基于RFID技术的防伪平台的设计与实现

芦 佳,卫 强,陈 兵
(南京航空航天大学 计算机科学与技术学院,江苏 南京 210016)

摘 要:针对商品市场传统防伪手段的缺陷,提出基于射频识别(RFID)技术的防伪机制。该防伪平台利用公钥基础设施技术建立身份认证体系,将数字签名技术应用到电子标签的识别验证中来,设计了防伪流程和验证方法,以此搭建商品防伪追溯模型,并做了模型的安全性分析,最后实现了以酒类为代表的防伪系统。该系统采用Java EE设计开发,以第三方可信防伪平台为基础,支持手机RFID扫描查询、网站查询、短信查询、RFID终端查询等方式,通过商品信息的共享达到防伪验证的目的。

关键词:防伪;射频识别;公钥基础设施;加密机制
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2012)05-0233-04

Design and Implementation of Anti-Counterfeit System Based on RFID

LU Jia, WEI Qiang, CHEN Bing
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract: Due to the shortcoming of the traditional anti-counterfeiting means in commercial field, an RFID-based(Radio Frequency Identification) anti-counterfeit mechanism was presented. It realizes an anti-counterfeit system for wine products, which designes a PKI(Public Key Infrastructure) identification system to help trace back the product source, and safety analysis for this model is also included. The security process and verification method are in details. In order to offer convenient and efficient anti-counterfeit services, the manufactures' information is shared with consumers through an reliable third-party platform. The system is written in Java EE, which supports RFID cellphone scanning query, website query, SMS query and RFID terminal query etc.

Key words: anti-counterfeit; radio frequency identification; public key infrastructure; encryption mechanism

1 概 述

随着我国市场经济的蓬勃发展,假冒伪劣商品的生产和流通日益猖獗,涉及服装、食品、药品等各个领域,严重侵害企业和消费者的利益。目前防止假冒产品构成的四个主要因素:立法、执法、反仿冒政策、技术措施[1]。如何通过技术手段,有效鉴别和防止假冒商品在市场的流通,成为我国经济高速发展中急需解决的问题之一。

传统的防伪手段有激光全息防伪、荧光防伪、油墨防伪、电话短信防伪等,主要通过纸质印刷,肉眼识别的方法进行防伪鉴别。这种防伪方法需要主观判断,因而准确性不高、容易仿造和重复利用,难以满足现代防伪的需求。

RFID是通过无线电讯号识别特定目标并读写相关数据的一种无线通信技术[2],在防伪领域的应用具有显著的优势:每个标签都有一个全球唯一的ID码,无法修改和仿造;非接触式读写,无机械磨损,可工作于恶劣环境下;数据部分可以采用一些加密算法和认证过程,增加数据的安全性;数据存储量大,内容可多次擦写等[3]。

文中运用RFID技术和密码技术,构建一个完整的商品防伪平台。以可信第三方作为信任层次的根节点,引入公钥基础设施(Public Key Infrastructure, PKI),对不同厂商进行身份认证后,将其产品信息收录到防伪系统中,供消费者查询验证。该防伪平台在满足防伪查询途径多、防伪性强、识别效率高等优点的同时,还能够与商品物流平台、企业进销存系统等结合,形成一个完整地生产、运输、销售的信息链。

收稿日期:2011-09-10;**修回日期**:2011-12-15
基金项目:国家科技部计划项目:互联网潜在犯罪组织侦查与分析系统(2009GJE00035)
作者简介:芦 佳(1981-),男,黑龙江佳木斯人,硕士研究生,研究方向为计算机网络;陈 兵,博士,教授,硕士研究生导师,研究方向为计算机网络、通信与安全。

2 系统架构及防伪验证方法

2.1 基于 PKI 的总体架构

防伪系统需要保存来自生产厂商的产品信息，并以此作为数据库供消费者查询验证，经销商也需要录入商品流通信息来满足产品追溯的需求，而这整个的信息交换过程最便捷的方式就是以互联网作为通信网络。由于互联网的开放的网络环境特点，厂商和经销商的身份认证显得尤为重要，需要一定机制来防止不法分子冒充厂商录入虚假信息。文中采用基于 PKI 的身份认证体系，来保证信息录入的真实可靠。

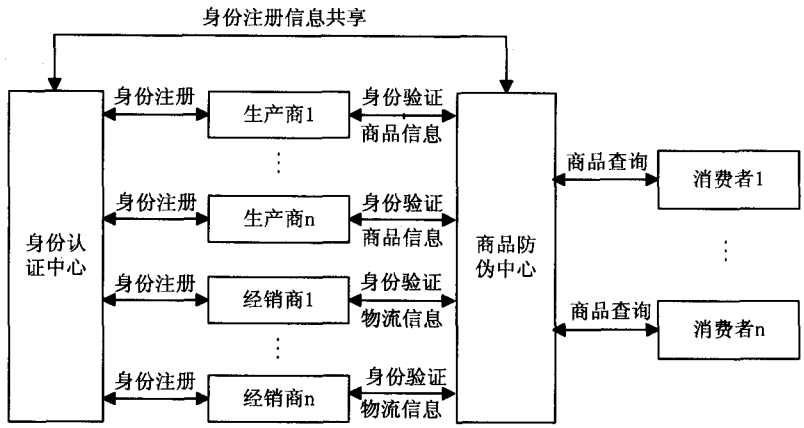


图 1 系统框架

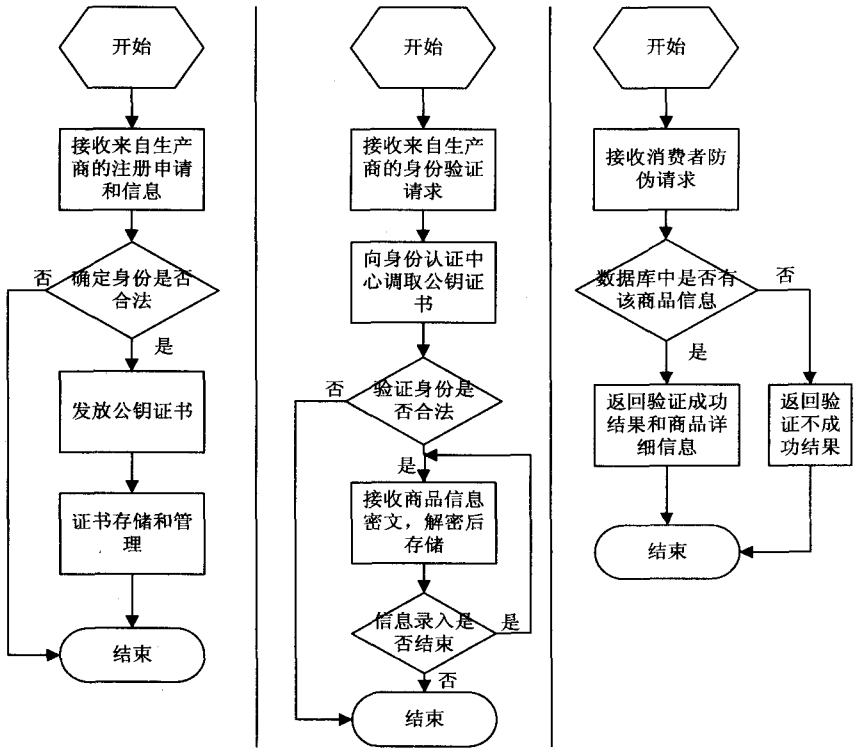
公钥基础设施是利用公钥理论和技术建立的提供信息安全服务的具有普适性的基础设施[4]，它是国际公认的互联网电子商务的安全认证机制，它利用现代密码学中的公钥密码技术在开放的 Internet 网络环境中提供数据加密以及数字签名服务的统一技术框架[5]。PKI 主要由认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口(API)等基本构成部分[6]。PKI 的核心技术就围绕着数字证书的申请、颁发、使用与撤销等整个生命周期进行展开。

文中采用的 PKI 公钥加密算法是椭圆曲线密码(Elliptic Curve Cryptography, ECC)[7]，该加密算法是基于椭圆曲线算数的一种公钥密码方法。椭圆曲线密码的安全性[8]，依赖于椭圆曲线离散对数问题的难解性，其具有密钥长度短、抗攻击性强、单位比特的安全性强度较高等特点，目前尚未找到可行的破解方法。

防伪系统作为第三方可信平台，可以为多个厂家和各自的产品提供防伪认证服务，包括生产商、经销商、消费者、身份认证中心和商品防伪中心五个实体部分。其中身份认证中心与商品防伪中心是两个逻辑独立的功能模块，共享身份注册信息、公钥密钥等信息，在实际应用中可以建设在同一个服务器上，具体系统框架如图 1 所示。

2.2 防伪流程设计

防伪平台的整体流程分为三部分：生产商和经销商的身份注册、商品信息的录入和商品防伪验证。由于生产商与经销商在身份注册、验证和商品信息录入等流程类似，故仅对生产商进行讨论，具体流程如图 2 所示。



(a) 身份注册流程 (b) 商品信息录入流程 (c) 商品防伪验证流程

图 2 系统流程图

2.3 防伪验证方法

根据文献[9]电子标签依据功能划分为五大类，文中采用只具有信息存储功能、不具有密码处理能力的 Class 1 类型标签。产品采用 EPC 码对产品进行唯一标识，符合当前物联网发展建设的标准。电子产品编码(Electronic Product Code, EPC)是目前欧美普遍支持的商品的电子编码方式，其目的是为每一个产品提供唯一的电子标识符，其中包括生产厂商、产品分类等信息。文中通过 Hash 函数对 EPC 码提取数字摘要，

并进行加密处理来防止EPC码的伪造和篡改。Hash函数以当前应用比较广泛的SHA-1为例,加密方式同样采用公钥ECC加密算法,验证过程如图3所示。

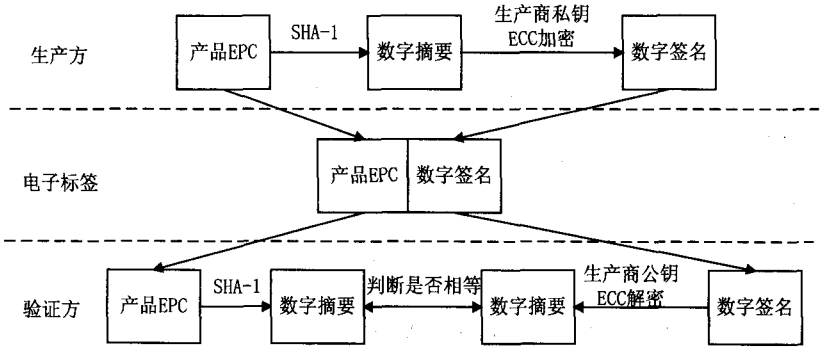


图3　电子标签验证流程

电子标签的验证分为两个阶段:在生产阶段,厂家将产品的EPC码通过SHA-1提取数字摘要,并用自身的私钥进行加密处理,得到数字签名,将产品的EPC码连同签名一起存入标签;在验证阶段,一方面将EPC码进行SHA-1处理,得到预期的数字摘要,另一方面用该厂家提供的公钥对其数字签名进行解密,得到实际的数字摘要,并与预期值进行比较,如果相等,则标签合法有效,提交到数据库查询产品具体信息并返回结果,反之则无效。

2.4　防伪验证的安全性分析

(1)基于PKI的身份认证方式,通过对生产商和经销商颁发和定期更换数字证书,保证了生产商和经销商向防伪中心提交信息的合法身份,杜绝了攻击者冒充厂家向防伪中心提交虚假信息的可能。

(2)对于信息传输录入阶段,生产商和经销商使用自身私钥加密后向防伪中心提交数据,在保证私钥安全的前提下,造假者无法伪造和篡改信息,保证了通信阶段的安全。

(3)标签EPC码经过SHA-1和ECC两次加密处理,攻击者无法伪造数字签名,也就杜绝了对于EPC码仿造和篡改的可能性。即使能够估算出厂家商品的EPC码,也无法仿造其签名,不能伪造标签。

综上所述,虽然防伪系统建立在互联网的基础之上,但不法分子在试图伪装合法厂家攻击防伪中心或伪造、恶意篡改标签的时候,都不可避免的会遇到ECC加密的破解问题,而对于椭圆曲线离散对数问题的难解性,从目前的技术水平,无法在有效时间内破解,所以,本防伪平台能够满足安全性要求。

3　基于RFID的酒类防伪系统设计

3.1　EPC编码

目前的EPC编码结构标准包括:EPC-64,EPC-96,EPC-256,考虑目前发展的主流编码体制以及成本和酒类出货量,选择EPC-96进行编码,其编码长度为96bit,分为表头8bit、厂商识别代码28bit、产品分类代码24bit和序列号bit四个部分[10]。对于同一个厂家来说,厂商识别代码是相同的,对于同一种商品来说,产品分类代码是相同的,而序列号则对每件商品进行区分。

3.2　标签设计

根据系统防伪需要以及成本的控制,采用无源式超高频(UHF)的Class1型RFID电子标签。对于标签的销毁设计,目前有软件破坏和硬件破坏两种。软件破坏方式是通过授权的读写器向标签发送kill指令[11],使标签受到永久性破坏。这种标签的缺点是标签需要具有自毁功能,制造成本增加,并且在酒品出售到消费者手里后,不再具有查询防伪功能,对于不一定会立即饮用、经常转赠他人的酒品来说并不适合。本系统采用硬件破坏的方式,即标签的存储模块和天线在标签内分为两部分,通过导线相连,将该标签粘贴在酒瓶和瓶盖之间,当开启瓶盖时,则存储模块与天线物理分离,使其永久性破坏,不可再次利用。

3.3　功能模块设计

防伪系统从功能上分为身份认证、信息录入、防伪追溯、数据管理和决策支持五个模块,具体设计如图4所示。身份认证模块主要负责检查验证企业和经销商的数字签名,确定其合法身份,包括从CA获得电子证书,对证书定期更新等功能;信息录入模块负责将企业和经销商提供的商品信息以及流通情况录入系统,包括信息传输过程中的加密解密等;防伪追溯模块负责提供产品信息查询、防伪验证及产品的追溯查询,提供网页、短信、读写器终端通信等多种查询手段,保证在分级销售和最终消费者提供全程查询验证服务;数据管理模块直接负责数据库的管理,如删除已经过时的产品信息、定期数据备份、数据导出等,保证数据库运

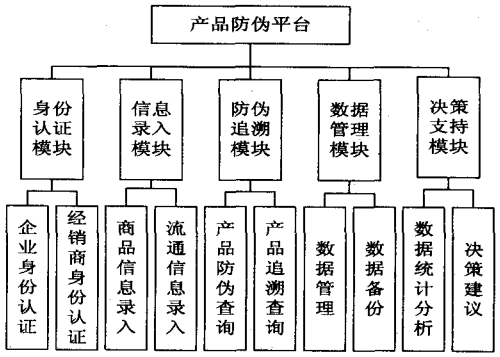


图4　系统功能模块

行的高效和数据的安全;决策支持模块是对系统的后续开发做准备,当数据库有了一定量的信息积累,通过品对产生产、销售等相关信息的分析和处理,可以为企业管理者提供部分决策数据支持,以此提高企业经营决策的科学性。

3.4 技术架构

系统以 Java EE 平台进行开发,采用 Struts 的结构框架,运用 Internet 网络传输、无线 GPRS 网络接入以及短信通信等多种通信方式,其结构如图 5 所示。读写器与防伪中心的数据传输采用简单对象访问协议(SOAP)[12]。SOAP 是一种轻量级的、基于 HTTP 协议的采用 XML 格式的传输协议,具有穿透网络任何路由器、防火墙或代理服务器等优点,并且可以在异构程序间通信,满足本系统需求。

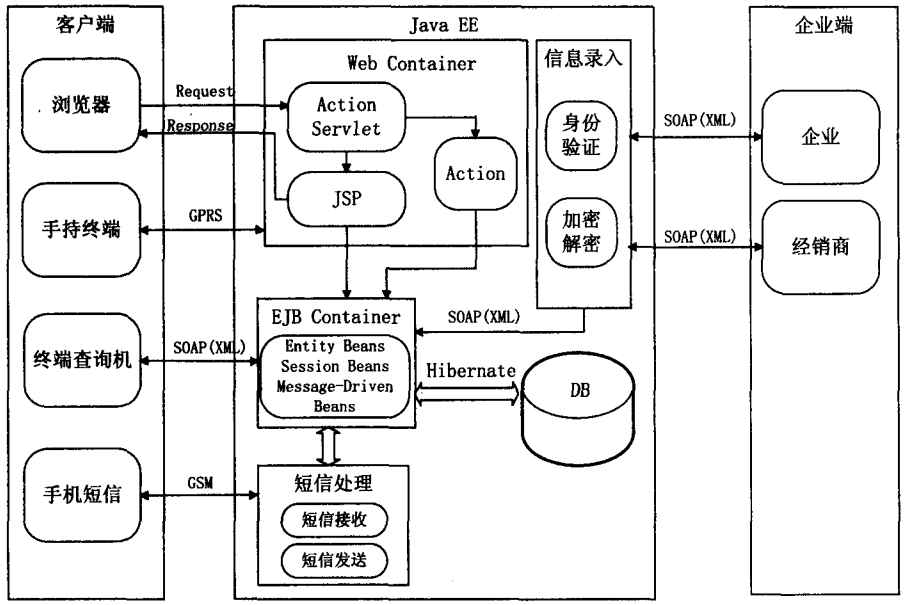


图 5 系统架构图

客户端采用以下四种防伪查询手段:

(1)通过浏览器登录防伪网站,输入 EPC 码进行查询验证;

(2)使用具备 GPRS 网络功能的手持终端或具有读取标签信息功能的手机,通过 GPRS 网络与防伪平台通信,接收返回的产品信息;

(3)使用专卖店或商场销售商的终端机,通过基于 Web 的 SOAP 协议,传输 XML 格式的消息,返回查询结果;

(4)通过手机短信将查询码发送到防伪平台,经过平台处理后,将结果以短信方式发回到客户手机上,达到防伪查询的目的。

企业端将产品信息加密后传递到服务器端,服务器端在身份验证通过后,接收信息并解密,经过处理后保存进数据库。服务器端支持多种方式的数据请求服务,经相关模块处理并与数据库交换数据,交换方式采用 Hibernate 的框架模式。

4 基于 RFID 防伪技术性能分析

文中设计的防伪系统采用 RFID 的防伪技术,在有效控制标签成本的同时,能够较好地满足防伪需要,具有仿造难度大、存储信息量大、适应环境强、验证效率高等优点,并支持产品追溯功能。表 1 比较了当前主流的几种防伪技术的性能,可以看出,基于 RFID 技术的防伪手段有着较强的优势。

射频识别防伪具有多方面优点的同时,也面临一些问题:

(1)防伪系统建设前期投入成本较高;

(2)防伪过程需要读写器支持,普通用户无法读取标签信息,随着手机功能的拓展,支持扫描电子标签的手机已经出现,随着该手机的逐渐普及,将解决这一问题;

(3)通信网络采用专网费用较高,采用互联网对安全性要求较高。

5 结束语

文中基于RFID技术提出了一套商品的防伪方

表 1 防伪技术比较

防伪技术	防伪造性	信息量	可靠性	标签成本	环境适应性	验证效率	追溯功能
条码防伪	低	低	低	低	低	高	有
光学防伪	低	低	低	低	低	低	无
生物防伪	高	高	高	低	低	低	无
材料防伪	低	低	低	高	低	低	无
印刷防伪	低	低	低	低	低	低	无
RFID 防伪	高	高	高	低	高	高	有

(下转第 241 页)

型的 * _属性规则(如表1所示),禁止向高敏感级别的客体进行写入,只允许写同敏感级别的客体,保证了计算机系统上敏感信息的完整性。

表1　多级可信主体的安全规则

BLP安全模型规则	低可信主体[0,0.5)	中等可信主体[0.5,1)	可信主体[1]
简单安全条件	√	√	×
* -属性	×	√	×

4　结束语

文中对传统的敏感信息安全控制多级安全模型BLP模型进行了分析,指出传统BLP模型在敏感信息安全控制上存在的无法保证客体敏感信息可用性及完整性的安全隐患。针对该安全隐患,文中提出了一个基于动态可信度量的敏感信息安全控制模型DTMSISCM及其实现架构,通过在传统BLP模型基础上增加主体动态可信度量及可信度分级,并定义主体可信度规则和敏感信息安全控制规则,对不同可信度的主体实施与其可信度相适应的敏感信息安全控制规则。通过对DTMSISCM的安全性分析,在维持与BLP模型相同的保密性的基础上,提高了系统在敏感信息安全控制方面的可用性和完整性。

未来,将进一步结合可信计算的技术研究如何更加准确地度量主体的可信度,提高主体动态度量的实时性。

参考文献:

[1] 杨　智,金舒原,段　毅,等.多级安全中敏感标记的最优化挖掘[J].软件学报,2011,22(5):1020-1030.

[2] 武延军,梁洪亮,赵　琛.一个支持可信主体特权最小化的多级安全模型[J].软件学报,2007,18(3):730-738.

[3] Trusted Information System Inc. Trusted mach mathematical model[R].[s.l.]:Trusted Information System Inc.,1996.

[4] Tmp L. Using mandatory integrity to enforce commercial security[C]//Proceedings of the IEEE Symposium on Security and Privacy.[s.l.]:[s.n.],1988:140-146.

[5] Bell D E,LaPadula L J. Secure computer system:unified exposition and multics interpretation[R]. Bedford,MA:The MITRE Corporation,1976.

[6] Bell D E,LaPadula L J. Secure computer systems:mathematical foundations[R]. Bedford,MA:Electronic Systems Division,Air Force System Command,Hanscom AFB,1973.

[7] Bell D E,LaPadula L J. Secure computer systems:a mathematical model[R]. Bedford,MA:Electronic Systems Division,Air Force System Command,Hanscom AFB,1973.

[8] 季庆光,卿斯汉,贺也平.一个改进的可动态调节的机密性策略模型[J].软件学报,2004,15(10):1547-1557.

[9] 石文昌,孙玉芳,梁洪亮.经典BLP安全公理的一种适应性标记实施方法及其正确性[J].计算机研究与发展,2001,38(11):1366-1372.

[10] Trusted Computing Group. TCG Specification Architecture Overview Revision 1.4[S].[s.l.]:TCG,2007.

[11] 张晓菲,许　访,沈昌祥.基于可信状态的多级安全模型及其应用研究[J].电子学报,2007,35(8):1511-1515.

(上接第236页)

案,通过第三方可信防伪平台的数据共享,将客户与企业、经销商有效地联系起来,融入了基于公钥加密技术的PKI身份认证体系,在采用低成本的不具有加密能力的电子标签的前提下,提出了一种较为有效的防伪机制。针对酒类防伪平台,设计了具体的功能模块,提出了系统的架构设计,支持手持终端、终端查询机以及短信等多种手段的防伪查询,并对商品追溯、销售信息的挖掘利用提供了依据。通过分析比较,RFID防伪技术优势明显,随着技术的不断完善和市场认可,必将在防伪领域逐步普及开来。

参考文献:

[1] Organization for Economic Co-operation and Development (OECD)(1998)The Economic Impact of Counterfeiting[S]. www.oecd.org/dataoecd/11/11/2090589.pdf.

[2] Weinstein R. RFID:a technical overview and its application to the enterprise[J]. IT Professional,2005,7(3):27-33.

[3] 蒋玉杰,曹岳辉.基于RFID技术的系统方案设计[J].计算机技术与发展,2011,21(4):9-12.

[4] 沈昌祥.信息安全导论[M].北京:电子工业出版社,2009.

[5] 落红卫,程　伟.RFID安全威胁和防护措施[J].电信网技术,2010(4):38-40.

[6] 陈　翔,庄　毅,吴学成.椭圆曲线加密算法及其在PKI中应用模型的研究[J].计算机技术与发展,2006,16(3):129-131.

[7] 周国祥,张庆胜.ECC应用于PKI之研究[J].合肥工业大学学报(自然科学版),2003,26(6):101-107.

[8] 李　湛.一种改进的椭圆曲线密码实现算法[J].电子科技,2004(7):31-33.

[9] Thieseh F, Floerkemeier C,Harrison M,et al. Technology, standards,and real-world deployments of the EPC network [J]. IEEE Internet Computing,2009,13(2):36-42.

[10] 黎　利.EPC系统中的中间件的研究[D].成都:电子科技大学,2006.

[11] 祝胜林,杨　波,张明武.RFID协议及其安全性研究[J].信息安全与通信保密,2007(8):168-170.

[12] Brogden B. SOAP与JAVA编程指南[M].北京:电子工业出版社,2002.