面向 Web 页面的电子签章控件的实现①

郭腾芳，韩建民，李 静，罗方炜

(浙江师范大学 数理信息学院，金华 321004)

摘 要：提出了一个面向 Web 页的电子签章控件的设计方法，该控件可实现对 Web 页上任何元素子集的数字签名，并可将带有电子印章的 Web 页面保存成本地文件，实现离线验证。论述了该控件的实现方法及相关技术，并将该控件应用于基于 Web 的电子合同中。实际应用表明，该控件能够保证签章 Web 页面中重要信息的完整性和不可否认性。

关键词：数字签名；电子签章；ActiveX；数字证书

Implementation of Electronic Signature Control Oriented to Web Page

GUO Teng-Fang, HAN Jian-Min, LI Jing, LUO Fang-Wei

(College of Mathematics Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China)

Abstract: The paper proposes an approach to designing an electronic signature control oriented Web page, which can implement digital signature for any html elements set on the Web page. The control can also save Web page with the electronic seal as local document for offline verification. The paper discusses the implementation method related technologies of the control, and applies the control to Web-based electronic contract system. Practical application shows that the control mate the integrity and non-repudiation of web page with electronic seal.

Keywords: digital signature; electronic signature; ActiveX; certificate

1 引言

随着网络技术快速发展，电子商务和电子政务得到越来越广泛的应用。随之电子文档与交易信息在网络上的安全问题也显现出来。尽管数字签名技术可以实现电子文档和交易信息的完整性和不可抵赖性，但数字签名是一组不可见的数据，使用者无法通过肉眼来识别。而可视印章在中国的认证体制中，已根深蒂固，因此研究在网页上的电子签章技术，切实实现无纸化办公，具有重要的意义。

电子签章是指以数字化的形式存在于电子公文之上，用以表明文件批准者的身份及其合法性的信息。电子签章并非是书面印章的数字图像化，而是以一种代码的形式存在，用于辨识电子文件签署者的身份，保证文件的完整性、可靠性和不可抵赖性。有关电子签章的研究工作，已有了一些，袁晓宇等[1]提出了基于 ECDSA 的电子签章方法，它采用椭圆曲线密码(Elliptic Curve Cryptosystems)公钥密码体制，与常用的 RSA 相比，具有密钥长度小、签名长度短等特点。丁惠春等[2]提出了在电子政务中使用中间件技术来实现电子签章的方法。王飞等[3]提出了基于易碎水印和数字签名的电子签章方法。张飞等[4]研究了基于时间戳服务的电子签章验证方法。以上工作主要针对 Microsoft Office 文档的。而在电子商务和电子政务中很大一部分信息是通过 Web 页面进行交互的，如：通知公告、在线合同、网上审批、网上报税等。与 Office 文档不同的是，这些信息在服务器端是存储在一定的字段和数据表中，整个 Web 页面的数据是动态生成的，而不是存储在一个固定的文档里。所以，对 Web 页面进行数字签名，首先要有针对性地获取页面中的信息，在进一步对提取的动态信息进行签名。

① 基金项目:浙江省基金(Y1100191)

收稿时间:2010-08-04;收到修改稿时间:2010-09-09

目前面向 Web 页面的电子签章产品不多，功能也不强，主要有：金格网络科技有限责任公司的 HTML 网页签章套件、点聚信息技术有限公司的 WebSign 印章、软航科技有限公司的 NTKO 安全电子印章系统 HTML 版等。但这些产品目前只能对 HTML 表单元素进行签名，不能对 Web 页面中 HTML 非表单元素进行签名，也不能将加盖电子印章后的 Web 页面保存到本地机，不能实现脱机验证。针对以上问题，本文设计并实现了面向 Web 页面的电子签章控件，即 WebSeal 控件。

2　Web签章控件的功能设计

Web 页面的签章流程总体上可以分为三个过程：首先是预处理过程，定义页面中需要保护和进行签名的元素或者域的 ID，并按定义好的格式进行组织；其次是盖章过程，打开页面并选择盖章，对页面进行签名；最后是提交过程，页面完成盖章后，要将页面提交给服务器进行保存，分别将印章信息和无印章页面信息保存到印章数据库和业务数据库。具体如图 1 所示。

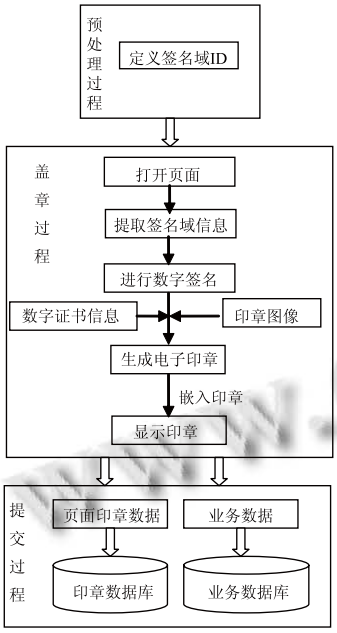

图 1　签章流程

为实现图 1 的签章流程，本文设计了可以嵌入在 Web 页内的 WebSeal 控件。WebSeal 控件实现了 Web 页面的盖章、数字签名和签名认证功能。WebSeal 控件的接口函数有：

(1) 用户身份认证：系统为提高安全性能，使用 USB-Key 盘存储用户数字证书、密钥、印章图像等。在盖章时，先验证用户 USB-Key 盘的 PIN 码，验证通过才能访问 USB-Key 盘。

(2) 加盖印章：首先由 USB-Key 盘认证用户身份，通过之后，根据页面签章域 ID，提取签章域的信息。再提取摘要信息，并进行数字签名，将产生的数字签名、摘要和从 USB-Key 盘中读取的证书信息等嵌入到印章控件中，最后在页面中加载印章控件。

(3) 撤销印章：撤销时，先检查印章是否处于可撤销状态，如果是，并通过 USB-Key 盘的 PIN 认证身份，则删除印章。

(4) 保存为本地文件：将盖章后的 Web 页面保存到本机，在保存时，分别将页面内容和印章信息各自保存起来。其中，将 Web 页面保存为单一文档格式。系统设计专用的阅读器，并将阅读器编译成资源文件，作为文件头与页面内容和印章数据进行合并，保存到本地文件。打开时，系统打开阅读器，然后阅读器从文件中提取页面内容与印章信息，并在阅读器上显示页面及印章。

(5) Hash 验证：用于实现文档的完整性验证。印章从页面中获取已定义签章域的信息，并提取摘要信息，再与盖章时保存在印章中的摘要信息进行比较，验证当前 Web 页面是否被篡改。

(6) 签名验证：用于实现签署者的不可抵赖性验证。进行签名验证时，印章首先从页面中获取已定义签章域的信息，并提取摘要信息。再以公钥解密印章中的签名信息获取摘要信息。比较两个摘要信息，验证当前 Web 页面的完整性和签署者的身份。

(7) 证书预览：无需身份验证，任务用户都可查看印章所属用户证书信息。盖章时，从用户 USB-Key 盘中获取嵌入到印章控件中。预览时，直接从印章控件中读出来。

(8) 提交：提交当前 Web 页面给服务器端进行保存。

(9) 加载：从服务器加载当前页面印章信息。

3　签章控件的实现技术

签章控件的主要功能是对页面中的数据进行数字签名，从而保证数据的完整性和签署者的不可抵赖性。为此，签章控件在实现的过程中，要解决以下几个关

键技术：

(1) 签署者及相关信息(如：印章图像、文档摘要、签名等)与印章绑定技术

为实现签署者的不可抵赖性，签署者的信息须与电子印章绑定在一起。为此建立一个签章类，该类定义了签署者信息、印章图像、文档摘要、签名等私有属性。盖章时，在印章控件中创建该类的实例，通过该实例将印章图像及相关属性绑定在一起。

(2) 签章图像在 Web 页面中的显示、拖动及删除等功能实现技术

本文基于 ActiveX 技术实现 Web 签章控件，控件可以完成印章读写、显示、文档的数字签名和验证以及文档的本地保存等功能。

Web 浏览器是 ActiveX 控件容器，首先将图章图像嵌入在 ActiveX 控件的 OLE 容器中，再采用 HTML 的 object 标签引入 ActiveX 组件技术将控件嵌入 Web 页面中，既实现了签章图像在 Web 页面中的显示，同时控件的事件和封装好的功能（如：拖动、删除等）也可以被响应。

(3) 网页数据的提取技术

Web 网页包含各种元素，本文利用 MSHTML 和 WebBrowser 组件。MSHTML 是一个 COM 组件。该组件把 HTML 语言中的所有元素及其属性都封装成像 IHTMLInputElement 、 IHTMLInputButtonElement 、 IHTMLInputTextElement 、 IHTMLTextAreaElement 、 IHTMLTitleElement、IHTMLFormElement 等组件接口。通过其提供的标准接口，可以访问指定网页的所有元素，从而完成元素对象的内容提取、赋值等操作。

在盖章前，将定义的签名域 ID 按定义好的格式(如：本文采用以“;”隔开)组合起来，作为参数传递给签章控件。签章时，控件解析签名域字符串，调用上述的接口函数获取敏感数据，并进行签名。

(4) 签章页面签名及验证技术

在签名前，本文利用 SHA-1 算法，对从页面签名域中提取的信息取 hash 值，生成一个固定长度(160 位)的数据摘要，然后对这个摘要用私钥加密，生成签名信息。

验证部分，本文从摘要信息和数字签名两方面进行。当一个 Web 页面加入电子印章后，其摘要信息和数字签名都会被保存到签章控件中。在验证时，签章控件重新对 Web 页面提取摘要，并与签章控件中所保存的摘要信息进行对比。如果相同，则 Web 页面有效，否则 Web 页面被修改过。在进行数字签名验证时，签章控件重新对 Web 页面提取摘要，同时用公钥解密签章控件中的签名获取摘要，两者进行比较，根据结果判断页面是否有效。两个验证流程分别如图 2 和图 3 所示。

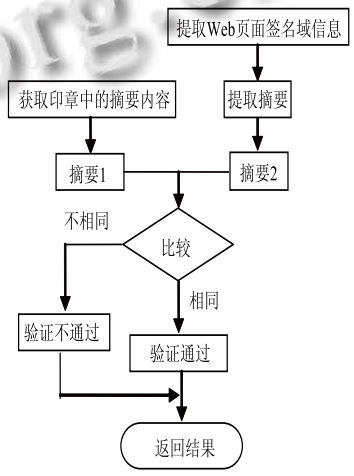

图 2 Hash 验证流程

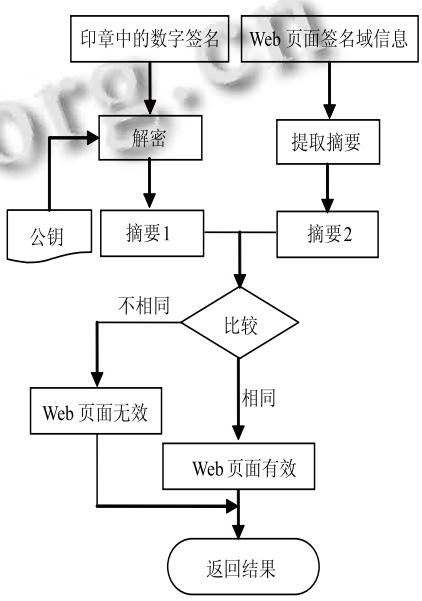

图 3 数字验证流程

(5) 签章页面的本地保存及打开技术

电子印章中不仅包含有印章图像信息，还含有签章者信息、数字证书及数字签名等信息。因此保存带有电子印章的 Web 页面到客户机时，除了要保存网页内容外，还要将印章的相关信息保存下来。本文采取将上述两部分内容分开处理，再将两者合并到一个文件。在保存网页内容方面，将 Web 页面保存为 MHT 文件。MHT 叫 Web 单一文件，将网页中包含的图片，CSS 文件以及 HTML 文件全部放到一个 MHT 文件里面。最后，将两个文件进行合并成一个数据流。另外，本文根据合并之后的数据流格式，设计了相应的阅读器来解析和打开文件。为了用户使用方便，采用资源编译工具 BRCC32.EXE，将阅读器编译成资源文件。保存时，将阅读器资源文件作为文件头，数据流拼接在尾部，合并保存到本地机上。打开时，双击本地文件，系统打开阅读器， 阅读器提取文件尾部的数据，并将 MHT 文件和印章数据分别解析出来，并在阅读器上以 WebBrowser 控件打开 MHT 文件内容，再调用页面中的 JS 函数，将印章签章到页面中。

(6) 签章页面的提交与加载

当一个页面加盖电子印章之后，用户提交页面时，除了要提交相应的表单数据外，电子印章也要进行提交。页面盖章时，签章控件把印章相关数据保存到临时文件中。当提交页面时，签章控件把临时文件中的印章数据传送给服务器保存。同样地，当用户打开含有电子印章的页面时，签章控件通过向服务器提交一个命令，服务器接收到之后，返回当前页面的印章数据，并由签章控件解析并显示印章。

4 应用实例

本文利用 Delphi7.0 实现 Web 签章控件，并将实现的签章控件应用于由 JSP 开发的电子合同签订系统，完成 Web 文档的盖章、提交、保存本地文件以及验证等功能。其主要有以下几个步骤：

(1) 控件的加载。首先，要在 JSP 网页中加载控件。JSP 页面中加载控件的代码如下为：

<object id="WebSeal" classid = "clsid:6FCDE4C1-F8DE- 453B-A2C8-5D871B6438E1" width=100% height=100%> </object>

(2) 打开页面，编辑 Web 文档。在网页浏览器中打开电子合同签订系统，输入网页表单内容。如图 4 所示。

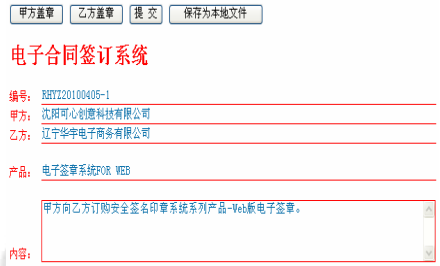

图 4　电子合同签订系统

(3) 盖章。完成 Web 文档编辑之后，点击盖章按钮，完成盖章操作。鼠标右键点击电子印章，会弹出菜单，如图 5 所示。用户可以选文档验证、印章锁定、印章解锁、撤销签章、数字验证以及查看数字证书操作。

图 5　盖章合同

(4) 文档验证。一旦 Web 文档内容被修改，印章上就会加上两条灰色的横线以表示当前文档已失效同时会给用户相应的提示，如图 6 所示。

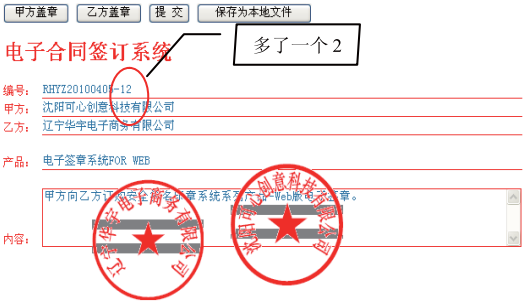

图 6　印章验证

（下转第 135 页）

图 4 生产早会系统数据显示界面

5 结语

本文在分析 CORBA 和 Web Services 的基础上，设计并实现了一种 CORBA 与 Web Services 的集成中间件，通过该中间件将基于 CORBA 的电能量管理系统扩展到 Internet 上，以供其他 Web 客户端（各种需要与电能量系统共享信息的应用系统）调用；从而实现了该分布式应用系统更大范围内的信息共享。

目前，无论国内还是国外，中间件这个领域都还处于深入研究阶段，需要在实际应用中做进一步的探索和改进，首先，对 Web Services 的查找是通过关键字匹配完成的，不能解析语义方面的差异，还需要对语义匹配方面进行研究；其次，对于系统的安全性考虑的不多，例如，如何对数据加密，建立安全的数据传输通道，确保数据传输的安全性和可靠性[8]。

然而，随着我国信息化程度的提高，异构电力应用系统方面的需求和应用将越来越多，本文的研究工作应当会有一定的参考意义。

参考文献

1 谢俊,段献忠,石东源.电力系统异构应用信息共享和互操作理论与方法研究.华中科技大学学报,2008,7:130−271.

2 IEEE Distributed Systems Online. [2010-06-21]. www.dsonline.computer.org

3 张驰,吴健,胡正国,周淑莉.CORBA 与 Web 服务的比较与集成.计算机工程与设计,2005,26(8):2213−2218.

4 OMG.CORBA to WSDL/SOAP interworking specification. OMG document number ptc. [2003-01-14].

5 朱亚光,刘峰,杨芳南.Web Services/CORBA 网关系统的研究与实现.微计算机信息,2006,22(5-3):85−88.

6 吴敏强,张潇.从分布式对象到 Web 服务.计算机科学,2002,29(11):12−15.

7 李华飚.Java 中间件技术及其应用开发.北京:中国水利水电出版社,2007.

8 朱斌,师春科,刘惠芳.CORBA 中间件在电力系统中的应用研究.计算机工程,2002,8:236−239.

（上接第 156 页）

(5) 文档的提交与加载。页面编辑和盖章完成后，提交给服务器。服务器接收数据，并将印章数据保存到印章数据库中，页面信息保存到业务数据库中。另外，签章控件还支持将带有电子印章的 Web 文档保存到本地，方便用户查看。

5 总结

本文在研究数字签名技术和 ActiveX 控件技术的基础上，实现了面向 Web 页的电子签章控件并将该控件应用于基于 Web 的电子合同签订系统，取得了较好的效果。该控件可应用于其他 Web 应用系统中，来保证 Web 页面完整性、不可否认性，具有较好的应用前景。

参考文献

1 袁晓宇,张其善.基于 EcDsA 的电子签章系统研究.计算机工程与设计,2005,26(5):1233−1235.

2 丁惠春,谷建华,张凡,等.面向电子政务应用的电子签章中间件设计与实现.计算机应用与研究,2005,2(3):135−137.

3 王飞,汤光明,孙怡峰,等.基于易损水印和数字签名的电子印章系统.计算机应用研究,2004,1(4):118−121.

4 张飞,肖刚,程振波.基于时间戳服务的电子签章验证方法研究.浙江工业大学学报,2009,37(3):300−305.