气象部门国产化电子签章云服务的设计与实现

王甫棣 王帅 汪芳

（国家气象信息中心，北京 100081）

摘要 通过在电子文档上加盖电子印章，可以满足政府部门电子公文流转过程的信息完整性、合法性和不可抵赖性的需求。气象部门在 2005 年开始在电子公文系统中推广电子印章应用，有效地加快了部门内部全流程电子化、提升办公效率。随着国家安全自主可控的发展战略和“互联网＋政务服务”的纵深推进，在气象政务管理信息系统集约化总体框架下，建设一套基于国产密码算法和国产版式文件的电子签章服务平台，通过云服务的方式为电子公文系统以及行政审批电子证照应用提供电子签章服务。该系统投入业务后运行稳定，显著提升了业务的安全性和可扩展性。

关键词 电子签章；国产化；自主可控；云服务；国密算法；版式文件

中图分类号：P409 **DOI**：10.19517/j.1671-6345.20210080 **文献标识码**：A

引言

推进电子政务是国家网络安全和信息化工作的重要部分，是全面深化改革、以信息化推进国家治理体系和治理能力现代化的重要途径[1-3]。电子政务办公已成为政府部门工作的标准方式。随着电子政务逐步深入的开展，为实现电子政务的无纸化办公目标，电子文档得到了大量的利用[4-5]，但也随之带来电子文档安全、完整、保密流转的安全需求。通过引入以数字签名技术模拟传统实物印章的电子印章技术，使用电子印章签署电子文档并关联签章人的数字证书便能有效降低办公电子文档的安全风险，还同时保留了与实物印章一致的管理和使用体验[6-8]。这个载入电子印章信息和签名信息数据的过程便称为电子签章[9]。

1 气象部门电子印章建设现状与需求

1.1 发展与现状

中国气象局从 2005 年开始推广使用电子印章应用，已经历 2 次换代升级。

2005 年，基于 Lotus Domino/Notes（IBM 公司的企业级通讯、协同工作平台）开发的中国气象局机关文档一体化系统正式启用第 1 代 SEP（Suresense Electronic Paper，书生电子文书）版本产品，实现的功能包括对 Microsoft Office（美国微软公司办公套件）文档版式转换、基于对称加密方式盖章等（图 1）。此时的电子印章制作采用本地管理方式，对应的签章身份验证方式使用 PCI（Peripheral Component Interconnect，外设部件互连标准）总线硬件加密卡[10]方式。随着全国气象宽带网[11-12]的建设推进，2012 年中国气象局建设并推广了国、省两级部署的

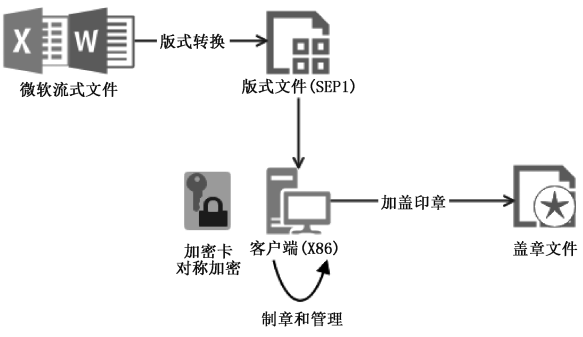

图 1 气象部门第 1 代版式文件（SEP1）电子签章应用流程

国家气象信息中心网络安全与“创新”技术研发创新团队（NMIC-202011-05）攻关任务、中国气象局 2017 年小型业务项目“国家级气象政务管理平台”项目资助

作者简介：王甫棣，男，1982 年生，正高级工程师，主要从事气象通信、Web 服务、电子政务方面研究，Email：wangfd@cma.gov.cn

收稿日期：2021 年 2 月 18 日；定稿日期：2021 年 4 月 22 日

综合管理信息系统[13]并延续了第 1 代电子印章应用,虽然进行了印章管理功能的升级迭代,但此时的单机运行模式的电子印章仍然存在终端的运行环境高依赖性,较高的制章管理应用成本以及对称加密方式的低安全性等问题。

随着气象宽带网能力进一步增强,2016 年国家级一级集约部署的气象政务管理系统(简称“气政通”)开始建设。以集约化部署为特征的第 2 代的电子印章系统投入应用,通过集中制管中国气象局、局直属单位、各省市县等各级单位电子印章,有效减少了单机模式的应用成本。如图 2 所示,这个时期的电子印章升级支持了非对称加密算法 RSA2048 的增强型第 2 代 SEP 版式文件印章格式,主要服务于气政通电子公文系统,安全性得到一定增强。如图 3 所示,将电子印章管理的核心功能程序嵌入到现有气政通电子印章管理系统中,在电子公文系统中直接以 OCX(Object Linking and Embedding (OLE) Control Extension,对象链接和嵌入用户控件)控件方式调用公文处理核心功能完成文件的加密、盖章、分发、打印、浏览等操作。

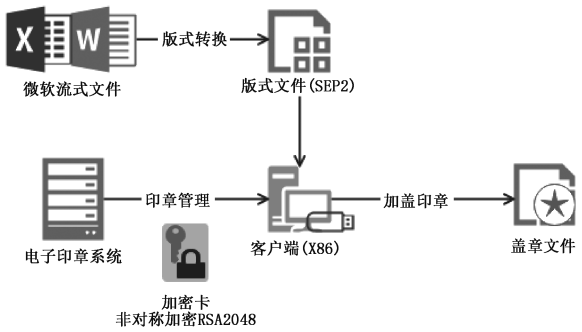

图 2　气象部门第 2 代版式文件(SEP2)电子签章系统应用流程

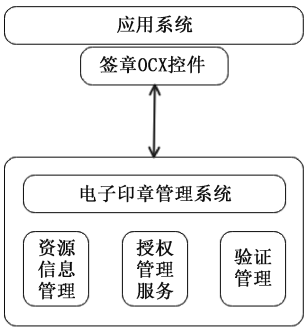

图 3　气象部门第 2 代电子签章应用模式

OCX 是一种可以由在 Windows 操作系统中运行的应用软件创建使用的特殊用途的程序。应用 OCX 可以很快地在各类应用程序中加入特殊的功能,比如公文系统中通过 OCX 的方式可以很好地融合电子公文处理流程与电子签章的功能。但是 IE 浏览器可以通过脚本语言调用控件,利用控件的属性设置进行操作系统注册表读写或者本地文件系统的操作,具有极大的危害性。由于 OCX 控件仅在 Windows 环境应用,这对于操作系统环境和版本的依赖也制约了应用的兼容扩展性。

另一方面,此时的电子印章的用户身份信息以 USBKEY 介质存储,独立于中国气象局整体身份认证(CA)体系,可扩展性和可维护性依旧不高。

1.2　应用需求

为深入推进“互联网+政务服务”,推进“放管服”改革,全面提升政务服务规范化、便利化水平,2018 年底,全国一体化在线政务服务平台加速推进。按照全国一体化平台数字证书认证相关标准规范,为了实现数字证书跨地方跨部门互信互认,需要改造支撑电子印章,以实现与部门内、外统一的身份认证体系对接。除了电子公文系统外,行政审批各类文书和证照也需要引入电子签章,这不仅对气象部门电子签章的功能提出了新的需求,也对其应用的可扩展性和灵活性提出了较高要求。同时,伴随着当今国际形势的发展,国家又提出基础软件产品“安全可靠,自主可控”的发展方针,大力提倡使用国产加密算法(SM 系列算法),应用国产 OFD 版式(Open Fixed-layout Document,开放版式文档)文件。这些需求都亟待通过新一代的国产化电子签章系统建设得以解决。

2　第 3 代电子签章系统应用技术

2.1　国产 OFD 版式技术

OFD 标准是由国家主管部门牵头制订的公开、公正、自主可控格式,使中国版式文档行业摆脱了对国外技术标准和私有标准的依赖,是对 PDF 标准的替代[14]。它基于 XML(Extensible Markup Language,可扩展标记语言)和压缩技术(ZIP 格式以及 Deflate 压缩算法),借助 XML signature(一个定义数字签名的 XML 语法的 W3C 推荐标准)实现安全控制。OFD 文件为多个 XML 关联文件打包形成,对 OFD 文件的签章过程即为通过增量修改方式向

OFD 文件中添加可视化印章数据和电子签章的过程。

OFD 标准加强了安全性控制，加强了对加密和数字签名机制的支持，对脚本和可执行程序的限制更严格。除了兼容国际同类技术标准外，还针对国内电子文件的处理需求，内置相应特性支持，包括加密、签名、权限控制、元数据管理等，基本满足了对电子文件进行全程统一管理的要求。

2.2 国产密码技术

要实现电子签章的对外服务和互信互认，除了需要具备统一的电子签章格式外，还需要满足签名算法、消息摘要算法（又称译杂凑算法、哈希算法）的一致性条件[15]。根据国家密码管理局颁布的 GM/T0031—2014《安全电子签章密码技术规范》，电子签名数据应符合 GM/T0009《SM2 密码算法使用规范》，需要应用 SM2 非对称密码算法作为数字签名算法，使用 SM3 作为消息摘要算法。

为确保原始 OFD 版式文件的真实性和完整性，签名对象应包含所有内容和资源的整个 OFD 文件摘要值[16-17]。授权用户对 OFD 文件进行签章时，系统计算出摘要值和签名值，组装成签章数据并添加到 OFD 文件中，签章过程结束。通过获取签章 OFD 文件的签名描述文件和电子签章数据，并与该 OFD 文件内容和资源的摘要数据进行比对，以验证签章的真实性，此为验章过程。

2.3 Web 服务

Web 服务提供一种基于标准的方法用来支持跨平台程序对程序之间的通信，可以有效解决原有集成技术在远程通信方面的问题[18-19]。这种分布式应用思想在气象大数据云平台建设得到充分体现，通过将各类数据管理功能以服务的形式发布，为不同租户提供“数算一体”的平台化服务，全面支撑“云＋端”的气象业务，构成集约化、标准化、发放发展的气象新业态，即 SaaS（Software-as-a-Service，软件即服务）。

遵循气象大数据云平台的体系，利用气象统一基础资源池设施[20-23]，气象政务管理平台为实现各类应用系统的统一用户、统一认证、统一消息服务提供了服务基础支持和标准化管理。作为一项公共服务，统一的电子签章服务也应纳入气象政务管理平台并为各类应用提供支撑。

3 电子签章云平台设计

3.1 总体设计

为了保证业务系统用印业务功能的稳定接入和规范管理，电子签章服务平台以云服务方式为需要进行签章的各级用户和各类应用系统提供基础服务，业务系统可以通过 Web 服务调用方式接入，无需进行底层复杂的电子印章、签章接口调用，即可实现文件签章、文书打印输出、文件浏览、打印份数控制、验章等功能，瘦客户端方式也有助于快速适配国产化终端环境的应用，提升安全性的同时解决应用的可扩展性问题[24]。

如图 4 虚线框部分所示，对比第 2 代电子签章系统应用模式，本次建设的电子签章服务平台以松耦合方式提供应用服务，解决了原有 OCX 控件方式的应用强绑定以及安全性问题。同时，接入气象部门统一政务 CA 体系，应用证书加密的方式对接信任服务体系，将电子印章存储在移动介质上并且绑定用户 CA 证书，为签名的互信互认应用扩展和身份管理安全审计提供必要的支持。

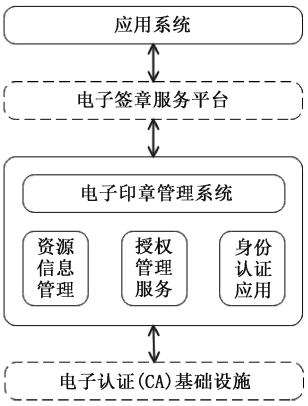

图 4 气象部门第 3 代电子签章应用模式

电子印章管理系统基于信任服务体系、电子认证基础设施，提供电子印章基础服务，制章业务，签章、验章服务接口，密码运算能力以及信任服务体系支撑。电子签章服务平台为需要进行用印签章的业务系统提供了一个基础云服务，可实现文件签章、文书打印输出、文件浏览、打印份数控制、验章等功能。如图 5 所示，在整体国产化环境下，各收发文终端，通过可编辑软件起草文件，经过流转、审核并定稿后，将 WPS（Word Process System，金山公司国产

化流式文件编辑工具)文件转换生成 OFD 版式文件。电子公文系统将调用电子签章服务,完成对 OFD 文件的签章和验章功能。收文单位接收来文后,对 OFD 文件进行浏览、验章、反馈、打印及操作。

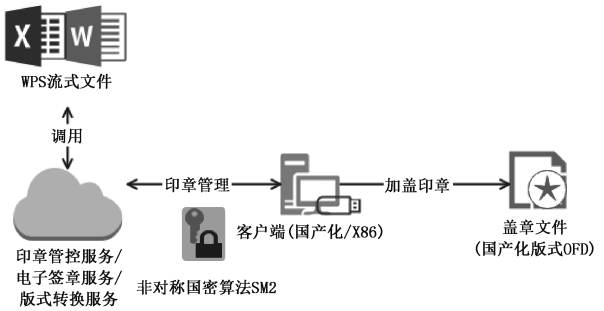

图 5　气象部门第 3 代版式文件(OFD)电子签章应用流程

3.2　流程设计

构建电子签章服务平台一朵“云”,支撑各类已有业务应用多个“端”用印的整体流程,如图 6 所示。在需要加盖电子印章的时候通过访问电子签章系统的签章组件服务接口实现电子印章的加盖,电子印章在整个生命周期都受到电子签章系统的监督和管控;而印章的具体使用则由印章的具体使用单位通过业务系统来实现管控,电子签章系统负责印章的制发管理、有效性管理、印章使用日志管理。

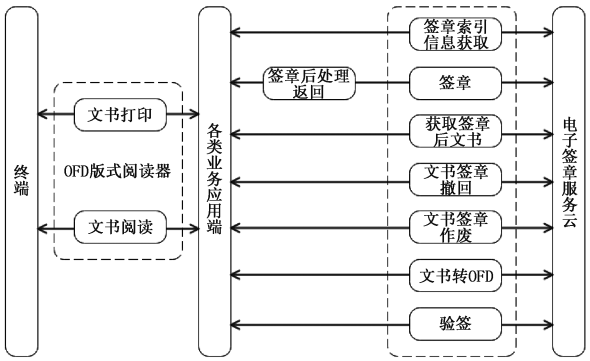

图 6　电子签章云+端服务对接流程

所有云端的 Web 服务接口均以 JSON 格式的数据信息进行传递,相关盖章文书以 HTTP 协议向应用端进行传输,整体云服务各类服务场景流程设计如下:①业务系统提供“用印后处理返回”服务给签章服务平台调用,签章服务平台通过调用此服务回传用印后的文书文件;②签章服务平台提供“用印索引信息获取”服务给业务系统调用,业务系统通过调用此服务获取当前用户可用的印章列表;③印章系统提供“用印”服务给业务系统调用,业务系统通过调用此服务传入待用印文书信息及文书文件;④签章服务平台提供“获取用印后文书”服务给业务系统调用,业务系统通过调用此服务获取印章系统用印后的文书文件;⑤签章服务平台提供“文书用印撤回”服务给业务系统调用,业务系统通过调用此服务撤销之前发起的用印操作;⑥签章服务平台提供“文书用印作废”服务给业务系统调用,业务系统通过调用此服务作废已用印的文书;⑦签章服务平台提供“验章”接口给业务系统调用,业务系统通过调用此服务验证已用印的章的合法性;⑧签章服务平台提供“文书转 OFD/PDF 文件”服务给业务系统调用,业务系统通过调用此服务将文书文件转换为指定格式的文件,实现用印前的预览功能;⑨阅读器提供“文书打印”接口给业务系统调用,业务系统通过调用此接口打印已用印后的文书,并支持设置打印份数;⑩阅读器提供“文书查看”接口给业务系统调用,业务系统通过调用此接口预览文件。

3.3　安全设计

在一个云化环境服务对电子签证服务提出了更高的安全性要求,结合整体气象政务管理平台安全体系,主要从 3 方面增强系统安全性:①安全审计。电子印章系统及签章平台采用包括系统管理员、安全保密员和安全审计员的 3 员管理策略,以及 3 员权限分立的制衡机制。系统管理员负责系统设置及用户的创建,安全保密员负责用户的授权,安全审计员负责日志检查。②加密传输。存储在设备上的印章数据以密文的方式存储,密钥由印章拥有者所有,呈现形式为印章口令。在制作印章的时候,对用户设置的印章口令进行变换得到密钥,调用商密算法 SM2 加密算法完成对印章数据加密。通过商密对称算法 SM3 保证印章数据的安全性,密钥通过口令变换,没有密钥分发过程。③权限控制。为确保系统的安全,需要对系统中的每一用户或与之相连的服务器或终端设备进行有效的标识与鉴别,只有通过鉴别的用户才能被赋予相应的权限,进入系统并在规定的权限内操作,利用 CA 证书实现用户身份的鉴别。

通过以上不同 Web 服务场景的建设,使得电子签章服务具有灵活特性,可根据不同业务场景(比如行政审批 8 类不同事项的电子印章、电子证照服务)

或者不同终端类型(传统 X86 体系以及国产化终端)进行快速适配。

4 业务应用

4.1 应用功能

采用统一的、标准的服务接口方式,有效降低各类需要应用签章服务系统的对接难度。提供接入申请的审批、备案、注册管理以及统一用户身份认证功能。满足电子签章的 3 种场景:①直接登录平台进行统一批量用印;②在业务系统内远程调用签章页面进行盖章;③静默调用平台底层接口完成指定位置、指定公章名称进行盖章,然后把盖章后的文件返回给业务系统。

实现的应用功能包括:①系统接入审批备案。平台提供了对签章应用系统接入申请的审批、备案、注册管理,签章管理员对应用系统进行签章授权配置管理,设置应用系统对签章服务平台中相应签章调用的权限,授权其可调用的印章列表。②用户认证。电子签章服务平台与 CA 身份认证服务系统对接,实现了统一用户身份认证。③签章服务。签章处理人根据业务系统发送的签章文件信息、领导审批单,根据业务系统指定的印章编号(或印章名称)与电子印章在线服务系统对接,经过身份鉴别后,根据签章人权限获取印章,返回电子印章数据;电子签章客户端提供对接签章运算接口,经过身份鉴别后,进行签章运算,返回电子签章数据,进行签章操作,签章完成后,系统自动调用时间戳服务进行日志记录。签章操作支持批量签章、联合签章等。④验章服务。电子签章服务平台与电子印章发布验证系统对接,提供签章验证对接接口,进行电子签章验证,完成电子签章验证的验证流程。系统提供 2 种验章服务:在线验证,提供在盖章前的电子印章在线验证功能和签章后电子印章的验证功能;离线验证,提供对签章文件离线验证功能。⑤日志服务。系统提供注册申请日志,记录应用系统签章申请注册、审批、备案日志;签章申请日志,记录应用系统签章申请日志;签章用印日志,记录应用系统签章受理日志。

4.2 应用场景

如图 7 所示,除了在气政通电子公文系统的应用外,气象行政审批平台是电子签章服务的另一重要应用领域。

按照国家一体化政务服务平台电子印章相关标准规范,部门的行政审批平台需要建立电子印章系统,完成与国家平台统一电子印章系统对接,同时实现中国气象局及下属各机关单位电子印章的统一管理,使整个系统所辖的公章、部门章以及行政审批专用章的有效管控,为各种业务应用系统提供签章与验章的应用支持,以及监控系统内所有电子印章使用情况。

采用云服务的方式,可以灵活快速地根据国家平台接口标准快速实现系统注册(电子印章制作系统和状态发布系统注册)、制作主体注册(电子印章制作主体注册和信息推送)、制作系统对接(电子印章信息备案)、状态发布系统对接(电子印章状态信息推送和状态信息查询)、CA 互认互信对接等接口,并将接口信息补充到印章管控服务中,通过电子外网通道实现部门行政审批平台与国家政务服务平台印章数据的互信互认。

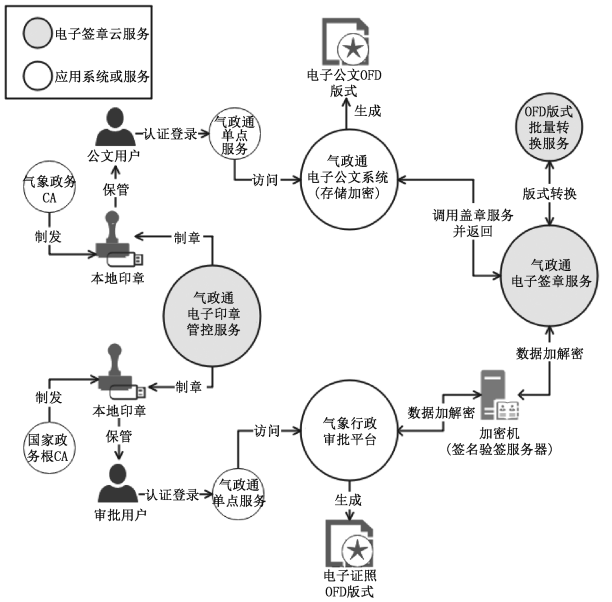

图 7 国产化签章云服务应用场景

4.3 应用效果

2020 年 5 月,支撑气象行政审批平台的电子印章服务正式部署上线,提供审批服务电子印章的制作、发布、电子证照的签章、数据共享等功能,目前已实现国家级 3 个事项(42008 气象专用技术装备使用审批(含人工影响天气作业设备)、42010 外国组织和个人在华从事气象活动审批、42006 气象台站迁建审批)的审批流程和处理要求,以及电子签章、电子证照数据推送国家政务服务平台的功能。

2020 年 12 月,气象部门国产化电子签章云服务正式适配国产化终端操作系统的气政通电子公文系统也投入业务运行。经过反复测试证明,对非区域中心省级的县级气象部门电子签章签发平均响应时间小于 3 s,可满足业务需求。同时,该签章服务可以实现文件盖章时在版式文件 OFD 中通过可视化拖拽指定盖章位置,完成盖章操作,整体电子签章系统产品既满足在国产操作系统下(统信 UOS 或者麒麟 OS)的适配盖章,同时满足与 Windows 操作系统的互认互信。

5　结论与讨论

建设集印章、签章、转换、审计、管理为一体的气象部门电子签章云服务平台,大大减少了部署、实施、维护的成本,同时支持多种版式格式的签章以及多种签章方式的应用,为电子公文系统、行政审批平台对电子印章使用场景提供全面支撑,有效促进部门无纸化办公的发展。通过基于国产算法的 OFD 版式文件电子签章系统的应用,推动了国产版式文件技术、国产密码算法事业的发展。

未来,还将继续推动电子签章服务对省级以下事项的应用推广。同时,还需要开展签章云服务基础设施的国产化适配工作,满足在国产化数据库、Web 中间件的部署应用,进一步提升自控安全性。

参考文献

[1] 沈文海.“智慧气象”内涵及特征分析[J].中国信息化,2015(1):80-91.

[2] 杨道玲.我国电子政务发展现状与“十三五”展望[J].电子政务,2017(3):58-65.

[3] 王甫棣,王帅,赵希鹏.气象部门管理信息化系统设计初探[J].信息技术,2019,43(3):156-160.

[4] 朱庆刚,马璧玉.电子政务与办公自动化初探[J].电脑知识与技术(学术交流),2007,3(5):1362-1363.

[5] 曹炀.云端电子签章技术[J].中国建设信息化,2016(24):75-76.

[6] 覃克服.电子签章运用的两种技术[J].广西大学学报(哲学社会科学版),2002,24(5):46-46.

[7] 谢淑翠,武瑞瑞.电子签章技术在电子政务中的应用[J].信息通信,2012(5):97-98.

[8] 吴皓文.上海市电子政务云电子印章公共服务云平台架构设计[J].信息通信,2019(6):86-87.

[9] 密码行业标准化技术委员会.GM/T 0031-2014 安全电子签章密码技术规范[S].北京:中国标准出版社,2014.

[10] 利佩贤,林海丹,陈永建.基于 PCI 总线加密卡的设计与实现[J].微计算机信息,2005,21(10-2):147-149.

[11] 林润生,孙周军,谭小华,等.新一代国内气象通信系统设计与实现[J].气象,2011,37(3):356-362.

[12] 郎洪亮.全国气象宽带网络系统体系结构研究[J].气象科技,2006,34(增刊 1):1-4.

[13] 戴纲.中国气象局综合管理信息系统的性能优化实践[J].内蒙古气象,2012(6):40-42.

[14] 胡荣磊,左珮良,蒋华.版式文档 OFD 签章模块的研究与实现[J].信息技术,2016(8):76-80.

[15] 许盛伟,张珍珍,崔敏龙.电子印章系统的互信互验关键技术研究与设计[J].计算机工程与设计,2016,37(7):1777-1780+1835.

[16] 王聪,李海波,丛培勇,等.国家版式文档格式规范(OFD)中的技术方案[J].信息技术与标准化,2012(9):19-21.

[17] 密码行业标准化技术委员会.GM/T 0031-2014 安全电子签章密码技术规范[S].北京:中国标准出版社,2014.

[18] 王甫棣,林润生,胡英楣.基于 Web 服务的气象数据服务[J].计算机工程,2009,35(8):280-282.

[19] 郝江波,唐卫,王慕华,等.基于微服务的气象信息决策支撑系统重构与实践[J].气象科技,2020,48(6):53-59.

[20] 沈文海.从云计算看气象部门未来的信息化走向[J].气象科技进展,2012,2(2):49-56.

[21] 华连生,唐怀瓯,王根,等.安徽省气象业务资源池设计与应用[J].气象科技,2017,45(2):269-275+297.

[22] 王甫棣,赵希鹏,王帅.基于 SOA 的任务调度框架的设计与实现[J].气象科技,2020,48(3):362-367.

[23] 许皓皓,姚日升,沃伟峰.标准化气象数据服务接口设计与实现[J].气象科技,2018,46(4):685-691.

[24] 李强,高超航,何智,等.一种基于区块链的电子签章验证平台设计[J].信息安全研究,2019,5(12):1089-1095.

Design and Implementation of China Meteorological Administration E-signature Cloud Service in Nationalization Environment

WANG Fudi WANG Shuai WANG Fang
(National Meteorological Information Centre, Beijing 100081)

Abstract: By stamping the E-signature on the electronic documents, it can meet the needs of information integrity, legitimacy and non-repudiation in the process of electronic office documents of government departments. In 2005, China Meteorological Administration began to promote the E-signature application in the electronic official document system, which effectively accelerated the whole electronic process within the China Meteorological Administration and improved the management efficiency. With the development of independent and controllable national security and Internet Plus government services, the E-signature service platform based on domestic cryptography and domestic format documents is built under the overall framework of the meteorological administration information system. The system provides electronic signature services for electronic document systems and administrative approval electronic certification applications through cloud services. The system runs stably in operation and improves the security and scalability of the business significantly.

Keywords: E-signature; nationalization; self-control; cloud service; national secret algorithm; format documents