# Meninjau Keamanan Penyelenggara Sertifikasi Digital Mekari eSign: PT Tilaka Nusa Teknologi

Abraham Manuel Hotasi B. 18219083 (*Author*)
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 18219083@std.stei.itb.ac.id

***Abstract*—Menurut Pasal 1 Peraturan Direktur Jenderal Pajak Nomor PER-04/PJ/2020, sertifikat elektronik atau digital adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Sejak 2018, Kementrian Komunikasi dan Informatika Indonesia (KOMINFO) telah menetapkan peraturan untuk mengenai penyelenggaraan dan tata kelola sertifikat elektronik mengingat pesatnya perkembangan teknologi dan kolaborasi yang membutuhkan keamanan digital yang lebih baik. Saat ini, terdapat 9 Penyelenggara Sertifikasi Elektronik (PSrE) yang diakui oleh Kominfo, salah satunya adalah PT. Tilaka Nusa Teknologi yang merupakan penyedia layanan bagi Mekari eSign (PT Mekari Identitas Digital), salah satu penyedia tanda tangan elektronik di Indonesia. Pada makalah ini, akan dianalisis keamanan PT. Tilaka Nusa Teknologi sebagai PSrE Emelalui profil, *repository*, kebijakan privasi, dan tata kelola sertifikat digital. Hasil analisis dari makalah ini adalah PT. Tilaka Nusa Teknologi memiliki tingkat keamanan yang cukup baik sebagai sebuah PSrE.**

***Keywords—PSrE; Mekari eSign; Sertifikat digital; Kriptografi; certification authority; kebijakan privasi; penyelenggara sertifikasi digital; Certification pratice statement***

## I. PENDAHULUAN

Sertifikat digital memiliki peran penting dalam menjaga keamanan dan keabsahan transaksi elektronik. Sertifikat digital adalah dokumen elektronik yang digunakan untuk mengidentifikasi dan memverifikasi identitas pemilik kunci publik. Sertifikat digital menggunakan teknik kriptografi untuk melindungi informasi yang terkandung di dalamnya. Dalam sertifikat digital, kunci publik dan kunci privat digunakan untuk memastikan keaslian dan kerahasiaan informasi yang ditransmisikan. Kunci publik digunakan untuk mengenkripsi data, sementara kunci privat digunakan untuk mendekripsinya. Proses ini memastikan bahwa hanya pihak yang memiliki kunci privat yang sah yang dapat mengakses dan memverifikasi informasi yang terkandung dalam sertifikat digital.

Di Indonesia, Penyelenggara Sertifikasi Elektronik (PSrE) memainkan peran sentral dalam penerbitan dan manajemen sertifikat digital. PSrE adalah entitas yang dipercaya untuk mengeluarkan, mengelola, dan mencabut sertifikat digital. Mereka bertindak sebagai pihak yang independen dan netral yang melakukan verifikasi identitas pemilik sertifikat sebelum mengeluarkan sertifikat digital kepada pengguna. PSrE juga menggunakan teknik kriptografi yang kuat dalam proses pembuatan sertifikat, termasuk pembuatan pasangan kunci publik dan pribadi yang berkaitan dengan sertifikat. Selain itu, PSrE bertanggung jawab untuk mengawasi pembaruan, pencabutan, dan penggantian sertifikat digital yang telah berakhir atau terjadi masalah keamanan. Pada makalah ini, akan dianalisis salah satu PSrE yang diakui oleh Pemerintah Indonesia di bawah Kementrian Komunikasi dan Informatika Indonesia, yaitu PT Tilaka Nusa Teknologi yang juga merupakan penyedia layanan untuk Mekari eSign, sebuah aplikasi yang menyediakan layanan *end-to-end* manajemen tanda tangan elektronik.

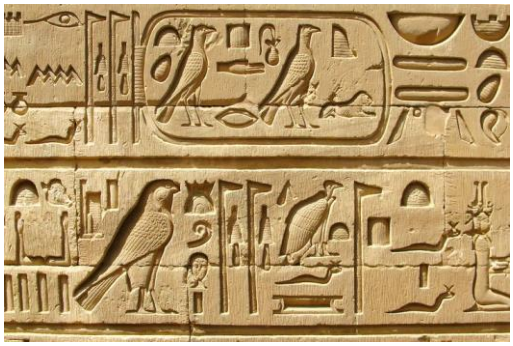
## II. STUDI LITERATUR

### *A.* Tanda Tangan

Sebuah tanda tangan (*signature*) adalah sebuah gambaran yang ditulis oleh tangan dari nama atau panggilan seseorang, atau bahkan simbol ”X” atau simbol lainnya yang seseorang tulis, cap, atau goreskan pada suatu dokumen atau surat sehingga menjadi bukti identitas orang tersebut [5]. Bahkan di beberapa negara, orang yang buta huruf dapat membubuhkan cap jembol pada dokumen resmi sebagai pengganti tanda tangan tertulis.

Gambar 1. Tanda tangan John Hancock (sumber: https://upload.wikimedia.org/wikipedia/commons/thumb/d/d5/JohnHancocksSignature.svg/1280px-JohnHancocksSignature.svg.png)

Pada zaman dahulu, tanda tangan basah lebih banyak digunakan oleh bangsawan dan kaum elit dengan memakai simbol khas sebagai cap tanda identitas tanda tangan mereka. Contohnya, pada zaman Mesir kuno, orang-orang di sana memakai simbol gambar dan piktograf sebagai identitas untuk kertas dan tablet batu. Tetapi, tanda tangan mulai berkembang pesat dan diterapkan luas ketika pendidikan dan tingkat literasi masyarakat semakin berkembang karena setiap individu sudah mempunyai kemampuan untuk menulis dan membaca. Hal ini menyebabkan tanda tangan pada surat resmi atau dokumen menjadi hal yang lumrah.



Gambar 2. Hieroglif mesir (sumber: https://asset.kompas.com/crops/-2p5x7ajZZiaYsAOZyFatHLdd90=/0x0:1548x1032/750x500/data/photo/2021/04/16/60795c8edca30.jpg)

Secara tradisional, fungsi tanda tangan adalah untuk membubuhkan identitas pribadi unik seseorang secara permanen dan menjadi bukti fisik seseorang yang tidak dapat disangkal sebagai pengesahan isi atau bagian tertentu dari sebuah dokumen cetak.

Tanda tangan mempunyai karakteristik sebagai berikut: 1) Tanda tangan adalah bukti yang otentik; 2) Tanda tangan tidak dapat dilupakan; 3) Tanda tangan tidak dapat dipindah untuk digunakan ulang; 4) Dokumen yang telah ditandatangani tidak dapat diubah; 5) Tanda tangan tidak dapat disangkal [5].

Tanda tangan tradisional memiliki beberapa kelebihan, seperti: 1) Dapat dilakukan tanpa listrik atau internet; 2) Unik bagi setiap individu; 3) Mengharuskan penandatangan bertemu dengan pihak lainnya sehingga tanda tangan dapat dikonfirmasi kebenarannya; 4) Bisa diwakilkan melalui surat kuasa; 5) Mudah untuk dilakukan berbagai kalangan usia dan latar belakang [5].

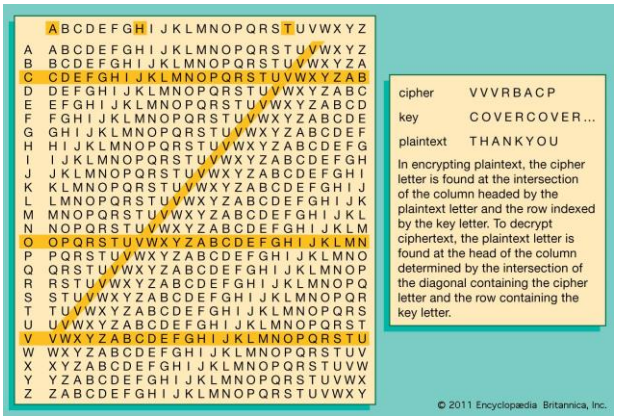
Kendati demikian, terdapat pula beberapa kekurangan: 1) Mengharuskan penandatangan bertemu dengan pihak lain, yang menjadi sulit jika terjadi pandemi, bencana alam, dan sebagainya; 2) Rawan untuk dipalsukan dan ditiru; 3) Membutuhkan media fisik, baik dalam selembar kertas, dokumen, dan sejenisnya [5].

*B.* Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan, integritas data, dan otentikasi [1]. Kata kriptografi berasal dari bahasa Yunani ”cryptós” yang artinya tersembunyi atau rahasia dan ”gráphein” yang artinya tulisan sehingga arti kriptografi adalah tulisan tersembunyi atau rahasia. Secara umum, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan [2]**.**

Terdapat 4 layanan kriptografi: 1) Kerahasiaan pesan (*confidentiality/secrecy*); 2) Keaslian pesan (data integrity); 3) Keaslian pengirim dan penerima pesan (*authentication*); 4) Anti penyangkalan (*non-repudiation*) [20].

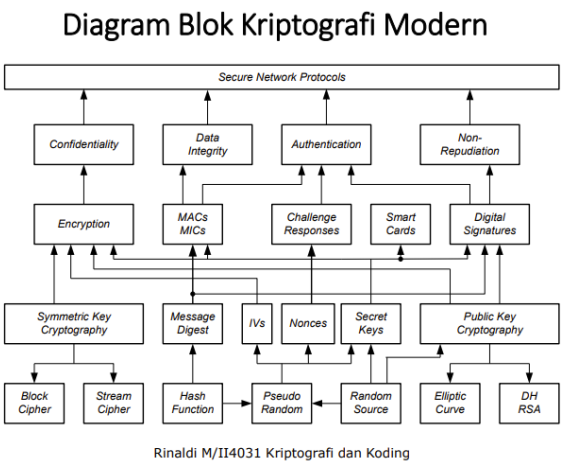
Kriptografi sendiri sudah ada sejak awal peradaban manusia di bumi dan secara historis diasosiasikan dengan aktivitas pemerintahan dan militer. Kriptografi klasik (sebelum ditemukannya komputer digital) hanya mengenkripsi huruf dan angka menggunakan kertas dan pena saja, tetapi semua *cipher*-nya sudah kadaluarsa dan tidak aman karena telah berhasil dikriptanalisis. Salah satu contoh kriptografi klasik adalah Vigenere *cipher* yang terkenal pada zaman renaisans hingga abad 19 dan dipublikasikan oleh diplomat Perancis bernama Blaise de Vigenere pada tahun 1586 [20].




Gambar 3. Vigenere *cipher* (sumber: https://cdn.britannica.com/50/7850-050-219843C0/letter-plaintext-table-Vigenere-cipher-intersection-row.jpg)

Terdapat 3 jenis algoritma kriptografi, yaitu: 1) *Symmetric-key cryptograhy*; 2) *Asymmetric-key cryptograhy*; 3) Fungsi *hash*. Kriptografi klasik termasuk dalam jenis kriptografi kunci-simetri dan biasanya disusun oleh dua teknik dasar yaitu teknik substitusi (mengganti huruf plainteks dengan huruf cipherteks) dan transposisi (mengubah susunan atau posisi huruf plainteks menjadi susunan huruf cipherteks). Kombinasi kedua Teknik tersebut membentuk *product cipher* atau superenkripsi. [12]

Setelah ditemukannya penggunaan komputer digital untuk keamanan pesan, algoritma kriptografi modern mengalami perkembangan yang pesat. Komputer digital yang merepresentasikan data dalam bentuk biner mengakibatkan kriptografi modern beroperasi dalam mode bit atau *byte* untuk mengamankan informasi. Walaupun demikian, kriptografi modern tetap menggunakan teknik algoritma klasik: substitusi dan transposisi, tetapi lebih kompleks agar sangat sulit untuk dikriptanalisis. [12]




Gambar 4. Diagram kriptografi modern (sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/4%20-%20Kripto-modern-2021.pdf)

*C.* Tanda Tangan Elektronik (TTE)

Tanda tangan elektronik (TTE) adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Berdasarkan Pasal 60 Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, terdapat 2 jenis TTE: Tersertifikasi dan Tidak Tersertifikasi. [6]

Tanda tangan elektronik Tersertifikasi adalah TTE yang dibuah oleh jasa Penyelenggara Sertifikasi Elektronik (PSrE), baik dari pemerintah maupun swasta. Menurut Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2008 (UU ITE), PSrE adalah badan hukum yang berfungsi sebagai pihak yang dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.

Selain itu, kekuatan hukum *e-signature* sah dan tertera juga pada UU ITE. Pada UU ITE, tercantum beberapa syarat sah dari *e-siganture*, yaitu: 1) Data pembuatan tanda tangan hanya diketahui pemiliki tanda tangan; 2) Hanya pemilik tanda tangan yang berhak menggunakan TTE; 3) Seluruh perubahan terkait informasi elektronik yang terjadi setelah pembuatan tanda tangan dapat diketahui; 4) Terdapat suatu cara untuk mengetahui pemilik tanda tangan tersebut. Selain pada UU ITE, legalitas *e-signature* juga diatur dalam PP No. 71 Tahun 2019.

TTE Tersertifikasi dapat dicek keasliannya melalui wesbite Kementrian Komunikasi dan Informatika yang nantinya akan muncul informasi penandatanganan yang diambil dari Direktorat Jenderal Kependudukan dan Pencatatan Sipil sehingga memiliki kekuatan hukum. TTE Tersertifikasi dienkripsi dengan kunci privat dan hanya bisa dibuka oleh kunci publik serta berupa barisan kode acak. Kemudian, Sertifikat TTE, kunci publik, dan cipherteks dilekatkan ke dokumen tersebut. Bila cipherteks di kunci publik dan cipherteks di dokumen sama, maka dokumen persis sama dan tidak ada perubahan atau berintegritas. Maka dari itu, TTE Tersertifikasi membuat seseorang tidak bisa menyangkal bila ada dokumenn yang terkirim atas namanya.

Sebaliknya, TTE Tidak Tersertifikasi tidak melibatkan PSrE atau Kementrian Komunikasi dan Informatika, tetapi biasanya memiliki sertifikat Adobe Approved Trust List (AATL) dengan validasi identitas melalui alamat *email* pribadi dan bukan Direktorat Jenderal Kependudukan dan Pencatatan Sipil. Tetapi, tidak semua aplikasi tanda tangan *online* menyediakan sertifikat AATL dan seringkali tanpa sertifikat sama sekali. TTE Tidak Tersertifikasi tidak menggunakan *e-Know Your Customer* (KYC) ataupun algoritma kriptografi.

Terdapat beberapa fungsi TTE, yaitu: 1) Dapat membuktikan keaslian dan keabsahan dokumen digital; 2) Memperkuat keamanan dokumen karena *e-signature* sulit dipalsukan; 3) Mempercepat proses tanda tangan; 4) Mempermudah proses tanda tangan jarak jauh dengan berbagai pihak; 5) Mempersingkat proses pengambilan keputusan; 6) Meningkatkan produktivitas; 7) Mengurangi risiko kerusakan dokumen; 8) Menghemat pengeluaran. Berikut tabel perbedaan TTE Tersertifikasi dan Tidak Tersertifikasi.

TABLE I. PERBEDAAN TTE TERSERTIFIKASI DAN TIDAK TERSEERTIFIKASI [6]

| **Perbedaan** | **TTE Tersertifikasi** | **TTE Tidak Tersertifikasi** |
|---|---|---|
| Bentuk | Terdapat algoritma kriptografi dalam pembuatan sehingga tidak sama dengan tanda tangan basah | Data dalam bentuk elektronik yang terlekat pada suatu dokumen elektronik dan bentuknya tidak terbatas |
| Proses pembuatan | Menggunakan algoritma kriptografi asimetris dan proses e-KYC | Proses pembuatan menggunakan *scan* tanda tangan dari kertas |
| Kekuatan hukum | Dasar hukum tertulis di UU 11/2008 tentang informasi dan transaksi elektronik (UU ITE) dan kekuatan hukum dijelaskan di pasal 52 ayat 2 PP nomor 82/2012 | Tidak disebutkan pada pasal 54 ayat 1 yang menjelaskan tentang asal usul TTE |
| Fungsi | Identifikasi lebih akurat dan terpercaya pada dokumen penting (perjanjian | Digunakan untuk identifikasi data yang tidak memerlukan kekuatan hukum |

| | | |
|---|---|---|
| | kerjasama, kontrak elektronik, dan lainnya) | |

Dari penjelasan sebelumnya, dapat disimpulkan bahwa TTE Tersertifikasi mempunyai pembuktian yang kuat di mata hukum, validasi pengguna yang tepercaya sehingga sulit dimanipulasi, jaminan keamanan dengan algoritma kriptografi.

*D.* Sertifikat Digital di Indonesia

*Public key certificate* atau sertifikat digital adalah dokumen dalam bentuk elektronik yang digunakan untuk membuktikan kepemilikan sebuah perangkat menggunakan *public key*. Kunci publik yang tersedia secara publik perlu disertifikasi dengan memberikan sertifikat digital agar kunci publik dapat diidentifikasi pemiliknya dengan tepat. *Certification authority* atau CA adalah pemegang otoritas sertifikasi yang mengeluarkan sertifikat digital dan sertifikat digital juga ditandatangani oleh CA. Terdapat 4 informasi minimal dalam sertifikat digital: 1) Identitas subjek (perusahaan/individu pemilik kunci publik); 2) Kunci publik subjek; 3) Nama CA (*issuer*); 4) Tanda tangan CA (*issuer*). Nomor seri sertifikat dan waktu kadaluarsa juga dapat ditambahkan.

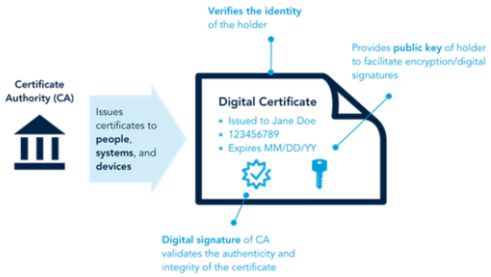
Agar setifikat digital dapat diverifikasi kebenarannya, maka kunci publik CA juga harus diketahui secara luas. Dengan mengetahui kunci publik CA, seseorang dapat memverifikasi tanda tangan digital dalam sertifikat. Sertifikat digital juga dapat dilihat secara publik dan tersimpan pada *certificacte repositories* CA.

X.509 adalah standard sertifikat digital agar semua sertifikat digital yang dikeluarkan oleh berbagai CA seragam. Terdapat tiga versi standard X.509: V1, V2, dan V3. Berikut *field* utama di dalam sertifikat digital standard X.509.

| *Field* | Arti |
|---|---|
| *Version* | Versi X.509 |
| *Serial Number* | Nomor ini plus nama CA secara unik digunakan untuk mengidentifikasi sertifikat |
| *Certificate Signature Algorithm* | Algoritma yang digunakan untuk tanda-tangan digital. Contoh: MD5RSA, SHA1RSA |
| *Issuer* | Nama CA yang mengeluarkan sertifikat digital. Biasanya nama domain. |
| *Validity period* | Waktu awal dan akhir periode valid |
| *Subject name* | Entitas (individu atau organisasi) yang disertifikasi |
| *Subject Public Key Info* | Kunci publik subjek dan algoritma kriptografi kunci-publik yang digunakan (misalnya RSA). |
| *Issuer ID* | ID opsional yang secara unik mengidentifikasi certificate's issuer. |
| *Subject ID* | ID opsional yang secara unik mengidentifikasi certificate's subject |
| *Extensions* | Banyak ekstensi yang telah didefinisikan (opsional). |
| *Signature* | Tanda-tangan digital (ditandatangani dengan kunci privat CA). |
| *Signature algorithm* | Algoritma tanda-tangan digital yang digunakan. |

Gambar 5. *Field* utama standard sertifikat digital X.509 (https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/18-Sertifikat-digital-2023.pdf)

Dengan adanya waktu kadaluarsa pada sertifikat digital, pemilik harus mengubah kunci publik dan kunci privat secacra periodik sehingga lebih sulit dikriptanalisis. Ketika pasangan kunci diubah, sertifikat digital yang lama harus ditarik kembali dan diganti dengan yang baru. CA memberitahu ke publik bahwa sertifikat digital ditarik dengan mengeluarkan *certificate revocation list* (CRL) secara periodik yang berisi nomor seri sertifikat digital yang ditarik. Sertifikat digital yang sudah kadaluarsa (yang secara otomatis dianggap tidak sah) juga akan dimasukkan ke dalam CRL. [21]




Gambar 6. Sertifikat digital (sumber: https://id4d.worldbank.org/sites/id4d-ms8.extcc.com/files/inline-images/18%20digital%20certificates.png)

Di Indonesia, CA yang berperan dalam menerbitkan dan menandatangani sertifikat digital untuk membuktikan keasliannya serta memeriksa masa kadaluarsanya adalah PsrE INDUK. PSrE INDUK merupakan singkatan dari Penyelenggara Sertifikat Elektronik Induk atau *Certification Authority* (CA dan dikelola Direktorat Pengendalian Aptika, Kementerian Kominfo sebagai Penyelenggara Sertifikat Elektronik Induk atau Root CA.

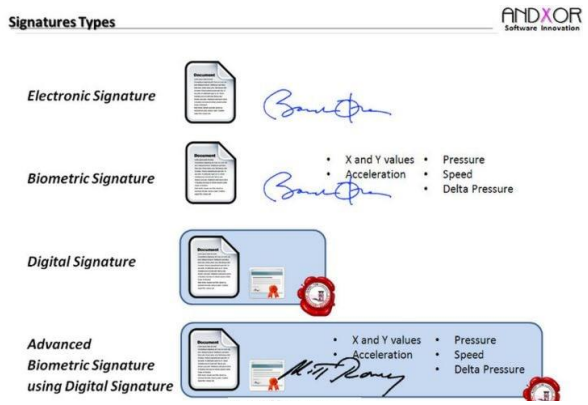
*E.* Tanda Tangan Digital

Tanda tangan digital (digital *signature*) adalah sebuah *e-signature* yang dilengkapi dengan sebuah sertifikat digital (*digital certificate*). Dalam kriptografi, tanda tangan digital tidak sama dengan *digitized signature* yang merupakan tanda tangan dengan cara dipindai atau difoto. Tanda tangan digital berbeda-beda untuk satu pesan dengan lainnya sedangkan tanda tangan seseorang pada dokumen cetak selalu sama. [20]

*Digital signature* aman karena dilengkapi dengan sertifikat digital yang memberikan bukti identitas seseorang. Ketika menggunakan sertifikat digital yang diperoleh dari pihak yang tepercaya, tanda tangan digital yang dihasilkan hampir tidak mungkin dipalsukan karena sertifikat digital tersebut memberikan bukti penanda tangan yang kuat bahwa dokumen yang ditandangani tidak diubah dan tanda tangan tersebut sah.

Pada tanda tangan digital, terdapat 2 proses penting: 1) *Signing*; 2) *Verification*. *Signing* berarti menandatangani pesan dan *verification* berarti memeriksa keabsahan tanda tangan. Dalam menandatangani pesan, dapat dilakukan dengan 2 cara, yaitu mengenkripsi pesan untuk pesan rahasia dan

menggunakan kombinasi fungsi *hash* dan kriptografi kunci-publik untuk pesan yang tidak terlalu rahasia.




Gambar 7. Tanda tangan digital (sumber: https://kominfo.ponorogo.go.id/wp-content/uploads/2019/09/contoh-tanda-tangan-elektronik.jpg)

*F.* Mekari E-Sign

Gambar 8. Logo Mekari eSign (sumber: https://mekarisign.com/wp-content/uploads/2022/10/Mekari-eSign-New-Logo-scaled.webp)

Mekari eSign (PT Mekari Identitas Digital) adalah penyedia layanan Tanda Tangan Elektronik Tersertifikasi yang bermitra dengan PT Tilaka Nusa Teknologi sebagai *Certificate Authority* (CA) dari Kementerian Komunikasi dan Informatika Indonesia. Mekari eSign menyediakan layanan solusi *end-to-end* yang mempermudah proses penandatanganan dan manajemen dokumen menjadi lebih praktis dan efisien. [14]

Mekari eSign memiliki beberapa fitur utama, yaitu: 1) *Dashboard*; 2) Sistem penyimpanan *cloud*; 3) Mendukung beragam format dokumen. Sampai saat ini, lebih dari 35.000+ perusahaan di berbagai industri menggunakan produk Mekari.

Dengan menggunakan Mekari eSign, pengguna dapat: 1) Mempersingkat biaya dan proses administrasi; 2) Mendapat laporan progress pengesahan dokumen secara *real-time*; 3) Memperkuat kolaborasi antar tim dengan pengingat otomatis. Maka dari itu, pengguna dapat mendapatkan tanda tangan banyak pihak dalam hitungan menit dan dapat memvalidasi serta mengirim dokumen secara massal. [14]

eSign dapat dilakukan dalam 4 langkah: 1) Pengguna mendaftar dan melengkapi e-KYC; 2) Pengguna mengunggah berkas dan menentukan pihak penandatangan; 3) Menambahkan dan mengatur *e-signature* pengguna; 4) Mengirim dokumen melalui *email* ke pihak terkait. [14]

## III. METODOLOGI PENELITIAN

*A.* Batasan penelitian

Analisis keamanan Mekari eSign hanya dilakukan dengan menggunakan data sekunder yang didapat dari *repository* PT Tilaka Nusa Teknologi dan Mekari eSign. Tidak dilakukan percobaan tertentu untuk menguji keamanan.

*B.* Sumber dan teknik pengumpulan data

Data yang digunakan adalah data resmi dari Kementrian Komunikasi dan Informatika, Mekari eSign, PT Tilaka Nusa Teknologi, dan sumber relevan lainnya yang berasal dari situs resmi.

## IV. PEMBAHASAN

*A.* PT. Tilaka Nusa Teknologi

PT Tilaka Nusa Teknologi berdiri pada tahun 2019 dan berperan bagi kebutuhan bisnis di berbagai industri terkait legalitas dan keamanan data pada dunia digital.

Gambar 9. Logo PT Tilaka Nusa Teknologi (sumber: https://tilaka.id/wp-content/uploads/2022/11/logo-3.png)

Diambil dari situs PSrE Kominfo, berikut profil PT Tilaka Nusa Teknologi.

TABLE II. INFO DETAIL PT. TILAKA NUSA TEKNOLOGI [11]

| | |
|---|---|
| Nama perusahaan | PT Tilaka Nusa Teknologi |
| No SK Pengakuan | Nomor 423 tahun 2021 |
| Alamat website | https://tilaka.id/ |
| Penanggung jawab | Muammar |
| No Telepon | (021) 57940988 |
| Jenis PSrE | PSrE Non-Instansi |
| Status Pengakuan | BERINDUK |
| Riwayat pengakuan | 10-09-2021 |
| Masa berlaku | 10-09-2021 s.d 10-09-2024 |

PT Tilaka Nusa Teknologi saat ini memiliki 5 fitur kunci [18]:
1. Identity *proofing*: layanan untuk memastikan bahwa pengguna adalah pemilik sah dari data dengan cara menggunakan *biometric face recognition*, baik untuk autentikasi maupun otorisasi.
2. Tilaka ID: 13 digit digital ID yang akan otomatis ter-*generate* setiap ada proses pendaftaran pengguna baru maupun proses e-KYC yang mengadopsi standard *world bank*.
3. Tilaka sign: layanan tanda tangan elektronik tersertifikasi, yang mengikuti standar KOMINFO. Tilaka *sign* terdiri dari tiga

layanan: 1) SaaS (*software as a service*) bagi pengguna personal atau perusahaan yang tidak memerlukan integrasi rumit dan solusi siap pakai; 2) API, sehingga perusahaan dapat mengintegrasikan kebutuhan mereka; 3) *On premise*, perusahaan dapat menggunakan layanan Tilaka tanpa perlu *traffic* dokumen ke Tilaka.
4. Tilaka *verify*: layanan validasi data menggunakan user consent dan authorization sehingga *third-party* dapat melakukan verifikasi data, dan pengguna akan diminta consent mengenai data apa yang bisa diberikan akses, dan pengguna akan melakukan otorisasi terhadap request akses tersebut.
5. Tilaka API: layanan yang mencakup semua *service* tilaka, antara lain, registrasi, e-KYC, *manual verification*, tandatangan elektronik tersertifikasi, dan digital ID yang dapat di kustomisasi sesuai kebutuhan partner.

Berdasarkan PP Nomor 82/2012, PT Tilaka Nusa Teknologi adalah PSrE Berinduk Non-Instansi yang berarti CA telah diakui oleh PSrE Induk, yaitu Pemerintah Indonesia, di bawah KOMINFO. Selain itu, PT Tilaka Nusa Teknologi bekerjasama dan telah mendapat pengakuan dari lembaga resmi, seperti:
1. Tersertifikasi ISO/IEC 27001:2013
2. Sub CA Kominfo SK No 423 tahun 2021
3. PKS Dukcapil No 119/6569/Dukcapil
4. Tercatat di OJK
5. Anggota dari AFTECH
6. Anggota dari KADIN

*B.* PSrE Non-Instansi

PSrE yang beroperasi di Indonesia wajib mendapatkan pengakuan Menteri Kominfo ke PSrE Induk. Berdaasarkan situs resmi Kominfo, berikut persayaratan untuk menjadi PSrE Non-Instansi.[10]
1. Surat Permohonan Pengakuan Status Berinduk
2. Proposal Penyelenggara Sertifikat Elektronik
3. Dokumen Tanda Daftar Penyelenggara Sertifikat Elektronik
4. Akte Pendirian Perusahaan
5. Surat Izin Usaha, Bidang Teknologi Informasi
6. Surat Pernyataan Fasilitas dan Peralatan di Indonesia
7. Prosedur Pengoperasian Fasilitas dan Peralatan
8. Interoperabilitas Mengacu Pada Standar Kominfo
9. Salinan Bukti Laporan Sertifikasi Atas Audit Terhadap Standar Fasilitas dan Peralatan
10. Dokumen Rencana Bisnis, Rencana Keberlangsungan Bisnis, Rencana Penanggulangan Bencana dan Dokumen Laporan Pengujian Sistem Elektronik
11. CP/CPS sesuai dengan CP/CPS PSrE Induk
12. Salinan Sertifikat Kelaikan Sistem Elektronik
13. Tidak Berinduk dan Tidak Menjadi Induk pada PSrE lain
14. Memiliki 12 Orang Ahli Operasional
15. Jaminan kerugian Pemilik Sertifikat Elektronik
16. Modal Rp 30 Miliar
17. Pakta Integritas dan Rekam Jejak
18. Surat Keterangan Non Pailit

Karena PT Tilaka Nusa Teknologi telah memenuhi kedelapanbelas persyaratan di atas, PT Tilaka Nusa Teknologi dinyatakan sebagai PSrE Non-Instansi.

*C.* Analisis Keamanan Penyelenggara Sertifikasi Elektronik Indonesia: PT Tilaka Nusa Teknologi

Akan ditinjau keamanan Penyelenggara Sertifikasi Elektronik, PT Tilaka Nusa Teknologi, melalui 3 aspek: kebijakan privasi, Root CA, dan *certificate practice statement* (CPS).

1. Kebijakan Privasi

Kebijakan privasi yang dibahas adalah ketentuan mengenai cara Tilaka memperoleh, mengumpulkan, mengolah, menyimpan, menampilkan, mengumumkan, mengirimkan, dan memusnahkan data pribadi Pemilik Layanan Tanda Tangan Elektronik Tilaka.

Peraturan yang diatur dalam kebijakan tunduk terhadap ketentuan dan peraturan perundang-undangan yang berlaku, termasuk Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika nomor 11 tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik, Peraturan Menteri Komunikasi dan Informatika nomor 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, dan Certificate Policy PSrE Induk. [22]

Berdasarkan Kebijakan Privasi yang efektif pada tanggal 20 Oktober 2022, Tilaka memperoleh dan mengumpulkan Data Pribadi berikut, yaitu permohonan penerbitan, pencabutan, dan/atau penerbitan ulang Sertifikat Pemilik, pengajuan perubahan data pada Sertifikat, riwayat menghubungi dan/atau dihubungi oleh Tilaka, penggunaan layanan Tanda Tangan Elektronik Tilaka [22].

Selain itu, Tilaka juga mengklaim bahwa Data Pribadi yang diperoleh dan dikumpulkan saat menggunakan layanan atau mengajukan permohonan penerbitan, perubahan, atau pencabutan Sertifikat adalah nama, Nomor Induk Kependudukan (NIK), salinan dokumen e-KTP, data biometrik berupa swafoto yang telah teruji menggunakan mekanisme *liveness detection*, dan alamat *email*. Saat menghubungi Tilaka, data yang diperoleh adalah alamat *email*, nomor telepon, dan informasi yang berkaitan dengan laporan, keluhan dan/atau permohonan. Terakhir, ketika menggunakan layanan, data berikut akan diperoleh: IP *Address*, *login information*, *browser client* & *version*, *timestamp of activities*, dan data transaksi yang berkaitan dengan penggunaan Layanan Tanda Tangan Elektronik Tilaka. [22]

Berdasarkan dokumen kebijakan privasi Tilaka, Data Pribadi yang tadi diperoleh dan dikumpulkan akan digunakan untuk menerbitkan, mencabut, dan/atau menerbitkan ulang Sertifikat Pemilik; Menyediakan dan memperbaiki Layanan Tanda Tangan Elektronik Tilaka; Mengirimkan informasi tentang produk dan/atau layanan yang dibuat dan dikembangkan;

Mengirimkan informasi kegagalan perlindungan Data Pribadi Anda melalui email; Mengirimkan instruksi terkait *compromise* atau penyalahgunaan Sertifikat Pemilik; Melakukan publikasi *Certificate Revocation List* ("CRL"); Mengirimkan informasi perubahan Dokumen Publik; Membantu penegakan hukum berdasarkan perintah dari pengadilan atau Aparat Penegak Hukum sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. [22]

Tilaka juga menyatakan bahwa berkaitan dengan pihak ketiga, terdapat beberapa pihak ketiga dapat memperoleh beberapa Data Pribadi pengguna yang diperoleh atau dikumpulkan oleh Tilaka seperti: penyelenggara jasa sistem pembayaran, auditor, advokat, dan/atau konsultan yang ditunjuk, telah mendapat izin, dan telah menandatangani *Non-Disclosure Agreement* (NDA) dengan Tilaka [22].

Pun jika Tilaka membagi Data Pribadi pengguna, Tilaka menjamin bahwa pihak ketiga hanya akan: Melihat Data Pribadi hanya di tempat Tilaka dan dilarang untuk memindahkannya; Menggunakan Data Pribadi sesuai dengan ketentuan yang telah disepakati sebelumnya; Menghancurkan atau mengembalikan Data Pribadi setelah tidak ada kebutuhan lagi. [22]

Tilaka juga telah memperoleh sertifikasi ISO 27001:2013 untuk Sistem Keamanan Manajemen Informasi sebagai bukti komitmen pengolahan dan penyimpanan yang aman di dalam database Tilaka. [22]

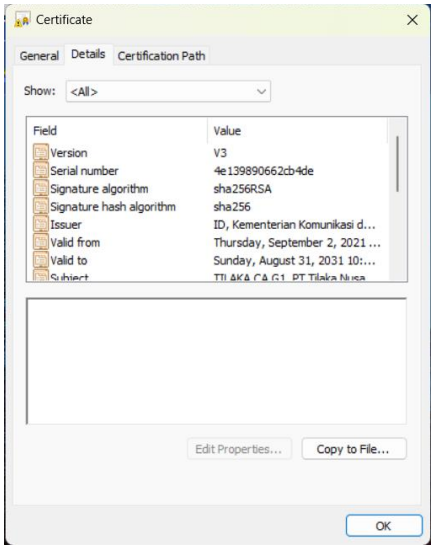
Terkait Data Pribadi yang disimpan, Tilaka juga menjamin bawha data hanya akan disimpan jika sertifikat pemilik masih dalam masa berlaku atau ketika permohonan penerbitan Sertifikat Pemilik ditolak. Ketika jangka waktu berlaku Sertifikat Pemilik sudah melewati masa berlaku, maka Tilaka akan menyimpan Data Pribadi pengguna selama 5 tahun sejak tanggal penolakan penerbitan Sertifikat Pemilik atau sejak jangka waktu berlaku Sertifikat Pemilik habis. Setelah masa berlaku habis atau terdapat permohonan penghapusan Data Pribadi, maka Data Pribadi akan dihapus untuk mencegah penyalahgunaan atau akses yang tidak sah. [22]

2. Root CA

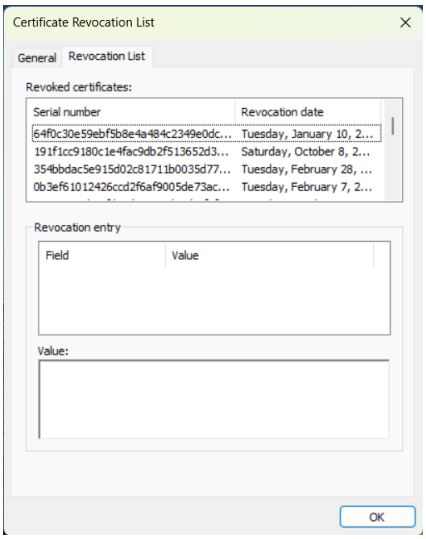
Berdasarkan daftar Root CA pada situs KOMINFO, Tilaka hanya memiliki 1 Root CA yang menggunakan *fingerprint* yang dienkripsi dengan fungsi *hash* SHA-1 dan dapat diunduh [13]. Kunci publik Tilaka dienkripsi menggunakan algoritma RSA (4096 bit). Pada *repository* Tilaka (terpisah dengan pranala menuju Root CA di situs KOMINFO), terdapat *certification Revocation List* (CRL) yang dapat diunduh dan berisi sertifikat yang sudah tidak terdaftar pada Root CA, entah karena masa berlaku yang kadaluarsa atau karena permohonan penerbitan ulang Sertifikat. Root CA PSrE akan kadaluarsa pada tahun 2031.


Gambar 10. Root CA Tilaka (sumber: https://www.rootca.id/)


Gambar 11. Sertifikat PEM Tilaka (sumber: dokumentasi pribadi)




Gambar 12. Tampilan sertifikat TILAKA CA G1 (sumber: dokumentasi pribadi)



Gambar 13. Tampilan CRL Tilaka (sumber: dokumentasi pribadi)

3. Certification Practice Statement (CPS)

*Certification practice statement* (CPS) adalah persyaratan procedural dan operasional yang dianut oleh Tilaka saat menerbitkan dan mengelola objek yang ditandatangani secara elektronik dalam lingkungan *Public Key Infrastructure* Indonesia. [3]

CPS Tilaka mengacu pada ketentuan *Certificate Policy* (CP) PSrE Induk dan sesuai dengan standar *Request for Comments* 3647 (RFC 3647) dari *Internet Engineering Task Force* (IETF) tentang Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework*. [3]

Tilaka menjamin akan bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat, termasuk dalam proses: 1) Pengendalian proses pendaftaran; 2) Verifikasi dan Validasi; 3) Penerbitan Sertifikat; 4) Publikasi Sertifikat; 5) Validasi Sertifikat; 6) Pencabutan Sertifikat; dan 7) Memastikan seluruh aspek layanan, operasional, dan infrastruktur dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan CPS.

Berdasarkan CPS, penggunaan sertifikat pemilik dibatas sesuai *key usage* dan *extended key usage* pada *certificate extension*. Maka dari itu, sertifikat dari Tilaka dapat digunakan untuk menerbitkan sertifikat pemilik untuk transaksi yang memerlukan *digital signature* dan *non-repudiation*. Tilaka hanya menyediakan sertifikat pemlik dengan level verifikasi identitas level 4 dengan tingkat jaminan tinggi dan memerlukan vertifikasi identitas sesuai e-KTP dan swafoto pemohon.

Sertifikat yang dibuat dan ditandatangani oleh Tilaka menggunakan subyek *distinguished name* (DN) yang *non-null* sesuai standar X.509.

TABLE III. TIPE SERTIFIKAT TILAKA [3]

| Tipe sertifikat | *Distinguished Name* (DN) |
|---|---|
| Sertifikat Tilaka | cn=TILAKA CA G1, o=PT Tilaka Nusa Teknologi, c=ID |
| Sertifikat Pemilik | Untuk Pelanggan Korporasi:<br>cn=<nama lengkap Pemilik>, o=<nama perusahaan>, c=ID, e=<email><br><br>Untuk Pelanggan Personal:<br>cn=<nama lengkap Pemilik>, o=Personal, c=ID, e=<email> |

Untuk sertifikat pemilik, pasangan kunci dibangkitkan menggunakan modul kriptografi yang memenuhi persyaratan FIPS 140-2 level 3 dan hanya dapat diakses oleh Pemilik dengan minimal 2 faktor autentikasi berupa *username*, *password*, dan *one-time password* (OTP), *personal identification number* (PIN), atau data biometrik lainnya yang memenuhi unsur "*what you are".* Tilaka juga menjamin akan melindungi kunci privat pemilik dengan *hardware security module* (HSM). [3]

Terdapat beberapa skenario agar Tilaka mencabut dan membekukan sertifikat pemilik, yaitu permohonan pencabutan Sertifikat Pemilik oleh Pemilik atau Aparat Penegak Hukum, terdapat informasi yang tidak valid pada Sertifikat Pemilik, dan terjadi kebocoran atau kerusakan Kunci Privat Pemilik. Selain itu, Tilaka juga dapat mencabut sertifikat pemilik secara sepihak jika pemilik terbukti melanggar ketentuan dalam CPS, kebijakan privasi, atau perjanjian Kerjasama, terjadi kebocoran atau kehilangan kunci privat Tilaka, atau kegiatan usaha Tilaka berenti atau dihentikan. Sertifikat pemilik yang telah dicabut dimasukan ke dalam CRL (yang akan dipublikasikan 30 menit setelah CRL diperbaharui) dan ditampilkan pada OCSP *responder* [3].

Mengenai fasilitas, manajemen, dan kendali operasional, Tilaka juga menjamin bahwa lokasi dan konstruksi dari fasilitas telah menjalani audit sistem manajemen keamanan informasi dengan menggunakan kriteria ISO/IEC 27001. [3]

Pergantian kunci juga ddilakukan oleh Tilaka secara berkala, yaitu 1 kali dalam 10 tahun untuk meminimalisir risiko kebocoran. Sejak kunci privat tersebut diubah, hanya kunci baru yang bisadigunakan untuk penandatanganan Sertifikat Pemilik. Sertifikat Tilaka lama masih berlaku, tetapi penggunaannya terbatas untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat Pemilik yang ditandatangani menggunakan Kunci Privat pada Sertifikat Tilaka lama tersebut melewati batas jangka waktu Sertifikat. Jika Kunci Privat lama Tilaka digunakan untuk menandatangani CRL, maka kunci lama disimpan dan dilindungi. Jika Tilaka memperbarui Kunci Privat, maka Tilaka akan memiliki Kunci Publik baru. [3]

Dalam kasus kunci privat hilang atau algoritma yang digunakan untuk membangkitkan kunci privat dan sertifikat pemilik bocor,

Tilaka menjamin akan mencabut seluruh sertifikat pemilik terkait dan melakukan pembangkitan pasangan kunci serta menerbitkan ulang sertifikat pemilik tanpa menghentikan layanan. Hal yang serupa dilakukan ketika ada kebocoran kunci privat Tilaka atau kunci privat dari PSrE Induk hilang atau bocor dengan tambahan: memberitahukan PSrE Induk, menghentikan layanan, memberitahukan semua pemilik, melakukan pencabutan semua sertifikat pemilik, dan menerbitkan CRL terbaru. [3]

Saat membangkitkan pasangan kunci pemilik dengan modul kriptografi yang sesuai standar FIPS 140-2 level 3, kunci privat pemilik hanya akan disimpan oleh Tilaka, tidak dititipkan kepada pihak manapun, dan tidak diserahkan ke pemilik. Penggunaan Kunci Privat oleh Pemilik dilakukan melalui Layanan Tanda Tangan Elektronik Tilaka menggunakan multifaktor autentikasi. Kemudian, Tilaka membuat pasangan kunci menggunakan algoritma RSA dan *secure hash algorithm* (SHA)-2 dengan detail:

TABLE IV. UKURAN KUNCI SERTIFIKAT [3]

| Sertifikat | *Digest algorithm* | *Encryption algorithm* | |
|---|---|---|---|
| | Tipe | Tipe | Panjang kunci |
| Tilaka | SHA-256 | RSA | 4096-bit |
| Pemilik | SHA-256 | RSA | 2048-bit |

Tujuan penggunaan kunci Tilaka adalah untuk *digital signature, key certificate sign,* dan CRL *sign*. Kunci pemilik digunakan untuk *digital signature* dan *non-repudiation*. [3]

Tilaka juga menjamin keamanan komputer dengan adanya *login* terautentikasi yang dilengkapi dengan MFA, menyediakan *role-based access control*, kapabilitas audit keamanan, memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data, dan menyediakan perlindungan mandiri untuk sistem operasi. Selain itu, semua komponen Tilaka secara berkala juga disinkronisasikan dengan *network time protocol* (NTP) untuk menentukan waktu validitas waktu permulaan sertifikat Tilaka, pencabutan sertifikat, pembaruan CRL dan OCSP, dan penerbitan sertifikat pemilik.

Berdasarkan CPS, Profil Sertifikat mengikuti standard RFC 5280 "*Internet X.509 Public Key Infrastructure*: *Certificate and Certificate Revocation List (CRL) Profile"* daan dilakukan peninjauan profil minimal satu kali dalam 1 tahun. Tilaka menerbitkan Sertifikat dengan versi X.509 v3.

TABLE V. KEY USAGE [3]

| *Field* | Sertifikat Tilaka | Sertifikat Pemilik |
|---|---|---|
| Critical | *True* | *True* |
| digitalSignature | *True* | *True* |
| nonRepudiation | *False* | *True* |
| keyEncipherment | *False* | *False* |
| dataEncipherment | *False* | *False* |
| keyAgreement | *False* | *False* |
| keyCertSign | *True* | *False* |
| cRLSign | *True* | *False* |
| encipherOnly | *False* | *False* |
| decipherOnly | *False* | *False* |

Pengidentifikasian objek algoritma, OID, menggunakan standar X.509 versi 3. Algoritma menggunakan enkripsi RSA untuk kunci subjek dan SHA256 dengan enkripsi RSA untuk tanda tangan elektronik.

rsaEncryptionOBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)
1}.
sha256withRSAEncryption OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-1(1) 11}.

Terakhir, Sertifikat Pemilik yang diterbitkan oleh Tilaka berlaku selama 1 tahun sejak diterbitkan dan akan dikirimkan pemberitahuan kepada Pemilik agar melakukan perpanjangan masa berlaku terhadap Sertifikat Pemilik miliknya 1 bulan sebelum masa berlaku Sertifikat Pemilik kadaluarsa. Pemilik juga mengklaim bahwa pemilik tidak diberikan kewenangan untuk menggunakan Sertifikat Pemilik yang telah dicabut. [3]

## V. KESIMPULAN

Dari analisis dan pemaparan mengenai masing-masing aspek keamanan padad bagian sebelumnya, PT Tilaka Nusa Teknologi dapat dikatakan *secure* dan mematuhi ketentuan privasi dan perlindungan data, serta sebagai PSrE Berinduk Non-Instansi. Terdapat 6 hal yang mendukung kesimpulan tersebut:

1) PT Tilaka Nusa Teknologi adalah PSrE Berinduk Non-Instansi yang sudah diakui oleh Pemerintah Indonesia, di bawah KOMINFO. Hal ini berarti PSrE Tilaka dapat memberikan layanan sertifikasi digital;

2) PT Tilaka Nusa Teknologi mematuhi kebijakan PSrE dan privasi data yang terdapat pada Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika nomor 11 tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik, Peraturan Menteri Komunikasi dan Informatika nomor 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik, dan *Certificate Policy* PSrE Induk.

3) PT Tilaka Nusa Teknologi menggunakan algoritma kriptografi RSA dan SHA-2 untuk pembangkitan pasangan kunci serta mempunyai CRL yang diperbaharui secara berkala.

4) PT Tilaka Nusa Teknologi menjamin keamanan sertifikasi dari sisi non-teknis (manusia) dan teknis (*software*, sistem, komputer) secara detail melalui CPS.

5) PT Tilaka Nusa Teknologi menyediakan penjelasan langkah-langkah lengkap bagaimana sertifikat dapat diterbitkan, dicabut, diterbitkan ulang, bahkan kasus jika kunci privat bocor atau PT Tilaka dihentikan.

6) PT Tilaka Nusa Teknologi menggunakan standard sertifikat digital X.509 v3 yang diakui secara internasional serta tersertifikasi ISO 27001:2013 tentang Sistem Keamanan Manajemen Informasi sebagai bentuk komitmen Tilaka.

## UCAPAN TERIMA KASIH

Penulis memanjatkan rasa syukur sebesar-besarnya terhadap Tuhan Yang Maha Esa karena telah menganugerahkan tenaga, pikiran, dan kesehatan serta penyertaan-Nya dalam menyelesaikan makalah ini. Penulis juga ingin mengucapkan terima kasih sebesar-besarnya kepada Dr. Ir. Rinaldi Munir, M. T. selaku dosen mata kuliah II4031 Kriptografi dan Koding yang telah membagikan ilmu dan pengetahuannya terkait Kriptografi selama satu semester.

## REFERENSI

Berikut sumber referensi yang digunakan dalam pembuatan makalah Kriptografi ini.

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, 2018. doi:10.1201/9780429466335

[2] B. Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C. New York: Wiley, 1996.

[3] "Certification practice statement (CPS)," https://repository.tilaka.id/CP_CPS.pdf (accessed May 20, 2023).

[4] Haekal, M. M., "Mengenal Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia," Mekari eSign, https://mekarisign.com/id/blog/apa-itu-psre/ (accessed May 20, 2023).

[5] Haekal, M. M., "Tanda Tangan Basah vs. Tanda Tangan Digital: Mana Yang Lebih Baik?", Mekari eSign, https://mekarisign.com/id/blog/tanda-tangan-basah/ (accessed May 21, 2023).

[6] Haekal, M. M., "Mengenal Perbedaan Tanda Tangan Elektronik tersertifikasi Dan Tidak tersertifikasi. Mekari eSign." https://mekarisign.com/id/blog/tanda-tangan-elektronik-tersertifikasi/ (accessed May 21, 2023).

[7] Ika, A., "Fintech dan Tanda Tangan Elektronik," https://tte.kominfo.go.id/blog/5db508bce2467517f4493af8#:~:text=Dalam%20UU%20ITE%2C%20tanda%20tangan,sebagai%20alat%20verifikasi%20dan%20autentikasi (accessed May 21, 2023).

[8] "Kebijakan privasi," https://repository.tilaka.id/kebijakan-privasi.pdf (accessed May 21, 2023).

[9] "Keuntungan Pakai TTE Tersertifikasi. Kominfo Penyelenggara Sertifikat Elektronik," https://tte.kominfo.go.id/blog/60f0f35a7eec0973a8711c38 (accessed May 21, 2023).

[10] "Kominfo Penyelenggara Sertifikat Elektronik," https://tte.kominfo.go.id/requirement (accessed May 21, 2023).

[11] "Kominfo Penyelenggara Sertifikat Elektronik," https://tte.kominfo.go.id/listpsrenew (accessed May 21, 2023).

[12] Munir, R., "Kriptografi Modern," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2021-2022/4%20-%20Kripto-modern-2021.pdf (accessed May 21, 2023).

[13] "PSrE Induk," https://www.rootca.id/ (accessed May 21, 2023).

[14] "Repository," Mekari eSign, https://mekarisign.com/id/repository/ (accessed May 21, 2023).

[15] "Sertifikat Elektronik pada Tanda Tangan Elektronik," https://tte.kominfo.go.id/blog/606ea623e4db24035ea6574d#:~:text=Tanda%20Tangan%20Elektronik%20(TTE)%20Tersertifikasi%20adalah%20Tanda%20Tangan%20Elektronik%20yang,tanpa%20menggunakan%20jasa%20PSrE%20Indonesia (accessed May 21, 2023).

[16] "Solusi Tanda Tangan Online, e-meterai, Stempel; Kontrak Digital," Mekari eSign, https://mekarisign.com/id/ (accessed May 21, 2023).

[17] "Tanda Tangan Elektronik. Mekari eSign," https://mekarisign.com/id/fitur/tanda-tangan-elektronik/ (accessed May 21, 2023).

[18] Tilaka.id, https://tilaka.id/ (accessed May 21, 2023).

[19] "Repository," Tilaka, https://repository.tilaka.id/?_ga=2.259559114.1149804039.1684720887-1511015118.1684720885 (accessed May 21, 2023).

[20] Munir, R., "Tanda Tangan Digital," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/16-Tanda-tangan-digital-2023.pdf (accessed May 21, 2023).

[21] Munir, R., "Sertifikat Digital," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/18-Sertifikat-digital-2023.pdf (accessed May 21, 2023).

[22] "Kebijakan privasi," https://repository.tilaka.id/kebijakan-privasi.pdf (accessed May 21, 2023).

## 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, 22 Mei 2023

Abraham Manuel Hotasi B.
18219083