Implementation of Digital Signature Using a SWOT Analysis to Improve Information Security

Nanda Iryani[1], Denny Setiawan[2,3]

[1]Institute Teknologi Telkom Purwokerto
[2]*Electrical Engineering, Universitas Mercu Buana*
[3]*Ministry of Communcication & Information Technology of the Republic of Indonesia,*
[1]nanda@ittelkom-pw.ac.id [2,3]denny.setiawan@mercubuana.ac.id

Abstract

At present in the digitalization era, online transactions continue to grow as well as digital signatures are becoming known to the public. Renewal of research and improvements continues to be made to improve the implementation of digital signatures in Indonesia. There needs to be research to find out the differences between the providers of electronic certificates that are developing in Indonesia. Digital signatures are expected to be able to simplify the administrative process and be implemented properly at Perum LKBN Antara. The application of digital signatures is protected by Ministerial Regulation No. 11 of 2018 and Government Regulation No. 82 of 2012 concerning the implementation of systems and electronic transactions (PSTE). In this study using the SWOT analysis (Standard, Weakness, Opportunities, Threat) as a problem-solving method. There are 4 criteria assessed, namely the ease, security, work system and speed of the system category. In-depth discussion using the privyID application system. The application of using privyID is classified as good at Perum LKBN Antara.

***Keywords*:** Digital signature; Electronic certificate; SWOT; privyID

DOI: 10.22441/incomtech.v9i2.6473

1. INTRODUCTION

Business and electronic transactions have become a rapidly growing trend in information technology. The communication and data information media are increasingly aggressive in dominating the life sector but on the other hand there is a threat in the form of threats to attack communication data that cannot be ruled out, for example by breaking passwords so that data can be accessed by irresponsible parties. Security in using and accessing data is a convenience for users that emphasizes the importance of electronic information security.

The Indonesian government has provided a public legal umbrella for electronic transactions as stated in Law No. 11 of 2008 concerning information and electronic transactions in addition to that also issued Government Regulation No.82 Year concerning the Implementation of Electronic Transaction Systems (PP PSTE).

Many types of electronic transactions that have developed in the world of information technology include digital signatures. Sometimes the number of documents that must be signed by leaders who are not in place causes the process of signatures to take quite a long time, resulting in making operations often disrupted. Digital signatures are not easily imitated by others, and can be automatically timed [1].

Digital signatures provide data origin, authentication and data integrity [2] have a basis for public key cryptographic algorithms that have different encryption and description codes. The key use of asymmetric cryptography has strength depending on the length of the key and the algorithmic approach used. The longer the key used, the safer the data is sent and the more complicated the algorithm is used, the more data encryption results will be safe [3].

The research objective is to find out the comparison of digital signature of SiVION, iotentic, OSD and privyID products in Indonesia and to know the implementation of digital signatures at LKBN Antara.

2. RELATED WORK

2.1 Related Research

In this study, there are various literatures that form the theoretical basis of the authors in conducting research, the literature consists of various scientific books and papers in accordance with research. The initial literature study was conducted by gathering information, both literature in the form of papers, journals, books and the results of previous studies regarding information system security. Related research will be explained based on the following points:

Table 1. Matrix Related Research

No	Author	Title	Method	Aim
1	Dea saka kurnia putra dan Edit prima	Evaluating Certificate Policy - Certification Practice Statement of Unique Government Certification Authority using Public Key Infrastructure Assessment Guidelines: Research in Progress	**PKI Assessment Guidelines**	evaluate OSD PSE operations compliance with CA's environmental control principles from TSPCCA version 2.0
2	Abdul Gani Putra Suratma, Abdul Azis	Digital Signature uses QR Code with the Advanced Encryption Standard Method		Digital signatures can function as leadership signature authentication as well as verification of legal document retrieval.
3	Ida Nurhaida, Desi Ramayanti dan Rhema Riesaputra	Digital Signature & Encryption Implementation for Increasing Authentication, Integrity, Security and Data non-Repudiation		digital signature and encryption functions can be effectively implemented in the process of sending data / information via email
5	Nanda Iryani & Denny Setiawan	Application of Digital Signatures Using Swot Analysis to Improve Information Security	**SWOT Analysis**	Application of Digital Signatures Using SWOT Analysis to Improve Information Security

2.2. Electronic Certificates

Electronic certificates and certificates of reliability of electronic certificates are electronic certificates and contain electronic signatures and identities indicating the legal status of the parties in electronic transactions issued by Electronic

Certification Organizers (PSrE). The PSRE authority based on Article 60 PP PSTE, [5] includes:

A. Examination of candidates for Electronic Certificate holders.
B. Issuance of Electronic Certificates
C. Extension of validity period of Electronic Certificate.
D. Blocking and revocation of Electronic Certificates.
E. Validation of Electronic Certificates.
F. Making a list of active and frozen Electronic Certificates.

In digital certificates there is public key info and info on the public key owner. The info is entered into Signature information on the signed electronic document. Through the signature info, the recipient can confirm the identity of the giver of the electronic signature. Each electronic certificate is generated by the Electronic Certification Center (BSE) under the State Code Institute (Lemsaneg). BSE is an entity that has the authority to carry out electronic certificate management such as publishing, revocation and renewal [2].

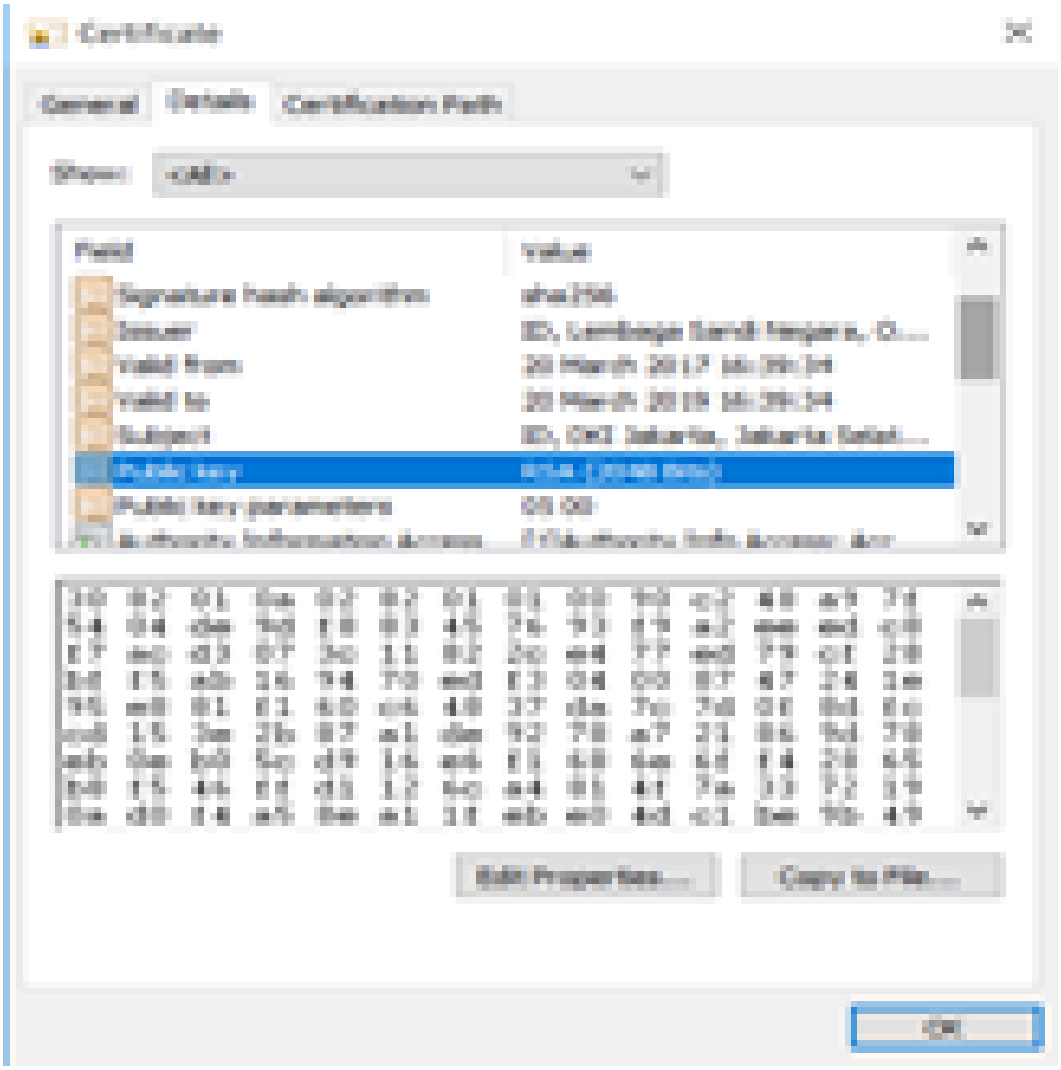

Figure 1. Fill in the Electronic Certificate

2.3. Digital Signature

Explanation of digital signatures is examined including using qr code and using the encryption method, for example research conducted by Suratma, "digital signatures use the qr code with the advanced encryption standard digital signature method using the advanced encryption standard method Azis [1] describe digital signatures with the AES encryption method. Zhang [2] describes digital signatures using the Algorithm ESS encryption method. Nurhaida [3] describe digital signatures with the application of e-mail using Open PGP encryption.

2.4.Information Security

Information security as safeguarding information from all possible threats in an effort to ensure or guarantee business continuity, minimize business risk (reduce business risk) and maximize or accelerate investment returns and business opportunities.

Information Security consists of protection against the following aspects:

a. Confidentiality aspects that ensure the confidentiality of data or information, ensure that information can only be accessed by authorized persons and ensure the confidentiality of data sent, received and stored.
b. Integrity (integrity) aspects that guarantee that data will not be changed without permission from the authorized party, maintain the accuracy and integrity of information and process methods to ensure this integrity aspect.
c. Availability (availability) aspects that ensure that data will be available when needed, ensuring that eligible users can use information and related devices (related assets when needed) [16].

The SMKI is implemented as a management plan to protect information assets from all security problems and implement security controls that have been adjusted to the needs of the organization [17].

2.5. HASH Function

The hash function basically functions in one direction. This means that the original message will be converted into a digest message. But, the message generated by the digest cannot be reversed into the original message. Senders and recipients have a way for data integrity to be investigated [12].

2.6. Regulation in Indonesia

Policy or regulation is an anticipatory step, the Indonesian government against the threat of information security. Regulations that have been issued by the Indonesian government regarding information security include:

a. Law of the Republic of Indonesia No. 11 of 2008 concerning Information and electronic transactions: The Law on Electronic Information and Transactions (ITE) has mandated the obligation of providers of electronic systems both private and public to operate electronic systems that can protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information
b. Decree of the Minister of Communication and Information Number: 133/KEP/ M/KOMINFO/04/2010: The decree issued by the Minister of Communication and Information contains the establishment of the Indonesian Information Security Coordination Team which has the task of coordinating, formulating policies, compiling technical instructions, organizing awareness campaign, as

well as monitoring and submitting implementation reports on information security in Indonesia.

c. Circular of the Minister of Communication and Information Number: 01/SE/ M.KOMINFO/02/2011: This circular letter contains the Implementation of Electronic Systems for Public Services in the State Administration Agency.
d. Circular of the Minister of Communication and Information Number: 5/SE/ M.KOMINFO/07/2011 concerning Implementation of Information Security Governance for Public Service Providers
e. PP No. 82, 2012 concerning the Implementation of Systems and Electronic Transactions (PSTE). This regulation regulates the implementation of electronic systems, the implementation of electronic transactions, electronic signatures, the implementation of electronic certification and the trustmark and management of domain names.
f. PP No. 11 of 2018 that speaks related to industry. CAs are explained to have 3 types, namely indexed, fermented and registered.

2.7. SWOT Analysis

SWOT analysis is one technique to analyze strategies that focus on analysis of Strengths, Weaknesses, Opportunities, and Threats.

There are 4 main indicators used in each aspect of the SWOT analysis which include systems, infrastructure, applications, and HR [9].

The IT division is in a growth strategy, meaning that it can carry out an activity to increase the type of service to users, improve facilities and information technology through internal and external development through acquisitions or joint ventures with other institutions both in the same industry and industries that support the smooth delivery of services IT Division [10].

3. METODOLOGY

3.1. Method of Collecting Data

Data collection is done to get the desired information for the achievement of research objectives. The following is how to collect data carried out by the author to find out the process and stages of the digital signature document system in the form of an electronic certificate:

A. Interview
B. Library
C. Questionnaire

3.2. Analysis Method

This study uses the method of SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats. SWOT analysis serves to analyze the strengths and weaknesses of the electronic certificate system using a questionnaire on the internal conditions of LKBN Antara, in addition to analyzing the opportunities and threats faced by LKBN Antara do a questionnaire on external conditions Perum LKBN Antara. Following the method used [8].

4. IMPLEMENTATION & RESULTS

4.1. Digital signatures in Indonesia

4.1.1. SiVION

The Online Verification System (SiVION) is a program owned by the Ministry of Communication and Information through the Directorate General of Information Applications in order to use signatures that provide digital certificates to applicants which is validation for him to use digital signatures in conducting transactions in electronic systems.

To realize SiVION, the Ministry of Communication and Information has made policies and regulations, prepared a National Root CA (Certification Authority) by legalizing Government CAs and Private CAs, and also provides education for the community because there are additional business processes in online transactions. In the infographic scheme it can be described in Figure 2.

Figure 2. National Identity Verification System (SiVION)

4.1.1.1. Work and Technical Systems

To realize SiVION, the Ministry of Communication and Information has made policies and regulations, prepared a National Root CA (Certification Authority) by legalizing Government CAs and Private CAs, and also provides education for the community because there are additional business processes in online transactions.

4.1.1.2.Application of application in life

SiVION provides digital certificates for individuals, organizations and servers belonging to the community and government. Validation of digital certificates will be done immediately (real time) on each Electronic Certification Operator (PsrE) with a certificate issuer (Root Certification Authority / Root CA).

4.1.1.3. Strengths

By using a digital certificate capable of proving the authenticity of the owner of a message or digital document, the security of digital certificates can be proven if there is a change in the data in the document, it will bring up invalid data information.

4.1.1.4. Weakness

Digital identity and digital legal system. Digital identity is an identity issued by a third party, validating the identity of the applicant using existing verification (bank, post, etc.), the use of digital identities is different according to the level of equal identity validation, the use of digital identity adjusts to the level of accuracy of online service identity.

4.1.2. Iotentik

iOTENTIC is used for public services and non-public services in government agencies that require security with digital certificates. Digital certificates guarantee security in the form of authentication, data integrity and no denying the use of digital certificates.

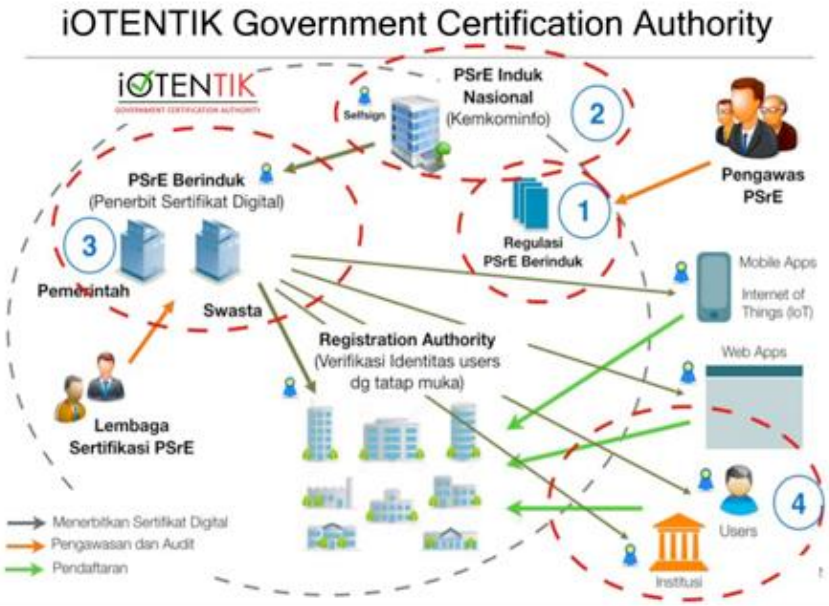

Figure 3. iOTENTIK Goverment Certification Authority

4.1.2.1.Work and Technical Systems

As an organizer of electronic certificates, iOTENTIK has a role as: CA (Certification Authority) which functions to issue electronic certificates; VA (Validation Authority) which functions to validate electronic certificates; and RA (Registration Authority) which functions as the registration for issuing electronic certificates.

4.1.2.2.Application of application in life

iOTENTIK uses EJBCA's CA and VA system directly while for RA systems, iOTENTIC uses RA Box to facilitate configuration. RA Box is a RA package which is a modification of EJBCA's RA which consists of RA application, operating system, security system, and storage media in the form of USB Tokens. RA application on RA Box was built using JAVA programming and MySQL database.

4.1.2.3. Strengths

CA operations are resistant to various attacks so that electronic certification services continue to run well. Some activities that can be done to safeguard the security of the CA include limiting access to CAs, maintaining the security of the CA private key from unauthorized parties, conducting digital signatures on all certificate requests, and ensuring that the CAs used have been verified by outside entities.

4.1.2.4. Weakness

IKP technology is still little applied to support e-government services so that it has not become a special concern.

4.1.3. OSD

Lemsaneg State Institution Digital Certificate Authority (OSD) is a CA (Certification Authority) whose function is to issue, distribute and manage digital certificates with government institutions.

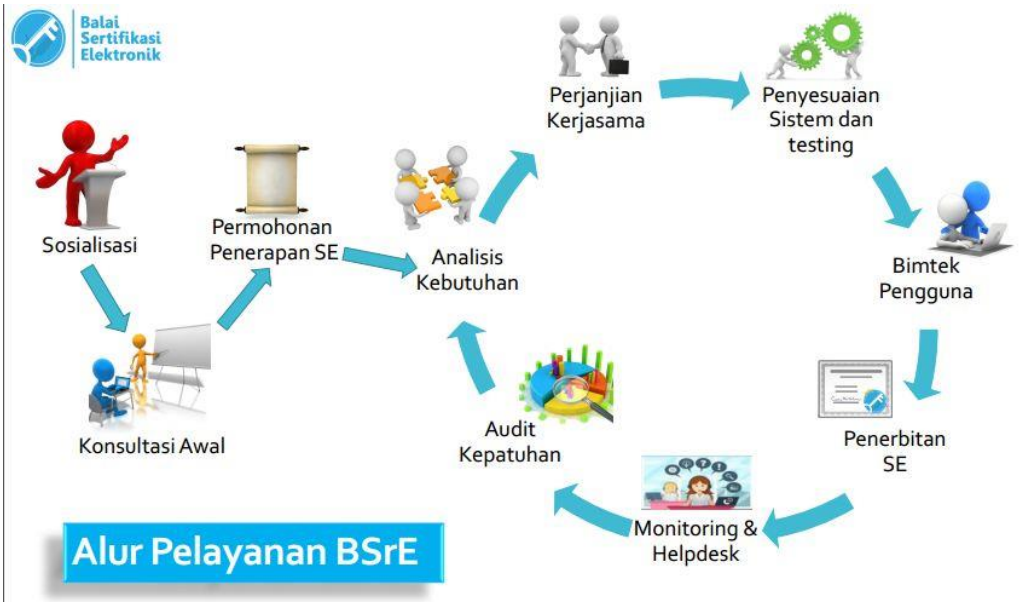

Figure 4. Service flow obtains certification from BSrE State Code Institutions

4.1.3.1.Work and Technical Systems

Lemsaneg OSD is managed by a government institution called the Electronic Certification Hall (BSrE). BSrE aims to manage and issue electronic certificates used in electronic systems to meet aspects of electronic information security in government agencies. BSrE publishes and ensures electronic certificates in accordance with the provisions stipulated in CP. Certificate Policy, hereinafter abbreviated as CP, is a provision and policy that regulates all parties related to the use of electronic certificates issued by BsrE.

4.1.3.2.Application of application in life

OSD PSE has a cryptoperiod key pair of 5 years. According to the OSD PSE key cryptoperiod, BSrE as OSD PSE government agent must extend the OSD PSE cryptoperiod key pair. The key ceremony was held in 2016 to produce OSD PSE G2, OSD LU K1, OSD LU K2, OSD LU K key pair K3, and OSD LU K4 with 10 years cryptoperiod [8].

4.1.3.3. Strengths

Facilitate managing and issuing Electronic Certificates used in electronic systems to meet aspects of electronic information security in government agencies.

4.1.3.4. Weakness

a. Only can be applied to all PNS members in Indonesia.
b. Only works on Windows and Linux but does not support Android and some Apple products.

4.1.4. PrivyID

PrivyID can increase the effectiveness of the business of companies in the country, because they present a solution that allows two parties to provide official documents without having to be in the same place or send them by courier.

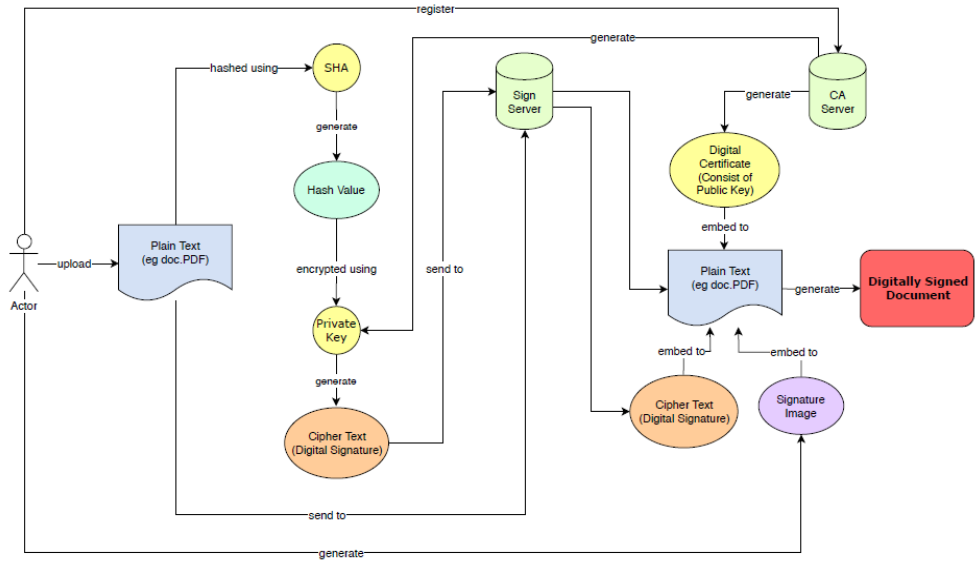

Figure 5. Flow of the publishing process

4.1.4.1.Application of application in life

PrivyID automatically proves the user's identity when the user signs using the Digital Certificate owned. PrivyID provides certainty about user involvement in signing actions.

4.1.4.2. Strengths

a) Time efficiency
b) Low Cost
c) Paper less
d) Easy implementation
e) Easily accessible

4.1.4.3. Weakness

It cannot cross between privyID, for example SiVION service providers and privy ID publishers. And Registrants must have eKTP data, e-mail, cellphone numbers and selfies.

4.2. Realization

Table 2. Comparison of Digital Signature Applications

	PrivyID	**Sivion**	**OSD**	**iOtentik**
Server	*Sign Server*	*Client server*	*Client server*	*Client server*
Pendaftaran	Foto selfie, KTP, E-mail, No HP	KTP, E-mail	KTP, E-mail	KTP, E-mail
Fungsi	Pendaftaran, penyelenggara & penerbit sertifikat elektronik	Pennyelenggara sertifikat elektronik	Penerbit sertifikat elektronik	Penerbit sertifikat elektronik
Pengguna	Swasta dan Instansi Pemerintahan	Swasta dan Instansi Pemerintahan	Instansi Pemerintahan	Instansi Pemerintahan

a. The use of SiVION at the Antara LKBN Perum There has been a change in the communication regulation No. 11 of 2018 which states officially that the SiVION function has changed to root Ca and is not an electronic certificate provider.
b. not an electronic certificate organizer. Use of Authentic at Perum LKBN Antara
c. Cannot be realized due to the limitations that those who register or prospective iOtentik users must have an NIP (Employee Number). In accordance with ministerial regulation no.82 of 2012 article 58 no.2.
d. Use of OSD at Perum LKBN Antara Cannot be realized due to the limitations that those who register or prospective iOtentik users must have an NIP (Employee Number). In accordance with ministerial regulation no.82 of 2012 article 58 no.2.

Results of the SWOT Analysis

4.2.1. PrivyID questionnaire table

Table 3. privyID security categories

NO	PERTANYAAN / PERNYATAAN	NILAI				
		1	2	3	4	5
1	Apakah aplikasi melakukan upaya-upaya untuk melindungi kerahasiaan data pengguna ?					
2	Apakah aplikasi menjamin bahwa setiap konten yang diunggah dan dikirim oleh pengguna akan tersimpan secara aman ?					
3	Apakah terdapat notifikasi bila terdapat kebocoran data pengguna ?					
4	Dokumen yang telah dibubuhkan tanda tangan elektronik hanya bisa diakses oleh orang yang behasngkutan.					

Table 4. Categories of privyID work systems

NO	PERTANYAAN / PERNYATAAN	NILAI				
		1	2	3	4	5
1	Apakah aplikasi dapat membantu kinerja pegawai yang bersangkutan ?					
2	Apakah aplikasi dapat mempercepat proses surat menyurat / administrasi ?					
3	Peletakan tanda tangan elektronik fleksibel.					
4	Apakah terdapat notifikasi pemeritahuan jika tanda tangan digital kadaluarsa ?					

Table 5. PrivyID ease category

NO	PERTANYAAN / PERNYATAAN	NILAI				
		1	2	3	4	5
1	Apakah informasi yang disediakan oleh aplikasi mudah dimengerti ?					
2	Apakah aplikasi menyediakan informasi yang detail ?					
3	Apakah tampilan menu mudah untuk dikenali ?					
4	Apakah penggunaan menu atau fitur menu aplikasi mudah digunakan ?					
5	Apakah aplikasi mudah dioperasikan ?					
6	Apakah apliakasi mempunyai kemampuan dan fungsi sesuai yang diharapkan ?					
7	Apakah aplikasi mudah dipelajari ?					

Table 6. PrivyID speed

NO	PERTANYAAN / PERNYATAAN	NILAI				
		1	2	3	4	5
1	Apakah aplikasi cepat diakses ?					
2	Aplikasi cepat dalam membuat tanda tangan elektronik untuk dokumen.					
3	Aplikasi cepat dalam membubuhkan tandatangan elektronik ke dokumen.					

4.2.2. Results of Questionnaire Calculations

The questionnaire was distributed in 4 parts of the Division consisting of: Human Resources (HR) Division, Information Technology, Corporate Secretariat and Editorial Secretariat. Of the total 55 collected 47 questionnaires were filled.

a. Results of assessment of application ease of use category.

Pertanyaan	1	2	3	4	5	6	7	TOTAL
Total per-Pertanyaan	177	172	185	181	176	180	178	1249
Rata-rata	3.93	3.82	4.11	4.02	3.91	4.00	3.96	3.97

b. Results of assessment of application security categories

Pertanyaan	1	2	3	4	Total
Total per-Pertanyaan	181	185	186	190	742
Rata-rata	3.85	3.94	3.96	4.04	4.04

c. Results of assessment of application performance categories.

Pertanyaan	1	2	3	4	Total
Total per-Pertanyaan	193	193	186	182	754
Rata-rata	4.11	4.11	3.96	3.87	4.01

d. Results of assessment of application speed categories

Pertanyaan	1	2	3	TOTAL
Total per-Pertanyaan	172	184	180	536
Rata-rata	3.74	4.00	3.91	3.91

In the questionnaire table, it can be seen from the four categories assessed as showing an average yield of 4, so it can be concluded that the application of digital signatures using PrivyID applications at the LKBN Antara Corporation is well implemented.

5. CONCLUSIONS

In the use of digital signatures that use electronic certificates the most suitable to be implemented at the LKBN Antara Corporation is .privyID due to:

a. PrivyID has the authority to accept registration, verify, and issue electronic certificates and electronic signatures for Indonesian citizens. So that the application can be done well.
b. The LKBN Antara company is classified as a private consumer which can be managed related to digital signatures by private institutions, namely privyID.
c. Implementation is easier because it is done using an application.

REFERENCES

[1] A. A. Abdul Gani Putra Suratma, "tanda tangan digital menggunakan qr code dengan metode advanced encryption standard digital *signature* using qr code by advanced encryption standard method abdul gani putra suratma , abdul azis," vol. 18, no. 1, pp. 59–68, 2017.

[2] Q. Zhang, Z. Li, And C. Song, "the improvement of digital *signature* algorithm based on elliptic curve cryptography," pp. 1689–1691, 2011.

[3] I. Nurhaida, "digital *signature* & encryption implementation for increasing authentication , integrity , security and data non-repudiation," vol. 4, no. 11, pp. 4–14, 2017.

[4] W. Pradono and Y. Yourdan, "analisis kebijakan standardisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan keamanan nasional (policy analysis on telecommunication devices security standardization to support national security and defence policy)," *bul. Pos dan telekomun.*, vol. 13, no. 2, p. 151, 2015.

[5] A. B. Setiawan, "the ecosystem of electronic certificate implementation in electronic commerce system ahmad budi setiawan," *j. Penelit. Dan pengemb. Komun. Dan inform.*, vol. 6, no. 2, pp. 15–27, 2015.
[6] A. Cryptography And T. Ciphers, *foreword by whitfield diffie preface about the author chapter 1 — foundations part i — cryptographic protocols chapter 2 — protocol building blocks chapter 3 — basic protocols chapter 4 — intermediate protocols chapter 5 — advanced protocols*. .
[7] A. J. Menezes, P. C. Van Oorschot, And S. A. Vanstone, "applied cryptography."
[8] Hakak, S., Kamsin, A., Tayan, O., Idna Idris, M. Y., Gani, A., & Zerdoumi, S. (2017). preserving content integrity of digital holy quran: survey and open challenges. *ieee access*, *5*, 7305–7325.
[9] Y. Handri, E., & Ferina, F. (2016). penentuan model kepercayaan infrastruktur kunci publik di indonesia dengan pendekatan analytic hierarchy process.
[10] Krisna, S. A., & Purwadi, H. (2018). international journal of multicultural and multireligious understanding utilization of public key infrastructure to facilitates the role of *certification authority* in cyber notary context in indonesia, (2009), 345–355.
[11] D. P. K. Suwarno, "keabsahan tanda tangan elektronik pada perjanjian kontrak bisnis di indonesia," 2017.
[12] M. A. Fauzan And E. Paulus, "journal of computing and applied informatics a framework to ensure data integrity and safety," vol. 1, no. 2, pp. 1–12, 2018.
[13] S. Rahayu, D. Malik, And M. M. Minarsih, "strategi pengembangan sumber daya manusia guna meningkatkan kinerja karyawan melalui analisis swot divisi cash processing center (studi kasus pada pt advantage scm kota semarang)."
[14] D. S. K. Putra and E. Prima. (n.d.). evaluating certificate policy-certification practice statement of unique government *certification authority* using public key infrastructure assessment guidelines: research in progress edit prima.
[15] Lembaga Sandi Negara. (2015). kerjasama lkpp-lemsaneg, (november).
[16] Dewi, A. C., Nugroho, E., Hartanto, R., Grafika, J., Yogyakarta, N., & Sumur, B. (2017). manfaat perealisasian tata kelola keamanan informasi berbasis sni iso/iec 27001:2009 produksi film animasi (kasus), 843–847.
[17] Riadi, F. T., Manuputty, A. D., & Saputra, A. (2018). evaluasi manajemen risiko keamanan informasi dengan menggunakan cobit 5 subdomain edm03 (ensure risk optimisation) (studi kasus : satuan organisasi xyz – lembaga abc). *jutei*, *2*(1), 1–10.