基于PKI的电子印章系统

李 新 孙玉芳

(中国科学院软件研究所 开放系统与中文信息中心 北京100080)

摘 要 本文将数字签名技术应用于电子印章,设计了一套基于PKI的电子印章系统。这套电子印章系统采用XML数据格式、原始文档、印章图片和落款等盖章信息在盖章文件中分开存放,支持多次盖章和同时盖章。通过客户端浏览器插件和Office插件,可以在浏览器和Office中完成盖章、验证、浏览等功能。最后,本文给出了基于B/S结构的电子印章系统结构,并以甲、乙双方在同一文档上盖章为例,介绍了盖章、验证和再盖章的过程。

关键词 电子印章,数字签名

An Electric Seal System Based on Public Key Infrastructure

LI Xin SUN Yu-Fang

(Open System & Chinese Information Processing Center, Institue of Software, Chinese Academy of Sciences, Beijing, P. R. China, 100080)

Abstract An electric seal system based on PKI and digital signature is set up in this paper. The file data format of sealed document is XML. The original sealed document, seal picture and inscriber etc are saved in different element of sealed document. Seal, verify and view sealed document can be done in Office and Internet Explore through software plug in. The structure of electric seal system based on Browser/Server is recommended and a example of two person seal on one document is referred to show the process of seal, verify and seal again.

Keywords Electric seal, Digital signature

中国自古以来便认定"章"是权力的象征,如封建王朝的皇帝玉玺、官印;现代社会的公章、私章等等,"章"在中国已经有几千年使用和发展历史。在数字时代,提倡电子化的办公环境里,印章制度渐渐有所转变,正在由传统的实物章转为电子印章。

从技术的角度而言,电子印章与数字签名采用的是同一种认证技术,实现数字签名有很多方法,目前数字签名采用较多的是公钥加密技术。基于公钥加密技术的电子印章数字签名系统可用于电子政务中签发电子文档、电子商务中签定合同、确定交易双方的真实身份、保证电子文档的真实性、完整性、不可修改性、不可否认性等等,是电子商务、电子政务中保障信息安全的基础,具有广泛的适用范围[1~6]。

1 数字签名与电子印章

传统的实物印章依靠印模的复制困难来保证文档的真实性,随着科学技术的发展和普及,印模的复制越来越容易,传统的实物印章已经变得十分不可靠,迫切需要新的认证技术来代替。对于电子文档来说,传统的印章表现为文档中的一张图片,由于电子图片的复制十分容易,依靠印章图片来保证电子文档的真实性已经毫无意义。

数字签名的安全性远远高于传统印章,按理说,在电子文档中,完全可以用数字签名代替印章来保证文档的真实性,而不必考虑印章图片有关问题,但实际情况并没有那么简单。

首先,传统的印章概念在中国根深蒂固,如果在电子印章中完全抛弃传统的印章概念,简单地用数字签名代替电子印章,用户往往难以接受,因此,国内市场上出现了一些基于印章或签名图片的安全技术,其中的一些理论基础并不充分。

其次,与数字签名相比较,电子印章的需求更复杂。如果是对原文件的一次盖章,在对原文件插入印章图片、落款和盖章日期后进行数字签名,用数字签名代替电子印章没有任何问题,但是,很多情况下,往往是一个文件需要盖多个印章,即要对同一个文件多次插入印章图片、落款和盖章日期。传统的纸文件原件只有一份,实际的盖章过程只能在同一个文件上进行,也就是说即便是甲乙双方同时盖章,盖章也是有顺序的,而电子文档却有可能出现真正的同时盖章的情况。数字签名的基本要求是原文件不能修改,在原文件中插入印章图片、落款和盖章日期等会使数字签名验证无法通过,如果只对插入印章图片、落款和盖章日期之前的文件进行签名,图片、落款和盖章日期这些信息就得不到有效保护,因此不能简单地用数字签名代替电子印章。

2 电子印章原理

利用数字签名技术的电子印章系统,需要对数字签名进行一些改进,主要解决两个问题:(1)在签名文档中插入图片、落款和盖章日期等信息后,仍然能够保证原来的签名通过验证;(2)印章图片、落款和盖章日期等盖章时产生的信息需要同原始文档一起受到签名保护。

根据电子印章对数字签名的要求,可以将电子印章的签名文档分成两部分:原始文档和附加信息(即:印章图片、落款和盖章日期等)。对于同一文档的不同电子印章,原始文档相同而附加信息各不相同,电子印章中的数字签名实际上是对原始文档和附加信息合成的新文档提取数字摘要,然后对摘要进行私钥加密。

我们将加盖了电子印章的文件称为"盖章文件"。为了能够在Internet上方便、稳定地传输,"盖章文件"最理想的格式应该是纯文本,同时,"盖章文件"应该能够方便地合成和解析。基于以上考虑,本文设计了一种基于XML的"盖章文件"格式。在"盖章文件"中原始文件和印章图片、落款、盖章日期分别存放在不同的元素中,只是在向用户显示时才将它们合成在一起,这样可以保证多次盖章后原文件不被修改。同时与印章相对应的数字签名不是对原始文件的数字签名,而是对"盖章申请"的签名。与"盖章文件"一样,"盖章申请"采用

李 新 博士,主要研究领域为信息安全、工作流。

XML 文件格式。"盖章申请"中包含了原文件的数字摘要和印章图片、落款、盖章日期等信息，从而保证了所有这些信息都受到数字签名的保护。

"盖章文件"包含原始文档、印章图片、落款、盖章日期、对"盖章申请"的数字签名、签名证书等信息，这些信息按照一定的规则存储在 XML 文件的元素中，根据这些信息，用户可以从"盖章文件"中恢复"盖章申请"、验证数字签名或将新的盖章信息加入"盖章文件"中(即：对原始文件加盖新印章)。"盖章文件"中原始文件、印章图片、数字签名和签名证书等二进制数据都经过了 Base64编码。

为了能够正确恢复和显示盖章后的原始文档，"盖章文件"中应该包含原始文档类型、显示和编辑原始文档的软件名称、印章图片在原始文档中的位置等信息。"盖章文件"解析程序可以做成 Office 或浏览器插件，这些插件程序可以按照"盖章文件"中存储的信息，正确显示原始文件及印章图片。同时，插件程序还具有验证数字签名、根据用户要求生成"盖章申请"、合成"盖章文件"等功能。

3 电子印章文件格式

"盖章文件"由原始文件正文(经过 Base64编码)、原始文件基本信息(文件名，文件类型，文件编辑器，文件查看器等)、零个或多个印章组成：

〈!ELEMENT 盖章文件 (文件名?,文件类型,文件编辑器*,文件查看器*,正文编码方式,正文,印章*)〉

其中："文件名"为原始文件名称(可选)，用于为用户从"盖章文件"中提取原始文件时提供默认的文件名称；"文件类型"为原始文件的类型(如：DOC、PDF、XLS 等)；"文件编辑器"为处理原始文件的编辑软件(如：WINWORD. EXE、EXCEL. EXE 等)；"文件查看器"为查看原始文件的软件(如：IEXPLORE. EXE、ACRORD32. EXE)；"正文编码方式"，将正文编码为文本的算法(目前为 Base64)；"正文"，经过 Base64编码的原始文档；"印章"包含与盖章有关的信息，可以是零个或多个，零个对应没有印章的情况。

"印章"由印章图片、数字签名、印章基本信息(名称、显示落款、显示日期、盖章日期等)组成：

〈!ELEMENT 印章 (名称?,显示落款?,显示日期?,盖章日期,印章图片?,数字签名)〉

其中："名称"为印章名称(可选)；"显示落款"为显示于正文的印章落款；"显示日期"为显示于正文的盖章日期；"盖章日期"为盖章的实际时间，由印章服务器填写；"印章图片"为显示于正文的印章图片；"数字签名"为印章对应的数字签名。

"显示落款"包括"落款"和"落款位置"两个元素：

〈!ELEMENT 显示落款 (落款,落款位置?)〉

其中："落款"为显示于正文的落款内容；"落款位置"描述"落款"在正文中显示的位置，据此可以将"落款"显示在正文的合适位置。位置的表达方式可以按照页号、水平位置(字符或绝对坐标毫米等)、垂直位置(行或绝对坐标毫米等)的方式表示，也可以采取"其它表示法"，如：提前在正文模板中做插入标记，按照这些标记插入印章"落款"：

〈!ELEMENT 落款位置 (页号?,水平位置?,垂直位置?,其它表示法?)〉

印章的"显示日期"和"印章图片"的位置表示方式与"显示落款"类似。

"数字签名"包括签名证书和签名算法等内容：

〈!ELEMENT 数字签名 (证书编码算法,证书编码,正文摘要算法,数字签名摘要算法,数字签名编码算法,数字签名)〉

其中："证书编码"是经过编码的签名证书，存放在"盖章文件"中，用来验证数字签名；"正文摘要算法"用来提供生成"盖章申请"时的"正文摘要"；"数字签名编码"为对"盖章申请"的数字签名，经过 Base64编码。

"盖章申请"是盖章插件提供给印章服务器，要求签名盖章的 XML 文件，"盖章文件"包含"正文编码摘要"和"印章"两个元素。其中，"正文编码摘要"保证了对"盖章申请"的签名能够提供对原始文档的签名保护；"印章"与盖章文件中的"印章"元素结构相同：

〈!ELEMENT 盖章申请 (正文编码摘要,印章)〉

印章服务器得到"盖章申请"后，填写"盖章时间"，然后按照"盖章申请"要求的算法对"盖章申请"进行数字签名，然后将签名证书、签名编码等信息添写到"盖章申请"文件中，将"盖章申请"反馈给用户，由盖章插件合成"盖章文件"。

为保证数字签名的稳定性，在对"盖章申请"签名前，应该删除"盖章申请"中的空格、注释、回车换行等字符。

4 电子印章系统实现

印章系统与 CA 系统服务器配合使用，即电子印章系统的印章证书来自于 CA 服务器，电子印章系统通过 CA 系统生成、发布、吊销电子印章证书。同时印章服务器维护和管理印章数据库，印章数据库中包含印章图片、印章证书密钥及印章授权使用情况记录。

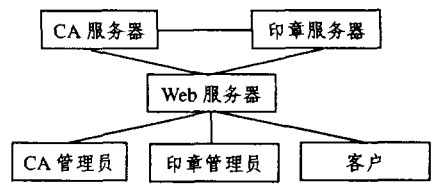

图1 电子印章系统结构

由于印章密钥存放于印章服务器，印章服务器应该处于高度安全的环境保护下，包括物理隔离和网络安全等等，同时印章的使用情况应该有完整的日志记录。

系统以 B/S 方式实现。CA 服务器和印章服务器通过 Web 服务器管理印章、密钥、证书、接受用户盖章申请等。

以下通过一个甲方"盖章"、乙方"验证"、再"盖章"的过程，说明电子印章系统的使用过程。"盖章"、"验证"、再"盖章"过程需要客户端软件(浏览器插件或 Office 插件)支持。

甲方盖章过程：(1)首先是将原文件 Base64编码保存，然后从印章服务器得到印章图片，再将图片插入正文合适的位置(供用户查看和调节印章位置)，同时插入印章落款、盖章时间等信息，客户端软件搜集这些信息，与原文件 Base64编码摘要一起打包成"盖章申请"。(2)将"盖章申请"发送到印章服务器，印章服务器将实际盖章时间写入"盖章申请"中，然后对"盖章申请"数字签名，将"盖章申请"、数字签名以及印章证书一起打包成"盖章数据"，发送到客户端。(3)客户端将原文件 Base64编码、"盖章数据"等信息打包成盖章文件。

乙方印章验证及再盖章过程：(1)首先是从盖章文件中提取原文件 Base64编码、印章图片、落款、数字签名、数字证书等信息，恢复盖章申请原貌，验证数字签名以确认盖章是否有效。(2)恢复原文件显示给用户。(3)按照盖章程序再盖章。

结论 电子印章系统是 PKI 数字签名技术在传统印章电子化过程中的应用。电子印章系统的设计，不仅体现了现代计算机技术对传统公文和印章的影响；同时，中国传统文化对计算机技术的渗透也清晰可见。在设计电子印章系统的过程中，不仅要考虑电子公文本身的安全性，还要照顾用户使用印章的传统习惯，如：印章图片等。唯有如此，才能保证现代计算

机技术的顺利推广和普及。

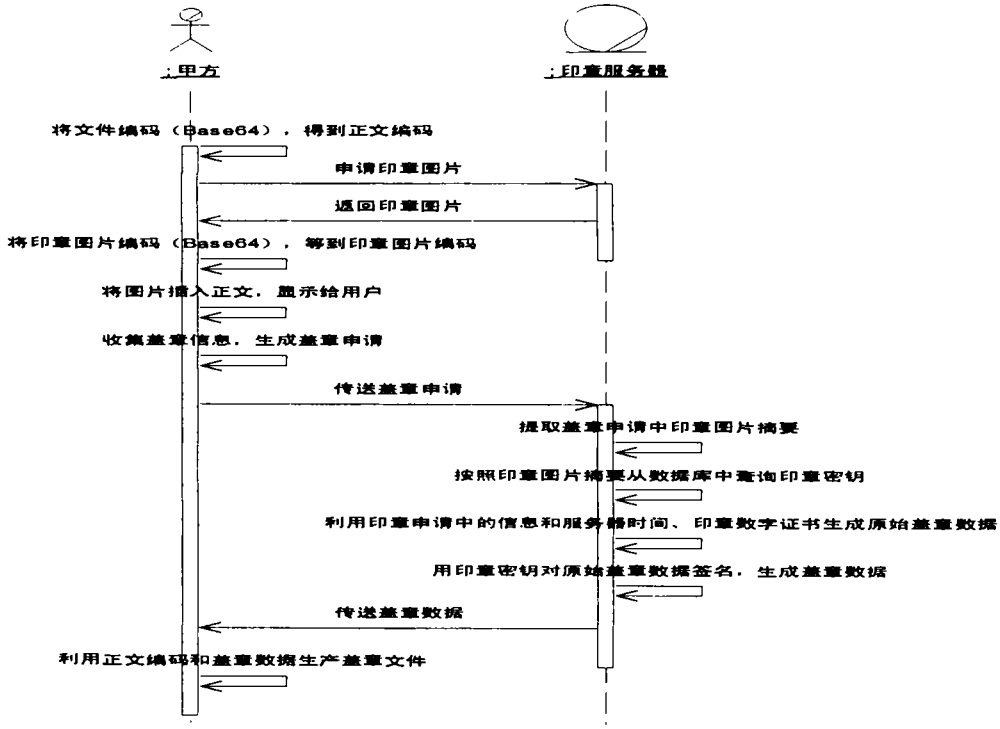

图2　盖章过程交互图

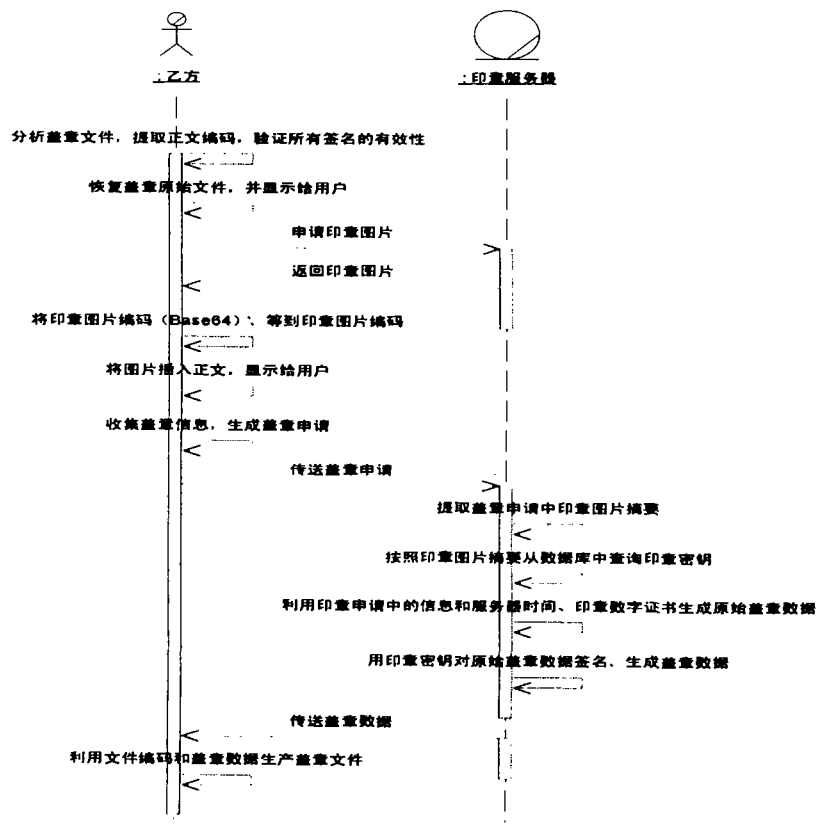

图3　印章验证及再盖章过程交互图

参 考 文 献

1　张小绵，柳松，古元. 印章网络管理系统的设计与实现. 株洲工学院学报，2002，16(4)：45～48

2　肖攸安，李腊元. 数字签名技术的研究. 武汉理工大学学报，2002，26(6)：667～671

3　吕皖丽，钟诚. 数字签名方案的分析. 广西科学院学报，2002，18(4)：161～164

4　张大陆，时慧. 电子公文中数字签名的设计与实现. 计算机应用研究，2001，18(6)：78～79

5　于增贵. 数字签名和数字签名标准. 四川通信技术，2001，31(5)：51～53

6　黄伟，唐世钢，崔世军. 基于 RSA 公钥体制的多重数字签名研究. 哈尔滨理工大学学报，2001，6(5)：57～59