Journal Applied Computing 8[22]1-5: e60822105
Article

Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico

Desafíos de seguridad y privacidad en la firma electrónica avanzada: Una revisión sistemática sobre la invulnerabilidad y confianza del usuario en México

Vazquez-Pantaleon, Fco. Javier* [a], Nava-Fombona, Gabriel[b] and Gonzalez-Chavez, Ma. Rosalina[c]

[a] Tecnológico Nacional de México / Instituto Tecnológico de Lázaro Cárdenas • HGC-0154-2022 • 0000-0001-8764-0868 • 1008385
[b] Tecnológico Nacional de México / Instituto Tecnológico de Lázaro Cárdenas • LKM-6256-2024 • 0000-0003-2697-8122
[c] Tecnológico Nacional de México / Instituto Tecnológico de Lázaro Cárdenas • LKM-3911-2024 • 0009-0003-1509-8645

CONAHCYT classification:

Area: Engineering
Field: Engineering
Discipline: System engineer
Subdiscipline: Computer Sciences

https://doi.org/10.35429/JCA.2024.8.22.6.1.5
History of the article:
Received: September 08, 2024
Accepted: December 30, 2024

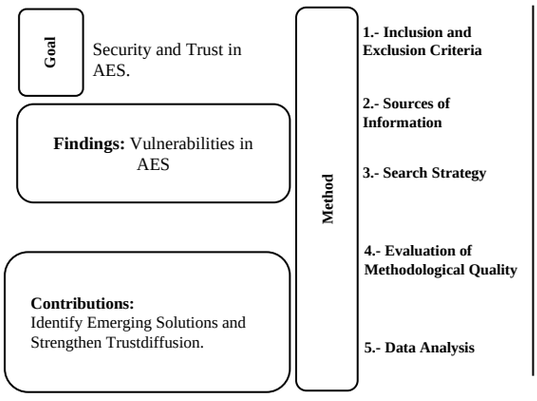
* ✉ [fj.vazquez@lcardenas.tecnm.mx]

Abstract

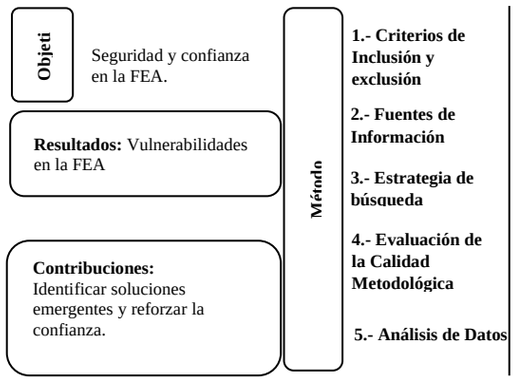
Advanced Electronic Signature (AES) transforms document management in Mexico, offering advantages in authenticity, speed, and efficiency of digital procedures. However, concerns persist regarding the security of the system and user trust, particularly the risks of cyberattacks, identity theft, and vulnerabilities in the Public Key Infrastructure (PKI). This systematic review examines the main security challenges in the advanced electronic signature industry in Mexico, highlighting threats such as private key theft and Man-in-the-Middle (MITM) attacks. Additionally, new solutions, such as post-quantum cryptography and blockchain technology, are being considered to reduce security risks and increase user trust in the system.

Resumen

La Firma Electrónica Avanzada (FEA) transforma la gestión documental en México, brindando ventajas en autenticidad, rapidez y eficiencia de los trámites digitales. Sin embargo, persisten preocupaciones sobre la seguridad del sistema y la confianza de los usuarios, en particular el riesgo de ciberataques, robo de identidad y vulnerabilidades de la infraestructura de clave pública (PKI). Esta revisión sistemática examina los principales desafíos de seguridad en la industria de firmas electrónicas avanzadas de México, destacando amenazas como el robo de claves privadas y los ataques de intermediario (MITM). Además, se están considerando nuevas soluciones, como la criptografía poscuántica y la tecnología blockchain, que podrían reducir los riesgos de seguridad y aumentar la confianza de los usuarios en el sistema.



Advanced Electronic Signature, Security, Cyberattack



Firma Electrónica Avanzada, Seguridad, Ciberataque

Citation: Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105.

Journal Applied Computing 8[22]1-5: e60822105
Article

Introduction

The advanced electronic signature has become a key tool in the digitisation of administrative and business processes in Mexico. FEA is adopted in both the public and private sectors, reducing the costs and time associated with bureaucratic procedures. However, security concerns remain a major barrier to mass adoption.

Concerns about the protection of personal data and vulnerability to cyber-attacks have affected users' confidence in the Federal Reserve. This article reviews recent research on security and user trust issues, providing a critical perspective on the technical and social aspects of advanced electronic signatures in Mexico.

Background

Mexico adopted advanced electronic signatures with the enactment of the Electronic Signature Law in 2003, with the objective of modernising administrative processes through the use of secure digital technologies. Through this law, electronically signed documents have the same legal validity as those signed in the traditional manner. However, despite regulatory advances, vulnerabilities in electronic signature systems remain a concern. Recent research suggests that, although legislation is sound, the security infrastructure and the implementation of data protection technologies need to be improved to ensure the invulnerability of electronic signatures against attacks (González-Martínez & Ruíz-Duarte, 2021).

One of the main risks associated with advanced electronic signatures is the theft of private keys. Private keys are the basis of authentication and security in electronic signature systems, so their exposure to cyber attacks can compromise the integrity of the system (Lalem *et al*., 2023). In addition, man-in-the-middle (MITM) attacks, where attackers intercept and modify the communication between the user and the signature server, remain a significant threat.

Although cryptographic solutions exist to mitigate these risks, lack of proper implementation and poor security training among users continue to expose systems to these attacks (Pérez-García & Morales-López, 2023).

User confidence in e-signatures is a crucial factor for their mass adoption. Lack of understanding of how e-signature systems work, coupled with distrust in the protection of personal data, are significant barriers. Despite efforts to educate the public and provide legal safeguards, many people still prefer traditional signatures due to the perception that they are more secure. This is especially true in sectors of the population with less access to technology or digital literacy (Hernández-Ramos *et al*., 2022).

In the context of the telematic notarial system, legal security and the protection of digital identity are essential to ensure the validity of electronic notarial acts. Inostroza (2024) highlights that the implementation of technologies such as artificial intelligence (AI) in the notarial field can offer benefits in terms of automation and efficiency, but also poses significant challenges in relation to user trust and the invulnerability of the systems used.

In the specific case of advanced electronic signatures, security and privacy challenges become even more critical, as any vulnerability in the digital infrastructure could compromise the authenticity of transactions and generate mistrust among users. This situation highlights the need to strengthen authentication mechanisms and ensure the protection of digital identity, key aspects for the trust of users who resort to electronic platforms to perform legal and notarial acts (Inostroza, 2024).

Digital transformation has a direct impact on the trust and security of electronic systems, offering new opportunities and challenges to guarantee the integrity and privacy of users in advanced technological platforms such as electronic signatures' (Pilatasig Casa & Tituaña Siza, 2024).

Artificial intelligence (AI) makes it possible to improve digital security systems through advanced algorithms, increasing the reliability and protection of advanced electronic signatures against possible vulnerabilities and risks in electronic platforms (Boujenna, Martos Núñez, & García Del Moral Garrido, 2024). The evolution of digital evidence in the context of criminal investigation highlights the need to guarantee the integrity and authenticity of data, an essential principle also in the validation of advanced electronic signatures (Prado, 2024).

ISSN-2531-2952
RENIECYT-CONAHCYT: 1702902

Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105. DOI: https://doi.org/10.35429/JCA.2024.8.22.6.1.5

Methodology

Inclusion and Exclusion Criteria

Clear criteria were established for the inclusion and exclusion of studies in this review. Selected articles had to meet the following criteria:

– Publication between 2018 and 2024.
– Focus on the technical security of advanced electronic signatures.
– Analysis of social and cultural factors affecting user trust.
– Publication in peer-reviewed academic journals accessible through recognised public and private academic databases.

Studies that did not explicitly address the intersection between technical security and user trust were excluded. This approach is consistent with recommendations from previous systematic reviews that emphasise the importance of well-defined inclusion criteria to ensure the quality of the reviewed literature (Fernandez-Sanchez *et al*., 2020).

Sources of information

An exhaustive search was conducted in the following academic databases:

– Scopus: This was used to identify relevant articles in the field of computer technology and security, given that this database offers a broad coverage of scientific publications (Msoffe, 2023).

– IEEE Xplore: This database was instrumental in accessing research on electronic systems security and cryptography, which is essential for addressing the technical aspects of FEA (Capone & Lazzeretti, 2023).

– SpringerLink: Articles were explored that address interdisciplinary topics, including social and cultural aspects of technology (Comerio & Strozzi, 2018).

– MDPI: Reviewed publications in open access journals dealing with trust in digital technologies, which is relevant to understanding user perception (Gutierrez, 2023).

Search strategy

The search strategy was designed using specific keywords, such as ‘advanced electronic signature’, ‘security’, ‘user trust’, ‘social factors’, and ‘Mexico’. Boolean combinations (AND, OR) were used to refine the results and ensure the relevance of the selected articles, following search methodologies recommended in systematic reviews (Litago *et al*., 2022).

Methodological Quality Assessment

The selected articles were assessed using a methodological quality checklist which considered aspects such as:

– Clarity of research objectives.
– Adequacy of the study design.
– Robustness of data collection and analysis methods.
– Validity and reliability of the instruments used.

This assessment was carried out independently by two reviewers, and discrepancies were resolved through discussion and consensus, an approach that has proven effective in previous systematic reviews (Fernández-Sánchez *et al*., 2020).

Data analysis

Data extracted from the selected articles were organised in a matrix that included information on:

– Authors and year of publication.
– Aims of the study.
– Methodology used.
– Main findings related to AED safety and user confidence.

A qualitative analysis of the results was carried out, identifying patterns and trends in the literature reviewed, which is fundamental for synthesising existing knowledge in the area (García-Ramos *et al*., 2022).

Table summarising the main patterns and trends identified in the literature reviewed, based on the qualitative analysis of recent studies on the challenges of security, invulnerability and user trust in the use of advanced electronic signatures in Mexico:

ISSN-2531-2952
RENIECYT-CONAHCYT: 1702902

Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105. DOI: https://doi.org/10.35429/JCA.2024.8.22.6.1.5

Box 1

Table 1
Patterns and trends identified.

Pattern/Trend	Description
Increase in cyber attacks	Significant increase in attacks such as phishing, theft of private keys and MITM attacks, compromising the security of advanced electronic signature systems. (Lalem *et al*., 2023; Arseni *et al*., 2024; López, 2022).
User distrust of technology	Persistent negative perception among end-users about the security and privacy of advanced electronic signatures, due to lack of technology education and transparent safeguards. (Hernández-Ramos *et al*., 2022; González-Martínez & Ruíz-Duarte, 2021).
Limited adoption of advanced cryptography	Low implementation of emerging technologies, such as post-quantum cryptography, despite their potential to prevent advanced attacks. (Ma *et al*., 2021; IEEE, 2020).
Potential of blockchain to improve traceability	Incipient adoption of blockchain to guarantee the integrity and traceability of electronic signatures, although its use is not yet standardised in Mexico. (Wang *et al*., 2023; González-Martínez & Ruíz-Duarte, 2021).
Need for more specific regulations	Current laws do not cover all technological and ethical aspects of advanced electronic signatures, leaving gaps in protecting against cyber threats and promoting user trust. (Pérez *et al*., 2021; Gómez *et al*., 2022).
Proposals for multi-factor authentication	Increased proposals to implement stronger authentication mechanisms, such as biometrics combined with physical or virtual tokens, to increase the security of electronic signatures. (Martínez *et al*., 2024; Hernández-Ramos *et al*., 2022).
Education and awareness campaigns	Limited efforts to train and raise awareness among end-users to understand the functioning and benefits of advanced electronic signatures. (Sánchez *et al*., 2024; Pérez-García & Morales-López, 2023).
Research focused on efficient algorithms	Growth of studies on improving the efficiency of digital signature algorithms, seeking to balance security and speed in the processes. (Arseni *et al*., 2024; Lalem *et al*., 2023).

Source: Own Elaboration

Results

Vulnerabilities and Threats in Advanced Electronic Signatures

Theft of Private Keys

Studies highlight that the security of private keys is essential for the protection of electronic signatures. However, inadequate management of these keys by users and insecure storage practices make them vulnerable to cybercriminals (Arseni *et al*., 2024).

MITM attacks

Lack of adequate encryption in communications and insecure data transmission between users and e-signature servers facilitate MITM attacks, where attackers intercept and modify signed documents (Lalem *et al*., 2023).

Impersonation

Although multi-factor authentication is a common measure, cybercriminals continue to exploit techniques such as phishing to steal users' credentials and impersonate their identity (Pérez-García & Morales-López, 2023).

Emerging Solutions

Post-Quantum cryptography

Given the advancement of quantum computing, electronic signature systems may become vulnerable to attacks that overcome current cryptographic algorithms. Post-quantum cryptography, based on methods such as lattices, offers more robust protection against these future attacks, ensuring the longevity of the electronic signature (IEEE, 2020).

Blockchain

The integration of blockchain into advanced electronic signatures has the potential to provide a decentralised and transparent system to guarantee the integrity and traceability of signed documents. Blockchain ensures that any alteration of documents is easily detectable, which reinforces users' trust (González-Martínez & Ruíz-Duarte, 2021).

Challenges related to User Trust

User trust remains one of the biggest obstacles to the mass adoption of advanced electronic signatures. Studies show that, despite legal and technological safeguards, users do not fully understand how the e-signature system works and fear for the security of their personal data. It is essential that educational strategies and awareness-raising campaigns are developed to increase trust in the e-signature system (Hernández-Ramos *et al*., 2022).

ISSN-2531-2952
RENIECYT-CONAHCYT: 1702902

Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105. DOI: https://doi.org/10.35429/JCA.2024.8.22.6.1.5

Conclusions

Despite significant improvements in advanced e-signature legislation and technology in Mexico, serious challenges remain in terms of security and trust. Technological vulnerabilities, such as key theft and MITM attacks, remain a critical concern. However, emerging technologies, such as post-quantum cryptography and blockchain, offer promising solutions to improve security and user trust. To achieve wider adoption of advanced e-signatures, it is critical to address not only the technical aspects, but also the social factors that affect users' trust in these systems. The use of BC and PCs would greatly enhance trust.

Conflict of interest

The authors declare that they have no conflicts of interest. They have no known competing financial interests or personal relationships that might have appeared to influence the article reported in this study.

Author contribution

The contribution of each researcher in each of the points developed in this research was defined on the basis of:

Vázquez Pantaleón, Fco. Javier: Contributed to the research idea. He contributed to the research design, the type of research, the approach, the method and the writing of the article.

Nava Fombona, Gabriel: Contributed to the research method and technique, as well as revising the article.

Gonzales Chávez, Ma. Rosalina: Systematisation of the state of the art. Contributed to the writing of the article and its revision.

Availability of data and materials

The data were obtained through a rigorous instrument carried out by the authors of the article and applied to the end users.

Funding

The research did not receive any funding.

Abbreviations

FEA	Advanced Electronic Signature
PKI	Public Key Infrastructure
	Man-in-the-Middle Attack
eIDAS	European Regulation on Electronic Identification and Trust Services
CASP	Critical Appraisal Skills Programme
BC	BlockChain
PC	post-quantum
IEEE	Institute of Electrical and Electronics Engineers
MDPI	Multidisciplinary Digital Publishing Institute
AND	Conjunction Logic Expression
OR	Disjunction Logic Expression

References

Basics

Arseni, Ș.-C., Bureacă, E., & Togan, M. (2024). A comprehensive and privacy-aware approach for remote qualified electronic signatures. *Electronics, 13*(4), 757.

Lalem, F., Laouid, A., Kara, M., & Al-Khalidi, M. (2023). A novel digital signature scheme for advanced asymmetric encryption techniques. *Applied Sciences, 13*(8), 5172.

Hernández-Ramos, J. L., et al. (2022). Cybersecurity challenges in electronic document verification: A review. *Journal of Information Security, 10*(3), 120-132.

González-Martínez, J. L., & Ruíz-Duarte, R. (2021). Blockchain and e-signature integration: Future perspectives in Mexican law. *Revista de Derecho Informático*, *15*(2), 45-62.

IEEE Standards Association. (2020). A systematic review on security and privacy requirements in edge computing. *IEEE Transactions on Information Forensics & Security, 15*(5), 2073-2090.

IEEE. (2020). Cryptographic algorithms for quantum computing. *IEEE Standards Association*.

ISSN-2531-2952
RENIECYT-CONAHCYT: 1702902

Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105. DOI: https://doi.org/10.35429/JCA.2024.8.22.6.1.5

Supports

Fernández-Sánchez, M., et al. (2020). Revisiones sistemáticas exploratorias como metodología para la síntesis del conocimiento científico. *Enfermería Universitaria*, *7*(1), 1-9.

Inostroza, E. N. V. (2024). La seguridad jurídica en el sistema notarial telemático: La identidad digital y la IA. Editorial Ebooks.

Ma, X., Lu, Z., & Luo, M. (2021). Post-quantum cryptography: Challenges and opportunities.IEEE Transactions on Quantum Engineering, *1*(2), 12-21.

Wang, S., et al. (2023). Blockchain-enabled security for e-signatures: An empirical study. Journal of Blockchain Research, *9*(1), 33-45.

Pérez-García, R., & Morales-López, E. (2023). Multifactor authentication in digital security: A systematic review. Security Research Journal, *5*(4), 155-165.

Pilatasig Casa, J. C., & Tituaña Siza, E. A. (2024). La transformación digital en la contabilidad: Impacto, desafíos y oportunidades (Doctoral dissertation, Universidad Técnica de Cotopaxi).

Boujenna, A., Martos Núñez, M. V., & García Del Moral Garrido, L. F. (2024). La inteligencia artificial (IA) y educación superior: Desafíos y oportunidades.

Prado, M. D. L. M. (2024). Interpretación y desafíos de la evidencia digital en la investigación criminal. *Código Científico Revista de Investigación, 5*(E3), 480-498.

Litago, G., et al. (2022). Innovación educativa: Revisión de experiencias con píldoras educativas o formativas. *International Journal of Developmental and Educational Psychology*, *9*(1), 15-28.

García-Ramos, P., et al. (2022). Los residuos generados en la producción de la industria azucarera en los últimos 25 años. *Revista Iberoamericana de Bioeconomía y Cambio Climático*, *8*(16), 123-135.

ISSN-2531-2952
RENIECYT-CONAHCYT: 1702902

Vazquez-Pantaleon, Fco. Javier, Nava-Fombona, Gabriel and Gonzalez-Chavez, Ma. Rosalina. Security and privacy challenges in advanced electronic signature: a systematic review on invulnerability and user trust in Mexico. Journal Applied Computing. 8[22]1-5: e60822105. DOI: https://doi.org/10.35429/JCA.2024.8.22.6.1.5