(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103067174 B
(45)授权公告日 2015.06.17

(21)申请号 201210578627.6

(22)申请日 2012.12.27

(73)专利权人 飞天诚信科技股份有限公司
地址 100085 北京市海淀区学清路9号汇智大厦B座17层

(72)发明人 陆舟 于华章

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

(56)对比文件
CN 101576843 A,2009.11.11,
CN 102662692 A,2012.09.12,
CN 102752104 A,2012.10.24,

审查员 李韧

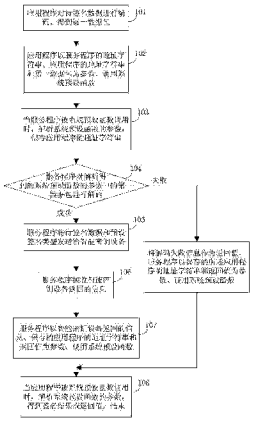
权利要求书6页 说明书16页 附图5页

(54)发明名称

一种在移动操作系统中完成数字签名的方法和系统

(57)摘要

本发明公开一种在移动操作系统中完成数字签名的方法和系统，该方法包括：应用程序对待签名数据进行编码得到第一数据包；以服务程序的地址字符串、应用程序的地址字符串和第一数据包为参数调用系统预设函数；当服务程序被系统预设函数调用时，解析函数参数，保存应用程序的地址字符串；对第一数据包进行解码，成功则将待签名数据和预设签名类型发送到智能密钥设备，否则将解码失败信息作为返回值，以应用程序的地址字符串和返回值为参数，调用系统预设函数；接收智能密钥设备返回的信息；以智能密钥设备返回的信息、应用程序的地址字符串和返回值为参数调用系统预设函数；应用程序解析系统预设函数参数，得到签名结果或返回值，结束。



CN 103067174 B

1. 一种在移动操作系统中完成数字签名的方法，其特征在于，所述方法包括：

当应用程序被调用时，执行以下步骤：

步骤 S1：所述应用程序对待签名数据进行编码，得到第一数据包；

步骤 S2：所述应用程序以服务程序的地址字符串、所述应用程序的地址字符串和所述第一数据包为参数，调用系统预设函数；

步骤 S3：当服务程序被所述系统预设函数调用时，解析所述系统预设函数的参数，保存所述应用程序的地址字符串；

步骤 S4：所述服务程序对解析得到的所述系统预设函数的参数中的所述第一数据包进行解码，如解码成功则得到所述待签名数据，执行步骤 S5，否则将解码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

步骤 S5：所述服务程序将所述待签名数据和预设签名类型发送给智能密钥设备；

步骤 S6：所述服务程序接收所述智能密钥设备返回的信息；

步骤 S7：所述服务程序以所述智能密钥设备返回的信息、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数，所述返回值为错误码或者表示签名成功的数值；

步骤 S8：当所述应用程序被所述系统预设函数调用时，所述应用程序解析所述系统预设函数的参数，得到签名结果或所述返回值，结束。

2. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S6 至步骤 S8 替换为：

步骤 S6'：所述服务程序接收所述智能密钥设备返回的信息，判断所述智能密钥设备返回的信息是否为签名结果，是则执行步骤 S7'，否则将签名错误信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8'；

步骤 S7'：所述服务程序以所述签名结果、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数，所述返回值为错误码或者表示签名成功的数值；

步骤 S8'：当所述应用程序被所述系统预设函数调用时，所述应用程序解析所述系统预设函数的参数，解析得到的返回值是否为表示正确信息的返回值，是则得到所述签名结果，结束，否则得到错误信息，结束。

3. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S1 包括：

步骤 S1-1：所述应用程序等待接收用户输入的信息及第一用户按键信息，并判断是否接收到所述用户输入的信息及第一用户按键信息，是则执行步骤 S1-3，否则执行步骤 S1-2；所述用户输入的信息包括第一账户、第二账户、传输信息、证书用户名和所述智能密钥设备的序列号；

步骤 S1-2：所述应用程序通过显示屏将提示信息输出，返回步骤 S1-1；

步骤 S1-3：所述应用程序对所述用户输入的信息中的所述证书用户名进行加密；

步骤 S1-4：所述应用程序根据所述第一用户按键信息判断用户按键类型，若所述用户按键类型为原文签名则执行步骤 S1-5，否则执行步骤 S1-7；

步骤 S1-5：所述应用程序将标志位置位，对第一信息、第二信息和第三信息进行组合，得到所述待签名数据，对所述待签名数据进行加密；所述第一信息为所述用户输入的信息

的一部分，所述第二信息由所述用户输入的信息的剩余部分与所述应用程序中的预设信息组合得到，所述第三信息为所述应用程序中的预设信息；

步骤 S1-6：所述应用程序对所述待签名数据的加密结果进行编码，根据编码结果生成所述第一数据包，执行步骤 S2；

步骤 S1-7：所述应用程序将标志位复位，对所述第一信息、第二信息和第三信息分别进行加密；

步骤 S1-8：所述应用程序分别对所述第一信息、第二信息和第三信息的加密结果进行编码，根据编码结果生成所述第一数据包，执行步骤 S2。

4. 根据权利要求 3 所述的方法，其特征在于，所述生成第一数据包具体为：根据所述编码结果和所述标志位生成第一数据包，所述编码结果中包括所述智能密钥设备的序列号和加密后的证书用户名。

5. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S2 替换为：

步骤 S2'：所述应用程序以服务程序的地址字符串、所述应用程序的地址字符串、预设的第一认证参数和所述第一数据包为参数，调用所述系统预设函数。

6. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S2 之后还包括：

步骤 S2-1：所述应用程序获取所述系统预设函数的返回值，判断所述返回值类型，若为是则启动所述服务程序，否则结束。

7. 根据权利要求 5 所述的方法，其特征在于，所述步骤 S3 包括：

步骤 S3-0：当所述服务程序被所述系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第一认证参数并判断是否认证成功，是则保存解析得到的所述应用程序的地址字符串，否则结束。

8. 根据权利要求 3 所述的方法，其特征在于，所述步骤 S3 具体为：

步骤 S3-1：当所述服务程序接收到用户输入的第二用户按键信息时，根据所述第二用户按键信息判断用户按键类型，若是确定键则执行步骤 S3-2，否则将用户取消信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

步骤 S3-2：所述服务程序通过显示屏将模态框输出；

步骤 S3-3：所述服务程序解析所述系统预设函数的参数，并保存所述应用程序的地址字符串；

步骤 S3-4：所述服务程序获取所述智能密钥设备的序列号，判断获取的所述智能密钥设备的序列号与解析得到的所述智能密钥设备的序列号是否相同，是则执行步骤 S4，否则将验证所述智能密钥设备序列号的失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

9. 根据权利要求 8 所述的方法，其特征在于，所述步骤 S4 包括：

步骤 S4-1：所述服务程序判断所述标志位是否置位，是则执行步骤 S4-2，否则执行步骤 S4-3；

步骤 S4-2：所述服务程序对所述第一数据包进行解码，对解码结果进行解密，如解密成功则得到所述用户输入的证书用户名和所述待签名数据，执行步骤 S4-4，否则将解码解密失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返

回值为参数，调用所述系统预设函数，执行步骤 S8 ；

步骤 S4-3 ：所述服务程序对所述第一数据包进行解码，对解码结果进行解密，如解密成功则得到所述用户输入的证书用户名、所述第一信息、所述第二信息和所述第三信息，将所述第一信息、所述第二信息和所述第三信息进行组合，得到所述待签名数据，执行步骤 S4-4，否则将解码解密失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8 ；

步骤 S4-4 ：所述服务程序验证用户输入的 PIN 码，如验证成功则执行步骤 S4-5，否则将验证 PIN 码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8 ；

步骤 S4-5 ：所述服务程序从所述智能密钥设备中的证书中获取证书公钥和证书用户名 ；

步骤 S4-6 ：所述服务程序用所述获取得到的证书用户名验证所述用户输入的证书用户名，如验证成功则执行步骤 S5，否则将验证证书用户名失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

10. 根据权利要求 9 所述的方法，其特征在于，所述步骤 S4-4 之前包括 ：所述服务程序接收用户输入的 PIN 码。

11. 根据权利要求 10 所述的方法，其特征在于，所述步骤 S4-4、步骤 S4-5 和步骤 S4-6 替换为 ：

步骤 S4-4’ ：所述服务程序从所述智能密钥设备中的证书中获取证书公钥和证书用户名 ；

步骤 S4-5’ ：所述服务程序用所述获取得到的证书用户名验证所述用户输入的证书用户名，如验证成功则执行步骤 S4-6’，否则将验证证书用户名失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8 ；

步骤 S4-6’ ：所述服务程序验证用户输入的 PIN 码，如验证成功则执行步骤 S5，否则将验证 PIN 码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

12. 根据权利要求 1 所述的方法，其特征在于，所述步骤 S5 之前还包括 ：所述服务程序连接所述智能密钥设备。

13. 根据权利要求 11 所述的方法，其特征在于，所述步骤 S7 替换为 ：

步骤 S7-1 ：所述服务程序以预设的第二认证参数、所述保存的所述应用程序的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数，清除所述模态框，结束 ；所述返回值为错误码或者表示签名成功的数值。

14. 根据权利要求 2 所述的方法，其特征在于，所述步骤 S6’ 和步骤 S7’ 替换为 ：

步骤 S6’ -1 ：所述服务程序接收所述智能密钥设备返回的信息，判断所述智能密钥设备返回的信息是否为签名结果，是则执行步骤 S7’，否则将签名错误信息作为返回值，所述服务程序以预设的第二认证参数、所述保存的所述应用程序的地址字符串和所述返回值为参数，调用系统预设函数，执行步骤 S8’ ；

步骤 S7’-1 :所述服务程序以所述第二认证参数、所述保存的所述应用程序的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数 ;所述返回值为错误码或者表示签名成功的数值。

15. 根据权利要求 13 所述的方法，其特征在于，所述步骤 S8 包括 :

步骤 S8-0 :当所述应用程序被系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第二认证参数，判断是否认证成功，是则得到签名结果或返回值，结束，否则结束。

16. 根据权利要求 14 所述的方法，其特征在于，所述步骤 S8’包括 :

步骤 S8’-0 :当所述应用程序被系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第二认证参数并判断是否认证成功，如认证成功则判断解析得到的返回值是否为表示正确信息的返回值，是则得到签名结果，结束，否则得到错误信息，结束 ;如认证失败则结束。

17. 根据权利要求 16 所述的方法，其特征在于，所述步骤 S8’还包括 :显示所述签名结果或根据所述返回值显示相应信息。

18. 一种在移动操作系统中完成数字签名的系统，其特征在于，所述系统包括 :应用装置和服务装置 ;

所述应用装置包括编码模块、第一调用模块和第一响应模块 ;

所述编码模块，用于对待签名数据进行编码，得到第一数据包 ;

所述第一调用模块，用于以服务装置的地址字符串、所述应用装置的地址字符串和所述第一数据包为参数，调用系统预设函数 ;

所述第一响应模块，用于当应用装置被系统预设函数调用时，解析所述系统预设函数的参数 ;

所述服务装置包括 :解析模块、存储模块、解码模块、发送模块、第二接收模块和第二调用模块 ;

所述解析模块，用于当服务装置被所述系统预设函数调用时，解析所述系统预设函数的参数 ;

所述存储模块，用于保存所述应用装置的地址字符串 ;

所述解码模块，用于对解析得到的所述系统预设函数的参数中的所述第一数据包进行解码 ;

所述发送模块，用于将所述解码模块解码成功得到的所述待签名数据和预设签名类型发送给智能密钥设备 ;

所述第二接收模块，用于接收所述智能密钥设备返回的信息 ;

所述第二调用模块，以所述智能密钥设备返回的信息、所述保存的所述应用装置的地址字符串和返回值为参数，调用所述系统预设函数，或者，以所述保存的所述应用装置的地址字符串和返回值为参数，调用所述系统预设函数，所述返回值为错误码或者表示签名成功的数值。

19. 根据权利要求 18 所述的系统，其特征在于，所述服务装置中的所述第二接收模块包括接收单元和第一判断单元 ;

所述接收单元，用于接收所述智能密钥设备返回的信息 ;

所述第一判断单元，用于判断所述智能密钥设备返回的信息是否为签名结果；

所述应用装置中还包括第一判断模块；

所述第一判断模块，用于判断所述返回值是否为表示正确信息的返回值。

20. 根据权利要求 18 所述的系统，其特征在于，所述应用装置还包括第一接收模块和组合模块；

所述第一接收模块包括第一接收单元，第二判断单元、第一显示单元、第一加密单元和第三判断单元；

所述第一接收单元，用于接收用户输入的信息及第一用户按键信息；

所述第二判断单元，用于判断是否接收到所述用户输入的信息及第一用户按键信息；

所述第一显示单元，用于通过显示屏将提示信息输出；

所述第一加密单元，用于对所述用户输入的信息中的证书用户名进行加密；

所述第三判断单元，用于根据所述第一用户按键信息判断用户按键类型；

所述组合模块包括标志位单元、第一组合单元和第二加密单元；

所述标志位单元，用于将标志位置位或将标志位复位；

所述第一组合单元，用于对第一信息、第二信息和第三信息进行组合，得到所述待签名数据；

所述第二加密单元，用于对所述待签名数据进行加密，或者，对所述第一信息、第二信息和第三信息分别进行加密。

21. 根据权利要求 18 所述的系统，其特征在于，所述第一调用模块还用于以所述服务装置的地址字符串、所述应用装置的地址字符串、预设的第一认证参数和所述第一数据包为参数，调用所述系统预设函数。

22. 根据权利要求 18 所述的系统，其特征在于，所述第一调用模块包括第一调用单元、第一获取单元和第四判断单元；

所述第一调用单元，用于以所述服务装置的地址字符串、所述应用装置的地址字符串和所述第一数据包为参数，调用所述系统预设函数；

所述第一获取单元，用于获取所述系统预设函数的返回值；

所述第四判断单元，用于判断所述系统预设函数的返回值类型。

23. 根据权利要求 21 所述的系统，其特征在于，所述服务装置包括第二响应模块，用于响应所述系统预设函数；

所述第二响应模块包括第二认证单元和第五判断单元；

所述第二认证单元，用于认证解析得到的第一认证参数；

所述第五判断单元，用于判断是否成功认证所述第一认证参数。

24. 根据权利要求 20 所述的系统，其特征在于，所述服务装置还包括验证模块，用于验证所述解析模块得到的智能密钥设备的序列号；

所述验证模块包括第二接收单元、第六判断单元、第二显示单元、第二获取单元和第七判断单元；

所述第二接收单元，用于接收第二用户按键信息；

所述第六判断单元，用于根据所述第二用户按键信息判断用户按键类型；

所述第二显示单元，用于通过显示屏将模态框输出；

所述第二获取单元，用于获取所述智能密钥设备的序列号；

所述第七判断单元，用于判断获取得到的所述智能密钥设备的序列号与解析得到的所述智能密钥设备序列号是否相同。

25. 根据权利要求 24 所述的系统，其特征在于，所述解码模块包括第八判断单元、解码单元、解密单元、第二组合单元、第一验证单元、第三获取单元和第二验证单元；

所述第八判断单元，用于判断解析得到的所述标志位是否置位；

所述解码单元，用于对解析得到的所述第一数据包进行解码；

所述解密单元，用于对所述解码单元解码成功的结果进行解密；

所述第二组合单元，用于当所述解密单元解密成功时将所述解密得到的第一信息、所述第二信息和所述第三信息进行组合，得到所述待签名数据；

所述第一验证单元，用于验证所述用户输入的 PIN 码；

所述第三获取单元，用于从所述智能密钥设备中的证书中获取证书公钥和证书用户名；

所述第二验证单元，用于根据所述第三获取单元获取的证书用户名验证所述用户输入的证书用户名。

26. 根据权利要求 25 所述的系统，其特征在于，所述第二接收单元还用于接收用户输入的 PIN 码。

27. 根据权利要求 26 所述的系统，其特征在于，所述应用装置还包括连接模块，用于与所述智能密钥设备进行连接。

28. 根据权利要求 27 所述的系统，其特征在于，所述第二调用模块还用于以预设的第二认证参数、所述保存的所述应用装置的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数，清除所述模态框；所述返回值为错误码或者表示签名成功的数值。

29. 根据权利要求 28 所述的系统，其特征在于，所述第一响应模块包括解析单元、第一认证单元和第九判断单元；

所述解析单元，用于当应用装置被系统预设函数调用时，解析所述系统预设函数的参数；

所述第一认证单元，用于认证解析得到的第二认证参数；

所述第九判断单元，用于判断是否成功认证所述第二认证参数。

30. 根据权利要求 18 所述的系统，其特征在于，所述应用装置还包括显示模块，用于显示所述签名结果或根据返回值显示相应错误信息。

一种在移动操作系统中完成数字签名的方法和系统

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种在移动操作系统中完成数字签名的方法和系统。

背景技术

[0002] iOS（iPhone Operating System，苹果操作系统）设备是使用 iOS 作为其操作系统的设备，包括 iPhone、iPad、iPod Touch 以及 Apple TV 等苹果产品。随着 iOS 设备的迅速普及，对 iOS 设备的应用软件的使用及需求也日益增多。

[0003] iOS 设备软件开发者在编写软件的时候，由于设计人员考虑不全面或程序功能不完善，在软件发行后，通常需要对软件不断进行修改或升级。软件开发者对程序修改或加入新的功能后，以补丁的形式发布的方式，用户把这些补丁更新，即修改或升级完成。软件修改或升级是为了更好的满足用户的需求和防止病毒的入侵。

[0004] 现有技术中，系统修改或升级时，需要同时对服务端软件、客户端软件进行升级，修改或升级过程比较繁琐。

发明内容

[0005] 本发明的目的是为了克服现有技术的不足，提供一种在移动操作系统中完成数字签名的方法和系统，实现了软件的独立部署。

[0006] 本发明提供的一种在移动操作系统中完成数字签名的方法，包括：

[0007] 当应用程序被调用时，执行以下步骤：

[0008] 步骤 S1：所述应用程序对待签名数据进行编码，得到第一数据包；

[0009] 步骤 S2：所述应用程序以服务程序的地址字符串、所述应用程序的地址字符串和所述第一数据包为参数，调用系统预设函数；

[0010] 步骤 S3：当服务程序被所述系统预设函数调用时，解析所述系统预设函数的参数，保存所述应用程序的地址字符串；

[0011] 步骤 S4：所述服务程序对解析得到的所述系统预设函数的参数中的所述第一数据包进行解码，如解码成功则得到所述待签名数据，执行步骤 S5，否则将解码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

[0012] 步骤 S5：所述服务程序将所述待签名数据和预设签名类型发送给智能密钥设备；

[0013] 步骤 S6：所述服务程序接收所述智能密钥设备返回的信息；

[0014] 步骤 S7：所述服务程序以所述智能密钥设备返回的信息、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数；

[0015] 步骤 S8：当所述应用程序被所述系统预设函数调用时，所述应用程序解析所述系统预设函数的参数，得到签名结果或所述返回值，结束。

[0016] 所述步骤 S6 至步骤 S8 替换为：

[0017] 步骤 S6’：所述服务程序接收所述智能密钥设备返回的信息，判断所述智能密钥设备返回的信息是否为签名结果，是则执行步骤 S7’，否则将签名错误信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数；

[0018] 步骤 S7’：所述服务程序以所述签名结果、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数；

[0019] 步骤 S8’：当所述应用程序被所述系统预设函数调用时，所述应用程序解析所述系统预设函数的参数，解析得到的返回值是否为表示正确信息的返回值，是则得到所述签名结果，结束，否则得到错误信息，结束。

[0020] 所述步骤 S1 包括：

[0021] 步骤 S1-1：所述应用程序等待接收用户输入的信息及第一用户按键信息，并判断是否接收到所述用户输入的信息及第一用户按键信息，是则执行步骤 S1-3，否则执行步骤 S1-2；所述用户输入的信息包括第一账户、第二账户、传输信息、证书用户名和所述智能密钥设备的序列号；

[0022] 步骤 S1-2：所述应用程序通过显示屏将提示信息输出，返回步骤 S1-1；

[0023] 步骤 S1-3：所述应用程序对所述用户输入的信息中的所述证书用户名进行加密；

[0024] 步骤 S1-4：所述应用程序根据所述第一用户按键信息判断用户按键类型，若所述用户按键类型为原文签名则执行步骤 S1-5，否则执行步骤 S1-7；

[0025] 步骤 S1-5：所述应用程序将标志位置位，对第一信息、第二信息和第三信息进行组合，得到所述待签名数据，对所述待签名数据进行加密；所述第一信息为所述用户输入的信息的一部分，所述第二信息由所述用户输入的信息的剩余部分与所述应用程序中的预设信息组合得到，所述第三信息为所述应用程序中的预设信息；

[0026] 步骤 S1-6：所述应用程序对所述待签名数据的加密结果进行编码，根据编码结果生成所述第一数据包，执行步骤 S2；

[0027] 步骤 S1-7：所述应用程序将标志位复位，对所述第一信息、第二信息和第三信息分别进行加密；

[0028] 步骤 S1-8：所述应用程序分别对所述第一信息、第二信息和第三信息的加密结果进行编码，根据编码结果生成所述第一数据包，执行步骤 S2。

[0029] 所述生成第一数据包具体为：根据所述编码结果和所述标志位生成第一数据包，所述编码结果中包括所述智能密钥设备的序列号和加密后的证书用户名。

[0030] 所述步骤 S2 替换为：

[0031] 步骤 S2’：所述应用程序以服务程序的地址字符串、所述应用程序的地址字符串、预设的第一认证参数和所述第一数据包为参数，调用所述系统预设函数。

[0032] 所述步骤 S2 之后还包括：

[0033] 步骤 S2-1：所述应用程序获取所述系统预设函数的返回值，判断所述返回值类型，若为是则启动所述服务程序，否则结束。

[0034] 所述步骤 S3 包括：

[0035] 步骤 S3-0：当所述服务程序被所述系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第一认证参数并判断是否认证成功，是则保存解析得到的所

述应用程序的地址字符串，否则结束。

[0036] 所述步骤 S3 具体为：

[0037] 步骤 S3-1：当所述服务程序接收到用户输入的第二用户按键信息时，根据所述第二用户按键信息判断用户按键类型，若是确定键则执行步骤 S3-2，否则将用户取消信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

[0038] 步骤 S3-2：所述服务程序通过显示屏将模态框输出；

[0039] 步骤 S3-3：所述服务程序解析所述系统预设函数的参数，并保存所述应用程序的地址字符串；

[0040] 步骤 S3-4：所述服务程序获取所述智能密钥设备的序列号，判断获取的所述智能密钥设备的序列号与解析得到的所述智能密钥设备的序列号是否相同，是则执行步骤 S4，否则将验证所述智能密钥设备序列号的失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

[0041] 所述步骤 S4 包括：

[0042] 步骤 S4-1：所述服务程序判断所述标志位是否置位，是则执行步骤 S4-2，否则执行步骤 S4-3；

[0043] 步骤 S4-2：所述服务程序对所述第一数据包进行解码，对解码结果进行解密，如解密成功则得到所述用户输入的证书用户名和所述待签名数据，执行步骤 S4-4，否则将解码解密失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

[0044] 步骤 S4-3：所述服务程序对所述第一数据包进行解码，对解码结果进行解密，如解密成功则得到所述用户输入的证书用户名、所述第一信息、所述第二信息和所述第三信息，将所述第一信息、所述第二信息和所述第三信息进行组合，得到所述待签名数据，执行步骤 S4-4，否则将解码解密失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

[0045] 步骤 S4-4：所述服务程序验证用户输入的 PIN 码，如验证成功则执行步骤 S4-5，否则将验证 PIN 码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8；

[0046] 步骤 S4-5：所述服务程序从所述智能密钥设备中的证书中获取证书公钥和证书用户名；

[0047] 步骤 S4-6：所述服务程序用所述获取得到的证书用户名验证所述用户输入的证书用户名，如验证成功则执行步骤 S5，否则将验证证书用户名失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

[0048] 所述步骤 S4-4 之前包括：所述服务程序接收用户输入的 PIN 码。

[0049] 所述步骤 S4-4、步骤 S4-5 和步骤 S4-6 替换为：

[0050] 步骤 S4-4’：所述服务程序从所述智能密钥设备中的证书中获取证书公钥和证书用户名；

[0051] 步骤 S4-5’：所述服务程序用所述获取得到的证书用户名验证所述用户输入的证

书用户名，如验证成功则执行步骤 S4-6’，否则将验证证书用户名失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8 ；

[0052] 步骤 S4-6’：所述服务程序验证用户输入的 PIN 码，如验证成功则执行步骤 S5，否则将验证 PIN 码失败信息作为返回值，所述服务程序以所述保存的所述应用程序的地址字符串和所述返回值为参数，调用所述系统预设函数，执行步骤 S8。

[0053] 所述步骤 S5 之前还包括：所述服务程序连接所述智能密钥设备。

[0054] 所述步骤 S7 替换为：

[0055] 步骤 S7-1：所述服务程序以预设的第二认证参数、所述保存的所述应用程序的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数，清除所述模态框，结束。

[0056] 所述步骤 S6’和步骤 S7’替换为：

[0057] 步骤 S6’-1：所述服务程序接收所述智能密钥设备返回的信息，判断所述智能密钥设备返回的信息是否为签名结果，是则执行步骤 S7’，否则将签名错误信息作为返回值，所述服务程序以预设的第二认证参数、所述保存的所述应用程序的地址字符串和所述返回值为参数，调用系统预设函数 ；

[0058] 步骤 S7’-1：所述服务程序以所述第二认证参数、所述保存的所述应用程序的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数。

[0059] 所述步骤 S8 包括：

[0060] 步骤 S8-0：当所述应用程序被系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第二认证参数，判断是否认证成功，是则得到签名结果或返回值，结束，否则结束。

[0061] 所述步骤 S8’包括：

[0062] 步骤 S8’-0：当所述应用程序被系统预设函数调用时，解析所述系统预设函数的参数，认证解析得到的所述第二认证参数并判断是否认证成功，如认证成功则判断解析得到的返回值是否为表示正确信息的返回值，是则得到签名结果，结束，否则得到错误信息，结束；如认证失败则结束。

[0063] 所述步骤 S8’还包括：显示所述签名结果或根据所述返回值显示相应信息。

[0064] 一种在移动操作系统中完成数字签名的系统，包括：应用装置和服务装置 ；

[0065] 所述应用装置包括编码模块、第一调用模块和第一响应模块 ；

[0066] 所述编码模块，用于对待签名数据进行编码，得到第一数据包 ；

[0067] 所述第一调用模块，用于以服务程序的地址字符串、所述应用程序的地址字符串和所述第一数据包为参数，调用系统预设函数 ；

[0068] 所述第一响应模块，用于当应用程序被系统预设函数调用时，解析所述系统预设函数的参数 ；

[0069] 所述服务装置包括：解析模块、存储模块、解码模块、发送模块、第二接收模块和第二调用模块 ；

[0070] 所述解析模块，用于当服务程序被所述系统预设函数调用时，解析所述系统预设函数的参数 ；

[0071] 所述存储模块，用于保存所述应用程序的地址字符串；

[0072] 所述解码模块，用于对解析得到的所述系统预设函数的参数中的所述第一数据包进行解码；

[0073] 所述发送模块，用于将所述解码模块解码成功得到的所述待签名数据和预设签名类型发送给智能密钥设备；

[0074] 所述第二接收模块，用于接收所述智能密钥设备返回的信息；

[0075] 所述第二调用模块，以所述智能密钥设备返回的信息、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数，或者，以所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数。

[0076] 所述服务装置中的所述第二接收模块包括接收单元和第一判断单元；

[0077] 所述接收单元，用于接收所述智能密钥设备返回的信息；

[0078] 所述第一判断单元，用于判断所述智能密钥设备返回的信息是否为签名结果；

[0079] 所述应用装置中还包括第一判断模块；

[0080] 所述第一判断模块，用于判断所述返回值是否为表示正确信息的返回值。

[0081] 所述应用装置还包括第一接收模块和组合模块；

[0082] 所述第一接收模块包括第一接收单元，第二判断单元、第一显示单元、第一加密单元和第三判断单元；

[0083] 所述第一接收单元，用于接收用户输入的信息及第一用户按键信息；

[0084] 所述第二判断单元，用于判断是否接收到所述用户输入的信息及第一用户按键信息；

[0085] 所述第一显示单元，用于通过显示屏将提示信息输出；

[0086] 所述第一加密单元，用于对所述用户输入的信息中的证书用户名进行加密；

[0087] 所述第三判断单元，用于根据所述第一用户按键信息判断用户按键类型；

[0088] 所述组合模块包括标志位单元、第一组合单元和第二加密单元；

[0089] 所述标志位单元，用于将标志位置位或将标志位复位；

[0090] 所述第一组合单元，用于对第一信息、第二信息和第三信息进行组合，得到所述待签名数据；

[0091] 所述第二加密单元，用于对所述待签名数据进行加密，或者，对所述第一信息、第二信息和第三信息分别进行加密。

[0092] 所述第一调用模块还用于以所述服务程序的地址字符串、所述应用程序的地址字符串、预设的第一认证参数和所述第一数据包为参数，调用所述系统预设函数。

[0093] 所述第一调用模块包括第一调用单元、第一获取单元和第四判断单元；

[0094] 所述第一调用单元，用于以所述服务程序的地址字符串、所述应用程序的地址字符串和所述第一数据包为参数，调用所述系统预设函数；

[0095] 所述第一获取单元，用于获取所述系统预设函数的返回值；

[0096] 所述第四判断单元，用于判断所述系统预设函数的返回值类型。

[0097] 所述服务装置包括第二响应模块，用于响应所述系统预设函数；

[0098] 所述第二响应模块包括第二认证单元和第五判断单元；

[0099] 所述第二认证单元，用于认证解析得到的第一认证参数；

[0100] 所述第五判断单元，用于判断是否成功认证所述第一认证参数。

[0101] 所述服务装置还包括验证模块，用于验证所述解析模块得到的智能密钥设备的序列号；

[0102] 所述验证模块包括第二接收单元、第六判断单元、第二显示单元、第二获取单元和第七判断单元；

[0103] 所述第二接收单元，用于接收第二用户按键信息；

[0104] 所述第六判断单元，用于根据所述第二用户按键信息判断用户按键类型；

[0105] 所述第二显示单元，用于通过显示屏将模态框输出；

[0106] 所述第二获取单元，用于获取所述智能密钥设备的序列号；

[0107] 所述第七判断单元，用于判断获取得到的所述智能密钥设备的序列号与解析得到的所述智能密钥设备序列号是否相同。

[0108] 所述解码模块包括第八判断单元、解码单元、解密单元、第二组合单元、第一验证单元、第三获取单元和第二验证单元；

[0109] 所述第八判断单元，用于判断解析得到的所述标志位是否置位；

[0110] 所述解码单元，用于对解析得到的所述第一数据包进行解码；

[0111] 所述解密单元，用于对所述解码单元解码成功的结果进行解密；

[0112] 所述第二组合单元，用于当所述解密单元解密成功时将所述解密得到的第一信息、所述第二信息和所述第三信息进行组合，得到所述待签名数据；

[0113] 所述第一验证单元，用于验证所述用户输入的 PIN 码；

[0114] 所述第三获取单元，用于从所述智能密钥设备中的证书中获取证书公钥和证书用户名；

[0115] 所述第二验证单元，用于根据所述第三获取单元获取的证书用户名验证所述用户输入的证书用户名。

[0116] 所述第二接收单元还用于接收用户输入的 PIN 码。

[0117] 所述应用装置还包括连接模块，用于与所述智能密钥设备进行连接。

[0118] 所述第二调用模块还用于以预设的第二认证参数、所述保存的所述应用程序的地址字符串、所述智能密钥设备返回的信息和返回值为参数，调用所述系统预设函数，清除所述模态框。

[0119] 所述第一响应模块包括解析单元、第一认证单元和第九判断单元；

[0120] 所述解析单元，用于当应用程序被系统预设函数调用时，解析所述系统预设函数的参数；

[0121] 所述第一认证单元，用于认证解析得到的第二认证参数；

[0122] 所述第九判断单元，用于判断是否成功认证所述第二认证参数。

[0123] 所述应用装置还包括显示模块，用于显示所述签名结果或根据返回值显示相应错误信息。

[0124] 本发明与现有技术相比，具有以下优点：

[0125] 服务端为客户端提供服务接口，用户按照接口规范编写完程序后，服务端修改或升级服务程序，客户端程序不需要改变；反之，客户端程序进行修改或升级，服务端不需要改变，系统升级简单方便。

附图说明

[0126] 图 1 是本发明实施例 1 提供的一种在移动操作系统中完成数字签名的方法流程图；

[0127] 图 2、图 3 和图 4 是本发明实施例 2 提供的一种在移动操作系统中完成数字签名的方法流程图；

[0128] 图 5 是本发明实施例 3 提供的一种在移动操作系统中完成数字签名的系统的方框示意图。

具体实施方式

[0129] 目前 iOS4 及其以上版本的多任务机制并不是传统意义上的多任务，即任何程序都可以自由地在后台运行。苹果开放给第三方软件开发者的后台运行接口只包括音频播放(例如网络电台软件)、地理位置侦测(例如，GPS 软件)和网络电话(例如，网络即时语音沟通工具 Skype)等几个功能。在 iOS4 及其以上版本里，如果用户单击 Home 退到桌面，那么正在运行的软件并没有退出，而是被冻结。虽然软件被置入后台，处于凝滞状态，但仍然在运行，之前分配给软件的系统资源仍然在位。因此，当用户重新回到这个软件时，软件可以立即恢复到上次退出时的状态，这就是 iOS4 及其以上版本的多任务功能的核心所在。处于冻结状态的软件可以进行某些操作，例如音频播放，但并不是所有操作都能进行，而且，iOS 系统会因为需要省出内存而终止某个程序。

[0130] 综上所述，为满足一种应用程序与服务程序相互调用的需求，本发明采用 openURL 函数跳转方式以解决此问题。

[0131] 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，所描述的实施例仅仅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做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。

[0132] 实施例 1

[0133] 本发明的实施例 1 提供一种在移动操作系统中完成数字签名的方法，如图 1 所示，本方法包括：

[0134] 当应用程序被调用时，执行以下步骤：

[0135] 步骤 101：应用程序对待签名数据进行编码，得到第一数据包；

[0136] 步骤 102：应用程序以服务程序的地址字符串、应用程序的地址字符串和第一数据包为参数，调用系统预设函数；

[0137] 步骤 103：当服务程序被系统预设函数调用时，解析系统预设函数的参数，保存应用程序的地址字符串；

[0138] 步骤 104：服务程序对解析得到的系统预设函数的参数中的第一数据包进行解码，如解码成功则得到待签名数据，执行步骤 105，否则将解码失败信息作为返回值，服务程序以保存的所述应用程序的地址字符串和返回值为参数，调用系统预设函数，执行步骤 108；

[0139] 步骤 105：服务程序将待签名数据和预设签名类型发送给智能密钥设备；

[0140] 具体地，本实施例中，该步骤之前还包括服务程序连接智能密钥设备；智能密钥设备接收到待签名数据和预设签名类型后，根据预设签名类型对应的算法对待签名数据进行签名，并将签名结果返回给服务程序；如智能密钥设备中没有与预设签名类型对应的算法，则给服务器返回签名错误的信息；

[0141] 步骤 106：服务程序接收智能密钥设备返回的信息；

[0142] 具体地，本实施例中，智能密钥设备返回的信息包括签名结果或签名错误信息；

[0143] 步骤 107：服务程序以智能密钥设备返回的信息、保存的应用程序的地址字符串和返回值为参数，调用系统预设函数；

[0144] 步骤 108：当应用程序被系统预设函数调用时，解析系统预设函数的参数，得到签名结果或返回值，结束。

[0145] 本实施例中提供的一种在移动操作系统中完成数字签名的方法，当应用程序进行修改或升级时，服务程序不需要改变；反之，服务程序进行修改或升级时，应用程序不需要改变，实现了应用程序和服务程序的独立部署。

[0146] 实施例 2

[0147] 本发明的实施例 2 提供一种在移动操作系统中完成数字签名的方法，如图 2、图 3 和图 4 所示，应用程序和服务程序配置文件中的 URL 选项预先设置，本方法包括：

[0148] 当应用程序被调用时，执行以下步骤：

[0149] 步骤 201：应用程序等待接收用户输入的信息及第一用户按键信息，应用程序判断是否接收到用户输入的信息及第一用户按键信息，是则执行步骤 203，否则执行步骤 202；

[0150] 优选地，本实施例中，用户从预置列表中选择是否调用该应用程序；除此之外，也可以根据配置文件选择是否调用该应用程序；

[0151] 例如，本实施例中，用户输入信息包括第一账户、第二账户、传输信息、CN 字段和智能密钥设备的序列号；

[0152] 例如，本实施例中第一账户为：123456789，第二账户为 987654321，传输信息为 12，CN 字段为 test，智能密钥设备的序列号为 FFFFFFFFFF；

[0153] 步骤 202：应用程序通过显示屏将提示信息输出，返回步骤 201；

[0154] 例如，本实施例中，提示信息为：用户需输入第一账户、第二账户、传输信息、CN 字段和智能密钥设备序列号；

[0155] 步骤 203：应用程序对用户输入的 CN 字段进行加密；

[0156] 例如，本实施例中，使用对称加密算法对 CN 字段进行加密，优选地，使用 3DES 对称加密算法，CBC 模式，2key，采用 PKCS#5 补位，密钥由多个因子生成，包括内置密钥、会话标识、随机因子，以上因子依次拼接后进行 SHA1 摘要，取前 16 字节作为密钥；其中内置密钥预先存储在智能密钥设备中；

[0157] 步骤 204：应用程序根据第一用户按键信息判断用户按键类型，若用户按键为原文签名则执行步骤 205，若用户按键为 Xml 签名则执行步骤 209；

[0158] 步骤 205：应用程序将标志位设为 1，对显示信息、Xml 信息和扩展信息进行组合，得到待签名数据，对待签名数据进行加密；

[0159] 具体地，本实施例中，显示信息由用户输入，Xml 信息由预先设置在应用程序中的

信息和用户输入的信息组合而成，扩展信息预先设置在应用程序中；

[0160] 本实施例中，该步骤加密方法与步骤 203 相同；优选地，本实施例中，应用程序对显示信息、Xml 信息和扩展信息进行 TLV 组合；

[0161] 例如，本实施例中，组合报文为：1100000009662100000000848<?xml version="1.0" encoding="UTF-8"?><TradeData><field name="\u91d1\u989d" value="1\u5143" DisplayOnScreen="TRUE"/><field name="\u5927\u5199\u91d1\u989d" value="\u58f9\u4f70\u8d30\u62fe\u53c1\u5143\u6574" DisplayOnScreen="TRUE"/><field name="\u6c47\u6b3e\u5355\u4f4d\u540d\u79f0" value="\u5317\u4eac\u634c\u96f6\u540e\u5e7f\u544a\u5236\u4f5c\u6709\u9650\u516c\u53f8" DisplayOnScreen="TRUE"/><field name="\u6c47\u6b3e\u5355\u4f4d\u8d26\u53f7" value="1222" DisplayOnScreen="TRUE"/><field name="\u6c47\u6b3e\u5355\u4f4d\u5f00\u6237\u884c\u540d\u79f0" value="\u548c\u5e73\u8857\u652f\u884c" DisplayOnScreen="TRUE"/><field name="\u6536\u6b3e\u5355\u4f4d\u540d\u79f0" value="\u591a\u6765\u63d0\u00b7\u7a46\u6d77\u9ea6\u63d0" DisplayOnScreen="TRUE"/><field name="\u6536\u6b3e\u5355\u4f4d\u8d26\u53f7" value="1222" DisplayOnScreen="TRUE"/><field name="\u6536\u6b3e\u5355\u4f4d\u5f00\u6237\u884c\u540d\u79f0" value="xxxx" DisplayOnScreen="TRUE"/><field name="\u767b\u9646ID" value="80hou0.c.0200" DisplayOnScreen="TRUE"/><field name="\u4ea4\u6613\u63d0\u4ea4\u65f6\u95f4" value="2012061416" DisplayOnScreen="TRUE"/></TradeData>220000000082\u91d1\u989d:1\u5143

[0162] \u6c47\u6b3e\u8d26\u53f7:1222(\u5de5\u5546\u94f6\u884c)

[0163] \u6536\u6b3e\u8d26\u53f7:1222(\u5de5\u5546\u94f6\u884c)230000000000；

[0164] 步骤 206：应用程序对加密后的待签名数据进行编码，得到第一数据包；

[0165] 优选地，本实施例中，应用程序对加密后的组合报文进行 Base64 编码；

[0166] 步骤 207：应用程序以服务程序的 URL 字符串、应用程序的 URL 字符串、第一认证参数和请求报文信息为参数，调用 openURL 函数，执行步骤 211；

[0167] 本实施例中，openURL 函数为 iOS 系统的系统函数；

[0168] 具体地，本实施例中，第一认证参数用于在服务程序中认证应用程序；

[0169] 具体地，本实施例中，第一认证参数和服务程序的 URL 字符串预先设置在应用程序中；

[0170] 本实施例中，请求报文信息包括标志位、应用程序的 URL 字符串、用户输入的智能密钥设备的序列号、用户输入的 CN 字段和第一数据包；具体地，标志位为请求报文信息中的报文类型(MessageType)，应用程序的 URL 字符串为请求报文信息中的应用名称(APPURLName)，用户输入的智能密钥设备的序列号为请求报文信息中的介质凭证号(U_SerialNumber)，用户输入的 CN 字段为请求报文信息中的客户证书标识(U_CertCN)，第一数据包为请求报文信息中的 Sign_PlainText；

[0171] 除此之外，本实施例中，请求报文信息还包括：报文版本号(Version)、会话标识(SessionID)、随机因子(Random、APP)版本号(APPVersion)、U 盾介质凭证号(U_

SerialNumber)、U盾语言标识(U_Language)、U盾字符集(U_Charset)、签名警告信息(Sign_WarningInfo)和备用字段(Reserve);以上请求报文信息均预先设置在应用程序中;

[0172] 例如,本实施例中,调用openURL函数的方式为:

[0173] openURL:url

[0174] openURL函数的参数为:

[0175] url=cn.com.xxxx.ftsafe.pad://MessageType=0&Version=1.0.0.0&SessionID=11111111111111111111111111111111111111111&Random=222222222222222222222222222222222222222&APPURLName=cn.com.xxxx.pad&APPVersion=1.0.0.0&U_SerialNumber=FFFFFFFFFF&U_CertCN=//RWwp6uvnQ=&U_Language=zh_CN&U_Charset=UTF-8&Sign_WarningInfo=Warning&Sign_PlainText=A0IZ2oEy5YjkAk_aHWmnvS41J94c0iikwppHANJ9rj2dPui8Fcpoir3d4UbK9xL_s1azL4n5pOwGGkKJtcLrw9qPHeYOd5Ai6PvMniIbKakpUT9whmWftUFXvnOXWrSYtsq1AAjnbUjafgGVgmDxLspLz9ZdeTDxOjrJvDJUzMYGkhrDah6bGhe2acKjXUOXte0W2vBApbScP5avN_QHL3Cqfmqrlo1LDCdtx7mPgRR3twaT0JhI0iNCWru4b6Lg361scWCuWnX-AXvJyXuBso8OuGmUVLqKDX2aBscG98b62ao4PCZNC01V1SfZmZKvtCNpJY1Z-Br1TVQZoSpTfq50je-_2S-tdWI4a3MPN7Fwr55pc1hsF_bGtUfupXo-pENE2XafQ8AN00vaIHz6p4iydX_4-_EV29aiBwwdSTLZ1r2FTvnTdNYjJOBg3a9r1Zy9gni78c0S0f7kwG62cUU4xvgz1WcFMwvxhPut7QVOphng4Xi3XDzYp6pqvAamv_9mVKO-27GpLjQ2QHpST0CUzhJDZH15RV811BDDuT78I7VBcuGa3bAL7eBXCUA81K7UWpzC-dBVCcD0LmnEaCFOMuLF3EGyak5LSoeGb3Xu4toIVjS_XgbtEKMFaEZo_1ktehAKqPq1vJE3QnDskLo1YQPK3LuDe2AR0YJmB0x6swsKvXPpNInFEQBCsm2cSb3PZGjLzyUBwKDYCfzK4tbZ60PvbYYzJUNYmQgptqPum7inq1i6j000bjrsMFbG-jiXGIRd0-xEZeN6gpuVKWtVI0a5-Jd3TGF9B5tBqjgT4b0oVy9B4R20Vr6HKHMun6_jid3dr9Y1xDG314-B9f8KfPKq_ftA4MG2C6R0iXtAhDLNqm17QIRP7MeWBSho7HfiH3FHTIhuXpkJ_v_JZi0rIt83kB5-nnwjSK0sCDCfsvX3zW0090NinNLIct2cnfK3xz6HAdU5Ved1_2T8nID8JAVbyzbFPYPX0b3mcJPpwkFgXTcTawupSVM8___mt_Oa-0GqXFogHTRJRQ4wgnzX6QTK92dsseXNgtAc80iWGLmPP0ERyj99oF8JcIAl35tpdLlqB_WxrtkPgCyT5w80jiTv8sPnPkkxlcM7daMw64rFjauv79CnIIrtS88mdd_1iWMo8xMuZc258GTbrs8aRlocYa1LnwVwx3t97qSy-_O4DH9JcJsywhmy43hmAY17epdZD5U9_z5eBhFccnKg7IYiZVIe9o7rQN8CD_dRwgnduuh_i6D5n4SmzDAGfamLKgGZA-M9kjWSt8D9hNcIRU1jQF9JxRUu6QK0a1qiI_YFo28rrfos1JUTTrS5H3VXgqqRcIZDA23M0DJZK4S8xW_-Vp7w&Sign_XMLInfo=&Sign_KeyInfo=&Sign_FileInfo=&Reserve=

[0176] 步骤208:应用程序将标志位设为0,对显示信息、Xml信息和扩展信息分别进行加密;

[0177] 本实施例中,该步骤加密方法与步骤203相同;

[0178] 例如,本实施例中,显示信息为:\u91d1\u989d:12\u5143

[0179] \u6c47\u6b3e\u8d26\u53f7:123456789(\u5de5\u5546\u94f6\u884c)

[0180] \u6536\u6b3e\u8d26\u53f7:987654321(\u5de5\u5546\u94f6\u884c);

[0181] 加密后的显示信息为:poNPdZy7rcYeSYECejXLR5E+Xd21Q80fp

[0182] MUupuSiJgBtRySw3HcydrCL/XPHYmH1ugdhJO5IFLU1mcFg4XxYCu4L7s81/UBf08EKPA/figdoODV8Nnf/+fFcNJ62SEs/;

[0183] 步骤 209 :应用程序对加密结果分别进行编码 ;

[0184] 优选地,本实施例中,应用程序对加密结果分别进行 Base64 编码 ;

[0185] 具体地,该步骤中,加密结果包括加密后的 CN 字段,加密后的显示信息、Xml 信息和扩展信息 ;

[0186] 例如,本实施例中,对加密后的显示信息进行编码,结果为 :poNPdZy7rcYeSYECejXLR5E-Xd2lQ8OfpMUupuSiJgBtRySw3HcydrCL_XPHYmH1ugdhJO5IFLU1mcFg4XxYCu4L7s81_UBfO8EKPA_figdoODV8Nnf_-fFcNJ62SEs ;

[0187] 步骤 210 :应用程序以服务程序的 URL 字符串、应用程序的 URL 字符串、第一认证参数和请求报文信息为参数,调用 openURL 函数 ;

[0188] 本实施例中,openURL 函数为 iOS 系统的系统函数 ;

[0189] 具体地,本实施例中,第一认证参数用于在服务程序中认证应用程序 ;

[0190] 具体地,本实施例中第一认证参数和服务程序的 URL 字符串预先设置在应用程序中 ;

[0191] 具体地,本实施例中,标识位为请求报文信息中的报文类型(MessageType),应用程序的 URL 字符串为请求报文信息中的应用名称(APPURLName),用户输入的智能密钥设备的序列号为请求报文信息中的介质凭证号(U_SerialNumber),加密编码后的显示信息为请求报文信息中的 Sign_KeyInfo,加密编码后的 Xml 信息为请求报文信息中的 Sign_XMLInfo,加密编码后的扩展信息为请求报文信息中的 Sign_FileInfo ;

[0192] 除此之外,本实施例中,请求报文信息还包括 :报文版本号(Version)、会话标识(SessionID)、随机因子(Random)、APP 版本号(APPVersion)、介质凭证号(U_SerialNumber)、客户证书标识(U_CertCN)、U 盾语言标识(U_Language)、U 盾字符集(U_Charset)、签名警告信息(Sign_WarningInfo)和备用字段(Reserve);以上请求报文信息均预先设置在应用程序中 ;

[0193] 步骤 211 :应用程序获取 openURL 函数的返回值,判断返回值类型,若为 YES 则启动服务程序,若为 NO 则结束 ;

[0194] 具体地,本实施例中,openURL 函数的返回值是 BOOL 类型的 ;

[0195] 具体地,该步骤中,openURL 函数根据服务程序的 URL 字符串查找注册过的 URL Schemes 选项的 app,找到则 openURL 函数返回 YES,找不到则返回 NO ;

[0196] 例如,本实施例中,服务程序的 URL 为 :cn.com.xxxx.ftsafe.phone ;

[0197] 步骤 212 :当服务程序被 openURL 函数调用时,认证第一认证参数,判断是否成功认证第一认证参数,是则执行步骤 213,否则结束 ;

[0198] 具体地,服务程序判断第一认证参数与预先设置在服务程序中的认证参数是否相同,是则执行步骤 213,否则结束 ;

[0199] 步骤 213 :当服务程序接收到用户输入的 PIN 码及第二用户按键信息时,根据第二用户按键信息判断用户按键类型,若是确定则执行步骤 214,若是取消则将用户取消信息作为返回值,执行步骤 227 ;

[0200] 步骤 214 :服务程序通过显示屏将模态框输出 ;

[0201] 例如,本实施例中,模态框的内容为 :正在签名,请等待 ;

[0202] 步骤 215 :服务程序解析 openURL 函数的参数,并将解析得到的 APPURLName 中应

用程序的 URL 字符串保存在 APPURLName_str 中，连接智能密钥设备；

[0203] 例如，本实施例中，openURL 函数的参数为：

[0204] cn.com.xxxx.ftsafe.pad://MessageType=0&Version=1.0.0.0&SessionID=11111111111111111111111111111111111111111&Random=22222222222222222222222222222222222222&APPURLName=cn.com.xxxx.pad&APPVersion=1.0.0.0&U_SerialNumber=FFFFFFFFFF&U_CertCN=//RWwp6uvnQ=&U_Language=zh_CN&U_Charset=UTF-8&Sign_WarningInfo=Warning&Sign_PlainText=A0IZ2oEy5YjkAk_aHWmnvS41J94c0iikwppHANJ9rj2dPui8Fcpoir3d4UbK9xL_s1azL4n5p0wGGkKJtcLrw9qPHeY0d5Ai6PvMniIbKakpUT9whmWftUFXvn0XWrSYtsq1AAjnbUjafgGVgmDxLspLz9ZdeTDx0jrJvDJUzMYGkhrDah6bGhe2acKjXU0Xte0W2vBApbScP5avN_QHL3Cqfmqrlo1LDCdtx7mPgRR3twaT0JhI0iNCWru4b6Lg361scWCuWnX-AXvJyXuBso8OuGmUVLqKDX2aBscG98b62ao4PCZNC01V1SfZmZKvtCNpJY1Z-Br1TVQZoSpTfq50je-_2S-tdWI4a3MPN7Fwr55pc1hsF_bGtUfupXo-pENE2XafQ8AN00vaIHz6p4iydX_4-_EV29aiBwwdSTLZ1r2FTvnTdNYjJOBg3a9r1Zy9gni78c0S0f7kwG62cUU4xvgz1WcFMwvxhPut7QV0phng4Xi3XDzYp6pqvAamv_9mVK0-27GpLjQ2QHpST0CUzhJDZH15RV811BDDuT78I7VBcuGa3bAL7eBXCUA81K7UWpzC-dBVCcD0LmnEaCF0MuLF3EGyak5LSoeGb3Xu4toIVjS_XgbtEKMFaEZo_1ktehAKqPq1vJE3QnDskLo1YQPK3LuDe2AR0YJmB0x6swsKvXPpNInFEQBCsm2cSb3PZGjLzyUBwKDYCfzK4tbZ60PvbYYzJUNYmQgptqPum7inq1i6j000bjrsMFbG-jiXGIRd0-xEZeN6gpuVKWtVI0a5-Jd3TGF9B5tBqjgT4b0oVy9B4R20Vr6HKHMun6_jid3dr9Y1xDG314-B9f8KfPKq_ftA4MG2C6R0iXtAhDLNqm17QIRP7MeWBSho7HfiH3FHTIhuXpkJ_v_JZi0rIt83kB5-nnwjSK0sCDCfsvX3zW0090NinNLIct2cnfK3xz6HAdU5Ved1_2T8nID8JAVbyzbFPYPX0b3mcJPpwkFgXTcTawupSVM8___mt_0a-0GqXFogHTRJRQ4wgnzX6QTK92dsseXNgtAc80iWGLmPP0ERyj99oF8JcIA135tpdLlqB_WxrtkPgCyT5w80jiTv8sPnPkkx1cM7daMw64rFjauv79CnIIrtS88mdd_1iWMo8xMuZc258GTbrs8aRlocYa1LnwVwx3t97qSy-_O4DH9JcJsywhmy43hmAY17epdZD5U9_z5eBhFccnKg7IYiZVIe9o7rQN8CD_dRwgnduuh_i6D5n4SmzDAGfamLKgGZA-M9kjWSt8D9hNcIRUljQF9JxRUu6QK0a1qiI_YFo28rrfos1JUTTrS5H3VXgqqRcIZDA23M0DJZK4S8xW_-Vp7w&Sign_XMLInfo=&Sign_KeyInfo=&Sign_FileInfo=&Reserve=

[0205] 步骤 216：服务程序从智能密钥设备中获取序列号，判断获取的智能密钥设备的序列号与应用程序发送的智能密钥设备的序列号是否相同，是则执行步骤 217，否则将验证智能密钥设备的序列号失败信息作为返回值，执行步骤 227；

[0206] 步骤 217：服务程序判断标志位是否为 1，是则执行步骤 218，否则执行步骤 219；

[0207] 步骤 218：服务程序对第一数据包进行解码，对解码结果进行解密，如解密成功则得到待签名数据，执行步骤 221，否则将解码解密失败信息作为返回值，执行步骤 227；

[0208] 步骤 219：服务程序对第一数据包进行解码，对解码结果进行解密，成功则得到 CN 字段、显示信息、Xml 信息和扩展信息，执行步骤 220，否则将解码解密失败信息作为返回值，执行步骤 227；

[0209] 例如，本实施例中，编码后的数据为：poNPdZy7rcYeSYECejXLR5E-Xd21Q8

[0210] OfpMUupuSiJgBtRySw3HcydrCL_XPHYmH1ugdhJ05IFLU1mcFg4XxYCu4L7s81_UBf08EKPA_figdoODV8Nnf_-fFcNJ62SEs；

[0211] 进行解密并解码后得到：

[0212] \u91d1\u989d:12\u5143

[0213] \u6c47\u6b3e\u8d26\u53f7:123456789(\u5de5\u5546\u94f6\u884c)

[0214] \u6536\u6b3e\u8d26\u53f7:987654321(\u5de5\u5546\u94f6\u884c)；

[0215] 步骤 220：服务程序将解密后的显示信息、Xml 信息和扩展信息进行组合，得到待签名数据；

[0216] 优选地，本实施例中，服务程序对显示信息、Xml 信息和扩展信息进行 TLV 组合；

[0217] 步骤 221：服务程序验证用户输入的 PIN 码，判断验证是否成功，是则执行步骤 222，否则将验证 PIN 码失败信息作为返回值，执行步骤 227；

[0218] 具体地，该步骤中服务程序验证用户输入的 PIN 码的方法为：服务程序比较用户输入的 PIN 码与预先存储在智能密钥设备中的 PIN 码是否相同，是则执行步骤 222，否则将验证 PIN 码失败信息作为返回值，执行步骤 227；

[0219] 例如，本实施例中 PIN 码为 12345678；

[0220] 步骤 222：服务程序从智能密钥设备中读取证书中的证书公钥和 CN 字段；

[0221] 具体地，本实施例中，服务程序通过读取智能密钥设备中证书来获取证书公钥和 CN 字段；

[0222] 步骤 223：服务程序验证 CN 字段，判断是否验证成功，是则执行步骤 224，否则将验证证书用户名失败信息作为返回值，执行步骤 227；

[0223] 具体地，该步骤中服务程序验证 CN 字段的方法为：服务程序比较解密后的 CN 字段与从智能密钥设备中获取的 CN 字段是否相同，是则执行步骤 224，否则将验证证书用户名失败信息作为返回值，执行步骤 227；

[0224] 步骤 224：服务程序将待签名数据、待签名数据的长度、证书、证书长度、签名类型和智能密钥设备的序列号发送到智能密钥设备；

[0225] 具体地，本实施例中，签名类型预先设置在服务程序中；

[0226] 智能密钥设备接收到服务程序发送的数据后，根据局待签名数据的长度验证待签名数据，验证成功后根据证书、证书长度获取对应用户私钥对待签名数据进行加密，然后使用与签名类型对应的算法对加密加过进行签名得到签名结果并返回给服务程序；如验证失败或没有与签名类型对应的算法则给服务程序返回签名错误信息；

[0227] 步骤 225：服务程序接收智能密钥设备返回的信息，判断智能密钥设备返回的信息是否为签名结果，是则执行步骤 226，否则执行步骤 227；

[0228] 步骤 226：服务程序以保存在 APPURLName_str 中应用程序的 URL 字符串、第二认证参数、应答报文的信息和返回值为参数，调用 openURL 函数，清除模态框，执行步骤 228；

[0229] 具体地，本实施例中，第二认证参数预先设置在服务程序中，用于在应用程序中认证服务程序；

[0230] 具体地，本实施例中，该步骤中返回值为 0；

[0231] 本实施例中，应答报文信息包括签名结果和返回值，具体地，签名结果为应答报文信息中的签名包(Sign_PKCS7Info)，返回值为应答报文信息中的应答码(ResponseCode)；

[0232] 除此之外，本实施例中，应答报文信息还包括：报文类型(MessageType)、报文版本号(Version)、会话标识(SessionID)、随机因子(Random)、U 盾 APP 版本号(U_APPVersion)、U 盾介质凭证号(U_SerialNumber)、U 盾公钥密文(U_PublicKeyC) 和备

用字段(Reserve)；其中，报文类型(MessageType)、报文版本号(Version)、会话标识(SessionID)和随机因子(Random)由应用程序通过openURL函数发送给服务程序，服务程序在解析参数时写入相应位置，U盾APP版本号(U_APPVersion)预先设置在服务程序中，获取的智能密钥设备的序列号为U盾介质凭证号(U_SerialNumber)，读取的智能密钥设备的证书公钥为U盾公钥密文(U_PublicKeyC)；

[0233] 例如，本实施例中，保存在APPURLName_str中应用程序的URL字符串为：cn.com.xxxx.phone；

[0234] 步骤227：服务程序以保存在APPURLName_str中应用程序的URL字符串、第二认证参数和返回值为参数，调用openURL函数，清除模态框，执行步骤228；

[0235] 具体地，该步骤中，服务程序将相应的错误码作为返回值；例如，若服务程序Base64解码失败则返回值为402，若服务程序解密失败则返回值为423，若用户按键为取消则返回值为404，若智能密钥设备签名失败则返回值为420；

[0236] 步骤228：当应用程序被openURL函数调用时，认证第二认证参数，判断是否成功认证第二认证参数，是则执行步骤229，否则应用程序结束；

[0237] 具体地，应用程序判断第二认证参数与预先设置在应用程序中的认证参数是否相同，是则执行步骤229，否则应用程序结束；

[0238] 步骤229：应用程序解析openURL函数的参数，判断解析得到的返回值是否为0，是则执行步骤230，否则执行步骤231；

[0239] 例如，本实施例中，返回值为0则表示签名成功，返回值不为0则表示错误；

[0240] 步骤230：应用程序显示签名结果，结束；

[0241] 步骤231：应用程序根据返回值显示相应错误信息，结束；

[0242] 本实施例中，服务程序验证PIN码步骤和验证CN字段步骤的顺序可以交换，也可以在步骤216和步骤217之间执行验证PIN码和验证CN字段的步骤。本实施例中提供的一种在移动操作系统中完成数字签名的方法，当应用程序进行修改或升级时，服务程序不需要改变；反之，服务程序进行修改或升级时，应用程序不需要改变，实现了应用程序和服务程序的独立部署。

[0243] 实施例3

[0244] 本发明的实施例3提供一种在移动操作系统中完成数字签名的系统，如图5所示，包括：应用装置31和服务装置32；

[0245] 应用装置31包括编码模块31A、第一调用模块31B和第一响应模块31C；

[0246] 编码模块31A，用于对待签名数据进行编码，得到第一数据包；

[0247] 第一调用模块31B，用于以服务程序的地址字符串、应用程序的地址字符串和第一数据包为参数，调用系统预设函数；

[0248] 第一响应模块31C，用于当应用程序被系统预设函数调用时，解析系统预设函数的参数；

[0249] 服务装置包括：解析模块32A、存储模块32B、解码模块32C、发送模块32D、第二接收模块32E和第二调用模块32F；

[0250] 解析模块32A，用于当服务程序被所述系统预设函数调用时，解析系统预设函数的参数；

[0251] 存储模块 32B，用于保存应用程序的地址字符串；

[0252] 解码模块 32C，用于对解析得到的系统预设函数的参数中的第一数据包进行解码；

[0253] 发送模块 32D，用于将待签名数据和预设签名类型发送到智能密钥设备；

[0254] 第二接收模块 32E，用于接收智能密钥设备返回的信息；

[0255] 第二调用模块 32F，以所述智能密钥设备返回的信息、所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数，或者，以所述保存的所述应用程序的地址字符串和返回值为参数，调用所述系统预设函数。

[0256] 服务装置 32 中的所述第二接收模块 32E 包括接收单元和第一判断单元；

[0257] 接收单元，用于接收所述智能密钥设备返回的信息；

[0258] 第一判断单元，用于判断所述智能密钥设备返回的信息是否为签名结果；

[0259] 应用装置 31 中还包括第一判断模块 31D；

[0260] 第一判断模块 31D，用于判断所述返回值是否为表示正确信息的返回值。

[0261] 应用装置 31 还包括第一接收模块 31E 和组合模块 31F；

[0262] 第一接收模块 31E 包括第一接收单元 31E-1、第二判断单元 31E-2、第一显示单元 31E-3、第一加密单元 31E-4 和第三判断单元 31E-5；

[0263] 第一接收单元 31E-1，用于接收用户输入的信息及第一用户按键信息；

[0264] 第二判断单元 31E-2，用于判断是否接收到用户输入的信息及第一用户按键信息；

[0265] 第一显示单元 31E-3，用于通过显示屏将提示信息输出；

[0266] 第一加密单元 31E-4，用于对用户输入的证书用户名进行加密；

[0267] 第三判断单元 31E-5，用于根据第一用户按键信息判断用户按键类型；

[0268] 组合模块 31F 包括标志位单元 31F-1、第一组合单元 31F-2 和第二加密单元 31F-3；

[0269] 标志位单元 31F-1，用于将标志位置位或将标志位复位；

[0270] 第一组合单元 31F-2，用于对第一信息、第二信息和第三信息进行组合，得到待签名数据；

[0271] 第二加密单元 31F-3，用于对待签名数据进行加密，或者，对所述第一信息、第二信息和第三信息分别进行加密。

[0272] 第一调用模块 31B 还用于以服务程序的地址字符串、应用程序的地址字符串、第一认证参数和第一数据包为参数，调用系统预设函数。

[0273] 第一调用模块 31B 包括第一调用单元 31B-1、第一获取单元 31B-2 和第四判断单元 31B-3；

[0274] 第一调用单元 31B-1，用于以所述服务程序的地址字符串、所述应用程序的地址字符串和所述第一数据包为参数，调用所述系统预设函数；

[0275] 第一获取单元 31B-2，用于获取系统预设函数的返回值；

[0276] 第四判断单元 31B-3，用于判断系统预设函数的返回值类型。

[0277] 服务装置 32 包括第二响应模块 32G，用于响应系统预设函数；

[0278] 第二响应模块 32G 包括第二认证单元 32G-1 和第五判断单元 32G-2；

[0279] 第二认证单元 32G-1，用于认证解析得到的第一认证参数；

[0280] 第五判断单元 32G-2，用于判断是否成功认证第一认证参数。

[0281] 服务装置 32 包括验证模块 32H，用于验证智能密钥设备的序列号；

[0282] 验证模块 32H 包括第二接收单元 32H-1、第六判断单元 32H-2、第二显示单元 32H-3、第二获取单元 32H-4 和第七判断单元 32H-5；

[0283] 第二接收单元 32H-1，用于接收第二用户按键信息；

[0284] 第六判断单元 32H-2，用于根据第二用户按键信息判断用户按键类型；

[0285] 第二显示单元 32H-3，用于通过显示屏将模态框输出；

[0286] 第二获取单元 32H-4，用于获取智能密钥设备的序列号；

[0287] 第七判断单元 32H-5，用于判断获取得到的智能密钥设备的序列号与应用程序发送的智能密钥设备序列号是否相同。

[0288] 解码模块 32C 包括第八判断单元 32C-1、解码单元 32C-2、解密单元 32C-3、第二组合单元 32C-4、第一验证单元 32C-5、第三获取单元 32C-6 和第二验证单元 32C-7；

[0289] 第八判断单元 32C-1，用于判断标志位是否置位；

[0290] 解码单元 32C-2，用于对第一数据包进行解码；

[0291] 解密单元 32C-3，用于对解码结果进行解密；

[0292] 第二组合单元 32C-4，用于当所述解密单元解密成功时将解密得到的第一信息、第二信息和第三信息进行组合，得到待签名数据；

[0293] 第一验证单元 32C-5，用于验证用户输入的 PIN 码；

[0294] 第三获取单元 32C-6，用于从智能密钥设备中的证书中获取证书公钥和证书用户名；

[0295] 第二验证单元 32C-7，用于验证用户输入的证书用户名。

[0296] 第二接收单元 32H-1 还用于接收用户输入的 PIN 码。

[0297] 应用装置 32 还包括连接模块 32I，用于连接智能密钥设备。

[0298] 第二调用模块 32F 还用于以第二认证参数、保存的应用程序的地址字符串、智能密钥设备返回的信息和返回值为参数，调用系统预设函数，清除所述模态框。

[0299] 第一响应模块 31C 包括解析单元 31C-1、第一认证单元 31C-2 和第九判断单元 31C-3；

[0300] 解析单元 31C-1，用于当应用程序被系统预设函数调用时，解析系统预设函数的参数；

[0301] 第一认证单元 31C-2，用于认证第二认证参数；

[0302] 第九判断单元 31C-3，用于判断是否成功认证第二认证参数。

[0303] 应用装置 31 还包括显示模块 31G，用于显示签名结果或根据返回值显示相应错误信息。

[0304] 以上所述，仅为本发明较佳的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明公开的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应该以权利要求的保护范围为准。

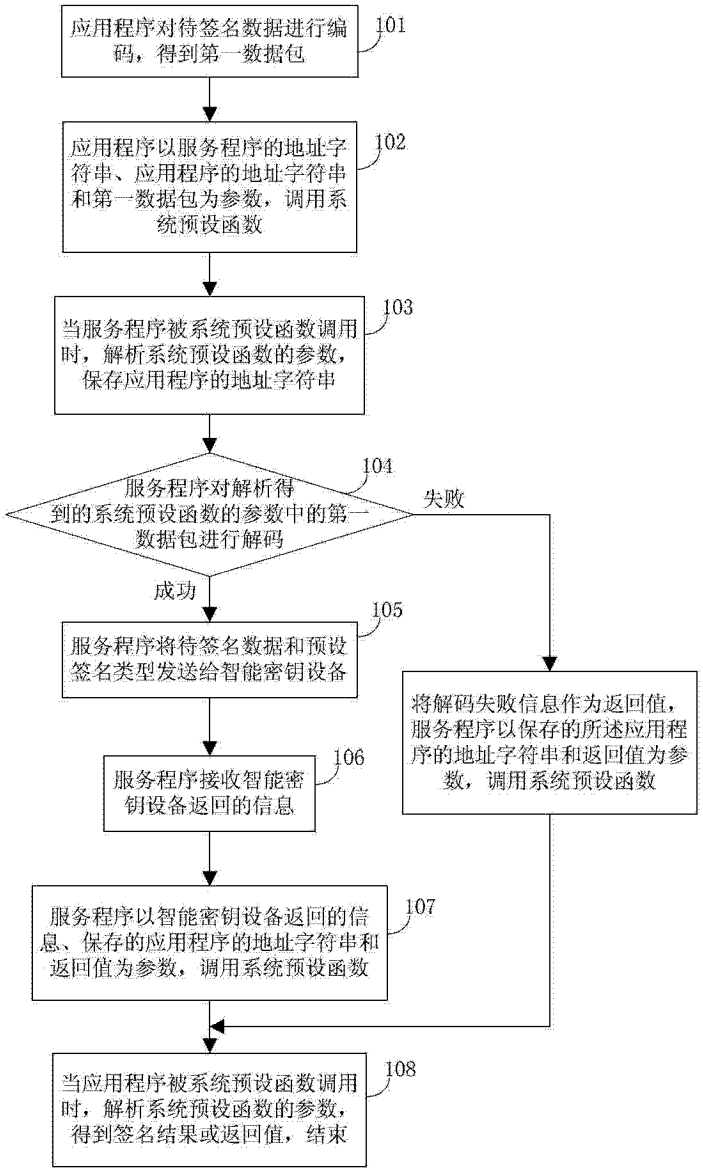

应用程序对待签名数据进行编码，得到第一数据包
101
应用程序以服务程序的地址字符串、应用程序的地址字符串和第一数据包为参数，调用系统预设函数
102
当服务程序被系统预设函数调用时，解析系统预设函数的参数，保存应用程序的地址字符串
103
服务程序对解析得到的系统预设函数的参数中的第一数据包进行解码
104
失败
成功
服务程序将待签名数据和预设签名类型发送给智能密钥设备
105
将解码失败信息作为返回值，服务程序以保存的所述应用程序的地址字符串和返回值为参数，调用系统预设函数
服务程序接收智能密钥设备返回的信息
106
服务程序以智能密钥设备返回的信息、保存的应用程序的地址字符串和返回值为参数，调用系统预设函数
107
当应用程序被系统预设函数调用时，解析系统预设函数的参数，得到签名结果或返回值，结束
108

图 1

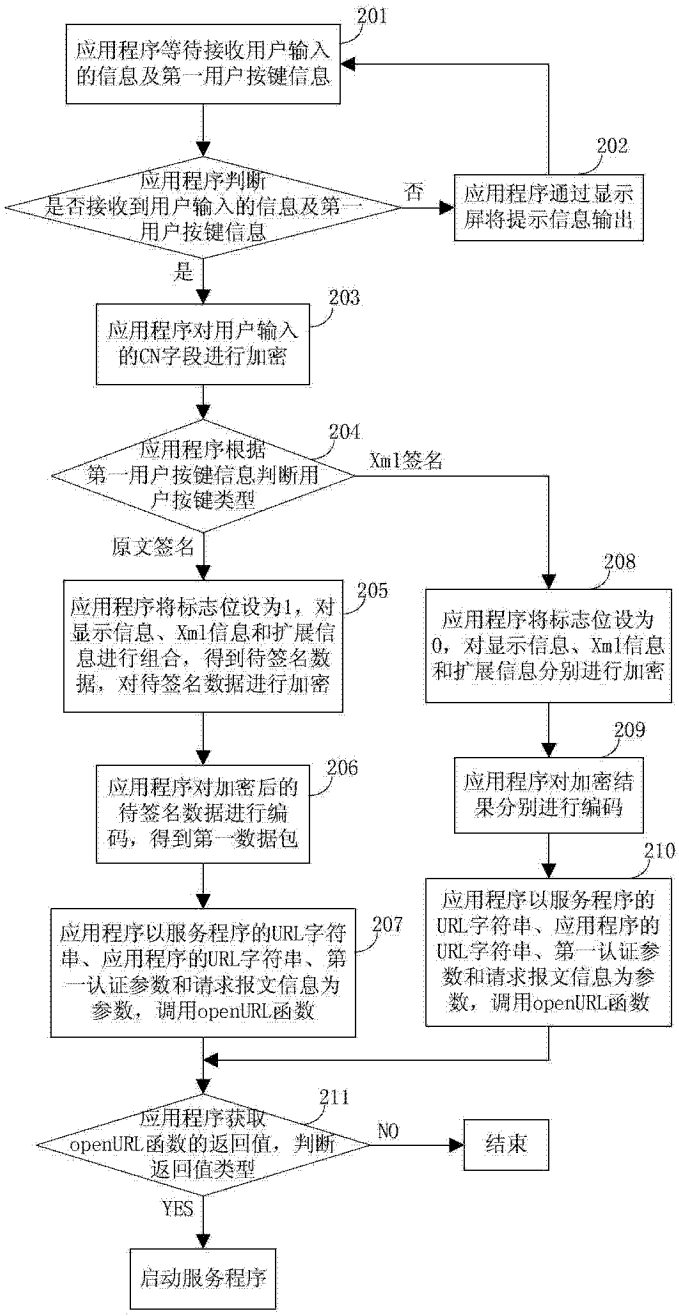

201
应用程序等待接收用户输入的信息及第一用户按键信息
应用程序判断是否接收到用户输入的信息及第一用户按键信息
否
202
应用程序通过显示屏将提示信息输出
是
203
应用程序对用户输入的CN字段进行加密
204
应用程序根据第一用户按键信息判断用户按键类型
Xml签名
原文签名
205
应用程序将标志位设为1，对显示信息、Xml信息和扩展信息进行组合，得到待签名数据，对待签名数据进行加密
208
应用程序将标志位设为0，对显示信息、Xml信息和扩展信息分别进行加密
209
应用程序对加密结果分别进行编码
206
应用程序对加密后的待签名数据进行编码，得到第一数据包
210
应用程序以服务程序的URL字符串、应用程序的URL字符串、第一认证参数和请求报文信息为参数，调用openURL函数
207
应用程序以服务程序的URL字符串、应用程序的URL字符串、第一认证参数和请求报文信息为参数，调用openURL函数
211
应用程序获取openURL函数的返回值，判断返回值类型
NO
结束
YES
启动服务程序

图 2

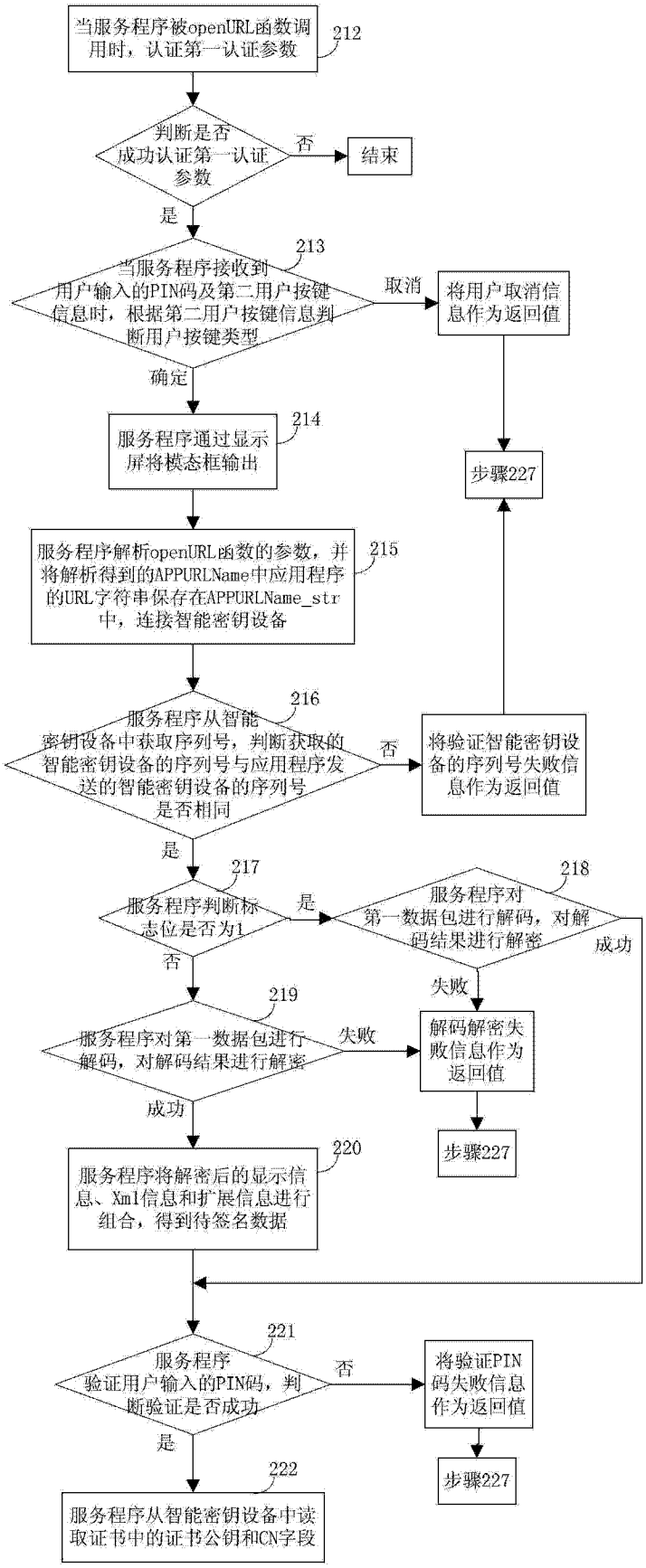

当服务程序被openURL函数调用时，认证第一认证参数
212
判断是否成功认证第一认证参数
否
结束
是
当服务程序接收到用户输入的PIN码及第二用户按键信息时，根据第二用户按键信息判断用户按键类型
213
取消
将用户取消信息作为返回值
确定
服务程序通过显示屏将模态框输出
214
步骤227
服务程序解析openURL函数的参数，并将解析得到的APPURLName中应用程序的URL字符串保存在APPURLName_str中，连接智能密钥设备
215
服务程序从智能密钥设备中获取序列号，判断获取的智能密钥设备的序列号与应用程序发送的智能密钥设备的序列号是否相同
216
否
将验证智能密钥设备的序列号失败信息作为返回值
是
服务程序判断标志位是否为1
217
是
服务程序对第一数据包进行解码，对解码结果进行解密
218
成功
失败
否
服务程序对第一数据包进行解码，对解码结果进行解密
219
失败
解码解密失败信息作为返回值
步骤227
成功
服务程序将解密后的显示信息、Xml信息和扩展信息进行组合，得到待签名数据
220
服务程序验证用户输入的PIN码，判断验证是否成功
221
否
将验证PIN码失败信息作为返回值
步骤227
是
服务程序从智能密钥设备中读取证书中的证书公钥和CN字段
222

图 3

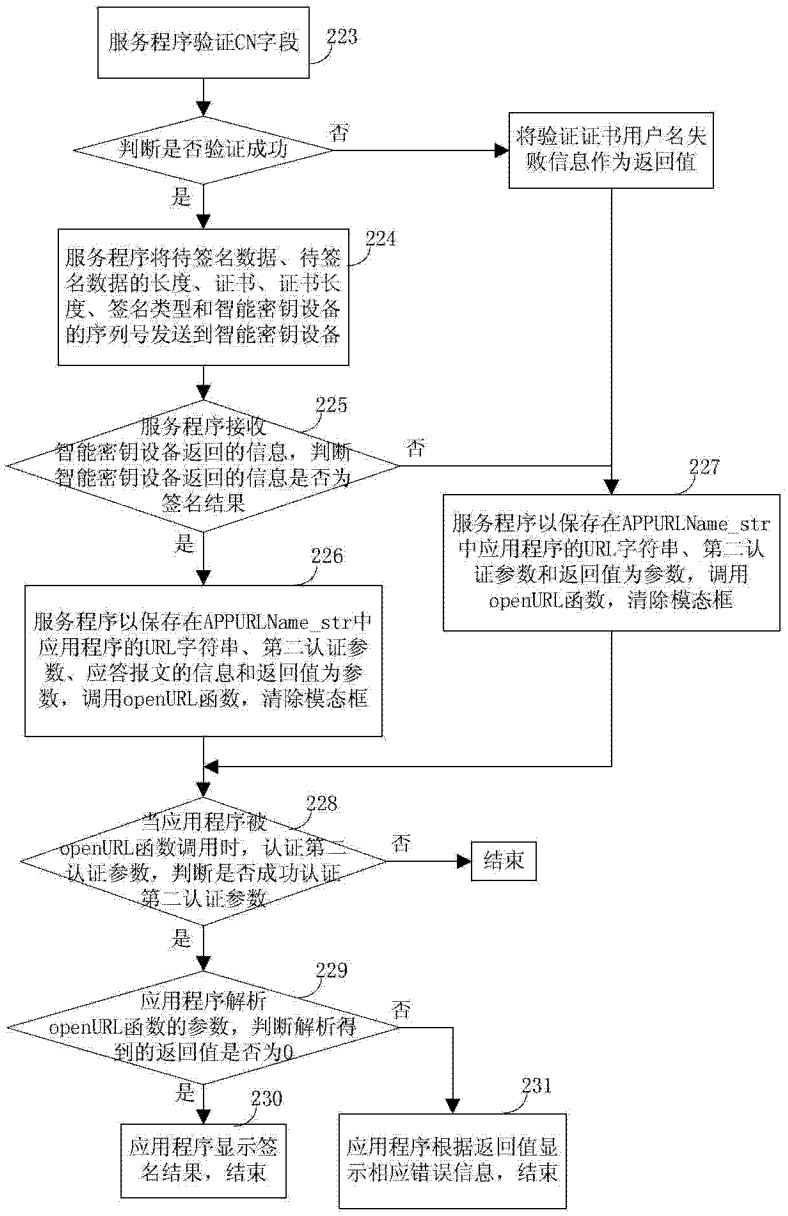

服务程序验证CN字段
223
判断是否验证成功
否
将验证证书用户名失败信息作为返回值
是
服务程序将待签名数据、待签名数据的长度、证书、证书长度、签名类型和智能密钥设备的序列号发送到智能密钥设备
224
服务程序接收智能密钥设备返回的信息，判断智能密钥设备返回的信息是否为签名结果
225
否
是
226
服务程序以保存在APPURLName_str中应用程序的URL字符串、第二认证参数、应答报文的信息和返回值为参数，调用openURL函数，清除模态框
227
服务程序以保存在APPURLName_str中应用程序的URL字符串、第二认证参数和返回值为参数，调用openURL函数，清除模态框
当应用程序被openURL函数调用时，认证第二认证参数，判断是否成功认证第二认证参数
228
否
结束
是
应用程序解析openURL函数的参数，判断解析得到的返回值是否为0
229
否
是
230
应用程序显示签名结果，结束
231
应用程序根据返回值显示相应错误信息，结束

图 4

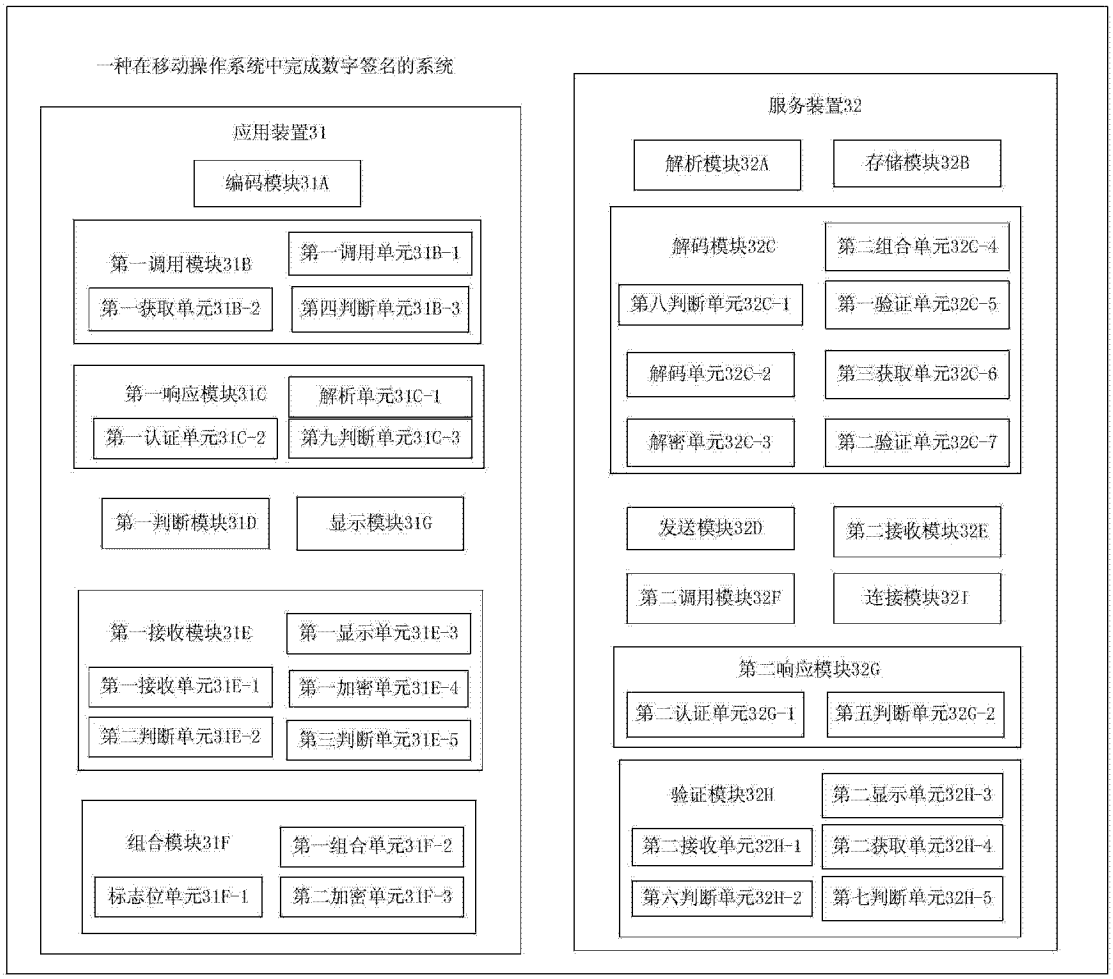

一种在移动操作系统中完成数字签名的系统
应用装置31
编码模块31A
第一调用模块31B
第一调用单元31B-1
第一获取单元31B-2
第四判断单元31B-3
第一响应模块31C
解析单元31C-1
第一认证单元31C-2
第九判断单元31C-3
第一判断模块31D
显示模块31G
第一接收模块31E
第一显示单元31E-3
第一接收单元31E-1
第一加密单元31E-4
第二判断单元31E-2
第三判断单元31E-5
组合模块31F
第一组合单元31F-2
标志位单元31F-1
第二加密单元31F-3
服务装置32
解析模块32A
存储模块32B
解码模块32C
第二组合单元32C-4
第八判断单元32C-1
第一验证单元32C-5
解码单元32C-2
第三获取单元32C-6
解密单元32C-3
第二验证单元32C-7
发送模块32D
第二接收模块32E
第二调用模块32F
连接模块32I
第二响应模块32G
第二认证单元32G-1
第五判断单元32G-2
验证模块32H
第二显示单元32H-3
第二接收单元32H-1
第二获取单元32H-4
第六判断单元32H-2
第七判断单元32H-5

图 5