浅谈电子签名技术的优势和隐患

高 亮 温 娜 王淑敏
（中国标准化研究院）

摘 要：电子信息化的发展，推动着人类进入了信息化时代，无纸化办公操作越来越深受人们的喜爱，电子签名技术的出现，逐渐代替了传统的手写签名。而数字签名作为电子签名技术中最常见和最安全的一种形式，被广泛用于保护电子文档和交易的安全。本文深入分析电子签名技术的涵义，对电子签名技术的分类进行逐一描述，着重分析以数字签名为代表的电子签名的情况，探讨了电子签名技术的优势和隐患。

关键词：电子签名，数字签名，优势，隐患
DOI编码：10.3969/j.issn.1674–5698.2024.07.011

On the Advantages and Hidden Dangers of Electronic Signature Technology

GAO Liang WEN Na WANG Shu-min
（China National Institute of Standardization）

Abstract: With the development of electronic informatization, human beings have entered the information age, and paperless office operation has become more and more popular. The emergence of electronic signature technology has gradually replaced the traditional handwritten signature. As the most common and safest form of electronic signature technology, digital signature is widely used to protect the security of electronic documents and transactions. This paper provides an in-depth analysis of the meaning of electronic signature technology, and describes the different classification of electronic signature technology one by one. It focuses on the analysis of electronic signature represented by digital signature, and discusses the advantages and hidden dangers of electronic signature technology.

Keywords: electronic signature, digital signature, advantages, hidden dangers

0 引言

随着我国经济的飞速发展，国内IT行业的发展速度以超过国际上各个国家的3~4倍快速增长，而电子签名技术为我国各个部门、行业、企业等信息化的发展给予了极大的帮助。当下中国顺应全球化的潮流，积极投身于全球性的交流与竞争。如何增强中国政府部门的工作效率？如何在中西方国家之间顺利地开展政治、经济、文化的交流和贸易往来？诸如此类问题需要电子商务和电子政务系

基金项目：本文是国家市场监管总局科研条件专项资金项目“面向多边贸易合作的技贸措施研究能力建设”（一期）（项目编号：[2060503]150019000000210006）研究成果。

作者简介：高亮，工程师，硕士研究生，研究方向为数据与知识工程相关技术标准化。
温娜，高级工程师，博士，研究方向为数据与知识工程相关技术标准化。
王淑敏，助理研究员，硕士研究生，研究领域为知识管理与知识产权标准化。

统提供方便的手段，而这些电子系统的完善离不开电子签名技术。

1 电子签名技术的概述

1.1 电子签名的概念

宏观来说，电子签名[1]即所有不是以传统方式的手写签名或者盖章的形式签订文件，而是在数据电文中确定签署人身份及确保签字人认可电文中的信息。而微观来说，电子签名就是在PKI体系的基础上进行的数字签名。

首先，介绍下传统签名[2]的概念，在商务交流的活动中，为了确保双方交易过程中的安全性，在签订合同协议或公文要事的时候，要求其当事人或者代表人物签名、盖章，在此前提下，交易的两者可以明确签订的合同协议的具体内容，保证签订的人承认合同协议的内容，这样该协议的合法性得到了保证。

然后，解释下电子签名的概念，在电子商务的互联网信息化时代，合同协议或者签署文件是以电子文档的形式进行传递的。但是，在电子文档中，手写签名无法操作，此时，在电子文件中若要实现与传统签名同等效果则需提供必要的技术手段进行操作。所以，电子签名的涵义也随之出现，即在电子文档中证明两者交易人的身份，以此来保障合同协议的可靠与真实，同时其作用与传统的手写签名一致，称为电子签名。

1.2 电子签名的分类

当前在法律上承认的合法的电子签名方式大致可以分为两大类：数字签名和生物特征识别技术签名。

数字签名[3]是基于PKI公钥密码技术的电子签名技术，是目前比较成熟的世界先进国家普遍使用的电子签名技术。所以，目前使用的电子签名技术中，一般指的就是“数字签名”。美国的相关部门在电子签名标准中（DSS，FIPS186-2）对数字签名作了如下解释：“利用一套规则和一个参数对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性”。

生物特征识别技术签名[4]主要以静态和动态两种形式相结合进行表达。静态生物识别方式主要以指纹、面部识别为代表，该识别方式本身具有客观存在的性质，仅能表达签署人的身份信息而无法确认签署人的认同意愿；这时就需要结合动态行为来确定一份合同的有效性，即签字的笔迹，该行为具有一定的主观表达意愿的优点，于是静态和动态行为的结合成为了电子签名身份确认和行为确认的最佳方案。

1.2.1 数字签名技术

数字签名在国际标准化组织的ISO 7498-2标准中定义[5]为：“附加在数据单元上的一些数据，或者是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如：接收者）进行伪造”。

数字签名技术是基于PKI（公钥基础设施）的电子签名[6]，PKI运用非对称密码算法原理，采用公钥和私钥结合的方式，公钥对外公开，私钥由个人保存。使用数字签名时，发送者对数据运用公钥加密，生成加密文件，然后，接收者运用私钥解密，若解密后的文档与原始数据一致，则验证通过。

总结而言，数字签名技术是当下现代化的电子签名技术，该技术通过使用非对称密钥算法对原始数据进行处理，能够很好地替代传统的手写签名。该技术具有身份认证、数据安全、传输稳定等优势。而基于PKI的数字签名技术是目前广泛使用且技术成熟的电子签名技术，提供了多种在线安全服务。

1.2.2 生物识别技术

生物识别技术其原理是利用人体生物特征行为进行身份认证，生物特征因其本身每个人不同的表征特性，可以进行测量、自动识别和验证的操作。

生物识别系统的操作分三步进行，首先，采集人体的生物特征行为，将取得的信息数字化处理；然后，将数字化信息转换成数字代码；最后，将这些数字代码经生物识别系统处理为特征模板并保存在生物识别数据中。当进行身份认证时，只需将信息在数据库中进行比对即可确定信息是否匹

配，从而确定是否是本人或负责人。

生物识别技术[7]主要有以下几种。

（1）指纹识别技术[8]。不同人的指纹各不相同，并且每个人的指纹是一生不变的。而指纹识别技术的原理是采用比对匹配的方法，对此人的指纹与生物识别系统数据库中的信息进行匹配，即可得出该人的身份信息。在确认身份后，将相关的材料或电子数据电文按手印验证。缺陷是需要庞大的数据库进行操作，一般用于现场办理，线上办理存在一定的困难。

（2）视网膜识别技术[9]。视网膜识别技术有精度较高的特点，作为一种极其稳定的生物特征信息，其原理是利用激光技术采集人类眼球信息，然后经过视网膜识别技术的处理后储存在信息库中。缺陷是使用复杂，不适合线上办理。

（3）声音识别技术。声音识别技术采集的是人类行为信息，其原理是使用声音录制设备记录声音波形信息，再进行频谱分析，经数字化处理后储存在数据库中。在使用该技术时，将采集到的现场声音波形信息进行频谱分析，并与数据库中预先存储的声音模板进行比对，以识别该人的真实身份。缺陷是精确度较低、使用复杂，因此不适用于直接数字签名和网络传输。

总结而言，以上3种生物识别技术适用于现场办理的情况，不适用于远程网络线上认证及大规模人群认证。

2 电子签名技术的优势

（1）数字签名实现了签名者不能否认签名的客观存在，同时确保接收者能够验证数字签名的真实性，有效防止他人造假签名[10]。另一方面，电子签名提供身份认证，确保邮件发送者的身份可信。借助数字证书，电子签名可以验证发送者的身份，防止身份冒用和欺诈行为的发生。

（2）电子签名可以保护邮件的完整性，保证邮件在传输过程中没有被更改。数字签名由于基于密码学技术，能够保护数据的完整和真实，避免伪造和篡改[11]。在电子邮件中，数字签名可以用来验证邮件发送者的身份，并确保邮件没有被篡改或修改过。

（3）电子签名具有不可抵赖性[12]，即发送者无法否认自己发送了该邮件。这是由于电子签名的实现是基于私钥加密的，只有发送者的私钥才能生成有效的数字签名，因此发送者无法否认发送过程中的任何细节。

（4）电子签名提高了邮件的安全性和机密性，有效地防止邮件内容被未经授权的人员访问和泄露。与传统的手写签名相比，数字签名提供了更为安全的保障机制，确保数据的完整性和真实性。通过数字签名，可以验证数据的真实来源，并确保在从源头到目的地的传输过程中未发生数据篡改，从而大大提升了签名的安全性水平。

（5）相对于手写签名，数字签名更精确地实现了签名的不可仿造性。通过伪造虚假的数字信息进行签名，从计算的角度来看都是不可行的。数字签名使用了复杂的加密算法和数学原理，使得任何未经授权的人都无法有效地伪造或篡改数字签名，确保签名的真实性和可靠性。

（6）数字签名确实可以实现防重放功能。当在数字签名的交易过程中，交易双方签订的协议，可通过数字签名的流水号或时戳技术避免双方抵赖，确保了签名行为的独特性和唯一性，有效地避免了重复利用签名文件造成的问题。

3 电子签名技术的隐患

（1）私钥的安全性是电子签名的关键[13]。若私钥被泄露或被别人获取，那么电子签名的有效性将受到威胁。因此，保护私钥的安全非常重要，需要使用安全的存储设备或加密算法来保护私钥的机密性。

（2）电子签名技术依赖于数字证书的有效性。如果数字证书被伪造或过期，那么电子签名的可信度将受到质疑。因此，数字证书的可靠性和有效性是至关重要的。

（3）数字签名需要相关的法律条文来支持以达到一定的合法性。比如：政府的立法部门应该对

数字签名提高重视度，立法部门应加快立法的脚步，制定有关电子签名的法律，保证数字签名技术的特殊鉴别作用。

（4）数字签名技术的时效性与以往的关键人物脱离不开[14]。比如：原先拥有权限的人在使用数字签名后离开组织，再访问原先的信息需要先前拥有权限的人操作，给协议流程的操作带来了困难。

（5）数字签名技术是基于网络系统进行操作的，系统可能存在漏洞与被入侵的可能性。数字签名技术建立在公钥密码体制的基础上，依赖于良好的管理机制和安全的技术实现。当私钥持有人不知情的情况下，黑客窃取私钥，合法用户的利益就容易受到侵害。

（6）数字签名技术可能被不法用户利用[15]。他们可能使用欺诈手段来终止合同的有效执行。这种情况虽然不常见，但确实存在潜在的风险。不法用户可能会利用伪造的数字签名或其他欺诈手段来声称合同是无效的，以此推翻签署的合同并试图逃避合同责任。这可能导致合同的执行受阻或出现争议。

4 总结

实践证明，电子签名技术在各个领域均有广泛的应用，并受到众多用户的喜爱。这些技术为使用者提供了最人性化的便利，取代了传统纸质签名的复杂流程，大大提高了人们的办公效率。在政府的电子政务系统中，电子笔迹和签名技术可以用于实现文件的数字化和电子化处理，提高办公效率和信息交流的安全性；在金融领域的安全信用应用系统中，通过电子笔迹和签名技术，可以实现用户身份验证、交易授权和风险评估等功能，确保交易的安全性和可靠性；在企业信息化的众多应用中，电子笔迹和签名技术可以用于合同签署、审批流程控制等方面，简化企业内部流程，提高管理效率。

总之，电子笔迹和签名技术在各个领域都能够带来便利和效益，提高工作效率、降低成本并提升安全性。随着技术的不断发展和普及，这些应用将会得到进一步的扩展和深化。

参考文献

[1] 卜凡金. 电子签名的技术实现及申领方式简述[J]. 信息技术与信息化, 2005(03):156-159.

[2] 电子签名技术提高效率服务中国信息化[J]. 办公自动化, 2003(07):39.

[3] 胡建宏,胡斌彦. 电子签名技术研究综述[J]. 卫生职业教育, 2007(10):155-157.

[4] 刘振翼,李玎. 电子签名技术在公证中的适用[J]. 中国公证, 2023(02):64-67.

[5] 陈琳. 关于电子签名技术的研究及应用[J]. 佛山科学技术学院学报(自然科学版), 2014,32(02):40-43+75.

[6] 刘蓓辉. 计量检测中的无纸记录和电子签名技术研究[J].电子制作, 2017(06):18-19.

[7] 徐阳. 前景光明的电子签名技术[J]. 中国标准导报, 2001(04):32.

[8] 张建莉. 浅谈电子签名技术[J]. 档案管理, 2007(05):73.

[9] 路菊苓. 浅谈数字签名技术的优势和隐患[J]. 中小企业管理与科技(上旬刊), 2014(03):306.

[10] 王金彦. 浅谈数字签名技术的优势和隐患[J]. 中小企业管理与科技(下旬刊), 2013(03):227-228.

[11] 程朝辉. 数字签名技术概览[J]. 信息安全与通信保密, 2020(07):48-62.

[12] 鱼双键. 详解数字签名[J]. 科技情报开发与经济, 2006(02):215-216.

[13] 张丽. 电子签名、数字签名及强化电子签名[J].北方经济,2005(14):67-68.

[14] 肖攸安,李腊元. 数字签名技术的发展[J].交通与计算机,2003(02):6-9.

[15] 王森. 数字签名技术在网络安全中的应用[J].电子测试,2019(06):66-67.