Certification Practice Statement (CPS)

PT TILAKA NUSA TEKNOLOGI

Nomor Dokumen	:	**TNT-CPS-001**
Versi	:	2.0
Tanggal Berlaku Efektif	:	20 Oktober 2022

Halaman Persetujuan Policy Authority

Menyetujui,

Chief Financial Officer

Christian Saortua

Riwayat Dokumen

Rev No	Tanggal Revisi	Deskripsi	Oleh
1.0	24 Ags 2021	Pertama kali terbit	IT Compliance
2.0	20 Okt 2022	• Perubahan nomor dokumen dari TNT-CP-001 menjadi TNT-CPS-001. • Penambahan Halaman Persetujuan Policy Authority. • Penghapusan rincian tanggung jawab PSrE Induk Indonesia (bagian 1.3.1). • Penambahan rincian tanggung jawab PSrE Berinduk (bagian 1.3.2). • Penambahan proses pemeriksaan keamanan fasilitas (bagian 5.1.2). • Perubahan persyaratan legalitas organisasi (bagian 4.1.2.1). • Perubahan untuk mengakomodasi Otoritas Pendaftaran/Registration Authority (RA) eksternal. • Perubahan untuk mengakomodasi Pelanggan Personal. • Perubahan redaksional dan perapihan tata penulisan.	Legal & Compliance

Daftar Isi

1. Pengantar

PT Tilaka Nusa Teknologi ("TILAKA") adalah suatu badan hukum yang menjalankan kegiatan usaha sebagai Penyelenggara Sertifikasi Elektronik ("PSrE") dan dalam menjalankan kegiatan usahanya tunduk kepada peraturan perundang-undangan yang berlaku, termasuk namun tidak terbatas pada Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah nomor 71 tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komunikasi dan Informatika nomor 11 tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik, berikut dengan segala perubahannya yang mungkin timbul di kemudian hari ("**PSrE TILAKA**"). PSrE TILAKA merupakan PSrE Berinduk dengan jenis PSrE Non-Instansi.

Certification Practice Statement ini ("CPS") mendefinisikan persyaratan prosedural dan operasional yang dianut oleh PSrE TILAKA saat menerbitkan dan mengelola objek yang ditandatangani secara elektronik dalam lingkungan Infrastruktur Kunci Publik ("IKP") Indonesia.

1.1 Ringkasan

CPS telah mengacu pada ketentuan *Certificate Policy* (CP) Penyelenggara Sertifikasi Elektronik Induk Indonesia ("PSrE Induk") dan sudah 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*.

CPS dibuat dengan asumsi bahwa pembaca telah membaca, mempelajari, dan memahami ketentuan yang diatur pada CP PSrE Induk Indonesia. Pembaca dapat mengunduh CP PSrE Induk Indonesia melalui https://www.rootca.id/.

CPS berlaku sesuai tanggal berlaku efektif sebagaimana tercantum pada halaman awal CPS. Setelah CPS berlaku efektif, maka CPS sebelumnya dinyatakan sudah tidak berlaku kecuali untuk kebutuhan yang berhubungan dengan Sertifikat Pemilik yang permohonan penerbitannya dilakukan sebelum CPS berlaku efektif. Atas kebutuhan yang berhubungan dengan Sertifikat Pemilik yang permohonan penerbitannya dilakukan setelah CPS berlaku efektif, maka ketentuan pada CPS telah berlaku. Dalam hal kebutuhan yang berhubungan dengan Sertifikat Pemilik yang permohonan penerbitannya dilakukan sebelum CPS berlaku efektif, maka ketentuan CPS yang berlaku adalah sesuai dengan CPS yang berlaku efektif pada saat permohonan penerbitan Sertifikat.

1.2 Identifikasi dan Nama Dokumen

Dokumen ini adalah dokumen CPS PSrE TILAKA. *Object Identifier* (OID) yang digunakan untuk CPS (tidak termasuk *Extended Validation Certificate*) ini adalah:

Digitally Signed Object	*Object Identifier* (OID)
OID PSrE Non-Instansi	2.16.360.1.1.1.3.12
OID non-Instansi PSrE TILAKA	2.16.360.1.1.1.3.12.5
OID CPS PSrE TILAKA	2.16.360.1.1.1.3.12.5.1
OID Verifikasi Level 4	2.16.360.1.1.1.4.4
OID Sertifikat untuk individu	2.16.360.1.1.1.7.1

1.3 Partisipan IKP

1.3.1 PSrE Induk

PSrE Induk adalah Induk dari IKP Indonesia yang dioperasikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo). PSrE Induk membawahi 2 (dua) jenis PSrE Berinduk yaitu PSrE Instansi dan PSrE Non-Instansi. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Berinduk, sebagaimana dirinci dalam CP PSrE Induk.

1.3.2 PSrE Berinduk

PSrE Berinduk adalah PSrE yang telah mendapatkan status pengakuan berinduk dari Kemenkominfo. PSrE TILAKA menerbitkan Sertifikat kepada Pemilik selain entitas Pemerintah Indonesia. Dalam hal ini, PSrE TILAKA tidak boleh berinduk selain kepada PSrE Induk dan tidak boleh menjadi induk bagi PSrE lainnya.

PSrE TILAKA bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat tersebut, sebagaimana dirinci dalam CPS termasuk proses:

1. Pengendalian terhadap 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 yang terkait dengan PSrE TILAKA dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS.

1.3.3 Otoritas Pendaftaran (RA)

Otoritas Pendaftaran/Registration Authority (RA) merupakan pihak yang menjalankan beberapa fungsi yang tunduk terhadap prosedur yang berlaku di PSrE TILAKA. Adapun fungsi tersebut adalah sebagai berikut:

1. Melakukan verifikasi dan validasi data identitas Pemohon;
2. Memulai dan/atau memproses permohonan penerbitan Sertifikat;
3. Memulai dan/atau memproses permohonan pencabutan Sertifikat Pemilik; dan
4. Memulai dan/atau memproses permohonan penerbitan ulang Sertifikat.

Dalam hal permohonan penerbitan Sertifikat oleh Pemohon diterima secara langsung oleh PSrE TILAKA, maka, dalam hal ini PSrE TILAKA berperan sebagai RA bagi dirinya sendiri. Selain itu, PSrE TILAKA dapat melakukan hubungan kontraktual dengan RA tertentu untuk menjalankan fungsi sebagai RA dan terhadap RA tersebut tunduk pada ketentuan CPS. PSrE TILAKA memiliki hak untuk melaksanakan audit atau pemeriksaan terhadap kesesuaian fungsi yang dijalankan oleh RA dengan CPS dan/atau peraturan perundang-undangan yang berlaku.

1.3.4 Pemilik

Pemilik adalah Warga Negara Indonesia yang berada dalam ruang lingkup Pelanggan dan merupakan subjek dari Sertifikat Pemilik. Sebelum dilakukannya verifikasi, validasi, dan penerbitan Sertifikat, Pemilik disebut sebagai Pemohon. Pemilik selanjutnya dapat mengajukan permohonan pencabutan dan/atau penerbitan ulang atas Sertifikat.

1.3.5 Pihak Pengandal

Pihak Pengandal adalah orang, entitas, organisasi, lembaga, atau badan usaha yang memercayai Sertifikat Pemilik dan tanda tangan elektronik yang diterbitkan oleh PSrE TILAKA. Pihak Pengandal terlebih dahulu memeriksa respon dari *Online Certificate Status Protocol* (OCSP) *responder* dan *Certificate Revocation Lists* (CRL) yang disediakan oleh PSrE TILAKA sebelum memanfaatkan informasi yang ada dalam Sertifikat Pemilik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat Pemilik.

Pihak Pengandal yang mengandalkan Sertifikat Pemilik yang diterbitkan oleh PSrE TILAKA wajib tunduk pada ketentuan yang diatur dalam CPS, Perjanjian Pihak Pengandal, dan peraturan perundang-undangan yang berlaku.

Pihak Pengandal dapat menggunakan informasi dalam Sertifikat Pemilik untuk:

1. Memeriksa tujuan penggunaan Sertifikat Pemilik;
2. Melakukan verifikasi tanda tangan elektronik;
3. Memeriksa apakah Sertifikat Pemilik termasuk di dalam CRL; dan
4. Persetujuan atas batas tanggung jawab dan jaminan.

Pihak Pengandal dapat meliputi bank, perusahaan *e-commerce*, dan entitas lain yang menggunakan tanda tangan elektronik di dalam layanannya.

1.3.6 Partisipan Lain

1.3.6.1 Layanan Pusat Data

PSrE TILAKA dapat melakukan hubungan kontraktual dengan Partisipan Lain yang berhubungan dengan penyediaan layanan pusat data untuk kegiatan operasional PSrE TILAKA.

1.4 Kegunaan Sertifikat

1.4.1 Penggunaan Sertifikat yang Semestinya

Penggunaan Sertifikat Pemilik dibatasi sesuai *Key Usage* dan *Extended Key Usage* pada *Certificate Extension*. Sertifikat PSrE TILAKA dapat digunakan untuk menerbitkan Sertifikat Pemilik untuk transaksi yang memerlukan:

1. *Digital Signature*; dan
2. *Non-Repudiation*.

PSrE TILAKA hanya menyediakan Sertifikat Pemilik dengan level verifikasi identitas level 4 dengan tingkat jaminan tinggi. Verifikasi identitas dilakukan dengan membandingkan kesesuaian data identitas yang tercatat pada instansi Pemerintah dengan e-KTP dan swafoto Pemohon.

Kelas Sertifikat	Tingkat Jaminan			Penggunaan	
	Jaminan Rendah	Jaminan Sedang	Jaminan Tinggi	*Digital Signature*	*Non-Repudiation*
Sertifikat Individu					
Level 4			✓	✓	✓

1.4.2 Penggunaan Sertifikat yang Dilarang

Sertifikat Pemilik yang diterbitkan PSrE TILAKA dilarang dipakai untuk penggunaan yang tidak dinyatakan pada bagian 1.4.1.

1.5 Otoritas Kebijakan

Otoritas Kebijakan/Policy Authority (PA) adalah karyawan ("personel") yang dipercaya oleh PSrE TILAKA untuk berperan dan bertanggung jawab dalam hal:

1. Menetapkan CPS; dan
2. Memastikan semua layanan, operasional, dan infrastruktur PSrE TILAKA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CPS.

1.5.1 Organisasi Pengelola Dokumen

CPS PSrE TILAKA dan dokumen publik lainnya dikelola oleh:

Telepon : +62 21-50100922

Email : compliance@tilaka.id

1.5.2 Kontak

Alamat Surat : Belleza Shoping Arcade Lantai 3 Unit SA 0380, Jl. Arteri Permata Hijau Nomor 34, RT.004/RW.002, Grogol Utara, Kebayoran Lama, Jakarta Selatan, 12210

Email : info@tilaka.id

URL : https://www.tilaka.id

Telp : +62 21-50100922

1.5.3 Personel yang Menentukan Kesesuaian CPS

PA PSrE TILAKA menentukan kesesuaian konten dengan penerapan dari CPS.

1.5.4 Prosedur Persetujuan CPS

PA PSrE TILAKA menyetujui CPS dan segala perubahannya. PA PSrE TILAKA menentukan ketika perubahan CPS membutuhkan pemberitahuan pihak terkait ataupun perubahan OID. Perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum melalui Repositori. PSrE TILAKA juga akan melakukan pemberitahuan melalui *email* kepada Pemilik Sertifikat terkait perubahan atau adendum terkait CPS.

1.6 Definisi dan Akronim

Lihat Lampiran I untuk Tabel Akronim dan Lampiran II untuk Tabel Definisi.

2. Tanggung Jawab Publikasi dan Repositori

2.1 Repositori

PSrE TILAKA berusaha dengan penuh kehati-hatian untuk menyediakan dan memelihara Repositori yang berisi dokumen publik, yang termasuk namun tidak terbatas pada:

1. *Certification Practice Statement* (CPS);
2. Kebijakan Privasi;
3. Perjanjian Pihak Pengandal;
4. Perjanjian Pemilik Sertifikat;
5. Kebijakan Jaminan;
6. Skema Harga;
7. Sertifikat PSrE TILAKA; dan
8. *Certificate Revocation List* (CRL).

2.2 Publikasi Informasi Sertifikat

PSrE TILAKA menyediakan dan memelihara Repositori dengan cara melakukan publikasi atas semua dokumen yang terdapat pada bagian 2.1 untuk dapat diakses oleh Publik melalui https://repository.tilaka.id/.

2.3 Waktu atau Frekuensi Publikasi

Dokumen publik yang terdapat pada bagian 2.1 akan dipublikasikan dengan waktu atau frekuensi sebagai berikut:

a. Bagian 2.1 poin 1, 2, 3, 4, 5, dan 6 dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui;
b. Bagian 2.1 poin 7 akan ditentukan sesuai ketentuan pada bagian 4.4.2; dan
c. Bagian 2.1 poin 8 akan ditentukan sesuai ketentuan pada bagian 4.9.7.

2.4 Kendali Akses pada Repositori

Informasi yang terpublikasi pada Repositori adalah informasi publik. PSrE TILAKA memberikan akses baca yang tidak terbatas pada Repositori dan menerapkan kendali kontrol logis dan fisik untuk mencegah pihak yang tidak berwenang untuk menambahkan, menghapus, dan/atau mengubah baik sebagian maupun seluruh isi dokumen di dalam Repositori. PSrE TILAKA akan berusaha dengan penuh kehati-hatian untuk melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

3. Identifikasi dan Autentikasi

3.1 Penamaan

3.1.1 Tipe Nama

Sertifikat yang dibuat dan ditandatangani oleh PSrE TILAKA menggunakan subyek *Distinguished Name* (DN) yang *non-null* dan telah sesuai dengan standar ITU X.500. DN yang digunakan oleh PSrE TILAKA berdasarkan CPS adalah sebagai berikut:

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

3.1.2 Kebutuhan Nama yang Bermakna

Sertifikat Pemilik yang diterbitkan sesuai dengan CPS akan bermakna hanya jika nama-nama yang muncul dalam Sertifikat Pemilik dapat dipahami dan digunakan oleh Pihak Pengandal. Nama yang digunakan dalam Sertifikat Pemilik mengidentifikasi objek tersebut.

Nama subjek dan penerbit yang terkandung dalam Sertifikat Pemilik menjelaskan bahwa PSrE TILAKA memiliki cukup bukti yang menunjukkan keterkaitan antara nama dengan Pemilik. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh Pemilik.

3.1.3 Anonimitas atau Pseudonimitas Pemilik

PSrE TILAKA tidak menerbitkan Sertifikat Pemilik anonim atau pseudonim.

3.1.4 Aturan Interpretasi Berbagai Bentuk Nama

DN dalam Sertifikat diinterpretasikan menggunakan standar X.500.

3.1.5 Keunikan Nama

DN dalam Sertifikat unik di dalam ranah PSrE TILAKA. DN diisi dengan informasi yang dikirimkan oleh Pemohon pada saat pengajuan permohonan penerbitan Sertifikat. Pemohon bertanggung jawab penuh terhadap informasi yang dikirimkan pada saat pengajuan permohonan penerbitan Sertifikat.

3.1.6 Pengakuan, Autentikasi, dan Peran Merek Dagang

Pemohon tidak diperbolehkan mengajukan permohonan penerbitan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE TILAKA tidak berkewajiban untuk melakukan verifikasi terhadap hak Pemohon dalam hal penggunaan merek dagang. Pemohon atau Pemilik bertanggung jawab penuh terhadap hak kekayaan intelektual pihak lain, terhadap informasi yang digunakan olehnya pada proses sebelum, saat, dan setelah pengajuan permohonan. PSrE TILAKA dapat menolak permohonan atau melakukan pencabutan Sertifikat Pemilik yang menjadi bagian dari konflik merek dagang.

3.2 Validasi Identitas Awal

3.2.1 Pembuktian Kepemilikan Kunci Privat

Untuk Sertifikat Pemilik, pasangan kunci dibangkitkan secara aman oleh PSrE TILAKA menggunakan modul kriptografi yang memenuhi persyaratan FIPS 140-2 level 3 dan hanya dapat diakses oleh Pemilik dengan minimal 2 (dua) dari 3 (tiga) faktor autentikasi berupa:

a. *Username*, *password*, dan *one-time password* (untuk selanjutnya disebut "OTP") atau lainnya yang memenuhi unsur "*what you know*"; atau
b. *Personal Identification Number* (PIN), token, atau lainnya yang memenuhi unsur "*what you have*"; atau
c. data biometrik atau lainnya yang memenuhi unsur "*what you are*".

3.2.2 Autentikasi Identitas Organisasi

Tidak ada ketentuan.

3.2.3 Autentikasi Identitas Individu

RA akan melakukan verifikasi dan validasi terhadap informasi yang diajukan oleh Pemohon sehubungan dengan permohonan penerbitan Sertifikat sesuai dengan peraturan perundang-undangan yang berlaku. Adapun informasi dan dokumen yang diajukan oleh Pemohon meliputi:

1. Nama;
2. Nomor Induk Kependudukan (NIK);
3. Salinan dokumen e-KTP;
4. Alamat surat elektronik (*email*) dan/atau nomor telepon; dan
5. Data biometrik berupa swafoto yang telah teruji menggunakan mekanisme *liveness detection*.

RA melakukan verifikasi dan validasi kebenaran informasi yang dikirimkan oleh Pemohon sehubungan dengan permohonan penerbitan Sertifikat dengan cara berikut ini:

1. Mengirimkan konfirmasi ke alamat *email* dan/atau nomor telepon yang didaftarkan;
2. Menggunakan sumber data dari kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional untuk melakukan verifikasi terhadap NIK, Nama dan swafoto yang dikirimkan oleh Pemohon;
3. Melakukan verifikasi terhadap swafoto menggunakan mekanisme *liveness detection*; dan
4. Melakukan validasi terhadap data Pemohon yang telah berhasil melewati proses verifikasi.

PSrE TILAKA dan/atau RA berkomitmen untuk menyimpan data terkait dengan proses verifikasi dan validasi terhadap informasi yang diajukan oleh Pemohon sehubungan dengan permohonan penerbitan Sertifikat Pemilik selama 5 (lima) tahun.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

PSrE TILAKA tidak menerbitkan Sertifikat kepada Pemohon yang tidak lolos proses verifikasi dan validasi sebagaimana ketentuan bagian 3.2.3.

3.2.5 Validasi Otoritas

Tidak ada ketentuan.

3.2.6 Kriteria Inter-Operasi

Tidak ada ketentuan.

3.3 Identifikasi dan Autentikasi untuk Permintaan Penggantian Kunci (*Re-Key*)

3.3.1 Identifikasi dan Autentikasi untuk Kegiatan *Re-Key* Rutin

Tidak ada ketentuan.

3.3.2 Identifikasi dan Autentikasi untuk *Re-Key* setelah Pencabutan

Tidak ada ketentuan.

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan

Permohonan pencabutan Sertifikat Pemilik selalu divalidasi atau diautentikasi. Permohonan pencabutan Sertifikat Pemilik akan dilakukan dengan cara sebagai berikut:

a. Permohonan pencabutan Sertifikat Pemilik yang dilakukan oleh Pemilik diautentikasi menggunakan data biometrik melalui Layanan Tanda Tangan Elektronik Tilaka; atau
b. Permohonan pencabutan Sertifikat Pemilik yang dilakukan oleh Admin Korporat atau Aparat Penegak Hukum divalidasi oleh petugas validator PSrE TILAKA.

4. Persyaratan Operasional Siklus Sertifikat

4.1 Permohonan Sertifikat

4.1.1 Siapa yang Dapat Mengajukan Sebuah Permohonan Sertifikat

Pihak yang dapat mengajukan permohonan penerbitan Sertifikat ke PSrE TILAKA adalah:

a. Individu (untuk Pelanggan Personal); atau
b. Individu yang berafiliasi dengan entitas korporasi (untuk Pelanggan Korporasi).

4.1.2 Proses Pendaftaran dan Tanggung Jawab

Pemohon memberikan informasi yang lengkap dan benar pada saat proses permohonan penerbitan Sertifikat agar RA dapat melakukan verifikasi dan validasi terhadap data tersebut. Sebelum menyelesaikan proses pendaftaran, Pemohon perlu menyetujui syarat dan ketentuan yang ditetapkan oleh PSrE TILAKA.

RA bertanggung jawab untuk melakukan verifikasi dan validasi terhadap data yang dikirimkan oleh Pemohon sehubungan dengan proses pendaftaran sesuai dengan peraturan perundang-undangan yang berlaku.

4.1.2.1 Pendaftaran Korporasi

Dalam hal permohonan penerbitan Sertifikat berasal dari Pelanggan Korporasi, maka RA akan menjalankan proses pendaftaran korporasi dengan tata cara sebagai berikut:

1. RA melakukan verifikasi dan validasi terhadap legalitas korporasi menggunakan salah satu atau lebih dokumen atau informasi yang termasuk namun tidak terbatas pada:
   a. Akta Pendirian Perusahaan dan Perubahan Akta Terakhir atau *email* resmi perwakilan korporasi;
   b. Nomor Induk Berusaha (NIB); dan/atau
   c. Nomor Pokok Wajib Pajak (NPWP) Perusahaan.
2. Setelah proses verifikasi dan validasi tehadap legalitas korporasi berhasil, maka Admin Tilaka akan mendaftarkan korporasi;
3. Setelah Admin Tilaka melakukan pendaftaran terhadap korporasi, Admin Korporat akan menerima *email* tautan pendaftaran; dan
4. Setelah Admin Korporat menerima *email* tautan pendaftaran, maka Admin Korporat akan mengisi data diri (NIK, nama, nomor telepon, foto e-KTP, dan *password* untuk *login*).

Proses selanjutnya yaitu proses pendaftaran Pemohon seperti yang dijelaskan di bagian 4.1.2.2.

4.1.2.2 Pendaftaran Pemohon

RA akan menjalankan proses pendaftaran Pemohon dengan tata cara sebagai berikut:

1. Admin Korporat mengirim undangan melalui *email* yang berisi tautan untuk proses pendaftaran Pemohon untuk Pelanggan Korporasi. Dalam hal Pemohon merupakan Pelanggan Personal, pendaftaran dapat diajukan tanpa memerlukan partisipasi dari Admin Korporat;
2. Pemohon melengkapi dan mengirimkan informasi yang dibutuhkan untuk melakukan pendaftaran kepada RA sesuai dengan ketentuan pada bagian 3.2.3;
3. Setelah Pemohon melengkapi dan mengirimkan informasi yang dibutuhkan untuk melakukan pendaftaran, RA akan melakukan verifikasi dan validasi terhadap informasi tersebut; dan
4. Jika hasil verifikasi dan validasi telah dinyatakan sesuai oleh RA, maka PSrE TILAKA akan menerbitkan Sertifikat Pemilik setelah Pemohon melakukan konfirmasi penerimaan Sertifikat Pemilik. Jika hasil verifikasi atau validasi dinyatakan tidak sesuai oleh RA, maka RA dapat meminta data dan informasi tambahan kepada Pemohon untuk mengulang proses verifikasi dan validasi.

4.2 Pemrosesan Permohonan Sertifikat

4.2.1 Melaksanakan Fungsi-Fungsi Identifikasi dan Autentikasi

Proses verifikasi dan validasi terhadap informasi yang telah dikirimkan oleh Pemohon sehubungan dengan permohonan penerbitan Sertifikat memenuhi persyaratan yang ditentukan seperti yang tertera pada bagian 3.2.

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat

Persetujuan atas permohonan penerbitan Sertifikat dapat dilakukan setelah seluruh rangkaian pendaftaran berhasil, dan data yang didaftarkan sesuai dengan hasil verifikasi dan validasi. Namun, permohonan penerbitan Sertifikat dapat ditolak dengan alasan berikut:

1. Khusus Pelanggan Korporasi, Nama Pemohon yang telah didaftarkan tidak sesuai dengan nama yang telah diajukan oleh Admin Korporat; atau
2. Informasi yang dikirimkan oleh Pemohon sehubungan dengan proses permohonan penerbitan Sertifikat tidak sesuai dengan data yang tercatat pada kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional.

Pemohon dapat mengajukan permohonan ulang atas ketidaksesuaian data tersebut.

Persetujuan atau penolakan terhadap permohonan penerbitan Sertifikat akan diinformasikan melalui *email* kepada Pemohon dengan tata cara yang dijelaskan pada bagian 4.1.

4.2.3 Waktu Pemrosesan Permohonan Sertifikat

PSrE TILAKA menerbitkan Sertifikat Pemilik maksimal 1 (satu) hari kerja setelah proses verifikasi dan validasi telah berhasil dilakukan.

4.3 Penerbitan Sertifikat

4.3.1 Tindakan PSrE selama Penerbitan Sertifikat

PSrE TILAKA menerbitkan Sertifikat Pemilik setelah RA melakukan verifikasi dan validasi terhadap permohonan penerbitan Sertifikat sesuai ketentuan bagian 3.2. Persetujuan terhadap syarat dan ketentuan layanan PSrE TILAKA yang dilakukan Pemohon sebelum menyelesaikan pendaftaran, juga merupakan bentuk persetujuan pada bagian 4.4 dan 9.6.

4.3.2 Pemberitahuan kepada Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

Pemberitahuan melalui *email* akan dilakukan oleh PSrE TILAKA untuk menginformasikan kepada Pemilik tentang Sertifikat yang berhasil diterbitkan maksimal 2 (dua) hari kalender sejak proses verifikasi dan validasi berhasil dilakukan. Sebelum menggunakan Sertifikat, Pemilik melakukan pemeriksaan atas seluruh informasi dan melakukan konfirmasi terhadap Sertifikat.

4.4 Penerimaan Sertifikat

4.4.1 Sikap yang Dianggap sebagai Menerima Sertifikat

Pemilik dianggap telah menerima Sertifikat yang diterbitkan oleh PSrE TILAKA apabila:

1. Telah memeriksa dan menyetujui informasi yang terkandung dalam Sertifikat; atau
2. Tidak memberikan tanggapan dalam jangka waktu 9 (sembilan) hari kalender sejak PSrE TILAKA mengirimkan *email* terkait penerbitan Sertifikat.

Pemilik dapat mengajukan keberatan kepada PSrE TILAKA jika terdapat kesalahan informasi yang terkandung dalam Sertifikat.

4.4.2 Publikasi Sertifikat oleh PSrE

PSrE TILAKA akan melakukan publikasi terhadap Sertifikat PSrE TILAKA pada Repositori sesuai ketentuan pada bagian 2.2 segera setelah Sertifikat PSrE TILAKA diterbitkan. PSrE TILAKA tidak akan

melakukan publikasi terhadap Sertifikat Pemilik, namun Pemilik dapat mengunduh Sertifikat pada Layanan Tanda Tangan Elektronik Tilaka dengan menggunakan metode autentikasi yang sesuai dengan ketentuan PSrE TILAKA.

4.4.3 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.5 Pasangan Kunci dan Penggunaan Sertifikat

4.5.1 Penggunaan Kunci Privat dan Sertifikat Pemilik

Pemilik menitipkan Kunci Privatnya ke PSrE TILAKA dalam rangka *remote signing*, maka dari itu, PSrE TILAKA akan berusaha dengan penuh kehati-hatian agar Kunci Privat Pemilik hanya dapat digunakan oleh Pemilik itu sendiri. Penggunaan Kunci Privat Pemilik hanya dapat dilakukan sesuai ketentuan bagian 3.2.1. PSrE TILAKA akan melindungi Kunci Privat Pemilik dengan menggunakan HSM (*Hardware Security Module*). Penggunaan Kunci Privat dan Sertifikat oleh Pemilik hanya dapat untuk tujuan yang sudah ditentukan pada CPS bagian 1.4.

4.5.2 Penggunaan Kunci Publik dan Sertifikat oleh Pihak Pengandal

Pihak Pengandal menggunakan perangkat lunak yang patuh kepada X.509. Dalam rangka mengandalkan Serifikat Pemilik, Pihak Pengandal tunduk pada ketentuan dalam CPS. Pihak Pengandal berhati-hati, mempertimbangkan keseluruhan keadaan, dan risiko kerugian sebelum mengandalkan Sertifikat Pemilik.

Pihak Pengandal selalu diasumsikan memahami bahwa, mengandalkan Sertifikat Pemilik yang belum diproses sesuai dengan standar yang berlaku dapat menyebabkan risiko baginya, Pihak Pengandal akan bertanggung jawab atas risiko tersebut jika terjadi. Pihak Pengandal mengajukan dan mendapatkan persetujuan dari PSrE TILAKA terlebih dahulu jika memerlukan jaminan tambahan dalam rangka mengandalkan Sertifikat Pemilik.

4.6 Pembaruan Sertifikat

4.6.1 Kondisi untuk Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.2 Siapa yang dapat Meminta Pembaruan

Tidak ada ketentuan.

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.4 Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Tidak ada ketentuan.

4.6.5 Sikap yang Dianggap sebagai Menerima Sertifikat yang Diperbarui

Tidak ada ketentuan.

4.6.6 Publikasi Sertifikat yang Diperbarui oleh PSrE

Tidak ada ketentuan.

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.7 Penggantian Kunci (*Re-Key*) Sertifikat

4.7.1 Keadaan *Re-Key* Sertifikat

Tidak ada ketentuan.

4.7.2 Siapa yang dapat Meminta Sertifikasi dari Sebuah Kunci Publik Baru

Tidak ada ketentuan.

4.7.3 Pemrosesan Permintaan *Re-Key* Sertifikat

Tidak ada ketentuan.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.7.5 Sifat yang Dianggap sebagai Menerima Sertifikat *Re-Key*

Tidak ada ketentuan.

4.7.6 Publikasi Sertifikat *Re-Key* oleh PSrE

Tidak ada ketentuan.

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.8 Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.1 Keadaan bagi Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.2 Siapa yang Berhak Meminta Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3 Pemrosesan Permintaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4 Pemberitahuan Tentang Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.8.5 Sikap yang Dianggap sebagai Menerima Sertifikat yang Dimodifikasi

Tidak ada ketentuan.

4.8.6 Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Tidak ada ketentuan.

4.8.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Keadaan untuk Pencabutan

PSrE TILAKA mencabut Sertifikat Pemilik jika terdapat permohonan pencabutan dengan salah 1 (satu) atau lebih keadaan sebagai berikut:

1. Permohonan pencabutan Sertifikat Pemilik oleh Pemilik, Admin Korporat, atau Aparat Penegak Hukum;
2. Terdapat informasi yang tidak valid pada Sertifikat Pemilik; dan/atau
3. Terjadi kebocoran atau kerusakan Kunci Privat Pemilik.

PSrE TILAKA dapat mencabut Sertifikat Pemilik secara sepihak dengan salah 1 (satu) atau lebih keadaan sebagai berikut:

1. Pemilik dan/atau Pelanggan terbukti melanggar ketentuan yang tercantum dalam CPS, Kebijakan Privasi, Perjanjian Kerja Sama, dan/atau Perjanjian Pemilik Sertifikat;
2. Terjadi kebocoran atau kehilangan Kunci Privat PSrE TILAKA (mengacu pada bagian 5.7.3);
3. Kegiatan usaha PSrE TILAKA berhenti atau dihentikan; dan/atau
4. Terjadi kebocoran atau kehilangan Kunci Privat PSrE Induk (mengacu pada bagian 5.7.3).

Sertifikat Pemilik yang telah dicabut dimasukkan dalam CRL dan/atau ditampilkan pada OCSP *responder*. Sertifikat Pemilik yang dicabut disertakan dalam semua publikasi baru tentang informasi status Sertifikat Pemilik sampai masa berlakunya berakhir.

4.9.2 Siapa yang dapat Meminta Pencabutan

Pemilik, Admin Korporat, dan Aparat Penegak Hukum dapat mengajukan permohonan pencabutan Sertifikat Pemilik.

4.9.3 Prosedur Permintaan Pencabutan

Pemilik mengajukan permohonan pencabutan Sertifikat dengan menyertakan alasan pencabutan. Prosedur pencabutan Sertifikat yang diajukan oleh Pemilik adalah sebagai berikut:

1. Pemilik mengajukan permohonan pencabutan Sertifikat Pemilik lewat Layanan Tanda Tangan Elektronik Tilaka dan memilih alasan pencabutan.
2. Setelah Pemilik mengajukan permohonan pencabutan Sertifikat, Pemilik melakukan autentikasi swafoto dengan menggunakan *liveness detection*.
3. Setelah proses autentikasi swafoto dilakukan, RA akan melakukan validasi terhadap swafoto yang dilakukan oleh Pemilik.

4. Jika hasil validasi telah dinyatakan sesuai oleh RA, maka proses pencabutan Sertifikat Pemilik akan diproses oleh PSrE TILAKA.

Admin Korporat atau Aparat Penegak Hukum mengajukan permohonan pencabutan Sertifikat Pemilik dengan menyertakan dokumen pendukung. Prosedur pencabutan Sertifikat Pemilik yang diajukan oleh Admin Korporat atau Aparat Penegak Hukum adalah sebagai berikut:

1. Mengirimkan permohonan pencabutan Sertifikat Pemilik kepada Admin Tilaka melalui *email* disertai dokumen pendukung sebagai berikut:
   a. Bukti bahwa Kunci Privat Pemilik telah terkompromi atau terungkap;
   b. Bukti bahwa penggunaan Sertifikat Pemilik tidak sesuai dengan CPS; atau
   c. Bukti surat keterangan atau sejenisnya dari Aparat Penegak Hukum atau Admin Korporat.
2. Setelah permohonan pencabutan Sertifikat Pemilik diajukan oleh Admin Korporat atau Aparat Penegak Hukum, RA akan melakukan validasi terhadap permohonan pencabutan Sertifikat Pemilik melalui *email* resmi Admin Korporat atau *email* resmi Aparat Penegak Hukum.
3. Setelah hasil validasi dinyatakan sesuai oleh RA, proses pencabutan Sertifikat Pemilik akan diproses oleh PSrE TILAKA.

Penjelasan lebih detail mengacu pada prosedur yang berlaku di PSrE TILAKA.

4.9.4 Masa Tenggang Permintaan Pencabutan

Tidak ada masa tenggang untuk pembatalan permohonan pencabutan Sertifikat Pemilik setelah permintaan pencabutan diverifikasi dan divalidasi.

4.9.5 Waktu Dimana PSrE Memproses Permintaan Pencabutan

PSrE TILAKA melakukan verifikasi dan validasi maksimal 2 (dua) hari kerja setelah permohonan pencabutan Sertifikat Pemilik diajukan sesuai dengan ketentuan 4.9.3, kecuali dalam hal *force majeure*.

4.9.6 Persyaratan Pemeriksaan Pencabutan bagi Pihak Pengandal

Pihak Pengandal melakukan pengecekan Sertifikat Pemilik pada OCSP *responder* dan CRL milik PSrE TILAKA. Pengecekan status Sertifikat Pemilik dilakukan menggunakan OCSP *responder*, lalu dilanjutkan menggunakan CRL.

4.9.7 Frekuensi Penerbitan CRL

PSrE TILAKA akan mengamankan CRL untuk menjamin integritas dan keautentikannya. Pembaharuan CRL dilakukan secara berkala setiap 24 (dua puluh empat) jam, dalam hal tertentu waktu maksimal pembaruan secara berkala setiap 26 (dua puluh enam) jam.

4.9.8 Latensi Maksimum CRL (Bila Berlaku)

PSrE TILAKA mempublikasikan CRL dalam waktu 30 (tiga puluh) menit setelah CRL diperbarui.

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status Daring

PSrE TILAKA menyediakan layanan pengecekan informasi status Sertifikat Pemilik melalui OCSP *responder* yang selalu tersedia pada URL https://ca.tilaka.id//ocsp, di luar waktu pemeliharaan yang ditentukan oleh PSrE TILAKA. Pemberitahuan mengenai waktu pemeliharaan dilakukan melalui *email* dan/atau Repositori. Jika OCSP *responder* dan CRL milik PSrE TILAKA sedang mengalami gangguan, maka PSrE TILAKA memberikan pengumuman terkait gangguan tersebut pada Repositori.

4.9.10 Persyaratan Pemeriksaan Pencabutan Daring

Tidak ada ketentuan.

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus Keterpaparan *Re-Key*

Tidak ada ketentuan.

4.9.13 Keadaan untuk Pembekuan

Tidak ada ketentuan.

4.9.14 Siapa yang dapat Meminta Pembekuan

Tidak ada ketentuan.

4.9.15 Prosedur Permintaan Pembekuan

Tidak ada ketentuan.

4.9.16 Batas Waktu Pembekuan

Tidak ada ketentuan.

4.10 Layanan Status Sertifikat

4.10.1 Karakteristik Operasional

PSrE TILAKA menyediakan layanan pemeriksaan informasi status Sertifikat Pemilik melalui OCSP *responder* atau CRL yang dipublikasi pada Repositori.

4.10.2 Ketersediaan Layanan

PSrE TILAKA melakukan semua tindakan yang diperlukan untuk menjamin ketersediaan layanan untuk dapat memvalidasi status Sertifikat Pemilik.

4.10.3 Fitur Opsional

Tidak ada ketentuan.

4.11 Akhir Berlangganan

Pelanggan mengakhiri langganan dengan membiarkan masa berlaku Sertifikat Pemilik berakhir, melakukan permohonan pencabutan Sertifikat Pemilik tanpa melakukan permohonan penerbitan ulang Sertifikat, atau khusus untuk Pelanggan Korporasi berakhirnya langganan juga dapat disebabkan oleh berakhirnya Perjanjian Kerja Sama antara Pelanggan Korporasi dengan PSrE TILAKA.

4.12 Pemulihan dan Penitipan Kunci

4.12.1 Kebijakan dan Praktik Pemulihan dan Eskro Kunci

PSrE TILAKA tidak menyediakan layanan eskro Kunci Privat Pemilik dari dan kepada pihak lain. PSrE TILAKA memiliki kebijakan tidak akan mengeskrokan Kunci Privat PSrE TILAKA kepada pihak lain.

4.12.2 Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi

Tidak ada ketentuan.

5. Fasilitas, Manajemen, dan Kendali Operasional

5.1 Kendali Fisik

5.1.1 Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan PSrE TILAKA maupun lokasi tempat kerja yang digunakan untuk mengelola layanan PSrE TILAKA telah menjalani Audit Sistem Manajemen Keamanan Informasi dengan menggunakan kriteria ISO/IEC 27001.

5.1.2 Akses Fisik

Peralatan yang digunakan oleh PSrE TILAKA selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik yang dilakukan oleh PSrE TILAKA bertujuan untuk:

1. Memastikan tidak ada akses ke perangkat keras tanpa izin;
2. Menyimpan semua *removable media* dan kertas yang berisi informasi rahasia dalam tempat penyimpanan yang aman;
3. Memonitor akses yang tidak berwenang baik secara manual maupun otomatis;
4. Memelihara dan memeriksa log akses secara berkala;
5. Memastikan bahwa kendali akses fisik untuk modul kriptografi dan sistem komputer PSrE TILAKA dilakukan oleh 2 (dua) personel.

Operasional PSrE TILAKA yang sangat penting dan memiliki risiko tinggi dilakukan di dalam fasilitas yang aman dengan memiliki pengamanan berlapis untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif, yaitu terdiri dari 10 (sepuluh) lapis pengamanan untuk *data center* dan 8 (delapan) lapis pengamanan untuk *disaster recovery center*. Fasilitas tersebut terpisah secara fisik dari fasilitas lain yang dikuasai oleh PSrE TILAKA, sehingga hanya personel PSrE TILAKA yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat PSrE TILAKA wajib dilaksanakan sebelum personel PSrE meninggalkan fasiltas tersebut. Proses pemeriksaan memastikan hal-hal berikut:

1. Perangkat berada dalam kondisi yang sesuai dengan mode operasinya;
2. Semua *security container* (misalnya lemari besi) sudah diamankan (dikunci);
3. Sistem keamanan fisik (misalnya kunci pintu, pelindung ventilasi) berfungsi dengan baik; dan
4. Area diamankan dari akses yang tidak berhak.

PSrE TILAKA menunjuk 1 (satu) atau lebih personel yang berperan dan bertanggung jawab untuk melakukan pemeriksaan tersebut. Pemeriksaan tersebut dibuktikan dengan log yang dapat dipertanggungjawabkan. Jika fasilitas tidak ditempati setiap waktu, maka orang terakhir yang meninggalkan fasilitas membuat lembaran *sign out* yang menunjukkan tanggal dan waktu, serta menyatakan bahwa semua mekanisme pemeriksaan keamanan fasilitas telah ada dan aktif.

5.1.3 Daya dan Penyejuk Udara

PSrE TILAKA memiliki daya listrik cadangan yang cukup dan dapat digunakan ketika listik utama mati untuk menyelesaikan setiap proses yang tertunda dan merekam status perangkat sebelum kekurangan daya atau pengatur suhu ruangan berhenti beroperasi yang menyebabkan sistem *shutdown*. Sistem IKP telah dilengkapi daya dan genset yang cukup untuk beroperasi paling sedikit selama 72 (tujuh puluh dua) jam untuk *data center* saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

5.1.4 Pemaparan Air

Peralatan PSrE TILAKA ditempatkan pada tempat yang tidak terpapar air. Paparan air hanya dimungkinkan untuk pencegahan kebakaran dan tindakan perlindungan (misalnya *fire sprinkler* atau alat pemadam api ringan).

5.1.5 Pencegahan dan Perlindungan dari Kebakaran

Peralatan yang dimiliki oleh PSrE TILAKA telah ditempatkan pada fasilitas dengan sistem deteksi kebakaran dan sistem pemadaman kebakaran yang memadai.

5.1.6 Penyimpanan Media

Media penyimpanan yang dimiliki oleh PSrE TILAKA telah ditempatkan pada lokasi yang terpisah dan disimpan agar terlindungi dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media penyimpanan yang berisi informasi audit, arsip, atau cadangan diduplikasi dan disimpan di lokasi yang terpisah yang berbeda dari layanan PSrE TILAKA.

5.1.7 Pembuangan Limbah

Seluruh informasi sensitif yang tersimpan pada media penyimpanan dan perangkat kriptografis yang sudah tidak digunakan akan dihancurkan dan dibuang sesuai prosedur yang berlaku di PSrE TILAKA.

5.1.8 *Backup Off-Site*

Sistem *backup* PSrE TILAKA dilakukan secara berkala minimal 1 (satu) kali dalam 7 (tujuh) hari, tersimpan pada lokasi yang aman pada lokasi *off-site,* dan mampu memulihkan sistem ketika terjadi kegagalan. Setidaknya 1 (satu) salinan *backup* lengkap disimpan di lokasi *off-site* yang terpisah dari peralatan PSrE TILAKA utama, jarak minimal antara lokasi peralatan PSrE TILAKA utama dan lokasi *off-site* adalah 50 (lima puluh) kilometer. Data dari sistem *backup* TILAKA dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional PSrE TILAKA.

5.2 Kendali Prosedur

5.2.1 Peran Terpercaya

Peran terpercaya termasuk namun tidak terbatas pada:

1. Manajer Penyelenggara/Pimpinan
   Bertanggung jawab melakukan penetapan terkait kebutuhan bisnis dan kebijakan internal PSrE TILAKA.
2. Otoritas Kebijakan
   Bertanggung jawab menetapkan kebijakan PSrE TILAKA.
3. Operating System Administrator
   Bertanggung jawab melakukan operasional dan pemeliharaan sistem operasi PSrE TILAKA.
4. Application & Database Administrator
   Bertanggung jawab melakukan operasional dan pemeliharaan sistem aplikasi dan basis data PSrE TILAKA.
5. HSM Administrator
   Bertanggung jawab melakukan operasional dan pemeliharaan HSM PSrE TILAKA.

Peran tersebut secara detail dijelaskan melalui dokumen internal perusahaan.

5.2.2 Jumlah Orang yang Dibutuhkan per Tugas

Untuk kegiatan yang memerlukan kendali multipersonel, semua personel memegang peran terpercaya. Kendali multipersonel tidak boleh dilakukan dengan melibatkan personel yang bertugas dalam peran Auditor. PSrE TILAKA wajib menunjuk minimal 3 (tiga) orang personel dalam setiap tugas yang diberikan di bawah ini:

1. Pembangkitan kunci PSrE TILAKA;
2. Penandatanganan Sertifikat PSrE TILAKA; dan
3. Pencabutan Sertifikat PSrE TILAKA.

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran

Dalam hal menentukan personel untuk mengisi peran terpercaya, PSrE TILAKA telah memeriksa latar belakang personel tersebut untuk memastikan bahwa peran terpercaya diisi oleh personel yang tepat dan berkompeten dalam bidangnya.

5.2.4 Peran yang Membutuhkan Pemisahan Tugas

Setiap personel yang ditunjuk oleh PSrE TILAKA tidak dapat melakukan rangkap peran pada peran-peran berikut:

1. Policy Authority dan Administrator Operasional;
2. Internal Auditor dan semua peran lain;
3. Pengembang Aplikasi dan semua peran lain.

5.3 Kendali Personel

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan *Clearance*

Semua personel PSrE TILAKA adalah Warga Negara Indonesia dan dipilih atas dasar keterampilan, pengalaman, kepercayaan, dan integritas.

5.3.2 Prosedur Pemeriksaan Latar Belakang

Semua personel PSrE TILAKA yang mengisi peran terpercaya telah dinyatakan lulus dari pemeriksaan latar belakang. Lingkup pemeriksaan latar belakang setidaknya dilakukan terhadap informasi 5 (lima) tahun sebelum personel tersebut melakukan pendaftaran sebagai calon personel PSrE TILAKA, dengan mencakup area berikut:

1. Kontak referensi pekerjaan;
2. Pendidikan atau sertifikasi;
3. Identifikasi Kependudukan (KTP);
4. Surat Keterangan Catatan Kepolisian (SKCK); dan
5. Pemeriksaan keuangan sesuai dengan prosedur yang berlaku pada PSrE TILAKA.

5.3.3 Persyaratan Pelatihan

Semua personel PSrE TILAKA yang mengisi peran terpercaya telah dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan tersebut mencakup topik yang relevan, seperti pemahaman mengenai pentingnya keamanan siber, tanggung jawab operasional, prosedur yang berlaku di PSrE TILAKA, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personel PSrE TILAKA dilakukan 1 (satu) kali dalam 1 (satu) tahun sesuai dengan prosedur yang berlaku di PSrE TILAKA.

5.3.4 Frekuensi dan Persyaratan Pelatihan Ulang

PSrE TILAKA memberikan pelatihan ulang dan pembaruan pada personelnya sesuai kebutuhan untuk memastikan personel tersebut mempertahankan kompetensi yang dipersyaratkan untuk melakukan tugas dan tanggung jawab pekerjaannya.

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan

PSrE TILAKA memastikan bahwa pergantian personel tidak mempengaruhi efektivitas operasional layanan atau keamanan sistem.

5.3.6 Sanksi untuk Tindakan Tidak Terotorisasi

Sanksi disiplin yang sesuai diberikan pada personel yang melanggar ketentuan dan kebijakan dalam CPS atau prosedur yang berlaku di PSrE TILAKA berdasarkan peraturan perusahaan PSrE TILAKA.

5.3.7 Persyaratan Kontraktor Independen

Kontraktor independen yang melaksanakan fungsi yang berkaitan dengan operasional PSrE TILAKA tunduk pada persyaratan yang berlaku yang ditetapkan dalam CPS.

5.3.8 Dokumentasi yang Disediakan untuk Personel

PSrE TILAKA menyediakan sejumlah dokumen kepada para personel yang ditunjuk agar dapat menjalankan tugasnya. Dokumen tersebut termasuk namun tidak terbatas pada CPS, peraturan dan kebijakan PSrE TILAKA, kontrak kerja, serta dokumen teknis, operasional, dan administratif lainnya (misalnya panduan administrator, panduan pengguna, dan dokumen terkait lainnya).

5.4 Prosedur Log Audit

Log audit dibuat untuk semua kejadian yang terkait dengan keamanan PSrE TILAKA. PSrE TILAKA akan mengupayakan agar log audit keamanan dikumpulkan secara otomatis. Namun dalam kondisi tertentu, log audit keamanan juga dapat dilakukan secara manual menggunakan buku atau kertas formulir. Semua log audit keamanan baik yang dibuat dalam bentuk elektronik maupun non elektronik disimpan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai ketentuan pada bagian 5.5.2.

5.4.1 Jenis Kejadian yang Direkam

PSrE TILAKA mengaktifkan semua fitur audit keamanan dari sistem operasi dan aplikasi PSrE TILAKA sesuai ketentuan CPS. Oleh karena itu, sebagian besar dari kejadian yang teridentifikasi direkam

secara otomatis. PSrE TILAKA memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat Pemilik dicatat dalam log. Setiap rekaman audit (baik direkam dalam bentuk elektronik maupun non elektronik untuk setiap kejadian yang dapat diaudit) sekurang-kurangnya berisi hal berikut:

1. Jenis kejadian;
2. Nomor seri atau urutan rekaman;
3. Tanggal dan waktu kejadian;
4. Sumber perekaman;
5. Indikator sukses atau gagal yang sesuai; dan
6. Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut.

5.4.2 Frekuensi Pemrosesan Log

Log audit ditinjau sesuai dengan prosedur yang berlaku di PSrE TILAKA. Tinjauan tersebut termasuk melakukan verifikasi bahwa log tersebut tidak dirusak, tidak diacak, tidak adanya jenis gangguan lain terhadap log audit, dan kemudian secara singkat personel PSrE TILAKA memeriksa semua entri log dengan cara melakukan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan dalam log. Semua hasil peninjauan akan didokumentasikan.

5.4.3 Periode Retensi Audit Log

Log audit PSrE TILAKA disimpan dengan jangka waktu selama 1 (satu) tahun. Jangka waktu tersebut dapat mengalami perubahan sewaktu-waktu sesuai dengan hukum yang berlaku.

5.4.4 Proteksi Log Audit

Log audit dilindungi untuk mencegah perubahan, mendeteksi gangguan, dan memastikan bahwa hanya akses peran tepercaya yang mampu melakukan operasional PSrE TILAKA tanpa mempengaruhi integritasnya. Perlindungan log audit dilakukan sesuai dengan prosedur yang berlaku di PSrE TILAKA.

5.4.5 Prosedur Cadangan (*Backup*) Log Audit

Log audit PSrE TILAKA dicadangkan (*backup*) sedikitnya 1 (satu) kali dalam 1 (satu) bulan pada media *backup* yang ditempatkan secara lokal pada lokasi yang aman yang sama dengan media penyimpanan utama. Salinan kedua dari log audit diletakkan pada tempat terpisah dari media penyimpanan utama.

5.4.6 Sistem Pengumpulan Audit (Internal vs Eksternal)

PSrE TILAKA mengumpulkan log audit termasuk namun tidak terbatas pada log berikut ini:

1. Aplikasi;
2. *Database*;
3. *Operating System* (OS);
4. Jaringan;
5. *Firewall*;
6. *Fingerprint*;
7. *Closed Circuit Television* (CCTV);
8. *Intrusion Detection System* (IDS)-*Intrusion Prevention System* (IPS);
9. Akses penyedia pusat data;
10. Akses *safety deposit box*; dan
11. Media penyimpanan.

5.4.7 Pemberitahuan ke Subjek Penyebab Kejadian

Tidak ada ketentuan.

5.4.8 Asesmen Kerentanan dan Uji Penetrasi

PSrE TILAKA melakukan penilaian kerentanan sistem 1 (satu) kali dalam 1 (satu) minggu. PSrE TILAKA melakukan kegiatan *penetration test*, *load test*, dan *stress test* 1 (satu) kali dalam 1 (satu) tahun.

5.5 Pengarsipan Catatan (*Record*)

5.5.1 Tipe *Record* yang Diarsipkan

Catatan PSrE TILAKA akan diarsipkan untuk menentukan kesesuaian operasional PSrE TILAKA dan validitas Sertifikat Pemilik yang dikeluarkan oleh PSrE TILAKA, termasuk pada Sertifikat Pemilik yang telah dicabut atau yang telah melewati batas jangka waktu Sertifikat. Data minimal yang diarsipkan adalah sebagai berikut:

1. Data pendaftaran Pemohon atau data pribadi Pemilik;
2. Siklus hidup Sertifikat Pemilik termasuk di dalamnya permohonan penerbitan Sertifikat dan permohonan pencabutan Sertifikat Pemilik;
3. Semua Sertifikat Pemilik dan CRL yang diterbitkan atau dipublikasikan oleh PSrE TILAKA;
4. Data konfigurasi sistem IKP; dan
5. Dokumen CPS yang berlaku, termasuk juga segala perubahan atau adendum terhadap dokumen-dokumen tersebut.

5.5.2 Periode Retensi Arsip

PSrE melakukan pengarsipan atas catatan selama 5 (lima) tahun. PSrE TILAKA akan menyediakan dan memelihara aplikasi yang dibutuhkan untuk membaca catatan yang diarsipkan selama masa retensi. Sertifikat PSrE TILAKA yang telah melewati batas jangka waktu Sertifikat wajib diarsipkan secara permanen.

5.5.3 Perlindungan Arsip

Catatan yang diarsipkan oleh PSrE TILAKA dilindungi dari akses, perubahan, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan yang diarsipkan dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan dipelihara dan disediakan sesuai ketentuan dalam CPS.

5.5.4 Prosedur Cadangan (*Backup*) Arsip

PSrE TILAKA melakukan *backup* arsip yang memadai dan teratur yang telah dilakukan sesuai dengan prosedur yang berlaku di PSrE TILAKA, sehingga jika sistem operasional PSrE TILAKA mengalami kehilangan atau kerusakan arsip utama, maka sistem operasional PSrE TILAKA masih memiliki 1 (satu) set lengkap salinan *backup* yang ditempatkan pada lokasi yang terpisah. Salinan *backup* yang dimaksud mengacu pada ketentuan bagian 5.5.1.

5.5.5 Persyaratan Catatan (*Record*) Stempel Waktu

PSrE TILAKA memberikan label waktu (*timestamp)* pada saat melakukan pengarsipan catatan.

5.5.6 Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip di PSrE TILAKA dilakukan oleh internal personel PSrE TILAKA.

5.5.7 Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Media penyimpanan informasi arsip PSrE TILAKA diperiksa secara berkala 1 (satu) kali dalam 1 (satu) tahun. Sampel dari catatan yang diarsipkan diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya peran terpercaya dan pihak-pihak lain yang berwenang yang telah ditunjuk oleh PSrE TILAKA yang diijinkan untuk dapat mengakses catatan yang diarsipkan. Permintaan untuk mendapatkan dan memverifikasi catatan yang diarsipkan dikoordinasikan oleh peran terpercaya.

5.6 Pergantian Kunci

Kunci Privat PSrE TILAKA diubah secara berkala 1 (satu) kali dalam 10 (sepuluh tahun) untuk meminimalisir risiko kebocoran. Sejak Kunci Privat tersebut diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat Pemilik. Sertifikat PSrE TILAKA yang lama masih berlaku, namun penggunaannya terbatas untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat Pemilik yang ditandatangani menggunakan Kunci Privat pada Sertifikat PSrE TILAKA lama tersebut melewati batas jangka waktu Sertifikat. Jika Kunci Privat lama PSrE TILAKA digunakan untuk menandatangani CRL, maka kunci lama disimpan dan dilindungi. Jika PSrE TILAKA memperbarui Kunci Privat, maka PSrE TILAKA akan memiliki Kunci Publik baru. PSrE TILAKA akan memberitahukan kepada semua Pemilik dan Pihak Pengandal atas pembaharuan terhadap pasangan kunci tersebut.

5.7 Pemulihan Bencana dan Keadaan Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

PSrE TILAKA memiliki rencana tanggap darurat (*business continuity plan*) dan rencana pemulihan bencana (*disaster recovery plan*). Jika Kunci Privat PSrE TILAKA dicurigai telah terkompromi, maka penerbitan Sertifikat Pemilik oleh PSrE TILAKA segera dihentikan. Investigasi independen oleh pihak ketiga dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan diperiksa untuk menentukan prosedur perbaikan yang tepat sesuai dengan prosedur yang berlaku di PSrE TILAKA. Ketentuan pada bagian 5.7.3 akan diterapkan jika terdapat kecurigaan telah terkomprominya Kunci Privat PSrE TILAKA.

5.7.2 Sumber Daya Komputasi, Perangkat Lunak, dan/atau Data Rusak

Ketika peralatan IKP PSrE TILAKA mengalami kerusakan atau berhenti berfungsi, PSrE TILAKA melakukan hal berikut:

1. Memberitahukan kepada PSrE Induk sesuai jangka waktu yang ditentukan oleh prosedur PSrE TILAKA;
2. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir *backup*;
3. Mengoperasikan kembali sistem PSrE TILAKA dengan memprioritaskan kemampuan untuk membangkitkan informasi status Sertifikat Pemilik sesuai jadwal penerbitan CRL; atau
4. Jika kunci penandatanganan PSrE TILAKA rusak, maka operasional PSrE TILAKA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke *restore* pasangan kunci PSrE TILAKA yang terdapat pada media *backup*.

5.7.3 Prosedur Kunci Privat Entitas Terkompromi

Dalam kasus kehilangan Kunci Privat atau bocornya algoritma dan parameter yang digunakan untuk membangkitkan Kunci Privat dan Sertifikat Pemilik, maka PSrE TILAKA:

1. mencabut seluruh Sertifikat Pemilik yang terkait; dan
2. melakukan pembangkitan pasangan kunci dan penerbitan ulang Sertifikat Pemilik yang telah dicabut.

Proses di atas dilakukan tanpa menghentikan layanan.

Dalam kasus kehilangan atau kebocoran Kunci Privat PSrE TILAKA, maka:

1. PSrE TILAKA memberitahukan kepada semua Pemilik Sertifikat;
2. PSrE TILAKA memberitahukan kepada Pihak Pengandal;
3. PSrE TILAKA mencabut seluruh Sertifikat Pemilik;
4. PSrE TILAKA memberitahukan kepada PSrE Induk; dan
5. PSrE Induk mencabut Sertifikat PSrE TILAKA.

Jika Kunci Privat dari PSrE Induk hilang atau bocor, maka PSrE Induk memberitahukan kepada PA dan Pihak Pengandal melalui pengumuman publik. Selanjutnya, PSrE TILAKA:

1. menghentikan layanan;
2. memberitahukan kepada semua Pemilik;
3. melakukan pencabutan semua Sertifikat Pemilik;
4. menerbitkan CRL terbaru; dan
5. memberitahukan kepada kontak-kontak keamanan yang relevan.

Lalu PSrE Induk menyiapkan IKP PSrE Induk dengan pasangan kunci yang baru, kemudian menerbitkan ulang Sertifikat PSrE TILAKA menggunakan kunci PSrE Induk yang baru.

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah Terjadi Bencana

PSrE TILAKA telah menyiapkan suatu rencana pemulihan bencana yang telah diuji, ditinjau ulang, dan diverifikasi 1 (satu) kali dalam 1 (satu) tahun, rencana pemulihan bencana tersebut juga dapat diperbaharui jika dibutuhkan. Layanan kembali pulih dalam kurun waktu 24 (dua puluh empat) jam bila terjadi bencana. Fasilitas *disaster recovery center* PSrE TILAKA tersedia bila fasilitas utama berhenti beroperasi.

5.8 Penutupan PSrE TILAKA atau RA

Apabila PSrE TILAKA akan melakukan pengakhiran kegiatan usahanya, maka PSrE TILAKA melakukan pemberitahuan kepada PSrE Induk dan para Pemilik Sertifikat setelah mendapatkan persetujuan dari PA, sebelum melakukan pengakhiran kegiatan usaha. Pengakhiran kegiatan usaha dilakukan dengan mengikuti langkah-langkah berikut ini:

1. Memberitahukan kepada PSrE Induk, Pemilik, dan Pihak Pengandal;
2. Memberitahukan kepada RA, jika PSrE TILAKA memiliki hubungan kontraktual dengan RA tertentu dalam rangka menjalankan fungsi RA;
3. Menyediakan informasi status Sertifikat Pemilik yang bisa diakses hingga jangka waktu berakhir; dan
4. Menghancurkan sistem IKP yang berisi Kunci Privat PSrE TILAKA.

Apabila PSrE TILAKA melakukan hubungan kontraktual dengan RA tertentu untuk menjalankan fungsi sebagai RA, dan hubungan kontraktual dengan RA akan berakhir, maka pengakhiran hubungan kontraktual dilakukan dengan mengikuti langkah-langkah berikut ini:

1. PSrE TILAKA menutup akses layanan RA ke aplikasi yang mengakomodasi proses permohonan penerbitan Sertifikat;
2. RA mengirimkan pemberitahuan kepada Pemilik bahwa kerja sama antara PSrE TILAKA dan RA telah berakhir, dan menginformasikan bahwa penggunaan Sertifikat Pemilik selanjutnya tetap dapat di lakukan Layanan Tanda Tangan Elektronik Tilaka.

6. Kendali Keamanan Teknis

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan Pasangan Kunci

6.1.1.1 Pembangkitan Pasangan Kunci PSrE

Material kunci kriptografi yang digunakan oleh PSrE TILAKA untuk menandatangani Sertifikat Pemilik, CRL, atau informasi status dibuat di dalam modul kriptografi yang sesuai standar FIPS 140-2 level 3. Kendali multipersonel dibutuhkan untuk pembangkitan pasangan kunci PSrE TILAKA, seperti yang ditentukan pada bagian 6.2.2. Pembangkitan pasangan kunci PSrE TILAKA menghasilkan jejak audit yang dapat diverifikasi yang menunjukkan bahwa persyaratan kebutuhan keamanan telah diikuti berdasarkan dokumentasi pemisahan peran yang tepat. Pihak ketiga yang independen memvalidasi pelaksanaan proses pembangkitan kunci baik dengan menyaksikan pembangkitan kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci.

6.1.1.2 Pembangkitan Pasangan Kunci Pemilik

Pembangkitan pasangan kunci Pemilik dilakukan oleh PSrE TILAKA. PSrE TILAKA membangkitkan kunci menggunakan perangkat keras kriptografis yang tervalidasi FIPS 140-2 level 3.

6.1.2 Pengiriman Kunci Privat ke Pemilik

PSrE TILAKA membangkitkan pasangan kunci atas nama Pemilik. Kunci Privat Pemilik hanya disimpan oleh PSrE TILAKA, tidak dititipkan kepada pihak manapun, dan tidak diserahkan kepada Pemilik. Penggunaan Kunci Privat oleh Pemilik dilakukan melalui Layanan Tanda Tangan Elektronik Tilaka menggunakan multifaktor autentikasi sesuai ketentuan dalam bagian 3.2.1.

6.1.3 Pengiriman Kunci Publik ke Penerbit Sertifikat

Tidak ada ketentuan.

6.1.4 Pengiriman Kunci Publik PSrE kepada Pihak Pengandal

PSrE TILAKA tidak melakukan pengiriman Kunci Publik kepada Pihak Pengandal. Namun Pihak Pengandal dapat mengakses Kunci Publik PSrE TILAKA pada Repositori.

6.1.5 Ukuran Kunci

PSrE TILAKA membuat pasangan kunci menggunakan algoritma RSA dan *Secure Hash Algorithm* (SHA) versi 2 dengan detail sebagai berikut:

Sertifikat	*Digest Algorithm*	*Encryption Algorithm*	
	Tipe	Tipe	Panjang Kunci
PSrE TILAKA	SHA-256	RSA	4096-bit
Pemilik	SHA-256	RSA	2048-bit

6.1.6 Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

PSrE TILAKA membangkitkan pasangan kunci PSrE TILAKA dengan menggunakan modul kriptografi sesuai standar FIPS 140-2 level 3.

6.1.7 Tujuan Penggunaan Kunci (pada *Field Key Usage*-X509 V3)

Penggunaan sebuah kunci spesifik ditentukan oleh *key usage extension* dalam Sertifikat X.509. Kunci PSrE TILAKA digunakan untuk *Digital Signature*, *Key Certificate Sign*, dan *CRL Sign*. Kunci Pemilik digunakan untuk *Digital Signature* dan *Non-Repudiation*.

6.2 Kendali Kunci Privat dan Kendali Teknis Modul Kriptografi

6.2.1 Kendali dan Standar Modul Kriptografi

PSrE TILAKA menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 level 3 untuk operasionalnya.

6.2.2 Kendali Multipersonel (n of m) Kunci Privat

Semua Kunci Privat PSrE TILAKA diakses melalui kendali multipersonel seperti yang ditentukan pada bagian 5.2.2.

6.2.3 Penitipan Kunci Privat

Kunci Privat PSrE TILAKA tidak dititipkan.

6.2.4 Cadangan (*Backup*) Kunci Privat

Kunci Privat PSrE TILAKA dicadangkan (*backup*) di bawah kendali multipersonel yang sama dengan kunci yang asli. Ada 1 (satu) salinan dari Kunci Privat yang tersimpan di lokasi yang berbeda dengan lokasi utama (*data center*). Semua salinan Kunci Privat PSrE TILAKA dilindungi dengan cara yang sama dengan aslinya.

6.2.5 Pengarsipan Kunci Privat

Kunci Privat PSrE TILAKA tidak diarsipkan.

6.2.6 Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci Privat PSrE TILAKA diekspor dari modul kriptografi hanya untuk proses *backup*. Kunci Privat PSrE TILAKA tidak pernah sekalipun berada dalam bentuk *plaintext* di luar modul kriptografi. Jika sebuah Kunci Privat dipindahkan dari satu modul kriptografi ke yang lain, maka Kunci Privat dienkripsi selama pemindahan. *Smart card* yang digunakan untuk proses enkripsi Kunci Privat PSrE TILAKA dilindungi dengan menggunakan PIN.

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografi

Kunci Privat PSrE TILAKA disimpan pada modul kriptografi FIPS 140-2 level 3, dalam bentuk yang terenkripsi dan terlindungi oleh PIN.

6.2.8 Metode Pengaktifan Kunci Privat

Aktivasi operasi Kunci Privat PSrE TILAKA dilakukan oleh peran terpercaya dan memerlukan kendali multipersonel seperti yang dinyatakan dalam bagian 5.2.2.

6.2.9 Metode Penonaktifan Kunci Privat

Jika terdapat situasi yang mengharuskan Kunci Privat PSrE TILAKA dinonaktifkan, maka proses penonaktifan dilakukan oleh peran terpercaya sesuai dengan prosedur yang berlaku di PSrE TILAKA.

6.2.10 Metode Penghancuran Kunci Privat

Peran terpercaya akan menghancurkan Kunci Privat dengan cara menginisialisasi modul kriptografis serta *backup*nya dengan fungsi *factory reset* ketika Kunci Privat PSrE TILAKA tidak diperlukan lagi. Proses penghancuran Kunci Privat PSrE TILAKA dicatat ke dalam barang bukti sesuai dengan bagian 5.4.

6.2.11 Pemeringkatan Modul Kriptografis

Seperti diuraikan dalam bagian 6.2.1.

6.3 Aspek Lain dari Manajemen Pasangan Kunci

6.3.1 Pengarsipan Kunci Publik

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasional Sertifikat PSrE TILAKA dan pasangan kunci PSrE TILAKA berlangsung selama 10 (sepuluh) tahun dan 1 (satu) tahun untuk Sertifikat Pemilik.

6.4 Data Aktivasi

6.4.1 Pembuatan dan Instalasi Data Aktivasi

Data aktivasi dibuat secara otomatis oleh HSM yang melibatkan peran terpercaya. Detail pembuatan data aktivasi mengacu pada prosedur yang berlaku di PSrE TILAKA.

6.4.2 Perlindungan Data Aktivasi

Data aktivasi PSrE TILAKA dilindungi dari pengungkapan kerahasiaan, perlindungan diberikan melalui kombinasi antara kriptografi dan mekanisme kendali akses fisik. Data aktivasi untuk perangkat HSM dilindungi seperti ketentuan dalam bagian 6.2.2. PSrE TILAKA menyimpan data aktivasi dalam bentuk *smart card* dengan perlindungan PIN.

6.4.3 Aspek Lain dari Data Aktivasi

Tidak ada ketentuan.

6.5 Kendali Keamanan Komputer

6.5.1 Persyaratan Teknis Keamanan Komputer Khusus

PSrE TILAKA memastikan bahwa sistem yang menjaga perangkat lunak dan dokumen milik PSrE TILAKA aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem PSrE TILAKA telah dikonfigurasi dan dikuatkan menggunakan praktik terbaik.

Fungsi-fungsi keamanan komputer berikut dapat disediakan oleh sistem operasi, atau melalui suatu kombinasi dari sistem operasi, perangkat lunak, dan perlindungan fisik. Fungsi tersebut mencakup namun tidak terbatas pada:

1. Membutuhkan *login* terautentikasi yang dilengkapi dengan MFA;
2. Menyediakan *role-based access control*;
3. Menyediakan kapabilitas audit keamanan;

4. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data; dan
5. Menyediakan perlindungan mandiri untuk sistem operasi.

Untuk mendukung persyaratan penjaminan keamanan komputer, PSrE TILAKA beroperasi sesuai konfigurasi yang telah dievaluasi oleh personel PSrE TILAKA yang bertanggung jawab atas keamanan informasi.

6.5.2 Peringkat Keamanan Komputer

Tidak ada ketentuan.

6.6 Kendali Teknis Siklus Hidup

6.6.1 Kendali Pengembangan Sistem

Tidak ada ketentuan.

6.6.2 Kendali Manajemen Keamanan

Konfigurasi, modifikasi, dan peningkatan sistem PSrE TILAKA didokumentasikan dan dikontrol oleh manajemen PSrE TILAKA. Jika terdapat modifikasi yang tidak sah baik pada perangkat lunak maupun konfigurasi, maka PSrE TILAKA dapat mendeteksi hal tersebut sesuai dengan prosedur yang berlaku di PSrE TILAKA.

6.6.3 Kendali Keamanan Siklus Hidup

PSrE TILAKA melakukan pengawasan terhadap kebutuhan skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak yang telah dievaluasi dan disertifikasi.

6.7 Kendali Keamanan Jaringan

PSrE TILAKA menerapkan langkah-langkah keamanan jaringan yang sesuai dengan prosedur yang berlaku di PSrE TILAKA untuk memastikan bahwa sistem telah terjaga dari *denial of service* dan serangan intrusi. Tindakan tersebut mencakup penggunaan *firewall* dan *router* penyaring. *Port* jaringan dan layanan yang tidak dipakai dimatikan. Setiap perangkat lunak jaringan yang ada dipastikan berfungsi.

6.8 Stempel Waktu

Semua komponen PSrE TILAKA secara berkala disinkronisasikan dengan sebuah layanan waktu yang menggunakan *Network Time Protocol* (NTP). Waktu yang telah disinkronisasikan tersebut digunakan untuk menentukan waktu pada saat:

1. Validitas waktu permulaan untuk sebuah Sertifikat PSrE TILAKA;
2. Pencabutan Sertifikat PSrE TILAKA;
3. Pembaruan CRL dan OCSP; dan
4. Penerbitan Sertifikat Pemilik.

Proses sinkronisasi terhadap layanan waktu yang menggunakan *Network Time Protocol* (NTP) dipertahankan sesuai dengan prosedur yang berlaku di PSrE TILAKA. Proses sinkronisasi tersebut merupakan sebuah aktivitas yang dapat diaudit.

7. Profil OCSP, CRL dan Sertifikat

7.1 Profil Sertifikat

Profil Sertifikat mengikuti standar RFC 5280 "*Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*". PSrE TILAKA melakukan peninjauan terhadap profil Sertifikat secara berkala minimal 1 (satu) kali dalam 1 (satu) tahun.

7.1.1 Nomor Versi

PSrE TILAKA menerbitkan Sertifikat X.509 v3 (mengisi versi *field* dengan integer "2").

7.1.2 Ekstensi Sertifikat

PSrE TILAKA menggunakan ekstensi Sertifikat standar yang mematuhi RFC 5280.

7.1.2.1 *Key Usage*

Sertifikat X.509 Versi 3 diisi sesuai dengan RFC 5280: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. *Field criticality* dari ekstensi *Key Usage* diisi *TRUE*. *Key Usage* untuk semua kelas Sertifikat Pemilik yaitu *Digital Signature* dan *Non-Repudiation*.

Field	Sertifikat PSrE 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*

7.1.2.2 *Certificate Policies Extension*

Ekstensi *Certificate Policy* dari Sertifikat X.509 Versi 3 diisi dengan pengidentifikasi objek CPS sesuai dengan bagian 7.1.6 dan dengan kualifikasi kebijakan yang ditentukan dalam bagian 7.1. *Field criticality* dari ekstensi ini diisi *FALSE*.

7.1.2.3 *Basic Constraint*

Ekstensi *Basic Constraints* Sertifikat X.509 Versi 3 bagi Sertifikat PSrE TILAKA memiliki *field* CA yang diisi *TRUE* dan ekstensi *Basic Constraints* Sertifikat Pemilik memiliki *field* CA yang diisi *FALSE*. *Field criticality* dari ekstensi ini diisi *TRUE* untuk Sertifikat PSrE TILAKA dan diisi *TRUE* atau *FALSE* untuk Sertifikat Pemilik.

7.1.2.4 *Extended Key Usage*

Secara baku, *Extended Key Usage* diatur sebagai suatu ekstensi non-kritikal. Sertifikat PSrE TILAKA dapat memuat ekstensi *Extended Key Usage* sebagai suatu bentuk dari pembatasan teknis pada penggunaan Sertifikat-Sertifikat yang diterbitkan. Sertifikat Pemilik mengandung sebuah ekstensi *Extended Key Usage* untuk tujuan bahwa Sertifikat tersebut telah diterbitkan untuk Pemilik, dan tidak memuat nilai anyEKU. *Extended Key Usage* untuk semua kelas Sertifikat Pemilik yaitu *PDF Signing*.

7.1.2.5 *CRL Distribution Points*

Sertifikat X.509 Versi 3 diisi dengan suatu ekstensi *CRL Distribution Points* yang memuat URL dari lokasi dimana Pihak Pengandal dapat memperoleh suatu CRL untuk memeriksa status Sertifikat Pemilik. *Field criticality* dari ekstensi ini diisi *FALSE*.

7.1.2.6 *Authority Key Identifier*

Sertifikat X.509 Versi 3 diisi dengan ekstensi *Authority Key Identifier*. Metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik dari PSrE TILAKA telah dihitung sesuai dengan metode yang diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini diisi *FALSE*.

7.1.2.7 *Subject Key Identifier*

Dalam Sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini diisi dengan *FALSE* dan metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik subyek Sertifikat dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.

7.1.3 Pengidentifikasi 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}.

7.1.4 Format Nama

Sesuai konvensi penamaan dan batasan yang tercantum pada bagian 3.1.

7.1.5 Batasan Nama

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1.

7.1.6 Pengidentifikasi Objek Kebijakan Sertifikat

Sertifikat yang diterbitkan di bawah CPS menggunakan nomor OID yang sesuai dengan ketentuan yang diatur dalam bagian 1.2.

7.1.7 Penggunaan Ekstensi Batasan Kebijakan

Tidak ada ketentuan.

7.1.8 Sintaks dan Semantik Kualifer Kebijakan

Tidak ada ketentuan.

7.1.9 Semantik Pemrosesan bagi Ekstensi Kebijakan Sertifikat Kritis

Tidak ada ketentuan.

7.2 Profil CRL

7.2.1 Nomor Versi

PSrE TILAKA menerbitkan CRL X.509 versi 2.

7.2.2 CRL dan Ekstensi Entri CRL

PSrE TILAKA menggunakan CRL RFC 5280 dan ekstensi entri CRL.

7.3 Profil OCSP

Online Certificate Status Protocol (OCSP) yang diatur oleh PSrE TILAKA patuh terhadap standar RFC 6960 atau RFC 5019.

7.3.1 Nomor Versi

PSrE TILAKA menerbitkan respon OCSP versi 1.

7.3.2 Ekstensi OCSP

Tidak ada ketentuan.

8. Audit Kepatuhan dan Penilaian Lain

Semua kebijakan yang terdapat dalam CPS mencakup semua bagian yang relevan dari standar IKP yang saat ini diterapkan untuk berbagai macam industri IKP vertikal, dimana industri-industri tersebut membutuhkan PSrE TILAKA agar bisa beroperasi. PSrE TILAKA akan menjalani audit kepatuhan serta menyampaikan laporan secara berkala sesuai dengan ketentuan peraturan perundang-undangan mengenai PSrE.

8.1 Frekuensi atau Keadaan Asesmen

PSrE TILAKA menjalani audit kepatuhan dan menyampaikan laporan berkala dalam jangka waktu minimal 1 (satu) kali dalam 1 (satu) tahun sesuai dengan yang dipersyaratkan oleh peraturan perundang-undangan mengenai PSrE dan setiap terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan. Selain itu PSrE TILAKA juga menjalani Audit Sistem Manajemen Keamanan Informasi dengan menggunakan krtiteria ISO/IEC 27001 minimal 1 (satu) kali dalam 1 (satu) tahun.

8.2 Identitas/Kualifikasi Asesor

Auditor menunjukkan kompetensi pada bidang audit kepatuhan, dan benar-benar memahami persyaratan CPS. Auditor kepatuhan melakukan audit kepatuhan sebagai tanggung jawab utama.

Auditor kepatuhan memiliki kualifikasi sebagai berikut:

a. Audit dilaksanakan oleh tim asesmen independen yang *qualified*;
b. Auditor memiliki pengetahuan yang cukup tentang tanda tangan elektronik, Sertifikat, X.509 versi 3 *PKI Certificate Policy and Certification Practice Framework*, dan peraturan perundang-undangan mengenai PSrE;
c. Auditor memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
d. Auditor memiliki bukti bahwa dirinya memenuhi kualifikasi auditor yang dapat dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah; dan
e. Auditor menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan karyawan yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

8.3 Hubungan Asesor ke Entitas yang Dinilai

PSrE TILAKA memilih auditor/asesor yang independen.

8.4 Topik yang Dicakup oleh Asesmen

Audit yang dilaksanakan memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema audit yang terbaru berlaku pada tahun berikutnya.

8.5 Tindakan Yang Diambil Sebagai Hasil Dari Kekurangan

Ketika auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana PSrE TILAKA dirancang atau dioperasikan atau dipelihara dengan persyaratan CPS yang berlaku, maka PSrE TILAKA akan melakukan tindakan berikut:

1. Auditor kepatuhan memberitahukan kepada PSrE TILAKA tentang ketidaksesuaian;
2. PSrE TILAKA bertanggung jawab untuk memperbaiki ketidaksesuaian dengan menentukan tindakan lebih lanjut yang diperlukan sesuai dengan persyaratan CPS, dan kemudian melakukan tindakan tersebut tanpa penundaan.

8.6 Komunikasi Hasil

Laporan kepatuhan audit, termasuk identifikasi tindakan perbaikan yang dilakukan, diberikan kepada PA PSrE TILAKA sebagaimana diatur dalam bagian 8.1. Laporan tersebut mengidentifikasi versi CPS yang digunakan dalam penilaian. PSrE TILAKA mengomunikasikan hasil audit kepada personel PSrE TILAKA dan melakukan perbaikan.

8.7 Audit Internal

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan risiko gangguan pada proses bisnis. Audit internal dilaksanakan minimal 1 (satu) kali dalam 1 (satu) tahun.

9. Bisnis Lain dan Masalah Hukum

9.1 Biaya

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat

PSrE TILAKA dapat mengenakan biaya untuk penerbitan dan penerbitan ulang Sertifikat Pemilik. PSrE TILAKA menyediakan keterangan terkait detail biaya penerbitan dan penerbitan ulang Sertifikat Pemilik pada Repositori.

9.1.2 Biaya Pengaksesan Sertifikat

PSrE TILAKA tidak mengenakan biaya kepada Pemilik untuk mengakses Sertifikat Pemilik.

9.1.3 Biaya Pengaksesan Informasi Status atau Pencabutan

PSrE TILAKA tidak akan mengenakan biaya dalam proses pengaksesan terhadap CRL atau OCSP *responder*.

9.1.4 Biaya Layanan Lainnya

PSrE TILAKA dapat mengenakan biaya dalam hal penyediaan layanan tambahan lainnya. PSrE TILAKA menyediakan keterangan terkait detail biaya dalam penyediaan layanan tambahan lainnya pada Repositori.

9.1.5 Kebijakan Pengembalian

PSrE TILAKA tidak menyediakan pengembalian biaya untuk semua Layanan Tanda Tangan Elektronik Tilaka.

9.2 Tanggung Jawab Keuangan

9.2.1 Cakupan Asuransi

PSrE TILAKA menjamin kerugian akibat kesengajaan atau kelalaian kepada Pelanggan karena kegagalannya dalam mematuhi kewajiban yang ditentukan dalam dokumen Kebijakan Jaminan yang tercantum pada Repositori.

9.2.2 Aset Lainnya

Tidak ada ketentuan.

9.2.3 Jaminan Asuransi atau Garansi untuk Entitas Akhir

PSrE TILAKA memberikan jaminan atas kerugian dengan besaran yang telah diatur dalam dokumen Kebijakan Jaminan yang tercantum pada Repositori.

9.3 Kerahasiaan Informasi Bisnis

9.3.1 Cakupan Informasi Rahasia

PSrE TILAKA memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia dan terbatas. Yang termasuk dalam kategori informasi rahasia dan terbatas antara lain:

1. Informasi pribadi sebagaimana dijabarkan pada bagian 9.4;
2. Rekam jejak audit (*audit logs*) dari sistem PSrE TILAKA;
3. Data aktivasi pada saat pengaktifan Kunci Privat PSrE TILAKA sebagaimana dijabarkan pada bagian 6.4;
4. Dokumentasi bisnis proses PSrE TILAKA termasuk dokumen *business continuity plan* dan *disaster recovery plan*;
5. Laporan audit dari auditor independen sebagaimana dijabarkan pada bagian 8;
6. Kunci Privat PSrE TILAKA dan Kunci Privat Pemilik; dan
7. Dokumen rahasia dan terbatas lainnya sesuai dengan prosedur yang berlaku di PSrE TILAKA.

9.3.2 Informasi yang Tidak dalam Cakupan Informasi yang Rahasia

Informasi yang tidak termasuk pada bagian 9.3.1 dianggap informasi publik.

9.3.3 Tanggung Jawab untuk Melindungi Informasi yang Rahasia

PSrE TILAKA melindungi informasi rahasia. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:

1. Pelatihan atau peningkatan *awareness*;
2. Kontrak kerja dengan karyawan; dan
3. *Non-Disclosure Agreement* (NDA) dengan karyawan dan rekanan.

9.4 Privasi Informasi Pribadi

9.4.1 Rencana Privasi

PSrE TILAKA akan melindungi informasi pribadi Pemilik sesuai dengan ketentuan yang telah diatur dalam Kebijakan Privasi yang terdapat pada Repositori.

9.4.2 Informasi yang Dianggap Pribadi

PSrE TILAKA melindungi semua informasi pribadi Pemilik (termasuk yang telah diarsipkan) dari pengungkapan yang tidak sah, baik informasi yang diberikan pada saat pendaftaran maupun informasi yang diperoleh pada saat menggunakan Layanan Tanda Tangan Elektronik Tilaka. Informasi pribadi Pemilik (termasuk yang telah diarsipkan) tidak dapat diungkapkan kecuali yang diizinkan pada bagian 9.4.1.

9.4.3 Informasi yang Tidak Dianggap Pribadi

Informasi yang terdapat pada bagian 7 tidak dianggap sebagai informasi rahasia.

9.4.4 Tanggung Jawab Melindungi Informasi Pribadi

PSrE TILAKA menyimpan informasi pribadi secara aman sesuai dengan ketentuan yang telah diatur dalam Kebijakan Privasi yang terdapat pada Repositori. Informasi dalam bentuk elektronik maupun kertas disimpan sesuai dengan prosedur yang berlaku di PSrE TILAKA. *Backup* informasi pribadi selalu dienkripsi setiap kali dipindahkan ke media *backup*.

9.4.5 Catatan dan Persetujuan untuk Memakai Informasi Pribadi

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia, sehingga perlu persetujuan dari Pemohon untuk menggunakan informasi tersebut. Ketentuan terkait penggunaan informasi pribadi sesuai dengan ketentuan yang telah diatur dalam Perjanjian Pemilik Sertifikat dan Kebijakan Privasi yang terdapat pada Repositori.

9.4.6 Pengungkapan Berdasarkan Proses Peradilan atau Administratif

PSrE TILAKA tidak akan membuka informasi pribadi kepada pihak ketiga manapun kecuali ditentukan lain oleh CPS atau yang diatur dalam peraturan perundang-undangan yang berlaku.

9.4.7 Keadaan Pengungkapan Informasi Lain

Tidak ada ketentuan.

9.5 Hak atas Kekayaan Intelektual

Semua hak kekayaan intelektual PSrE TILAKA termasuk namun tidak terbatas pada merek dagang, hak cipta, dan semua dokumen PSrE TILAKA tetap menjadi milik dari PSrE TILAKA.

9.6 Pernyataan dan Jaminan PSrE

9.6.1 Pernyataan dan Jaminan PSrE

PSrE TILAKA menyatakan dan menjamin bahwa:

1. PSrE TILAKA mematuhi ketentuan yang diatur dalam CPS;
2. PSrE TILAKA menerbitkan dan memperbarui CRL secara berkala;
3. seluruh Sertifikat Pemilik yang diterbitkan memenuhi syarat yang diatur berdasarkan CPS; dan
4. PSrE TILAKA menampilkan informasi yang dapat diakses secara publik pada Repositori.

9.6.2 Pernyataan dan Jaminan RA

RA menyatakan dan menjamin bahwa:

1. tidak ada kekeliruan fakta dalam Sertifikat Pemilik yang diketahui oleh atau berasal dari RA;
2. tidak ada kesalahan informasi dalam Sertifikat Pemilik yang dilakukan oleh RA sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat Pemilik; dan
3. kegiatan pendaftaran dilakukan sesuai dengan CPS dan perjanjian kerja sama.

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat

Pemilik menjamin bahwa:

1. setiap Sertifikat yang dibuat menggunakan pasangan kunci berisi tanda tangan elektronik dan Sertifikat yang sudah disetujui oleh Pemilik, serta secara operasional Sertifikat tersebut belum dicabut dan belum melewati batas jangka waktu pada saat tanda tangan elektronik digunakan;
2. Kunci Privat Pemilik disimpan dan diamankan oleh PSrE TILAKA dan hanya Pemilik yang boleh mengakses Kunci Privat;
3. Pemilik sudah melakukan pemeriksaan terhadap informasi yang terdapat pada Sertifikat sebelum menyetujui Sertifikat;
4. semua informasi yang diberikan oleh Pemilik dan informasi yang berada di dalam Sertifikat adalah benar;
5. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kegunaan yang ada dalam CPS;
6. segera:
    a. melakukan permohonan pencabutan Sertifikat dan mengakhiri penggunaan Sertifikat serta Kunci Privat yang terasosiasi dengan Sertifikat Pemilik, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari Kunci Privat;

b. mengajukan permohonan pencabutan Sertifikat jika terdapat informasi yang tidak sesuai di dalam Sertifikat tersebut; dan
c. menghentikan penggunaan Kunci Privat yang Kunci Publiknya tercantum dalam Sertifikat yang telah dicabut;

7. menanggapi instruksi yang telah diberikan oleh PSrE TILAKA terkait *compromise* atau penyalahgunaan Sertifikat selambat-lambatnya 48 (empat puluh delapan) jam setelah instruksi tersebut diberikan;
8. menyetujui dan menerima bahwa PSrE TILAKA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat Pemilik jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam dokumen Perjanjian Pemilik Sertifikat di Repositori atau jika PSrE TILAKA menemukan bahwa Sertifikat Pemilik tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan, atau pendistribusian *malware*; dan
9. Pemilik merupakan pengguna akhir dan bukan merupakan PSrE, dan tidak menggunakan Kunci Privat yang Kunci Publiknya tercantum dalam Sertifikat untuk tujuan penandatanganan Sertifikat PSrE lain.

9.6.4 Pernyataan dan Jaminan Pihak Pengandal

Pihak yang mengandalkan Sertifikat Pemilik menjamin bahwa:

1. memiliki kemampuan teknis untuk memverifikasi Sertifikat Pemilik;
2. melakukan verifikasi informasi yang tercantum di dalam Sertifikat Pemilik, sebelum informasi tersebut digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut;
3. melaporkan kepada PSrE TILAKA melalui *email*, jika menyadari atau mencurigai bahwa telah terjadi kebocoran Kunci Privat;
4. telah memiliki cukup informasi untuk membuat keputusan apakah akan bergantung atau tidak pada informasi dalam Sertifikat Pemilik, dan menanggung konsekuensi hukum apabila tidak mematuhi kewajiban Pihak Pengandal yang ada pada CPS; dan
5. mematuhi ketentuan yang ditetapkan di CPS dan dokumen Perjanjian Pihak Pengandal yang terdapat pada Repositori.

9.6.5 Pernyataan dan Jaminan Partisipan Lain

Tidak ada ketentuan.

9.7 Pelepasan Jaminan

PSrE TILAKA tidak menjamin:

1. jika penggunaan Sertifikat Pemilik tidak sesuai *Key Usage* seperti yang tercantum pada bagian 1.4.1 dengan ketentuan detail sebagai berikut:
   a. Pemberian jaminan sesuai dengan dokumen Kebijakan Jaminan yang tercantum pada https://repository.tilaka.id/ tidak akan diberikan kepada Pelanggan jika dalam penggunaan Sertifikat oleh Pemilik tidak sesuai *Key Usage*;
   b. Pemberian jaminan sesuai dengan dokumen Perjanjian Pihak Pengandal yang tercantum pada https://repository.tilaka.id/ tidak akan diberikan kepada Pihak Pengandal jika dalam penggunaan Sertifikat oleh Pemilik tidak sesuai *Key Usage*.
2. keakuratan, keaslian, kelengkapan, atau kesesuaian dari setiap informasi yang ada dalam demo atau *testing* Sertifikat Pemilik; dan
3. kecuali untuk jaminan yang telah tercantum dalam CPS, dokumen Kebijakan Jaminan di Repositori, dan perjanjian kerja sama dan sepanjang diizinkan oleh hukum, PSrE TILAKA mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan, atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu.

9.8 Pembatasan Tanggung Jawab

9.8.1 Pembatasan Tanggung Jawab PSrE

PSrE TILAKA tidak bertanggung jawab atas penggunaan Sertifikat Pemilik yang tidak tepat, termasuk:

1. semua kerusakan yang dihasilkan dari penggunaan Sertifikat Pemilik atau pasangan kunci dengan cara lain selain yang didefinisikan dalam CPS, dokumen Kebijakan Jaminan di Repositori, perjanjian kerja sama, atau yang diatur dalam Sertifikat Pemilik itu sendiri;
2. semua kerusakan yang disebabkan oleh *force majeure*; dan
3. semua kerusakan yang disebabkan oleh *malware* (seperti virus atau *trojan*) di luar perangkat PSrE TILAKA.

9.8.2 Pembatasan Tanggung Jawab RA

RA tidak bertanggung jawab atas hal lain yang tidak disebutkan pada bagian 9.6.2.

9.9 Ganti Rugi

9.9.1 Ganti Rugi oleh PSrE TILAKA

Kebijakan ganti rugi oleh PsrE TILAKA mengacu pada dokumen Kebijakan Jaminan yang tercantum pada Repositori.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat

Kebijakan ganti rugi oleh Pemilik Sertifikat mengacu pada dokumen Perjanjian Pemilik Sertifikat yang tercantum pada Repositori.

9.9.3 Ganti Rugi oleh Pihak Pengandal

Kebijakan ganti rugi oleh Pihak Pengandal mengacu pada dokumen Perjanjian Pihak Pengandal yang tercantum pada Repositori.

9.10 Jangka Waktu dan Pengakhiran

9.10.1 Jangka Waktu

CPS dinyatakan tetap berlaku sampai terdapat pemberitahuan lebih lanjut oleh PSrE TILAKA melalui *email* dan Repositori.

9.10.2 Pengakhiran

Pada saat berakhirnya CPS, maka:

1. seluruh Sertifikat Pemilik yang diterbitkan dalam masa berlaku CPS, tetap mengacu pada CPS tersebut sampai dengan berakhirnya masa validitas Sertifikat Pemilik; dan
2. perubahan CPS ditandai dengan perubahan nomor versi yang jelas.

9.10.3 Efek Pengakhiran dan Keberlangsungan

PSrE TILAKA mengomunikasikan kondisi akibat dari penghentian CPS dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit melalui *email* dan Repositori.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

PSrE TILAKA menyediakan media komunikasi bagi para pihak terkait melalui *email* atau telepon. PSrE TILAKA akan memberikan tanggapan selambat-lambatnya 20 (dua puluh) hari kerja setelah mendapatkan informasi. Komunikasi yang ditujukan kepada PSrE TILAKA dialamatkan sesuai dengan ketentuan pada bagian 1.5.2.

9.12 Amandemen

9.12.1 Prosedur untuk Amandemen

PSrE TILAKA melakukan publikasi melalui Repositori dan melakukan pemberitahuan melalui *email* kepada Pemilik terkait perubahan besar atau signifikan dari CPS termasuk juga keterangan waktu ketika CPS hasil amandemen efektif berlaku. Amandemen CPS dilakukan sesuai dengan prosedur yang berlaku di PSrE TILAKA.

9.12.2 Periode dan Mekanisme Pemberitahuan

Ketika terjadi perubahan, CPS dipublikasikan selambat-lambatnya 7 (tujuh) hari kalender sejak tanggal ditandatangani melalui Repositori dan diberitahukan melalui *email* kepada Pemilik.

9.12.3 Keadaan Dimana OID Diubah

OID dapat mengalami perubahan setelah mendapatkan persetujuan dari PA, jika terdapat:

1. perubahan model bisnis PSrE TILAKA; atau
2. perubahan peraturan dari PSrE Induk.

9.13 Ketentuan Penyelesaian Sengketa

Jika terdapat sengketa terkait dengan penafsiran atau pelaksanaan dari CPS, maka para pihak sepakat untuk menyelesaikan secara musyawarah untuk mufakat. Apabila penyelesaian secara musyawarah untuk mufakat tersebut tidak tercapai, maka para pihak sepakat untuk menyelesaikannya melalui Pengadilan Negeri Jakarta Selatan sesuai domisili PSrE TILAKA.

9.14 Hukum yang Mengatur

CPS menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat Pemilik ataupun produk/layanan lainnya. Termasuk apabila Sertifikat Pemilik dipakai untuk kebutuhan komersil di negara lain, aturan hukum di Indonesia akan tetap diterapkan. Para pihak, termasuk PSrE TILAKA, rekanan, Pemilik, dan Pihak Pengandal tidak dapat membatalkan acuan hukum yang telah ditentukan di atas.

9.15 Kepatuhan atas Hukum yang Berlaku

PSrE TILAKA mematuhi hukum yang berlaku di Indonesia. Para pihak termasuk PSrE TILAKA, rekanan, Pemilik, dan Pihak Pengandal sepakat untuk mematuhi peraturan perundang-undangan dan regulasi yang berlaku di Indonesia.

9.16 Ketentuan yang Belum Diatur

9.16.1 Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2 Pengalihan Hak

Seluruh entitas yang beroperasi di bawah CPS tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari PSrE TILAKA.

9.16.3 Keterpisahan

Jika terdapat ketentuan dari CPS, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, maka bagian CPS selanjutnya ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CPS yang menjelaskan batasan tanggung jawab, dimaksudkan dapat dipisahkan dan bersifat independen dari ketentuan lain dan diberlakukan dengan sebagaimana harusnya.

9.16.4 Penegakan Hukum (Biaya Pengacara dan Pengalihan Hak-Hak)

PSrE TILAKA dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan PSrE TILAKA dalam menerapkan klausul ini dalam 1 (satu) kasus tidak menghilangkan hak PSrE TILAKA untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CPS. Segala hal terkait pelepasan hak dalam pengadilan disampaikan secara tertulis dan ditandatangani oleh PSrE TILAKA.

9.16.5 Keadaan Memaksa

PSrE TILAKA tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam melaksanakan CPS yang disebabkan oleh hal-hal yang berada di luar kendali yang wajar yang terjadi secara bersamaan di lokasi *data center* dan *disaster recovery center*, termasuk namun tidak terbatas pada tindakan otoritas sipil atau militer, bencana alam (seperti banjir dan gempa bumi), kebakaran, epidemi, kerusuhan, perang, sabotase, terorisme, pemadaman listrik secara terus menerus, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga.

9.17 Provisi Lain

Tidak ada ketentuan.

10. Lampiran

Lampiran I Tabel Akronim

Istilah	Definisi
API	*Application Programming Interface*
CA	*Certificate Authority*
CP	*Certificate Policy*
CPS	*Certification Practice Statement*
CRL	*Certificate Revocation List*
EV	*Extended Validation*
FIPS	*Federal Information Processing Standards*
HSM	*Hardware Security Module*
IKP	Infrastruktur Kunci Publik
Kemenkominfo	Kementerian Komunikasi dan Informatika
MFA	*Multi Factor Authentication*
NDA	*Non-Disclosure Agreement*
NIB	Nomor Induk Berusaha
NIK	Nomor Induk Kependudukan
NPWP	Nomor Pokok Wajib Pajak
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OTP	*One Time Password*
PA	Policy Authority
PIN	*Personal Identification Number*
PSrE	Penyelenggara Sertifikasi Elektronik
RA	*Registration Authority*
RFC	*Request for Command*
URL	*Uniform Resource Locator*

Lampiran II Tabel Definisi

Istilah	Definisi
Admin Korporat	Perwakilan dari Pelanggan Korporasi yang bertanggung jawab untuk mengirimkan permohonan penerbitan Sertifikat Pemilik dan mengelola akses akun Pemilik pada Layanan Tanda Tangan Elektronik Tilaka.
Admin Tilaka	Personel PSrE TILAKA yang bertugas untuk mengelola akun Admin Korporat dan Pemilik.
IKP Indonesia	Seperangkat perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan, dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan Sertifikat dan kunci yang dapat dipercaya berdasarkan pada kriptografi Kunci Publik sesuai peraturan Indonesia.
Kebijakan Jaminan	Ketentuan mengenai cara PSrE TILAKA memberikan batasan jaminan kepada Pelanggan. Kebijakan Jaminan tersedia di Repositori.
Kebijakan Privasi	Ketentuan mengenai cara PSrE TILAKA memperoleh, mengumpulkan, mengolah, menyimpan, menampilkan, mengumumkan, mengirimkan, dan memusnahkan data pribadi Pemilik Layanan Tanda Tangan Elektronik Tilaka. Kebijakan Privasi tersedia di Repositori.
Kebocoran Kunci/*Key Compromise*	Kunci Privat dikatakan terkompromi jika nilainya telah diungkapkan kepada orang yang tidak berkepentingan, orang yang tidak sah memiliki akses ke sana, atau ada praktek teknis yang memungkinkan orang yang tidak berwenang mendapatkan nilainya.
Kompromi/*Compromise*	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif.
Kunci Privat	Kunci dari pasangan kunci yang dirahasiakan oleh pemegang pasangan kunci, serta yang digunakan untuk membuat tanda tangan elektronik dan/atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.

Istilah	Definisi
Kunci Publik	Kunci dari pasangan kunci yang dapat diungkapkan secara terbuka oleh pemegang kunci pribadi terkait, serta yang digunakan oleh pihak yang mengandalkan untuk memverifikasi tanda tangan elektronik yang dibuat dengan kunci pribadi dan/atau untuk mengenkripsi pesan pemiliknya sehingga dapat didekripsi hanya dengan Kunci Privat yang sesuai.
Layanan Tanda Tangan Elektronik Tilaka	Aplikasi yang digunakan untuk mengakomodir layanan tanda tangan elektronik yang dapat diakses secara langsung melalui URL: https://corporate.tilaka.id/ca-corporate-portal/login.xhtml atau melalui aplikasi yang dibuat, dikelola, dikembangkan, atau dimiliki oleh pihak ketiga yang memiliki hubungan kontraktual dengan PSrE TILAKA.
Otoritas Pendaftaran (RA)	Pihak yang menjalankan fungsi untuk melakukan verifikasi dan validasi data identitas Pemohon, memulai dan/atau memproses permohonan penerbitan, pencabutan, dan/atau penerbitan ulang Sertifikat Pemilik. Dalam hal permohonan penerbitan, pencabutan, dan/atau penerbitan ulang Sertifikat Pemilik oleh Pemohon diterima secara langsung oleh PSrE TILAKA, maka dalam hal ini PSrE TILAKA berperan sebagai RA bagi dirinya sendiri. Selain itu, PSrE TILAKA dapat melakukan hubungan kontraktual dengan RA tertentu untuk menjalankan fungsi sebagai RA dan terhadap RA tersebut tunduk pada ketentuan CPS.
Pelanggan	Korporasi atau Personal yang berlangganan Layanan Tanda Tangan Elektronik Tilaka.
Pelanggan Personal	Pihak yang berlangganan Layanan Tanda Tangan Elektronik Tilaka serta menjadi subjek dari Sertifikat Pemilik.
Pelanggan Korporasi	Pihak yang berlangganan Layanan Tanda Tangan Elektronik Tilaka namun bukan merupakan subjek dari

Istilah	Definisi
	Sertifikat Pemilik. Terhadap Pelanggan Korporasi, subjek dari Sertifikat Pemilik adalah pekerja atau pihak lain yang memiliki hubungan kontraktual dengan pihak tersebut.
Pemilik	Warga Negara Indonesia yang berada dalam ruang lingkup Pelanggan dan merupakan subjek dari Sertifikat Pemilik.
Pemohon	Warga Negara Indonesia yang berada dalam ruang lingkup Pelanggan yang mengajukan permohonan penerbitan atau penerbitan ulang Sertifikat dalam ruang lingkup Pelanggan. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik.
Perjanjian Pemilik Sertifikat	Perjanjian antara PSrE TILAKA dan Pemilik yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pemilik Sertifikat tersedia di Repositori.
Perjanjian Pihak Pengandal	Perjanjian antara PSrE TILAKA dan Pihak Pengandal yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pihak Pengandal tersedia di Repositori.
Perjanjian Kerja Sama	Perjanjian antara PSrE TILAKA dan Pelanggan yang menentukan hak dan tanggung jawab para pihak.
Pihak Pengandal	Orang, entitas, organisasi, lembaga, atau badan usaha yang memercayai Sertifikat Pemilik dan tanda tangan elektronik yang diterbitkan oleh PSrE TILAKA.
PSrE	Entitas yang berwenang untuk mengeluarkan, mengelola, mencabut, dan memperbarui Sertifikat dalam lingkup IKP Indonesia.
PSrE Berinduk	Entitas legal yang Sertifikatnya ditandatangani oleh PSrE Induk dan bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Pemilik.
PSrE Induk	Entitas legal yang memiliki otoritas Sertifikasi tingkat teratas yang menandatangani Sertifikat PSrE Berinduk dalam rantai IKP Indonesia. PSrE Induk Indonesia adalah Kemenkominfo.

Istilah	Definisi
PSrE Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi.
PSrE Non-Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat non-Instansi.
PT Tilaka Nusa Teknologi (PSrE TILAKA)	PSrE dengan status pengakuan berinduk yang Sertifikatnya telah ditandatangani oleh PSrE Induk.
Repositori	Salah satu halaman dari Layanan Tanda Tangan Elektronik Tilaka yang menampilkan data terkait Dokumen Publik yang dibuat, dikuasai, dan dimiliki oleh PSrE TILAKA, yang dapat diakses melalui URL: https://repository.tilaka.id/.
Sertifikat	Sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik.
Sertifikat Pemilik	Sertifikat yang diterbitkan oleh PSrE TILAKA.
Sertifikat PSrE TILAKA	Sertifikat yang diterbitkan dan ditandatangani oleh PSrE Induk.
Skema Harga	Dokumen yang berisi informasi terkait biaya penggunaan Layanan Tanda Tangan Elektronik Tilaka. Skema Harga tersedia di Repositori.
Certificate Policies (CP)	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum.
Certification Practice Statement (CPS)	Kebijakan utama yang mengatur PSrE TILAKA beserta persyaratan prosedural dan operasional yang dianut oleh PSrE TILAKA. *Certification Practice Statement* (CPS) tersedia di Repositori.
Certificate Revocation List (CRL)	Daftar terkini dari Sertifikat Pemilik yang telah dicabut, yang dibuat dan ditandatangani secara elektronik oleh

Istilah	Definisi
	PSrE TILAKA. *Certificate Revocation List* (CRL) tersedia di Repositori.
Extended Validation Certificate	Sertifikat elektronik yang berisi informasi yang ditentukan dalam pedoman EV dan yang telah divalidasi sesuai dengan pedoman tersebut.
Object Identifier (OID)	Sebuah tanda pengenal *alphanumeric* atau *numeric* yang terdaftar di bawah standar *International Organization for Standardization* untuk objek atau kelas objek tertentu.
Online Certificate Status Protocol (OCSP)	Protokol pemeriksaan Sertifikat secara *online* bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat.