的用户账户口令或密码的哈希值对装置密钥进行加密（服务端本身就知晓对应该用户账户的用户账户口令或密码或者这二者的哈希值），生成装置密钥密文之后，将装置密钥密文和装置公钥发送给终端。

[0193] 之后，终端根据用户输入的用户账户口令对上述装置密钥密文进行解密，以获取

装置密钥；并且，终端还产生用户公钥密钥对，该用户公钥密钥对包括第二用户密钥和第二用户公钥。进一步地，终端在接收到用户输入的第二用户生物特征之后，根据第二用户生物特征的哈希值对第二用户密钥加密，获取第二用户密钥密文和第二用户生物特征安全梗概，并将该第二用户密钥密文和第二用户生物特征安全梗概保存起来，以方便上述 S502 中终端根据所保存的第二用户密钥密文和第二用户生物特征安全梗概，并结合输入的第一用户生物特征，获取第一用户密钥，并方便终端根据第一用户密钥获取第一签名。

[0194] 进一步地，终端根据之前获取的装置密钥对第二用户公钥和用户 ID 进行签名处理，即对第二用户公钥和用户 ID进行签名计算（可以参照现有技术），获取第二签名。随后，终端根据之前所获取的装置密钥判断该第二签名是否正确，即判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的。由于装置公钥与装置密钥相对应，因此，利用装置公钥可以准确的判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，并且，判断该第二签名中有没有包括第二用户生物特征；若没有，则说明该第二签名正确。

[0195] S604：服务端接收所述终端发送的第二签名。

[0196] S605：服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0197] 具体的，终端将该第二签名发送给服务端，该第二签名是终端通过执行服务端预设在终端内部的第二生物特征处理指令集得到的，因此，对于服务端来说，其知道该第二签名是终端执行自己配置给终端的第二生物特征处理指令集得到的。服务端在收到该第二签名之后，利用装置公钥同样对该第二签名进行判断，即判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，若是，则说明该第二签名正确，用户的第二用户生物特征注册成功。

[0198] 本发明实施例提供的用户身份认证方法，服务端预先将第二生物特征处理指令集配置给终端，使得终端能够根据该第二生物特征处理指令集在服务端上注册用户的第二用户生物特征；之后，终端根据服务端预设在终端内部的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果后，并判断该第一结果是否正确，并在第一结果正确时，将所述第一结果发送给服务端，使得服务端根据第一结果确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性和应用弹性（即服务端可以适当的调整终端执行第一生物特征处理指令集比对生物特征时的比对阈值）；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私；同时，本发明提供的方法，终端无需保存用户完整的生物特征，因此不需要额外的安全存储硬件，节省了硬件设计的成本。

[0199] 图 7 为本发明提供的用户身份认证方法实施例七的信令流程图。本实施例涉及的终端和服务端相互配合对用户的身份进行认证的具体过程。该方法包括：

[0200] S701：服务端将第二生物特征处理指令集和第一生物特征处理指令集配置给所述终端。

[0201] 该第一生物特征处理指令集用于进行用户的生物特征注册，第二生物特征处理指

令集用于进行用户的生物特征验证。这两个生物特征处理指令集可以集成在终端内部的同一个模块中，也可以位于不同的模块中，本发明实施例对此并不做限制。

[0202] S702：终端向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户 ID 和终端 ID。

[0203] 具体的，终端在进行用户的第二用户生物特征注册之前，服务端会先通过其它如用户账户口令、密码、短信或语音等方式来认证用户，即用户需要先登录服务端，在用户身份首次被确认之后，才进行生物特征的注册。即，终端向服务端发送携带用户 ID 和终端 ID 的生物特征注册请求，以在服务端上注册第二用户生物特征。

[0204] S703：服务端产生装置公钥密钥对。

[0205] S704：服务端根据用户输入的用户账户口令的哈希值对装置密钥进行加密，获取装置密钥密文。

[0206] 具体的，服务端本身是可以获知用户的账户口令或用户账户口令的哈希值的。并且，可选的，服务端还可以通过用户账户的密码的哈希值对装置密钥进行加密，获得装置密钥密文。

[0207] S705：服务端将装置密钥密文和装置公钥发送给终端。

[0208] S706：终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

[0209] S707：终端产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥。

[0210] S708：终端接收用户输入的第二用户生物特征。

[0211] S709：终端根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0212] S710：终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0213] S711：终端根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名。

[0214] 具体的，终端根据之前获取的装置密钥对第二用户公钥和用户 ID 进行签名处理，即对第二用户公钥和用户 ID 进行签名计算（可以参照现有技术），获取第二签名。

[0215] S712：终端根据所述装置公钥判断所述第二签名是否正确；若是，执行 S713，若否，则结束流程。

[0216] 具体的，终端根据之前所获取的装置密钥判断该第二签名是否正确，即判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的。由于装置公钥与装置密钥相对应，因此，利用装置公钥可以准确的判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，并且，判断该第二签名中有没有包括第二用户生物特征；若没有，则说明该第二签名正确。

[0217] S713：终端将所述第二签名发送给所述服务端。

[0218] S714：服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。若是，则服务端确认第二用户生物特征注册成功，执行 S715；若否，结束流程。

[0219] 具体的，服务端在收到该第二签名之后，也需要利用装置公钥同样对该第二签名进行判断，即判断上述第二签名是不是终端通过装置密钥对第二用户公钥和用户 ID 进行签名处理得到的，若是，则说明该第二签名正确，用户的第二用户生物特征注册成功。

[0220] S715：服务端向所述终端发送携带挑战文的生物特征认证请求。

[0221] S716：终端接收用户输入的第一用户生物特征。

[0222] 具体的，当终端接收到服务端发送的生物特征认证请求之后，用户会在终端上输入第一用户生物特征。需要说明的是，这里的第一用户生物特征需要和第二用户生物特征是同类型的生物特征，即若用户在服务端注册的第二用户生物特征是指纹，则这里输入的第一用户生物特征也应该是指纹，而不能是瞳孔等其他的生物特征。

[0223] S717：终端根据所述第一用户生物特征、上述保存的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0224] 具体的，终端在收到用户当前输入的第一用户生物特征之后，执行服务端预设在终端内部的第一生物特征处理指令集，即终端结合预先存储的第二用户生物特征安全梗概，推算出第一生物特征编码（在终端中生物特征实际上都是以编码形式存在的）。然后，终端根据该第一生物特征编码的哈希值对预先存储的第二用户密钥密文进行解密，以获得与第一用户生物特征对应的第一用户密钥。

[0225] S718：终端根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

[0226] S719：终端根据预设的第二用户公钥判断所述第一签名是否正确；若是，执行S720，若否，结束流程。

[0227] 具体的，终端根据预设的第二用户公钥判断上述第一签名是否正确。可选的，终端根据预设的第二用户公钥判断第一签名是否与第三签名相同，该第三签名为终端预先根据第二用户密钥对挑战文进行签名处理得到的，也就是说，该第三签名是终端利用所注册的第二用户生物特征对应的正确的第二用户密钥对挑战文进行签名处理得到的，而这里的第一用户密钥是与用户输入的第一用户生物特征对应的，其正确性无法保证（若输入的第一用户生物特征是正确的，即用户输入的第一用户生物特征与注册的第二用户生物特征一致，则这个第一用户密钥就是正确的密钥；但是，若输入的第一用户生物特征本身就是错误的生物特征，则这里的第一用户密钥就是错误的），故利用第一用户密钥对同一挑战文进行签名处理得到的第一签名的正确性也无法保证。因此，终端可以利用与第二用户密钥对应的第二用户公钥判断该第一签名是否和第三签名相同，来判断该第一签名是否正确。当然，该第三签名中没有携带第二用户生物特征。

[0228] 若终端判断第一签名和第三签名相同，则说明第一签名正确。也就是说，该第一签名中没有携带第二用户生物特征。

[0229] S720：终端将所述第一签名和所述第二用户公钥发送给所述服务端。

[0230] 具体的，若终端判断第一签名和第三签名相同，则说明第一签名正确。也就是说，该第一签名中没有携带第二用户生物特征。之后，终端就将该第一签名和第二用户公钥发送给服务端。

[0231] S721：服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0232] 具体的，服务端在接收到第二用户公钥和第一签名之后，也根据第二用户公钥判断该第一签名是不是利用第二用户密钥对挑战文做签名处理后得到的，即服务端判断该第一签名是否和第三签名相同。若是，则服务端确认该第一签名是正确的，即服务端确定用户

当前输入的第一用户生物特征是正确的，用户身份通过认证。

[0233] 本发明实施例提供的用户身份认证方法，服务端预先将第二生物特征处理指令集配置给终端，使得终端能够根据该第二生物特征处理指令集在服务端上注册用户的第二用户生物特征；之后，终端根据服务端预设在终端内部的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果后，并判断该第一结果是否正确，并在第一结果正确时，将所述第一结果发送给服务端，使得服务端根据第一结果确定第一用户生物特征是否通过验证。本发明实施例提供的方法，由于第一生物特征处理指令集是服务端配置给终端的，因此，对于服务端来说，并不是完全依赖终端的比对结果，提高了服务端进行用户身份验证时的安全性和应用弹性（即服务端可以适当的调整终端执行第一生物特征处理指令集比对生物特征时的比对阈值）；另外，由于终端也会对上述获取的第一结果进行监控，避免将第二用户生物特征泄漏到非安全区域，确保了用户的隐私；同时，本发明提供的方法，终端无需保存用户完整的生物特征，因此不需要额外的安全存储硬件，节省了硬件设计的成本。

[0234] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0235] 图8为本发明提供的终端实施例一的结果示意图。如图8所示，该终端包括：获取模块10、判断模块11、发送模块12；其中，获取模块10，用于根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；判断模块11，用于判断所述第一结果是否正确；发送模块12，用于在所述判断模块11判断所述第一结果正确时，将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0236] 本发明实施例提供的终端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0237] 图9为本发明提供的终端实施例二的结构示意图。在图8所示实施例的基础上，进一步地，上述获取模块10，具体包括：第一接收单元101、第一获取单元102和第二获取单元103。其中，第一接收单元101，用于接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文；第一获取单元102，用于根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥；第二获取单元103，用于根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名。

[0238] 进一步地，上述判断模块11，具体用于根据预设的第二用户公钥判断所述第一签名是否正确；则上述发送模块12，具体用于若所述判断模块11判断所述第一签名正确时，将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0239] 更进一步地，上述第一获取单元102，具体用于根据所述第二用户生物特征安全梗

概和所述第一用户生物特征，获取第一生物特征编码；并根据所述第一生物特征编码的哈希值解密所述第二用户密钥密文，获得所述第一用户密钥。

[0240] 更进一步地，上述判断模块 11，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0241] 本发明实施例提供的终端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0242] 图 10 为本发明提供的终端实施例三的结构示意图。在上述图 9 所示实施例的基础上，进一步地，该终端还包括：注册模块 13，用于在所述获取模块 10 根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果之前，根据预设的第二生物特征处理指令集和所述第二用户生物特征，将所述第二用户生物特征注册在所述服务端上；其中，所述第二生物特征处理指令集为所述服务端配置给所述终端的。

[0243] 进一步地，该注册模块 13，具体包括：生成单元 131、第二接收单元 132、第三获取单元 133 和保存单元 134。其中，生成单元 131，用于产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥；第二接收单元 132，用于接收用户输入的第二用户生物特征；第三获取单元 133，用于根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概；保存单元 134，用于保存所述第二用户密钥密文和所述第二用户生物特征安全梗概。

[0244] 本发明实施例提供的终端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0245] 图 11 为本发明提供的终端实施例四的结构示意图。在上述图 10 所示实施例的基础上，进一步地，上述注册模块 13，还包括：发送单元 135、第三接收单元 136 和解密单元 137。其中，发送单元 135，用于在所述生成单元 131 产生用户公钥密钥对之前，向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；第三接收单元 136，用于接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥；解密单元 137，用于根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥。

[0246] 进一步地，上述注册模块 13，还可以包括：第四获取单元 138 和判断单元 139。其中，第四获取单元 138，用于在所述保存单元 134 保存所述第二用户密钥密文和所述第二用户生物特征安全梗概之后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；判断单元 139，用于根据所述装置公钥判断所述第二签名是否正确；则所述发送单元 135，还用于在所述判断单元 139 判断所述第二签名正确时，将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0247] 本发明实施例提供的终端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0248] 图 12 为本发明提供的服务端实施例一的结构示意图。如图 12 所示，该服务端包括：第一配置模块 20、第一接收模块 21 和第一确定模块 22。其中，第一配置模块 20，用于

预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征；第一接收模块 21，用于接收所述终端发送的所述第一结果；第一确定模块 22，用于根据所述第一结果确定所述第一用户生物特征是否通过验证。

[0249] 本发明实施例提供的服务端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0250] 图 13 为本发明提供的服务端实施例二的结构示意图。在上述图 12 所示实施例的基础上，进一步地，该服务端还可以包括：第一发送模块 23，用于在所述第一接收模块 21 接收所述终端发送的所述第一结果之前，向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥。

[0251] 进一步地，上述第一接收模块 21，具体用于接收所述终端发送的所述第一签名和所述第二用户公钥；则所述第一确定模块 22，具体用于根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证。

[0252] 本发明实施例提供的服务端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0253] 图 14 为本发明提供的服务端实施例三的结构示意图。在上述图 13 所示实施例的基础上，进一步地，该服务端还可以包括：第二配置模块 24、第二接收模块 25、第二发送模块 26、第三接收模块 27 和第二确定模块 28。其中，第二配置模块 24，用于在所述第一配置模块 20 将第一生物特征处理指令集配置给终端之前，将第二生物特征处理指令集配置给所述终端；第二接收模块 25，用于接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户身份标识 ID 和终端 ID；第二发送模块 26，用于将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户 ID 进行签名处理，获得所述第二签名；第三接收模块 27，用于接收所述终端发送的第二签名；第二确定模块 28，用于根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功。

[0254] 本发明实施例提供的服务端，可以执行上述用户身份认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0255] 图 15 为本发明提供的服务端实施例四的结构示意图。在上述图 14 所示实施例的基础上，进一步地，上述第二发送模块 26，具体包括：第一生成单元 261、第二生成单元 262 和发送单元 263。其中，第一生成单元 261，用于产生装置公钥密钥对；其中，所述装置公钥密钥对包括所述装置公钥和所述装置密钥；第二生成单元 262，用于根据所述用户账户口令的哈希值加密所述装置密钥，生成装置密钥密文；发送单元 263，用于将所述装置密钥密文和所述装置公钥发送给所述终端。

[0256] 进一步地，上述第一确定模块 22，具体用于根据所述第二用户公钥判断所述第一签名是否与第三签名相同；其中，所述第三签名为所述终端根据所述第二用户密钥对所述挑战文进行签名处理得到的。

[0257] 本发明实施例提供的服务端，可以执行上述用户认证方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0258] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

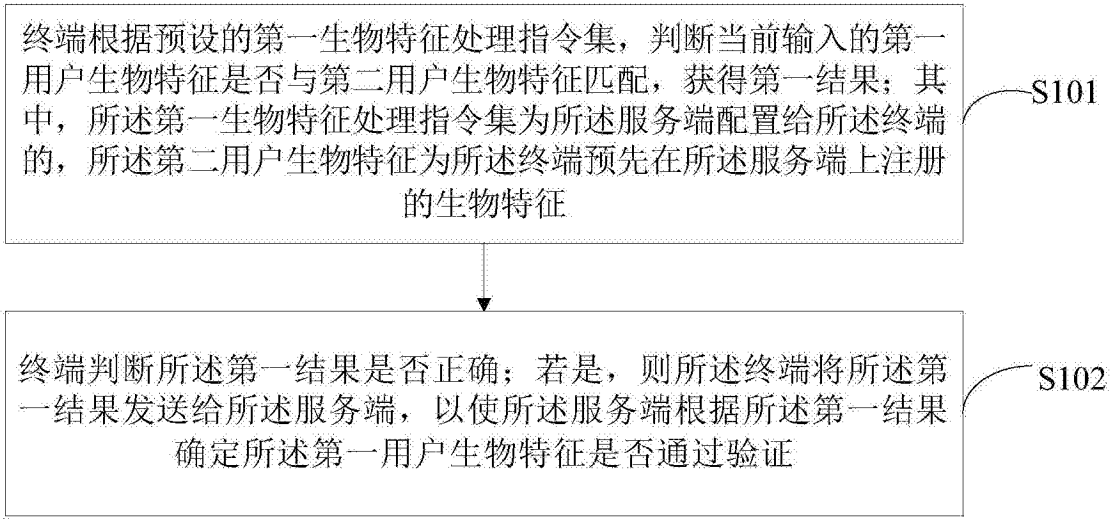

终端根据预设的第一生物特征处理指令集，判断当前输入的第一用户生物特征是否与第二用户生物特征匹配，获得第一结果；其中，所述第一生物特征处理指令集为所述服务端配置给所述终端的，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征
S101
终端判断所述第一结果是否正确；若是，则所述终端将所述第一结果发送给所述服务端，以使所述服务端根据所述第一结果确定所述第一用户生物特征是否通过验证
S102

图 1

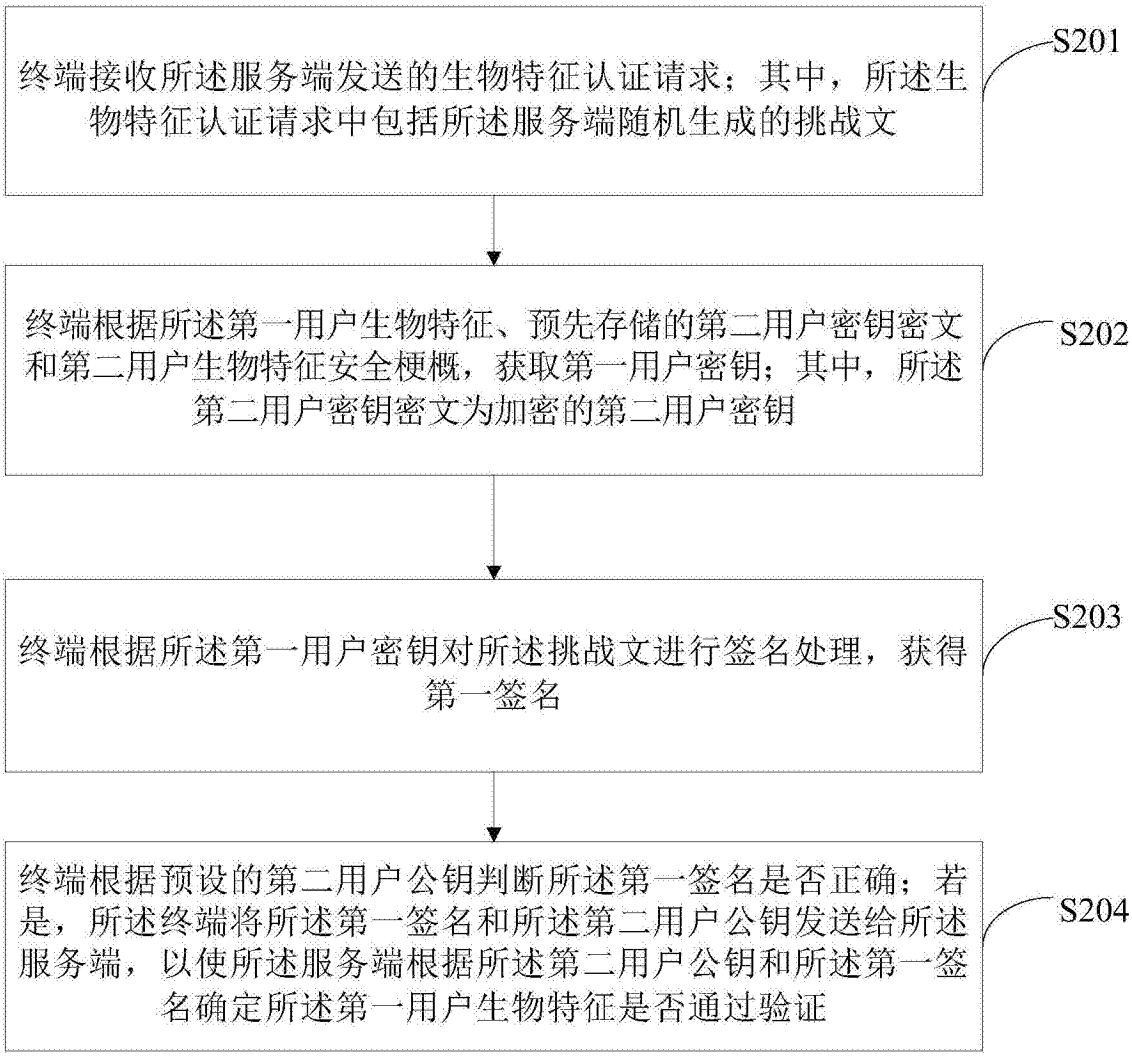

终端接收所述服务端发送的生物特征认证请求；其中，所述生物特征认证请求中包括所述服务端随机生成的挑战文
S201
终端根据所述第一用户生物特征、预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥
S202
终端根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名
S203
终端根据预设的第二用户公钥判断所述第一签名是否正确；若是，所述终端将所述第一签名和所述第二用户公钥发送给所述服务端，以使所述服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证
S204

图 2

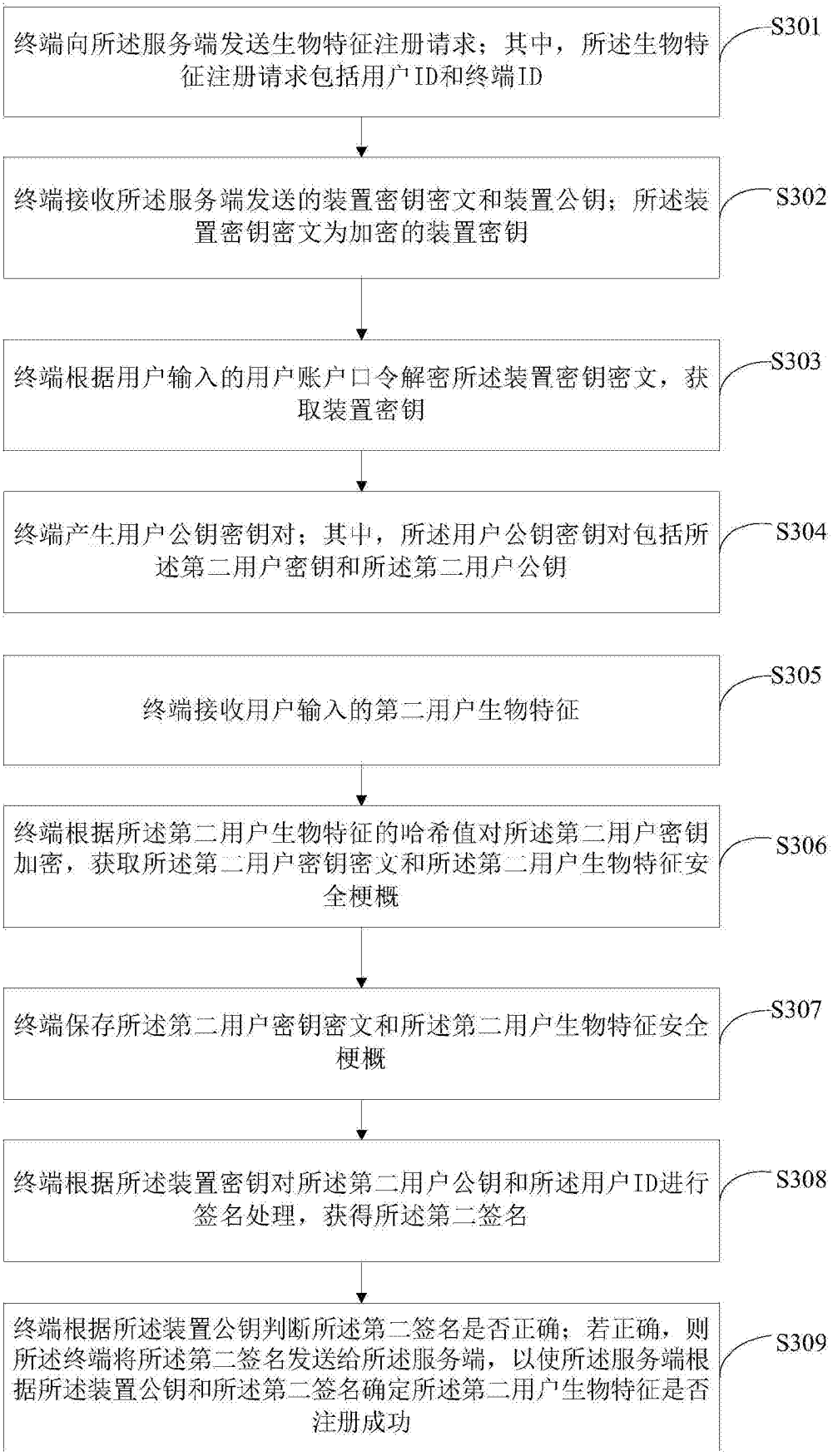

终端向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户ID和终端ID
S301
终端接收所述服务端发送的装置密钥密文和装置公钥；所述装置密钥密文为加密的装置密钥
S302
终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥
S303
终端产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥
S304
终端接收用户输入的第二用户生物特征
S305
终端根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概
S306
终端保存所述第二用户密钥密文和所述第二用户生物特征安全梗概
S307
终端根据所述装置密钥对所述第二用户公钥和所述用户ID进行签名处理，获得所述第二签名
S308
终端根据所述装置公钥判断所述第二签名是否正确；若正确，则所述终端将所述第二签名发送给所述服务端，以使所述服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功
S309

图 3

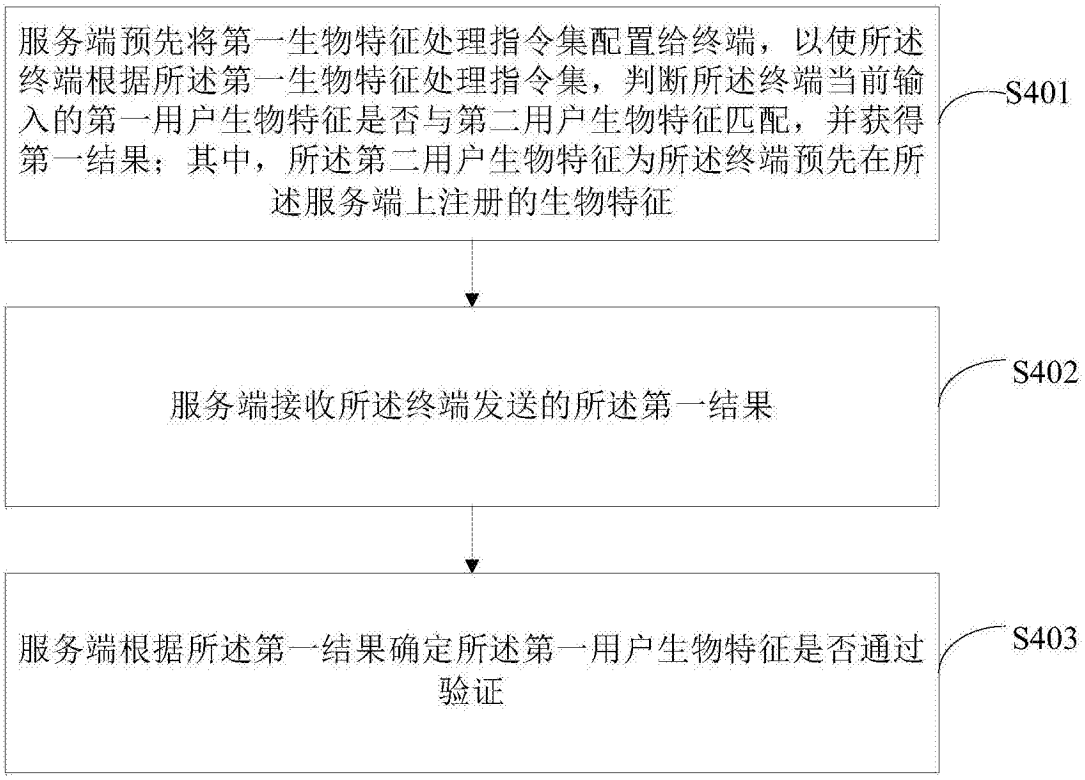

服务端预先将第一生物特征处理指令集配置给终端，以使所述终端根据所述第一生物特征处理指令集，判断所述终端当前输入的第一用户生物特征是否与第二用户生物特征匹配，并获得第一结果；其中，所述第二用户生物特征为所述终端预先在所述服务端上注册的生物特征
S401
服务端接收所述终端发送的所述第一结果
S402
服务端根据所述第一结果确定所述第一用户生物特征是否通过验证
S403

图 4

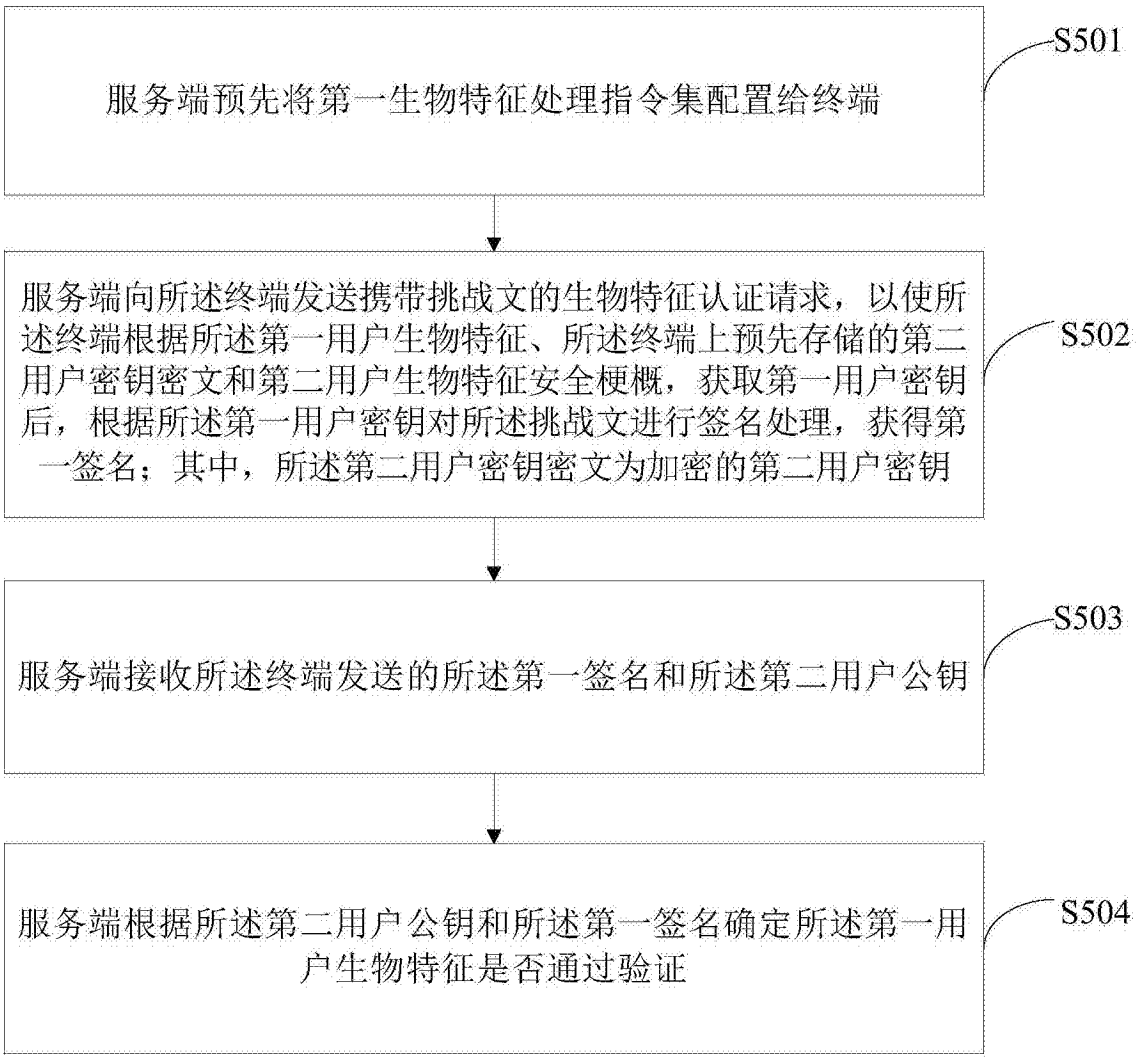

服务端预先将第一生物特征处理指令集配置给终端
S501
服务端向所述终端发送携带挑战文的生物特征认证请求，以使所述终端根据所述第一用户生物特征、所述终端上预先存储的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥后，根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名；其中，所述第二用户密钥密文为加密的第二用户密钥
S502
服务端接收所述终端发送的所述第一签名和所述第二用户公钥
S503
服务端根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证
S504

图 5

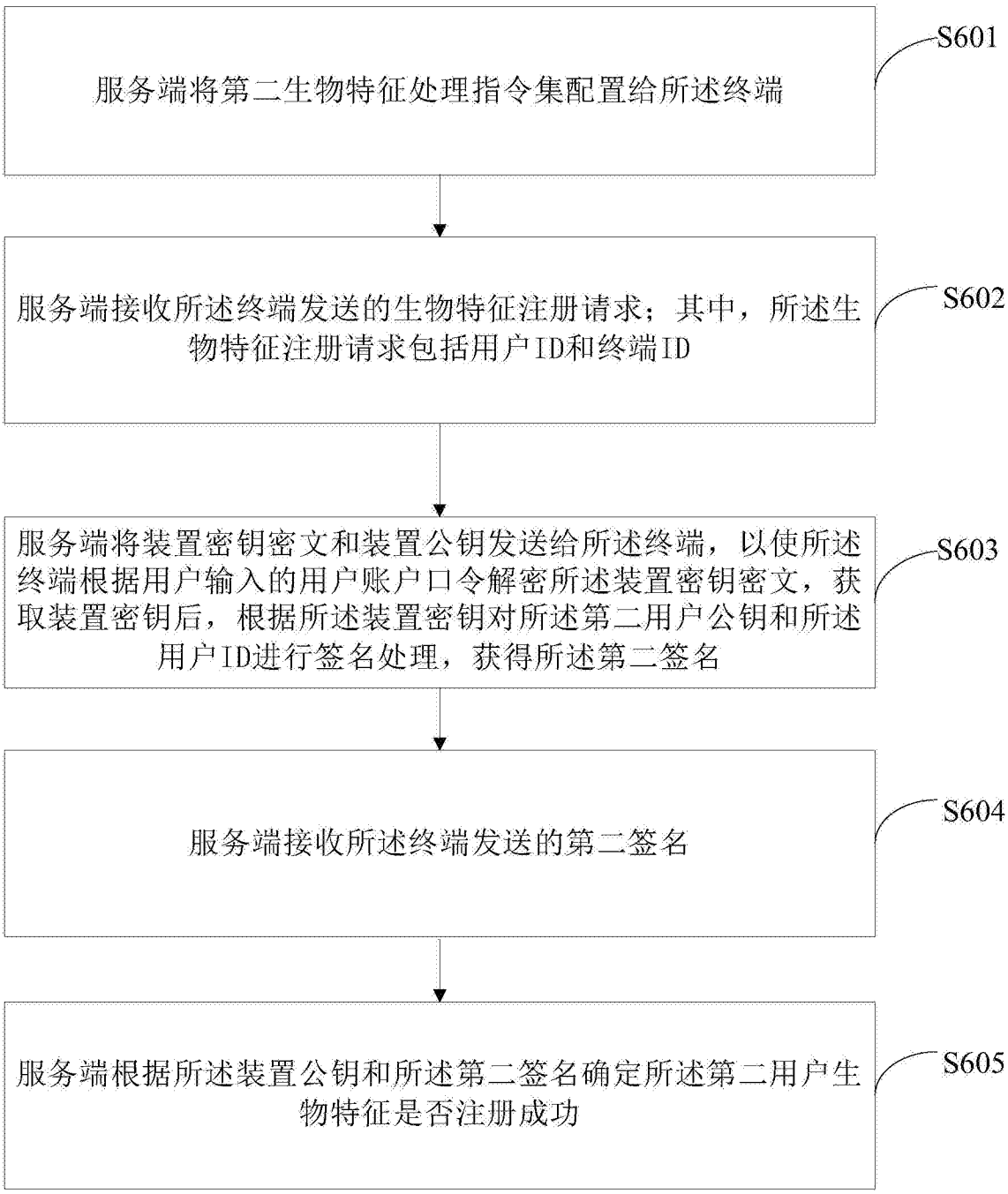

服务端将第二生物特征处理指令集配置给所述终端
S601
服务端接收所述终端发送的生物特征注册请求；其中，所述生物特征注册请求包括用户ID和终端ID
S602
服务端将装置密钥密文和装置公钥发送给所述终端，以使所述终端根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥后，根据所述装置密钥对所述第二用户公钥和所述用户ID进行签名处理，获得所述第二签名
S603
服务端接收所述终端发送的第二签名
S604
服务端根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功
S605

图 6

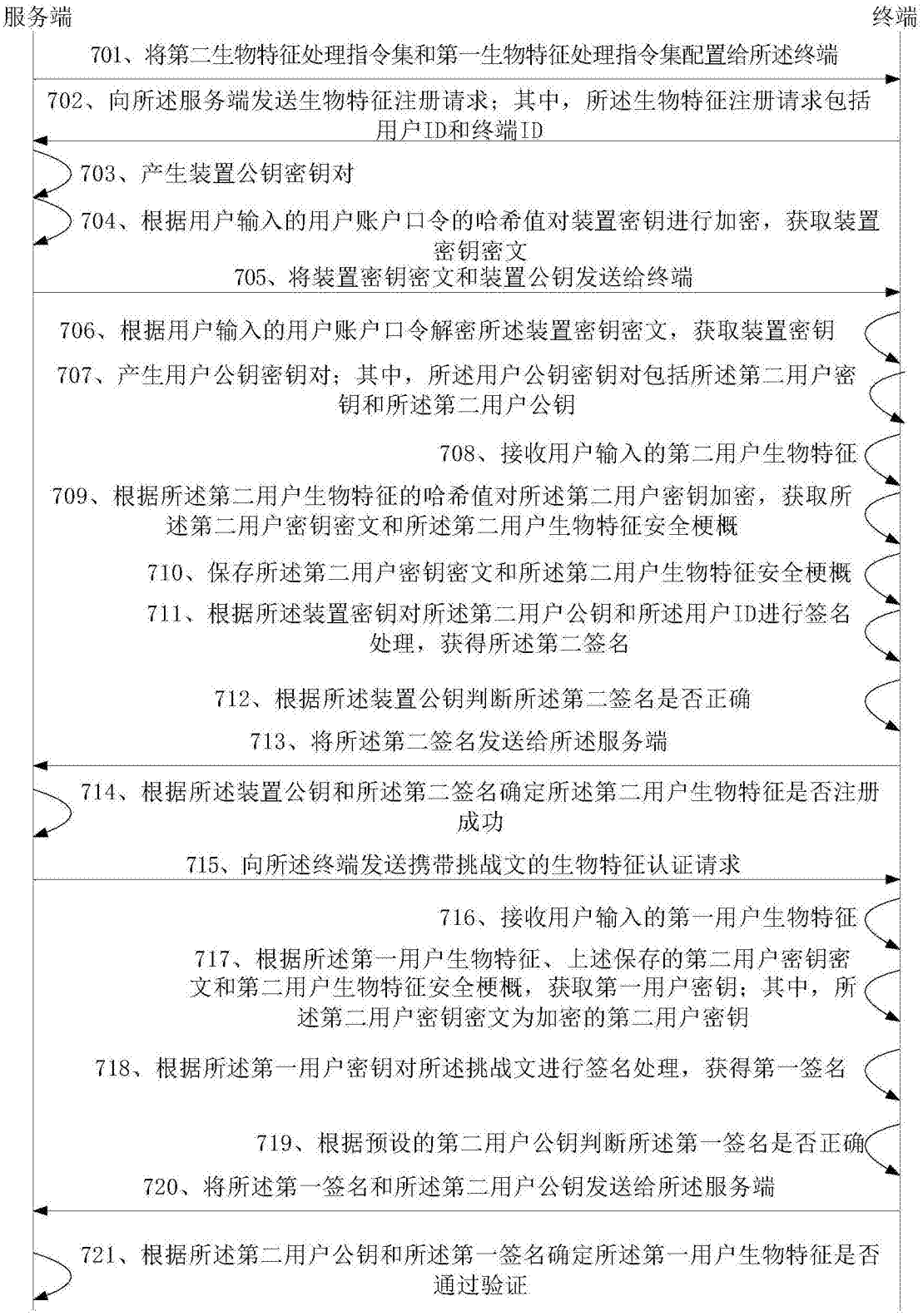

服务端
终端
701、将第二生物特征处理指令集和第一生物特征处理指令集配置给所述终端
702、向所述服务端发送生物特征注册请求；其中，所述生物特征注册请求包括用户ID和终端ID
703、产生装置公钥密钥对
704、根据用户输入的用户账户口令的哈希值对装置密钥进行加密，获取装置密钥密文
705、将装置密钥密文和装置公钥发送给终端
706、根据用户输入的用户账户口令解密所述装置密钥密文，获取装置密钥
707、产生用户公钥密钥对；其中，所述用户公钥密钥对包括所述第二用户密钥和所述第二用户公钥
708、接收用户输入的第二用户生物特征
709、根据所述第二用户生物特征的哈希值对所述第二用户密钥加密，获取所述第二用户密钥密文和所述第二用户生物特征安全梗概
710、保存所述第二用户密钥密文和所述第二用户生物特征安全梗概
711、根据所述装置密钥对所述第二用户公钥和所述用户ID进行签名处理，获得所述第二签名
712、根据所述装置公钥判断所述第二签名是否正确
713、将所述第二签名发送给所述服务端
714、根据所述装置公钥和所述第二签名确定所述第二用户生物特征是否注册成功
715、向所述终端发送携带挑战文的生物特征认证请求
716、接收用户输入的第一用户生物特征
717、根据所述第一用户生物特征、上述保存的第二用户密钥密文和第二用户生物特征安全梗概，获取第一用户密钥；其中，所述第二用户密钥密文为加密的第二用户密钥
718、根据所述第一用户密钥对所述挑战文进行签名处理，获得第一签名
719、根据预设的第二用户公钥判断所述第一签名是否正确
720、将所述第一签名和所述第二用户公钥发送给所述服务端
721、根据所述第二用户公钥和所述第一签名确定所述第一用户生物特征是否通过验证

图 7

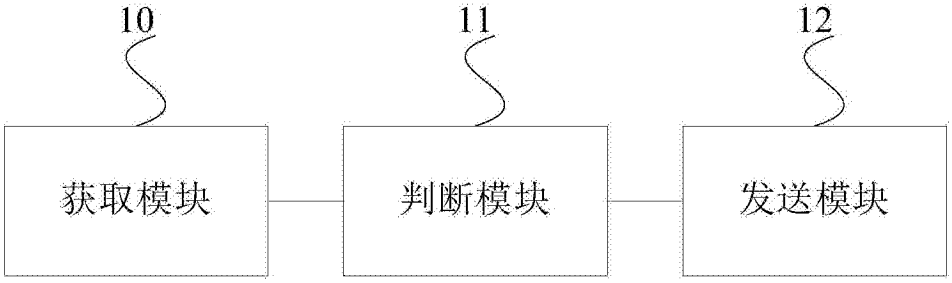

10
11
12
获取模块
判断模块
发送模块

图 8

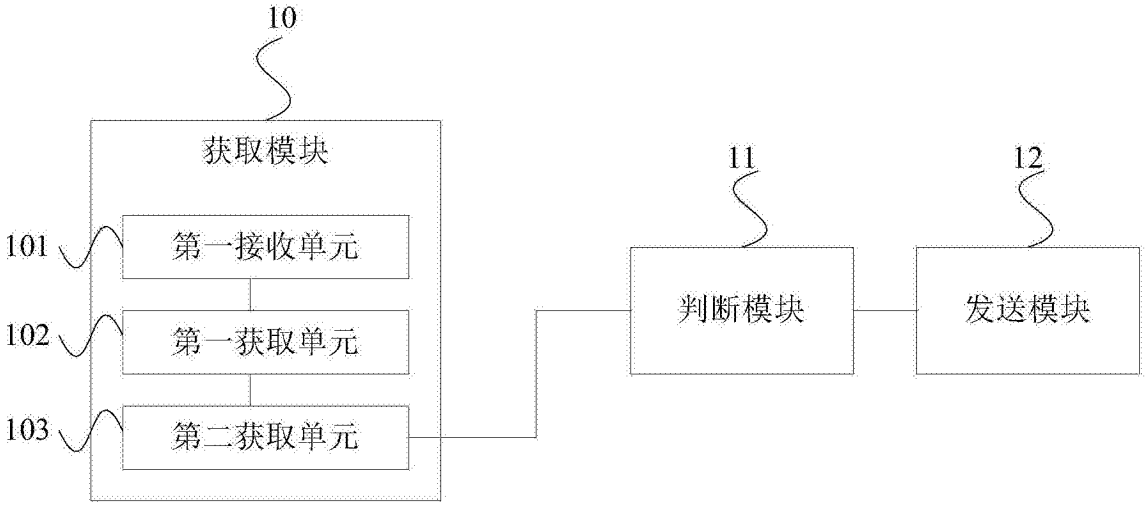

10
获取模块
101
第一接收单元
102
第一获取单元
103
第二获取单元
11
判断模块
12
发送模块

图 9

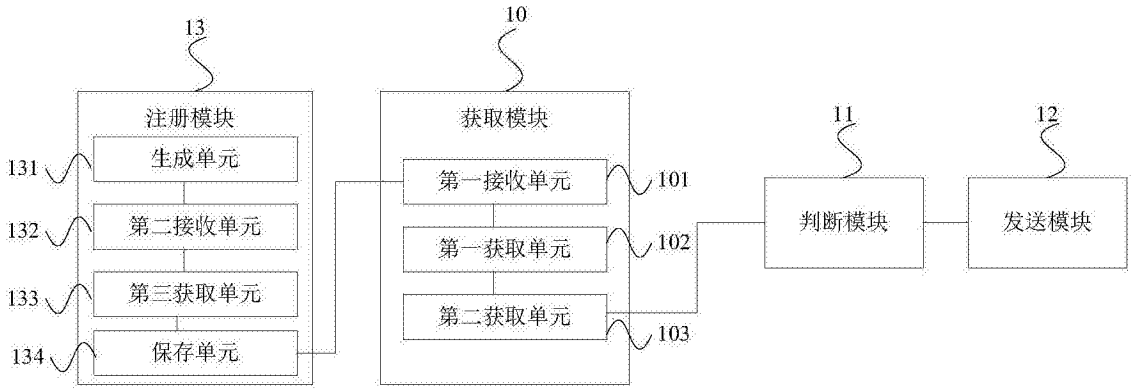

13
注册模块
131
生成单元
132
第二接收单元
133
第三获取单元
134
保存单元
10
获取模块
第一接收单元
101
第一获取单元
102
第二获取单元
103
11
判断模块
12
发送模块

图 10

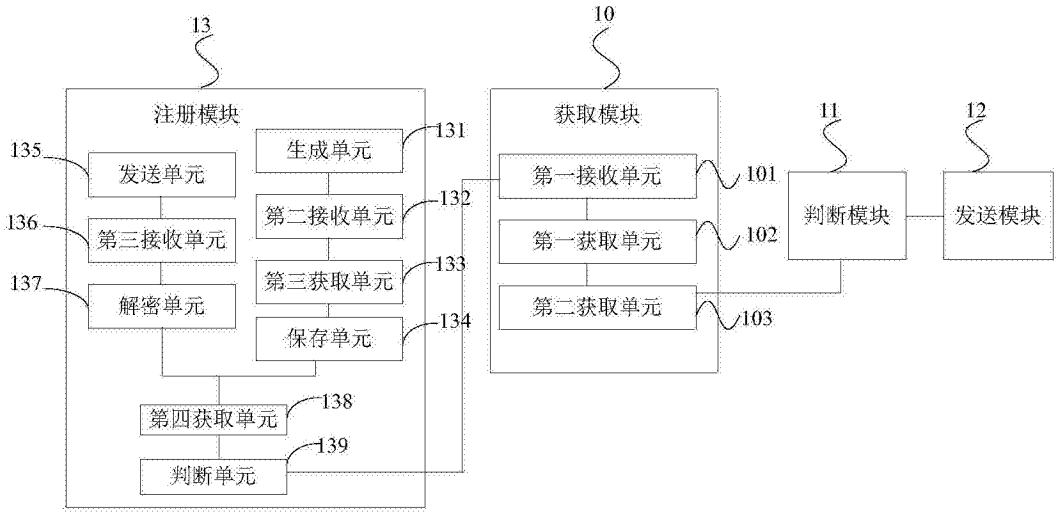

13
注册模块
生成单元
131
发送单元
135
第二接收单元
132
第三接收单元
136
第三获取单元
133
解密单元
137
保存单元
134
第四获取单元
138
判断单元
139
10
获取模块
第一接收单元
101
第一获取单元
102
第二获取单元
103
11
判断模块
12
发送模块

图 11


20
第一配置模块
21
第一接收模块
22
第一确定模块

图 12

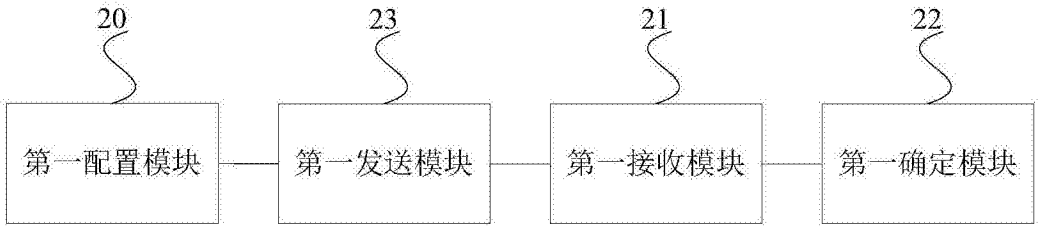

20
第一配置模块
23
第一发送模块
21
第一接收模块
22
第一确定模块

图 13

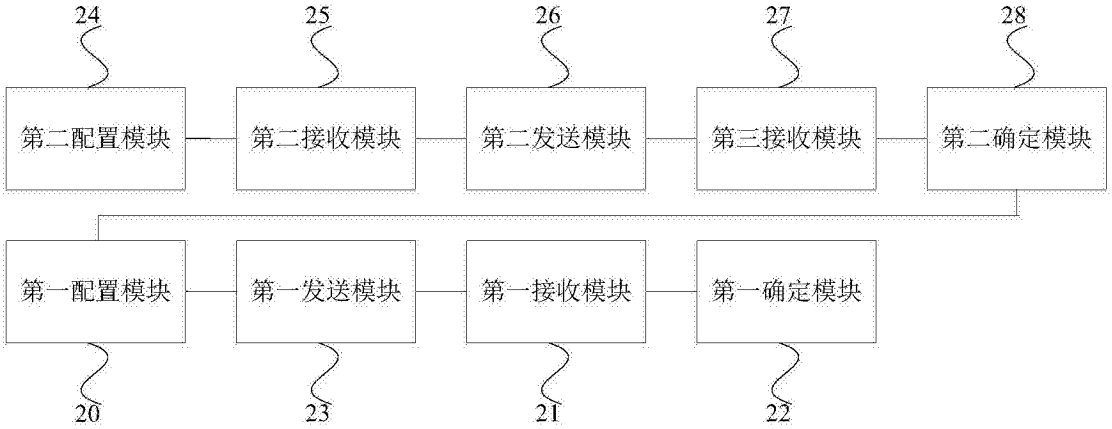

24
25
26
27
28
第二配置模块
第二接收模块
第二发送模块
第三接收模块
第二确定模块
第一配置模块
第一发送模块
第一接收模块
第一确定模块
20
23
21
22

图 14

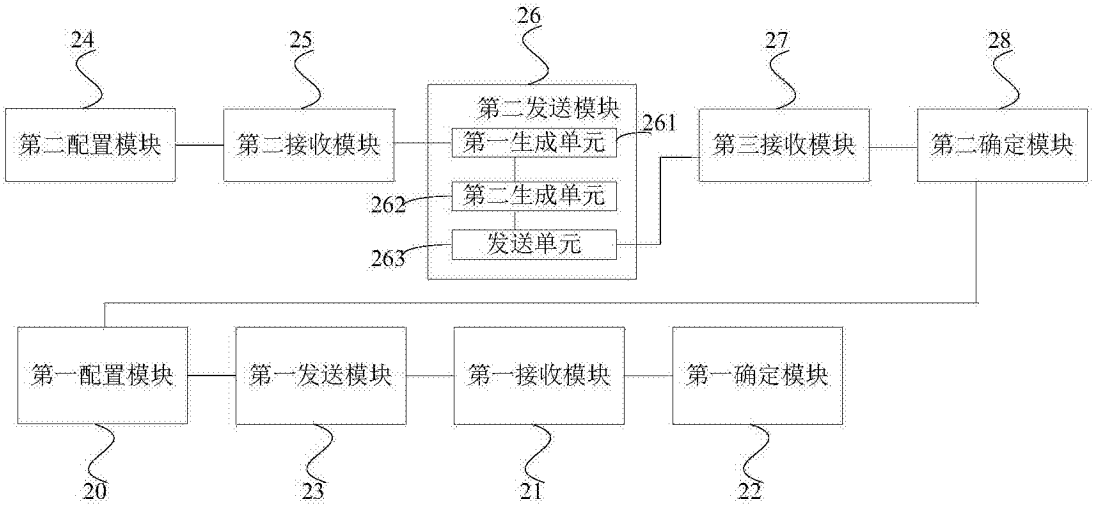

24
25
26
27
28
第二配置模块
第二接收模块
第二发送模块
第一生成单元
261
第二生成单元
262
发送单元
263
第三接收模块
第二确定模块
第一配置模块
第一发送模块
第一接收模块
第一确定模块
20
23
21
22

图 15