

Implementation of Electronic Signatures in Official Document Management: An Analysis of Legal Certainty and Legal Effectiveness at UIN K.H. Abdurrahman Wahid Pekalongan

Dyah Syifa Herawati¹, Qothrun Nada^{2*}, Chusna Shoimmah³

^{1,2,3} UIN K.H. Abdurrahman Wahid Pekalongan, Indonesia

*Correspondence: qothrun.nada@uingusdur.ac.id

Received: 21 August 2026

Accepted: 24 September 2026

Published: 18 October 2026

Abstrak

Penelitian ini bertujuan untuk menganalisis kepastian hukum dan efektivitas implementasi tanda tangan elektronik (TTE) dalam tata naskah dinas elektronik di UIN K.H. Abdurrahman Wahid Pekalongan serta mengidentifikasi faktor-faktor yang memengaruhi penerapannya. Penelitian ini menggunakan metode penelitian hukum dengan pendekatan yuridis empiris. Data diperoleh melalui studi kepustakaan, wawancara, dan observasi, kemudian dianalisis secara kualitatif dengan menggunakan teori efektivitas hukum dan teori implementasi kebijakan. Hasil penelitian menunjukkan bahwa implementasi TTE telah berjalan dan didukung oleh konsistensi pimpinan serta ketersediaan aplikasi TTE yang memadai. Namun, efektivitas penerapannya belum optimal karena belum tersedianya regulasi internal yang secara komprehensif mengatur prosedur penggunaan, penjaminan keabsahan, dan mekanisme penanganan kendala TTE. Selain itu, pemahaman dan sosialisasi kepada petugas masih perlu ditingkatkan, proses pembaruan sertifikat elektronik memerlukan koordinasi berjenjang dengan Kementerian Agama dan Balai Sertifikasi Elektronik (BSrE), serta proses disposisi surat masuk masih dilakukan secara manual. Berdasarkan temuan tersebut, diperlukan penguatan regulasi internal, peningkatan kompetensi sumber daya manusia, perencanaan pembaruan sertifikat elektronik, dan penyusunan mekanisme penanganan kendala yang terstandar. Dengan demikian, efektivitas implementasi TTE tidak hanya bergantung pada ketersediaan teknologi, tetapi juga pada kepastian regulasi, kesiapan sumber daya manusia, dan dukungan tata kelola kelembagaan yang terintegrasi.

Kata Kunci: Tanda Tangan Elektronik; Efektivitas Hukum; Tata Naskah Dinas.

Abstract

This study aims to analyze the legal certainty and implementation effectiveness of electronic signatures (TTE) within the electronic official document management system at UIN K.H. Abdurrahman Wahid Pekalongan, as well as to identify the factors influencing their application. This study employs a legal research method using an empirical juridical approach. Data were collected through literature review, interviews, and observations, and subsequently analyzed qualitatively using legal effectiveness theory and policy implementation theory. The findings indicate that the implementation of electronic signatures is currently underway, supported by consistent leadership and adequate electronic signature applications. However, its effectiveness remains sub-optimal due to the lack of comprehensive internal regulations governing usage procedures, validity assurance, and troubleshooting mechanisms for electronic signatures. Furthermore, staff understanding and dissemination still need improvement, the electronic certificate renewal process

requires multi-tiered coordination with the Ministry of Religious Affairs and the Electronic Certification Center (BSrE), and incoming mail disposition is still carried out manually. Based on these findings, it is necessary to strengthen internal regulations, enhance human resource competencies, plan electronic certificate renewals, and establish standardized mechanisms for handling technical issues. Consequently, the effectiveness of electronic signature implementation relies not only on technological availability, but also on regulatory certainty, human resource readiness, and integrated institutional governance support.

Keywords: Electronic Signatures; Legal Effectiveness; Official Document Management.

INTRODUCTION

Technological development is driving the transition toward digital administrative governance in higher education. UIN K.H. Abdurrahman Wahid Pekalongan has undertaken this transition as part of the implementation of Indonesia's Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE).

SPBE is the administration of government through information and communication technology to provide services to its users, including government institutions, civil servants, businesses, the public, and other parties. Its objectives include faster, more transparent, and more accessible governance. SPBE encompasses internal administration, public services, and digitally supported policymaking. The digitalization of administrative governance is therefore one means of implementing electronic government.¹

In practice, UIN K.H. Abdurrahman Wahid Pekalongan has digitalized administrative governance through E-Model, in which electronic official documents are prepared, approved through a hierarchy, and authenticated electronically. Electronic signatures (tanda tangan elektronik, TTE) facilitate document approval where obtaining a handwritten signature is delayed because the authorized official is working outside the office or undertaking official travel.

Electronic signatures also support efforts to reduce paper use at UIN K.H. Abdurrahman Wahid Pekalongan. Their legal basis is established in Law Number 11 of 2008 concerning Electronic Information and Transactions and further regulated in Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions. These instruments recognize their legal force and legal effects where the applicable requirements are fulfilled.²

Despite these advantages and an established legal basis, the implementation of electronic signatures in the university's electronic official document management continues to encounter practical challenges and debate.

Implementation has not fully achieved its intended objectives. A gap remains between the legal certainty established by regulation and the effectiveness of implementation in government institutions, including State Islamic Religious Higher Education Institutions (Perguruan Tinggi Keagamaan Islam Negeri, PTKIN). This gap concerns technical operation, institutional arrangements, information security,

¹ Angel Firstia Kresna, *Legalitas Tanda Tangan Elektronik Pejabat Dalam Rangka Mendukung E-Government*, 2019.

² Rizka Indriani Julfitri and Cathas Teguh Prakoso, *eJournal Administrasi Publik* 11, no. 3 (2023).

consistency in correspondence management, and staff understanding of electronic signature procedures.

At UIN K.H. Abdurrahman Wahid Pekalongan, staff understanding of electronic signature procedures remains uneven. Technical training and information sessions dealing specifically with operating procedures, legal requirements, and verification mechanisms remain limited. Implementation consequently depends heavily on individual users' understanding, creating risks of procedural errors, inconsistent practice, and uncertainty about the validity of the resulting electronic documents.

Implementation also faces cybersecurity challenges. Electronic signatures depend on the electronic systems through which they are applied. Without adequate information security, these systems may be exposed to unauthorized access, digital identity theft, misuse of electronic certificates, intrusion, and document forgery. Such risks may weaken confidence in electronic signatures and raise questions about authentication, integrity, and non-repudiation in electronic transactions.

The Integrated Dynamic Archival Information System (Sistem Informasi Kearsipan Dinamis Terintegrasi, SRIKANDI) has also not been implemented optimally as a national correspondence system. Although the National Archives of the Republic of Indonesia (ANRI) has issued policies encouraging its use for electronic official document management in government institutions, implementation continues to encounter system disruptions, limited interoperability, and differences in institutional information technology infrastructure. These conditions have hindered its use in PTKIN institutions under the Ministry of Religious Affairs.

Incomplete implementation of SRIKANDI has contributed to the absence of a uniform electronic correspondence system across PTKIN institutions. Universities consequently develop or adopt different applications according to their institutional needs. This creates variations in document issuance, electronic signing, electronic archiving, and document classification and coding. Official document and archive management in government institutions should nevertheless be orderly, standardized, and consistent with the principles established in Law Number 43 of 2009 concerning Archives.

These differences raise legal questions about documents bearing electronic signatures. Although such signatures are recognized in law, their application through different correspondence systems raises issues concerning compliance with national electronic system standards, the validity of authentication, and consistency in electronic archive governance across government institutions.

Against this background, the study analyzes the legality of electronic signatures in official document management at UIN K.H. Abdurrahman Wahid Pekalongan through an examination of the relevant regulations. It also identifies and analyzes the legal, technical, and administrative factors affecting implementation.

RESEARCH METHOD

This study employs an empirical juridical method combining normative analysis of legislation with field evidence on the use of electronic signatures in official document management at UIN K.H. Abdurrahman Wahid Pekalongan. It is descriptive and analytical: it systematically describes legality, obstacles, and implementation effectiveness, then examines them against the applicable legal framework. The instruments examined include the Electronic Information and Transactions Law, Government Regulation Number 71 of 2019 concerning the

Operation of Electronic Systems and Transactions, Presidential Regulation Number 95 of 2018 concerning SPBE, Minister of Religious Affairs Decision Number 9 of 2016, and internal university rules. Primary data are drawn from interviews with correspondence managers, administrative personnel, and officials using electronic signatures. Secondary data are obtained through a literature review. The materials are analyzed descriptively and qualitatively.

Methodological Limitations and Operationalization of Variables

The empirical juridical approach combines the interviews recorded in the research materials with an examination of relevant regulations. The available documentation does not fully identify the total number of informants, selection procedures, dates of individual interviews, units observed, or access to application logs and standard operating procedures (SOPs). Informants' accounts are therefore treated as evidence of their implementation experience. Assessing procedural compliance requires authorization documents, anonymized archive samples, and administrative records for triangulation.

RESULTS AND DISCUSSION

1. Electronic Signature Implementation through the Theory of Legal Effectiveness

The study applies Soerjono Soekanto's theory of legal effectiveness, which identifies five factors: the law itself, law enforcement actors, supporting facilities, society, and culture.

a. The Legal Framework

The legal framework cannot be established by a general reference to the Electronic Information and Transactions Law alone. Article 11 of Law Number 11 of 2008, as amended, including by Law Number 1 of 2024, establishes requirements for the legal force of electronic signatures; Article 5 regulates electronic information and documents as evidence within statutory limits. Government Regulation Number 71 of 2019, particularly Articles 59–60, specifies requirements and distinguishes certified from uncertified electronic signatures. Certified signatures use certificates issued by an Indonesian electronic certification provider and certified signature-creation devices. Uncertified signatures are not automatically invalid, but must still be assessed against legal requirements, authentication, and document integrity. The use of TNDE E-Model, SRIKANDI, or another application does not itself determine signature validity.

The university's official document management guidelines address document types and authority for preparation, determination, and signing; document drafting; correspondence management; authorized signatories; document form, format, and numbering; and archival classification. They do not, however, specify which document types may use electronic signatures and which still require handwritten signatures. Documents differ in their characteristics and significance. Some may be processed entirely electronically, while others require particular treatment because of their nature, purpose, or applicable rules. Unclear classification may therefore lead to different practices across university units and inconsistent official document management.

Legal certainty requires verifiable procedures: matching the signatory's identity to the authority of the office; checking the certificate issuer and chain;

examining file integrity and certificate revocation status; establishing certificate validity at the time of signing; and retaining evidence of time and audit records. These checks must be distinguished from administrative examination of document numbers, archive classification, and signing authority. Documents produced by different correspondence applications are not automatically invalid; interoperability and retention are separate archive management questions.

The internal system should allocate responsibilities clearly. Signatories are responsible for substantive approval, use of their personal credentials, and reporting suspected misuse. Correspondence operators are responsible for administrative completeness, routing, and audit trails within their access permissions, but must not use signatories' credentials. Information technology managers are responsible for technical security, backup, recovery, and incident recording. Suspected unauthorized certificate use should be examined separately from questions of document invalidity and its implications for data protection and staff discipline.

Electronic archiving requires retention standards under Law Number 43 of 2009 and the applicable technical archival rules. These include access classification, backup copies, format-change controls, version tracking, and preservation of signature verification information after a certificate expires. A certificate expiring after signing must be distinguished from a certificate that was invalid or revoked when the signature was applied. Internal SOPs should document long-term validation strategies, document recovery procedures, and authority to access archives.³

b. Actors Implementing Administrative Rules

In applying Soerjono Soekanto's framework, the law enforcement factor is used here by analogy to actors implementing administrative norms. University officials and operators are not equated with police officers, prosecutors, or judges. The analysis concerns institutional capacity, appropriate delegation, procedural consistency, and internal supervision. Policy implementers must be distinguished from actors possessing formal law enforcement powers.⁴

The findings indicate an institutional allocation of roles in document preparation, verification, and signing. University leaders have also consistently used electronic signatures for designated documents while retaining verification before signing. Implementation effectiveness nevertheless remains affected by several factors.

First, staff understanding remains uneven. Some employees understand the procedures, while others view electronic signatures simply as substitutes for handwritten signatures. Understanding authority, authentication, security, and legal consequences is necessary for orderly administration.

Second, staff competence in operating the system needs improvement. Some users can operate it independently, while newly appointed or transferred personnel still experience difficulties. The absence of regular training contributes to uneven capability and potential dependence on particular operators.

³ Nurfitriyani Siregar, "Efektivitas Hukum," *JHI* 4, no. 3 (2020): 75–86.

⁴ Tiara Jabbar Purwanto and Djumadi Purwoadmojo, "Tinjauan Yuridis Legalitas Penggunaan Tanda Tangan Elektronik Dalam Akta Notaris," *Notarius* 16, no. 2 (2023): 989–97, <https://doi.org/10.14710/nts.v16i2.42261>.

Third, procedural compliance indicates that electronic signing follows the prescribed process for certain documents, while other document types continue to use handwritten signatures. Consistency should therefore be strengthened with regard to document characteristics and the applicable requirements.

Fourth, the consistency of authorized officials supports implementation. Interview accounts indicate that they consistently use electronic signatures for designated documents. This practice provides an example for staff and encourages greater consistency in electronic administration.

Fifth, coordination between correspondence managers and information technology personnel has supported implementation, particularly account and certificate management and assistance from central administrators. Resolving technical problems may nevertheless require coordination with the external application developer. Coordination should therefore be strengthened to address technical and administrative problems effectively.

Sixth, user information sessions and guidance have not been sustained. Initial training and information sessions took place when TNDE E-Model was introduced in 2021, while new employees have largely relied on more experienced users for assistance. This may produce differences in understanding, particularly when systems or procedures change. Regular training and guidance are consequently needed to support a shared understanding of electronic signature rules and procedures.⁵

The interview accounts indicate that roles and electronic signing practices have been established, but differences in understanding and continuity of training require further examination. A finding of relative effectiveness cannot be quantified from interviews without identified document counts, sampled units, verification failure frequencies, and training records. The defensible finding is evidence of implementation accompanied by supervision and documentation gaps; university-wide effectiveness remains unmeasured.

c. Supporting Facilities and Infrastructure

Facilities and infrastructure are among the factors affecting electronic signature implementation at the university. Interviews with Saiful Anam, a pioneer of the university's TNDE system, indicate that supporting facilities generally include E-Model, internet connectivity, computers, and facilities supporting electronic signatures certified through BSrE.⁶

These findings indicate institutional efforts to provide infrastructure for electronic official document administration. Such infrastructure is a necessary condition: a legal basis alone cannot implement electronic signatures without the technology needed to apply the rules in practice.

An informant reported delays in electronic certificate renewal and changes in the application process. The documentation does not, however, identify the title and number of the legal instrument underlying those changes, its effective date, application numbers, service durations, or evidence explaining the delays. The account therefore requires triangulation with application forms, helpdesk logs, and

⁵ Nur Aripkiah and Khairunnisa Noor Asufie, "Tinjauan Yuridis Tindak Pidana Pemalsuan Tanda Tangan Elektronik dalam Kerangka Hukum Positif Indonesia" 3, no. 1 (2024).

⁶ Saiful Anam (TNDE pioneer), interview by Dyah, UIN K.H. Abdurrahman Wahid Pekalongan, Pekalongan, July 22, 2026.

official correspondence from the certification provider. It does not establish that regulatory change necessarily caused the delays.

The findings also indicate that the availability of facilities does not necessarily mean they are used optimally. Interview accounts describe problems involving network disruption, system stability, equipment limitations, and certificate renewal and recovery. One informant stated that E-Model did not provide adequate archiving, making separate archiving necessary. Another observed that several letter formats in E-Model did not conform to the relevant official document management rules. The issue therefore concerns the capacity of facilities to support administrative needs consistently, as well as their availability.

In Soerjono Soekanto's theory, these conditions relate to the facilities supporting legal implementation. A legal rule is unlikely to be effective without adequate facilities. Although electronic signatures have a legal basis, implementation effectiveness depends substantially on the technological infrastructure available to personnel.⁷

Network disruptions reportedly continue in certain circumstances, sometimes delaying document signing and distribution. Processes that could otherwise be completed promptly must wait for the system or network to recover. Infrastructure quality therefore affects implementation: more stable facilities reduce obstacles to compliance with electronic signature procedures.

The effectiveness of electronic signatures cannot be measured solely by the presence of an application or signing facility. Assessment must consider its ability to support the entire administrative process. The system should make document issuance accessible, timely, secure, and reliable. Indicators therefore concern both the availability of facilities and their functionality and usability.

The study also identifies limited technical support from the university's UTIPD team because E-Model continues to involve an external developer. According to Saiful Anam, users experiencing technical problems must seek assistance from the developer, which may take considerable time. Technical support is therefore integral to implementation infrastructure. Digital systems require continuing management to operate reliably.

From a legal effectiveness perspective, technical support connects rules with practice. Personnel facing technical problems can continue to perform their duties where a clear and timely resolution mechanism exists. Where problems remain unresolved, users may return to manual procedures. Repeated recourse to those procedures may impede the objectives of digital official document management.⁸

Informants reported that some incoming correspondence routing and disposition processes still involve printing and manual archiving. Without document counts, a defined observation period, and investigation of administrative reasons in individual units, the study cannot estimate university-wide paper use. The accounts suggest a possible hybrid process requiring assessment against archive classification SOPs and the characteristics of documents for which a particular form remains legally required.

⁷ Naurah Imtiyazah et al., "Tinjauan Aspek Legalitas Dan Keamanan Penggunaan Tanda Tangan Elektronik Pada Rekam Medis Elektronik Di Rumah Sakit X Kota Cimahi," *OJS* 19, no. 3 (2024): 4014–22.

⁸ Nazaruddin Lathif, "Teori Hukum Sebagai Sarana Alat Untuk Memperbaharui atau Merekayasa Masyarakat," *Pilar Pakuan Law Review* 3, no. 1 (2017): 402.

These conditions may indicate both limitations in infrastructure and issues concerning implementing personnel and legal culture. The factors in Soerjono Soekanto's framework do not operate independently. Adequate facilities must be supported by competent and compliant personnel and a working culture that accepts electronic administration.

The availability of TNDE, equipment, and connectivity supports electronic signing but does not establish effectiveness throughout the administrative process. The interview documentation examined does not provide incident logs, verification success rates, signing durations, or archive retention measures. The study therefore does not assign an empirical effectiveness score. Its assessment is descriptive and qualitative and identifies risks requiring audit.

Facilities and infrastructure have contributed to implementation, but effectiveness depends on their quality and continuity. Within Soerjono Soekanto's framework, facilities support legal effectiveness where they enable accessible, secure, prompt, and sustainable electronic signing. System failures, network limitations, incomplete integration, and weak technical support may instead hinder implementation.

Strengthening implementation at UIN K.H. Abdurrahman Wahid Pekalongan consequently requires institutional policies and applications to be supported by better connectivity, reliable systems, system integration, equipment and application maintenance, and responsive technical assistance. These measures are needed to ensure that infrastructure can sustain the transition from conventional to electronic official document management.

2. Electronic Signature Implementation through Policy Implementation Theory

Electronic signature implementation at UIN K.H. Abdurrahman Wahid Pekalongan forms part of the transition toward electronic government administration intended to improve effectiveness, efficiency, security, and accountability in official document management. It concerns the translation of policy into working procedures, staff readiness, infrastructure, and coordination among the units involved, as well as the technology used to sign documents.

George C. Edward III's policy implementation theory identifies four principal variables affecting implementation: communication, resources, implementers' disposition or attitudes, and bureaucratic structure. These variables provide a framework for examining electronic signature implementation in the university's official document management.⁹

a. Communication

Implementation requires clear and consistent information for everyone involved in official document management. This includes the policy basis, application and activation mechanisms, operating procedures, signing authority, and procedures for responding to technical difficulties.¹⁰

At the university, implementation involves leaders holding signing authority, administrative units managing official documents, and information technology units supporting technical operations. Effective communication across these units is therefore necessary.

⁹ Muhammad Sinathria Maharaksa et al., *Implementasi Kebijakan Publik: Pengertian, Model-Model dan Penerapannya dalam Contoh Studi Kasus*, n.d.

¹⁰ Ibrahim Kristofol Kendi, *Implementasi Kebijakan Publik*, n.d.

Where implementers do not share an understanding of electronic signature procedures, administrative practices may differ, creating procedural errors, dependence on particular operators, and signing delays. Written policies must therefore be supported by continuing communication through information sessions, technical guidance, user assistance, and help services.

The interviews did not identify these communication problems as a general feature of practice at the university. They described electronic signing as following established procedures with a degree of consistency across units. Central administrators nevertheless still need to clarify instructions to individual units when errors occur.

b. Resources

Resources are another important implementation variable. They include personnel, facilities, infrastructure, budgets, and information system support, as well as technological equipment.¹¹

Implementation requires personnel who understand electronic official document procedures and can operate the system. Limited digital competence may make implementation dependent on particular technically proficient employees. This can threaten continuity when those employees are unavailable.

Implementation also depends on internet connectivity, computers, electronic correspondence systems, and certificate services. Network disruption, incomplete system integration, and expired certificates may prevent signing and delay administrative services.

Reports of expired certificates indicate that technology resource management must include certificate maintenance and lifecycle management. Certificate validity should be monitored and renewal coordinated systematically so that it can be completed before expiry.

From Edward III's perspective, electronic signature implementation is unlikely to achieve its policy objectives without adequate resources, even where policies and procedures are already available.

c. Implementers' Disposition

Disposition concerns implementers' attitudes, commitment, acceptance, and willingness to carry out a policy.¹² In electronic signature implementation, staff acceptance of the transition from conventional to electronic administration is therefore an important element of organizational change.¹³

Electronic signatures change working practices previously based on paper documents, handwritten signatures, and direct physical distribution. Personnel must adapt to this transition. Where staff understand and support administrative digitalization, electronic signatures can accelerate work and reduce reliance on physical documents.

Where staff instead retain conventional practices because they consider them easier or more familiar, electronic signatures may be implemented administratively without substantially changing organizational working culture. Implementation

¹¹ Kendi, *Implementasi Kebijakan Publik*.

¹² Kendi, *Implementasi Kebijakan Publik*.

¹³ Maharaksa et al., *Implementasi Kebijakan Publik: Pengertian, Model-Model dan Penerapannya dalam Contoh Studi Kasus*.

should therefore be understood as part of a transition toward digital, effective, and accountable administrative governance.

At UIN K.H. Abdurrahman Wahid Pekalongan, several stages of the electronic signature application process already operate electronically under TNDE procedures. Incoming correspondence routing and disposition nevertheless continue to use physical files for checking and reducing errors.

d. Bureaucratic Structure

Implementation is also affected by the bureaucratic structure allocating authority, procedures, and coordination across units. Official document management requires clarity about who may prepare, examine, process, and sign documents electronically.¹⁴

SOPs are needed to support consistent use across units. They should govern the electronic document process from drafting, verification, and initialling where required, through signing, distribution, and archiving.

Clear authority and straightforward procedures make implementation easier. Lengthy procedures, overlapping powers, and unclear problem-resolution mechanisms may instead reduce administrative effectiveness.

The research materials link the absence of a mechanism for handling electronic signature problems to the regulatory framework, including Minister of Religious Affairs Regulation Number 12 of 2026 concerning Electronic Official Document Management within the Ministry of Religious Affairs. They indicate that procedures for renewal and other difficulties remain insufficiently specified. Internal rules also require strengthening because PTKIN electronic document management systems are not centrally uniform and institutions have scope to develop their own systems.

The four variables in Edward III's framework show that implementation results from the interaction of policy communication, resource adequacy, implementers' attitudes, and bureaucratic structure. Technology availability is only one component.

Existing electronic signing practices indicate that digital official document policy has been translated into administration. Expired certificates, renewal requirements, dependence on technical support, and differences in user understanding nevertheless suggest a need for stronger signature management, coordination, staff competence, and standardized procedures.

Electronic signatures can be said to have been implemented in the practices described by informants. The examined data do not, however, provide cross-unit or longitudinal measures permitting a quantified assessment of effectiveness. Conclusions must distinguish the existence of policy, operational compliance in observed samples, and institutional service outcomes.

Academically, successful implementation should be assessed by the extent to which electronic signatures are consistently integrated throughout official document management, improve service efficiency, support document security and validity, and sustain effective administration. The number of electronically signed documents alone does not establish these outcomes.

¹⁴ Maharaksa et al., *Implementasi Kebijakan Publik: Pengertian, Model-Model dan Penerapannya dalam Contoh Studi Kasus*.

3. Operational Factors Affecting Electronic Signature Implementation

a. Communication

Communication requires effective information exchange among signatories, document management units, and administrative staff so that they share an understanding of electronic signature procedures. It includes information transmission, clarity, and consistency. These interconnected dimensions influence whether a policy is understood and applied correctly.¹⁵

Information Transmission

Information transmission concerns how electronic signature policy and operating procedures are communicated to the parties involved. Informants reported several technical information sessions before E-Model was introduced. These sessions explained the process from document submission to electronic signing.

The sessions indicate efforts to communicate policy to implementers. Implementation depends on users' ability to understand and follow established procedures as well as on system availability. Clear communication to signatories and document management staff can reduce operating errors.

Information Clarity

Information must use language and procedures that application users can understand. Staff need to know when electronic signatures are used, who may sign, which documents may be signed electronically, and how the process operates. Although the study did not identify a dedicated SOP governing E-Model electronic signatures, implementation has been supported by direct instructions from signatories to application administrators. Administrators receive guidance on the documents that may be prepared and processed in E-Model and on hierarchical approval, from drafting and examination to approval and electronic signing by the authorized official. These instructions have helped administrators understand the workflow.

Information Consistency

Information consistency concerns continuing communication before and after implementation. This continuity is needed to maintain user understanding when staff change or E-Model procedures are updated. Initial information sessions were held before implementation, but regular follow-up sessions have not been established. New staff consequently experience difficulties despite guidance from more experienced colleagues.¹⁶

Communication has supported implementation, particularly through initial information transmission and direct instructions from signatories. These have helped staff understand E-Model procedures. Continuing communication remains weaker because regular follow-up information sessions have not been established.

b. Facilities and Infrastructure

Electronic signatures depend on information technology infrastructure, including computers or laptops, internet connectivity, signing applications, servers,

¹⁵ Julfitri and Prakoso, *eJournal Administrasi Publik* 11, no. 3 (2023).

¹⁶ Julfitri and Prakoso, *eJournal Administrasi Publik* 11, no. 3 (2023).

security equipment, and supporting facilities. These resources enable document preparation, submission, signing, and verification.¹⁷

Adequate infrastructure is a prerequisite for consistent implementation at the university. Appropriate equipment enables staff to access the system and process documents electronically. Equipment limitations, network disruption, system problems, and unstable application access may instead obstruct administration.

Effectiveness depends on the quality and reliability of technology. Accessible and stable TNDE or SRIKANDI systems that process documents promptly can support faster services. The research nevertheless identifies shortcomings in TNDE, including letter formats reported as inconsistent with Minister of Religious Affairs Regulation Number 12 of 2026 and inadequate electronic archiving. System development is therefore needed. Informants also described limitations in the document types supported by their use of SRIKANDI, including rector's decisions and certain university regulations, which impeded its application at the university.

Security is another element of system development. Electronically signed official documents require protection against forgery, unauthorized alteration, and unauthorized signature use. Digital security infrastructure is therefore integral to implementation. The E-Model application uses passwords for leaders' accounts and passphrases intended to be known only to the relevant electronic signature holder.

Facilities and infrastructure support implementation, but further development is needed to improve service quality, electronic archiving, and security.

c. Bureaucratic Culture

Implementation is also affected by the university's bureaucratic culture: the values, habits, assumptions, norms, and behavior guiding staff in their work. New technology requires a change from conventional to digital working practices.¹⁸

This transition may face difficulties where established procedures remain familiar and comfortable. Some staff prefer physical documents, handwritten signatures, or administrative processes used for many years. The university's experience indicates that digitalization depends on organizational readiness to accept change as well as technological capability.

The university's bureaucratic culture has also supported innovation by encouraging employees to accept electronic signatures as part of everyday work. Staff openness to change provides a basis for further implementation.

Leadership has a strategic role in providing direction, examples, supervision, and encouragement. Leadership commitment nevertheless needs fuller expression through clear internal policies, information sessions, assistance, evaluation, and support for staff facing difficulties. Establishing electronic signatures as part of official working procedures can help form new organizational habits.

Bureaucratic culture therefore includes the organization as a whole, as well as individual attitudes. An adaptive, service-oriented organization that accepts innovation and is supported by committed leaders is better placed to integrate electronic signatures into everyday work. Technological change can then be accompanied by changes in administrative behavior and practices.

¹⁷ Maharaksa et al., *Implementasi Kebijakan Publik: Pengertian, Model-Model dan Penerapannya dalam Contoh Studi Kasus*.

¹⁸ Maharaksa et al., *Implementasi Kebijakan Publik: Pengertian, Model-Model dan Penerapannya dalam Contoh Studi Kasus*.

d. Human Resources

Personnel directly implement electronic signature procedures and are therefore central to effectiveness. University staff have different levels of technological competence, which may influence the speed and accuracy of system use.¹⁹

Staff familiar with digital applications and services tend to understand electronic signature mechanisms more readily. Those less familiar with digital administration need more time to adapt. Such difficulties can affect newly appointed or transferred staff who lack computer skills or understanding of the administrative workflow.

Relevant competencies include system operation, understanding signing procedures, following document submission workflows, conducting verification, and resolving basic operating problems.

For example, uploading the wrong document, selecting the wrong signatory, using an incorrect format, or failing to follow submission stages may require a document to be returned and processed again. These errors affect administrative completion times.

Competence therefore includes understanding working procedures as well as technical operation. Staff must know which official may sign a document, how to submit it, how to check its status, and how to respond to problems.

Operators and other personnel providing user assistance are also important. Their deeper knowledge of the system helps resolve problems beyond ordinary users' capabilities and prevents technical difficulties from immediately stopping administration.

Training and information sessions should consequently continue after initial implementation, particularly when systems, applications, procedures, or the staff responsible for administration change.

Staff willingness to adapt also matters. Implementation is difficult where users comply only out of obligation without seeking to understand the system. Staff willing to learn are better able to manage change and incorporate electronic signatures into routine work.

Effective implementation therefore requires technical competence together with adaptability, discipline, and responsibility for electronic administration.

4. A Model for Strengthening Legal Certainty in Electronic Signature Use

Electronic signatures are intended to make government administration, particularly document signing, easier and faster. Their use nevertheless requires legal certainty, security, validity, and accountability. Clear internal rules and mechanisms are needed to support orderly and accountable implementation.

A strengthening model should reflect each institution's circumstances. The regulatory basis should support secure signing and a clear allocation of authority. It should also identify documents that still require handwritten signatures, whether because appropriate formats or system support are unavailable or because applicable rules require a particular form.²⁰

¹⁹ Aripkhan and Asufie, "Tinjauan Yuridis Tindak Pidana Pemalsuan Tanda Tangan Elektronik dalam Kerangka Hukum Positif Indonesia."

²⁰ Kendi, *Implementasi Kebijakan Publik*.

Informants reported that electronic signatures are already used in official administration and documentation, but are not supported by comprehensive university rules specifically governing their use. Minister of Religious Affairs Circular Letter Number 39 of 2020 provides technical guidance on electronic signatures, including implementation, reporting, and supervision. The university nevertheless lacks a comprehensive internal standard identifying which documents may use electronic signatures and which require handwritten signatures. According to the interviews, some personnel, agreement, and financial documents continue to use handwritten signatures. The respective scope of the two methods therefore needs clarification.

As a comparison, UIN Maulana Malik Ibrahim Malang issued Rector's Circular Letter Number 1642 of 2024 concerning Electronic Signature Use, providing more detailed internal arrangements. The research materials describe provisions addressing problems in electronic signing, exceptions for confidential or otherwise particular documents, and signatures applied while an official is undertaking official duties or outside working days. Such internal arrangements can clarify authority, conditions, exceptions, and problem resolution.

The findings indicate that each signatory has a personal authentication code intended to be known only to that official. This provides a security mechanism by keeping signing under the authorized official's control. Security nevertheless depends on preserving the confidentiality of those credentials. Internal rules should expressly regulate confidentiality, prohibit credential sharing, and allocate responsibility for misuse. Security would then be supported by enforceable institutional rules as well as individual conduct.

The proposed model combines a leadership decision establishing institutional authority with operational SOPs implementing technical controls. Rector-level policy should identify document scope, authorized officials, certified signature systems, risk owners, and accountability. SOPs should govern certificate issuance and renewal, identity and integrity checks, access controls, retention, backup, audit logs, incident reporting, and alternative procedures during service disruption. Performance can be measured only when auditable administrative data are available.

Table 1. Proposed Evaluation Framework and Required Evidence

Dimension	Audit indicator	Required evidence	Available evidence
Validity	Percentage of valid signatures; active certificates and mandates	Original PDFs, certificate validation, delegation decisions	No testing figures available
Service speed	Median submission-to-approval duration	TNDE logs and document samples	Not available
Availability	Disruption duration and recovery time	Helpdesk incidents and uptime records	Informant accounts only
Personnel	Training coverage and types of errors	Attendance, training materials, correction logs	No consolidated figures

Dimension	Audit indicator	Required evidence	Available evidence
Archives	Retention, backup, audit logs, recovery	Retention schedule, SOPs, backup evidence	Document verification required
Paper use	Proportion of printed routing and disposition records per unit	Document routing registers for a defined period	No proportion data

Table 2. Proposed Internal Policy and Operational Instruments

Subject	Rector-level decision or policy	Technical SOP
Authority	Authorized officials and document classification	Mandate checks by document type
Certified signatures	Certification providers and service requirements	Issuance, renewal, validation, revocation
Access	Credential-sharing prohibition and institutional responsibility	Multi-factor authentication, activity logs, access management
Archives	Retention principles and responsible officials	Backup, recovery, long-term validation
Incidents	Accountability and response to violations	Reporting, isolation, investigation, documentation
Alternative services	Authorization of emergency procedures	Queuing, approval, post-incident reconciliation

CONCLUSION

Electronic signatures in official document management at UIN K.H. Abdurrahman Wahid Pekalongan form part of the development toward electronic institutional administration under Presidential Regulation Number 95 of 2018 concerning SPBE.

From a legal certainty perspective, electronic signatures may meet validity requirements where the signatory's identity, file integrity, consent, and control over signature-creation data can be demonstrated under the Electronic Information and Transactions Law and Government Regulation Number 71 of 2019. A particular platform is not the sole determinant of validity. Interview accounts indicate implementation, but the study lacks quantitative data across units to establish the effectiveness of institutional services as a whole. Its defensible findings concern gaps in SOPs, verification, credential protection, archiving, training, and incident documentation.

Under Edward III's variables of communication, resources, disposition, and bureaucratic structure, the reported obstacles concern continuing information sessions, operator skills, infrastructure disruption, and technical coordination. Causal relationships cannot be established without frequency data, defined periods, and

archive samples. Prescriptively, the rector should establish authority, certificate governance, and accountability. Technical managers should complete SOPs for verification, maintenance, incident response, retention, and backup services. Periodic evaluation should examine document accuracy, successful validation, processing time, user errors, access security, and archival completeness before assigning an overall effectiveness rating.

REFERENCES

- Anam, Saiful (TNDE pioneer), interview by Dyah. UIN K.H. Abdurrahman Wahid Pekalongan, Pekalongan, July 22, 2026.
- Angel Firstia Kresna, *Legalitas Tanda Tangan Elektronik Pejabat Dalam Rangka Mendukung E-Government*, 2019.
- Aripkah, Nur, and Khairunnisa Noor Asufie. Tinjauan Yuridis Tindak Pidana Pemalsuan Tanda Tangan Elektronik dalam Kerangka Hukum Positif Indonesia. 3, no. 1 (2024).
- Julfitri, Rizka Indriani, and Cathas Teguh Prakoso. *eJournal Administrasi Publik* Volume 11, Nomor 3, 2023. 2023.
- Kendi, Ibrahim Kristofol. *Implementasi Kebijakan Publik*. n.d.
- Maharaksa, Muhammad Sinathria, Hary Dermawan Triharjono, Fadla Nur Fadilah, Sadira Az Zahra Kania, Siti Mutia Firda, and Zahra Aulia Hidayat. *Implementasi Kebijakan Publik: Pengertian, Model-model dan Penerapannya Dalam Contoh studi kasus*. n.d.
- Naurah Imtiyazah, et al., Tinjauan Aspek Legalitas Dan Keamanan Penggunaan Tanda Tangan Elektronik Pada Rekam Medis Elektronik Di Rumah Sakit X Kota Cimahi, OJS Vol. 19, No. 3 (2024):4014-4022.
- Nazaruddin Lathif, "Teori Hukum Sebagai Sarana Alat Untuk Memperbaharui atau Merekayasa Masyarakat," *Pilar pakuan law review* 3, no. 1 (2017): 402.
- Purwanto, Tiara Jabbar, and Djumadi Purwoadmojo. "Tinjauan Yuridis Legalitas Penggunaan Tanda Tangan Elektronik Dalam Akta Notaris." *Notarius* 16, no. 2 (2023): 989–97. <https://doi.org/10.14710/nts.v16i2.42261>.
- Republic of Indonesia. Government Regulation Number 71 of 2019 concerning the Operation of Electronic Systems and Transactions, particularly Articles 59–62. https://jdih.komdigi.go.id/produk_hukum/view/id/695/t/common.
- Republic of Indonesia. Law Number 11 of 2008 concerning Electronic Information and Transactions, as last amended by Law Number 1 of 2024, particularly Articles 5 and 11.
- Republic of Indonesia. Law Number 43 of 2009 concerning Archives.
- Siregar, nurfitriyani, "Efektivitas Hukum", *JHI* IV, no. 3 (2020): 75-86.