电子商务身份认证标准化技术研究

刘东华

（中国标准化研究院国家标准馆）

摘　要：本文旨在深入探讨当今电子商务信息安全领域中的标准化身份认证技术，着重分析了基于零知识证明理论的身份认证技术。针对WebOA办公系统在身份认证方面的独特需求和安全性标准，我们引入了零知识证明的理念。本文详细展示了这一改进方案的具体身份认证过程，并全面分析了其在安全性方面的独特优势。

关键词：WebOA，身份认证，零知识证明

DOI编码：10.3969/j.issn.1674-5698.2024.07.009

Research on the Standardization Technology of E-commerce Identity Authentication

LIU Dong-hua

（National Library of Standards, China）

Abstract: This paper aims to explore the standardized identity authentication technology in the field of e-commerce information security today, with a focus on analyzing identity authentication technology based on zero knowledge proof theory. It introduces the concept of zero knowledge proof to address the unique needs and security standards of WebOA office systems in identity authentication. It provides a detailed presentation of the specific identity authentication process of this improved solution, and comprehensively analyzes its unique advantages in terms of security.

Keywords: WebOA, identity authentication, zero knowledge proof

0 引言

在数字化时代的今天，电子商务已经成为全球经济的重要组成部分。随着越来越多的业务迁移到在线平台，用户的身份认证变得至关重要。身份认证是验证用户是否具有访问特定资源或执行特定操作的权限的过程。在电子商务中，身份认证不仅关系到用户的安全和隐私，还直接影响到在线交易的信任和可靠性。

电子商务身份认证涵盖了各种技术和方法，包括传统的用户名和密码认证、生物特征识别认证、证书和公钥基础设施（PKI）认证、多因素认证、单点登录（SSO）系统以及匿名认证技术[1]。这些技术的不断演进和创新，使得用户体验更加便捷，但也伴随着安全威胁和隐私风险的增加。

在这一复杂的背景下，标准化身份认证技术变

基金项目：本文受中央基本科研业务费项目“基于数字孪生的国家数字标准馆建设关键技术研究及验证”（项目编号：252024Y-11460）资助。

作者简介：刘东华，硕士研究生，研究方向为高新技术及信息技术领域的标准化研究。

得至关重要。然而，电子商务身份认证标准化领域存在许多挑战。快速发展的技术和不断变化的威胁使得标准化变得复杂而困难。此外，不同国家和地区的法规和隐私要求也增加了标准化的复杂性。

本文深入探讨电子商务身份认证标准化技术，并分析其对电子商务安全性和可信度的影响。回顾身份认证技术的演进，探讨主要身份认证标准组织和相关标准和规范，以及研究标准化技术在电子商务中的应用。

1 身份认证标准化技术发展现状

电子商务身份认证是一种用于验证在线用户或实体身份的过程，以确保他们有权进行特定的在线交易或访问敏感信息。这一过程涉及确认用户提供的身份信息的真实性，通常通过用户名和密码、生物识别技术、智能卡、数字证书等手段来实现。身份认证的目标是建立可信度，降低欺诈行为，保护用户的隐私，维护在线交易的安全性[2]。

身份认证技术的演进历程是一个跨越古代至现代的进程，从最初的物理特征确认、手写签名、印章等传统方式，逐渐过渡到更为安全和高效的生物特征识别、密码和PIN码、智能卡、双因素认证、移动身份认证等数字化方法[3]。随着科技的飞速发展，生物特征识别不断完善，包括指纹、虹膜、掌纹、面部等各种生物特征，提供了更高层次的安全性。此外，区块链技术的出现和密码学技术的进步也为身份认证领域注入了新的活力，区块链提供了去中心化的身份验证方式，而密码学技术则支持零知识证明等高级认证手段[4]。最新的趋势涵盖了生物密码学、AI和机器学习，允许更智能地分析和验证用户身份，从而不断提高安全性，并保护用户的隐私。未来，我们可以期待更多创新，以进一步加强身份认证的安全性和可信度，以适应不断演变的威胁和技术环境。

电子商务身份认证标准化技术的研究不断发展，包括制定和推广一系列标准和规范，以确保在电子商务环境中进行身份认证的一致性和安全性。这些标准化技术通常包括数字证书、加密协议、安全通信标准、身份验证流程和数据隐私保护措施等，以确保用户身份得到有效保护。

2 电子商务身份认证技术

2.1 用户名和密码认证

用户名和密码认证[5]是一种常见的方式，通过用户选择的唯一用户名和保密密码来验证其身份。在注册过程中，用户选择用户名和设置密码，然后在登录时提供这些信息，系统验证其合法性。为了增强安全性，密码通常以哈希方式存储，并可以采用额外的安全措施，如：多因素认证。然而，这种方式存在忘记密码、密码泄露等问题。

2.2 生物特征识别认证

电子商务身份认证中的生物特征识别认证[6]是一种高度先进和安全的身份验证方法，其基本原理是通过捕获和分析个体独特的生物特征数据，如：指纹、虹膜、人脸或声音等，与预先存储的模板进行比对，从而确认用户的真实身份。这种技术的独特之处在于生物特征的唯一性，难以伪造或冒用，从而大大减少了身份欺诈的风险。生物特征识别认证不仅提高了安全性，还提供了便捷性，因为用户无需记住复杂的密码或携带身份证明文件，只需使用自己的生物特征即可完成身份验证。它在金融领域用于加强支付和交易的安全性，在移动设备上用于解锁手机或进行支付，还可用于医疗保健机构的访问控制以及国际边境的安全检查。然而，尽管生物特征识别认证带来了显著的便捷和安全性，但也引发了隐私和法规合规等重要问题，需要细致思考和管理。

2.3 证书和公钥基础设施（PKI）认证

电子商务身份认证中的证书是一种数字化文件，其中包含了个体或实体的身份信息以及与之相关的公钥。这些证书通常由受信任的证书颁发机构（CA）签发，以确保其真实性和合法性。证书的主要功能是标识和验证在线参与者的身份，同时提供了用于保护通信的公钥，从而确保了信息的保密性和完整性。公钥基础设施（PKI）认证[7]是

一种全面的框架，用于管理、分发和验证这些数字证书。PKI包括了CA、注册机构（RA）、目录等组件，它们协同工作，以确保证书的有效性和可信性。CA负责签发数字证书并通过数字签名验证其真实性，建立了一个信任链，而RA则用于验证证书请求者的身份。此外，PKI中的目录用于存储和检索证书，以供其他实体验证证书的有效性。这些技术共同构建了一个安全、可信的电子商务环境，确保了交易的机密性、数据完整性和身份真实性，为在线交易提供了可靠的保障。

2.4 零知识证明理论身份认证技术

零知识证明（Zero-Knowledge Proof，ZKP）[8]是电子商务身份认证领域的一项先进密码学技术，其核心概念在于允许一个实体（通常是用户）向另一个实体（通常是验证方）证明他们拥有某些特定信息或属性，但同时不必泄露这些信息的实际内容，从而在维护用户隐私的同时实现身份验证。这种技术的运作方式是通过一种交互式过程，验证方可以确认主体具备所需信息的能力，却无法获知这一信息的具体细节，从而为用户提供了高度的数据保护和隐私保密。随着对数字身份认证和隐私保护的不断关注，零知识证明技术在电子商务领域日益受到欢迎，同时也在标准化方面取得了重要进展，以确保其在不同系统和应用中的有效性和安全性，进一步推动了数字身份认证的发展和用户数据的安全保护。

零知识证明分为交互式零知识证明和非交互式零知识证明。交互式零知识证明[9]是一种密码学工具，用于证明某个主张的真实性，需要多轮的交互来完成。证明者通过向验证者发送一系列信息，不断地逐步建立验证者对主张的信任，同时不泄露主张的具体内容。这种方法广泛用于隐私保护、身份验证和加密货币领域。而非交互式零知识证明[10]只需要单一消息，无需多轮的交互。证明者生成一个特殊的证明，验证者可以单方面验证它来确信主张的真实性，同时不需要揭示主张的具体内容。这种方法在数字身份验证、区块链和密码学协议中得到广泛应用，提供高度的隐私保护和安全性。

3 WebOA办公系统身份认证特点和安全性要求

WebOA（Web Office Automation）系统[11]是一种基于Web的办公自动化系统，旨在提高办公效率和工作流程的管理。通常包括文档管理、任务分配、日程安排等功能，使企业和组织能够更高效地协作和管理工作。随着远程工作和在线协作的兴起，WebOA系统已经成为许多组织不可或缺的工具。其在各个领域的应用日益广泛，包括企业、政府机构和教育机构等。

身份认证在WebOA系统中具有关键性的作用，其重要性体现在以下几个方面。

首先，WebOA系统通常涉及敏感信息和操作，如：公司文件、个人数据等。因此，确保只有合法用户能够访问和执行这些操作是至关重要的。身份认证是实现访问控制的基础，它确保用户的身份是合法的，只有合法用户才能执行特定操作。

其次，随着数据隐私和合规性要求的增加，WebOA系统必须能够保护用户数据的隐私。身份认证是确保只有经过验证的用户能够访问这些数据的关键手段。这有助于满足法律法规和隐私要求，避免潜在的法律问题。

另外，WebOA系统还需要有效地防止未经授权的访问。通过身份认证，系统能够减少潜在的威胁和风险，防止数据泄露和恶意攻击。

因此，对于WebOA系统，安全性要求十分重要。这些安全性要求[12]包括以下几项。

（1）用户身份验证：系统需要强大的用户身份验证机制，以确保只有经过验证的用户才能登录和使用系统。这可能包括用户名和密码的验证，以及其他可能的身份验证方式，如：多因素身份验证。

（2）会话管理：有效的会话管理对于防止会话劫持和滥用至关重要。系统需要能够管理用户会话，确保用户在一定时间内不活动时自动注销，并提供安全的单点登录功能。

（3）安全协议：在WebOA系统中，使用安全的通信协议是必不可少的。HTTPS等加密协议可以确保数据在传输过程中的机密性和完整性。

（4）审计和监控：系统需要具备审计和监控功能，以便检测潜在的安全威胁和不正常活动。这包括日志记录、异常检测和警报机制。

（5）强密码策略：强密码策略有助于减少密码猜测攻击的风险。系统应该要求用户使用复杂的密码，并定期要求他们更改密码。

（6）防护措施：除了身份认证，WebOA系统还需要其他安全防护措施，如：防火墙、入侵检测系统和反病毒软件，以应对各种网络威胁。

4 零知识证明理论在WebOA中的应用

为解决传统身份认证方法[13,14]可能存在的一些安全漏洞，如：密码泄露、中间人攻击等问题，引入了零知识证明理论作为身份认证的新方法。零知识证明允许用户在证明自己的身份时，不需要透露身份信息的具体细节。这意味着用户可以证明自己是合法用户，而无需将密码或其他敏感信息传输给系统。这种方法的引入对WebOA系统具有重要的意义，因为它提高了系统的安全性，同时保护了用户的隐私。

4.1 改进方案的具体认证过程

（1）用户身份认证流程

改进方案的用户身份认证流程经过精心设计，以确保安全性和用户友好性。首先用户发起认证请求，用户访问WebOA系统并请求进行身份认证。系统随机生成一个应答，要求用户提供特定的身份认证信息。在认证过程中用户使用零知识证明技术生成零知识证明，证明其拥有所需的认证信息，同时不泄露任何关于该信息的具体内容。这个证明的生成过程是基于密码学算法的，并确保信息的机密性。之后由系统验证零知识证明，系统接收用户生成的零知识证明，并进行验证。验证过程不会披露用户的具体信息，但可以确定用户是否拥有所需的认证信息。最后如果零知识证明验证成功，系统将授权用户访问WebOA系统的敏感数据和功能。用户的身份得到确认，同时用户的隐私得到保护。

（2）零知识证明的实施

首先，选择合适的安全参数，包括密码算法和相关数值。其次，明确定义需要证明的内容，例如：证明知道某个秘密值但不透露它。然后，根据应用需求选择合适的零知识证明协议，如：zk-SNARKs或其他。接下来，生成证明，通常需要将证明内容转换为特定协议的格式，并进行一系列密码学运算以生成随机性质的证据。下一步是验证证明，接收者使用协议的公开信息来验证证明的有效性，而无需知道证明的具体内容。重要的是，确保证明不泄露额外的信息，以维护隐私。最后，将零知识证明系统部署到实际应用中，并定期维护以确保安全性和性能。这是一项复杂的技术，需要深入的密码学和计算机科学知识来实施，通常用于隐私保护、身份验证和数据隐私等领域。

在实际实施零知识证明时，通过使用现代密码学算法和协议，以确保安全性和效率。选择零知识证明的Schnorr协议或Bulletproofs，以确保用户身份认证的隐私保护和有效性。同时设置相关参数，包括挑战生成方式和证明的长度，以适应WebOA系统的需求和安全性要求。为保证通信的加密性和安全性，需进行通信协议设计，以抵御中间人攻击和数据泄露。密钥管理方面，采用安全的方法来生成、分发和存储密钥，以防止密钥泄露。最后，对零知识证明的性能进行优化，包括选择适当的密码学参数和可能的硬件加速，以确保身份认证过程的高效性。通过这些实施细节，确保零知识证明技术在WebOA系统中的有效应用，实现用户隐私的高度保护，并提高系统的安全性。

4.2 安全性分析

通过广泛的安全性分析，以验证改进方案的可信度。首先，根据可能的攻击和威胁分析：中间人攻击是一种常见的威胁，但由于零知识证明不泄露身份信息，攻击者无法获取有用的信息。此外，窃听者无法窃听到有用的信息，因为零知识证明的加密性质保护了通信的机密性。重放攻击也是一种潜在的威胁，但由于每次认证会话都使用不同的挑战和零知识证明，重放攻击在实践中变得不可行。其次，分析零知识证明技术在WebOA系统中的独特优势：它提供了无与伦比的隐私保护，因为

用户只需证明拥有所需的信息，而无需透露具体细节。此外，零知识证明增加了对密码破解攻击的保护，因为攻击者无法获取足够的信息来尝试破解密码。通过提高身份认证的安全性，降低了系统的风险，确保WebOA系统的可信度和用户隐私得到了充分保护。

5 结语

通过深入研究电子商务信息安全领域中的标准化身份认证技术，本文侧重介绍了基于零知识证明理论的身份认证技术。将零知识证明理论引入WebOA办公系统，以满足其独特的身份认证特点和安全性要求。同时深入分析了该方案在安全性方面的独特特点。零知识证明理论与WebOA办公系统的结合，为电子商务信息安全领域的身份认证提供了有力的理论支持和实践指导，为未来的安全性研究和系统开发提供了有价值的参考。

参考文献

[1] 申石,岑荣伟,沈宇超,等.基于行为主动权限识别的安全身份认证技术[J]. 信息安全研究, 2016,2(06):553-557.

[2] 李慧. 基于PKI和指纹识别技术的身份认证研究和实现[J]. 信息技术, 2004, 28(7):70-72+85.

[3] 宋宪荣,张猛. 国外网络可信身份认证技术发展现状、趋势及对我国的启示[J]. 网络空间安全, 2018,009(002):6-11.

[4] 庹小忠. 区块链在身份认证中的应用[J]. 科技经济导刊, 2017(3):26-27.

[5] 张虎强,洪佩琳,李津生,等. 用户名密码认证方案的安全性分析及解决方案[J]. 计算机工程与应用, 2006, 42(33):102-106+190.

[6] 何国辉,甘俊英. 基于多生物特征识别的网络身份认证研究[J]. 计算机应用研究, 2006,23(10):119-121.

[7] 刘微微,程海蓉. 信息安全专题介绍之二: 公钥基础设施PKI/CA认证安全体系[J]. 计算机辅助工程, 2002,11(1):73-78.

[8] 宋浩. 零知识证明——一种新的身份验证方法[C]//中国电子学会计算机工程与应用学会安全保密学组,中国计算机学会计算机安全专业委员会.第三次全国计算机安全技术交流会论文集[出版者不详], 1988:171-174.

[9] 张践明,谭柏华. 交互式零知识证明的哲学意义[J]. 湘潭大学学报（哲学社会科学版）, 2017,41(01):138-142.

[10] 李威翰,张宗洋,周子博,等. 简洁非交互零知识证明综述[J]. 密码学报, 2022,9(03):379-447.

[11] 王凯,邓淼磊. 基于WEB的办公自动化系统的设计与实现[J]. 电脑知识与技术, 2016,12(27):66-69.

[12] 常青,赵芳. 基于零知识证明的身份认证系统的研究[J].价值工程, 2010,29(24):167.

[13] 刘小青, 等. PKI网络身份认证技术在办公自动化系统中的应用[J]. 科技创业月刊, 2017, 30(8):123-125.

[14] 赵福通,郭卫斌. 基于动态密码和入侵容忍的身份认证方案[J]. 华东理工大学学报：自然科学版, 2009, 35(4):596-599.