(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 106408314 A
(43)申请公布日 2017.02.15

(21)申请号 201610857913.4

(22)申请日 2016.09.28

(71)申请人 北京飞凡士科技有限公司
地址 100022 北京市朝阳区广渠路39号院2号楼二层(双井孵化器1022号)

(72)发明人 党凡 文庆福 周鹏飞 姜世琦

(51)Int.Cl.
G06Q 30/00(2012.01)
G06K 17/00(2006.01)

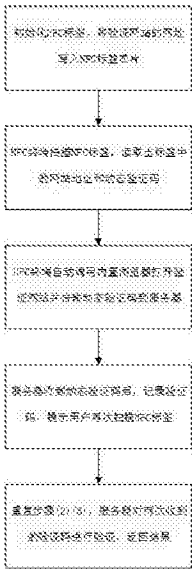
权利要求书1页 说明书2页 附图1页

(54)发明名称

一种基于NFC技术的商品防伪方法

(57)摘要

本发明提出一种新的基于NFC技术的商品防伪方法,该方法包括以下步骤:(1) 初始化NFC标签,将验证网站的网址写入NFC标签芯片;(2) NFC终端扫描NFC标签,读取出标签中的网站地址和动态验证码;(3) NFC终端自动调用内置浏览器打开验证网站并传输动态验证码到服务器;(4) 服务器收到动态验证码后,记录验证码,提示用户再次扫描NFC标签;(5) 重复步骤(2)(3),服务器收到第二次发送的动态验证码,对两次收到的验证码进行验证,在浏览器上显示验证结果。与现有防伪方法相比,一方面不需要在终端安装任何额外的软件,另一方面双重验证机制可以有效解决NFC标签中验证信息被复制的问题。



CN 106408314 A

1.一种基于NFC技术的商品防伪方法，其特征在于包括以下几个步骤：

初始化NFC标签，将验证网站的网址写入NFC标签芯片；

NFC终端靠近扫描NFC标签，当NFC终端感应到标签时，读取出NFC标签中的内容，包括步骤(1)写入的验证网站地址和读取时标签生成的动态验证码，动态验证码将附在网址后面，作为URL的一部分；

NFC终端读取到包括验证网站地址和动态验证码的URL后，操作系统会直接启动内置浏览器，并打开该网址进入到验证网站，同时将动态验证码以URL参数的形式传输到服务器；

服务器收到终端浏览器所发送的动态验证码后，记录验证码，根据验证信息在终端的浏览器上显示对应商品的信息，同时并提示用户再次扫描NFC标签完成真伪验证；

当用户再次扫描NFC标签，重复步骤(2)(3)，服务器收到第二次发送的动态验证码，对两次收到的验证码进行验证，在终端浏览器上显示验证结果。

2.如权利要求1所述的基于NFC技术的商品防伪方法，其特征在于：

所属步骤(2)中，NFC终端靠近扫描NFC标签，当NFC终端感应到标签时，读取出NFC标签中的内容，包括步骤(1)写入的验证网站地址和读取时标签生成的动态验证码，动态验证码将附在网址后面，作为URL的一部分。

3.如权利要求1所述的基于NFC技术的商品防伪方法，其特征在于：

所述步骤(3)中，当NFC终端读取到包括验证网站地址和动态验证码的URL后，操作系统会直接启动内置浏览器，并打开该网址进入到验证网站，同时将动态验证码以URL参数的形式传输到服务器。

4.如权利要求1所述的基于NFC技术的商品防伪方法，其特征在于：

所述步骤(4)中，服务器收到终端浏览器所发送的动态验证码后，记录验证码，根据验证信息在终端的浏览器上显示对应商品的信息，同时并提示用户再次扫描NFC标签完成真伪验证。

5.如权利要求1所述的基于NFC技术的商品防伪方法，其特征在于：

所述步骤(5)中，当用户再次扫描NFC标签，重复步骤(2)(3)，服务器收到第二次发送的动态验证码，对两次收到的验证码进行验证，在终端浏览器上显示验证结果。

一种基于NFC技术的商品防伪方法

技术领域

[0001] 本发明涉及商品防伪技术领域，特别涉及一种基于NFC技术的商品防伪方法。

背景技术

[0002] 近场通信(Near Field Communication, NFC)技术是一种短距离的高频无线通信技术，允许电子设备之间(在10厘米内)进行非接触式数据传输。这个技术由射频识别(RFID)发展而来，最早由飞利浦半导体(现恩智浦半导体)、诺基亚和索尼共同开发而成。这一技术的一种典型应用是商品的防伪验证。首先，我们预先将商品的验证信息写入到NFC标签中并将标签附在商品上。在验证阶段，采用NFC智能终端(如手机)扫描商品上的NFC标签，读取出其中内容并验证真伪。

[0003] 目前，基于NFC技术的防伪方法一般做法是，首先将验证信息写入到NFC标签中，然后NFC终端上预装好一个应用软件，当用NFC终端扫描标签，应用软件就可以读取出标签中的验证信息，软件就可以在终端上验证信息真伪或是将信息发给远端服务器进行验证真伪，最终将验证结果呈现出来。

[0004] 授权公开号为CN104320250A的专利申请文件中，提出了一种基于NFC芯片的防伪认证方法，不需要在终端上安装应用软件，直接采用内置浏览器将信息发送给远端服务器进行验证，最终呈现验证结果。但是这一方法存在不足，尽管验证信息是动态生成的，但验证信息可以被终端读取出来后写入到其他芯片，造成合法数据外泄，从而进行大规模复制。

发明内容

[0005] 为了解决上述方法存在的技术问题，本发明提出一种基于NFC技术的商品防伪方法，采用双重验证机制来避免验证信息可以被复制的问题。为了实现上述发明目的，本发明采用下述技术方案：

一种基于NFC技术的商品防伪方法，包括以下步骤：

(1)初始化NFC标签，将验证网站的网址写入NFC标签芯片；

(2)NFC终端靠近扫描NFC标签，当NFC终端感应到标签时，读取出NFC标签中的内容，包括步骤1写入的验证网站地址和读取时标签生成的动态验证码，动态验证码将附在网址后面，作为URL的一部分；(3)NFC终端读取到包括验证网站地址和动态验证码的URL后，操作系统会直接启动内置浏览器，并打开该网址进入到验证网站，同时将动态验证码以URL参数的形式传输到服务器；

(4)服务器收到终端浏览器所发送的动态验证码后，记录验证码，根据验证信息在终端的浏览器上显示对应商品的信息，同时并提示用户再次扫描NFC标签完成真伪验证；

(5)当用户再次扫描NFC标签，重复步骤2和步骤3，服务器收到第二次发送的动态验证码，对两次收到的验证码进行验证，在终端浏览器上显示验证结果。

[0006] 与现有基于NFC技术的防伪方法相比，一方面本发明不需要再终端安装任何额外的软件，另一方面双重验证机制可以有效解决NFC标签中验证信息被复制的问题，防止伪

造。

附图说明

[0007] 图1是本发明所提出的防伪方法流程图。

具体实施方式

[0008] 下面结合附图对本发明的技术内容作进一步说明。

[0009] 图1所示的是本发明所提出的商品防伪方法的流程图，该方法包括以下几个步骤：

1.初始化NFC标签，将验证网站的网址写入NFC标签芯片。

[0010] 2.使用NFC终端靠近扫描NFC标签，当NFC终端感应到标签时，会读取出NFC标签中的内容，包括步骤1写入的验证网站地址和读取时标签生成的动态验证码，动态验证码将附在网址后面，作为URL的一部分。这里的动态验证码由芯片的序列号、加密的随机数、芯片被读取次数以及前面三者的加密校验值四部分构成。每一次读取后，芯片中的随机数生成模块和加密模块就会重新生成随机数和加密，更新动态验证码。

[0011] 3.当NFC终端读取出验证网站地址和动态验证码时，NFC终端会自动调用内置浏览器打开验证网站并将动态验证码发送到远端服务器，用以信息验证真伪。

[0012] NFC终端读取到验证网站地址和动态验证码后，判断收到的数据类型，如果数据类型是网址类型，NFC终端的操作系统会直接启动内置浏览器，并打开该网址进入到验证网站，同时将动态验证码以URL中参数的形式传输到服务器。

[0013] 4.服务器收到终端浏览器所发送的动态验证码后，记录验证码，根据验证信息在终端的浏览器上显示对应商品的信息，同时提示用户再次扫描NFC标签完成真伪验证。

[0014] 5.当用户再次扫描NFC标签，重复步骤2和步骤3，服务器收到第二次发送的动态验证码，对两次收到的验证码进行验证，在终端浏览器上显示验证结果。

[0015] 第一次扫描NFC标签后，NFC标签会重新生成新的动态验证码，再次扫描NFC标签，读取动态验证码发送到服务器，将两次的验证码一并进行真伪验证。如果只扫描一次NFC标签，NFC标签中的验证网址和有效的动态验证码可以被复制写入到其他NFC标签，无法区分真伪标签。采用双重验证机制，可以避免NFC标签中的数据被复制，防止伪造。

[0016] 最后应说明的是，以上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精神和范围。

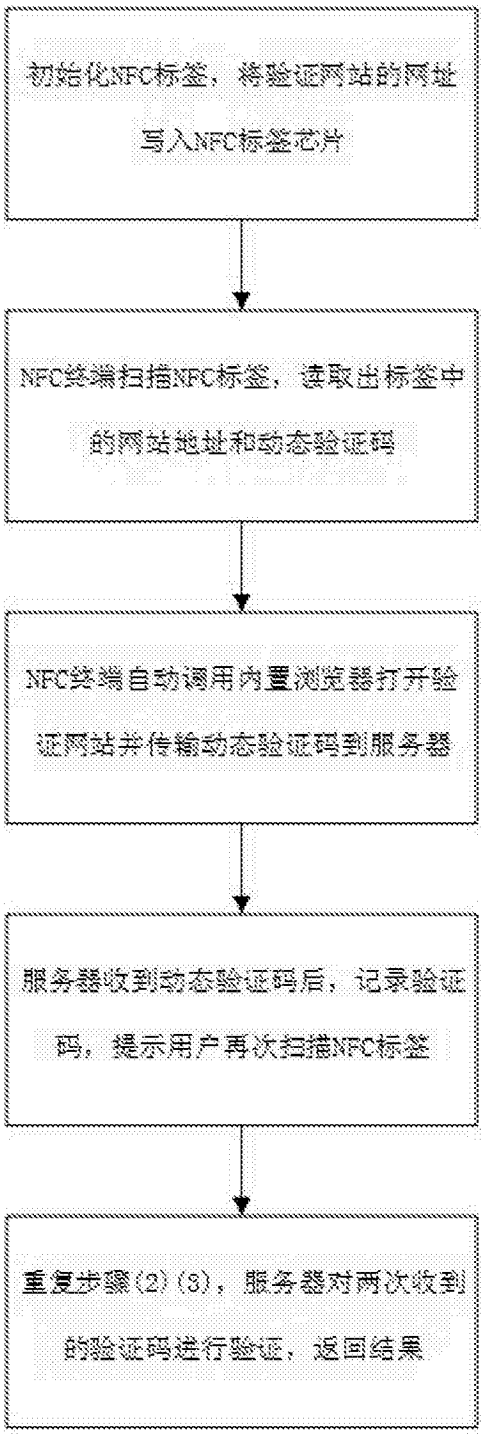

初始化NFC标签，将验证网站的网址写入NFC标签芯片
NFC终端扫描NFC标签，读取出标签中的网站地址和动态验证码
NFC终端自动调用内置浏览器打开验证网站并传输动态验证码到服务器
服务器收到动态验证码后，记录验证码，提示用户再次扫描NFC标签
重复步骤(2)(3)，服务器对两次收到的验证码进行验证，返回结果

图 1