Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia: PT Privy Identitas Digital

Wita Dewisari Tasya 18218037(*Author*)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: 18218037@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas sisi keamanan penyelenggara sertifikasi elektronik Indonesia yaitu PT Privy Identitas Digital. Keamanan akan ditinjau dari sertifikasi digital di Indonesia, profil Privy, dan repositori Privy dengan lampiran yang ada. Kesimpulan dari makalah ini adalah Privy sudah memenuhi standar keamanan yang ditetapkan di Indonesia dengan proses menjadi PSrE berinduk yang sudah dilakukan dan juga pemenuhan standar keamanan data pribadi.**

Keywords—sertifikasi digital; tanda tangan elektronik; penyelenggara sertifikasi digital; keamanan data; kriptografi

I. PENDAHULUAN

Dalam peresmian dokumen-dokumen digital, diperlukan adanya tanda tangan elektronik (bukan tanda tangan fisik yang dibuat digital) untuk memastikan keaslian dan keresmian dari dokumen tersebut. Berdasarkan web Kementerian Komunikasi dan Informatika (Kominfo), terdapat beberapa Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia atau biasa disebut juga dengan *certification authority* (CA) [1]. Salah satunya PT Privy Identitas Digital atau Privy.id. Makalah ini akan meninjau keamanan layanan Privy.id sebagai penyedia layanan sertifikasi digital berupa tanda tangan digital.

II. METODOLOGI PENELITIAN

A. Jenis Penulisan

Sebuah paragraph berisikan text untuk diisi dengan konten yang sebenarnya. Makalah dituliskan dengan metodologi deskriptif analitis dengan analisis yang dilakukan setelah mengkaji sumber studi literatur. Penulisan dilakukan dengan *template* penulisan IEEE berisi paragraf dan diakhiri dengan kesimpulan hasil analisis.

B. Batasan Penulisan

Analisis keamanan Privy.id hanya dilakukan melalui data sekunder dari berbagai web dan kebijakan yang dirilis. Tidak dilakukan percobaan tertentu untuk menguji keamanan.

C. Sumber Data dan Teknik Pengumpulan Data

Data yang akan digunakan didapatkan dari penerbitan jurnal, web, buku, dan sumber relevan lainnya yang dapat ditemukan secara daring. Sumber yang digunakan hanyalan yang berasal dari situr resmi atau situs yang penulisnya memiliki reputasi baik dalam bidang terkait.

III. STUDI LITERATUR DAN PEMBAHASAN

Studi literatur dilakukan dengan meninjau teori mengenai sertifikat digital, meninjau perusahaan PT Privy Identitas Digital dan layanan yang disediakan, serta bagaimana aspek keamanan dari layanan tersebut.

A. Serfitikasi Digital di Indonesia

Sertifikat elektronik merupakan tanda tangan elektronik (TTE) dan identitas yang mewakili status subjek hukum pihak-pihak yang terlibat dalam transaksi elektronik [2]. Sertifikat digital ini diterbitkan oleh Penyelenggara Sertifikasi Elektronik (PSrE).

PSrE dijelaskan pada Peraturan Menteri Kominfo Nomor 11 Tahun 2018 tentang Penyelenggara Sertifikat Elektronik. Penyelenggaraan sertifikasi elektronik adalah kegiatan menyediakan, mengelola, mengoperasikan infrastruktur Penyelenggara Sertifikasi Elektronik, dan/atau memberikan dan mengaudit Sertifikat Elektronik [6]. Penyelenggara sertifikasi elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

PSrE yang beroperasional di Indonesia menganut prinsip satu induk dan PSrE harus mendapatkan pengakuan dari Menteri [2]. Pengakuan tersebut didapatkan dengan berinduk kepada PSrE induk yang diselenggarakan oleh Menteri. Lembaga sertifikasi PSrE terakreditasi akan melakukan penilaian kepada PSrE Indonesia. PSrE dapat menyediakan berbagai layanan yaitu:

- Tanda tangan elektronik (TTE).
- Segel elektronik.
- Penanda waktu elektronik.
- Layanan pengiriman elektronik.
- Autentikasi situs web.
- Preservasi tanda tangan elektronik dan/atau segel elektronik.

PSrE dibagi menjadi dua jenis yaitu PSrE Induk dan PSrE berinduk. PSrE induk merupakan CA yang dijalankan oleh pemerintahan Indonesia. PSrE induk berada di bawah Direktoran Keamanan Informasi, Kementerian Komunikasi, dan Informatika Indonesia. PSrE induk menerbitkan sertifikat elektronik bagi PSrE berinduk. PSrE berinduk merupakan CA yang sudah diakui PSrE induk dan dapat menjalankan jasa sertifikasi digital untuk perseorangan maupun suatu lembaga [7].

Tanda tangan elektronik merupakan tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya [2]. Tanda tangan elektronik (TTE) digunakan sebagai alat verifikasi maupun autentikasi untuk memastikan aspek keamanan yang disediakan oleh kriptografi dapat terjaga.

Fungsi dari tanda tangan elektronik sangat beragam Berikut merupakan fungsi yang dinyatakan pada web kominfo [2]:

- Menggantikan fungsi tanda tangan basah pada dokumen elektronik. Tanda tangan basah tidak dapat memberikan kekuatan hukum kepada dokumen elektronik. Karena itu, dalam meresmikan dokumen elektronik dibutuhkan TTE.
- Pemungkin terselenggaranya sistem perkantoran pemerintah dan swasta tanpa kertas. Dengan menggunakan TTE, berkas perkantoran dapat diverifikasi dan dapat dilakukan autentikasi.

TTE dibuat dan dibuktikan menggunakan sertifikat elektronik. Sertifikat elektronik tersebut diterbitkan oleh PSrE Indonesia. Implementasi TTE di Indonesia dapat dilakukan karena sudah dilindungi dengan UU ITE Pasal 11 yang sudah berlaku sejak tahun 2008. Selain itu, TTE juga sudah dipercaya oleh lembaga swasta, lembaga pemerintah, dan sistem peradilan nasional [2].

B. Privy.id

Privy.id dikembangkan oleh PR Privy Identitas Digital. Pada Tabel I. Profil PT Privy Identitas Digital disampaikan profil lengkap PT Privy Identitas Digital yang diambil dari web kominfo [1].

Gambar I Logo PT Privy Identitas Digital

TABEL I. PROFIL PT PRIVY IDENTITAS DIGITAL

Aspek	Keterangan
Nama	PT Privy Identitas Digital
No SK Pengakuan	Nomor 84 Tahun 2021
Alamat Website	https://privy.id/
Penanggung Jawab	Marshall Pribadi
No Telepon	+6221 22715509
Jenis PSrE	PSrE Non-Instansi
Status Pengakuan	Berinduk

Privy menyediakan layanan tanda tangan digital, permintaan tanda digital, dan mengelola dokumen dengan tanda tangan digital. Layanan tanda tangan tersebut dapat diakses melalui aplikasi web maupun melalui ponsel pintar. Tanda tangan digital yang diberikan juga dilengkapi dengan sertifikat digital yang dienkripsi untuk memastikan keamanan, validitas, dan keresmian dari dokumen yang ditandatangani [4]. Layanan verifikasi PDF dilakukan melalui web PSrE kominfo, tidak melalui aplikasi Privy [5].

Untuk menjadi PSrE Non-Instansi, PT Privy Identitas Digital harus memenuhi persyaratan-persyaratan agar dapat diakui oleh PSrE induk. Berikut merupakan persyaratan yang berlaku:

- Surat Permohonan Pengakuan Status Berinduk
- Proposal Penyelenggara Sertifikat Elektronik
- Dokumen Tanda Daftar Penyelenggara Sertifikat Elektronik
- Akte Pendirian Perusahaan
- Surat Izin Usaha, Bidang Teknologi Informasi
- Surat Pernyataan Fasilitas dan Peralatan di Indonesia
- Prosedur Pengoperasian Fasilitas dan Peralatan
- Interoperabilitas Mengacu Pada Standar Kominfo
- Salinan Bukti Laporan Sertifikasi Atas Audit Terhadap Standar Fasilitas dan Peralatan
- Dokumen Rencana Bisnis, Rencana Keberlangsungan Bisnis, Rencana Penanggulangan Bencana dan Dokumen Laporan Pengujian Sistem Elektronik
- CP/CPS sesuai dengan CP/CPS PSrE Induk
- Salinan Sertifikat Kelaikan Sistem Elektronik
- Tidak Berinduk dan Tidak Menjadi Induk pada PSrE lain
- Memiliki 12 Orang Ahli Operasional
- Jaminan Kerugian Pemilik Sertifikat Elektronik
- Modal Rp 30 Miliar
- Pakta Integritas dan Rekam Jejak

- Surat Keterangan Non Pailit

PT Privy Identitas Digital sudah memenuhi persyaratan tersebut sehingga dapat dinyatakan sebagai CA/PSrE berinduk di Indonesia.

C. Analisis Keamanan pada Privy.id

Sebagai lembaga penyelenggara sertifikasi digital, tentunya Privy.id harus memiliki faktor keamanan yang terjamin. Karena itu, repositori Privy.id akan ditinjau.

1. *Root/Subordinate* CA

Privy.id memiliki delapan *root/subordinate* CA dengan fingerprint yang di-*hash* menggunakan algoritma SHA-256 [8]. Masing-masing *root* memiliki sertifikat yang dapat diunduh. Setiap *root* juga memiliki *Certificate Revocation List* (CRL) yang dapat ditinjau (kecuali pada *root* Root CA Indonesia DS G1 tidak disertakan pranala untuk diakses). CRL berisi sertifikat yang sudah kadaluarsa dan tidak dapat digunakan beserta info-info metadata lain. Pada Tabel II. Daftar *Root* atau *Subordinate* CA, dicantumkan *fingerprint* dari delapan *root*/*subordinate* yang dimiliki.

TABEL II. DAFTAR *ROOT* ATAU *SUBORDINATE* CA

Root*/*Subordinate	***Fingerprint* (SHA-256)**
Root CA Privy CA	581EB03701213870489C7D6E8DF0AFC9DEA6607B9050B0C8585EC6058A50D721
Privy CA Class 1	656C5B2BBF09A4A77DDD8BDA2CC21A99B06E3DB4439481D12609A3819D9E61B1
Privy CA Class 2	FCEE6C563D36C64566D1C263FE34BE7CC00098766207193 38DE0ABE607524890
Root CA Privy CA G2	97CA0824C4DB56DCA00BF9168A4489E8AE9CF6763B5EE4E1CBFF334F17923B12
Privy CA Class 1 G2	3418566DE8FE35525A48914CED07FEF3FC46A208518624AE57DEC37B436FAFC6
Root CA Indonesia DS G1	B5F36672FD7CFD401E01EF640B2FE61F816F32F447B280B76F536244CF42FCDF
Privy CA Class 3 G2	E0CC332DF3FEF19EAB3426D0413AC5C4599F9B10BB31DE866DC384E9C8F59EF8
Privy CA Class 4 G2	2F40C9D594D365220FAE03D76D0BF95C18F42770BB8D4E94AE4904DAF9591698

2. Kebijakan Privasi

Kebijakan privasi yang diterbitkan oleh Privy memberikan informasi yang ditujukan kepada pengguna Privy tentang cara Privy mengumpulkan, membagikan, menggunakan, memproses, dan mengamankan data pribadi pengguna untuk operasional layanan Privy [9].

Privy mengumpulkan data dari pengguna dengan meminta langsung dari pengguna ketika mendaftar ke sistem Privy, data yang terkumpul secara otomatis, data yang pengguna berikan, data dari pihak ketiga seperti otoritas pendaftaran, dan *cookies* [9]. Data pribadi yang diminta oleh Privy adalah nama lengkap, tempat dan tanggal lahir, foto KTP dengan informasi yang jelas, nomor telepon seluler, alamat surat elektronik, dan data biometrik berupa swafoto. Privy berhak menolak permohonan pembuatan akun pengguna atau menangguhkan atau memberhentikan maupun memberhatikan Sebagian atau keseluruhan layanan Privy jika ditemukan informasi data pribadi yang tidak tepat. Data yang otomatis dikumpulkan di antara lainnya IP *Address*, *login information*, *geolocation*, *browser client* & *version*, *timestamp of activities*, *operating system*, dan data transaksi yang didapatkan Privy Ketika pengguna melakukan aktivitas pada aplikasi.

Data pribadi yang sudah disebutkan pada bagian sebelumnya digunakan untuk menerbitkan Privy ID, membuat akun pengguna Privy, juga menerbitkan, mengelola, dan mencabut sertifikat elektronik dari Privy [9]. Selain itu, data aktivitas penggunaan layanan Privy juga dikumpulkan, direkam, dan dianalisis. Informasi mengenai penggunaan akun seperti penggunaan layanan dan informasi berbentuk promosi Privy akan digunakan untuk menyediakan layanan Privy. Data tersebut juga digunakan untuk memperbaiki dan meningkatkan produk dan layanan Privy.

Dokumen kebijakan privasi menyatakan bahwa data pribadi pengguna akan dibagikan untuk memenuhi layanan Privy yang digunakan pengguna saja [9]. Privy mengklaim tidak menjual dan/atau membagikan data pribadi pengguna kepada pihak lain tanpa adanya persetujuan dari pengguna yang bersangkutan. Privy dapat mengungkapkan data pribadi pengguna kepada pengguna lain yang bersinggungan Ketika menggunakan layanan, individu, organisasi, entitas, atau otoritas pemerintahan yang memiliki hak untuk mengetahui data karena adanya ketentuan hukun dan peraturan perundang-undangan, agen, kontraktor, atau pihak ketiga yang berkaitan dengan Privy agar layanan dapat berjalan bagi pengguna, ataupun organisasi atau badan hukum yang mana pengguna diasosiasikan dan didaftarkan kepada organisasi tersebut melalui layanan Privy.

Privy menyatakan bahwa mereka melakukan upaya pengamanan dan penyimpanan dengan hati-hati untuk melindungi kerahasiaan data pengguna [9]. Privy juga tersertifikasi ISO 27001:2013 mengenai *Information Security Management System* sehingga Privy dapat dinyatakan menjaga data pribadi pengguna agar tidak disalahgunakan. Di sisi lain, pengguna juga harus menjaga keamanan data pribadi yang dikumpulkan oleh Privy dengan tidak berbagi kata sandi dan *One Time Password* (OTP).

Pengguna Privy memiliki hak untuk meminta permohonan akses data pengguna, mengajukan

permohonan perubahan data, dan permohonan penghapusan data atau penutupan akun [9]. Pembatasan tanggung jawab dijelaskan dalam dokumen.

3. Tata Cara Pengelolaan Sertifikat

Tata Cara Pelaksanaan Sertifikat PSrE/*Certificate Practice Statement* (CPS) berisi persyaratan usaha, hukum, dan teknis yang mengatur mengenai Penyelenggara Sertifikasi Elektronik Privy oleh peserta di dalam Infrastruktur Kunci Publik/*Public Key Infrastructure* (PKI) [10]. CPS ini dibuat dengan standar X.509 versi 3 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework*. CPS juga dibuat memenuhi kriteria yang diatur oleh *Certificate Policy* dari PSrE Induk. *Object Identifier* (OID) Privy ditetapkan dengan nomor identifikasi joint-iso-itu-t (2) country(16) id(360) gov(1) kominfo (1) rootca(1) psre-berinduk(3) non-asn(12) privy(1).

Pada dokumen tersebut, Privy menjamin tiga faktor yang seharusnya disediakan oleh tanda tangan elektronik [10]. Faktor tersebut adalah *non-repudiation*, *authentication*, dan *integrity*. Ketiga faktor tersebut seharusnya dapat terjamin dari kriptografi. Dengan pernyataan ini, ketiga kebutuhan keamanan tersebut dapat diasumsikan terjamin. Layanan Privy dapat digunakan pengguna untuk menjamin tiga faktor keamanan tersebut.

Privy menerbitkan sertifikat elektronik dengan level verifikasi identitas level 3 dan juga level 4 [10]. Penyediaan sertifikat ini sesuai dengan peraturan perundang-undangan Indonesia yang berlaku yang mengatur mengenai penyelenggaraan sertifikasi elektronik. Sertifikat kelas tiga diterbitkan sesuai dengan level verifikasi identitas level tiga dan sertifikat kelas empat diterbitkan sesuai dengan level verifikasi identitas level empat.

CPS menyatakan penjelasan bahwa repositori menunjang penyelenggaraan layanan PKI seperti *Public Key Certificate* PSrE, CRL dan/atau Status Keaktifan Sertifikat, CP dan CPS, Perjanjian Pemegang Sertifikat, dan Perjanjian Pihak Pengandal. Privy menerbitkan Sertifikat Kunci Publik PSrE paling lambar 1x24 jam setelah pasangan kunci dibangkitkan [10].

Kunci yang dibangkitkan Privy, kunci privatnya akan disimpan dan diamankan dengan modul kriptografis yang memenuhi standar persyaratan Federal Information Protection Standards (FIPS)-140 level 2 [10]. Pembuktian penguasaan kunci privat yang terasosiasi dengan sertifikat pemohon terkait untuk penandatanganan menggunakan metode autentikasi yang ditentukan oleh Privy, meliputi dua dari tiga faktor yang ada. Faktor tersebut adalah *something you know*, *something you have*, *something you are*.

Privy menyediakan layanan untuk autentikasi organisasi dengan identitas dari perwakilan. KTP dari pemegang jabatan akan dicek bersama dengan surat kuasa jika dibutuhkan dan juga dokumen-dokumen pendukung pengesahan badan hukum/badan usaha [10]. Privy akan menyimpan catatan mengenai jenis dan rincian dari identifikasi yang akan digunakan untuk autentikasi bagi organisasi.

Selain itu, autentikasi identitas individu maupun perorangan difasilitasi juga oleh Privy [10]. Pemohon diwajibkan memberikan identitas yang diperlukan dan Privy akan melakukan beberapa mekanisme untuk menghindari keraguan. Mekanisme *active* atau *passive liveness detection* digunakan untuk memastikan bahwa swafoto benarlah diambil oleh pengguna yang hidup. *Remote customer onboarding* dilakukan menggunakan media *video conference* dan verifikator akan bertanya atau memberikan instruksi.

Dalam keberjalanan layanan, pemegang sertifikat menitipkan kunci privat yang dimilikinya ke Privy [10]. Hal ini didasarkan pada perjanjian pemegang sertifikat dengan Privy. Privy menyimpan kunci privat dengan menggunakan *Hardware Security Module* (HSM) dengan spesifikasi minimal FIPS 140-2 Level 2. Sementara itu, pihak pengandal dapat memiliki akses ke *Public Key Certificate* Privy melalui repositori Privy. Privy tidak melakukan pembaruan sertifikat.

Dalam beberapa kondisi, Privy dapat melakukan pencabutan dan penangguhan sertifikat [10]. Adapun keadaan yang menyebabkan adanya pencabutan sertifikat adalah sebagai berikut:

- Pemegang sertifikat mengajukan permohonan pencabutan sertifikat
- Kunci privat yang ada terkompromi, hilang, dan/atau rusak
- Terjadi perubahan pada standar industri, kebijakan pemerintah, dan/atau perubahan pada peraturan perundang-undangan yang memungkinkan adanya pengaruh kepada keabsahan sertifikat
- Informasi yang tercantum di dalam sertifikat tidak akurat atau menyesatkan bagi pihak lain
- Permohonan penerbitan sertifikat yang dilakukan oleh pengguna tidak sah, melalui cara yang kurang sesuai
- Penerbitan sertifikat dilakukan tidak sesuai dengan peraturan dan ketentuan yang tercantum pada CPS
- Pemegang sertifikat melanggar ketentuan yang ada di dalam CPS atau di dalam perjanjian pemegang sertifikat
- Sertifikat Privy mengalami kebocoran sehingga keamanan tidak lagi dapat terjamin

- Privy berhenti beroperasi dan tidak dapat memberikan layanan kepada pengguna
- Alasan lain yang bisa menjadi alas an pencabutan sertifikat menurut Privy

Selain dari sisi teknologi, Privy juga melakukan kontrol terhadap pihak yang bekerja sebagai pemegang kepercayaan. Privy melakukan pengecekan latar belakang karyawan hingga catatan criminal untuk memastikan posisis tersebut diampu oleh oran dengan pengalaman, terampil dalam bekerja, dapat dipercaya, dan beintegritas [10]. Setelah diterima ke dalam perusahaan, karyawan akan diberikan pelatihan sebelum dapat mengisi *trusted roles*. Pelatihan tersebut meliputi pemahaman mengenai konsep dasar PKI, CP/CPS, SOP internal mengenai kegiatan operasional PKI, dokumentasi tata cara penggunaan sistem PKI, dan pemahaman mengenai pentingnya keamanan siber terutama mengenai cara *phising* dan *social engineering*. Selain pelatihan, karyawan juga akan dievaluasi minimal sekali dalam setahun. Pelatihan dilakukan rutin setiap kuartal untuk menjamin keamanan layanan dan data Privy.

Secara teknis, selain yang sudah disebutkan sebelumnya, berikut merupakan keterangan ukuran kunci yang tercantum pada dokumen CPS [10].

TABEL III. UKURAN KUNCI PRIVY.ID [10]

Sertifikat	***Digest Algorithm***	***Encryption Algorithm***	**Panjang Kunci**
Privy CA	SHA-256	RSA	4906-bit
End User	SHA-256	ECC	256-bit

Dari Tabel III. Ukuran Kunci Privy.id dapat dilihat bahwa Panjang kunci Privy CA jauh lebih Panjang dibandingkan dengan milik *end user* sehingga keamanan Privy jauh lebih aman dan sulit dipecahkan. Hal ini sesuai dengan fungsinya sebagai penyelenggara sertifikasi elektronik yang perlu menjamin keamanan pengguna layanan.

Selain itu, masa operasional sertifikat dan masa penggunaan pasangan kunci sudah tercantum. Tabel IV. Masa Operasional Maksimum Pasangan Kunci menyatakan jenis sertifikat beserta jangka waktu operasional untuk setiap sertifikatnya.

TABEL IV. MASA OPERASIONAL MAKSIMUMPASANGAN KUNCI [10]

Jenis Sertifikat	**Jangka Waktu Operasional**
Privy CA Class 3	10 tahun
Privy CA Class 4	10 tahun
Sertifikat Kelas 3	1 tahun
Sertifikat Kelas 4	1 tahun

IV. KESIMPULAN

PT Privy Identitas Digital dapat dikatakan aman dan memenuhi ketentuan sebagai Penyelenggara Sertifikasi Elektronik (PSrE) karena faktor-faktor berikut:

1. PT Privy Identitas Digital sudah diakui merupakan PSrE berinduk yang artinya PT Privy Identitas Digital sudah resmi diakui PSrE sebagai CA dan dapat memberikan layanan sertifikasi digital.
2. PT Privy Identitas Digital sudah memenuhi persyaratan pada bagian III. Studi Literatur dan Pembahasan B. Privy.id Ketika PT Privy Identitas Digital mau mengajukan permohonan pengakuan status berinduk.
3. Repositori PT Privy Identitas Digital sudah menyediakan informasi *root/subordinate* CA beserta CRL dan *fingerprint* yang di-*hash* menggunakan algoritma SHA-256.
4. PT Privy Identitas Digital memberikan keterangan jelas kepada pengguna mengenai data apa saja yang digunakan dalam proses penyediaan layanan tanda tangan digital. PT Privy Identitas Digital juga menyatakan untuk hanya menggunakan data tersebut untuk keperluan operasional dan tidak menyalahgunakan data yang ada.
5. PT Privy Identitas Digital tersertifikasi ISO 27001:2013 mengenai *Information Security Management System* sehingga keamanan data pengguna terjamin kerahasiaannya.
6. PT Privy Identitas Digital memenuhi tata cara pengelolaan sertifikat dengan pelaksanaan layanan yang memenuhi PKI. Ketiga faktor non-repudiation, authentication, dan integrity terpenuhi dalam layanan yang diberikan.
7. PT Privy Identitas Digital menyediakan informasi lengkap mengenai bagaimana kunci privat dan kunci publik ditangani, diamankan, dan dihapus atau ditariknya sertifikat.
8. PT Privy Identitas Digital memastikan sisi non-teknis yaitu sumber daya manusia yang memegang tanggung jawab memiliki pengetahuan dan amanah yang sesuai.

Dari delapan factor tersebut, PT Privy Identitas Digital pengembang aplikasi *web* dan mobile Privy.id dapat dijamin aman dan terbuka dalam menampaikan data dan kebijakan yang berlaku kepada pengguna. Privy juga menjaga kualitasnya dengan prosedur-prosedur yang berlaku.

REFERENCES

[1] Kementerian Komunikasi dan Informatika, "Kominfo Penyelenggara Sertifikat Elektronik - Daftar PSrE," 2021. [Online]. Available: https://tte.kominfo.go.id/listPSrE/_. [Accessed 24 Mei 2022].

[2] Kominfo Penyelenggara Sertifikat Elektronik, "Penyelenggara Sertifikasi Elektronik Indonesia," 2021. [Online]. Available: https://tte.kominfo.go.id/apaitu. [Accessed 24 Mei 2022].

[3] Pemerintah Pusat, "Peraturan Pemerintah (PP) tentang Penyelenggaraan Sistem dan Transaksi Elektronik," 2019.

[4] PT Privy Identitas Digital, "Sign, Share, and Manage Documents with Trusted Digital Signature: PrivySign | Privy," 2020. [Online]. Available: https://privy.id/privysign. [Accessed 24 Mei 2022].

[5] Kominfo Penyelenggara Sertifikat Elektronik, "Verifikasi PDF Kominfo," 2021. [Online]. Available: https://tte.kominfo.go.id/verifyPDF. [Accessed 24 Mei 2022].

[6] Kementerian Komunikasi dan Informatika, "Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik," 2018.

[7] SERTISIGN , "Apa itu Penyelenggara Sertifikasi Elektronik (PSrE)," 2022. [Online]. Available: https://tandatangandigital.co.id/apa-itu-penyelenggara-sertifikasi-elektronik-psre. [Accessed 24 Mei 2022].

[8] PT Privy Identitas Digital, "Repository PrivyCA," 2022. [Online]. Available: https://repository.privy.id/. [Accessed 24 Mei 2022].

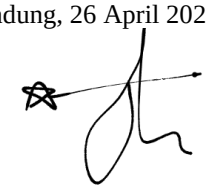
[9] PT Privy Identitas Digital, "Kebijakan Privasi," 20 April 2022. [Online]. Available: https://repository.privy.id/doc/Kebijakan-Privasi-Privy-Final-Update-Repository-April-2022.pdf. [Accessed 24 Mei 2022].

[10] PT Privy Identitas Digital, "Tata Cara Pengelolaan Sertifikat (Certification Practice Statement)," 19 November 2021. [Online]. Available: https://repository.privy.id/doc/CPS-PrivyID-v2.1.pdf. [Accessed 25 Mei 2022].

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 26 April 2021



Wita Dewisari Tasya (18218037)