(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 106603461 A
(43)申请公布日 2017.04.26

(21)申请号 201510660391.4

(22)申请日 2015.10.14

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 徐俊

(74)专利代理机构 北京鸿德海业知识产权代理事务所(普通合伙) 11412
代理人 孟繁琦

(51)Int.Cl.
*H04L 29/06*(2006.01)

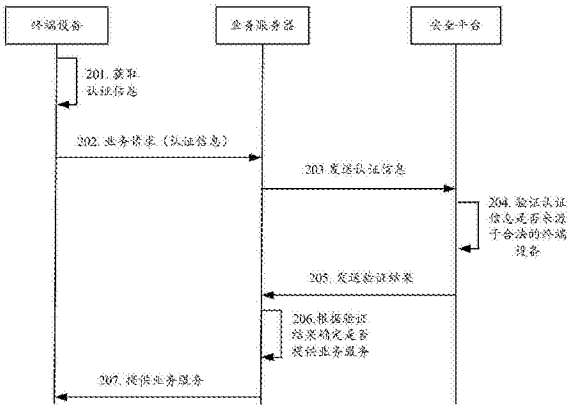
权利要求书6页 说明书17页 附图7页

(54)发明名称

一种业务认证的方法、装置和系统

(57)摘要

本发明提供了一种业务认证的方法、装置和系统，其中方法包括：接收终端设备发送的包含认证信息的业务请求；将所述认证信息发送给安全平台，由所述安全平台验证所述认证信息是否来源于合法的终端设备；依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务。本发明实现了在提供业务服务时基于终端的身份进行认证，能够有效地禁止对一些非法的终端设备提供业务服务。




CN 106603461 A

1. 一种业务认证的方法，其特征在于，该方法包括：

接收终端设备发送的包含认证信息的业务请求；

将所述认证信息发送给安全平台，由所述安全平台验证所述认证信息是否来源于合法的终端设备；

依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务。

2. 根据权利要求 1 所述的方法，其特征在于，所述认证信息包含所述终端设备的唯一设备标识；或者，

所述认证信息包含利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；或者，

所述认证信息包含明文信息或密文信息，所述明文信息包含所述终端设备的唯一设备标识，所述密文信息为利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；

所述密钥信息是所述安全平台预先提供给合法的终端设备的。

3. 根据权利要求 2 所述的方法，其特征在于，所述密钥信息为所述安全平台针对合法的终端设备的唯一设备标识生成的公钥 - 私钥对中的公钥或私钥。

4. 根据权利要求 1 所述的方法，其特征在于，依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务包括：

如果所述安全平台返回的验证结果为所述认证信息来源于合法的终端设备，则向所述终端设备提供业务服务；或者，

如果所述安全平台返回的验证结果为所述认证信息来源于非法的终端设备，则禁止向所述终端设备提供业务服务；或者，

如果所述安全平台返回的验证结果为一致性验证失败，则向所述终端设备返回一致性验证失败的提示信息。

5. 根据权利要求 1 至 4 任一权项所述的方法，其特征在于，所述业务服务包括：

对所述终端设备的激活、云端数据存储服务或者下发多媒体数据。

6. 一种业务认证的方法，其特征在于，该方法包括：

安全平台接收认证信息；

验证所述认证信息是否来源于合法的终端设备；

返回验证结果，以便业务服务器根据验证结果确定是否向发送所述认证信息的终端设备提供业务服务。

7. 根据权利要求 6 所述的方法，其特征在于，所述安全平台存储有合法终端设备的唯一设备标识；

验证所述认证信息是否来源于合法的终端设备包括：

判断所述认证信息包含的设备标识是否为所述安全平台存储的合法终端设备的唯一设备标识，如果是，则确定所述认证信息来源于合法的终端设备。

8. 根据权利要求 7 所述的方法，其特征在于，所述认证信息包括利用密钥信息对所述设备标识进行加密后得到的密文信息；

所述密钥信息为所述安全平台预先生成并提供给合法的终端设备的；

该方法还包括：所述安全平台利用本地保存的所述设备标识对应的密钥信息对所述认

证信息中的密文信息进行解密，得到所述设备标识。

9. 根据权利要求 7 所述的方法，其特征在于，所述认证信息包含明文信息和密文信息，所述明文信息包含所述设备标识，所述密文信息为利用密钥信息对包含所述设备标识的信息进行加密后的密文信息；

所述密钥信息为所述安全平台预先生成并提供给合法的终端设备的；

该方法还包括：所述安全平台利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密；

将解密得到的信息与所述明文信息进行一致性验证，如果验证失败，则返回一致性验证失败的验证结果。

10. 根据权利要求 8 或 9 所述的方法，其特征在于，所述安全平台提供给合法的终端设备的密钥信息为所述安全平台生成的公钥 - 私钥对中的公钥，所述安全平台解密时采用的为所述公钥对应的私钥；或者，

所述安全平台提供给合法终端设备的密钥信息为所述安全平台生成的公钥 - 私钥对中的私钥，所述安全平台解密时采用的为所述私钥对应的公钥。

11. 根据权利要求 7 所述的方法，其特征在于，所述安全平台存储的合法终端设备的唯一设备标识由标识分配设备分配。

12. 根据权利要求 11 所述的方法，其特征在于，所述标识分配设备分配合法终端设备的唯一设备标识包括：

所述标识分配设备接收针对合法终端设备的标识分配请求；

针对所述合法终端设备分配唯一设备标识；

发送所述设备标识，供标识写入设备将所述唯一设备标识写入所述合法终端设备。

13. 根据权利要求 12 所述的方法，其特征在于，针对所述合法终端设备分配唯一设备标识包括：

所述标识分配设备依据预设的标识生成规则以及利用所述标识分配请求包含的合法终端设备的设备信息，生成唯一的设备标识。

14. 根据权利要求 13 所述的方法，其特征在于，所述标识生成规则包括：

设备标识依次包括设备标识符、厂商编号、待分配标识的设备信息和随机数。

15. 根据权利要求 13 或 14 所述的方法，其特征在于，所述合法终端设备的设备信息包括：

待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。

16. 根据权利要求 12 所述的方法，其特征在于，该方法还包括：

所述标识分配设备针对所述待分配标识的设备分配许可信息；

发送所述许可信息；

接收到许可信息后，若接收到的许可信息与分配的许可信息一致，则发送所述设备标识。

17. 根据权利要求 16 所述的方法，其特征在于，所述标识分配请求包含密钥信息；

发送的所述许可信息为利用所述密钥信息加密后的许可信息。

18. 根据权利要求 16 所述的方法，其特征在于，该方法还包括：所述标识分配设备保存针对所述合法终端设备生成的唯一设备标识和许可信息的对应关系；

发送所述唯一设备标识包括：发送接收到的许可信息对应的唯一设备标识。

19. 根据权利要求 12 所述的方法，其特征在于，所述标识分配设备分配合法终端设备的唯一设备标识还包括：

所述安全平台生成密钥信息；

将生成的密钥信息的全部或部分连同所述设备标识一起发送，供所述标识写入设备将所述密钥信息的全部或部分写入所述合法终端设备。

20. 根据权利要求 19 所述的方法，其特征在于，若所述标识分配设备生成密钥信息时采用对称加密算法，则将生成的密钥信息的全部连同所述设备标识一起发送；

若所述标识分配设备生成密钥信息时采用非对称加密算法，则将生成的私钥或公钥中的一个连同所述设备标识一起发送。

21. 根据权利要求 13 所述的方法，其特征在于，所述安全平台包括颁发中心和各级分发中心；

所述颁发中心下发标识生成规则给各级分发中心，由各级分发中心负责接收所述标识分配请求、生成所述设备标识、发送给标识写入设备并将生成的设备标识上报所述颁发中心；或者，

由各级分发中心负责接收所述标识分配请求并转发给所述颁发中心；由所述颁发中心按照标识生成规则生成设备标识，再将设备标识经由各级分发中心转发给标识写入设备。

22. 根据权利要求 21 所述的方法，其特征在于，所述安全平台还包括：各级认证中心；

各级认证中心接收到所述认证信息后，判断本地是否存储有所述认证信息包含的设备标识，如果是，则确定所述认证信息来源于合法的终端设备，并返回验证结果；否则，将所述认证信息上报给其上一级的认证中心或颁发中心；

所述颁发中心接收到所述认证信息后，判断本地是否存储有所述认证信息包含的设备标识，如果是，则确定所述认证信息来源于合法的终端设备，并经由各级认证中心返回验证结果；否则，将确定所述认证信息来源于非法的终端设备，并经由各级认证中心返回验证结果。

23. 根据权利要求 22 所述的方法，其特征在于，该方法还包括：

所述颁发中心预先将本地存储的设备标识分发给各级认证中心进行存储；或者，

若验证结果为所述认证信息来源于合法的终端设备，则接收到该验证结果的各级认证中心在本地存储所述认证信息中的设备标识。

24. 一种业务认证的方法，其特征在于，该方法包括：

终端设备获取认证信息；

发送包含所述认证信息的业务请求。

25. 根据权利要求 24 所述的方法，其特征在于，所述终端设备获取认证信息包括：

所述终端设备获取被写入的唯一设备标识。

26. 根据权利要求 25 所述的方法，其特征在于，所述终端设备获取认证信息还包括：

所述终端设备获取被写入的密钥信息；

利用所述密钥信息对所述唯一设备标识进行加密，形成密文信息；

利用所述密文信息形成所述认证信息，或者利用包含所述唯一设备标识的明文信息以及所述密文信息形成所述认证信息。

27. 一种业务认证的装置，其特征在于，该装置包括：

终端侧交互单元，用于接收终端设备发送的包含认证信息的业务请求；

网络侧交互单元，用于将所述认证信息发送给安全平台，由所述安全平台验证所述认证信息是否来源于合法的终端设备；接收所述安全平台返回的验证结果；

业务处理单元，用于依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务。

28. 根据权利要求 27 所述的装置，其特征在于，所述认证信息包含所述终端设备的唯一设备标识；或者，

所述认证信息包含利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；或者，

所述认证信息包含明文信息或密文信息，所述明文信息包含所述终端设备的唯一设备标识，所述密文信息为利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；

所述密钥信息是所述安全平台预先提供给合法的终端设备的。

29. 根据权利要求 28 所述的装置，其特征在于，所述密钥信息为所述安全平台针对合法的终端设备的唯一设备标识生成的公钥 - 私钥对中的公钥或私钥。

30. 根据权利要求 27 所述的装置，其特征在于，所述业务处理单元具体用于：

如果所述安全平台返回的验证结果为所述认证信息来源于合法的终端设备，则向所述终端设备提供业务服务；或者，

如果所述安全平台返回的验证结果为所述认证信息来源于非法的终端设备，则禁止向所述终端设备提供业务服务；或者，

如果所述安全平台返回的验证结果为一致性验证失败，则向所述终端设备返回一致性验证失败的提示信息。

31. 根据权利要求 27 至 30 任一权项所述的装置，其特征在于，所述业务处理单元执行的业务服务包括：

对所述终端设备的激活、云端数据存储服务或者下发多媒体数据。

32. 一种业务认证的装置，该装置设置于安全平台，其特征在于，该装置包括：

接收单元，用于接收认证信息；

第一验证单元，用于验证所述认证信息是否来源于合法的终端设备；

发送单元，用于返回验证结果，以便业务服务器根据验证结果确定是否向发送所述认证信息的终端设备提供业务服务。

33. 根据权利要求 32 所述的装置，其特征在于，该装置还包括：

维护单元，用于存储合法终端设备的唯一设备标识；

所述第一验证单元，具体用于判断所述认证信息包含的设备标识是否为所述安全平台存储的合法终端设备的唯一设备标识，如果是，则确定所述认证信息来源于合法的终端设备。

34. 根据权利要求 33 所述的装置，其特征在于，所述认证信息包括利用密钥信息对所述设备标识进行加密后得到的密文信息；

该装置还包括：第一加解密单元，用于预先生成所述密钥信息并提供给合法的终端设

备；利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密，得到所述设备标识。

35. 根据权利要求 33 所述的装置，其特征在于，所述认证信息包含明文信息和密文信息，所述明文信息包含所述设备标识，所述密文信息为利用密钥信息对包含所述设备标识的信息进行加密后得到的；

该装置还包括：第一加解密单元，用于预先生成所述密钥信息并提供给合法的终端设备；利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密；

所述第一验证单元，还用于将所述第一加解密单元解密得到的信息与所述明文信息进行一致性验证，如果验证失败，则触发所述发送单元返回一致性验证失败的验证结果给所述业务服务器。

36. 根据权利要求 34 或 35 所述的装置，其特征在于，所述第一加解密单元提供给合法的终端设备的密钥信息为生成的公钥－私钥对中的公钥，解密时采用的为所述公钥对应的私钥；或者，

所述第一加解密单元提供给合法终端设备的密钥信息为生成的公钥－私钥对中的私钥，解密时采用的为所述私钥对应的公钥。

37. 根据权利要求 33 所述的装置，其特征在于，该装置还包括：

分配单元，用于分配合法终端设备的唯一设备标识。

38. 根据权利要求 37 所述的装置，其特征在于，所述接收单元，还用于接收针对合法终端设备的标识分配请求；

所述分配单元针对所述合法终端设备分配唯一设备标识；

所述发送单元，还用于发送所述设备标识，供标识写入设备将所述唯一设备标识写入所述合法终端设备。

39. 根据权利要求 38 所述的装置，其特征在于，所述分配单元，还用于依据预设的标识生成规则以及利用所述标识分配请求包含的合法终端设备的设备信息，生成唯一的设备标识。

40. 根据权利要求 39 所述的装置，其特征在于，所述标识生成规则包括：

设备标识由设备标识符、厂商编号、待分配标识的设备信息和随机数依次组成。

41. 根据权利要求 39 或 40 所述的装置，其特征在于，所述合法终端设备的设备信息包括：

待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。

42. 根据权利要求 38 所述的装置，其特征在于，该装置还包括第二验证单元；

所述分配单元，还用于针对所述待分配标识的设备分配许可信息；

所述发送单元，还用于发送所述许可信息；

所述接收单元，还用于接收许可信息；

所述第二验证单元，用于验证所述接收单元接收到的许可信息是否与所述分配单元分配的许可信息一致，如果是，则触发所述发送单元发送所述设备标识。

43. 根据权利要求 42 所述的装置，其特征在于，所述标识分配请求包含密钥信息；该装置还包括：

第二加解密单元，用于利用所述密钥信息对所述分配的许可信息进行加密；

所述发送单元发送加密后的许可信息。

44. 根据权利要求 42 所述的装置，其特征在于，所述维护单元，还用于保存针对所述合法终端设备生成的唯一设备标识和许可信息的对应关系；

所述发送单元在发送所述唯一设备标识时，具体发送所述接收单元接收到的许可信息对应的唯一设备标识。

45. 根据权利要求 38 所述的装置，其特征在于，该装置还包括：

第一加解密单元，用于生成密钥信息，并将生成的密钥信息的全部或部分提供给所述发送单元，由所述发送单元连同所述设备标识一起发送，供所述标识写入设备将所述密钥信息的全部或部分写入所述合法终端设备。

46. 一种业务认证的装置，该装置设置于终端设备，其特征在于，该装置包括：

认证服务单元，用于获取认证信息；

业务服务单元，用于发送包含所述认证信息的业务请求。

47. 根据权利要求 46 所述的装置，其特征在于，所述认证服务单元，具体用于：获取被写入的唯一设备标识。

48. 根据权利要求 47 所述的装置，其特征在于，所述认证服务单元，还用于获取被写入的密钥信息，利用所述密钥信息对所述唯一设备标识进行加密，形成密文信息；

所述业务服务单元，具体用于利用所述密文形成所述认证信息，或者利用包含所述唯一设备标识的明文信息以及所述密文信息形成所述认证信息。

49. 一种业务认证的系统，其特征在于，该系统包括：终端设备、业务服务器和安全平台；

所述终端设备包括如权利要求 46 至 48 任一权项所述的装置；

所述业务服务器包括如权利要求 27 至 30 任一权项所述的装置；

所述安全平台包括如权利要求 32 至 35、37 至 40、42 至 45 任一权项所述的装置。

# 一种业务认证的方法、装置和系统

## 【技术领域】

[0001] 本发明涉及计算机应用技术领域，特别涉及一种业务认证的方法、装置和系统。

## 【背景技术】

[0002] 现有大部分的服务提供者在提供业务服务时需要进行身份认证，而目前进行的身份认证均是针对用户身份的。即用户在终端设备上登录账户，终端设备在进行业务请求时会携带用户的账户信息，业务服务器对该账户信息进行认证，如果身份合法，则向该终端设备提供业务服务。

[0003] 在提供业务服务时，未发现对于终端设备的身份进行认证的技术。但往往有一些这样的场景需求，可能存在对于一些非法的终端设备，例如仿冒的终端设备，需要禁止对这些非法的终端设备提供业务服务。

## 【发明内容】

[0004] 有鉴于此，本发明提供了一种业务认证的方法和装置，以便于实现在提供业务服务时基于终端设备的身份进行认证。

[0005] 具体技术方案如下：

[0006] 本发明提供了一种业务认证的方法，其特征在于，该方法包括：

[0007] 接收终端设备发送的包含认证信息的业务请求；

[0008] 将所述认证信息发送给安全平台，由所述安全平台验证所述认证信息是否来源于合法的终端设备；

[0009] 依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务。

[0010] 根据本发明一优选实施方式，所述认证信息包含所述终端设备的唯一设备标识；或者，

[0011] 所述认证信息包含利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；或者，

[0012] 所述认证信息包含明文信息或密文信息，所述明文信息包含所述终端设备的唯一设备标识，所述密文信息为利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；

[0013] 所述密钥信息是所述安全平台预先提供给合法的终端设备的。

[0014] 根据本发明一优选实施方式，所述密钥信息为所述安全平台针对合法的终端设备的唯一设备标识生成的公钥－私钥对中的公钥或私钥。

[0015] 根据本发明一优选实施方式，依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务包括：

[0016] 如果所述安全平台返回的验证结果为所述认证信息来源于合法的终端设备，则向所述终端设备提供业务服务；或者，

[0017] 如果所述安全平台返回的验证结果为所述认证信息来源于非法的终端设备，则禁

止向所述终端设备提供业务服务；或者，

[0018] 如果所述安全平台返回的验证结果为一致性验证失败，则向所述终端设备返回一致性验证失败的提示信息。

[0019] 根据本发明一优选实施方式，所述业务服务包括：

[0020] 对所述终端设备的激活、云端数据存储服务或者下发多媒体数据。

[0021] 本发明还提供了一种业务认证的方法，该方法包括：

[0022] 安全平台接收认证信息；

[0023] 验证所述认证信息是否来源于合法的终端设备；

[0024] 返回验证结果，以便业务服务器根据验证结果确定是否向发送所述认证信息的终端设备提供业务服务。

[0025] 根据本发明一优选实施方式，所述安全平台存储有合法终端设备的唯一设备标识；

[0026] 验证所述认证信息是否来源于合法的终端设备包括：

[0027] 判断所述认证信息包含的设备标识是否为所述安全平台存储的合法终端设备的唯一设备标识，如果是，则确定所述认证信息来源于合法的终端设备。

[0028] 根据本发明一优选实施方式，所述认证信息包括利用密钥信息对所述设备标识进行加密后得到的密文信息；

[0029] 所述密钥信息为所述安全平台预先生成并提供给合法的终端设备的；

[0030] 该方法还包括：所述安全平台利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密，得到所述设备标识。

[0031] 根据本发明一优选实施方式，所述认证信息包含明文信息和密文信息，所述明文信息包含所述设备标识，所述密文信息为利用密钥信息对包含所述设备标识的信息进行加密后的密文信息；

[0032] 所述密钥信息为所述安全平台预先生成并提供给合法的终端设备的；

[0033] 该方法还包括：所述安全平台利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密；

[0034] 将解密得到的信息与所述明文信息进行一致性验证，如果验证失败，则返回一致性验证失败的验证结果。

[0035] 根据本发明一优选实施方式，所述安全平台提供给合法的终端设备的密钥信息为所述安全平台生成的公钥－私钥对中的公钥，所述安全平台解密时采用的为所述公钥对应的私钥；或者，

[0036] 所述安全平台提供给合法终端设备的密钥信息为所述安全平台生成的公钥－私钥对中的私钥，所述安全平台解密时采用的为所述私钥对应的公钥。

[0037] 根据本发明一优选实施方式，所述安全平台存储的合法终端设备的唯一设备标识由标识分配设备分配。

[0038] 根据本发明一优选实施方式，所述标识分配设备分配合法终端设备的唯一设备标识包括：

[0039] 所述标识分配设备接收针对合法终端设备的标识分配请求；

[0040] 针对所述合法终端设备分配唯一设备标识；

[0041] 发送所述设备标识，供标识写入设备将所述唯一设备标识写入所述合法终端设备。

[0042] 根据本发明一优选实施方式，针对所述合法终端设备分配唯一设备标识包括：

[0043] 所述标识分配设备依据预设的标识生成规则以及利用所述标识分配请求包含的合法终端设备的设备信息，生成唯一的设备标识。

[0044] 根据本发明一优选实施方式，所述标识生成规则包括：

[0045] 设备标识依次包括设备标识符、厂商编号、待分配标识的设备信息和随机数。

[0046] 根据本发明一优选实施方式，所述合法终端设备的设备信息包括：

[0047] 待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。

[0048] 根据本发明一优选实施方式，该方法还包括：

[0049] 所述标识分配设备针对所述待分配标识的设备分配许可信息；

[0050] 发送所述许可信息；

[0051] 接收到许可信息后，若接收到的许可信息与分配的许可信息一致，则发送所述设备标识。

[0052] 根据本发明一优选实施方式，所述标识分配请求包含密钥信息；

[0053] 发送的所述许可信息为利用所述密钥信息加密后的许可信息。

[0054] 根据本发明一优选实施方式，该方法还包括：所述标识分配设备保存针对所述合法终端设备生成的唯一设备标识和许可信息的对应关系；

[0055] 发送所述唯一设备标识包括：发送接收到的许可信息对应的唯一设备标识。

[0056] 根据本发明一优选实施方式，所述标识分配设备分配合法终端设备的唯一设备标识还包括：

[0057] 所述安全平台生成密钥信息；

[0058] 将生成的密钥信息的全部或部分连同所述设备标识一起发送，供所述标识写入设备将所述密钥信息的全部或部分写入所述合法终端设备。

[0059] 根据本发明一优选实施方式，若所述标识分配设备生成密钥信息时采用对称加密算法，则将生成的密钥信息的全部连同所述设备标识一起发送；

[0060] 若所述标识分配设备生成密钥信息时采用非对称加密算法，则将生成的私钥或公钥中的一个连同所述设备标识一起发送。

[0061] 根据本发明一优选实施方式，所述安全平台包括颁发中心和各级分发中心；

[0062] 所述颁发中心下发标识生成规则给各级分发中心，由各级分发中心负责接收所述标识分配请求、生成所述设备标识、发送给标识写入设备并将生成的设备标识上报所述颁发中心；或者，

[0063] 由各级分发中心负责接收所述标识分配请求并转发给所述颁发中心；由所述颁发中心按照标识生成规则生成设备标识，再将设备标识经由各级分发中心转发给标识写入设备。

[0064] 根据本发明一优选实施方式，所述安全平台还包括：各级认证中心；

[0065] 各级认证中心接收到所述认证信息后，判断本地是否存储有所述认证信息包含的设备标识，如果是，则确定所述认证信息来源于合法的终端设备，并返回验证结果；否则，将所述认证信息上报给其上一级的认证中心或颁发中心；

[0066] 所述颁发中心接收到所述认证信息后，判断本地是否存储有所述认证信息包含的设备标识，如果是，则确定所述认证信息来源于合法的终端设备，并经由各级认证中心返回验证结果；否则，将确定所述认证信息来源于非法的终端设备，并经由各级认证中心返回验证结果。

[0067] 根据本发明一优选实施方式，该方法还包括：

[0068] 所述颁发中心预先将本地存储的设备标识分发给各级认证中心进行存储；或者，

[0069] 若验证结果为所述认证信息来源于合法的终端设备，则接收到该验证结果的各级认证中心在本地存储所述认证信息中的设备标识。

[0070] 本发明还提供了一种业务认证的方法，其特征在于，该方法包括：

[0071] 终端设备获取认证信息；

[0072] 发送包含所述认证信息的业务请求。

[0073] 根据本发明一优选实施方式，所述终端设备获取认证信息包括：

[0074] 所述终端设备获取被写入的唯一设备标识。

[0075] 根据本发明一优选实施方式，所述终端设备获取认证信息还包括：

[0076] 所述终端设备获取被写入的密钥信息；

[0077] 利用所述密钥信息对所述唯一设备标识进行加密，形成密文信息；

[0078] 利用所述密文信息形成所述认证信息，或者利用包含所述唯一设备标识的明文信息以及所述密文信息形成所述认证信息。

[0079] 本发明还提供了一种业务认证的装置，该装置包括：

[0080] 终端侧交互单元，用于接收终端设备发送的包含认证信息的业务请求；

[0081] 网络侧交互单元，用于将所述认证信息发送给安全平台，由所述安全平台验证所述认证信息是否来源于合法的终端设备；接收所述安全平台返回的验证结果；

[0082] 业务处理单元，用于依据所述安全平台返回的验证结果，确定是否向所述终端设备提供业务服务。

[0083] 根据本发明一优选实施方式，所述认证信息包含所述终端设备的唯一设备标识；或者，

[0084] 所述认证信息包含利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；或者，

[0085] 所述认证信息包含明文信息或密文信息，所述明文信息包含所述终端设备的唯一设备标识，所述密文信息为利用密钥信息对包含所述终端设备的唯一设备标识的信息进行加密后的密文信息；

[0086] 所述密钥信息是所述安全平台预先提供给合法的终端设备的。

[0087] 根据本发明一优选实施方式，所述密钥信息为所述安全平台针对合法的终端设备的唯一设备标识生成的公钥－私钥对中的公钥或私钥。

[0088] 根据本发明一优选实施方式，所述业务处理单元具体用于：

[0089] 如果所述安全平台返回的验证结果为所述认证信息来源于合法的终端设备，则向所述终端设备提供业务服务；或者，

[0090] 如果所述安全平台返回的验证结果为所述认证信息来源于非法的终端设备，则禁止向所述终端设备提供业务服务；或者，

[0091] 如果所述安全平台返回的验证结果为一致性验证失败，则向所述终端设备返回一致性验证失败的提示信息。

[0092] 根据本发明一优选实施方式，所述业务处理单元执行的业务服务包括：

[0093] 对所述终端设备的激活、云端数据存储服务或者下发多媒体数据。

[0094] 本发明还提供了一种业务认证的装置，该装置设置于安全平台，该装置包括：

[0095] 接收单元，用于接收认证信息；

[0096] 第一验证单元，用于验证所述认证信息是否来源于合法的终端设备；

[0097] 发送单元，用于返回验证结果，以便业务服务器根据验证结果确定是否向发送所述认证信息的终端设备提供业务服务。

[0098] 根据本发明一优选实施方式，该装置还包括：

[0099] 维护单元，用于存储合法终端设备的唯一设备标识；

[0100] 所述第一验证单元，具体用于判断所述认证信息包含的设备标识是否为所述安全平台存储的合法终端设备的唯一设备标识，如果是，则确定所述认证信息来源于合法的终端设备。

[0101] 根据本发明一优选实施方式，所述认证信息包括利用密钥信息对所述设备标识进行加密后得到的密文信息；

[0102] 该装置还包括：第一加解密单元，用于预先生成所述密钥信息并提供给合法的终端设备；利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密，得到所述设备标识。

[0103] 根据本发明一优选实施方式，所述认证信息包含明文信息和密文信息，所述明文信息包含所述设备标识，所述密文信息为利用密钥信息对包含所述设备标识的信息进行加密后得到的；

[0104] 该装置还包括：第一加解密单元，用于预先生成所述密钥信息并提供给合法的终端设备；利用本地保存的所述设备标识对应的密钥信息对所述认证信息中的密文信息进行解密；

[0105] 所述第一验证单元，还用于将所述第一加解密单元解密得到的信息与所述明文信息进行一致性验证，如果验证失败，则触发所述发送单元返回一致性验证失败的验证结果给所述业务服务器。

[0106] 根据本发明一优选实施方式，所述第一加解密单元提供给合法的终端设备的密钥信息为生成的公钥-私钥对中的公钥，解密时采用的为所述公钥对应的私钥；或者，

[0107] 所述第一加解密单元提供给合法终端设备的密钥信息为生成的公钥-私钥对中的私钥，解密时采用的为所述私钥对应的公钥。

[0108] 根据本发明一优选实施方式，该装置还包括：

[0109] 分配单元，用于分配合法终端设备的唯一设备标识。

[0110] 根据本发明一优选实施方式，所述接收单元，还用于接收针对合法终端设备的标识分配请求；

[0111] 所述分配单元针对所述合法终端设备分配唯一设备标识；

[0112] 所述发送单元，还用于发送所述设备标识，供标识写入设备将所述唯一设备标识写入所述合法终端设备。

[0113] 根据本发明一优选实施方式，所述分配单元，还用于依据预设的标识生成规则以及利用所述标识分配请求包含的合法终端设备的设备信息，生成唯一的设备标识。

[0114] 根据本发明一优选实施方式，所述标识生成规则包括：

[0115] 设备标识由设备标识符、厂商编号、待分配标识的设备信息和随机数依次组成。

[0116] 根据本发明一优选实施方式，所述合法终端设备的设备信息包括：

[0117] 待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。

[0118] 根据本发明一优选实施方式，该装置还包括第二验证单元；

[0119] 所述分配单元，还用于针对所述待分配标识的设备分配许可信息；

[0120] 所述发送单元，还用于发送所述许可信息；

[0121] 所述接收单元，还用于接收许可信息；

[0122] 所述第二验证单元，用于验证所述接收单元接收到的许可信息是否与所述分配单元分配的许可信息一致，如果是，则触发所述发送单元发送所述设备标识。

[0123] 根据本发明一优选实施方式，所述标识分配请求包含密钥信息；该装置还包括：

[0124] 第二加解密单元，用于利用所述密钥信息对所述分配的许可信息进行加密；

[0125] 所述发送单元发送加密后的许可信息。

[0126] 根据本发明一优选实施方式，所述维护单元，还用于保存针对所述合法终端设备生成的唯一设备标识和许可信息的对应关系；

[0127] 所述发送单元在发送所述唯一设备标识时，具体发送所述接收单元接收到的许可信息对应的唯一设备标识。

[0128] 根据本发明一优选实施方式，该装置还包括：

[0129] 第一加解密单元，用于生成密钥信息，并将生成的密钥信息的全部或部分提供给所述发送单元，由所述发送单元连同所述设备标识一起发送，供所述标识写入设备将所述密钥信息的全部或部分写入所述合法终端设备。

[0130] 本发明还提供了一种业务认证的装置，该装置设置于终端设备，该装置包括：

[0131] 认证服务单元，用于获取认证信息；

[0132] 业务服务单元，用于发送包含所述认证信息的业务请求。

[0133] 根据本发明一优选实施方式，所述认证服务单元，具体用于：获取被写入的唯一设备标识。

[0134] 根据本发明一优选实施方式，所述认证服务单元，还用于获取被写入的密钥信息，利用所述密钥信息对所述唯一设备标识进行加密，形成密文信息；

[0135] 所述业务服务单元，具体用于利用所述密文形成所述认证信息，或者利用包含所述唯一设备标识的明文信息以及所述密文信息形成所述认证信息。

[0136] 本发明还提供了一种业务认证的系统，该系统包括：终端设备、业务服务器和安全平台。

[0137] 由以上技术方案可以看出，本发明在向终端设备提供业务服务之前，通过终端设备在业务请求中携带的认证信息对终端设备是否合法的身份进行验证，并根据验证结果确定是否向终端设备提供业务服务。基于这种对终端设备的身份认证，能够有效地禁止对一些非法的终端设备提供业务服务。

【附图说明】

[0138] 图 1 为本发明实施例提供的系统架构图；

[0139] 图 2 为本发明实施例提供的主要方法流程图；

[0140] 图 3 为本发明实施例提供的标识生成系统的架构图；

[0141] 图 4 为本发明实施例提供的生成设备标识的主要方法流程图；

[0142] 图 5 为本发明实施例提供的一个详细的生成设备标识的方法流程图；

[0143] 图 6 为本发明实施例提供的终端设备的激活服务的认证方法流程图；

[0144] 图 7 为本发明实施例提供的云端数据存储服务的认证方法流程图；

[0145] 图 8 为本发明实施例提供的一种安全平台的服务器联盟架构图；

[0146] 图 9 为本发明实施例提供的一种装置结构图；

[0147] 图 10 为本发明实施例提供的另一种装置结构图；

[0148] 图 11 为本发明实施例提供的再一种装置结构图；

[0149] 图 12 为本发明实施例提供的一个实例图。

【具体实施方式】

[0150] 为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

[0151] 本发明提供的业务认证方法所基于的系统架构可以如图 1 中所示，主要包括：终端设备、业务服务器和安全平台。其中业务服务器和安全平台可以位于网络侧，业务服务器负责应终端设备的业务请求为终端设备提供业务服务，其主要功能可以如下：

[0152] 1) 接收终端设备发送的业务请求，其中该业务请求包含终端设备的认证信息。

[0153] 2) 将认证信息发送给安全平台，并获取安全平台返回的对该认证信息的验证结果。

[0154] 3) 依据验证结果，确定是否向终端设备提供业务服务。

[0155] 安全平台可以是位于网络侧的服务器或者服务器集群，其的主要功能如下：

[0156] 1) 接收到业务服务器发送来的认证信息后，验证该认证信息是否来源于合法的终端设备。在进行验证时，是基于本地存储的合法终端设备的唯一设备标识。

[0157] 2) 返回验证结果给业务服务器。

[0158] 3) 为合法终端设备生成唯一设备标识，并在本地存储合法终端设备的唯一设备标识。

[0159] 终端设备的主要功能包括：在请求业务服务时，获取认证信息，将包含认证信息的业务请求发送给业务服务器。

[0160] 本发明实施例所涉及的终端设备可以是诸如手机、电脑、智能家居设备、可穿戴设备、智能医疗器械等。其中电脑可以包括但不限于 PC、笔记本电脑、平板电脑等。智能家居设备可以包括但不限于智能电视、智能空调、智能加湿器、智能热水器、智能厨电设备、智能门窗、智能空气净化器等。可穿戴设备可以包括但不限于：智能手环、智能手表、智能眼镜等等。智能医疗器械可以包括但不限于：智能血压计、智能体重计、智能血糖仪、智能按摩椅等。

[0161] 图 2 为本发明实施例提供的主要方法流程图，如图 2 中所示，该方法可以包括以下

步骤：

[0162] 在201中，终端设备在请求业务服务时，获取认证信息。

[0163] 在本发明实施例中，终端设备的认证信息可以包括该终端设备被写入的唯一设备标识。

[0164] 更进一步地，为了保证安全性，终端设备还可以利用预设的密钥信息对唯一设备标识进行加密，将加密后得到的密文信息作为认证信息。该密钥信息可以是安全平台预先提供给合法的终端设备的。

[0165] 上述唯一设备标识的写入以及密钥信息的提供将在后续实施例中进行详细描述。

[0166] 在202中，终端设备将包含认证信息的业务请求发送给业务服务器。

[0167] 需要说明的是，对于诸如可穿戴设备等终端设备，除了自己将包含认证信息的业务请求发送给业务服务器之外，如果可穿戴设备无法接入网络，也可以通过近场通信的方式将认证信息发送给与之配对的手机或电脑等设备，由与之配对的手机或电脑等设备将包含认证信息的业务请求转发给业务服务器。

[0168] 在203中，业务服务器将认证信息发送给安全平台。

[0169] 在204中，安全平台验证该认证信息是否来源于合法的终端设备。具体地，在安全平台本地可以存储有合法终端设备的唯一设备标识，在本步骤中可以判断认证信息中携带的唯一设备标识是否与本地存储的一致，也就是说，判断本地是否存储有认证信息中携带的唯一设备标识，如果是，则确定该认证信息来源于合法的终端设备，否则，确定该认证信息来源于非法的终端设备，即验证了终端设备的身份合法性。

[0170] 如果认证信息中携带的是密文信息，则安全平台利用密钥信息对密文信息进行解密，得到终端设备的唯一设备标识，然后在对该唯一设备标识进行上述验证。

[0171] 其中，安全平台可以采用对称加密算法，这样上述的密钥信息可以是安全平台生成并预先提供给合法终端设备的一个密钥。安全平台也可以采用非对称加密算法，这种情况下，安全平台可以预先生成公钥-私钥对，然后将公钥-私钥对中的公钥提供给合法终端设备，在解密时，利用公钥-私钥对中的私钥对密文信息进行解密；或者安全平台可以将公钥-私钥对中的私钥提供给合法终端设备，在解密时，利用公钥-私钥对中的公钥对密文信息进行解密。

[0172] 在205中，安全平台将验证结果返回给业务服务器。

[0173] 在206中，业务服务器根据验证结果确定是否向终端设备提供业务服务。如果验证结果表明认证信息来源于合法的终端设备，即发送业务请求的终端设备为合法终端设备，则在207中向终端设备提供业务服务；否则可以拒绝向该终端设备提供业务服务。

[0174] 通过上述流程，业务服务器能够基于终端设备的身份是否合法，对业务服务的提供进行控制。

[0175] 作为一种优选的实施方式，上述终端设备的唯一设备标识可以是由安全平台生成，然后由标识写入设备写入终端设备中的。也就是说，将终端设备的唯一设备标识的生成和管理统一由网络端的安全平台实现，只有安全平台生成的唯一设备标识才是合法的，从而为本发明实施例中的认证方式提供依据。为了方便理解，在此先对唯一设备标识的生成过程进行详细描述。

[0176] 图3为本发明实施例提供的标识生成系统的架构图，如图3中所示，该系统可以包

括管理设备、标识分配设备和标识写入设备。其中管理设备可以设置于厂商处，称为厂商管理设备，也可以设置于其他设备出厂环节。在本发明实施例中所涉及的“厂商”可以包括设备的实际生产商、设备的技术提供商等等，其需求就是请求并获取设备标识，以将设备标识写入设备。标识分配设备可以设置于安全平台中，在本发明实施例中标识分配设备以安全平台为例进行描述、管理设备以厂商管理设备为例。

[0177] 其中厂商管理设备设置于厂商侧，负责设备生产过程中对设备相关的管理。标识写入设备可以设置于厂商侧，也可以独立设置，负责将设备标识写入终端设备。安全平台设置于网络侧，可以是服务器，也可以是服务器集群，负责针对设备生成唯一的设备标识。

[0178] 图4为本发明实施例提供的生成设备标识的主要方法流程图，如图4中所示，该方法可以包括以下步骤：

[0179] 在401中，厂商管理设备向安全平台发送标识分配请求。

[0180] 其中标识分配请求中可以包括待分配标识的设备信息，例如待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。还可以包括待分配标识的设备数量信息。

[0181] 需要说明的是，在本实施例中，待分配标识的设备即为图2所示实施例中合法的终端设备，只是在本实施例中该合法的终端设备尚未被分配设备标识。

[0182] 在402中，安全平台针对待分配标识的设备生成唯一的设备标识。

[0183] 在本步骤中，安全平台可以利用标识分配请求中携带的设备信息，为待分配标识的设备生成设备标识，一个设备标识能够唯一标识一个设备，已与其他设备相区别。

[0184] 另外，除了利用设备信息生成设备标识之外，安全平台还可以利用其它信息生成设备信息，例如采用生成随机数的方式来生成设备信息，只要保证生成的设备信息的唯一性即可。

[0185] 除了接收到标识分配请求后，实时生成设备标识的方式之外，也可以预先生成一些设备标识构成标识池，在接收到标识分配请求后，从标识池中分配一个设备标识给待分配标识的设备。

[0186] 在403中，安全平台将生成的设备标识发送给标识写入设备。

[0187] 需要说明的是，安全平台可以将生成的设备标识直接发送给标识写入设备，也可以经由厂商管理设备发送给标识写入设备。

[0188] 在404中，标识写入设备将设备标识写入待分配标识的设备。

[0189] 本步骤中，标识写入设备可以采用烧录等方式，将设备标识写入待分配标识的设备芯片中。写入设备的设备标识不能够更改，并且设备能够在需要时，获取自身的设备标识，以该设备标识表征自己的身份以及身份的合法性。

[0190] 为了提升生成设备标识流程中的安全性，可以更具体地采用如图5中所示流程。图5为本发明实施例提供的一个详细的生成设备标识的方法流程图，如图5中所示，该方法可以具体包括以下步骤：

[0191] 在501中，厂商管理设备生成公钥-私钥对。

[0192] 在502中，厂商管理设备将待分配标识的设备信息与公钥携带在标识分配请求中发送给安全平台。

[0193] 在503中，安全平台针对待分配标识的设备分别生成唯一的设备标识并生成许可

信息。

[0194] 标识分配请求中可以携带待分配标识的设备数量信息，如果是多于一个待分配标识的设备，例如 n 个，那么安全平台生成 n 个设备标识，可以针对各待分配标识的设备分别生成许可信息，也可以针对该 n 个待分配的设备生成一份许可信息，在安全平台维护设备标识与许可信息之间的对应关系。在本发明实施例中优选生成一份许可信息的方式。

[0195] 具体在生成标识信息时，可以按照预设的标识生成规则，生成对于各设备而言是唯一的，能够与其他设备相区别的信息。下面举一个标识生成规则的实例：

[0196] 生成的设备标识可以由 17 个字符构成，采用 8 个字节存储。格式可以采用：Y-AAAA-BBBB-XXXXXXXX

[0197] 其中，第一个字符“Y”可以采用固定字符，作为设备标识的标识符。

[0198] 四个字符“AAAA”可以采用十六进制字符，代表厂商编号。

[0199] 四个字符“BBBB”可以采用十六进制字符，代表待分配设备的芯片型号。当然，也可以采用诸如系统版本号等。

[0200] 最后八个字符“XXXXXXXX”可以采用十六进制字符，由一串随机数组成。

[0201] 上面仅仅是本发明实施例所列举的一个实例，也可以采用其他长度的字符，其中的部分内容也可以采用其他设备信息。

[0202] 许可信息可以依据日期、设备信息、厂商信息、随机数等中的一种或任意组合生成。除了在本步骤中实时生成许可信息之外，还可以预先维护一个许可信息池，在本步骤中从许可信息池中获取一个标识为可分配的许可信息，然后将该许可信息在许可信息池中标识为不可分配。在后续步骤 309 完成对该许可信息对应的设备信息的分配后，可以将该许可信息进行回收，即在许可信息池中将该许可信息重新标识为可分配。

[0203] 在 504 中，安全平台利用标识分配请求携带的公钥对许可信息进行加密后发送给厂商管理设备。

[0204] 在 505 中，厂商管理设备将加密的许可信息以及私钥提供给标识写入设备。

[0205] 在 506 中，标识写入设备利用私钥对加密的许可信息进行解密，得到解密后的许可信息。

[0206] 在 507 中，将解密后的许可信息发送给安全平台。

[0207] 需要说明的是，上述对许可信息进行的加解密过程是为了保证许可信息的安全性，但本发明并不限于这种方式，也可以发送和接收未进行加密处理的许可信息。

[0208] 在 508 中，安全平台判断接收到的许可信息是否与生成的许可信息一致，如果一致，则执行 509。如果不一致，则结束流程，或者向厂商管理设备或标识写入设备返回错误提示信息。

[0209] 在 509 中，安全平台将许可信息对应的设备标识发送给标识写入设备。

[0210] 在 510 中，标识写入设备将设备标识烧录至待分配标识的设备芯片。

[0211] 在步骤 509 中，安全平台还可以进一步生成密钥信息，将该密钥信息中的全部或部分连同设备标识一起发送给标识写入设备，由标识写入设备将接收到的设备标识和密钥信息都烧录至待分配标识的设备芯片。其中安全平台可以生成一个密钥，除了自身维护该密钥之外，将该密钥连同设备信息发送给标识写入设备。安全平台也可以生成公钥 - 私钥对，除了自身维护该公钥 - 私钥对之外，将公钥或者私钥连同设备信息发送给标识写入设

备以写入终端设备。

[0212] 为了保证安全，可以将标识信息连同密钥信息一起写入设备的安全存储。安全存储可以是利用诸如 ARM TrustZone 或 Secure Element 或 TI M-Shield 等机制在硬件上隔离出的安全区域，也可以是利用虚拟化机制隔离出一个独立的安全环境，安全存储保证了存入的密钥信息以及设备标识不可篡改和擦除。

[0213] 另外，需要说明的是，在图 5 所示的步骤 501 中，厂商管理设备实际上是生成并维护了密钥信息，公钥 - 私钥对是采用非对称加密算法时对应的密钥信息。本发明实施例中也可以采用对称算法，此时厂商管理设备在步骤 501 中可以生成一个密钥，在步骤 502 中将该密钥携带在标识分配请求中发送给安全平台。安全平台在步骤 504 中利用该密钥对许可信息进行加密后发送给厂商管理设备；然后在步骤 505 中厂商管理设备再将该密钥提供给标识写入终端设备，以便标识写入设备在步骤 506 中利用该密钥对许可信息进行解密。

[0214] 本发明实施例中提供的如图 2 所示的认证方式可以应用于多种业务场景，可以包括但不限于：终端设备的激活服务、云端数据存储服务、多媒体数据下发服务等。下面结合具体实施例对其中的终端设备的激活服务以及云端数据存储服务的认证流程进行描述。

[0215] 图 6 为本发明实施例提供的终端设备的激活服务的认证方法流程图，如图 6 中所示，该方法可以包括以下步骤：

[0216] 当终端设备首次开机时，通常需要对终端设备进行激活，只有激活了的终端设备才能够正常使用对应业务。例如对于智能手机而言，只有进行了操作系统的激活才能够正常使用智能手机。那么当移动设备首次开机时，在 601 中，获取移动设备被写入的唯一设备标识和公钥，并利用公钥对唯一设备标识进行加密形成密文信息。其中，该公钥是由安全平台生成的公钥 - 私钥对中的公钥。

[0217] 具体地，在形成密文信息时，可以对唯一设备标识和随机数进行加密，得到密文信息。

[0218] 在 602 中，将明文信息和密文信息作为激活请求的激活参数发送给激活业务服务器。其中明文信息为唯一设备标识。

[0219] 在 603 中，激活业务服务器接收到激活请求后，从激活请求中获取明文信息和密文信息，将该明文信息和密文信息发送给安全平台。

[0220] 在 604 中，安全平台利用私钥对密文信息进行解密，利用解密得到的信息与明文信息进行一致性验证，如果通过一致性验证，则进一步验证本地是否存储有接收到的唯一设备标识。

[0221] 在本步骤中，安全平台首先利用私钥对密文信息进行解密，然后在进行一致性验证时，可以将解密得到的唯一设备标识与明文信息的唯一设备标识进行比对，如果一致，则通过一致性验证；否则一致性验证不通过。如果一致性验证不通过，则可以直接返回一致性验证未通过的验证信息给激活业务服务器。

[0222] 如果通过一致性验证，则进一步判断安全平台本地是否存储有接收到的唯一设备标识，如果是，则确定该唯一设备标识来源于合法终端设备，即发送业务请求的终端设备的身份合法。

[0223] 需要说明的是，上述认证信息中也可以仅包括上述的密文信息，这种情况下无需进行一致性验证。

[0224] 在 605 中，将验证结果返回给激活业务服务器。

[0225] 在 606 中，激活业务服务器根据验证结果确定是否激活终端设备，如果验证结果表明发送业务请求的终端设备的身份合法，则在 607 中针对终端设备执行激活处理，并在 608 中向终端设备返回激活结果。

[0226] 如果验证结果表明一致性验证未通过，则激活业务服务器可以将该验证结果的提示信息返回给终端设备，终端设备可以再次发送激活请求。如果验证结果表明终端设备的身份非法，则激活业务服务器可以拒绝对该终端设备执行激活处理。

[0227] 图 7 为本发明实施例提供的云端数据存储服务的认证方法流程图，如图 7 中所示，该方法可以包括以下步骤：

[0228] 当终端设备使用到云端数据存储服务时，例如需要将移动设备本地的数据存储到云端，则在 701 中，触发移动设备获取被写入的唯一设备标识和公钥，并利用公钥对唯一设备标识进行加密形成密文信息。

[0229] 在 702 中，将明文信息和密文信息作为云端存储请求中的参数发送给云端存储服务器。

[0230] 在 703 中，云端存储服务器接收到云端存储请求后，从云端存储请求中获取明文信息和密文信息，将该明文信息和密文信息发送给安全平台。

[0231] 在 704 中，安全平台利用私钥对密文信息进行解密，利用解密得到的信息与明文信息进行一致性验证，如果通过一致性验证，则进一步验证本地是否存储有接收到的唯一设备标识。

[0232] 在本步骤中，安全平台首先利用私钥对密文信息进行解密，然后在进行一致性验证时，可以将解密得到的唯一设备标识与明文信息的唯一设备标识进行比对，如果一致，则通过一致性验证；否则一致性验证不通过。如果一致性验证不通过，则可以直接返回一致性验证未通过的验证信息给云端存储服务器。

[0233] 如果通过一致性验证，则进一步判断安全平台本地是否存储有接收到的唯一设备标识，如果是，则确定该唯一设备标识来源于合法终端设备，即发送业务请求的终端设备的身份合法。

[0234] 在 705 中，将验证结果返回给云端存储服务器。

[0235] 在 706 中，云端存储服务器根据验证结果确定是否允许终端设备存储数据至云端，如果验证结果表明发送云端存储请求的终端设备的身份合法，则在 707 中针对终端设备提供云端存储服务，即将终端设备上传的数据存储于云端，并在 708 中向终端设备返回处理结果。

[0236] 如果验证结果表明一致性验证未通过，则云端存储服务器可以将该验证结果的提示信息返回给终端设备，终端设备可以再次发送云端存储请求。如果验证结果表明终端设备的身份非法，则激活业务服务器可以拒绝对该终端设备提供云端存储服务。

[0237] 另外，对于安全平台而言，可以由一个服务器完成上述功能，也可以由一个服务器联盟来完成上述功能。下面对以服务器联盟的实现架构进行描述。

[0238] 图 8 为本发明实施例提供的一种安全平台的服务器联盟架构图，如图 8 中所示，该安全平台可以包括颁发中心、各级分发中心以及各级认证中心，图 8 中以两级分发中心和两级认证中心为例。

[0239] 其中对于生成设备标识的部分而言，颁发中心负责下发标识生成规则给各级分发中心，由各级分发中心负责接收来自厂商的标识分配请求，然后生成设备标识并发送给设备写入设备。另外，各级分发中心可以将生成的设备标识上报至颁发中心进行统一备份。这种实现方式下，颁发中心实际上将设备标识的生成权限给各级分发中心，颁发中心仅负责制定和下发标识生成规则以及对设备标识进行统一备份。

[0240] 其中，颁发中心在下发设备生成规则给各级分发中心时，可以将设备标识的长度、各部分所对应的内容等下发给各级分发中心。仍以上面实施例中所举的格式“Y-AAAA-BBBB-XXXXXXXX”为例，在将该格式下发给各级分发中心之外，还可以对各级分发中心所采用的随机数“XXXXXXXX”的号段（即范围）进行下发，各级分发中心可以在对应的号段内产生随机数并用以生成设备标识。

[0241] 这种分布式地实现方式将对一台服务器的性能压力分担到多台服务器上，也同时能够对表征设备身份的设备标识进行备份，提高安全性。

[0242] 还存在另外一种实现方式，各级分发中心负责接收来自厂商管理设备的标识分配请求，将该标识分配请求转发给颁发中心，由颁发中心按照标识生成规则生成设备标识，再经由各级分发中心转发给标识写入设备。

[0243] 对于认证部分而言，各级认证中心接收到包含唯一设备标识的认证信息后，可以先判断本地是否存储有该唯一设备标识，如果是，则可以直接向业务服务器返回该认证信息所来源的终端设备为合法终端设备的验证结果；否则可以向上一级认证中心转发认证信息。接收到认证信息的各级认证中心均执行相类似的处理。

[0244] 若认证信息转发至颁发中心，则颁发中心判断本地是否存储有该唯一设备标识，如果是，则经由各级认证设备向业务服务器返回该认证信息所来源的终端设备为合法终端设备的验证结果；否则经由各级认证设备向业务服务器返回该认证信息所来源的终端设备为非法终端设备的验证结果。

[0245] 其中，颁发中心可以预先将本地存储的唯一设备标识分发至各级认证设备进行存储。或者，各级认证设备在接收到的验证结果为认证信息来源于合法的终端设备时，则在本地存储认证信息中的唯一设备标识，这样下次再接收到该唯一设备标识就可以直接进行验证。

[0246] 以上是对本发明提供的方法进行的详细描述，下面结合实施例对本发明提供的装置进行详细描述。

[0247] 图 9 为本发明实施例提供的一种装置结构图，该装置可以设置于业务服务器中，用于完成业务服务器的上述功能。如图 9 中所示，该装置可以包括：终端侧交互单元 01、网络侧交互单元 02 和业务处理单元 03，各组成单元的主要功能如下：

[0248] 终端侧交互单元 01 负责接收终端设备发送的包含认证信息的业务请求。

[0249] 网络侧交互单元 02 负责将认证信息发送给安全平台，由安全平台验证认证信息是否来源于合法的终端设备；接收安全平台返回的验证结果。

[0250] 其中，上述的认证信息可以包含终端设备的唯一设备标识；或者，认证信息可以包含利用密钥信息对包含终端设备的唯一设备标识的信息进行加密后的密文信息；或者，认证信息可以包含明文信息或密文信息，明文信息包含终端设备的唯一设备标识，密文信息为利用密钥信息对包含终端设备的唯一设备标识的信息进行加密后的密文信息。其中密钥

信息是安全平台预先提供给合法的终端设备的，该密钥信息可以为安全平台针对合法的终端设备的唯一设备标识生成的公钥－私钥对中的公钥或私钥。优选地，该密钥信息可以由安全平台发送给标识写入设备，由标识写入设备写入合法的终端设备。

[0251] 业务处理单元03负责依据安全平台返回的验证结果，确定是否向终端设备提供业务服务。

[0252] 具体地，如果安全平台返回的验证结果为认证信息来源于合法的终端设备，则业务处理单元03可以向终端设备提供业务服务。如果安全平台返回的验证结果为认证信息来源于非法的终端设备，则业务处理单元03可以禁止向终端设备提供业务服务。如果安全平台返回的验证结果为一致性验证失败，则业务处理单元03可以向终端设备返回一致性验证失败的提示信息。

[0253] 上述业务服务器可以是执行各种业务的服务器，具体地，业务处理单元03执行的业务服务可以包括但不限于：对终端设备的激活、云端数据存储服务或者下发多媒体数据。

[0254] 图10为本发明实施例提供的另一种装置结构图，该装置可以设置于安全平台，如图10中所示，该装置可以包括：接收单元11、第一验证单元12和发送单元13，还可以包括维护单元14、第一加解密单元15、分配单元16、第二加解密单元17和第二验证单元18。各组成单元的主要功能如下：

[0255] 接收单元11负责接收认证信息，该认证信息可以是业务服务器发送的。第一验证单元12负责验证认证信息是否来源于合法的终端设备。发送单元13负责返回验证结果，可以返回给业务服务器，以便业务服务器根据验证结果确定是否向发送认证信息的终端设备提供业务服务。

[0256] 其中，上述认证信息中可以包含上述终端设备的设备标识。维护单元存储有合法终端设备的唯一设备标识，由第一验证单元12判断认证信息包含的设备标识是否为安全平台存储的合法终端设备的唯一设备标识，如果是，则确定认证信息来源于合法的终端设备。

[0257] 为了保证信息的安全性，上述认证信息可以包括利用密钥信息对设备标识进行加密后得到的密文信息。该密钥信息可以是第一加解密单元15预先生成并提供给合法的终端设备的。另外，第一加解密单元15还可以利用本地保存的设备标识对应的密钥信息对认证信息中的密文信息进行解密，得到设备标识，然后交由第一验证单元12进行验证。

[0258] 还存在另外一种实现方式，即认证信息可以包含明文信息和密文信息，其中，明文信息包含设备标识，密文信息为利用密钥信息对包含设备标识的信息进行加密后得到的。该密钥信息可以是第一加解密单元15预先生成并提供给合法的终端设备的。

[0259] 另外，第一加解密单元15可以利用本地保存的设备标识对应的密钥信息对认证信息中的密文信息进行解密。然后第一验证单元12将第一加解密单元15解密得到的信息与明文信息进行一致性验证，如果验证失败，则触发发送单元13返回一致性验证失败的验证结果给业务服务器。

[0260] 其中，第一加解密单元15提供给合法的终端设备的密钥信息为生成的公钥－私钥对中的公钥，解密时采用的为公钥对应的私钥；或者，第一加解密单元15提供给合法终端设备的密钥信息为生成的公钥－私钥对中的私钥，解密时采用的为私钥对应的公钥。

[0261] 对于安全平台而言，所存储的合法终端设备的唯一标识设备可以是安全平台针对

各合法终端设备分配的。即分配单元 16 负责分配合法终端设备的唯一设备标识。

[0262] 具体地，接收单元 11 可以接收厂商管理设备发送的针对合法终端设备的标识分配请求，然后由分配单元 16 针对合法终端设备分配唯一设备标识，再由发送单元 13 将唯一设备标识发送给标识写入设备，供标识写入设备将唯一设备标识写入合法终端设备。

[0263] 其中分配单元 16 可以依据预设的标识生成规则以及利用标识分配请求包含的合法终端设备的设备信息，生成唯一的设备标识。

[0264] 作为一种实施方式，标识生成规则可以包括：设备标识由设备标识符、厂商编号、待分配标识的设备信息和随机数依次组成。其中合法终端设备的设备信息可以包括但不限于：待分配标识的设备的型号信息、系统版本信息以及芯片信息中的至少一种。

[0265] 分配单元 16 还可以针对合法终端设备生成许可信息，由发送单元 13 将许可信息发送给厂商管理设备，由厂商管理设备将许可信息提供给标识写入设备。接收单元 11 接收标识写入设备发送的许可信息后，由第二验证单元 18 验证接收单元 11 接收到的许可信息与分配单元 16 生成的许可信息是否一致，如果是，则触发发送单元 13 将唯一设备标识发送给标识接入设备。

[0266] 为了保证生成设备标识过程的安全性，上述的标识分配请求中可以包含密钥信息，此时第二加解密单元 17 可以利用标识分配请求中携带的密钥信息对许可信息进行加密，由发送单元 13 将第二加解密单元 17 加密后的许可信息返回给厂商管理设备，由厂商管理设备将加密后的许可信息以及密钥信息提供给标识写入设备。接收单元 11 接收标识写入设备发送的许可信息，该许可信息由标识写入设备对加密后的许可信息进行解密得到。

[0267] 维护单元 14 可以保存针对合法终端设备生成的唯一设备标识和许可信息的对应关系。发送单元 13 在发送唯一设备标识时，可以将接收单元 11 接收到的许可信息对应的唯一设备标识发送给标识写入设备。

[0268] 另外，上述的第一加解密单元 15 可以在生成唯一设备标识的过程中，生成密钥信息，并将生成的密钥信息的全部或部分提供给发送单元 13，由发送单元 13 连同设备标识一起发送给标识写入设备，供标识写入设备将密钥信息的全部或部分写入合法终端设备。

[0269] 图 11 为本发明实施例提供的再一种装置结构图，该装置可以设置于终端设备，如图 11 中所示，该装置可以包括：认证服务单元 21 和业务服务单元 22。

[0270] 其中，认证服务单元 21 负责获取认证信息。通常，认证服务单元 21 可以由业务服务单元 22 触发执行获取认证信息的操作，即当有业务请求要发送时，业务服务单元 22 可以触发认证服务单元 21 获取认证信息。

[0271] 业务服务单元 22 负责将包含认证信息的业务请求发送给业务服务器。

[0272] 其中，认证服务单元 21 可以获取被写入的唯一设备标识，即认证信息中可以包括唯一设备标识。

[0273] 更进一步地，认证服务单元 21 还可以获取被写入的密钥信息，利用密钥信息对唯一设备标识进行加密，形成密文信息。业务服务单元 22 可以利用密文形成认证信息，或者利用包含唯一设备标识的明文信息以及密文信息形成认证信息。

[0274] 下面列举一个应用的实例，如图 12 中所示，假设厂商 A 生产出某智能电视 a，其厂商管理设备生成一个公钥 - 私钥对 (K1-k1)，将智能电视 a 的芯片型号以及公钥 K1 携带在标识分配请求中发送给安全平台。

[0275] 安全平台利用智能电视a的芯片型号生成一个唯一设备标识IDa并生成一个许可信息，将许可信息采用K1进行加密后发送给厂商管理设备后，由厂商管理设备将加密后的许可信息以及私钥k1发送给设置在厂商A处的标识写入设备。标识写入设备利用k1对许可信息进行解密后，将解密后的许可信息发送给安全平台。

[0276] 安全平台接收到上述许可信息后，生成公钥-私钥对(K2-k2)，将公钥K2和IDa发送给标识写入设备，由标识写入设备将IDa和K2一起写入智能电视a中。

[0277] 后续，如果智能电视a发起业务请求，例如请求播放视频流，那么在发送的业务请求中包含明文信息和密文信息，其中明文信息可以包含IDa，密文信息可以是对IDa、随机数等进行加密后得到的信息。

[0278] 当视频服务器接收到智能电视a的业务请求后，将其中的认证信息，即上述的明文信息和密文信息发送给安全平台。

[0279] 安全平台利用k2对该密文信息进行解密后，进行一致性验证。如果一致性验证通过，则判断本地是否存储有IDa，判断结果为是，那么将认证信息来源于合法终端设备的验证结果发送给视频服务器。视频服务器向智能电视a提供视频流。

[0280] 但是，如果另一个仿冒的智能电视b也向视频服务器发送业务请求，视频服务器将其中携带的认证信息发送给安全平台。对于仿冒的智能电视b而言，认证信息中可能会携带其自身的设备标识IDb，但其并不知道安全平台提供的公钥K2，因此可能没有密文信息，也可能密文信息采用的密钥信息并非K2。那么安全平台接收到该认证信息后，没有密文信息会导致验证失败；密文信息采用的密钥信息并非K2，也会导致验证失败；设备标识IDb并非安全平台生成的IDb也会导致验证失败。那么安全平台会向视频服务器返回认证信息来源于非法终端设备的验证结果，那么视频服务器就禁止向该智能电视b发送视频流。那么仿冒的智能电视b就无法进行正常的业务使用。

[0281] 在本发明所提供的几个实施例中，应该理解到，所揭露的系统，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0282] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0283] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0284] 上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)或处理器(processor)执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read-Only Memory，ROM)、随机存取存储器(Random Access Memory，RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0285] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精

神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

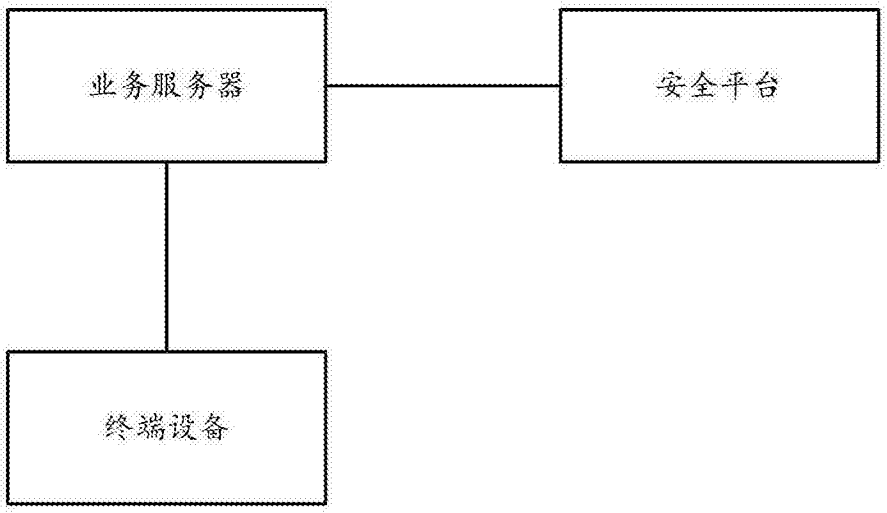

业务服务器
安全平台
终端设备

图 1

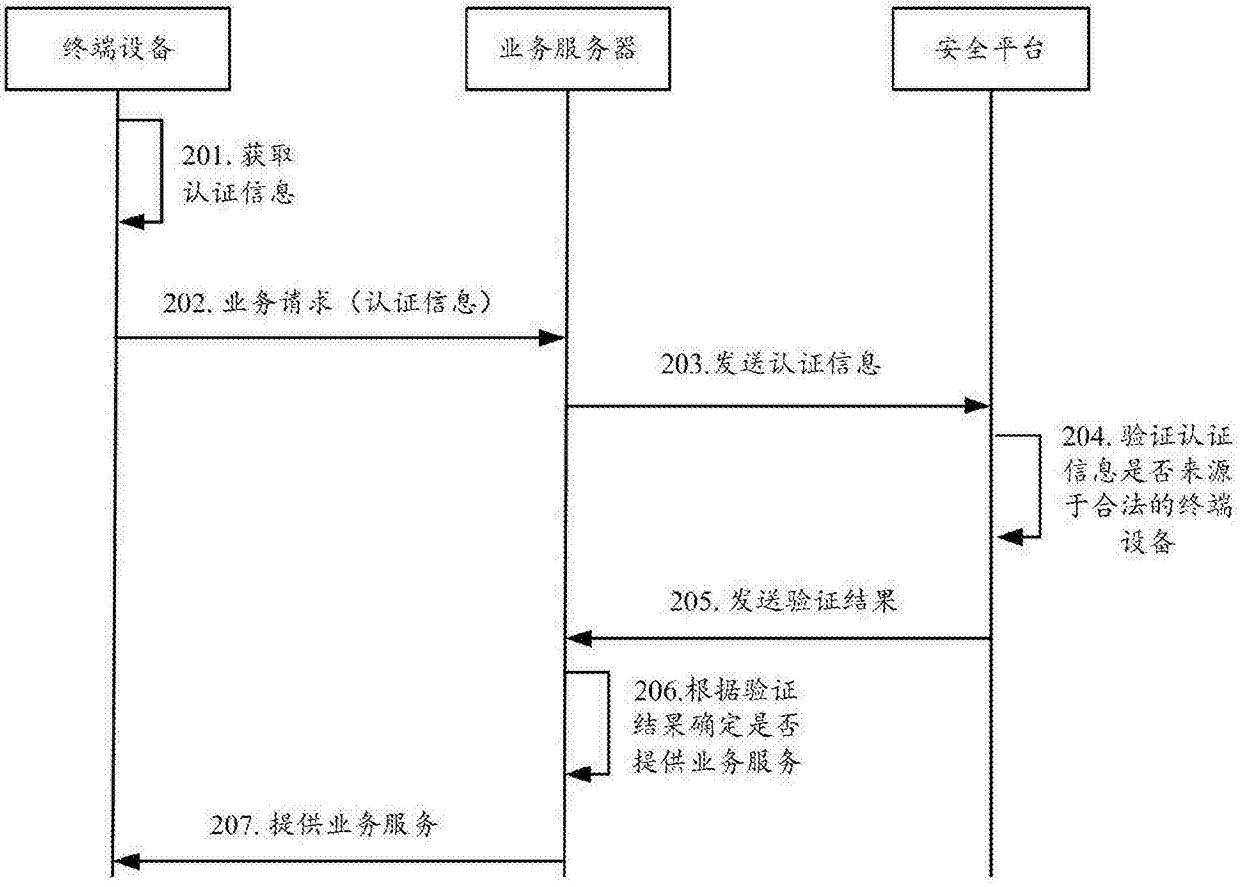

终端设备
业务服务器
安全平台
201. 获取认证信息
202. 业务请求（认证信息）
203. 发送认证信息
204. 验证认证信息是否来源于合法的终端设备
205. 发送验证结果
206. 根据验证结果确定是否提供业务服务
207. 提供业务服务

图 2

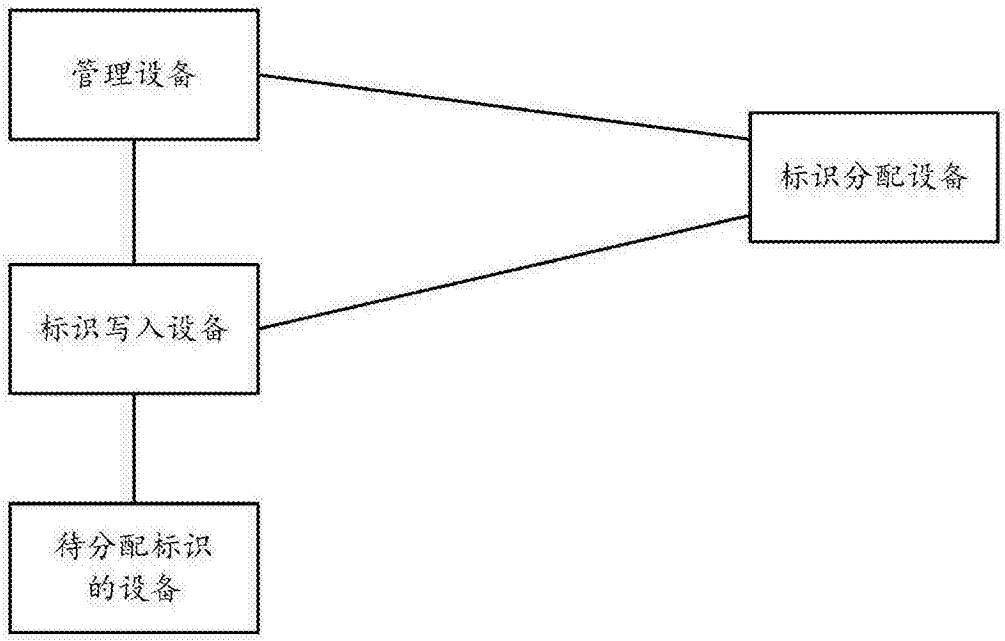

管理设备
标识分配设备
标识写入设备
待分配标识
的设备

图 3

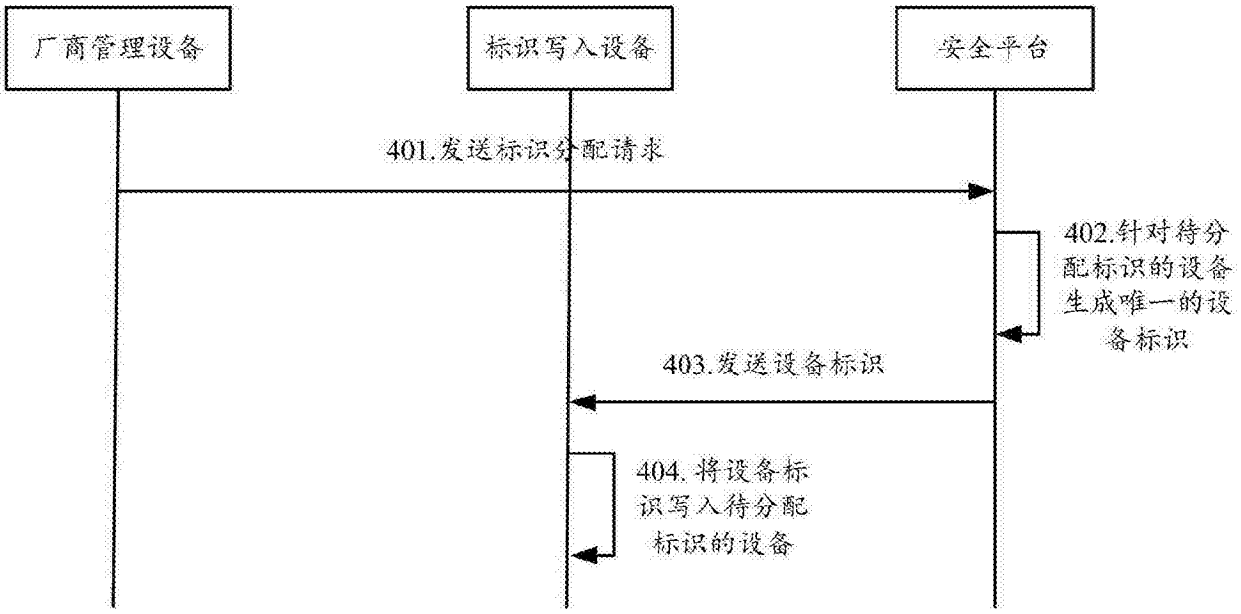

厂商管理设备
标识写入设备
安全平台
401.发送标识分配请求
402.针对待分配标识的设备生成唯一的设备标识
403.发送设备标识
404.将设备标识写入待分配标识的设备

图 4

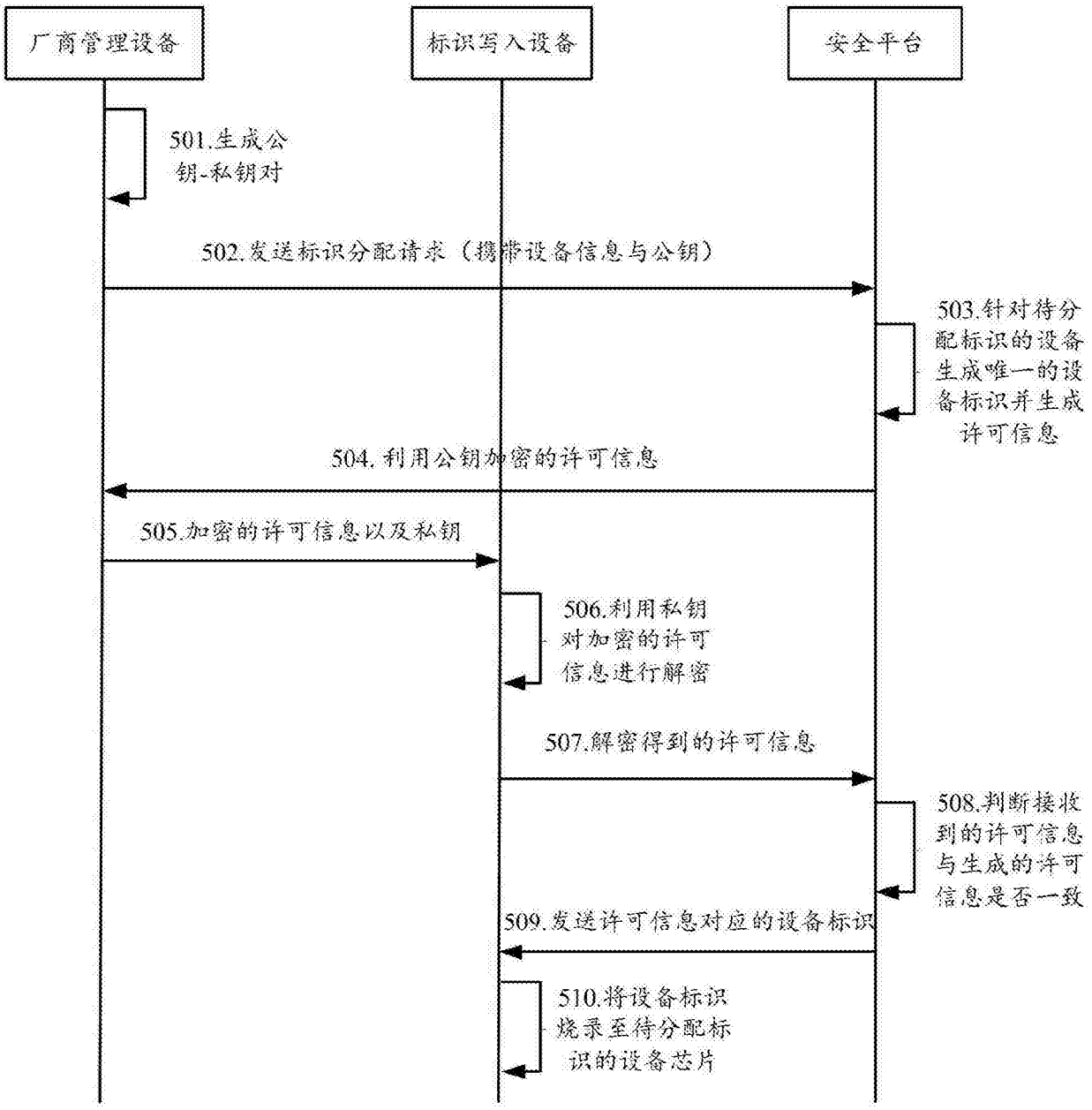

厂商管理设备
标识写入设备
安全平台
501.生成公钥-私钥对
502.发送标识分配请求（携带设备信息与公钥）
503.针对待分配标识的设备生成唯一的设备标识并生成许可信息
504.利用公钥加密的许可信息
505.加密的许可信息以及私钥
506.利用私钥对加密的许可信息进行解密
507.解密得到的许可信息
508.判断接收到的许可信息与生成的许可信息是否一致
509.发送许可信息对应的设备标识
510.将设备标识烧录至待分配标识的设备芯片

图 5

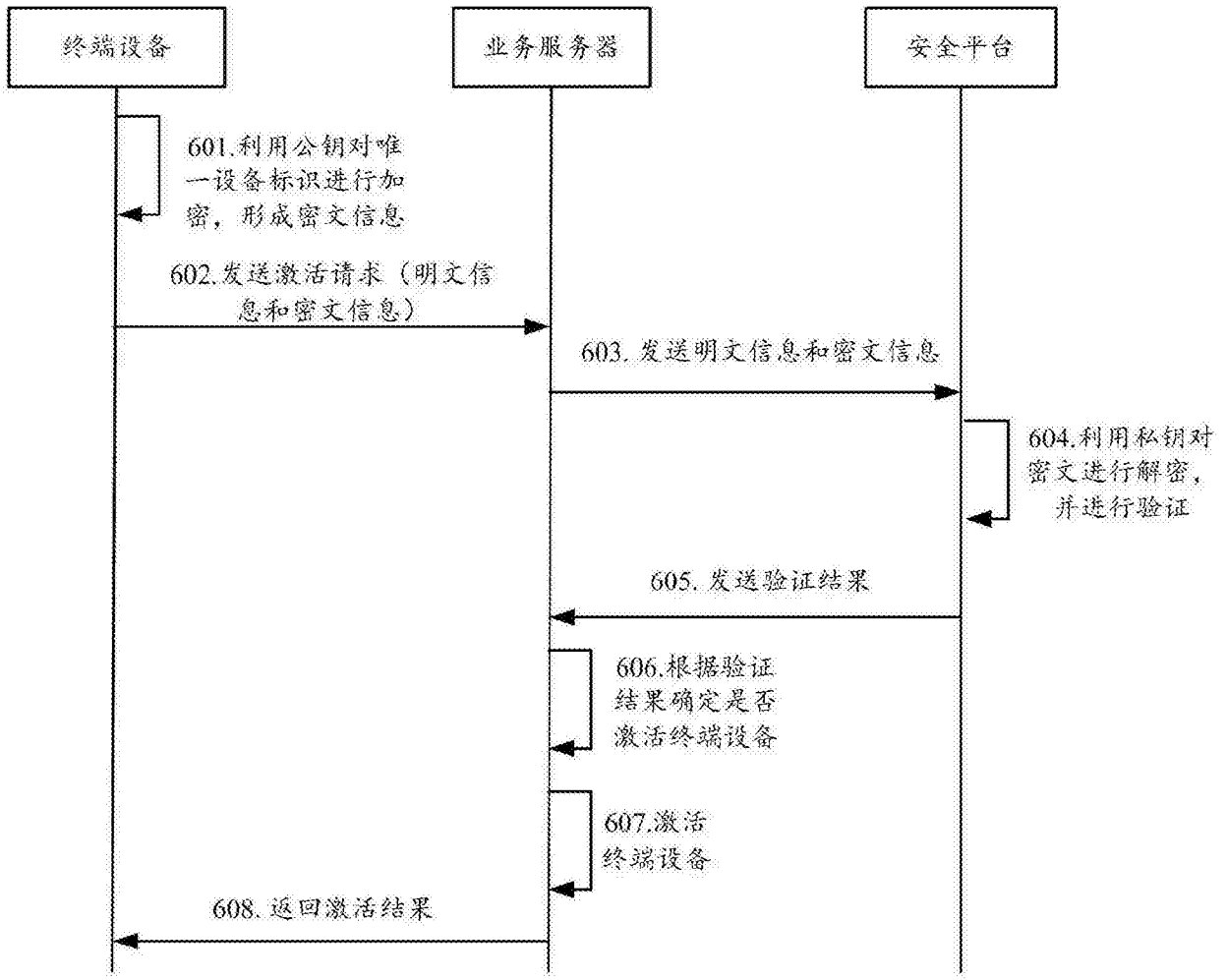

终端设备
业务服务器
安全平台
601.利用公钥对唯一设备标识进行加密，形成密文信息
602.发送激活请求（明文信息和密文信息）
603. 发送明文信息和密文信息
604.利用私钥对密文进行解密，并进行验证
605. 发送验证结果
606.根据验证结果确定是否激活终端设备
607.激活终端设备
608. 返回激活结果

图 6

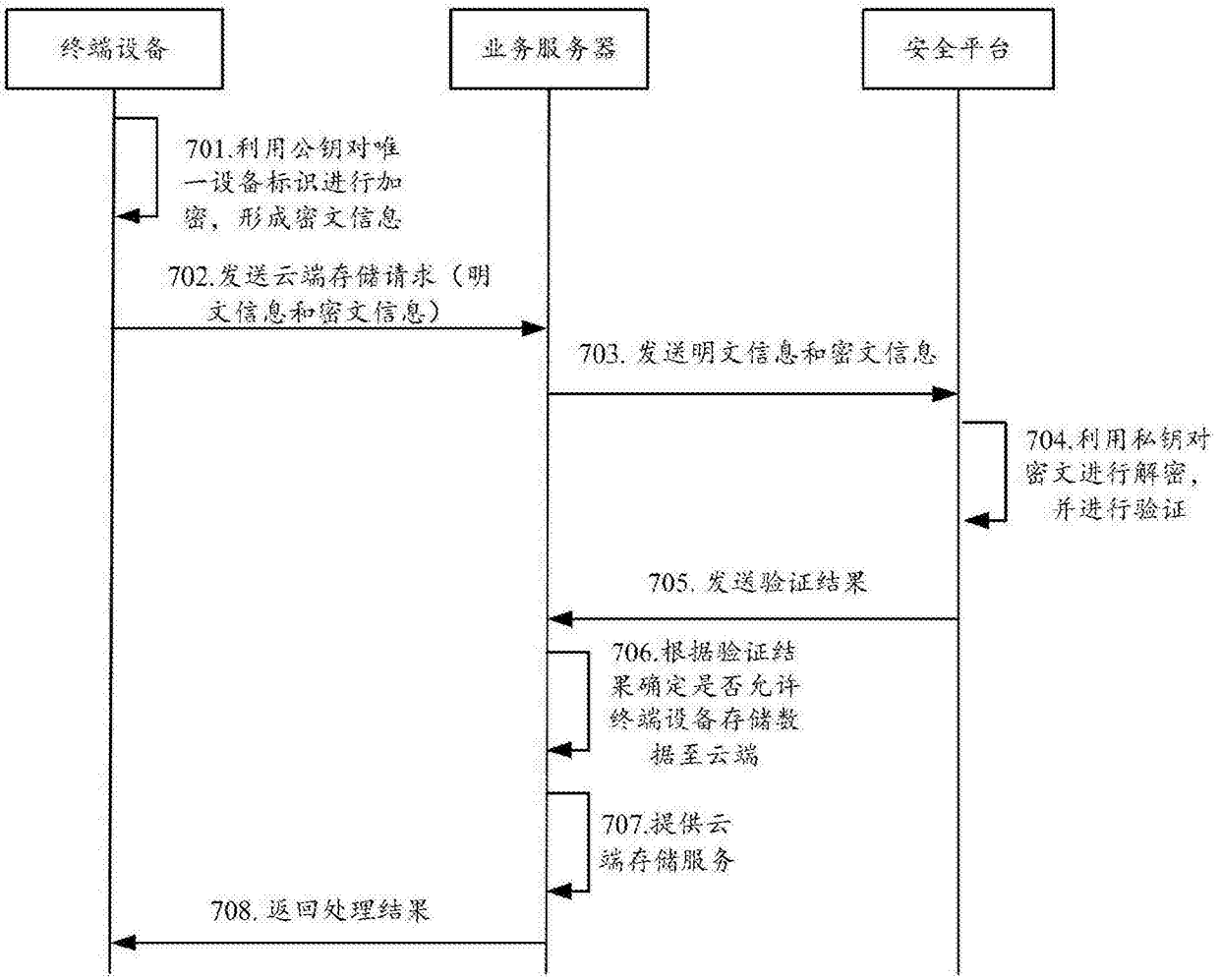

终端设备
业务服务器
安全平台
701.利用公钥对唯一设备标识进行加密，形成密文信息
702.发送云端存储请求（明文信息和密文信息）
703. 发送明文信息和密文信息
704.利用私钥对密文进行解密，并进行验证
705. 发送验证结果
706.根据验证结果确定是否允许终端设备存储数据至云端
707.提供云端存储服务
708. 返回处理结果

图 7

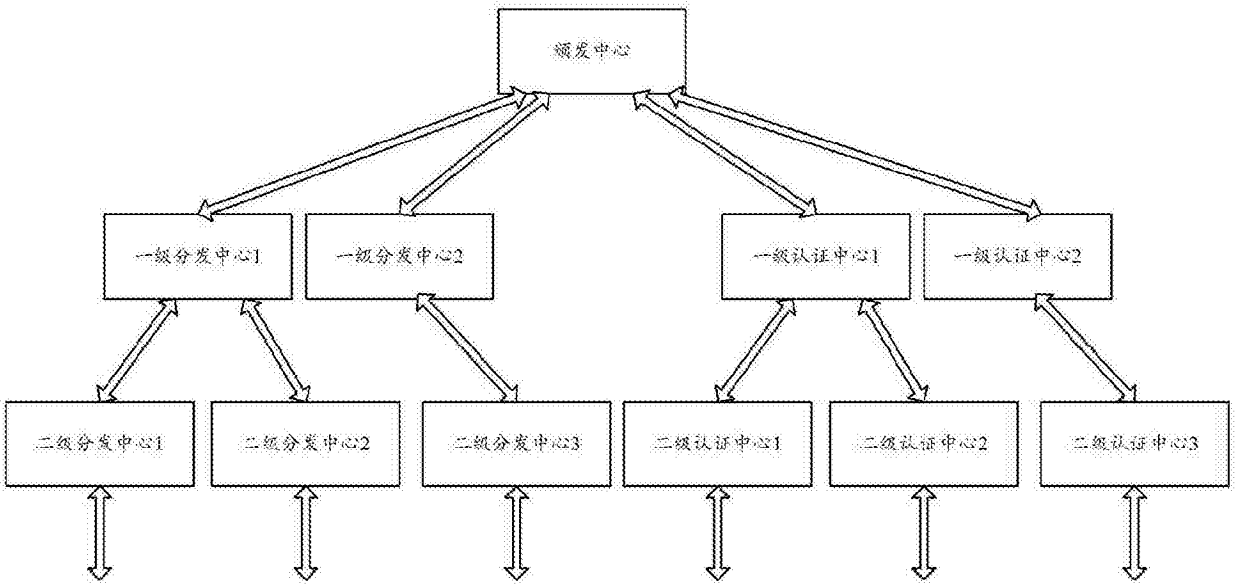

颁发中心
一级分发中心1
一级分发中心2
一级认证中心1
一级认证中心2
二级分发中心1
二级分发中心2
二级分发中心3
二级认证中心1
二级认证中心2
二级认证中心3

图 8

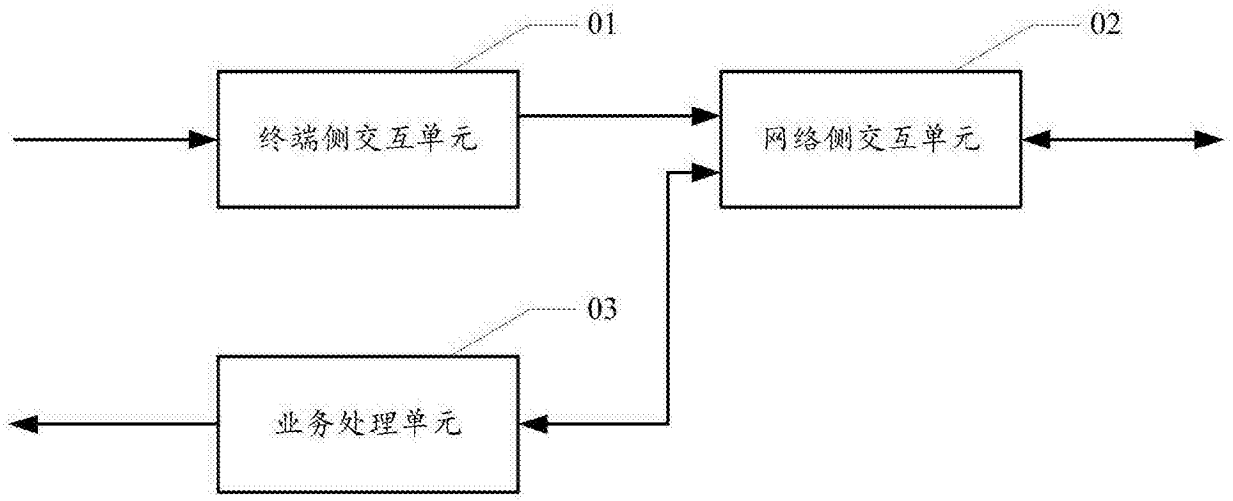

01
02
终端侧交互单元
网络侧交互单元
03
业务处理单元

图 9

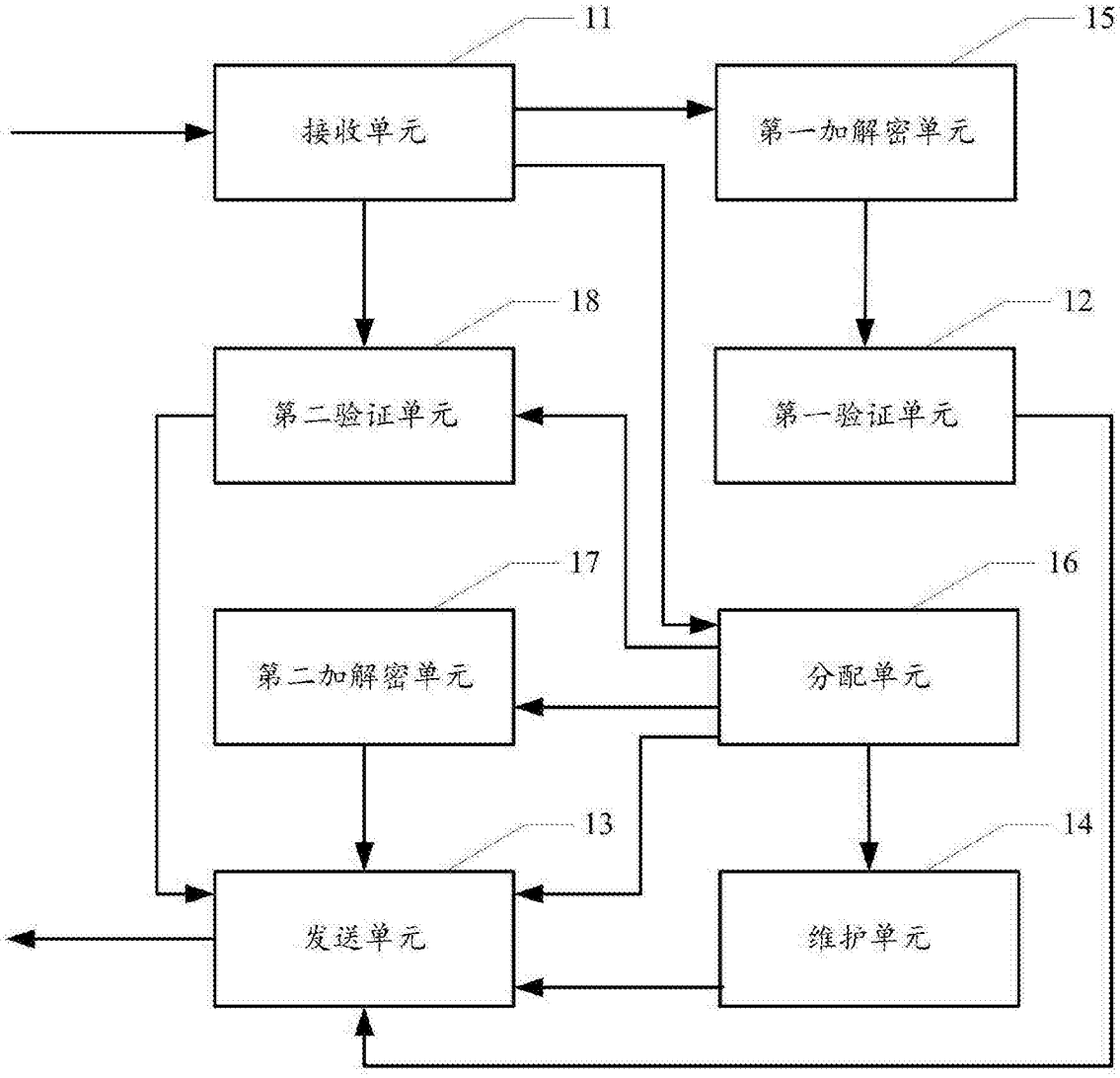

11
15
接收单元
第一加解密单元
18
12
第二验证单元
第一验证单元
17
16
第二加解密单元
分配单元
13
14
发送单元
维护单元

图 10

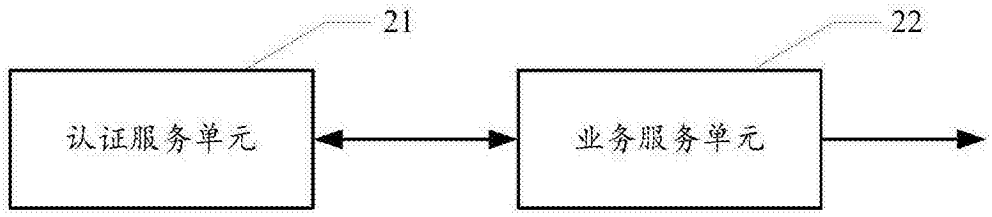



图 11

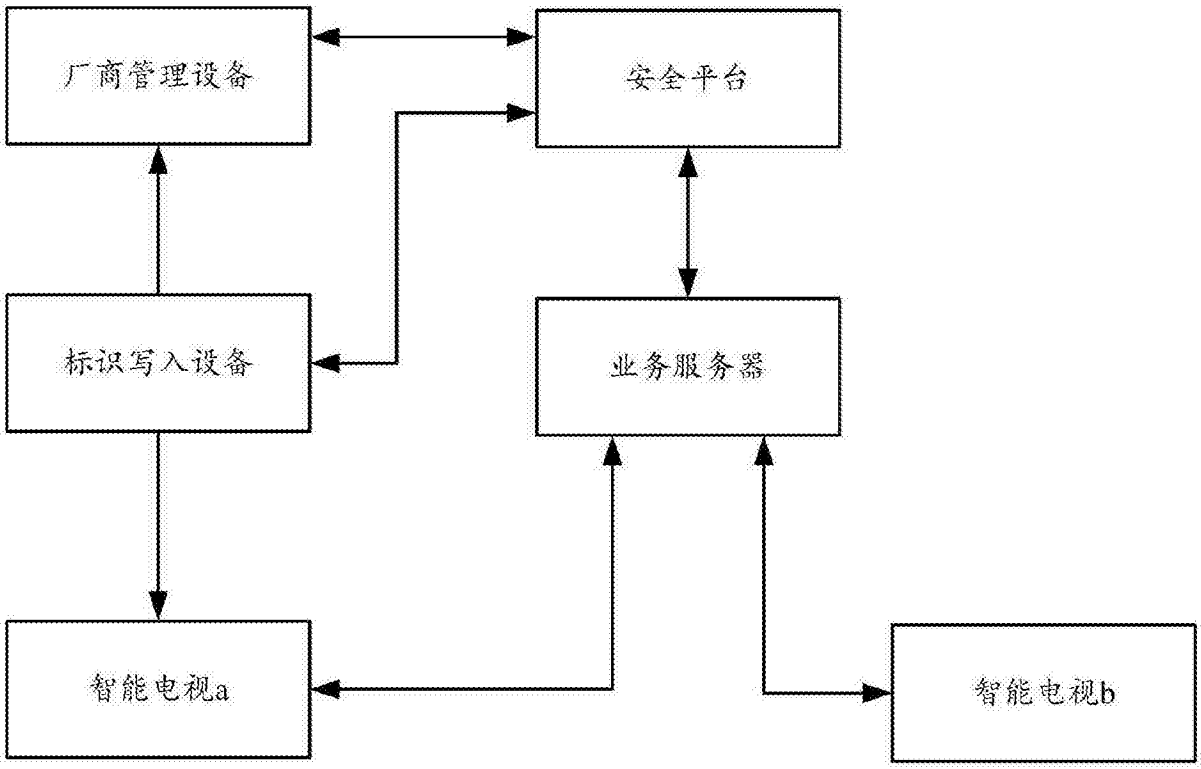



图 12