[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04W 12/02 (2009.01)
H04W 12/06 (2009.01)
H04B 5/00 (2006.01)
H04W 88/02 (2009.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910021006.6

[43] 公开日 2009 年 7 月 8 日

[11] 公开号 CN 101478749A

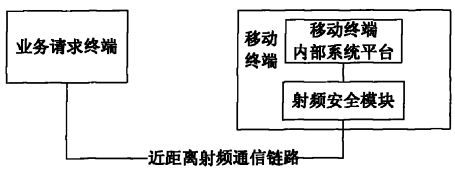
[22] 申请日 2009.1.21
[21] 申请号 200910021006.6
[71] 申请人 陕西海基业高科技实业有限公司
地址 710075 陕西省西安市高新一路 5 号正信大厦 B1306 室
[72] 发明人 李 晖 肖成生 芦文峰 吕 萌 肖 杰
[74] 专利代理机构 陕西电子工业专利中心
代理人 王品华
权利要求书 2 页 说明书 6 页 附图 2 页

[54] 发明名称

一种近距离射频通信的安全服务系统及方法

[57] 摘要

本发明公开了一种近距离射频通信的安全服务系统与方法，该系统包括业务请求终端、移动终端和射频安全模块。 用户通过业务请求终端生成业务信息，并通过近距离射频通信链路将业务信息发送给移动终端上的射频安全模块；射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对所显示的信息验证无误后从移动终端的键盘输入确认信息，射频安全模块捕获该确认信息后对业务信息进行数字签名和/或加解密等安全服务，并将安全服务产生的信息封装为应答信息，通过近距离射频通信链路发送业务请求终端；业务请求终端从应答信息中获得安全服务结果进行后续处理。 本发明具有安全可靠，操作简便之优点，特别适于电子交易和银行金融业务使用。



1. 一种近距离射频通信安全服务系统，包括：

业务请求终端，用于生成用户业务信息，将业务信息通过近距离射频通信发送到射频安全模块，并接收来自射频安全模块的应答信息；

移动终端，用于装载射频安全模块，显示业务信息，并获取用户确认信息传递给射频安全模块；

射频安全模块，用于接收业务信息，在移动终端弹出显示业务信息，对用户确认后的信息根据业务信息类型进行数字签名或加解密或数字签名和加解密处理，并将处理结果封装为应答信息通过近距离射频通信发送回业务请求终端。

2. 根据权利要求 1 所述的安全服务系统，其特征在于业务请求终端通过近距离射频通信链路与射频安全模块连接；射频安全模块通过用户识别卡接口或 SD 卡接口或 Mini SD 卡接口或 USB 接口与移动终端连接。

3. 根据权利要求 1 所述的安全服务系统，其特征在于射频安全模块由微处理器，射频电路组成，两者之间通过数据总线连接，并封装为薄膜器件。

4. 根据权利要求 3 所述的安全服务系统，其特征在于薄膜器件附接在用户识别卡和移动终端内部系统平台之间，移动终端内部系统平台通过该薄膜器件与用户识别卡连接。

5. 根据权利要求 1 所述的安全服务系统，其特征在于射频安全模块进一步封装为标准 IC 芯片，置于移动终端内，通过数据总线接口与移动终端连接。

6. 根据权利要求 5 所述的安全服务系统，其特征在于封装为 IC 芯片卡的射频安全模块，插在支持一机多卡的移动终端的用户识别卡座上，该用户识别卡对于 GSM 手机为 SIM 卡，对于 CDMA 手机为 UIM 卡，对于 3G 手机则为 USIM 卡。

7. 一种近距离射频通信的安全服务方法，包括如下步骤：

（1）用户通过业务请求终端生成业务信息，发送至射频安全模块；

（2） 射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行数字签名和加解密，并将数字签名和加解密产生的信息封装为应答信息，发送给业务请求终端；

（3） 业务请求终端根据业务类型从应答信息中获得数字签名和加解密后的信息

进行后续处理。

8．一种近距离射频通信的安全服务方法，包括如下步骤：

a. 用户通过业务请求终端生成业务信息，发送至射频安全模块；

b. 射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行业务信息进行数字签名，并将数字签名产生的信息封装为应答信息，发送给业务请求终端；

c. 业务请求终端根据业务类型从应答信息中获得数字签名后的信息进行后续处理。

9．一种近距离射频通信的安全服务方法，包括如下步骤：

（a）用户通过业务请求终端生成业务信息，发送至射频安全模块；

（b）射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行加解密，并将加解密产生的信息封装为应答信息，发送给业务请求终端；

（c）业务请求终端根据业务类型从应答信息中获得加解密后的信息进行后续处理。

一种近距离射频通信的安全服务系统及方法

技术领域

本发明属于通信技术领域，涉及一种对用户所请求业务信息进行安全服务的系统与方法，可用于金融、保险、电子商务、远程交易领域的安全信息传递。

背景技术

网上远程服务安全认证系统主要采用PC机程序或USBKEY对用户提交的业务信息进行数字签名和加密操作。目前针对PC机的攻击层出不穷，USBKEY虽然安全性较PC机高，但只能确保证书不被盗取，并不能阻挡黑客伪造文件骗取其签名，因而难以防止高水平的黑客及黑客程序的攻击。近来一种木马开始流行，在USBKEY签名之前修改请求信息，由于用户无法察觉请求信息被篡改，极易造成交易的混乱与纠纷。于是有些USBKEY中加入了液晶显示模块，将请求信息显示在液晶屏上，供用户查看核对，但这种方法的缺点是不够人性化、显示界面窄小、功能单一。

随着移动通信技术的发展，手机已经成为使用最广泛的通信方式。目前手机用户已经超过固定电话用户，成为用户数最大的一种通信及信息处理平台，利用手机这一平台开发各种信息应用已经成为一种潮流和趋势。目前针对手机的信息服务应用主要包括语音服务、短消息服务和各类数据业务服务如WAP、GPRS等。在数据业务需要认证签名时，通常是将证书下载到手机平台，同时还要装载适配及签名认证程序。由于手机有多种操作系统平台，各种手机所装操作系统都不尽相同，因而在实际应用中上述方式很难推广，几乎不被市场接受。同时还有一个重要原因就是证书放在手机平台上是不安全的，因为手机也有病毒及黑客程序。还有一种方式是通过手机上的用户身份识别模块或用户识别卡的STK功能完成签名，例如中国知识产权局公开的200510048881.5专利申请，这种签名方式的突出缺陷是在现实运营和管理中均无法实现，因为目前移动运营商提供的用户识别卡不具有加密和签名认证等安全功能，如果要使用用户必须首先换卡，而目前的用户识别卡由运营商所垄断，每一种应用及其升级都必须得到运营商的配合，所以这在现实中几乎是不可操作的。

发明内容

本发明的目的在于避免上述现有服务系统存在的缺陷，提供一种近距离射频通信的安全服务系统及方法，将移动终端与一射频安全模块绑定，由移动终端内部系统平台显示用户请求的业务信息，经用户输入确认信息后，再由射频安全模块进行数字签名和/或加解密安全服务，实现业务的安全性和操作的便捷性。

为实现上述目的，本发明的安全服务系统包括：

业务请求终端，用于生成用户业务信息，将业务信息通过近距离射频通信发送到射频安全模块，并接收来自射频安全模块的应答信息；

移动终端，用于装载射频安全模块，显示业务信息，并获取用户确认信息传递给射频安全模块；

射频安全模块，用于接收业务信息，在移动终端弹出显示业务信息，对用户确认后的信息根据业务信息类型进行数字签名或加解密或数字签名和加解密处理，并将处理结果封装为应答信息通过近距离射频通信发送回业务请求终端；

业务请求终端通过近距离射频通信链路与射频安全模块连接。

上述系统中射频安全模块通过用户识别卡接口或 **SD** 卡接口或 **Mini SD** 卡接口或 **USB** 接口与移动终端连接。

当射频安全模块与移动终端通过用户识别卡接口连接时，所述射频安全模块可封装为薄膜器件附接在用户识别卡上，移动终端内部系统平台通过薄膜器件与用户识别卡连接；该用户识别卡对于 GSM 手机为 SIM 卡，对于 CDMA 手机为 UIM 卡，对于 3G 手机则为 USIM 卡；当射频安全模块封装为 IC 芯片卡时，插接在支持一机多卡的移动终端的用户识别卡座上；射频安全模块也能进一步封装为标准 IC 芯片，置于移动终端内，通过数据总线接口与移动终端连接。

为实现上述目的，本发明的安全服务方法有 3 种方案：

第一种安全服务方法方法，包括如下步骤：

（1）用户通过业务请求终端生成业务信息，发送至射频安全模块；

（2） 射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行数字签名和加解密，并将数字签名和加解密产生的信息封装为应答信息，发送给业务请求终端；

（3） 业务请求终端根据业务类型从应答信息中获得数字签名和加解密后的信息

进行后续处理。

第二种安全服务方法方法，包括如下步骤：

a. 用户通过业务请求终端生成业务信息，发送至射频安全模块；

b. 射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行业务信息进行数字签名，并将数字签名产生的信息封装为应答信息，发送给业务请求终端；

c. 业务请求终端根据业务类型从应答信息中获得数字签名后的信息进行后续处理。

第三种安全服务方法方法，包括如下步骤：

（**a**）用户通过业务请求终端生成业务信息，发送至射频安全模块；

（**b**）射频安全模块在移动终端显示屏幕上自动弹出窗口显示业务信息，用户对该显示的信息验证无误后输入确认信息，射频安全模块对获取确认后的业务信息进行加解密，并将加解密产生的信息封装为应答信息，发送给业务请求终端；

（**c**）业务请求终端根据业务类型从应答信息中获得加解密后的信息进行后续处理。

本发明的系统由于采用射频安全模块，不仅能完成传统的 USBKEY 对业务信息签名的功能，而且能够与手机绑定，使用户很方便的查看业务内容是否数字签名和加解密被篡改，确保业务信息的安全性；同时由于本发明的移动终端使用数字签名和加解密或数字签名或加解安全服务对业务信息进行确认，不仅克服了现有服务系统中存在的安全风险，同时保证了业务请求来源的真实性和完整性，使得出现纠纷时，界定责任明确，便于得到法律支持；此外由于本发明将业务信息显示在移动终端屏幕上，当用户确认信息无误后再进行安全服务，因而能够有效防止木马程序篡改业务信息而不被察觉的情况。

附图说明

图 **1** 是本发明的近距离射频通信安全服务系统示意图；

图 2 是本发明系统采用的射频安全模块框图；

图 **3** 是本发明的安全服务方法流程图。

具体实施方式

下面给出射频安全模块通过用户识别卡接口与移动终端连接的实施例。

参照图 1，本发明的基于移动终端和近距离射频通信的安全服务系统主要由业务请求终端，移动终端和射频安全模块组成。其中：

业务请求终端，通过接口与射频转换装置连接，该接口包括但不限于 USB、蓝牙、红外和串行口；

射频安全模块，装载在移动终端内，该射频安全模块的结构如图 2 所示，它是由由微处理器，射频电路组成，微处理器中存储有签名、验证，加密、解密的密钥和相关程序，并设有公钥运算协处理器，以完成在业务信息的签名、验证，加密和解密处理等安全服务过程中的相关运算。微处理器与射频电路两者之间通过数据总线连接，并封装为薄膜器件，该薄膜器件与用户识别卡插接为一体，一面通过用户识别卡接口与移动终端内部系统平台连接，另一面与用户识别卡连接。

射频安全模块能进一步封装为标准 IC 芯片与移动终端通过接口连接，该接口为 SD 卡接口或 Mini SD 卡接口或 USB 接口，即当移动终端提供 SD 卡接口时，则射频安全模块通过 SD 卡接口与移动终端连接；当移动终端提供 Mini SD 卡接口时，则射频安全模块通过 Mini SD 卡接口与移动终端连接；当移动终端提供 USB 接口时，则射频安全模块通过 USB 接口与移动终端连接。此外，该射频安全模块也能够直接与移动终端系统平台进行通信，并且利用移动终端内部系统平台提供的用户识别卡扩展应用功能在移动终端中增加应用程序，例如提供 STK 扩展程序，完成对移动终端系统平台收发短消息的加密、解密、签名和签名验证。

工作时，首先由业务请求终端生成用户业务信息，并将业务信息通过近距离射频通信链路发送至射频安全模块，射频安全模块接收该业务信息并将其显示在移动终端上，待用户确认后，根据业务信息类型进行数字签名或加解密或数字签名和加解密处理，并将处理结果封装为应答信息通过近距离射频通信链路发送回业务请求终端。例如业务信息类型要求加解密时，则射频安全模块对业务信息进行加解密处理，并将该加解密的结果封装为应答信息通过近距离射频通信链路发送回业务请求终端；又如业务信息类型要求数字签名和加解密时，则射频安全模块对业务信息先进行数字签名，再进行加解密处理，并将该数字签名和加解密结果封装为应答信息通过近距离射频通信链路发送回业务请求终端。

参照图 3，本发明的安全处理方法有以下三种实例：

实例 1，本发明的安全处理方法，包括：

步骤 A，用户在终端上输入个人信息和业务请求内容，业务请求终端根据获取

用户输入的信息生成格式化的业务信息，并且在业务信息中包含业务类型字段，业务类型要求的安全服务包括但不限于数字签名、加解密、数字签名和加解密。

步骤 B，业务信息生成后，经近距离射频通信链路发送至射频安全模块。

步骤 C，射频安全模块捕获业务信息后，自动将该业务信息显示在移动终端上，由用户对其进行核对，待用户确认该业务信息无误后，在移动终端上通过按确认键输入确认信息；移动终端内部系统平台将确认信息传递给射频安全模块，射频安全获得该确认信息后，按照业务类型所要求的数字签名和加解密服务，对其业务信息先进行数字签名后再进行加解密，并将该处理结果封装为应答信息。

步骤 D，应答信息经近距离射频通信链路发送至业务请求终端。

步骤 E，业务请求终端从应答信息中获得数字签名和加解密结果进行后续处理。

实例 2，本发明的安全处理方法，包括

步骤一，用户在终端上输入个人信息和业务请求内容，业务请求终端根据获取用户输入的信息生成格式化的业务信息，并且在业务信息中包含业务类型字段，业务类型要求的安全服务包括但不限于数字签名、加解密、数字签名和加解密。

步骤二，业务信息生成后，经近距离射频通信链路发送至射频安全模块。

步骤三，射频安全模块捕获业务信息后，自动将该业务信息显示在移动终端上，由用户对其进行核对，待用户确认该业务信息无误后，在移动终端上通过按确认键输入确认信息；移动终端内部系统平台将确认信息传递给射频安全模块，射频安全获得该确认信息后，按照业务类型所要求的数字签名服务，对其业务信息进行数字签名，并将该数字签名封装为应答信息。

步骤四，应答信息经近距离射频通信链路发送至业务请求终端。

步骤五，业务请求终端从应答信息中获得数字签名进行后续处理。

实例 3，本发明的安全处理方法，包括

步骤 1，用户在终端上输入个人信息和业务请求内容，业务请求终端根据获取用户输入的信息生成格式化的业务信息，并且在业务信息中包含业务类型字段，业务类型要求的安全服务包括但不限于数字签名、加解密、数字签名和加解密。

步骤 2，业务信息生成后，经近距离射频通信链路发送至射频安全模块。

步骤 3，射频安全模块捕获业务信息后，自动将该业务信息显示在移动终端上，由用户对其进行核对，待用户确认该业务信息无误后，在移动终端上通过按确认键输入确认信息；移动终端内部系统平台将确认信息传递给射频安全模块，射频安全

获得该确认信息后，按照业务类型所要求的加解密服务，对其业务信息进行加解密，并将该密/明文封装为应答信息。

步骤 **4**，应答信息经近距离射频通信链路发送至业务请求终端。

步骤 **5**，业务请求终端从应答信息中获得加解密的结果进行后续处理。

本发明业务请求终端通过近距离射频通信方式将业务请求信息显示在用户的移动终端上，有效防止了木马篡改业务信息而不被用户察觉的情况，使安全服务较使用传统 **USB Key** 更加安全且使用方便。

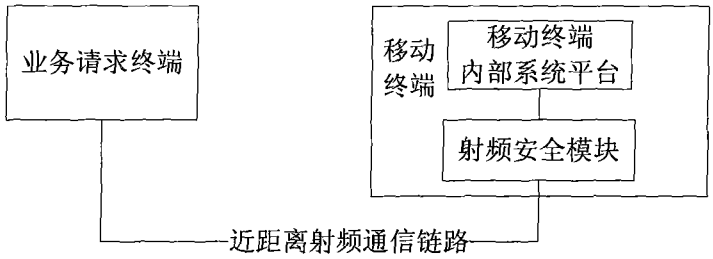

业务请求终端
移动终端
移动终端内部系统平台
射频安全模块
近距离射频通信链路

图 1

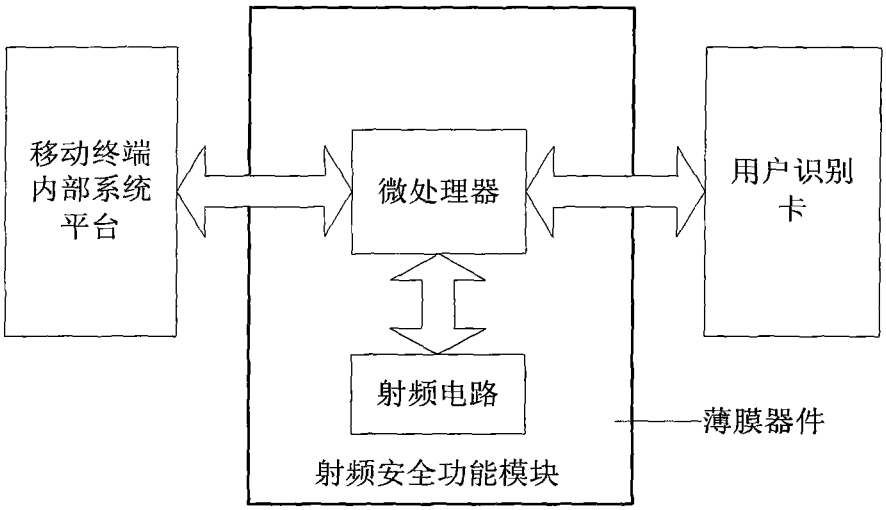

移动终端内部系统平台
微处理器
用户识别卡
射频电路
薄膜器件
射频安全功能模块

图 2

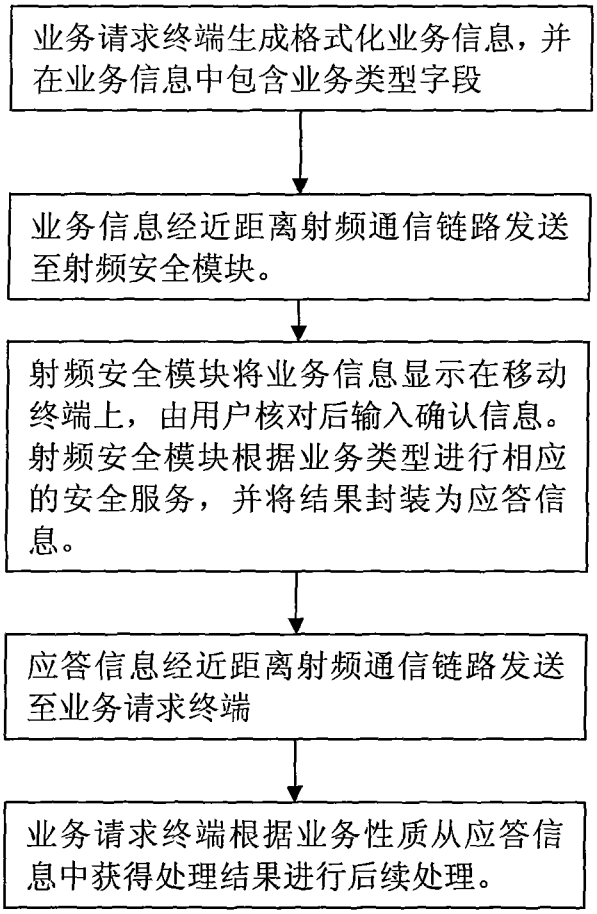

业务请求终端生成格式化业务信息，并在业务信息中包含业务类型字段
业务信息经近距离射频通信链路发送至射频安全模块。
射频安全模块将业务信息显示在移动终端上，由用户核对后输入确认信息。射频安全模块根据业务类型进行相应的安全服务，并将结果封装为应答信息。
应答信息经近距离射频通信链路发送至业务请求终端
业务请求终端根据业务性质从应答信息中获得处理结果进行后续处理。

图 3