Advances in Social Science, Education and Humanities Research, volume 558

Proceedings of the Asia-Pacific Research in Social Sciences and Humanities Universitas Indonesia Conference (APRISH 2019)

Electronic Information Security System for Notarial Deeds as National Archives

Chris Rivaldo Maengkom[1*]

[1]*Faculty of Law, Universitas Indonesia, Depok, Jawa Barat, Indonesia*
**Corresponding author. Email: valdomaengkom88@gmail.com*

ABSTRACT
Notaries are public officials authorized to make authentic deeds and other authorities, one if which is the authority to certify transactions carried out electronically, known as cyber notaries as stated in explanation of article 15, Law No. 2/2014 concerning Notary Officials (Revised Law No. 30/2004). The authority is followed by the notary's obligation to store, maintain and maintain the protocol because it is a state archive. At present, the notary has used information and communication technology both for jobs, office systems, and those related to state administration (for example Legal Entity Administration Systems “SABH”). While, there is an Archive Law that provides space for the existence of electronic records where the archive must have the function of authenticity and trustworthiness. With a normative juridical research method, using reference to the rules and principles that apply in the community, there is a need for research on information security systems for state archives managed by Notaries.

Keywords*: notary, electronic information system, security, national archives*

1. INTRODUCTION

It cannot be denied that nowadays, information technology is the basis of all lines of life, from economics, socio-culture, education, to law, especially since the issuance of the Electronic Information and Transaction Law No. 11 of 2008 (“UU ITE”). In the economic field, digitalization of trade transactions shifts direction, from the conventional one to electronic or e-Commerce. Meanwhile, in the line of government administration, especially public services are also promoting electronic-based services, so the e-Governance system emerges.

In terms of public services, there is one type of non-government service but is very closely related to the implementation of public services and thick with regulations because their duties and functions are regulated by law, namely Notary services. Notary services, such as the deed issued by a notary as a legal product that also a part of public service that go to the public, are still conventional, but along with the development of information technology, inevitably, this condition forces every line of life to migrate from conventional systems to electronic systems.

In carrying out his position, in addition to carrying out the deed and other supporting documents in the conventional notary protocol, the notary also keeps a copy of the document in an electronic system. So that, not only the physical form of the deed (in the notary office or warehouse) but also stored in the network. With the possibility of storing archives in electronic form that is accommodated in the Archive Law, the storage of electronic records must be in accordance with the rules in the Archive Law.

With these advancements in information, communication and computer technology, new problems arise, namely security and data and information problems. This might be an opportunity for people who are not responsible for using it as a crime, and certainly will harm certain parties. on Jalan Salemba Raya, Central Jakarta, there is a group of individuals who commit fraud, namely falsifying data and valuable documents. Mostly, the forged documents such as National ID card, family card, marriage certificate, birth certificate, school diploma and other authentic documents, especially notarial deeds.

2. NOTARY AND THE CONCEPT OF AUTHENTICITY AND TRUSTWORTHINESS OF ELECTRONIC FILLING SYSTEM IN INDONESIA

2.1. Notary and its Protocol as a National Achieves

Notary has a function to serve the interests of the community in making authentic deeds and he has an obligation to keep the deeds he made as part of the protocol that must be properly maintained and guarded. This is not only because the protocol is the first or original copy of everything in the deeds and may be admitted as evidence of its contents but also because it is a state document as stated in Notary Official Law Article 1 number 13.

According to Law No. 43 of 2009 concerning Archives, Notary protocol categorized as dynamic records, means an archive that can be used directly in the activities of the creator of the archive and stored for a certain period of time. In Indonesia, the period of retention of the notary protocol is 25 years and thereafter will be submitted to the regional supervisory board. However, due to the limitations of the supervisory board, it is not uncommon for a notary to save the protocol for the rest of his life and if he dies, the protocol will be kept by another designated notary. Storing and maintaining protocols that constitute the state archives are not easy so special guidelines are needed in accordance with those regulated not only by Notary Official Law but also by the Archives Law.

In practice, the notary does not have sufficient knowledge about how the notary protocol should be stored, maintained and safeguarded based on the rules of the archival law. In personal interview, Tjong Sendrawan, Notary in North Jakarta, explain that protocol safekeeping is carried out only based on the habits of the Notary which generally comes from previous Notary experiences. Notary Official Law does not regulate how to store the protocol. This is because there is no synchronization between the Notary Position Law and the Archive Law and also there is no standard arrangement on how the protocol should be stored as stipulated by the Indonesian Notary Association and the Ministry of Law and Human Rights. So that it becomes mandatory for the notary to study archival storage rules in accordance with applicable laws. (Adjie 2008, 33) This arrangement regarding filing can also be supported by coaching from the State Archives of the Republic of Indonesia ("ANRI") as the organizer of the national archives.

Some of the non-aligned arrangements contained in the Archive Law with other related laws effect the implementation of the National Archives have not yet been implemented maximally. National implementation should guarantee the establishment of reliable records management in the use of archives in accordance with the provisions of laws and regulations, guarantee the protection of state interests and people's civil rights through the management and utilization of authentic and reliable archives, and dynamize the implementation of national archives comprehensive and integrated.

2.2. Authenticity and Trustworthiness in the Electronic Filing System

According to Archive Law article 41, archives are records of activities or events carried out by the creators of the Archives. Then to produce an authentic, intact, and trusted archive, it must fulfill the structural components (physical format) and arrangement (intellectual format) of the archive created in the media so that the contents of the archive are communicated, content (data, facts or information recorded the implementation of activities of organizations or individuals), and the context (the administrative environment and the system used in the creation of the archive) from the archive.

Authentic archive is an archive on which there is an original signature with ink (not a photocopy or film) as a sign of validity of the contents of the relevant file. Authentic archives can be used as legal evidence. While the file is not authentic it is an archive on which there is no original signature in ink. (Meljono, 2001) While authentic understanding according to Article 1868 of the Civil Code concerning an authentic deed is a deed made in the form of a law by or in front of general employees in power for it, in the place where the deed was made. So that authenticity is proven if it meets these elements.

While in the perspective of technology and law regarding authenticity, authentic documents or data should be trusted because it has gone through a process of checking the integrity of data compared to the original copy of where the document or data came from. In this case the compiler of the archive law seeks to distinguish between formal integrity seen from the composition of letters and numbers that must be exactly the same as the original archive with material integrity that ensures that the information contained in the archive cannot be denied by the author. Based on this, an archive that is included in the authentic understanding according to the Civil Code and Notary Official Law is not necessarily authentic according to the archival perspective. The provisions of an authentic deed should include trustworthiness in the data, so that if the authentic provisions have been fulfilled, then it can be valid evidence.

3. CONCEPT OF ELECTRONIC INFORMATION SECURITY SYSTEM FOR NOTARIAL DEEDS

Recently, the notary not only keeps the archive in its original form, but also stores it in electronic form which of course has gone through a media transfer process. Copies of the deeds as electronic documents and its storage in an electronic system owned by a Notary, not only regulated in the Archive Law also stipulated in the ITE Law. It's just that electronic storage is collided with the problem of proof when legal issues occur, where often the panel of judges request physical evidence from these documents. For this reason, ANRI is currently limited to backing up these documents in digital form, and stored in cyberspace.

The storage of notary protocols in physical form with conventional methods has risks that can result in damage or destruction of the deeds and documents in the Notary protocol. The risk of damage to deed paper Notaries and documents due to termite or rat pests, fire, floods and theft. If the damage occurred is a matter beyond the will and not negligence of a notary so that it can be categorized as force majeure/overmacht. Sanctions against the notary concerned may not be imposed on him. However, the loss of this matter is undeniable, and the most disadvantaged are those who have an interest in the deed/document.

This model is also called modern archiving. Modern archive management or automatic filing is an archival system that uses electronic data processing facilities by utilizing computer facilities and other information technology. From the above understanding can be concluded that electronic archives are archives that are created, communicated, and managed electronically using computer technology or wireless internet networks such as cloud systems data or data stored in the internet database so that it can be used and accessed anywhere by whom just as long as they have internet access.

3.1. Security Classification Analysis and Archive Access

The Security Classification and Archive Access System are the rules for limiting the right of access to the physical archive and its information as a basis for determining the openness and confidentiality of archives in order to protect the rights and obligations of archival creators and users in archiving services. Security classification and access to archives are determined based on the nature of the archive that can be accessed consisting of open archives and closed archives. This is in accordance with the Regulation of The Head of The National Archives of the Republic of Indonesia Number 17 of 2011 about Guidelines for Classification Security Systems and Access to Dynamic Archives.

Based on this, the Notary in storing the Protocol electronically can use closed access to protect the contents of the deed made. Access to the protocol can still be opened in accordance with the provisions in the Notary Official Law as access to the Notary protocol physically, namely by the Notary Supervisory Board and the Notary Honorary Assembly in matters of supervision and interest in the judicial process.

3.2. Authentication System for Electronic Archives

In electronic archives, this type of archive requires a system of verification or authentication. Archival authenticity is threatened when files are sent across space (i.e. when sent to recipients or between systems or applications) or across time (i.e. when the archive is in storage or when hardware and software used to store, process, communicate, update or replace it)) Therefore, to ensure that electronic records remain an authentic archive, verification of the authenticity of electronic records is needed or the role of verification methods, namely systems of verification or authentication.

The verification method includes, but is not limited to: (1) comparison of the archives with copies of archives in other places or with back-up; (2) comparison of the archive with data in the registration of incoming and outgoing archives; (3) textual analysis of archive content; (4) forensic analysis of media, writing and so on; (5) review of audit trails as well; and (6) Testimony of trusted third parties.

Good management of electronic records will ensure the availability of evidence of government decisions and activities, show the fulfillment of the accountability of archival creators, support functions and tasks through the creation of reliable records that can be used, contribute to the efficiency and effectiveness of activities, and reduce risk by ensuring the right records are maintaining the performance and continuity of activities, related to this, guidelines for the preparation of general management of electronic records are needed as stated in Appendix of the Regulation of the Head of the National Archives of the Republic of Indonesia Number 14 of 2012 concerning Guidelines for Preparing General Policies for the Management of Electronic Archives.

3.3. Securing Electronic Information/Documents and its Physical Form

In carrying out their duties and positions, the Notary is obliged to maintain the security of information in the Notary deed because if the Notary is negligent in safeguarding the security of the opportunity arises the opportunity for persons with special interests to utilize the Notary's negligence to confuse the deed from the Notary which raises problems of legal problems in the future, because the information in the Notary deed is something that must be kept confidential and protected by law.

The existence of an electronic document is basically very vulnerable to be changed and falsified by unauthorized parties. The Deed that is stored electronically in order to facilitate the filing and making of copies to be given to the parties, the security of the authenticity of deed information is very important.

Basically to ensure that the copy of the deed is the same as the original, the Notary must affix a stamp on the copy of the deed as a legalization sign as provided in Notary Official Law article 56. Legalization is a form of statement about the validity that a copy is declared in accordance with the original, as referred to in Government Administration Law article 73. However, since the copy of the deed was made electronically, the affixing of the stamp is not possible. Considering the copy of the deed will be given through electronic media, then a system of legalization is carried out electronically. To meet this need, an electronic signature is needed that allows the notary to be able to put his signature on the copy of the electronic deed. This electronic signature is required as part of an electronic identification and authentication system.

Based on article 53 of the Government Provisions of Organizing Systems and Electronic Transactions, electronic signatures can be generated through various signing procedures. That means, the law knows all the procedures for signing electronically. In accordance with the times, today various types of signing procedures are known, such as scanned signatures, use of passwords, biometrics, barcodes, and digital signatures with or without utilizing Public Key Infrastructure (PKI).

Not much different from affixing a conventional signature, basically an electronic signature functions as a signature on paper, or what is called the functional equivalent approach. With this approach: (i) information is considered written if it can be stored and recovered, (ii) the information is considered authentic if it is stored and found and read again does not change its substance, or guarantees its authenticity and integrity, and (iii) the information is deemed signed if there is information that explains the existence of a legal subject responsible on it or there is a reliable authentication system that explains the identity and authorization of that party.

The electronic signature used is expected to guarantee that there are 6 communication security rules, namely: (i) authenticity of the information, (ii) authorization of authority to make or to do so, (iii) confidentiality of its information, (iv) integrity of its information, (v) availability, (vi) cannot be denied by counterparty (non-repudiation), or at least fulfills the minimum requirements stipulated in article 11 paragraph (1) ITE Law. The more fulfilled the rule, the higher the level of security, which in turn will have an impact on the level of authenticity of the information presented.

3.4. Method of Securing Deeds/Documents Electronically

As previously explained, the notary deed is included in a dynamic archive based on Archive Law. As the creator of the archive, the Notary is obliged to provide dynamic files for entitled archival users. In this case, the notary deed must be open and easily accessible to the parties who have a direct interest in the deed. The notary must make a quotation of the deed concerned to meet the needs of the parties.

It is undeniable that every notary has a different quality of service, from the quality of the safest service to the most insecure one. Conventionally, the notary will look for the deed at the depository every time the client requests a copy of the deed. Then for a notary without integrity, he will lend the original deed to the client. This raises a variety of problems, namely the problem of filing and deed security issues that are very vulnerable to damage and forgery. In terms of filing, it is conceivable if the notary saves thousands of deeds and must look for the deed when requested by the client. Then in terms of security, not all notaries have a good filing system. Deed will be very vulnerable to destruction and forgery.

To guarantee that the copy of the deed that is stored electronically is the same as the original, without prejudice to the Official Law article 56 Notarial provisions, the following methods will be needed, such as watermarking, barcode, QR Code, and cryptography. This is in accordance with the rules contained in the Regulation of the Head of the National Archives of the Republic of Indonesia No. 9 of 2018 concerning the Guidelines for the Maintenance of Dynamic Archives, article 27.

3.5. Responsibility for The Implementation of Electronic Systems

When a Notary keeps records in the network, the Notary must also pay attention to the network or electronic system he uses. This happens because the network is very vulnerable to accidents and damage to data if it is not protected. Poor network security can cause network security breach, and if left unchecked, it will be followed by breach data. Breach data itself is a security issue from unathorized exposure of personal and sensitive data.

Network security breach occurs when networks are accessed by unauthorized users. Right when the unauthorized user enters the network, he can steal data on the network and install viruses. To avoid network security breach, of course good network security is needed. Network security itself is a set of policies and practices implemented to prevent unauthorized access, data modification, Denial of Service (DoS), and Distributed Denial of Service (DdoS) attacks. Network security, which consists of several security rules, must at least meet five objectives, namely confidentiality, integrity, availability, authorization, and authenticity.

In discussing what security is right to be applied in network security, beforehand we need to know what threats to the network that are currently circulating, including:

1) System Vulnerabilites, the situation happens when laptops, PCs, and servers that don't have the latest security patches have serious problems in network security. {Trend Micro)
2) Improper Credentials, when a user has a password that is easy to guess/weak password that is eventually easily tracked by hackers.
3) Virus or Malware Through Email, this situation happens when Hackers usually use email and spam, to instant messaging, to spread viruses or malware.
4) Human Error, this situation can include document loss or document theft, hardware that is not encrypted, share account details, or send data via email or fax to the wrong recipient. (Farooq) Human error is called the main cause of breach data.

Then with all kinds of threats that cause network security breach can be reduced or prevented in several ways, namely, among others: (1) Firewall; (2) Automaticallyly Patch Operating Systems and Applications; (3) Use Strong User Authentication, (4) Enable Security Software or Anti Virus; (5) Provide Stakeholder Awareness Training; (6) Backup and Encrypt Data; and (7) Use Secure Socket Layer (SSL).

In Indonesia, regulations concerning Electronic systems are regulated in the ITE Law and Government Regulation No. 82 of 2012 concerning Organizing Systems and Electronic Transactions (PP PSTE), relating to how to build reliable, safe and operating Electronic Systems as they should. Reliable means that the Electronic System has the ability to suit the needs of its users. Safe means the Electronic system protecting physically and non-physically. Operating properly means the Electronic System has the capability in accordance with its specifications. Responsible means that there are legal subjects who are legally responsible for the operation of the Electronic System. This standard of feasibility must be fulfilled, because if the system is feasible, then it is ensured that the system is safe and the results of its authenticity can be accounted for.

In the case of the Implementation of Electronic Systems, the scope of arrangements for the Implementation of Electronic Systems for public services includes arrangements for registration, hardware, software, experts, governance, security, certification of feasibility, and supervision. Arrangements regarding the Safeguarding of the Implementation of Electronic Systems are regulated in articles 18-29. In article 19 it is stated that Electronic System Providers must protect the Electronic System components and Article 22 paragraph (1) stated that Electronic System Providers must maintain the confidentiality, integrity, authenticity, accessibility, availability and traceability of Electronic Information and/or Electronic Documents in accordance with the provisions of statutory regulations.

So it is mandatory for providers of electronic systems to maintain security for both the stored documents and the electronic system. Provisions regarding this matter are also contained in the Minister of Communication and Information Technology Regulation No. 4 of 2016 concerning information security management systems that apply SNI 27001. Furthermore, this will be accomplished by the Regulation of the Head of the Cyber and National Encryption Agency which receives delegations of authority on information security from the Ministry of Communication and Information in accordance with Presidential Regulation No. 53 of 2017 and Presidential Regulation No. 133/2017.

4. CONCLUSION

Along with the development of information technology, to ensure the security of the data stored in the electronic system so that it continues to meet the aspects of authenticity and reliability, the existence of an electronic deed security system is expected to be used by a Notary in carrying out its obligations to maintain and secure the protocol. Besides, when store the deeds electronically, not only the physical deeds that should be secure, but also the network that should be secured.

That in line with the expectations regarding the cyber notary, then as a state archive that is made possible electronically, the Notary needs to apply the use of electronic signatures and electronic certificates in making electronic records (original and copies) in order to have legitimate and binding powers in accordance with the Archive Law and ITE Law.

ACKNOWLEDGMENT

We wish to express appreciation to many colleagues for supporting this research after going through a lot of discussion and communication among them, Tjong Sendrawan, Notary in Jakarta as interviewees, Ayu Galuh Anggraini, Priska Putri Andini, and Aligar Syahan Putra from LKHT Faculty of Law Universitas Indonesia.

Thanks to the magister of notarial law lecturers' faculty of Law Universitas Indonesia especially the dean, Edmon Makarim as the research supervisor.

REFERENCES

[1] "Network Security Breach". Available:https://www.solarwindsmsp.com/content/network-security-breach.

[2] Canadian Centre for Cyber Security, "Baseline Cyber Security Controls for Small and Medium Organizations", Communications Security Establishment. Available: https://cyber.gc.ca/sites/default/files/publictions/Baseline%20Cyber%20Security%20ontrols%20for%20Small%20and%20Medim%20Organizations.pdf

[3] E. Makarim, Notaris dan Transaksi Elektronik, 2nd ed. Depok: Rajagrafindo Persada, 2013, pp. 49-50.

[4] H. Adjie, Hukum Notaris Indonesia: Tafsir Tematik terhadap UU No. 30 Tahun 2004 tentang Jabatan Notaris. Bandung: Rafika Aditama, 2008, p. 33.

[5] M. Irawan, "Manajemen Arsip Dinamis Suatu Pendekatan Kearsipan", Suara Badar, vol I., p. 16, 2001.

[6] P. Muljono, "Pengelolaan Arsip Modern" Pelatihan Otomasi Arsip Berbasis Teks Lengkap dalam Menyongsong Otonomi Daerah/Lembaga Angkatan V Institute Pertanian Bogor, 2001.

[7] Securitytrails Team, "Top 5 Ways to Handle a Data Breach". Available: https://securitytrails.com/blog/top-5-ways handle-data-breach.

[8] Trend Micro, "Data Breaches 101: How They Happen, What Gets Stolen, and Where It All Goes". Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101.

[9] U. Farooq, "Network Security Challenges". Available: https://www.researchgate.net/publication/326804623_Network_Security_Challenges.

[10] White Paper: Enterprise Security, "Anatomy of A Data Breach: Why Breaches Happen and What To Do About It". Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/banatomy_of_a_data_breach_WP_20049424-1.en-us.pdf.