**CPK防伪标签**

南湘浩

纸质防伪标签的防伪功能与RFID防伪标签大致相同，当然RFID标签具有防复制功能，而纸质标签则不具有。但如果能容易识别被复制的标签，同样可以达到防伪的目的。

在物流中，发货方和收货方之间形成虚拟防伪网络，货物的真伪由发货方负责，真伪检验则有收货方负责。

防伪的范围很大，要求也千差万别。因此，防伪是永远研究下去的题目。实际上，信息安全的核心是真伪识别，物体的真伪识别称防伪控制，通信地址的真伪识别，称接入控制，数据的真伪识别，称数据保护，软件的真伪识别，称可证操作，等等。虽然识别的方面不同，叫法也不同，但是其工作原理是相同的。

在纸质防伪网络中，采用竖向证明链和横向正明链形成防伪的虚拟网络。

**1 防伪的竖向证明链**

纸质防伪标签的最大弱点是容易复制，因此，怎样防止复制作案是纸质标签的主要任务。

一个商品在流通中形成多层购销环节，在各个环节之间可以互相制约构成竖向证明链。以发货方（第一层）和零售方（第二层）两层结构为例：

第一层防伪标签是：

发货方(supplier)提供发货方标识真实性证明和货物真实性证明。

发货方真实性证明是；

SIG*supplier*(time)=(*s*1,*c*1)

货物真实性证明是：

SIG*supplier*(chr)=(*s*2, *c*2)

其中，chr是货物特性。

第二层防伪标签是：

如果在批发市场的收货者变为零售市场的售货者(seller)，那么必须追加自己的真实性证明:

SIG*seller*(time)=(*s*1,*c*1)

再提供货物真实性证明：

SIG*seller*(chr)=(*s*2,*c*2)

于是在交易的各环节中形成真实性的证明链，如发货者证明和售货者证明之间形成竖向证明链。

因为所有证明是用数字签名实现的，标签具有溯源性和不可抵赖性。

**2 防伪的横向证明链**

在购销环节中，除了防伪标签之外，还形成价格标签、收据等。如果在各中标签之间建立互相制约的逻辑联系，那么可以建立横向的证明链。在商场标价标签和防伪标签之间形成互证关系， 在防伪标签和开具的收据（发票）之间又形成一层互证关系。

为了在各种标签和票据之间建立互相制约的逻辑关系，需要规范各种标签和票据的要素。

**2.1 标价标签要素**

各商场出售的商品都已贴有明码标价的标签，要素也定义清楚了。因此，在这种请款下只增加真实性证明即可。其要素应包括：

商场名：实名

商场名真实性证明：签名时间，签名码

物品名：实名

单价： xx元

物品名、单价真实性证明：签名码

注：CPK是基于标识的公钥体制，因此商场名真实性证明和物品名真实性证明是等价的，其中，商场真实性证明只用于有“事前鉴别”需求的场合，如果没有事前鉴别的需要，则可以省略，将上述要素可简化为：

商场名：

物品名：

商家对物品名的签名。

**2.2 收据要素**

各商场在收款后都打出收据。收据要素的设计要达到两个目的：第一是为了建立与防伪的逻辑关系，第二是考虑到收据的法律地位，使得收据能够起到发票的作用。其要素包括：

商场名：签名时间，签名码

物品名，数量，金额：签名码

注：同样，将上述要素可简化为：

商场名：

物品名：

商家对物品名的签名。

**2.3 防伪标签要素**

防伪标签要素，与其他标签雷同。

厂家名：签名时间，签名码

物品名：签名码

注：同样将上述要素简化为：

商场名：

物品名：

商家对物品名的签名。

防伪标签提供二维码，对准二维码即可验证：

**2.4 防伪验证显示**

如果签名码对，则显示二维码显示所有内容：

厂家（商家）名

物品名

厂家（商家）名是商家门口或在价格标签中明码给出的，购物者可以对比，是否一致。物品名也是在价格标签中明码给出的，购物者是可以识别的。

**3 证明链的有效性**

无论是竖向证明链或横向证明链，其防伪的能力是有限的。尽管这样，纸质防伪标签有它的优越性，提供证明的成本很低（不用RFID等额外部件），验证则免费开放，使人人具有验证功能，实现方法也简便易行，可以起到应有作用。

防伪的主要任务为广大购物者提供真伪识别的简便方法，同时要考虑到在发生纠纷的情况下提供法律依据的需要。

商家真实性是在发票或收据中一定体现。如果商家B出售商家A证明的商品，那么商家B开不出商家A的发票或收据。因此，在防伪标签和收据之间又形成一种证明链。尽管纸质的防伪标签容易被复制，但责任的溯源性、标签和发票的一致性，很容易使购货人识别出来。所有防伪标签和电子票据都提供二维码，手机上的NFC都能直接解读，为公众提供人人防伪的有力武器。

证明链的示意见图5.1。

标签链 收据链

A层标签

标签：制造商签名

收据：制造商签名

旁证

旁证

证明链

B层标签

标签：批发商签名

收据：批发商签名

旁证

证明链

证明链

C层标签

收据：批发商签名

标签：批发商签名

图5.1 防伪标签的证明链

对流通中货物，如果纸质防伪标签则不适用，则只能用RFID来实现。