© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713531

Legal Validity and Risk Assessment of Digital Signatures for Engineering Approvals in the Philippines

RACHELLE ANN M. FRANCISCO[1], MARVIN O. MALLARI[2]
[1] *Student, Nueva Ecija University of Science and Technology*
[1] *Faculty, FEU Pampanga*
[2] *Faculty, Nueva Ecija University of Science and Technology*

Abstract- ***The increasing digitalization of engineering workflows has accelerated the use of digital signatures for approving plans, reports, and certifications. While digital signatures promise efficiency, traceability, and improved document control, their legal validity and associated risks remain a concern for engineering professionals, particularly in safety-critical and regulated environments. This study examines the legal, technical, and organizational dimensions of digital signature use in engineering approvals in the Philippines. Using an integrative literature review, the paper analyzes Republic Act No. 8792 (Electronic Commerce Act of 2000), international standards such as the UNCITRAL Model Law on Electronic Signatures, and technical and cybersecurity literature related to cryptographic signing mechanisms. Findings indicate that digital signatures are legally valid when reliability requirements—identity authentication, integrity assurance, and signer control—are satisfied. However, risks related to key management, cybersecurity threats, inconsistent regulatory acceptance, and weak organizational governance persist. The study proposes a compliance-oriented digital signature framework tailored to engineering workflows, emphasizing governance, security controls, and long-term validation. The paper concludes that digital signatures can support professional accountability and legal defensibility when embedded within structured, risk-aware engineering management systems.***

Keywords: Digital Signatures, Engineering Approvals, RA 8792, Cybersecurity, Document Integrity, Non-Repudiation

I. INTRODUCTION

Engineering documents such as design plans, specifications, and certifications carry legal, contractual, and ethical implications. Traditionally authenticated through handwritten signatures and professional seals, these documents signify accountability and professional responsibility. With the shift toward digital workflows—intensified by remote work arrangements—engineering organizations increasingly rely on digital signatures to maintain operational continuity.

In the Philippine context, Republic Act No. 8792 provides the legal foundation for recognizing electronic and digital signatures. While the law affirms that electronic signatures cannot be denied legal effect solely due to their form, it offers limited engineering-specific guidance. This has resulted in inconsistent adoption across engineering firms and regulatory bodies. At the same time, cybersecurity literature highlights vulnerabilities in poorly implemented digital signature systems, raising concerns about document integrity and professional liability.

STATEMENT OF THE PROBLEM

1) While digital signatures are increasingly used for engineering document approvals, uncertainties remain regarding:
2) The extent to which digital signatures are legally valid for engineering documents under RA 8792.
3) The cybersecurity and technical risks associated with implementing digital signatures; and
4) The workflow requirements engineering firms must satisfy to ensure compliance, authenticity, and accountability.

OBJECTIVES OF THE STUDY

The study aims to:

1) Examine the legal validity of digital signatures for engineering approvals under RA 8792;

2) Identify technical and cybersecurity risks associated with digital signature implementation; and
3) Propose a governance-oriented framework suitable for engineering document approval workflows.

SIGNIFICANCE OF THE STUDY

The findings provide guidance for engineering professionals, managers, and regulators by clarifying legal requirements, identifying risk areas, and offering a structured framework for compliant digital signature adoption.

II. METHODOLOGY

RESEARCH DESIGN

This study adopts a qualitative integrative literature review design to examine the legal validity and risk landscape of digital signatures used in engineering approvals in the Philippines. An integrative review is particularly appropriate for this research because the subject matter spans multiple disciplines—law, cybersecurity, cryptography, and engineering management—each of which employs different analytical traditions and forms of evidence. Unlike systematic reviews that restrict inclusion to narrowly defined empirical studies, the integrative approach allows for the synthesis of statutory law, international legal frameworks, peer-reviewed research, industry standards, and professional guidelines.

The objective of the methodology is not to measure frequency or prevalence but to identify patterns, convergences, and gaps across diverse bodies of literature that collectively inform the reliability, defensibility, and risk implications of digital signatures in engineering practice. This design supports theory-building and framework development, which are central aims of the study.

SOURCES OF DATA AND LITERATURE SELECTION

The data sources for this study consist exclusively of secondary materials, categorized into five major groups:

Legal and Regulatory Sources

These include Republic Act No. 8792 (Electronic Commerce Act of 2000), related implementing rules, legal commentaries, and judicial interpretations where available. International references, particularly the UNCITRAL Model Law on Electronic Signatures, were included to provide comparative legal context and identify normative standards.

Technical and Cryptographic Literature

Peer-reviewed articles and authoritative technical references on public key infrastructure (PKI), hashing algorithms, encryption mechanisms, digital certificates, and time-stamping technologies were reviewed to establish the technical foundations of digital signature systems.

Cybersecurity and Risk Advisory Sources

Industry-recognized advisories and guidelines from organizations such as OWASP and NIST, as well as reports from cybersecurity research firms, were examined to identify known vulnerabilities, threat vectors, and mitigation strategies related to digital signature implementation.

Engineering Management and Information Systems Literature

Studies addressing document control, approval workflows, governance structures, and digital transformation in engineering and project-based organizations were included to contextualize digital signatures within real-world engineering operations.

Industry White Papers and Platform Documentation

Technical documentation and white papers from digital signature service providers were reviewed to understand common implementation practices, platform-level controls, and operational assumptions, while maintaining a critical stance regarding potential vendor bias.

SEARCH STRATEGY

A structured search strategy was employed to ensure comprehensive coverage of relevant literature. Academic databases and repositories used include Google Scholar, IEEE Xplore, ResearchGate, and university digital libraries. Legal texts and interpretations were accessed through LawPhil and official international organization repositories.

© JAN 2026 | IRE Journals | Volume 9 Issue 7 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I7-1713531

Search terms and combinations included, but were not limited to:
"digital signatures," "engineering approvals," "electronic signatures law," "RA 8792," "UNCITRAL electronic signatures," "PKI security," "digital signature risk," "engineering document control," and "cybersecurity key management."

Backward and forward citation tracking was used to identify seminal works and recent developments, ensuring both foundational and current perspectives were represented.

III. INCLUSION AND EXCLUSION CRITERIA

To maintain analytical rigor and relevance, explicit inclusion and exclusion criteria were applied.

Inclusion Criteria:
1) Literature explicitly addressing digital or electronic signature validity, reliability, or security
2) Sources discussing PKI, cryptographic authentication, and document integrity mechanisms
3) Studies examining legal, regulatory, or compliance aspects of electronic signatures
4) Engineering management literature relevant to document approval, governance, and accountability
5) Publications dated between 2000 and 2025, corresponding to the enactment of RA 8792 and subsequent developments

Exclusion Criteria:
1) Articles unrelated to authentication or digital signatures
2) Non-credible sources lacking identifiable authorship or institutional backing
3) Studies focused exclusively on non-engineering domains (e.g., medical or financial e-signatures) without transferable insights
4) Publications with insufficient methodological transparency or purely promotional content

IV. DATA ANALYSIS AND SYNTHESIS PROCEDURE

The selected literature was analyzed using a thematic coding approach, conducted in three iterative stages:

Open Coding
Initial readings identified recurring concepts such as identity verification, non-repudiation, key management, auditability, regulatory acceptance, and workflow governance.

Axial Coding
Related concepts were grouped into broader analytical categories corresponding to the study's conceptual domains: legal validity, technical assurance, cybersecurity risk, and organizational governance.

Selective Coding
The categories were integrated into a cohesive analytical framework that explains how legal, technical, and organizational factors collectively determine the reliability of digital signatures in engineering approvals.

This iterative process allowed findings from one domain to inform the interpretation of others, reinforcing the integrative nature of the analysis.

V. RELIABILITY, VALIDITY AND ANALYTICAL RIGOR

Although the study does not involve primary data collection, methodological rigor was ensured through several measures. Legal interpretations were cross-checked against official statutory texts. Technical findings were corroborated across multiple independent cybersecurity sources. Greater analytical weight was given to peer-reviewed literature and standards-setting organizations.

Potential bias arising from industry white papers was mitigated by triangulating vendor claims with independent academic and cybersecurity analyses. This triangulation strengthened the credibility and balance of the findings.

VI. ETHICAL CONSIDERATIONS

The study relies solely on publicly accessible documents and does not involve human participants, personal data, or confidential information. Ethical research practice was observed through accurate citation, faithful representation of sources, and avoidance of plagiarism. No conflicts of interest were identified in the conduct of the review.

VII. RESULTS AND DISCUSSION

This section presents an expanded synthesis of findings derived from legal texts, international frameworks, cybersecurity literature, and engineering management studies. Rather than reporting empirical measurements, the discussion critically evaluates patterns, convergences, and gaps across the reviewed literature. The results are organized into five interrelated domains: (1) legal validity, (2) alignment between Philippine and international frameworks, (3) technical assurance and limitations, (4) cybersecurity and operational risks, and (5) implications for engineering workflows and professional accountability.

A. Legal Validity of Digital Signatures Under Philippine Law

The literature consistently affirms that digital signatures are legally recognized in the Philippines under Republic Act No. 8792, provided that the method used satisfies the law's reliability requirement. Reliability is not defined by the mere use of digital technology but by the functional outcomes of the signing process. Legal analyses emphasize three essential conditions: the ability to uniquely identify the signer, the assurance that the signer retains sole control of the signing mechanism, and the capability to detect any alteration to the document after signing.

Unlike traditional handwritten signatures, which rely on visual inspection and expert testimony, digital signatures depend on demonstrable technical and procedural safeguards. Several legal commentaries note that courts and regulators are less concerned with the specific technology used and more focused on whether the signing process can withstand challenges related to authorship, intent, and document integrity. This finding supports the position that digital signatures, when properly implemented, can meet or exceed the evidentiary value of handwritten signatures.

However, the review also reveals that legal validity remains conditional rather than automatic. Digital signatures that lack verifiable identity proofing, proper key management, or audit trails may fail to satisfy the reliability threshold, exposing engineering documents to legal dispute.

B. Alignment and Gaps Between RA 8792 and UNCITRAL Principles

The analysis shows strong conceptual alignment between RA 8792 and the UNCITRAL Model Law on Electronic Signatures. Both frameworks adopt a technology-neutral approach and emphasize functional reliability rather than prescribing specific tools. UNCITRAL further refines this approach by distinguishing between different levels of electronic signatures, ranging from basic electronic signatures to advanced and qualified signatures.

Despite this alignment, a critical gap emerges at the implementation level. UNCITRAL provides clearer guidance on reliability assessment, certification authorities, and trust services, whereas RA 8792 leaves these determinations largely to practitioners, regulators, and the courts. For engineering practice, this gap introduces uncertainty because acceptance of digitally signed documents may vary across agencies, projects, and jurisdictions.

Engineering management literature highlights that this regulatory ambiguity leads to inconsistent adoption. Some local government units and agencies accept digitally signed plans, while others continue to require wet-ink signatures. This inconsistency increases transaction costs, delays project approvals, and discourages full digital transformation in engineering organizations.

C. Technical Strengths and Limitations of Digital Signatures

Technical literature overwhelmingly supports the cryptographic robustness of public key infrastructure (PKI)-based digital signatures. Studies consistently

demonstrate that modern cryptographic algorithms provide strong protection against forgery and unauthorized document alteration. Hash functions ensure that even minor modifications invalidate the signature, reinforcing document integrity and non-repudiation.

However, this study's findings challenge the assumption—common in earlier technical research—that cryptographic strength alone guarantees reliability. Multiple sources indicate that implementation failures, rather than algorithmic weaknesses, are the dominant causes of digital signature compromise. These failures include insecure private key storage, weak password practices, absence of multi-factor authentication, and inadequate device security.

From an engineering management perspective, these findings are significant. Engineering documents often remain in circulation for years or decades due to regulatory, contractual, and liability considerations. Without long-term validation mechanisms and proper certificate lifecycle management, digitally signed documents may become unverifiable over time, undermining their legal defensibility.

D. Cybersecurity Risks and Operational Vulnerabilities

Cybersecurity literature identifies several recurring threat vectors affecting digital signature systems. Private key compromise is consistently identified as the most critical risk. When a signing key is stolen or misused, all documents signed with that key become suspect, potentially exposing engineers and organizations to significant liability.

Document manipulation attacks also emerge as a concern, particularly in commonly used formats such as PDFs. While digital signatures are designed to detect tampering, studies show that improperly configured document workflows may allow incremental updates, metadata manipulation, or format conversions that weaken integrity assurance.

Platform-level risks further complicate the issue. Many commercial digital signature platforms prioritize usability and speed over high-assurance authentication. Engineering management literature cautions that platforms suitable for routine business transactions may be inadequate for engineering approvals, where the consequences of signature misuse are far more severe.

These findings reinforce the conclusion that digital signatures must be embedded within secure systems and governed by clear organizational policies rather than treated as standalone tools.

E. Engineering Workflow Implications and Professional Accountability

The review highlights that engineering workflows impose higher assurance requirements than most commercial document processes. Engineering documents frequently require multiple signatories from different disciplines, sequential approvals, and strict version control. A single failure in identity verification or document integrity can invalidate an entire approval chain.

The literature is particularly critical of the continued use of scanned handwritten signatures. Such practices provide no cryptographic protection, are easily replicated, and offer little defense in legal disputes. Courts and regulators may treat these methods as weak evidence of authenticity when challenged.

Professional accountability emerges as a central theme. Engineering signatures represent personal responsibility and ethical obligation, not merely administrative approval. As such, digital signatures used in engineering must be issued to individual licensed professionals, not shared or generic organizational accounts. This requirement aligns with both legal standards and professional ethics literature.

F. Synthesis of Findings

Taking together, the results demonstrate that digital signatures are legally and technically viable for engineering approvals, but only when supported by strong governance, secure operational practices, and clear regulatory guidance. The findings extend prior research by showing that the principal risks are organizational rather than cryptographic in nature.

This synthesis supports the study's central argument: digital signatures in engineering should be evaluated as socio-technical systems that integrate law,

technology, and management. Without this integrated approach, digital adoption may increase efficiency while simultaneously introducing new forms of professional and legal risk.

VIII. PEER REVIEW

Following the completion of the manuscript, the study underwent a peer review process involving colleagues with backgrounds in engineering management, information systems, and legal-regulatory studies. The purpose of the review was to critically evaluate the paper's conceptual rigor, legal interpretation, methodological coherence, and practical relevance to engineering practice.

Reviewers provided extensive comments focusing on the clarity of the research objectives, the sufficiency of legal and technical integration, and the strength of the discussion linking cybersecurity risks to engineering accountability. Particular attention was given to the interpretation of Republic Act No. 8792, the applicability of international frameworks such as UNCITRAL, and the consistency between the stated methodology and the conclusions drawn.

Several reviewers also assessed the paper's structure, noting areas where arguments could be strengthened through clearer transitions, deeper comparative analysis, and more explicit articulation of the study's contribution to engineering management literature. Constructive criticism was encouraged, and both major and minor comments were solicited to ensure robustness, even in sections where the author initially expressed high confidence.

The peer review process served as a critical validation step, ensuring that the research met academic standards for originality, analytical depth, and relevance prior to consideration for journal submission.

IX. IMPROVEMENT AS PER REVIEWER COMMENTS

All reviewer comments were carefully analyzed and categorized into substantive (major) and editorial (minor) revisions. Each comment was examined in relation to the study's objectives to determine whether it required clarification, expansion, restructuring, or methodological refinement.

Major Revisions Implemented

Clarification of Legal Interpretation

Reviewers recommended a clearer explanation of how RA 8792's reliability requirement applies specifically to engineering documents. In response, the discussion section was expanded to explicitly link legal criteria (identity authentication, signer control, and document integrity) to engineering approval workflows and professional accountability.

Strengthening the Law–Technology–Management Integration

To address comments regarding fragmentation between legal, technical, and organizational discussions, the Results and Discussion section was reorganized into interrelated domains. This improved coherence and reinforced the study's socio-technical perspective.

Expansion of Cybersecurity Risk Analysis

Reviewers noted that while cryptographic mechanisms were well discussed, operational risks required deeper emphasis. Additional analysis was incorporated on key management failures, platform-level vulnerabilities, and long-term validation issues relevant to engineering documents with extended legal lifespans.

Justification of Methodological Choice

Based on feedback, the methodology section was expanded to better justify the use of an integrative literature review. Explicit distinctions were made between integrative, systematic, and narrative reviews to strengthen methodological transparency.

Minor Revisions Implemented

1) Improved clarity and consistency of terminology (e.g., distinguishing "electronic signatures" from "PKI-based digital signatures")
2) Enhanced transitions between sections to improve readability
3) Refined objective statements to align more closely with conclusions and recommendations
4) Corrected formatting, numbering inconsistencies, and typographical errors

Addressing Critical Remarks

Some reviewers raised concerns regarding the absence of empirical validation. While acknowledging this limitation, the paper was revised to clearly position its contribution as theoretical, legal-analytical, and framework-building, rather than empirical testing. This clarification strengthened the paper's scope and prevented overextension of claims.

In cases where reviewer comments required domain-specific clarification, additional authoritative sources were consulted to ensure accuracy and confidence in the revisions. Rather than being discouraged by critical feedback, the comments were treated as opportunities to enhance the paper's scholarly depth and practical relevance.

X. CONCLUSION

Digital signatures are legally valid for engineering use in the Philippines when implemented in compliance with RA 8792 reliability requirements. However, cryptographic strength alone is insufficient; organizational governance and secure operational practices are equally critical. Engineering workflows demand higher assurance standards due to public safety and long-term liability considerations.

Conclusion 1: Digital signatures are legally valid for engineering under specific conditions.

RA 8792 clearly recognizes digital signatures, but their validity depends on demonstrating reliability through identity verification, control of signing keys, and tamper detection. This means not all signatures are automatically valid; scanned signatures, unsecured digital signatures, and signatures lacking proper audit trails may still be rejected in legal or regulatory contexts.

Conclusion 2: Technical security alone is insufficient to ensure validity.

Cryptographic strength must be supported by robust operational practices. The literature shows that private key protection, secure devices, MFA, timestamping, and document-locking mechanisms are essential to prevent misuse. Without these, even strong algorithms fail to safeguard authenticity.

Conclusion 3: Engineering workflows require higher assurance than typical digital transactions.

Engineering documents differ from general business documents because they impact public safety, infrastructure reliability, and long-term regulatory compliance. Engineering digital-signature systems must therefore sustain authentication and integrity over decades—a challenge requiring long-term validation strategies.

Conclusion 4: Organizational governance is a major determinant of signature reliability.

Without clear roles, approval matrices, procedures, and compliance policies, digital signatures cannot meet RA 8792's reliability requirement. Governance failures—not technical issues—are the most common source of liability exposure.

Conclusion 5: A structured framework is necessary for industry-wide adoption.

The Five-Pillar Framework developed in this study provides a clear, actionable path for engineering firms, regulators, and professionals. By integrating legal, technical, and workflow considerations, the framework bridges the gap between law and engineering practice.

ACKNOWLEDGMENT

The author would like to express sincere appreciation to the faculty and academic mentors of Nueva Ecija University of Science and Technology for their guidance and intellectual support throughout the conduct of this study. Their insights in engineering management, research methodology, and professional practice greatly contributed to the refinement of the paper.

Gratitude is also extended to peers and subject matter experts who provided critical reviews and constructive feedback during the manuscript evaluation process. Their comments were instrumental in strengthening the legal, technical, and organizational analyses presented in this research.

The author acknowledges the contributions of legal scholars, cybersecurity professionals, and engineering practitioners whose published works formed the foundation of the integrative literature

review. The availability of statutory materials, international frameworks, and cybersecurity guidelines significantly enriched the interdisciplinary perspective of the study.

Finally, the author expresses appreciation to the institutions and organizations that promote open access to academic, legal, and technical resources, which made this research possible. Any errors or omissions remain the sole responsibility of the author.

REFERENCES

[1] Cryptomathic. (2022, January 21). Managing risks in cryptographic key management. https://www.cryptomathic.com/blog/cryptographic-key-management-the-risks-and-mitigations

[2] eSignWS. (2025, March 17). What are the risks of using eSignatures? https://esign-blog.dmsworkspace.com/2025/03/17/what-are-the-risks-of-using-esignatures/

[3] Koonthamattam, L. (2024, May 21). How to overcome vulnerabilities in digital signatures. CybelAngel. https://cybelangel.com/blog/digital-signatures-are-the-cybersecurity-vulnerability-you-need-to-stop-ignoring/

[4] OWASP. (n.d.). Key management cheat sheet. OWASP Cheat Sheet Series. https://cheatsheetseries.owasp.org/

[5] Republic Act No. 8792, Electronic Commerce Act of 2000. (2000). Republic of the Philippines. https://lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html

[6] United Nations Commission on International Trade Law. (2002). UNCITRAL model law on electronic signatures with guide to enactment 2001. United Nations. https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf