Public Awareness, Perception and Acceptation: The Status of Digital Signatures in Malaysia and Worldwide

Noor Amin * , Retaj Ahmed Moustafa Abdelsalam Mogahed , Rana Amr Aldayan , Theerthika Devi A/P Ananth , Syed Muhammad Dayyan Shah , Amina Faisal

Posted Date: 5 December 2025

doi: 10.20944/preprints202512.0550.v1

Keywords: digital signatures; public awareness; digital trust; malaysia; certification authorities; cryptography; electronic signatures; e-governance; cybersecurity; data integrity; authentication; nonrepudiation; legal framework; digital inclusion

Article

Public Awareness, Perception and Acceptation: The Status of Digital Signatures in Malaysia and Worldwide

Noor Ul Amin, Retaj Ahmed Moustafa Abdelsalam Mogahed, Rana Amr Aldayan, Theerthika Devi A/P Ananth, Syed Muhammad Dayyan Shah and Amina Faisal

Taylor's University

* Correspondence: nooraminnawab@gmail.com

Abstract

This essay aims to explore the perception, public awareness, and acceptance of Digital Signatures globally as well as in Malaysia as a case study. It begins with a general overview of what Digital Signatures and their role in modern digital landscape then dives into public perception and general public sentiment surrounding its adoption followed by an analysis of their advantages and disadvantages, the potential challenges faced with their implementation, and their current status in Malaysia. The essay also shines light on the major Digital Signature Certification Authorities (CAs) in Malaysia and their details along with a general comparison between CAs followed by conclusion.

Keywords: digital signatures; public awareness; digital trust; malaysia; certification authorities; cryptography; electronic signatures; e-governance; cybersecurity; data integrity; authentication; non-repudiation; legal framework; digital inclusion

Introduction

The rise of digitalization has led to so many businesses digitalizing their records and transactions and in this process, the authentication of each transaction and the sender's identity is necessary and so is their protection. This is where cryptography plays a major role in our modern society. It encrypts data during transfer so nobody other than the person authorized can view it. It is here that Electronic Signatures (e-Signatures) and Digital Signatures play the role.

A digital signature is a cryptographic technique that validates the authenticity, integrity and non-repudiation of digital documents or electronic messages. They are practically the digital equivalents of handwritten signatures on paper documents. They serve the same purpose

i.e ensuring that the document is the original one from the sender and has not been altered since it was signed and dispatched (sent) to the receiver.

It can be argued that digital signature is in fact a type of e-signature. The main difference between the two is that unlike e-signature which can contain a range of items indicating a person's intent/consent, digital signature uses cryptographic techniques to ensure the integrity and authenticity of the signed document. The process includes the usage of a digital certificate that is given by a trusted Certification Authority (CA) and the usage of public-key cryptography to sign and verify documents (cleartax, 2025).

Overview of Digital Signatures

A digital signature plays a crucial role in confirming the authenticity and integrity of digital documents or messages, all thanks to cryptography. It employs public key cryptography to encrypt a message's hash using a private key. When the recipient receives the message, they can decrypt the hash with the public key and compare it to the current hash of the message. If the two hashes match, it means

 doi:10.20944/preprints202512.0550.v1

the message is intact and has indeed been sent by the signer. This cryptographic method upholds three key principles of secure digital communication: authenticity, integrity, and non-repudiation. Authenticity guarantees that the message comes from the claimed sender, integrity ensures the content remains unchanged, and non-repudiation prevents the sender from denying their signature since only they possess the private key used for signing. Unlike electronic signatures, which are simply images of a person's signature, digital signatures are much more advanced as they rely on mathematical algorithms (www.ssh.com, n.d.). As technology continues to evolve, digital signatures are essential for establishing trust in online transactions and electronically exchanged emails, highlighting their growing importance in our digital world.

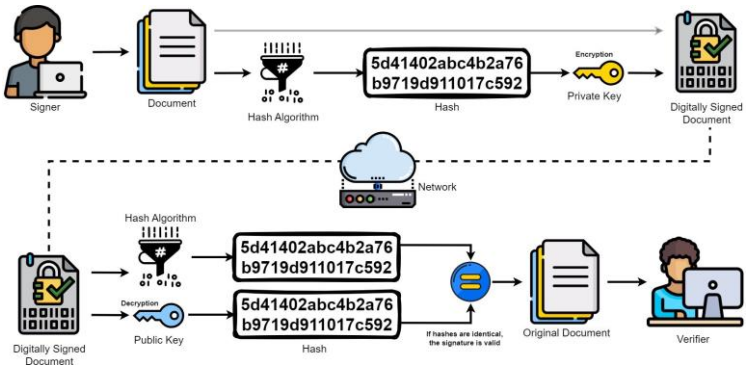

Figure 1. - *Diagram of how Digital Signature Works (Digital Signatures, 2023).*

In the world of digital signatures, tools like RSA, DSA, and ECDSA are employed, each with their own advantages and disadvantages in computation and strength of cryptography. As an illustration, when sending a message, algorithms like SHA-256 are used to extract unique fingerprints that are of shorter length and fixed size. The fingerprint is further processed by the sender's private key to create a digital signature (Day, 2023). Once the recipient receives the message, they use the sender's public key to decrypt the signature. Using the sender's public key allows one to verify the digital signature and with a decryption process, check whether the relevant hash has been matched. When both fingerprints are aligned, there is assurance that the message is altered or tampered with. This approach makes every transaction secure because information is not really encrypted, just compressed making everything smoother and efficient. Security is further improved with brute force and collisions. Owing to these qualities, digital signatures not only play a key role in securing emails and validating documents, but also support transactions conducted on blockchains, confirming identities digitally, and distributing software in a secure manner.

Role of Digital Signatures in modern-day society

In today's society, electronic signatures have become important for conducting transactions in a secure, provable, and efficient manner. With each digitization, the need for providing trust, responsibility, and protecting data in systems has also increased. Digital signatures serve this purpose by providing cryptographic evidence of a document's origin and its content[13–15]. They can be used in electronic commerce, banking, legal affairs, healthcare, government services, and many more. As an illustration, e-contracts permit participants to sign documents containing legally binding agreements from any location using digital signatures. In many jurisdictions, Malaysia for example, under the Digital Signature Act of 1997, issued digital signatures by certified authorities are treated equal in value to wet signatures. This has greatly hastened their acceptance in business, regulatory, and legal frameworks where authentication and auditability are needed (cleartax, 2025).

 doi:10.20944/preprints202512.0550.v1

Furthermore, they increase the trustability of software delivery, email transactions, and government communications through protecting against tampering and impersonation. Digital signatures are being used increasingly by government agencies for services like tax returns, licenses and procurement, to authenticate forms and protect data. Developers sign code and executables in software to help verify to users that the software has not been modified or replaced and that the software can be trusted by the user not to harm their system. Digital signatures are also an essential element in enabling secure email protocols like S/MIME, which not only encrypts messages but also verifies the identity of senders[16–19]. We can greatly minimize the chances of falling victim to phishing attacks. On a larger scale, these protocols are essential to the Public Key Infrastructure (PKI), which supports secure systems all over the internet—think HTTPS websites, secure messaging applications, and even blockchain transactions (cleartax, 2025) .

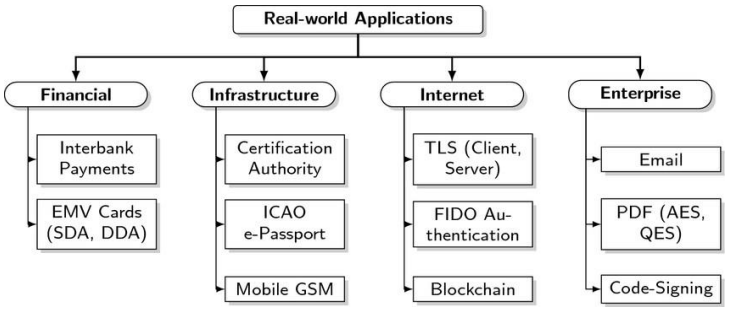

Figure 2. *- Diagram showing the Real-world applications of Digital Signatures (Tan, Szalachowski and Zhou, 2022).*

These applications show that digital signatures are more than just a technical tool; they are essential for establishing digital trust and protecting the process of digital transformation in both public and private sectors.

Benefits and Drawbacks of Using Digital Signature

Digital signatures offer a range of compelling advantages that position them as an essential component of secure digital communication. Most significantly, perhaps, is enhanced security. Digital signatures use strong cryptographic algorithms to tie the signer to the literal contents of a message in a way that any change after signing invalidates the signature. This makes them ideal for confidential communication, legal agreements, and regulatory submissions, where authenticity and integrity are crucial. Digital signatures also provide non-repudiation, in the sense that the signer cannot later deny having signed the message, since the private key used to generate the signature is unique and private to the signer. Beyond security, digital signatures also provide operational efficiency (SSL.com, 2025). They eliminate physical paperwork and approval process turnaround time, enabling individuals and organizations to sign documents remotely. This has been especially helpful in sectors like banking, real estate, and government where quick and verifiable transactions are required. Furthermore, digital signatures support environmental sustainability by effectively eliminating the use of paper, ink, and physical transport. Digital signatures have the legal acceptance in the majority of countries, including Malaysia, and therefore are a sufficient replacement for manual signing methods, opening the door to their broader application throughout the public and private sectors (cleartax, 2025).

 doi:10.20944/preprints202512.0550.v1

Table 1. *- Benefits and Drawbacks of using Digital Signatures (cleartax, 2025).*

Aspect	Benefits	Drawbacks
Security	Ensures data integrity, authenticity, and non-repudiation	Private key compromise may lead to fraud or unauthorized access
Legal Validity	Recognized under law in many countries, including Malaysia	Differences in global legal frameworks may cause interoperability issues
Efficiency	Speeds up document approval, reduces paperwork, supports remote signing	Requires technical infrastructure and knowledge to implement effectively
Cost & Environment	Saves on printing, storage, and transport costs; environmentally friendly	Initial setup and maintenance can be costly for small organizations
User Trust & Access	Builds confidence in secure transactions; supports digital transformation	Limited awareness or digital literacy may hinder widespread public adoption

Public Perception, Awareness, and Acceptance of Digital Signatures

The perception and acceptance of digital signature in Malaysia does occupy a complex intersection of technology, trust and digital literacy. While the legislative foundation anchored by the Digital Signature Act 1991 ("Electronic Signature and Attestation in Conveyancing Practice: A Malaysian Legal Perspective," 2022), provided the legal validity and structural legitimacy, public understanding still remains uneven across social and business sectors. The digital signature, even though it's increasingly integrated in different sectors such as governmental workflow, banking systems and large-scale enterprise platforms, has not yet achieved universal recognition or intuitive familiarity among the general public (Stanešić et al., 2025).

At the core of this lies a knowledge gap. Among digitally literate individuals and tech-forward organizations, digital signatures are largely perceived as an essential tool for secure, efficient, and legally binding communication (Lin, 2023). These users often understand the cryptographic principles behind these digital signatures, appreciate the assurance of integrity and non-repudiation (Rai et al., 2023) they offer, and recognize the institutional trust imbued by Certification Authorities (CAs). For them, digital signatures are not merely a technical formality, but a symbol of a maturing digital ecosystem.

However, a contrasting reality persists for small businesses, the older population, and segments of society with limited or no knowledge of digital education (Ł Tomczyk et al, 2023). For these groups, digital signatures can appear abstract, overly technical, or even intimidating. Many are unaware of how digital signatures function, their legal standing, or how to acquire and use them effectively. Even when exposed

 doi:10.20944/preprints202512.0550.v1

to the technology, these users often question its legitimacy, fearing fraud, misuse or hidden complexity. This lack of clarity becomes a significant barrier to widespread adoption.

Trust in Certification Authorities emerges as a pivotal factor. Studies and market observation show that public confidence in licensed CAs such as MSA Trustgate, DigiCert Malaysia or POS DigiCert, directly influences adoption rates (Pos Digicert Sdn Bhd, 2025). When users are made aware that these institutions are regulated under national cybersecurity standards and are subject to routine audits, their willingness to adopt digital signatures increases measurably. The CA, in this sense, serves not just as a technical entity issuing certificates but as a psychological anchor that provides assurance in a space often dominated by invisible algorithms[20–23].

In recent years, both the government and private sectors have recognized these psychological and educational barriers. Initiatives such as public awareness campaigns, training modules and simplified onboarding process for certificate acquisition have begun to show impact[24,25]. These efforts aim to demystify the concept, break down its component and position the digital signature not as a specialized corporate tool but as a n everyday enabler of secure interaction, much like physical signature once was.

Digital Signature Certification Authorities (CAs) in Malaysia

The following are the authorized Digital Certification Authorities in Malaysia that are recognized as legal as per the Malaysian Constitution's Digital Signature Act 1997 (DSA 1997) which was passed in 1998 (MCMC, 2024):

Pos Digicert Sdn Bhd is a licensed digital certification authority registered under Digital Signature Act 1997 (DSA 1997) under License no. LPBP-1/2020 (4) ,valid from 25 December 2020 to 24 December 2025 (when the next audit is due), provided by Malaysian Communications and Multimedia Commission (MCMC). It offers services that can be divided into 2 classes: Class 1 and Class 2 (Basic, Enhanced, Server ID, and Sub CA) services and makes use of RSA and ECC cryptographic standards. As per the latest audit, the firm did comply with DSA 1997 though the report does not specify to what extent but we know it does comply because the report clearly mentions their license was neither revoked nor were they asked to surrender it (something which happens in case of incompliance). The firm offers a certified guarantee of RM 2,000,000 and provides the public access to its certification and revocation lists through the LDAP directly. Furthermore the firm maintains a publicly available Certification Practice Statement (CPS) and has been issued a Certificate of Recognition for Repository along with a Certificate of Recognition for Date/Time Stamp Service (MCMC, 2024).

MSC Trustgate.Com Sdn Bhd is another licensed digital certification authority registered under Digital Signature Act 1997 (DSA 1997) under license no. LPBP-2/2020(4), valid from 24 July 2020 to 24 July 2025 (as of this essay's writing the authors were unable to find out whether the license got renewed or not as the ministry's official website says 'Renewal is in progress')provided by Malaysian Communications and Multimedia Commission (MCMC).

The firm offers various digital certification services such as AATL (Individual Basic, Individual Pro, Organization), Document Signing (Medium Assurance), Document Signing for Medium Assurance (Medium Assurance), MyDigital ID, SSL Domain Validation (non-public trusted), SSL Organization Validation (non-public trusted), and S/MIME (Mailbox, Individual, Sponsored, Organization). The certified guarantee reliance amount varies by service and as per the latest audit the firm was in substantial compliance with DSA 1997. Furthermore their digital certification and revocation records can be publicly accessed through their repository and CRL/OCSP services, with the Certification Practice Statement (CPS) structured according to RFC 3647 and available on their website. This firm has also been awarded a Certificate of Recognition for Repository along with a Certificate of Recognition for Date/Time Stamp Service (MCMC, 2024).

 doi:10.20944/preprints202512.0550.v1

Raffcomm Technologies Sdn Bhd operating under the brand name 'RAFFTECH' is registered under license no.LPBP-4/2024 (2) by DSA 1997 valid from 1 May 2024 to 30 April 2027. It offers products and services under the CypherSIgn branch namely Personal, Pro, Organizational, and Pro Max. It uses robust cryptographic measures like ECC and RSA repository and CRL/OCSP services, with the Certification Practice Statement (CPS) structured according to RFC 3647 and available on their website. It also provides a RM 2,000,000 guarantee returns and reliance amount depends from category to category. The latest audit mentions that it is in full compliance with regulatory measures and has also been awarded Certificate of Recognition for Repository along with a Certificate of Recognition for Date/Time Stamp Service (MCMC, 2024).

TM Technology Services Sdn Bhd is registered under license no. LPBP-3/2023 (3) valid from 14 April 2024 to 31 July 2024 (at the time of writing, the ministry website says their license renewal is 'in progress'). Its services include Digital Certificates, SSL, Repository, and Digital Signature. The firm uses the RSA algorithm. The latest audit said it was in substantial compliance with regularity measures. Certificate revocation details, repository URLs, and CPS documentation are publicly accessible. It also offers a guarantee of RM 2,000,000 and the reliance amount varies from class of service chosen. Furthermore the license issued to this firm was originally given to Telekom Applied Business Sdn Bhd. but then transferred and the firm has also received a Certificate of Recognition for Repository (MCMC, 2024).

Conclusion

To conclude, Digital signatures represent a significant step ahead in guaranteeing safe and legally recognized digital transactions of information. Globally and in Malaysia, studies show that when governments license CAs, it increases public confidence in them and subsequently in the technology of Digital Signatures itself. This is an incentive for the government to regulate the CA industry to ensure growth of digital signatures' usage worldwide. Our studies further showed that as of now Malaysia has four licensed CAs recognized by the Malaysian Communications and Multimedia Commission (MCMC). Our final takeaway is that Digital signatures are a useful technology when it comes to secure transactions and governments can play a major role by helping this grow by regulating and certifying CAs to encourage more use of digital signatures.

Turnitin Similarity Report - Question 5

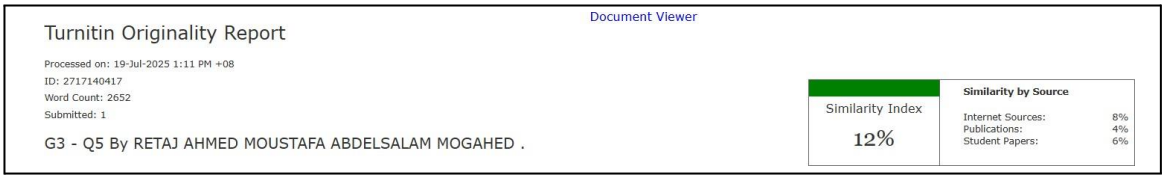

Table of Contributions

Student Name	Contribution made:
1) Retaj Ahmed Moustafa Abdelsalam Mogahed	Question 1 & 2
2) Rana Amr Aldayan	Question 3

 doi:10.20944/preprints202512.0550.v1

3) Amina Faisal	Question 4
4) Noor Ul Amin	Question 5 - Desktop Research
5) Syed Muhammad Dayyan Shah	Question 5 - Desktop Research
6) Theerthika Devi A/P Ananth	Question 5 - Desktop Research

 doi:10.20944/preprints202512.0550.v1

References

1. Electronic signature and attestation in conveyancing practice: A Malaysian legal perspective. (2022). F1000Research, 11, 325. https://doi.org/10.12688/f1000research.73548.3
2. Stanešić, J., Morić, Z., Regvart, D., & Bencarić, I. (2025). Digital signatures and their legal significance. Edelweiss Applied Science and Technology, 9(1), 431–440. https://doi.org/10.55214/25768484.v9i1.4154
3. Lin, W. (2023). Digital Signature (pp. 77–81). https://doi.org/10.1007/978-3-031-33386-6_15
4. Rai, A., Singh, M., Sudheendramouli, H. C., Panwar, V., Balaji, N., & Kukreti, R. (2023). Digital Signature for Content Authentication. 1–6. https://doi.org/10.1109/accai58221.2023.10200472
5. Tomczyk, Ł., Mascia, M. L., Gierszewski, D., & Walker, C. (2023). Barriers to digital inclusion among older people: a intergenerational reflection on the need to develop digital competences for the group with the highest level of digital exclusion.
6. Pos Digicert Sdn Bhd. (2025, May 9). The future of governance – Leveraging agentic AI and digital trust for responsible innovation. Pos Digicert. Retrieved July 18, 2025, from Pos Digicert website
7. www.ssh.com. (n.d.). How Digital Signatures Work? [online] Available at: https://www.ssh.com/academy/secure-information-sharing/how-digital-signatures-work
8. SSL.com. (2025). Digital Signatures vs. Electronic Signatures: 5 Key Differences - SSL.com. [online] Available at:

https://www.ssl.com/article/digital-signatures-vs-electronic-signatures-5-key-difference s/.

9. Day, B. (2023). Help Strengthen Your Cybersecurity Efforts with Electronic & D - Guardian Digital. [online] guardiandigital.com. Available at: https://guardiandigital.com/resources/blog/electronic-digital-signatures-cybersecurity.
10. cleartax (2025). *Digital Signatures in Malaysia: A Comprehensive Guide 2024*. [online] cleartax. Available at: https://www.cleartax.com/my/en/digital-signature-in-malaysia.
11. MCMC (2024). *ContentKeeper Content Filtering*. [online] Mcmc.gov.my. Available at: https://mcmc.gov.my/en/sectors/digital-signature/list-of-licensees
    - Note: In this link you can find the link to licenses of the four CA firms we have mentioned. Citation maker did not allow us to cite it
12. Tan, T.G., Szalachowski, P. and Zhou, J. (2022). Challenges of post-quantum digital signing in real-world applications: a survey. *International Journal of Information Security*, 21(4), pp.937–952. doi:https://doi.org/10.1007/s10207-022-00587-6.
13. Brohi, S., Jhanjhi, N. Z., & Pillai, T. R. (2025). A Research Landscape of Agentic AI and Large Language Models: Applications, Challenges and Future Directions. *Algorithms*, *18*(8), 499.
14. Chaubey, N., Jhanjhi, N. Z., Thampi, S. M., Parikh, S., & Amin, K. (Eds.). (2024). *Computing Science, Communication and Security: 5th International Conference, COMS2 2024, Mehsana, Gujarat, India, February 6–7, 2024, Proceedings* (Vol. 2174). Springer Nature.
15. Almufareh, M. F., Jhanjhi, N. Z., Khan, N. A., Almuayqil, S. N., Humayun, M., & Javed, D. (2024). BertSent: transformer-based model for sentiment analysis of penta-class tweet classification. *IEEE Access*.
16. Almazroi, A. A., Alsubaei, F. S., Ayub, N., & Jhanjhi, N. Z. (2024). Inclusive Smart Cities: IoT-Cloud Solutions for Enhanced Energy Analytics and Safety. *International Journal of Advanced Computer Science & Applications*, *15*(5).
17. Baligodugula, V. V. (2023). Unsupervised-based distributed machine learning for efficient data clustering and prediction.
18. Din, S. N. U., Muzammal, S. M., Bibi, R., Tayyab, M., Jhanjhi, N. Z., & Habib, M. (2024). Securing the Internet of Things in Logistics: Challenges, Solutions, and the Role of Machine Learning in Anomaly Detection. In *Digital transformation for improved industry and supply chain performance* (pp. 133-165). IGI Global.
19. Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024). IoT smart healthcare security challenges and solutions. In *Advances in Computational Intelligence for the Healthcare Industry 4.0* (pp. 234-247). IGI Global Scientific Publishing.

 doi:10.20944/preprints202512.0550.v1

20. Niveshitha, N., Amsaad, F., & Jhanjhi, N. Z. (2023, August). Air Quality Prediction in Smart Cities Using Cloud Machine Learning. In *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (pp. 1115-1119). IEEE.
21. Razaque, A., Frej, M. B. H., Bektemyssova, G., Almi'ani, M., Amsaad, F., Alotaibi, A., ... & Alshammari, M. (2023). Quality of Service Generalization using Parallel Turing Integration Paradigm to Support Machine Learning. *Electronics*, *12*(5), 1129.
22. Alex, S. A., Jhanjhi, N. Z., & Ray, S. K. (2023, February). Blockchain based e-medical data storage for privacy protection. In *International Conference on Mathematical Modeling and Computational Science* (pp. 125-133). Singapore: Springer Nature Singapore.
23. Chaudhary, M., Gaur, L., Chakrabarti, A., & Jhanjhi, N. Z. (2023). Unravelling the Barriers of human resource analytics: Multi-criteria decision-making approach. *Journal of Survey in Fisheries Sciences*, 306-321.
24. Gaur, L., Rana, J., & Jhanjhi, N. Z. (2023). Digital twin and healthcare research agenda and bibliometric analysis. *Digital Twins and Healthcare: Trends, Techniques, and Challenges*, 1-19.
25. Pal, S., VijayKumar, H., Akila, D., Jhanjhi, N. Z., Darwish, O. A., & Amsaad, F. (2023). Information-centric IoT-based smart farming with dynamic data optimization. *Computers, Materials & Continua*, *74*(1), 321-338.