Intellectual Law Review (ILRE)
Vol. 3, No. 2, October 2025, h. 77-87
ISSN 2987-9116 (Print)
ISSN 2987-6338 (Online)
Available Online at DOI: 10.59108/ilre.v3i2.114

The Role and Responsibility of the Government in Protecting the Rights of Electronic Certificate Holders in Accordance with the Principle of Legal Protection

Meiti Asmorowati
Sekolah Tinggi Hukum Bandung, Jawa Barat
**Email Corresponding: meitiasmorowati@yahoo.com*

Article Info

Article history:
Received 15 October 2025
Received in revised form 27 October 2025
Accepted 31 October 2025

Keywords: Article 28D of the 1945 Constitution; Electronic Certificates; Legal Certainty; Legal Protection; State Responsibility.

Abstract

This study aims to analyse the role and responsibility of the government in providing legal protection for holders of electronic certificates (e-certificates), particularly in ensuring legal certainty and data security in accordance with the mandate of Article 28D of the 1945 Constitution. This study uses a normative juridical method with a statute approach and a conceptual approach. Data analysis was conducted qualitatively and descriptively on secondary data covering primary, secondary, and tertiary legal materials. The results of the study show that although a formal legal basis exists (ITE Law, Government Regulation No. 18/2021, and ATR/BPN Ministerial Regulation No. 3/2023) that provides a framework for preventive and repressive protection, its implementation still faces crucial problems. These problems include: (1) uneven infrastructure and human resource readiness, which risks violating the principles of legal certainty and equal protection; (2) a legal culture gap or public doubt regarding the validity of electronic documents; (3) inconsistency and fragmentation of implementing regulations, giving rise to multiple interpretations; and (4) a lack of clear norms regarding state accountability mechanisms, compensation, and restoration of rights in the event of system failure or data leaks.

INTRODUCTION

In the current era of globalisation, advances in information and communication technology have brought about major changes in various aspects of life, including in the field of land administration (Adiyanti & Pidada, 2024) . The Indonesian government, through the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency (ATR/BPN), is striving to modernise public services by implementing electronic land certificates (e-certificates) (Kartono & Rakhmatullah, 2024) . This system is part of the digital transformation of land administration, which aims to improve efficiency, transparency, and security of land ownership data. Through electronic certificates, the public can print certificates independently, access land data through applications, and minimise the risk of loss or damage to physical documents. This step also supports the concept of *a paperless office* in line with global digital technology developments (Hidayah et al., 2024; Muri et al., 2025) .

However, the implementation of electronic certificates is not without legal issues. There are still doubts among the public regarding the validity of electronic certificates as evidence of land ownership (Priscilla et al., 2024) , the potential for data misuse due to weak digital security systems, and the unclear mechanism for resolving disputes in the event of

errors or data leaks in electronic systems (Jamil, 2025) . The lack of digital infrastructure in several regions is also an obstacle to the equitable implementation of this programme (Insany Rachman & Hastri, 2021) . In addition, the lack of synchronisation between implementing regulations has created legal uncertainty regarding the protection of the rights of electronic certificate holders (Ramasari & Aniscasary, 2022) .

The legal basis for electronic certificates in Indonesia can be traced back to several regulations, including Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) as last amended by Law No. 1 of 2024, as well as Government Regulation No. 18 of 2021 concerning Management Rights, Land Rights, Apartment Units, and Land Registration. Specifically, regulations concerning electronic certificates are stipulated in Minister of Agrarian Affairs and Spatial Planning/National Land Agency Regulation No. 1 of 2021 concerning Electronic Certificates, which was later updated with Minister of Agrarian Affairs and Spatial Planning/National Land Agency Regulation No. 3 of 2023 concerning the Issuance of Electronic Documents in Land Registration Activities, and clarified with Technical Guidelines No. 3 of 2024. These regulations are intended to promote efficiency and transparency in land administration. However, to date, there has been no harmonisation and integration between the main regulations and their implementing regulations, particularly in terms of data security guarantees, the legal validity of electronic documents, and the protection of certificate holders' rights.

The urgency of this research lies in the need for a legal-normative analysis of the protection mechanism for electronic certificate holders in the national land system. Digital transformation in the land sector still faces various obstacles, ranging from infrastructure readiness, bureaucratic competence, to the adequacy of regulations governing procedures and data management security. On the other hand, comprehensive studies discussing the state's responsibility in guaranteeing the rights of electronic certificate holders are still very limited. This is important considering that Article 28D paragraph (1) of the 1945 Constitution emphasises the state's obligation to provide recognition, guarantees, and adequate protection of citizens' rights in every public administration process.

Based on this description, the main issue of this study is the form of the government's role and responsibility in providing protection to electronic certificate holders amid the land digitalisation process. The focus of the study is on the effectiveness of government measures, particularly those of the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency, in ensuring system reliability and protecting people's land rights in the event of digital administration disruptions or failures. The objective of this study is to analyse the implementation of these responsibilities based on applicable legal provisions and to formulate policy recommendations that can strengthen the quality of land services in the digital era.

METHODOLOGY

The research method used is a normative legal research method (juridical normative) with *a statute* approach and a conceptual approach. The normative legal research method is used because the focus of the research is on analysing the laws and regulations governing

electronic certificates and the role and responsibilities of the government in providing legal protection to the holders of these certificates. This study does not examine the behaviour of society empirically, but examines the applicable legal norms, legal principles, and legal doctrines to find out what the ideal form of legal protection is and to what extent its implementation is in accordance with the principle of legal protection in Article 28D paragraph (1) of the 1945 Constitution. The legislative approach was carried out by reviewing various relevant regulations, such as Law No. 11 of 2008 concerning Electronic Information and Transactions and its amendments, Government Regulation No. 18 of 2021, and Minister of Agrarian Affairs and Spatial Planning/National Land Agency Regulations No. 1 of 2021 and No. 3 of 2023. Meanwhile, a conceptual approach was used to understand the concepts of legal protection, government responsibility, and legal certainty in the context of land administration digitalisation. The types and sources of data used are secondary data, which include primary legal materials (laws and regulations), secondary legal materials (books, journals, research results, and legal expert opinions), and tertiary legal materials (legal dictionaries and legal encyclopaedias). Data collection techniques were carried out through literature studies, while data analysis was conducted using qualitative-descriptive methods to describe, interpret, and assess the extent to which government regulations and policies have provided adequate legal protection for electronic certificate holders in Indonesia.

RESULTS AND DISCUSSION

A. Legal Protection for Electronic Certificate Holders Based on Applicable Regulations

From a formal legal perspective, legal protection for e-certificate holders has obtained a clear and hierarchical normative basis: starting from the provisions in the law (the scope of the ITE Law and the provisions on creative work that provide space for electronic documents), followed by Government Regulation No. 18/2021 which regulates the implementation of electronic land registration (Articles 84, 85, 96) (Aji Permana et al., 2024) and then Minister of Agrarian Affairs and Spatial Planning/National Land Agency Regulation No. 3/2023 along with Technical Guidelines No. 3/2024 which detail the procedures for issuing electronic documents (Putra & Winanti, 2024) . This foundation provides the basis that e-certificates have legal form as electronic documents stored in the Electronic Land Registry (BT-el) (Sinaga, 2025) and are authenticated with electronic signatures so that, normatively, they have the same evidentiary power as physical certificates. This normative position places e-certificates not merely as a technical innovation, but as a legal product recognised and protected by the regulatory framework (Priscilla et al., 2024) .

From the perspective of document security and validity, implementing regulations require the application of technical and procedural standards: storage systems are regulated as integrated databases (BT-el) (Puspita & Supriyo, 2025) , the use of certified electronic signatures, and the implementation of information security management (e.g. reference to ISO27001 standards and encryption and *backup/data centres)* as part of efforts to mitigate

the risk of data loss, falsification or leakage (Kamali Martin & Adiva Prita Ramadania, 2025) . Although these provisions set certain technical standards, the effectiveness of the guarantees provided still depends on operational implementation, including the quality of infrastructure, certification procedures, and the role of cybersecurity agencies such as BSSN. Thus, the level of protection provided needs to be proven through evaluation at the practical level, including through security audits, independent certification, and the implementation of measurable incident response mechanisms.

Critical analysis reveals real regulatory gaps and implementation risks. Research documents identify problems with harmonisation between implementing regulations, the incomplete national land map database, digital infrastructure disparities between regions, and public concerns about potential data misuse, all of which have the potential to undermine the legal certainty expected from digitalisation. The implication is that, although e-certificates are recognised normatively, in practice there are still loopholes that could cause legal losses for holders (e.g. failed access, data errors, or identity leaks). The transition period (e.g. the treatment of old evidence until 2026 for some customary rights) also creates a period of uncertainty that must be managed carefully.

Regarding state responsibility and recovery mechanisms, the regulatory framework thus far places the primary obligation on the state (through the Ministry of Agrarian Affairs and Spatial Planning/National Land Agency) to provide a reliable, secure system and fair administrative procedures. However, the regulations are not yet sufficiently explicit in regulating the form of state accountability (e.g. compensation, administrative sanctions for failures by administrators, special civil/administrative litigation channels) in the event of system damage or data breaches that harm rights holders. From the perspective of substantive legal protection (Article 28D of the 1945 Constitution as the basis for the right to legal certainty), more explicit norms are needed regarding corrective rights and compensation as well as electronic dispute resolution procedures so that e-certificate holders have effective access to legal remedies.

In the context of Indonesian administrative law, the issue of *state liability* is an important theoretical basis for assessing the government's obligations when failures in the electronic administration system cause losses to citizens. This concept is known through the doctrine of government liability, namely the principle that the state is not immune from legal claims if its actions or negligence cause losses, as practised through the State Administrative Court (PTUN) mechanism. Such liability may arise from unlawful acts by government agencies or officials (PMH Pemerintah), procedural errors, negligence in the provision of public services, or failures in information technology systems under state supervision. In the development of modern administrative law, state liability also includes the state's obligation to guarantee the quality of infrastructure, system reliability, and information security standards, so that in the event of system damage or data leaks in electronic services, this responsibility is not only moral or administrative in nature, but can also be juridical in the form of compensation and recovery. This theoretical affirmation strengthens the argument that protection for e-certificate holders is not merely a technical issue of digitalisation but is part of the state's constitutional obligation in the provision of public services.

Based on Philipus M. Hadjon's legal protection theory, legal protection of e-certificates can be understood in two forms:

Table 1. Legal Protection of E-Certificates

Type of Protection	Implementation in Electronic Certificates
Preventive	The existence of an identity verification system, BSSN-certified electronic signatures, data encryption, server backups, and controlled access through the Sentuh Tanahku application.
Repressive	Dispute resolution mechanisms and data correction through administrative objections, civil lawsuits, and legal actions in court.

Source: (Juliyanti et al., 2023)

Thus, normatively, the state has provided a legal protection framework to ensure *legal* certainty, data security, and the validity of electronic certificates as evidence of land rights. However, this legal certainty is conditional, depending on: a) the integration of land databases, b) the readiness of digital infrastructure, c) the capacity of implementing agencies, and d) public acceptance. In other words, legal protection has been regulated, but it is not yet fully operational throughout Indonesia.

The following are sharp recommendations based on normative findings (in accordance with the legislative and conceptual approach you use): (1) comprehensive harmonisation and technical revision of implementing regulations to ensure consistency; (2) strengthening of information security governance through independent audit mandates, BSSN involvement, and mandatory implementation of ISO27001 plus third-party certification; (3) establishment of a clear state accountability mechanism (compensation procedures, claim procedures, and sanctions for negligence on the part of the organiser); (4) transition guarantees that protect physical certificate holders (no coercion, rights remain intact) accompanied by a clear legal window for old rights; and (5) infrastructure equalisation and public education programmes to ensure inclusive access to and understanding of e-certificates. All of these solutions are also reflected in the solutions proposed in the research document.

The above analysis assesses that legal protection for electronic certificate holders formally exists and is multi-layered; however, the certainty and effectiveness of this protection are highly dependent on administrative-technical actions and regulatory harmonisation. Therefore, the policy recommendations that emerge are normative-practical in nature: strengthening implementing regulations, clarifying the state's responsibilities and compensation, and ensuring technical readiness and a balanced transition to maintain legal certainty of land rights in the digital era.

B. Problems in the Implementation of Electronic Certificates and Their Legal Analysis

1. Availability of infrastructure and readiness of human resources

The effective implementation of electronic certificates depends on two main components, namely adequate network and data infrastructure and the competence of human resources (HR) at the Land Office (Maulana et al., 2024; Syamsur et al., 2023) . Digital

access inequality between regions necessitates phased implementation in accordance with Article 84 paragraph (5) of Government Regulation No. 18/2021. Digital access inequality between regions makes gradual implementation—as stipulated in Article 84 paragraph (5) of Government Regulation No. 18/2021—a necessary adjustment mechanism, but differences in readiness levels have the potential to cause variations in the quality of services between regions. Juridically, this condition may affect the fulfilment of the principles of legal certainty and non-discrimination in public services, as access to land services and proof of rights is not always equal across all regions. Within the framework of fulfilling constitutional obligations as stipulated in Article 28D of the 1945 Constitution, more structured regulations are needed regarding technical readiness standards, including the establishment of minimum service levels, certification of human resource competencies, and implementation stages based on readiness audit results. These regulations are still scattered across various implementing regulations, so consistency in their application requires reinforcement through more comprehensive regulations.

2. Public doubts about the validity of electronic certificates (legal culture gap)

Public doubts that evidence must be physical reflect the gap between normative change (legislation that recognises electronic documents) and legal culture change (*legal consciousness*) (Masri & Hirwansyah, 2023) . Legally, although the Law and Ministerial Regulation recognise electronic documents and electronic signatures (and give formal legitimacy to e-certificates), gaps in socialisation, education, and procedural guarantees (e.g. verification mechanisms that are easily accessible to the public) mean that factual legitimacy is not yet strong: electronic evidence may be accepted in court in theory, but in practice, judges and parties in land cases still rely on physical evidence due to customary practices of evidence and public distrust. This raises the issue of functional legitimacy — positive law does not achieve its objectives without public acceptance — so policymakers must accompany the new norms with legal literacy programmes, practical guidelines for PPATs and the judiciary, and clear transitional rules so as not to create uncertainty for parties who already hold physical certificates. If left unaddressed, this gap will give rise to administrative disputes and litigation based on alternative evidence, which will burden the judiciary.

3. Vulnerability to data leakage or manipulation risks (security & state responsibility)

Although the Ministry claims to implement standards such as ISO 27001, encryption, electronic signatures, and 2-factor *authentication* mechanisms, from a legal perspective there are two issues: (1) technical standards do not automatically imply legal certainty regarding compensation and remedial mechanisms in the event of a breach; and (2) the existence of cyber threats actualises the state's constitutional obligation to protect individual rights (Article 28D) and the obligations of data processors under the Personal Data Protection Law. In the event of a leak/manipulation, a series of legal issues arise: proving the negligence of state operators, determining the form of liability (administrative, civil, or even criminal if the elements are met), and the procedure for restoring the rights of certificate holders.

Normatively, Ministerial Regulations/Government Regulations must be more explicit: they must outline the obligation to notify leaks, independent audit standards, administrative and civil compensation provisions, and rapid resolution mechanisms (e.g. temporary access blocking, issuance of secure copies) — not just claim technical compliance with " ". Without such certainty, victims of breaches face difficulties in claiming compensation, and the state/system operators risk avoiding responsibility by citing force majeure/cyber attacks.

4. Lack of synchronisation in implementing regulations (inconsistent norms and multiple interpretations)

Regulatory fragmentation (the ITE Law / Job Creation Law / Government Regulation No. 18/2021 / revoked and replaced ATR/BPN Ministerial Regulation / 2024 technical guidelines, and data protection regulations) has led to implementation gaps and multiple interpretations of crucial matters: who is responsible when data changes occur; how to transfer media from physical to electronic form; standards of evidence in court; and administrative mechanisms for certificate replacement. Legally, this inconsistency creates *legal uncertainty* that is counterproductive to the objectives of land registration — certainty and protection. In practical terms, Land Office officials may act differently between regions, advocates and PPATs are confused about procedures, and judges face defence arguments that depend on which norms are chosen. Therefore, harmonisation measures are needed: (1) the drafting *of lex specialis* that unifies important principles (validity, media transfer mechanisms, responsibility), (2) the issuance of binding technical implementing regulations (not merely interpretative guidelines), and (3) a mechanism for periodic regulatory review to close the harmonisation gap between the main and implementing regulations. Without synchronisation, the digitisation of certificates will only increase the number of legal conflicts that must be resolved.

To ensure that legal protection for e-certificate holders is not merely declarative, legislators and policymakers must (1) synchronise norms (lex specialis + operational implementing regulations), (2) mandate auditable technical readiness standards and human resource competencies, (3) establish rules on liability and remedies (notification of breaches, compensation, rapid recovery mechanisms), and (4) implement public literacy programmes and evidence guidelines for courts. These efforts are not merely IT technicalities but substantive legal requirements to bridge the gap between normative legitimacy and social legitimacy.

C. Solutions and Recommendations for Strengthening Legal Protection

From a regulatory perspective, strengthening legal protection for electronic certificate holders requires the establishment of special norms (*lex specialis*) that fill the regulatory void regarding technical aspects and the form of state responsibility. Normatively, the principle of legal certainty in agrarian law and land registration requires a change in the form of evidence from physical to electronic, accompanied by clarity regarding the status of evidence, data correction mechanisms, and provisions for administrative sanctions and compensation in the event of losses due to service failures. To that end, it is necessary to

issue a Ministerial Regulation or Head of BPN Regulation that explicitly regulates: 1) the order of priority of binding data sources (e.g., comparison between land registry data and electronic data); 2) procedures for data correction through administrative adjudication; 3) standards of state responsibility and compensation or recovery mechanisms; and 4) the obligation to record an unalterable audit trail.

The need to strengthen these derivative regulations is a direct implication of the requirement for harmonisation between the ITE Law, land registration regulations, and implementing regulations at the ministerial level. Theoretically, the proposed norms are based on two legal frameworks: (a) land registration theory, which emphasises the certainty and publicity of land data; and (b) *state liability* theory in administrative law, which requires the availability of prevention and recovery mechanisms for potential losses resulting from administrative actions or negligence by the state. From an agrarian perspective, electronic certificates must continue to fulfil their function as a strong means of proof, so that the conformity of physical-legal data with electronic data is an absolute requirement. From the perspective of state liability, if a system error results in losses, the elements of negligence, causal relationship, and loss must be proven; in addition, an administrative mechanism is needed to enable temporary recovery before civil proceedings take place. The framework of preventive and repressive protection (Hadjon; Heymen) remains relevant to balance the obligation of prevention through regulation and recovery measures when prevention fails.

At the institutional and governance levels, the recommended technical-administrative measures are implications of the state's legal obligations in the provision of public services. In the field of infrastructure, minimum security requirements must be established, such as the use of certified *public key infrastructure* (PKI), encryption for stored and transmitted data, multi-layered authentication for owners, non-modifiable logging, and the existence of a tested *disaster* recovery *centre*. The implementation of these standards should ideally involve the National Cyber and Crypto Agency (BSSN) for security certification and periodic audits, as well as independent institutions to ensure compliance with information security standards.

In terms of human resources, the legal implications are the need to increase capacity through national training on digital procedures, incident management, and data verification, including the creation of new functional positions relevant to electronic land data management.

The legal socialisation strategy must be designed as part of fulfilling the principles of transparency and accessibility of public services. This includes continuous education on the function of electronic certificates, guidelines for using verification applications, options for obtaining secure physical copies, and the provision of assistance services for vulnerable groups. In addition, training for PPATs, notaries, advocates, and judges is important to ensure that all judicial actors understand the implications of electronic evidence in land disputes. A public portal containing registration status (without displaying sensitive personal data) can strengthen the principle of publicity of land data.

Oversight and accountability require a layered design, including: (1) internal oversight by the National Land Agency (BPN) through routine digital audits and minimum

service standards; (2) external oversight by the Ombudsman for aspects of maladministration and by the National Cyber and Crypto Agency (BSSN) for security aspects; (3) a rapid administrative appeal mechanism to prevent further losses; and (4) detailed compensation provisions, including the possibility of a state- t insurance scheme for systemic risks. Verifiable audit trails and mandatory publication of incident reports are essential for administrative or civil liability.

The implementation stages can be outlined in a roadmap: short term (0–12 months) in the form of dispute and accountability mechanisms, standardised pilot projects, and initial security audits; medium term (12–36 months) in the form of cadastral database integration, human resource capacity building, and the establishment of an administrative compensation unit; and long term (>36 months) in the form of national regulatory harmonisation and periodic evaluations based on legal performance indicators such as the frequency of disputes and security incidents.

Overall, strengthening legal protection for electronic certificate holders requires an approach that combines clear norms, measurable state responsibility designs, and testable technical-operational mechanisms. The integration of legal norms, technical governance, public education, and oversight mechanisms will form a system capable of providing legal certainty, security, and proportional protection of rights for the community.

CONCLUSION AND SUGGESTION

The analysis shows that protection for electronic certificate holders has been regulated through the ITE Law, PP No. 18/2021, and Permen ATR/BPN No. 3/2023, which provide preventive and repressive mechanisms in accordance with the legal protection framework according to Philipus M. Hadjon. However, its effectiveness is not yet optimal because there is still a gap between normative legitimacy and actual implementation. Four main issues that hinder this effectiveness include disparities in digital infrastructure and human resource capacity between regions, fragmentation of norms in implementing regulations, public uncertainty regarding the use of digital evidence, and the absence of clear regulations regarding state accountability, including procedures for rights restoration and compensation schemes in the event of system disruptions or incidents that harm rights holders. This situation indicates that the protection of electronic certificate holders does not yet fully meet the constitutional standards as mandated by Article 28D paragraph (1) of the 1945 Constitution.

Efforts to strengthen protection for electronic certificate holders can be made through the harmonisation of implementing regulations so as not to give rise to multiple interpretations, ideally through the establishment of a comprehensive lex specialis; formulating explicit state accountability norms regarding incident notification obligations, compensation mechanisms, and rapid rights restoration procedures; implementing minimum technical readiness standards and independent security audits involving the National Cyber and Crypto Agency (BSSN) and certified auditors; increasing the capacity of human resources at the Land Office, accompanied by a digital law literacy programme for the community, PPAT, notaries, and law enforcement officials; and the application of regulatory

engineering, namely a risk-based regulatory design process and institutional design to ensure harmony between technological, legal, and governance aspects so that the implementation of electronic certificates can be carried out in a more measurable, consistent, and accountable manner.

ACKNOWLEDGEMENTS

The author would like to express his sincere gratitude to the entire leadership of the Bandung School of Law (STHB) for all the support, guidance, and institutional facilities that have been provided. The assistance and motivation provided contributed greatly to the author's ability to successfully complete this research entitled "The Role and Responsibility of the Government in Protecting the Rights of Electronic Certificate Holders in Accordance with the Principles of Legal Protection".

REFERENCES

Adiyanti, N. K. W. S., & Pidada, I. B. A. (2024). Peran Pejabat Pembuat Akta Tanah dalam Penerbitan Sertifikat Tanah Elektronik. *Student Research Journal*, *2*(4), 382–396. https://doi.org/https://doi.org/10.55606/srjyappi.v2i4.1421

Aji Permana, B., Halim, A., & Uraidi, A. (2024). Kekuatan Hukum Pembuktian Sertifikat Elektronik Dalam Perkara Perdata Menurut Peraturan Mentri ATR/Kepala BPN No 3 Tahun 2023 Tentang Penerbitan Sertifikat Elektronik Dalam Kegiatan Pendaftaran Tanah. *Jurnal Ilmiah AKSES*, *2*(1), 61–75. https://unars.ac.id/ojs/index.php/akses/article/view/4453

Hidayah, S., Semarang, U. N., Hariyani, E., Negeri, U., Adymas, S. M., & Fikri, H. (2024). Tantangan dan Peluang Sertifikat Elektronik dalam Reformasi Pendaftaran Tanah di Era Digital. *Jurnal Ilmiah Nusantara (JINU)*, *1*(6), 186–199. https://ejurnal.kampusakademik.co.id/index.php/jinu/article/view/2793

Insany Rachman, A. M., & Hastri, E. D. (2021). Analisis Kendala Implementasi Peraturan Menteri ATR / Kepala BPN Nomor 1 Tahun 2021 Tentang Sertipikat Elektronik. *Mulawarman Law Review*, *6*(2), 91–104. https://doi.org/10.30872/mulrev.v6i2.646

Jamil. (2025). Perlindungan Hukum Terhadap Pemegang Sertipikat Elektronik dalam Sistem Pertanahan Di Indonesia. *BHARASUMBA: Jurnal Multidisipliner*, *4*(03), 429–437. https://azramedia-indonesia.azramediaindonesia.com/index.php/bharasumba/article/view/1690

Juliyanti, N. K. E. D., Dharsana, I. M. P., & Ujianti, N. M. P. (2023). Perlindungan Hukum Terhadap Pemegang Sertifikat Tanah Digital Dikaitkan Dengan Keamanan Data Pribadi. *Jurnal Preferensi Hukum* |, *4*(1), 91–97. https://ejournal.warmadewa.ac.id/index.php/juprehum/article/view/6590

Kamali Martin, E., & Adiva Prita Ramadania, I. (2025). Tinjauan Etika Dalam Penerapan Sertifikat Tanah Elektronik: Mencegah Pemalsuan Dan Kekacauan Administrasi. *Jurnal Administrasi Publik Dan Pemerintahan STISIP Imam Bonjol (SIMBOL)*, *4*(1), 2025. https://doi.org/10.55850/simbol.v2i1

Kartono, S. A., & Rakhmatullah, B. R. (2024). Efektivitas Pendaftaran Tanah Sertipikat Elektronik Aset Pemerintah. *UMPurwokerto Law Review*, *4*(2), 309–320. https://jurnalnasional.ump.ac.id/index.php/umplr/article/view/19569

Masri, E., & Hirwansyah. (2023). Kebijakan Penerbitan Sertipikat Elektronik Pada Sistem Pendaftaran Tanah di Indonesia Untuk Mewujudkan Kepastian Hukum. *Krtha*

Bhayangkara, *17*(1), 157–174. https://doi.org/10.31599/krtha.v17i1.2109

Maulana, H., Nugraha, N., Arinda, R., Fikri, M., & Wahanisa, R. (2024). Urgensi Sertifikat Elektronik dengan Pemantauan Berbasis AI untuk Efisiensi Pendaftaran Tanah dan Mitigasi Mafia Tanah di Indonesia. *Journal Customary Law*, *2*(1), 1–9. https://doi.org/10.47134/jcl.v2i1.3304

Muri, D. P. D., Wibawanti, E. S., & Safitri, M. I. (2025). Sertipikat Elektronik Sebagai Jaminan Perlindungan Hak Atas Tanah Dalam Pelaksanaan Pendaftaran Tanah. *Jurnal USM Law Review*, *8*(2), 1126–1147. https://doi.org/https://doi.org/10.26623/julr.v8i2.12136

Priscilla, M., Nova, D. L., & Fajriah, S. N. (2024). Keabsahan Hukum Penerbitan Sertipikat Tanah Elektronik Sebagai Alat Bukti Kepemilikan Hak Atas Tanah Di Persidangan. *UIR Law Review*, *8*(2), 68–84. https://journal.uir.ac.id/index.php/uirlawreview/article/view/17888%0Ahttps://journal.uir.ac.id/index.php/uirlawreview/article/download/17888/7401

Puspita, E. F. D. P., & Supriyo, A. (2025). Perlindungan Hukum Terhadap Kepemilikan Sertipikat Tanah Elektronik. *PAGARUYUANG Law Journal*, *8*(2), 182–207. https://www.jurnal.umsb.ac.id/index.php/pagaruyuang/article/viewFile/6219/4135

Putra, R. A., & Winanti, A. (2024). Urgensi Dan Kendala Dalam Penerbitan Dokumen Sertifikat Tanah Elektronik Pasca Peraturan Menteri ATR/BPN Nomor 3 Tahun 2023. *Jurnal Usm Law Review*, *7*(2), 835–852. https://doi.org/10.26623/julr.v7i2.9178

Ramasari, R. D., & Aniscasary, S. (2022). Tinjauan Yuridis Kekuatan Hukum Sertifikat Tanah Elektronik Berdasarkan Peraturan Menteri Agraria dan Tata Ruang Nomor 1 Tahun 2021. *Jurnal Hukum Dan Etika Kesehatan*, *2*(1), 1–14. https://doi.org/https://doi.org/10.30649/jhek.v2i1.38

Sinaga, S. H. M. T. (2025). Kehadiran Sertipikat Tanah Elektronik dalam Perkembangan Hukum Pemnbuktian Sebagai Dampak Kemajuan Teknologi Informasi dan Komunikasi. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *11*(2), 478–497. https://doi.org/https://doi.org/10.55809/tora.v11i2.581

Syamsur, S., Madiong, B., & Tira, A. (2023). Analisis Hambatan Pemberlakuan Sertifikat Elektronik Serta Upaya Penyelesaiannya Di Kota Makassar. *Indonesian Journal of Legality of Law*, *6*(1), 97–105. https://doi.org/10.35965/ijlf.v6i1.3817

Conflict of Interers Statement: The author(s) declares that the research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest.

Intellectual Law Review (ILRE): Is an open-access and peer-reviewed journal published by Yayasan Studi Cendekia Indonesia (YSCI).