Certification Practice Statement (CPS)

PT TILAKA NUSA TEKNOLOGI

Nomor Dokumen	:	**TNT-CPS-001**
Versi	:	**4.0**
Tanggal	:	**17 Desember 2025**

Halaman Persetujuan Policy Authority

Menyetujui,

Chief Financial Officer	Direktur Pengawasan Ruang Digital
Christian Saortua	
Christian Saortua	Policy Authority PSrE Induk
Policy Authority PSrE TILAKA	

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
3.0	18 Jan 2024	• Perubahan kerangka dan judul sesuai dengan perubahan CP PSrE Induk. • Penambahan Undang-Undang nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (bagian 1). • Penambahan Undang-Undang nomor 1 tahun 2024 tentang Perubahan Kedua atas Undang-Undang nomor 11 tahun	Legal & Compliance

Rev No	Tanggal Revisi	Deskripsi	Oleh
		2008 tentang Informasi dan Transaksi Elektronik (bagian 1). • Perubahan menyesuaikan CP PSrE Induk (bagian 1.1, 1.3.1, 1.3.2, 1.5, 1.5.4, 3.1.6, 3.2.1, 3.2.2, 4, 4.1.1, 5.2.3, 5.4.1, 5.4.8, 5.5.1, 5.5.3, 5.6, 5.7.1 - 5.7.4, 5.8, 6.2.2, 6.3.1, 6.5.1, 6.6.1, 8.2, 8.5, 8.7, 9.2.2, 9.3.1, 9.3.3, 9.4.1 - 9.4.3, 9.4.6, 9.5, 9.6.1 - 9.6.3, 9.8.3, 9.10.2, 9.10.3, 9.15, 9.16.1, dan 9.16.5. • Perubahan OID Verifikasi Level 2 – WNI (bagian 1.2). • Penambahan ketentuan mengenai WNA (bagian 1.2, 1.3.3, 1.4.1, 3.2.3, 4.1.1, 4.1.2.1, dan 4.2.2) • Perubahan Kelas Sertifikat Individu menjadi Level 2 (bagian 1.4.1). • Penambahan pada isi Repositori (bagian 2.1) • Penghapusan ketentuan mengenai PIN sebagai unsur "*what you have*" (bagian 3.2.1). • Penambahan ketentuan mengenai penggantian kunci dan penerbitan ulang Sertifikat (bagian 3.3.1, 4.6, dan 4.7.1 - 4.7.6). • Perubahan ketentuan mengenai proses pencabutan Sertifikat Pemilik (bagian 3.4, 4.9.1, 4.9.2, dan 4.9.3). • Perubahan ketentuan mengenai lokasi OCSP *responder* (bagian 4.9.9).	

Rev No	Tanggal Revisi	Deskripsi	Oleh
		• Perubahan ketentuan mengenai persyaratan pemeriksaan pencabutan secara daring (bagian 4.9.10) • Perubahan ketentuan mengenai Akses Fisik dan perubahan lapisan pengamanan *data center* dan *disaster recovery center* (bagian 5.1.2). • Penambahan rincian Peran Terpercaya (bagian 5.2.1). • Penambahan ketentuan mengenai profil Sertifikat, CRL, dan OCSP (bagian 7.1-7.3). • Penghapusan ketentuan terkait Otoritas Pendaftaran/*Registration Authority* (RA) eksternal.	
4.0	17 Des 2025	• Penambahan ketentuan terkait Otoritas Pendaftaran/*Registration Authority* (RA) eksternal (bagian 1.3.2, 5.8). • Penambahan ketentuan mengenai WNA yang tinggal di luar Indonesia (bagian 1.3.1.2, 3.2.3). • Penambahan ketentuan mengenai persetujuan Sertifikat oleh Pemilik (bagian 4.4.1). • Penambahan ketentuan mengenai pengajuan pencabutan Sertifikat Pemilik yang dilakukan oleh Ahli Waris dan Advokat (bagian 3.4, 4.9.1, 4.9.2, 4.9.3). • Penambahan ketentuan mengenai pengiriman Kunci Publik kepada penerbit Sertifikat (bagian 6.1.3).	Legal & Compliance

Daftar Isi

1. Pengantar

PT Tilaka Nusa Teknologi ("TILAKA") adalah suatu badan hukum yang menjalankan kegiatan usaha sebagai Penyelenggara Sertifikasi Elektronik ("PSrE") yang selanjutnya disebut "**PSrE TILAKA**", dan dalam menjalankan kegiatan usahanya tunduk kepada ketentuan peraturan perundang-undangan yang berlaku, termasuk namun tidak terbatas pada:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2. Undang-Undang nomor 19 tahun 2016 tentang Perubahan atas Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik;
3. Undang-Undang nomor 1 tahun 2024 tentang Perubahan Kedua atas Undang-Undang nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik;
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; dan
5. Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik

berikut dengan segala perubahannya yang mungkin timbul di kemudian hari. PSrE TILAKA merupakan PSrE Berinduk dengan jenis PSrE non-Instansi.

Certification Practice Statement ("CPS") menetapkan prosedur bisnis, hukum, dan teknis yang dianut oleh PSrE TILAKA untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dalam Infrastruktur Kunci Publik ("IKP") Indonesia dan menyediakan layanan kepercayaan terkait dengan semua partisipan IKP Indonesia.

Dokumen ini ditujukan kepada:

1. PSrE TILAKA agar beroperasi sesuai dengan CPS, dimana CPS mengacu pada persyaratan yang diatur di dalam *Certificate Policy* (CP) Penyelenggara Sertifikasi Elektronik Induk Indonesia ("PSrE Induk") Indonesia;
2. Pemilik yang perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai pemegang Sertifikat yang diterbitkan oleh PSrE TILAKA dan bagaimana mereka dilindungi oleh PSrE TILAKA;
3. Pengandal yang perlu memahami seberapa besar tingkat kepercayaan terhadap Sertifikat Pemilik atau tanda tangan elektronik tersertifikasi (tanda tangan digital) dan layanan yang memanfaatkan sertifikat elektronik lain yang menjadi bagian dari rantai kepercayaan (*trust chain*) Sertifikat PSrE Induk.

1.1 Ringkasan

CPS telah mengacu pada ketentuan CP 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 berisi ringkasan proses, prosedur, dan ketentuan umum yang dilakukan oleh PSrE TILAKA untuk memenuhi CP PSrE Induk. Ringkasan proses, prosedur, dan ketentuan umum tersebut digunakan oleh PSrE TILAKA dalam menerbitkan dan memelihara Sertifikat.

PSrE TILAKA merupakan PSrE non-Instansi yang menyediakan layanan Tanda Tangan Elektronik bagi Warga Negara Indonesia (WNI) dan Warga Negara Asing (WNA). PSrE TILAKA membuat dan memelihara CPS yang berlaku untuk Layanan Tanda Tangan Elektronik, dan selaras dengan CP PSrE Induk.

CPS berlaku efektif sejak dipublikasikan di Repositori. 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:

	***Object Identifier* (OID)**
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 Orang Perseorangan/Individu – WNI Individu non-Instansi *Online* Level 2	2.16.360.1.1.1.5.1.2.2
OID Orang Perseorangan/Individu – WNA Individu WNA *Online* Level 2	2.16.360.1.1.1.5.2.2.2

1.3 Partisipan IKP

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1 PSrE Induk Indonesia

PSrE Induk adalah Induk dari IKP Indonesia. PSrE Induk menerbitkan dan/atau mencabut Sertifikat PSrE Indonesia (PSrE Instansi maupun PSrE non-Instansi) berdasarkan status pengakuan yang diberikan oleh Kementerian Komunikasi dan Digital Republik Indonesia (Kemenkomdigi). PSrE Induk tidak menerbitkan Sertifikat kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Indonesia.

1.3.1.2 PSrE Indonesia

PSrE Indonesia adalah PSrE yang telah mendapatkan status pengakuan berinduk dari Kemenkomdigi. PSrE TILAKA menerbitkan Sertifikat Pemilik orang perseorangan/individu bagi:

1. Warga Negara Indonesia ("WNI"), kecuali bagi Pemohon WNI yang Sertifikatnya digunakan oleh pegawai Instansi atau Instansi untuk kepentingan pemerintahan; dan
2. Warga Negara Asing ("WNA") baik yang tinggal di Indonesia maupun di luar Indonesia.

Dalam hal ini, PSrE TILAKA tidak berinduk selain kepada PSrE Induk dan tidak menjadi induk bagi PSrE lain.

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.

1.3.2 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. Menyusun dan melaksanakan prosedur penerimaan pendaftaran Pemohon Sertifikat;
2. Melakukan verifikasi dan validasi data identitas Pemohon;
3. Memulai dan/atau memproses permohonan penerbitan Sertifikat;
4. Memulai dan/atau memproses permohonan pencabutan Sertifikat;
5. Menyetujui atau menolak permohonan penggantian kunci (*re-key*); dan
6. 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.

Dalam hal PSrE TILAKA melakukan hubungan kontraktual dengan RA eksternal untuk menjalankan fungsi sebagai RA, PSrE TILAKA berpedoman pada CPS dan prosedur yang berlaku di PSrE TILAKA. Fungsi RA dimaksud dituangkan dalam Perjanjian Kerja Sama antara PSrE TILAKA dengan RA. Kerja sama dengan RA tidak melepaskan tanggung jawab PSrE TILAKA sesuai dengan ketentuan peraturan perundang-undangan. PSrE TILAKA juga melaksanakan audit atau pemeriksaan terhadap kesesuaian fungsi yang dijalankan oleh RA dengan CPS dan/atau peraturan perundang-undangan yang berlaku.

1.3.3 Pemilik

Untuk Sertifikat orang perseorangan/individu, Pemilik adalah WNI dan WNA yang bertindak baik untuk kepentingan dirinya maupun untuk entitas yang terafiliasi dengan badan usaha.

Dalam hal ini, Pemilik berada dalam ruang lingkup Pelanggan dan merupakan subjek dari Sertifikat Pemilik. Sebelum dilakukannya verifikasi, validasi, dan penerbitan Sertifikat, Pemilik disebut sebagai Pemohon.

1.3.4 Pengandal

Pengandal adalah orang, entitas, organisasi, lembaga, atau badan usaha yang memercayai Sertifikat Pemilik dan tanda tangan elektronik yang diterbitkan oleh PSrE TILAKA. 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. Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat Pemilik.

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

Pengandal 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.

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

1.3.5 Partisipan Lain

1.3.5.1 Layanan Pusat Data

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

PSrE TILAKA dalam bekerja sama dengan Partisipan Lain untuk menyelenggarakan layanan telah mendapat persetujuan dari Kemenkomdigi.

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 digunakan untuk menerbitkan Sertifikat Pemilik untuk transaksi yang memerlukan:

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

PSrE TILAKA menyediakan Sertifikat Pemilik orang perseorangan/individu baik untuk WNI maupun WNA dengan verifikasi *Online* level 2 dengan tingkat jaminan sedang.

Kelas Sertifikat	Tingkat Jaminan			Penggunaan	
	Jaminan Rendah	Jaminan Sedang	Jaminan Tinggi	*Digital Signature*	*Non-Repudiation*
Sertifikat Orang Perseorangan/Individu					
Individu non-Instansi *Online* Level 2 – WNI		✓		✓	✓
Individu *Online* Level 2 - WNA		✓		✓	✓

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 Administrasi Kebijakan

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

1. Menetapkan CPS;
2. Memastikan semua layanan, operasional, dan infrastruktur PSrE TILAKA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, pernyataan, dan jaminan dari CPS; dan
3. Menyetujui terjalinnya hubungan kepercayaan dengan IKP lainnya yang memiliki level verifikasi yang setara.

1.5.1 Organisasi Pengelola Dokumen

CPS dan dokumen publik lainnya dikelola oleh PA PSrE TILAKA.

1.5.2 Narahubung

PA PSrE TILAKA dapat dihubungi melalui:

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/compliance@tilaka.id

URL : https://www.tilaka.id

Telepon : +62 21-50100922

1.5.3 Personel yang Menentukan Kesesuaian CPS dengan Kebijakan

PA PSrE TILAKA menentukan kesesuaian konten dengan penerapan dari CPS.

1.5.4 Prosedur Persetujuan CPS

PA PSrE TILAKA menyetujui CPS dan segala perubahannya setelah mendapat persetujuan dari PSrE Induk. PA PSrE TILAKA menentukan apakah perubahan CPS membutuhkan pemberitahuan pihak terkait ataupun perubahan OID. Perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum melalui Repositori. PSrE TILAKA juga melakukan pemberitahuan melalui *email* kepada Pemilik 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 Pengandal;
4. Perjanjian Pemilik Sertifikat;
5. Kebijakan Jaminan;
6. Skema Harga;
7. Sertifikat PSrE TILAKA;
8. *Certificate Revocation List* (CRL); dan
9. OCSP *responder*.

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 diakses oleh Publik melalui https://repository.tilaka.id/.

2.3 Waktu atau Frekuensi Publikasi

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

1. Bagian 2.1 poin 1, 2, 3, 4, 5, dan 6 dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui;
2. Bagian 2.1 poin 7 ditentukan sesuai ketentuan pada bagian 4.4.2; dan
3. Bagian 2.1 poin 8 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 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, dnQualifier=userid> Untuk Pelanggan Personal: cn=<nama lengkap Pemilik>, ou=Personal, c=ID, dnQualifier=userid>

3.1.2 Kebutuhan Nama yang Bermakna

Sertifikat Pemilik yang diterbitkan sesuai dengan CPS bermakna hanya jika nama-nama yang muncul dalam Sertifikat Pemilik dapat dipahami dan digunakan oleh 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 dan PSrE TILAKA 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 menolak permohonan atau melakukan pencabutan Sertifikat Pemilik yang menjadi bagian dari konflik merek dagang.

3.2 Validasi Identitas Awal

PSrE TILAKA mempunyai prosedur dan dokumen yang mengatur rincian verifikasi identitas Pemohon yang mengacu pada ketentuan peraturan perundang-undangan dan sesuai dengan CPS. Autentikasi identitas mengacu pada Standar Verifikasi Identitas.

3.2.1 Metode 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:

1. *username*, *password*, dan *one-time password* (untuk selanjutnya disebut "OTP") atau lainnya yang memenuhi unsur "*what you know*"; atau
2. token atau lainnya yang memenuhi unsur "*what you have*"; atau
3. data biometrik atau lainnya yang memenuhi unsur "*what you are*".

Kunci Privat Pemilik ditempatkan di *data center/disaster recovery center tier* 4 (empat).

3.2.2 Autentikasi dari Identitas Organisasi

PSrE TILAKA tidak menerbitkan Sertifikat Elektronik untuk Badan Usaha.

3.2.3 Autentikasi Identitas Individu

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

1. Individu baik WNI maupun WNA (untuk Pelanggan Personal); atau
2. Individu WNI yang berafiliasi dengan entitas badan usaha (untuk Pelanggan Korporasi).

Bagi individu WNI dan WNA yang merupakan Pelanggan Personal, PSrE TILAKA hanya memproses permohonan penerbitan Sertifikat atas Pelanggan Personal yang mengajukan permohonan penerbitan Sertifikat melalui Channel yang memiliki hubungan kontraktual dengan PSrE TILAKA.

RA melakukan verifikasi dan validasi terhadap informasi yang diajukan oleh Pemohon sehubungan dengan permohonan penerbitan Sertifikat sesuai dengan peraturan perundang-undangan yang berlaku. Dalam hal permohonan penerbitan Sertifikat untuk Pemohon yang berasal dari Pelanggan Korporasi, PSrE TILAKA terlebih dahulu melakukan verifikasi dan validasi terhadap legalitas badan usaha.

Dalam hal Pemohon merupakan WNI, maka Pemohon wajib mengajukan informasi dan dokumen meliputi:

1. Nama;
2. Nomor Induk Kependudukan (NIK);
3. Salinan dokumen 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 yang merupakan WNI 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.

Dalam hal Pemohon merupakan WNA yang tinggal di Indonesia, maka Pemohon wajib mengajukan informasi dan dokumen meliputi:

1. Nama;
2. Nomor Induk Kependudukan (NIK) dan salinan dokumen KTP (jika Pemohon memiliki KTP);
3. Salinan dokumen KITAS atau KITAP (jika Pemohon tidak memiliki KTP);
4. Salinan dokumen Paspor;
5. Surat permohonan dari perusahaan yang ditandatangani oleh penanggung jawab dari institusi tempat Pemohon bekerja atau berafiliasi (jika Pemohon tidak memiliki KTP);
6. Alamat surat elektronik (*email*) dan/atau nomor telepon; dan
7. Data biometrik berupa swafoto yang telah teruji menggunakan mekanisme *liveness detection*.

RA melakukan verifikasi dan validasi kebenaran informasi yang dikirimkan oleh Pemohon yang merupakan WNA yang tinggal di Indonesia 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 (jika Pemohon memiliki KTP);
3. Melakukan verifikasi terhadap Nama dan Paspor dengan membandingkannya terhadap hasil swafoto Pemohon;
4. Melakukan verifikasi terhadap KITAS atau KITAP dengan membandingkannya terhadap hasil swafoto Pemohon (jika Pemohon tidak memiliki KTP);
5. Melakukan verifikasi terhadap surat permohonan dari perusahaan (jika Pemohon tidak memiliki KTP);

6. Melakukan verifikasi terhadap swafoto menggunakan mekanisme *liveness detection*; dan
7. Melakukan validasi terhadap data Pemohon yang telah berhasil melewati proses verifikasi.

Dalam hal Pemohon merupakan WNA yang tinggal di luar Indonesia, maka Pemohon wajib mengajukan informasi dan dokumen meliputi:

1. Nama;
2. Minimal 2 (dua) salinan dokumen identitas resmi yang diterbitkan oleh pemerintah di negara Pemohon yang memuat foto dalam bukti identitas tersebut;
3. Alamat surat elektronik (*email*) dan/atau nomor telepon; dan
4. Data biometrik berupa swafoto yang telah teruji menggunakan mekanisme *liveness detection*.

RA melakukan verifikasi dan validasi kebenaran informasi yang dikirimkan oleh Pemohon yang merupakan WNA yang tinggal di luar Indonesia sehubungan dengan permohonan penerbitan Sertifikat dengan cara berikut ini:

1. Mengirimkan konfirmasi ke alamat *email* dan/atau nomor telepon yang didaftarkan;
2. Melakukan verifikasi terhadap seluruh dokumen identitas resmi yang diberikan dan membandingkan foto wajah di dokumen identitas terhadap hasil swafoto 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 dan legalitas badan usaha sehubungan dengan permohonan penerbitan Sertifikat Pemilik yang diterima selama 5 (lima) tahun. Dalam hal permohonan penerbitan Sertifikat Pemilik ditolak, PSrE TILAKA dan/atau RA hanya menyimpan NIK Pemohon disertai alasan penolakan.

PSrE TILAKA tidak menerbitkan Sertifikat bagi Pemohon yang tidak dapat diverifikasi.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

PSrE TILAKA tidak mencantumkan informasi yang tidak dapat diverifikasi di dalam Sertifikat.

3.2.5 Validasi Otoritas

Tidak ada ketentuan.

3.2.6 Kriteria Inter-Operasi

PSrE TILAKA mengikuti Standar Interoperabilitas PSrE Indonesia dalam rangka melakukan interoperasi antar PSrE Indonesia.

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

3.3.1 Identifikasi dan Autentikasi untuk *Re-Key* Rutin

Paling cepat 30 (tiga puluh) hari kalender sebelum masa berlaku Sertifikat berakhir, Pemilik meminta penggantian kunci ("*re-key*") dan Pemilik diverifikasi melalui penandatanganan menggunakan Sertifikat yang berlaku.

Setelah masa berlaku Sertifikat berakhir, Pemilik mengajukan permohonan penerbitan ulang Sertifikat Pemilik sebagaimana diatur pada bagian 3.2.

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

Setelah pencabutan Sertifikat, Pemilik mengulang proses pendaftaran sebagaimana diatur pada bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan

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

1. Permohonan pencabutan Sertifikat Pemilik yang dilakukan oleh Pemilik diautentikasi menggunakan data biometrik melalui Layanan Tanda Tangan Elektronik Tilaka; atau
2. Permohonan pencabutan Sertifikat Pemilik yang dilakukan oleh Customer Validator, Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha divalidasi oleh RA.

Pencabutan Sertifikat mengacu pada ketentuan peraturan perundang-undangan terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik dan sesuai dengan yang tercantum dalam CPS.

4. Persyaratan Operasional Siklus Sertifikat

Siklus hidup Sertifikat meliputi pendaftaran, penerbitan, perubahan, dan pencabutan Sertifikat. Untuk perubahan Sertifikat, PSrE TILAKA melakukan perubahan Sertifikat dengan cara penggantian kunci Sertifikat sebagaimana diatur pada bagian 4.7 dan penerbitan ulang Sertifikat sebagaimana diatur pada bagian 4.1 – 4.4.

Setelah Sertifikat PSrE TILAKA diterbitkan, PSrE TILAKA:

1. Melindungi Kunci Privat dengan aman;
2. Mendapatkan persetujuan PA PSrE Induk terhadap perubahan CPS;
3. Melakukan operasional PSrE TILAKA sebagaimana diatur dalam ketentuan peraturan perundang-undangan, CP PSrE Induk, dan CPS;
4. Memperbarui CPS ketika terjadi perubahan pada kebijakan CP PSrE Induk atau sebagaimana diatur dalam panduan yang diterbitkan oleh PA PSrE Induk;
5. Mengumumkan informasi nama dan kontak dari pihak yang bertanggung jawab terhadap PSrE TILAKA;
6. Mengelola *website* dan menampilkan informasi Surat Keputusan Pengakuan PSrE TILAKA, Sertifikat PSrE TILAKA, Sertifikat Pemilik, dan otoritas validasi; dan
7. Mencabut semua Sertifikat Pemilik dan menerbitkan CRL sesegera mungkin dalam hal terjadi kebocoran kunci penandatanganan dan melaporkannya ke PSrE Induk sesegera mungkin.

4.1 Permohonan Sertifikat

4.1.1 Siapa yang Dapat Mengajukan Sebuah Permohonan Sertifikat

Pihak yang mengajukan permohonan penerbitan Sertifikat ke PSrE TILAKA bukan merupakan pegawai Instansi atau Instansi untuk kepentingan pemerintahan yang menjalankan kewenangan Instansinya, dengan ketentuan sebagai berikut:

1. Individu baik WNI maupun WNA (untuk Pelanggan Personal, mengacu pada proses yang dijelaskan di poin 4.1.2.2); atau
2. Individu WNI yang berafiliasi dengan entitas badan usaha (untuk Pelanggan Korporasi, mengacu pada proses yang dijelaskan di poin 4.1.2.1 dan 4.1.2.2).

Pihak yang mengajukan permohonan penerbitan Sertifikat ke PSrE TILAKA adalah bukan Instansi Pemerintah dan/atau Pegawai Instansi Pemerintah yang menjalankan kewenangan Instansi nya.

PSrE TILAKA yang ditunjuk oleh PSrE TILAKA melakukan verifikasi terhadap seluruh permohonan yang diterima sesuai dengan ketentuan peraturan perundang-undangan terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik dan Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk.

4.1.2 Proses Pendaftaran dan Tanggung Jawab

PSrE TILAKA bertanggung jawab memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat.

Pemohon bertanggung jawab dalam memberikan informasi yang lengkap dan benar pada saat proses permohonan penerbitan Sertifikat. Sebelum menyelesaikan proses pendaftaran, Pemohon perlu menyetujui syarat dan ketentuan yang ditetapkan oleh PSrE TILAKA.

PSrE TILAKA melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh Pemohon.

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 Badan Usaha

Dalam hal permohonan penerbitan Sertifikat Orang Perseorangan/Individu berasal dari Pelanggan Korporasi, maka PSrE TILAKA menjalankan proses pendaftaran badan usaha dengan tata cara sebagai berikut:

1. PSrE TILAKA melakukan verifikasi dan validasi terhadap legalitas badan usaha menggunakan salah 1 (satu) atau lebih dokumen atau informasi yang termasuk namun tidak terbatas pada:
   a. *Email* resmi perwakilan badan usaha; dan
   b. Nomor Induk Berusaha (“NIB”) dan Nomor Pokok Wajib Pajak (NPWP) Perusahaan, atau Akta Pendirian Perusahaan dengan disertai segala perubahannya sampai dengan yang terakhir kali.
2. Setelah proses verifikasi dan validasi tehadap legalitas badan usaha berhasil, maka Admin Tilaka mendaftarkan badan usaha;
3. Setelah Admin Tilaka melakukan pendaftaran terhadap badan usaha, Admin Korporat akan menerima *email* tautan pendaftaran; dan

4. Setelah Admin Korporat menerima *email* tautan pendaftaran, maka Admin Korporat akan mengisi data diri (NIK, foto KTP, dan *password* untuk *login*).

Proses selanjutnya yaitu proses pendaftaran Pemohon sebagaimana dijelaskan pada bagian 4.1.2.2.

4.1.2.2 Pendaftaran Pemohon

RA 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 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 menerbitkan Sertifikat Pemilik setelah Pemohon melakukan konfirmasi penerimaan Sertifikat Pemilik. Jika hasil verifikasi atau validasi dinyatakan tidak sesuai oleh RA, maka RA meminta data dan informasi tambahan kepada Pemohon untuk mengulang proses verifikasi dan validasi.

4.2 Pemrosesan Permohonan Sertifikat

4.2.1 Melaksanakan Fungsi Identifikasi dan Autentikasi

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

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat

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

1. Khusus Pelanggan Korporasi, Nama Pemohon yang telah didaftarkan tidak sesuai dengan nama yang telah diajukan oleh Admin Korporat;

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 atau instansi yang berwenang memberikan pengesahan badan usaha;
3. Hasil perbandingan swafoto tidak sesuai dengan informasi yang dikirimkan oleh Pemohon; dan/atau
4. Informasi yang dikirimkan oleh Pemohon tidak memenuhi persyaratan yang ditentukan dalam penerbitan Sertifikat Elektronik, tidak sesuai atau tidak akurat.

Pemohon dapat mengajukan permohonan ulang atas ketidaksesuaian data tersebut.

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

4.2.3 Waktu untuk Memproses 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. Saat seluruh persyaratan terpenuhi, PSrE TILAKA mempersiapkan dan menandatangani Sertifikat. PSrE Tilaka memastikan Pemilik menerima Sertifikat sesuai ketentuan pada bagian 4.4, serta memastikan Sertifikat tersedia bagi Pemilik setelah Pemilik secara formal menyetujui kewajibannya sesuai ketentuan pada bagian 9.6.3.

4.3.2 Pemberitahuan kepada Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

Pemberitahuan melalui *email* 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. PSrE TILAKA memberitahukan kepada Pemilik bahwa Pemilik harus melakukan pemeriksaan atas seluruh informasi dan melakukan konfirmasi terhadap Sertifikat sebelum menggunakan Sertifikat.

4.4 Pernyataan Persetujuan Sertifikat

4.4.1 Sikap yang Dianggap sebagai Menyetujui Sertifikat

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

1. Telah memeriksa dan menyetujui informasi yang terkandung dalam Sertifikat;
2. Tidak memberikan tanggapan dalam jangka waktu 9 (sembilan) hari kalender sejak PSrE TILAKA mengirimkan *email* terkait penerbitan Sertifikat; atau
3. Telah menggunakan Sertifikat sesuai dengan penggunaan Sertifikat sesuai ketentuan pada bagian 1.4.1.

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

4.4.2 Publikasi Sertifikat oleh PSrE

PSrE TILAKA melakukan publikasi terhadap Sertifikat PSrE TILAKA pada Repositori sesuai ketentuan pada bagian 2.2 segera setelah Sertifikat PSrE TILAKA diterbitkan. PSrE TILAKA tidak melakukan publikasi terhadap Sertifikat Pemilik, namun Pemilik 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 kepada Pihak Lain

Tidak ada ketentuan.

4.5 Penggunaan Pasangan Kunci dan Sertifikat

4.5.1 Penggunaan Kunci Privat dan Sertifikat oleh Pemilik

PSrE TILAKA melindungi Kunci Privatnya dari penggunaan tanpa izin atau pengungkapan oleh pihak lain dengan menggunakan *Hardware Security Module* (HSM) milik PSrE TILAKA.

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

PSrE TILAKA menerapkan multifaktor autentikasi sesuai ketentuan pada bagian 3.2.1 bagi Pemilik yang menggunakan Kunci Privatnya. Pemilik melindungi parameter autentikasi yang digunakan untuk mengaktifkan Kunci Privatnya.

4.5.2 Penggunaan Kunci Publik dan Sertifikat oleh Pengandal

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

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

4.6 Pembaruan Sertifikat

PSrE TILAKA tidak melakukan pembaruan Sertifikat. Namun, PSrE TILAKA melakukan perubahan Sertifikat Pemilik dengan cara:

1. Penggantian kunci Sertifikat sebagaimana diatur pada bagian 4.7; atau
2. Penerbitan ulang Sertifikat mengikuti permohonan penerbitan Sertifikat sebagaimana diatur pada bagian 4.1 – 4.4.

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 Menyetujui Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.6 Publikasi Pembaruan Sertifikat oleh PSrE

Tidak ada ketentuan.

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE kepada Pihak Lain

Tidak ada ketentuan.

4.7 Penggantian Kunci (*Re-Key*) Sertifikat

4.7.1 Kondisi *Re-Key* Sertifikat

Penggantian kunci (*re-key*) adalah pembuatan/penerbitan Sertifikat baru dengan Kunci Publik, *serial number*, dan *key identifier* yang baru, sementara informasi pribadi Pemilik yang terverifikasi dalam Sertifikat baru masih sama dengan Sertifikat lama. Sertifikat baru memiliki masa berlaku yang baru dan ditandatangani dengan kunci yang baru.

Pemilik melakukan *re-key* selama Sertifikat baru yang diterbitkan memiliki karakteristik (misalnya *key usage*) dan level verifikasi yang sama dengan Sertifikat yang lama.

PSrE TILAKA melakukan *re-key* bagi Pemilik selama:

1. Sertifikat lama yang akan diganti belum dicabut, terkompromi, atau kedaluwarsa;
2. PSrE TILAKA menerbitkan Sertifikat baru kepada Pemilik setelah Pemilik memberi persetujuan untuk pembangkitan pasangan kunci baru dan terasosiasi dengan Sertifikat; dan
3. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi.

Apabila Kunci Privat Pemilik atau PSrE TILAKA terkompromi atau Sertifikat kedaluwarsa atau dicabut, maka Pemilik mengajukan permohonan baru sebagaimana diatur pada bagian 4.1.

4.7.2 Pihak yang dapat Meminta *Re-Key* Sertifikat

Pemilik mengajukan permohonan *re-key* Sertifikat kepada PSrE TILAKA.

4.7.3 Pemrosesan Permintaan *Re-Key* Sertifikat

PSrE TILAKA mengikuti ketentuan sebagaimana diatur pada bagian 3.3.

PSrE TILAKA mengakomodir penggunaan masa berlaku Sertifikat baru yang berbeda dengan masa berlaku Sertifikat sebelumnya.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

PSrE TILAKA mengikuti ketentuan sebagaimana diatur pada bagian bagian 4.3.2.

4.7.5 Sikap yang Dianggap sebagai Menyetujui Sertifikat yang di *Re-Key*

PSrE TILAKA mengikuti ketentuan sebagaimana diatur pada bagian 4.4.1.

4.7.6 Publikasi Sertifikat *Re-Key* oleh PSrE

Sertifikat *re-key* dipublikasikan mengikuti ketentuan sebagaimana diatur pada bagian 4.4.2.

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE kepada Pihak Lain

Tidak ada ketentuan.

4.8 Modifikasi Sertifikat

Tidak ada ketentuan.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Kondisi 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, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha;
2. Terdapat informasi yang tidak valid pada Sertifikat Pemilik; dan/atau
3. Terjadi kebocoran atau kerusakan Kunci Privat Pemilik.

PSrE TILAKA 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 (sebagaimana diatur pada bagian 5.7.3);
3. Kegiatan usaha PSrE TILAKA berhenti atau dihentikan; dan/atau
4. Terjadi kebocoran atau kehilangan Kunci Privat PSrE Induk (sebagaimana diatur 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 Pihak yang dapat Meminta Pencabutan

Pemilik, Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha dapat mengajukan permohonan pencabutan Sertifikat Pemilik.

4.9.3 Prosedur Permintaan Pencabutan

PSrE TILAKA melakukan verifikasi identitas dan wewenang pihak yang meminta pencabutan Sertifikat. Validasi identitas dan wewenang pihak yang meminta pencabutan dibutuhkan sesuai ketentuan pada bagian 3.2.5 dan 3.4.

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 melakukan validasi terhadap swafoto yang dilakukan oleh Pemilik.
4. Jika hasil validasi telah dinyatakan sesuai oleh RA, maka proses pencabutan Sertifikat Pemilik diproses oleh PSrE TILAKA.

Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha mengajukan permohonan pencabutan Sertifikat Pemilik dengan menyertakan dokumen pendukung.

Prosedur pencabutan Sertifikat Pemilik yang diajukan oleh Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha adalah sebagai berikut:

1. Mengirimkan permohonan pencabutan Sertifikat Pemilik kepada PSrE 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, Kebijakan Privasi, dan/atau Perjanjian Pemilik Sertifikat; atau
   c. Bukti surat keterangan resmi atau sejenisnya dari Aparat Penegak Hukum, Admin Korporat, Channel, Ahli Waris, Advokat, atau perwakilan badan usaha.
2. Setelah permohonan pencabutan Sertifikat Pemilik diajukan oleh Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, atau perwakilan badan usaha, maka RA melakukan validasi terhadap permohonan pencabutan Sertifikat Pemilik kepada Admin Korporat, Channel, Aparat Penegak Hukum, Ahli Waris, Advokat, perwakilan badan usaha, atau Pemilik.
3. Setelah hasil validasi dinyatakan sesuai oleh RA, maka PSrE TILAKA memproses pencabutan Sertifikat Pemilik.

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.

Pihak yang disebutkan pada bagian 4.9.2 meminta pencabutan Sertifikat Pemilik segera setelah mengidentifikasi perlunya pencabutan Sertifikat.

4.9.5 Tenggat Waktu Dimana PSrE Harus 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 Pengandal

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 mengamankan CRL untuk menjamin integritas dan keautentikannya. Pembaruan CRL dilakukan secara berkala setiap 24 (dua puluh empat) jam. Dalam hal terdapat kendala dalam pembaruan CRL, waktu maksimal pembaruan secara berkala setiap 26 (dua puluh enam) jam.

4.9.8 Latensi Maksimum CRL

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

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status Secara Daring

PSrE TILAKA menyediakan layanan pengecekan informasi status Sertifikat Pemilik melalui OCSP *responder* yang selalu tersedia pada Repositori, 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 Secara Daring

PSrE TILAKA memberikan layanan pemeriksaan pencabutan secara daring.

OCSP *responder* dipublikasikan pada Repositori.

OCSP *responder* diimplementasikan sesuai dengan standar *Internet Engineering Task Force* (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas.

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus terkait Kebocoran Kunci

Tidak ada ketentuan.

4.9.13 Kondisi untuk Pembekuan

Tidak ada ketentuan.

4.9.14 Pihak 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 dipublikasikan 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, permohonan pencabutan Sertifikat Pemilik berhasil dilakukan tanpa ada 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 Eskro 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 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.

Sistem cadangan PSrE TILAKA disiapkan di *disaster recovery center*, dan mampu memulihkan layanan sistem ketika terjadi kegagalan di *data center*. *Disaster recovery center* berada di wilayah Indonesia, di lokasi yang berbeda dengan lokasi *data center*.

Pemilihan lokasi *data center* dan *disaster recovery center* dilakukan berdasarkan hasil analisa risiko dan telah mempertimbangkan *availability* layanan PSrE TILAKA.

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 setidaknya 4 (empat) lapis pengamanan untuk *data center* dan *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.

Modul kriptografis yang *removable* dinonaktifkan sebelum disimpan. Ketika tidak digunakan, modul kriptografis yang *removable*, informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografis ditempatkan pada tempat penyimpanan yang aman.

Data untuk aktivasi dicatat dan disimpan dengan pengamanan yang setara dengan pengamanan yang disediakan modul kriptografis, dan tidak disimpan bersamaan dengan modul kriptografis.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat PSrE TILAKA dilaksanakan sebelum personel PSrE TILAKA meninggalkan fasilitas 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 listrik 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 Keterpaparan 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

Dokumen yang mengandung informasi sensitif dihancurkan sampai tidak dapat direkonstruksi kembali.

Seluruh informasi sensitif yang tersimpan pada media penyimpanan dan perangkat kriptografis yang sudah tidak digunakan dihancurkan dan dibuang.

Seluruh perangkat kriptografis yang sudah tidak digunakan dihancurkan fisiknya sampai tidak dapat digunakan kembali sebelum dibuang.

Proses pembuangan limbah dilakukan 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 3 (tiga) bulan, 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 *data center* dan *disaster recovery center*. Data dari sistem *backup* TILAKA dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional PSrE TILAKA.

Sistem *backup* TILAKA berada di lokasi yang aman dan tidak terkena dampak jika ketika terjadi bencana alam baik pada *data center* maupun *disaster recovery center*.

5.2 Kendali Prosedur

5.2.1 Peran Terpercaya

Peran Terpercaya termasuk namun tidak terbatas pada:

1. Manajer PSrE/Pimpinan PSrE

   Bertanggung jawab melakukan penetapan terkait kebutuhan bisnis dan kebijakan internal PSrE TILAKA.
2. Otoritas Kebijakan

   Bertanggung jawab menetapkan kebijakan PSrE TILAKA.
3. Administrator Sistem Operasi

   Bertanggung jawab melakukan operasional dan pemeliharaan sistem operasi PSrE TILAKA.
4. Administrator Aplikasi PSrE

   Bertanggung jawab melakukan operasional dan pemeliharaan sistem aplikasi dan basis data PSrE TILAKA.
5. Administrator HSM

   Bertanggung jawab melakukan operasional dan pemeliharaan HSM PSrE TILAKA.
6. Cryptographic Materials Custodian

   Bertanggung jawab memegang credential (kartu/token fisik untuk kuorum HSM).
7. Security Officer

   Bertanggung jawab mengelola penerapan kebijakan dan praktik keamanan PSrE TILAKA.
8. RA Administrator

   Bertanggung jawab mengoperasikan layanan pendaftaran, termasuk verifikasi dan validasi Pemohon.
9. Key Shareholders

   Bertanggung jawab memegang akses fisik ke fasilitas PSrE TILAKA.
10. Internal Auditor

    Bertanggung jawab melakukan audit internal PSrE TILAKA.

Peran tersebut secara detail dijelaskan melalui dokumen internal perusahaan.

5.2.2 Jumlah Orang yang Dibutuhkan untuk Setiap Tugas

Kegiatan yang memerlukan kendali multipersonel dilakukan oleh Peran Terpercaya. Kendali multipersonel tidak dilakukan dengan melibatkan personel yang bertugas dalam peran Auditor. PSrE TILAKA menunjuk minimal 3 (tiga) orang personel dalam setiap tugas yang diberikan di bawah ini:

1. Pembangkitan kunci PSrE TILAKA;

2. Penandatanganan Sertifikat PSrE TILAKA;
3. Pencabutan Sertifikat PSrE TILAKA; dan
4. Pencadangan Kunci Privat 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 sesuai ketentuan pada bagian 5.3.2 untuk memastikan bahwa Peran Terpercaya diisi oleh personel yang tepat dan berkompeten dalam bidangnya.

Autentikasi Peran Terpercaya dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi dilakukan berdasarkan identifikasi orang yang mengakses ruangan atau sistem dan hak akses yang diatur sesuai dengan peran dan tanggung jawab orang tersebut.

5.2.4 Peran yang Membutuhkan Pemisahan Tugas

Setiap personel yang ditunjuk oleh PSrE TILAKA tidak 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.

Ketentuan mengenai pemisahan tugas *Trusted Roles* lebih lanjut diatur dalam Panduan Seremoni Pembangkitan Kunci (*Key Generation Ceremony*).

5.3 Kendali Personel

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan Penugasan

Semua personel PSrE TILAKA adalah WNI dan dipilih atas dasar keterampilan, pengalaman, kepercayaan, dan integritas. Personel yang ditunjuk untuk Peran Terpercaya secara resmi diangkat oleh pimpinan organisasi.

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 Diberikan kepada Personel

PSrE TILAKA menyediakan sejumlah dokumen kepada para personel yang ditunjuk untuk 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 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 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.

Waktu disinkronkan dengan otoritas sumber waktu dengan ketelitian 1 (satu) menit.

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 didokumentasikan.

5.4.3 Periode Retensi Log Audit

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 terpercaya yang mampu membaca dan mengarsipkan log audit, serta 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 kepada Subjek Penyebab Kejadian

Tidak ada ketentuan.

5.4.8 Asesmen Kerentanan

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 atau ketika terjadi perubahan signifikan pada sistem PSrE TILAKA.

5.5 Pengarsipan Catatan (*Record*)

5.5.1 Tipe *Record* yang Diarsipkan

Catatan PSrE TILAKA 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;
5. Dokumen CPS yang berlaku, termasuk juga segala perubahan atau adendum terhadap dokumen-dokumen tersebut;
6. Data audit; dan
7. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI):
    a. Penunjukan dan pencabutan peran dan kewenangan;
    b. Akses pengunjung ke fasilitas PSrE TILAKA;
    c. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
    d. Deteksi dan tindakan terhadap insiden keamanan;
    e. Latihan keadaan darurat;
    f. Tindakan dan penilaian risiko;
    g. Perubahan aset, prosedur, dan tanggung jawab; dan
    h. Perubahan dokumentasi.

Pengarsipan data pribadi Pemilik dilakukan sesuai dengan prosedur yang berlaku di PSrE TILAKA dan peraturan perundangan-undangan mengenai pelindungan data pribadi.

5.5.2 Periode Retensi Arsip

PSrE TILAKA melakukan pengarsipan atas catatan selama 5 (lima) tahun. PSrE TILAKA 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.

Muatan arsip tidak diungkapkan kecuali berdasarkan ketentuan pada bagian 9.3 dan 9.4. Catatan dari transaksi individu diungkap berdasarkan permintaan dari Pemilik yang terlibat dalam transaksi.

5.5.4 Prosedur Cadangan (*Backup*) Arsip

Tidak terdapat ketentuan.

5.5.5 Persyaratan Pemberian Penanda Waktu pada Rekaman Arsip

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 setidaknya 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 diizinkan untuk 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.

Tabel penjelasan kunci PSrE TILAKA dan masa berlakunya dijelaskan pada bagian 6.3.2.

Jika PSrE TILAKA memperbarui Kunci Privat dan menghasilkan Kunci Publik baru, PSrE TILAKA memberitahukan kepada semua Pemilik dan Pengandal atas pembaruan terhadap pasangan kunci tersebut.

PSrE TILAKA tidak membangkitkan Sertifikat Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat PSrE TILAKA. Dengan demikian, pasangan kunci PSrE TILAKA akan dibangkitkan kembali paling lambat pada saat Sertifikat PSrE TILAKA kedaluwarsa dikurangi masa berlaku Sertifikat Pemilik sesuai yang tercantum pada bagian 6.3.2.

5.7 Pemulihan Bencana dan Keadaan Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

PSrE TILAKA memiliki rencana penanganan insiden dan rencana pemulihan bencana. 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.

PSrE TILAKA menginformasikan kepada PSrE Induk apabila mengalami insiden, termasuk namun tidak terbatas pada:

1. Terdeteksinya atau adanya indikasi sistem PSrE TILAKA terkompromi;
2. Adanya upaya untuk menembus sistem PSrE TILAKA, baik secara fisik maupun elektronik;

3. Serangan *denial of service* pada sistem PSrE TILAKA;
4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam *field* "*next update*" pada CRLnya yang valid saat ini. PSrE TILAKA segera memulihkan penerbitan CRL secepat mungkin; dan/atau
5. CRL dan/atau OCSP *responder* tidak diakses oleh publik.

Prosedur diperbarui secara berkala sesuai kebutuhan.

Semua sistem pencadangan/pemulihan diuji minimal 1 (satu) tahun 1 (satu) kali.

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. Jika kemampuan untuk membangkitkan informasi status Sertifikat tidak beroperasi atau rusak, maka PSrE TILAKA memulihkan kemampuan untuk membangkitkan informasi status Sertifikat sesegera mungkin. Jika kemampuan PSrE TILAKA untuk membangkitkan informasi status Sertifikat tidak bisa dipulihkan dalam jangka waktu yang wajar, maka PSrE TILAKA menentukan apakah perlu untuk meminta pencabutan Sertifikat miliknya kepada PSrE Induk; dan
4. Jika kunci penandatanganan PSrE TILAKA rusak, maka operasional PSrE TILAKA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci PSrE TILAKA baru. PSrE TILAKA membangkitkan pasangan kunci PSrE TILAKA baru sesuai dengan prosedur yang ditetapkan oleh PSrE TILAKA.

Jika DC dan DRC tidak dapat memulihkan kemampuan pencabutan Sertifikat dalam jangka waktu yang wajar, maka sistem PSrE TILAKA akan diperlakukan sebagai PSrE terkompromi.

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

PSrE TILAKA meminta penerbitan Sertifikat baru ke Menteri sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CP PSrE Induk.

PSrE TILAKA membangkitkan pasangan kunci PSrE TILAKA baru sesuai dengan prosedur yang ditetapkan dalam CPS.

PSrE TILAKA menyelidiki penyebab kompromi atau kerugian dan tindakan yang diambil untuk mencegah kompromi tersebut terulang kembali.

Jika Kunci Privat dari PSrE Induk hilang atau bocor, maka PSrE TILAKA melakukan langkah-langkah berikut setelah mendapat pemberitahuan dari PSrE Induk:

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.

Setelah PSrE Induk menerbitkan ulang Sertifikat PSrE TILAKA, PSrE TILAKA melakukan penerbitan ulang Kunci Privat Pemilik akibat terkompromi, yang dilakukan oleh Pemilik dengan mengajukan permohonan Sertifikat sesuai ketentuan pada bagian 4.1.

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah Suatu 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 diperbarui jika dibutuhkan. Layanan kembali pulih dalam kurun waktu 24 (dua puluh empat) jam apabila terjadi bencana. Fasilitas *disaster recovery center* PSrE TILAKA tersedia apabila fasilitas utama berhenti beroperasi.

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan PSrE TILAKA rusak secara fisik dan semua salinan kunci penandatangan milik PSrE TILAKA hancur, PSrE TILAKA meminta agar Sertifikatnya dicabut. PSrE TILAKA mengikuti ketentuan pada bagian 5.7.3.

5.8 Penutupan PSrE TILAKA

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

1. Memberitahukan kepada PSrE Induk, Pemilik, dan 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 dilakukan Layanan Tanda Tangan Elektronik Tilaka.

Pengakhiran kegiatan usaha memperhatikan hal-hal berikut ini:

1. Memastikan agar segala gangguan yang diakibatkan oleh penutupan PSrE TILAKA diminimalisasi;
2. Memastikan agar rekaman arsip PSrE TILAKA tetap dipertahankan; dan
3. Menjamin agar proses pencabutan semua Sertifikat pada saat penutupan dilakukan sampai selesai.

6. Kendali Keamanan Teknis

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan Pasangan Kunci

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.

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 kepada 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 pada bagian 3.2.1.

6.1.3 Pengiriman Kunci Publik kepada Penerbit Sertifikat

Pemilik tidak bisa membangkitkan pasangan kunci bagi dirinya sendiri. PSrE TILAKA membangkitkan pasangan kunci atas nama Pemilik.

6.1.4 Pengiriman Kunci Publik PSrE kepada Pengandal

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

Penjelasan tanggung jawab tentang publikasi dan Repositori Sertifikat sesuai ketentuan pada bagian 2.1

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 186-4.

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, termasuk untuk pembangkitan pasangan Kunci Pemilik.

6.2.2 Kendali Multipersonel (n of m) Kunci Privat

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

Nama-nama pihak yang terlibat dalam kendali multipersonel dicatat dalam sebuah daftar yang tersedia untuk pemeriksaan selama audit.

6.2.3 Eskro Kunci Privat

Kunci Privat PSrE TILAKA tidak dititipkan. PSrE TILAKA tidak menerima layanan penitipan kunci Pemilik.

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 PSrE TILAKA yang tersimpan di lokasi yang berbeda dengan lokasi utama (*data center*). Semua salinan Kunci Privat PSrE TILAKA dilindungi dengan cara yang sama dengan aslinya.

Kunci Privat Pemilik dicadangkan (*backup*). Semua salinan Kunci Publik Pemilik dilindungi dengan cara yang sama dengan aslinya.

6.2.5 Pengarsipan Kunci Privat

Kunci Privat PSrE TILAKA dan Kunci Privat Pemilik 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.

Dalam hal PSrE TILAKA mengetahui bahwa Kunci Privat Pemilik disampaikan kepada orang atau entitas yang tidak berwenang, maka PSrE TILAKA mencabut semua Sertifikat yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografis

Kunci Privat PSrE TILAKA disimpan pada perangkat FIPS 140-2 level 3. Kunci Privat Pemilik disimpan pada perangkat FIPS 140-2 level 2. Kunci Privat 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 pada bagian 5.2.2.

Pengaktifan Kunci Privat Pemilik dilindungi dengan mekanisme keamanan yang dikendalikan oleh PSrE TILAKA. Pemilik bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemilik Sertifikat.

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.

Dalam hal PSrE TILAKA tidak lagi beroperasi, Kunci Privat PSrE TILAKA dihapus dari modul kriptografis.

6.2.10 Metode Penghancuran Kunci Privat

Peran Terpercaya menghancurkan Kunci Privat PSrE TILAKA 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.

PSrE TILAKA mengatur prosedur penghancuran Kunci Privat Pemilik.

6.2.11 Peringkat Modul Kriptografis

Seperti diuraikan pada 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. Semua Kunci Publik yang digunakan untuk tujuan verifikasi diarsipkan setidaknya selama 5 (lima) tahun sebagai satu kesatuan dari Sertifikat yang diterbitkan. Rincian tentang pengarsipan sebagaimana diatur pada bagian 5.5.

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasional Sertifikat dan pasangan kunci adalah sebagai berikut:

Jenis Sertifikat	Jangka Waktu
Sertifikat PSrE TILAKA	10 (sepuluh) tahun
Sertifikat Pemilik	1 (satu) tahun
Time Stamp Authority	1 (satu) tahun
OCSP *Responder*	1 (satu) tahun

6.4 Data Aktivasi

6.4.1 Pembangkitan dan Instalasi Data Aktivasi

Data aktivasi dibangkitkan secara otomatis oleh HSM yang melibatkan Peran Terpercaya. Detail pembangkitan data aktivasi mengacu pada prosedur yang berlaku di PSrE TILAKA.

Penggunaan data aktivasi Kunci Privat Pemilik dimasukkan oleh Pemilik saat aktivasi.

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 pada bagian 6.2.2. PSrE TILAKA menyimpan data aktivasi dalam bentuk *smart card* dengan perlindungan PIN.

Pemilik harus menjaga kerahasiaan data aktivasi.

6.4.3 Aspek Lain dari Data Aktivasi

Tidak ada ketentuan.

6.5 Kendali Keamanan Komputer

6.5.1 Persyaratan Teknis Keamanan Komputer Spesifik

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 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;
5. Menyediakan perlindungan mandiri untuk sistem operasi;
6. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
7. Mewajibkan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
8. Menyediakan perlindungan terhadap kode jahat (*malicious code*);

9. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
10. Mewajibkan pemeriksaan mandiri (*self-test*) terhadap layanan PSrE TILAKA.

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

Kendali pengembangan sistem PSrE TILAKA adalah sebagai berikut:

1. Pengadaan perangkat keras dan perangkat lunak dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen-komponen yang terdapat di dalam perangkat lunak dirusak;
2. Perangkat keras dan perangkat lunak didedikasikan untuk melaksanakan aktivitas IKP. Tidak ada aplikasi lain, perangkat lunak, koneksi jaringan, atau komponen perangkat lunak yang di-*install* yang bukan bagian dari operasional IKP;
3. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya untuk dimuat ke perangkat. Perangkat keras dan perangkat lunak PSrE TILAKA selalu dipindai untuk kode-kode berbahaya pada penggunaan;
4. Pembaruan perangkat keras dan perangkat lunak dibeli atau dikembangkan dengan cara yang sama dengan perangkat aslinya dan di-*install* oleh personel yang terpercaya dan terlatih melalui langkah-langkah yang terdokumentasi; dan
5. Perangkat lunak yang digunakan untuk manajemen Sertifikat diuji di lingkungan non-produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem atau komponennya melalui proses peninjauan kontrol manajemen perubahan dan persetujuan.

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 mendeteksi hal tersebut baik dengan cara melakukan pengawasan dan pemeriksaan oleh personel PSrE TILAKA maupun secara otomatis.

PSrE TILAKA memiliki prosedur dan jadwal untuk memantau dan mengontrol sistem, serta memelihara prosedur dan jadwal tersebut. Personel PSrE TILAKA yang bertanggung jawab melakukan pengawasan dan pemeriksaan sistem secara rutin. Sebagai tambahan dari pengawasan secara manual ditambahkan proses otomatis yang menginformasikan kepada Peran Terpercaya ketika ada aktivitas yang tidak wajar pada sistem.

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 Tanda 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.

PSrE TILAKA mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

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.

Rincian aturan profil Sertifikat mengacu ke Standar Interoperabilitas PSrE Indonesia.

1. *Basic Field*
   a. PSrE TILAKA

Field	Type	PSrE TILAKA
Certificate (seq)		
tbsCertificate	TBSCertificate	
signatureAlgorithm	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (SHA256WithRSAEncryption)
signatureValue	BIT STRING	Tanda tangan PSrE Induk
TBSCertificate (seq)		
version	INTEGER{v1(0), v2(1), v3(3)}	versi 3
serialNumber	INTEGER	RFC 5280
signature	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (SHA256WithRSAEncryption)
issuer	Name	DN PSrE Induk (CN=Root CA Indonesia DS G1, O=Kementerian Komunikasi dan Informatika, C=ID)
validity	Validity	10 tahun
Validity(seq)		
notBefore notAfter	UTCTime UTCTime	02-Sep-21 31-Aug-31
subject	Name	DN PSrE Indonesia (CN=TILAKA CA G1, O=PT Tilaka Nusa Teknologi, C=ID)
subjectPublicKeyInfo	SubjectPublicKeyInfo	
SubjectPublicKeyInfo (seq)		
algorithm	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 4096)
subjectPublicKey	BIT STRING	Kunci PublikTILAKA CA G1
extensions	EXPLICIT Extensions	
Extensions (seq size (1...MAX))		
extension	EXTENSION	
EXTENSION (seq)		
extnID	OBJECT IDENTIFIER	OID dari extension
critical	BOOLEAN DEFAULT FALSE	
extnValue	OCTET STRING	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

b. Pemilik

Field	Type	Pemilik
Certificate (seq)		
tbsCertificate	TBSCertificate	
signatureAlgorithm	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (SHA256withRSAEncryption)
signatureValue	BIT STRING	Tanda tangan PSrE Indonesia
TBSCertificate (seq)		
version	INTEGER{v1(0), v2(1), v3(3)}	versi 3
serialNumber	INTEGER	RFC 5280
signature	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (SHA256withRSAEncryption)
issuer	Name	DN PSrE Indonesia (CN=TILAKA CA G1, O=PT Tilaka Nusa Teknologi, C=ID)
validity	Validity	1 tahun
Validity(seq)		
notBefore	UTCTime	Waktu mulai validitas
notAfter	UTCTime	Waktu validitas berakhir
subject	Name	Orang-perseorangan Pribadi (CN={Nama Orang}[2], OU=Personal, C={2 digit ISO Code Negara}, dnQualifier=userid) Orang-perseorangan berafiliasi ke perusahaan (CN={Nama orang}[3], O=Nama Badan Usaha, C={2 digit ISO Code Negara}, dnQualifier=userid)
subjectPublicKeyInfo	SubjectPublicKeyInfo	
SubjectPublicKeyInfo (seq)		
algorithm	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
subjectPublicKey	BIT STRING	Kunci Publik Subscriber
extensions	EXPLICIT Extensions	
Extensions (seq size (1...MAX))		
extension	EXTENSION	
EXTENSION (seq)		
extnID	OBJECT IDENTIFIER	OID dari extension
critical	BOOLEAN DEFAULT	
	FALSE	
extnValue	OCTET STRING	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

2. *Standard Extension Field*

a. PSrE TILAKA

Field	Type	OID	PSrE TILAKA Information
AuthorityKeyIdentifier (seq)		2.5.29.35	
keyIdentifier	OCTET STRING		2968f95c56db1a6eabe223df92c26b12d2a9fe8d
authorityCertIssuer	GeneralNames		
authorityCertSerialNum ber	INTEGER		
SubjectKeyIdentifier		2.5.29.14	
subjectKeyIdentifier	OCTET STRING		1ac5165c85da3501512d7954bfc7809312c2bd85
KeyUsage		2.5.29.15	
keyUsage	BIT STRING		Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)
CertificatePolicies (seq size(1...MAX))		2.5.29.31	
policyInformation	PolicyInformation		
PolicyInformation (seq)			http://crl.rootca.id/RootCAIndonesiaDSG1.crl

b. Pemilik

Field	Type	OID	Subscriber/Pemilik Information
AuthorityKeyIdentifier (seq)		2.5.29.35	
keyIdentifier	OCTET STRING		1ac5165c85da3501512d7954bfc7809312c2bd85
authorityCertIssuer	GeneralNames		
authorityCertSerialNum ber	INTEGER		
SubjectKeyIdentifier		2.5.29.14	
subjectKeyIdentifier	OCTET STRING		Hash SHA-1 160 bit dari kunci publik Pemilik
KeyUsage		2.5.29.15	
keyUsage	BIT STRING		Digital Signature, Non-Repudiation (c0)
CertificatePolicies (seq size(1...MAX))		2.5.29.32	
policyInformation	PolicyInformation		
PolicyInformation (seq)			
policyIdentifier	OBJECT		[1]Certificate Policy: Policy Identifier=2.16.360.1.1.1.3.12.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://repository.tilaka.id [2]Certificate Policy: Policy Identifier=2.16.360.1.1.1.3.12 [2,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Sertifikat non-Instansi [3]Certificate Policy: Policy Identifier=2.16.360.1.1.1.7.1 [3,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Sertifikat Individu [4]Certificate Policy: Policy Identifier=2.16.360.1.1.1.3.12.5 [4,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Tilaka Nusa Teknologi Untuk WNI [5]Certificate Policy: Policy Identifier=2.16.360.1.1.1.5.1.2.2 [5,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=WNI Online Level 2 Untuk WNA [5]Certificate Policy: Policy Identifier= 2.16.360.1.1.1.5.2.2.2 [5,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=WNA Online Level 2
	IDENTIFIER		
policyQualifiers	Sequence Size (1...MAX) PolicyQualifierInfo		
SubjectAlternativeName		2.5.29.17	
subjectAlternativeName	GeneralNames		
IssuerAlternativeName		2.5.29.18	
issuerAlternativeName	GeneralNames		
BasicConstraint (seq)		2.5.29.19	
cA	BOOLEAN		FALSE
pathLenConstraint	INTEGER		
ExtendedKeyUsage (seq size (1...MAX))		2.5.29.37	Adobe PDF Signing (1.2.840.113583.1.1.5)
keyPurposeId	Object Identifier		
CRLDistributionPoints (seq size (1...MAX))		2.5.29.31	
DistributionPoint (seq)			
distributionPoint	DistributionPoin tName		https://ca.tilaka.id/tilakaCA.cr
reasons	ReasonFlags		
cRLIssuer	GeneralNames		CRL Issuer: Directory Address: C=ID O=PT Tilaka Nusa Teknologi CN=Tilaka CA G1
AuthorityInfoAccess (seq size (1..MAX))		2.5.29.1	
AccessDescription (seq)			
accessMethod	OBJECT IDENTIFIER		1.3.6.1.5.5.7.48.1
accessLocation	GeneralName		https://ca.tilaka.id/ocsp
AccessDescription (seq)			
accessMethod	OBJECT IDENTIFIER		1.3.6.1.5.5.7.48.2
accessLocation	GeneralName		https://ca.tilaka.id/certificates/tilakaCA.crt

7.2 Profil CRL

Profil CRL PSrE TILAKA menggunakan CRL dan CRL *entry extension* RFC 5280.

1. CRL *Profile*

Field	ASN.1 Type	Note	M
version	Integer	1 (version 2)	M
issuer	Name	CN = TILAKA CA G1 O = PT Tilaka Nusa Teknologi C = ID	M
thisUpdate	UTCTime	Issuing date	M
nextUpdate	UTCTime	According CA's policy	M
revokedCertificates			M
userCertificate	Integer		M
revocationDate	UTCTime		M
crlExtensions			M

2. CRL *Extension Field*

Field	ASN.1 Type	Value
authorityKeyIdentifier		1ac5165c85da3501512d7954bfc7809312c2bd85
cRLNumber	Integer	

7.3 Profil OCSP

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

1. *Basic Field*

Field	Type	OCSP Certificate
Certificate (seq)		
tbsCertificate	TBSCertificate	
signatureAlgorithm,	AlgorithmIdentifier	
AlgorithmIdentifi		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
parameters	ANY DEFINED BY algorithm OPTIONAL	NULL
signatureValue	BIT STRING	Tanda tangan PSrE Indonesia penerbit Sertifikat
TBSCertificate (seq)		
version	INTEGER{v1(0), v2(1), v3(2)}	versi 3
serialNumber	INTEGER	Serial number sertifikat
signature,memiliki	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	RSA algorithm identifier (1.2.840.113549.1.1.11)
issuer	Name	DN PSrE Indonesia (CN=TILAKA CA G1, O=PT Tilaka Nusa Teknologi, C=ID)
validity, memiliki	Validity	3 tahun
Validity(seq)		
notBefore	UTCTime	Waktu mulai validitas
notAfter	UTCTime	Waktu validitas berakhir
subject	Name	DN Pemilik Sertifikat (CN=OCSPSIGNERTILAKAVA, OU=OCSP Responder, O=PT Tilaka Nusa Teknologi, C=ID)
subjectPublicKeyInfo,	SubjectPublicKeyInfo	
SubjectPublicKeyInfo (seq)		
algorithm	AlgorithmIdentifier	
AlgorithmIdentifier (seq)		
algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
subjectPublicKey	BIT STRING	Kunci Publik End Entity
extensions, memiliki	EXPLICIT Extensions	
Extensions (seq size (1...MAX))		
extension	EXTENSION	
EXTENSION (seq)		
extnID	OBJECT IDENTIFIER	OID dari extension
critical	BOOLEAN DEFAULT FALSE	
extnValue	OCTET STRING	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

2. *Standard Extension Field*

Field		*Type*	OID	*OCSP Certificate*
AuthorityKeyIdentifier (seq)			2.5.29.35	
keyIdentifier		OCTET STRING		1ac5165c85da3501512d7954bfc7809312c2bd85
authorityCertIssuer		GeneralNames		
authorityCertSerialNumber		INTEGER		
SubjectKeyIdentifier			2.5.29.14	
subjectKeyIdentifier		OCTET STRING		SHA-1 160 bit
KeyUsage			2.5.29.15	
keyUsage		BIT STRING		digitalSignature
CertificatePolicies (seq size(1...MAX))			2.5.29.32	
policyInformation, memiliki		PolicyInformation		
	PolicyInformation (seq)			
	policyIdentifier	OBJECT IDENTIFIER		
	policyQualifiers	Sequence Size (1...MAX) PolicyQualifierInfo		
BasicConstraint (seq)			2.5.29.19	
cA		BOOLEAN		FALSE
pathLenConstraint		INTEGER		
ExtendedKeyUsage (seq size (1...MAX))			2.5.29.37	
keyPurposeId		Object Identifier		1.3.6.1.5.5.7.3.9 (OCSP Signing)

8. Audit Kepatuhan dan Penilaian Kelaikan Lainnya

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 menjalani audit kepatuhan serta menyampaikan laporan secara berkala sesuai dengan ketentuan peraturan perundang-undangan mengenai PSrE. PSrE TILAKA juga menjalani Audit Sistem Manajemen Keamanan Informasi dengan menggunakan kriteria ISO/IEC 27001.

8.1 Frekuensi atau Lingkup Penilaian

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 kriteria ISO/IEC 27001 minimal 1 (satu) kali dalam 1 (satu) tahun.

Layanan hasil kerja sama dengan Partisipan Lain yang tercantum pada bagian 1.3.5 masuk dalam lingkup penilaian.

8.2 Identitas/Kualifikasi Penilai

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:

1. Audit dilaksanakan oleh tim penilai independen yang *qualified*;
2. 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;
3. Auditor memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
4. Auditor memiliki bukti bahwa dirinya memenuhi kualifikasi auditor yang dibuktikan dengan sertifikasi, akreditasi, lisensi, atau penilaian lain yang sah;
5. 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; dan

6. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

8.3 Hubungan Penilai dengan Entitas yang Dinilai

PSrE TILAKA memilih auditor/penilai yang independen. Untuk memastikan independensi dan objektivitas, Penilai tidak mengembangkan atau memelihara fasilitas dan/atau CPS. PSrE Induk memastikan Penilai memenuhi persyaratan ini.

Dalam melaksanakan audit, Penilai memiliki hubungan kontrak yang jelas dengan PSrE TILAKA untuk menjaga independensi atau ketidakberpihakan para Penilai. Penilai melaksanakan audit dengan mempertahankan standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan pelaksanaan penilaian profesional yang independen dengan tunduk pada ketentuan peraturan perundang-undangan.

8.4 Topik Penilaian

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa PSrE TILAKA beroperasi sesuai dengan CP PSrE Induk dan ketentuan peraturan perundang-undangan. Penilaian Kelaikan mencakup penilaian CPS ini mengacu pada CP PSrE Induk untuk menentukan bahwa CPS ini telah diimplementasikan dan ditegakkan. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen PSrE TILAKA.

Audit yang dilaksanakan memenuhi kebutuhan dari skema audit yang digunakan dalam penilaian. Kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Skema audit baru diberlakukan paling lambat 1 (satu) tahun setelah dipublikasikan.

8.5 Tindakan yang Diambil Akibat Ketidaksesuaian

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

1. Mencatat ketidaksesuaian tersebut;
2. Memberitahukan kepada PSrE TILAKA tentang ketidaksesuaian; dan
3. Melaporkan kepada PSrE Induk.

PSrE TILAKA menentukan tindak lanjut yang diperlukan agar sesuai dengan persyaratan CPS dan/atau kontrak masing-masing, dan kemudian melakukan tindakan perbaikan tanpa penundaan.

8.6 Laporan Hasil Penilaian

Laporan kepatuhan audit, termasuk identifikasi tindakan perbaikan yang dilakukan, diberikan kepada PA PSrE TILAKA sebagaimana diatur pada bagian 8.5. 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.

PSrE TILAKA memantau kepatuhannya terhadap CP PSrE Induk, CPS, dan ketentuan peraturan perundang-undangan dan secara ketat mengontrol kualitas layanannya dengan melakukan audit mandiri minimal 1 (satu) tahun 1 (satu) kali terhadap sampel yang dipilih secara acak minimal 1 (satu) persen dari keseluruhan Sertifikat yang diterbitkan di tahun berjalan.

9. Bisnis Lain dan Masalah Hukum

9.1 Biaya

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat

PSrE TILAKA 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 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 Biaya

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

PSrE TILAKA mempertahankan kemampuan keuangan yang wajar untuk menjalankan operasional PSrE TILAKA dalam memenuhi kewajibannya kepada Partisipan IKP sebagaimana diatur pada bagian 1.3.

9.2.3 Cakupan Asuransi atau Garansi untuk Pemilik

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 dan RA;
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.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, pengungkapan informasi di atas dilakukan setelah mendapat persetujuan tertulis dari pemilik informasi.

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.

PSrE TILAKA menjaga kerahasiaan informasi bisnis rahasia yang secara jelas ditandai atau diberi label sebagai rahasia atau menurut sifatnya harus dipahami secara wajar sebagai rahasia, dan memperlakukan informasi tersebut dengan tingkat perhatian dan keamanan yang sama seperti PSrE TILAKA memperlakukan informasi rahasia miliknya sendiri.

9.4 Privasi Informasi Pribadi

9.4.1 Rencana Privasi

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

Kebijakan Privasi mengacu pada ketentuan peraturan perundangan-undangan mengenai pelindungan data pribadi, informasi, dan transaksi elektronik. Kebijakan Privasi mendokumentasikan informasi pribadi yang dikumpulkan, disimpan, dan diproses, serta kondisi yang membolehkan informasi tersebut untuk diungkapkan.

Pemilik diberikan akses dan kemampuan untuk mengajukan permintaan perubahan informasi pribadi atau organisasi kepada PSrE TILAKA. Informasi tersebut diberikan setelah PSrE TILAKA melakukan langkah-langkah untuk mengautentikasi identitas dari pihak yang meminta.

PSrE TILAKA mengumpulkan dan menggunakan data yang diperlukan untuk tujuan pendaftaran dan sertifikasi. Secara khusus, PSrE TILAKA tidak menggunakan data tersebut untuk tujuan komersial apa pun.

9.4.2 Informasi yang Diperlakukan sebagai Privat

PSrE TILAKA melindungi semua informasi pribadi Pemilik (termasuk yang telah diarsipkan) dari pengungkapan yang tidak sah, baik terhadap Pemohon yang Sertifikatnya berhasil diterbitkan maupun yang ditolak sesuai dengan Kebijakan Privasi yang dipublikasikan pada Repositori sebagaimana diatur pada bagian 2.1 CPS ini, termasuk penghapusan informasi pribadi Pemohon atas permohonan penerbitan Sertifikat Pemilik yang ditolak.

Informasi pribadi diungkapkan atas persetujuan Pemilik terhadap Pengandal. Informasi pribadi Pemilik (termasuk yang telah diarsipkan) tidak diungkapkan kecuali yang diizinkan pada bagian 9.4.1.

9.4.3 Informasi yang Tidak Dianggap Privat

Informasi yang disertakan dalam Sertifikat tidak dianggap privat dan tidak tunduk pada perlakuan yang diuraikan dalam bagian 9.4.2.

Pelanggaran atas penggunaan informasi pribadi diatur dalam ketentuan peraturan perundang-undangan yang berlaku.

9.4.4 Tanggung Jawab Melindungi Informasi Privat

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 Pemberitahuan dan Persetujuan untuk Menggunakan Informasi Privat

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 mengungkapkan informasi privat kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh CPS, diwajibkan oleh hukum, peraturan perundang-undangan, atau perintah pengadilan.

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. PSrE TILAKA tidak melanggar hak kekayaan intelektual pihak lain.

9.6 Pernyataan dan Jaminan

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 telah memenuhi syarat yang diatur berdasarkan CPS dan hanya informasi yang telah diverifikasi yang ditampilkan di Sertifikat;
4. PSrE TILAKA menampilkan informasi yang diakses secara publik pada Repositori;
5. Kunci Privat PSrE TILAKA terlindungi dan tidak diakses oleh pihak yang tidak berwenang;
6. semua pernyataan yang dibuat oleh PSrE TILAKA dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh PSrE TILAKA; dan
7. setiap Pemilik telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

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 PSrE TILAKA;
2. tidak ada kesalahan informasi dalam Sertifikat Pemilik yang dilakukan oleh RA sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat Pemilik;

3. kegiatan pendaftaran dilakukan sesuai dengan CPS dan perjanjian kerja sama; dan
4. Pemilik dikenakan kewajiban sebagaimana tercantum pada bagian 9.6.3. Pemilik mendapat informasi tentang konsekuensi atau akibat dari ketidakpatuhan terhadap kewajiban.

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 memiliki akses terhadap Kunci Privat;
3. melakukan peninjauan kembali atau melakukan verifikasi terhadap informasi yang terdapat pada Sertifikat Pemilik yang telah diterimanya untuk memastikan akurasi dari Sertifikat Pemilik tersebut;
4. Pemilik sudah melakukan pemeriksaan terhadap informasi yang terdapat pada Sertifikat sebelum menyetujui Sertifikat;
5. semua informasi yang diberikan oleh Pemilik dan informasi yang berada di dalam Sertifikat adalah benar;
6. Sertifikat digunakan hanya untuk tujuan yang legal dan sesuai dengan kegunaan yang ada dalam CPS;
7. 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;
8. menanggapi instruksi yang telah diberikan oleh PSrE TILAKA terkait *compromise* atau penyalahgunaan Sertifikat selambat-lambatnya 48 (empat puluh delapan) jam setelah instruksi tersebut diberikan;
9. 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

10. 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 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 Pengandal yang ada pada CPS; dan
5. mematuhi ketentuan yang ditetapkan di CPS dan dokumen Perjanjian 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 diberikan kepada Pelanggan jika dalam penggunaan Sertifikat oleh Pemilik tidak sesuai *Key Usage*;

b. Pemberian jaminan sesuai dengan dokumen Perjanjian Pengandal yang tercantum pada https://repository.tilaka.id/ tidak diberikan kepada 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, serta 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.

9.8.3 Pembatasan Tanggung Jawab Pemilik

Tanggung jawab Pemilik dan/atau batasannya diuraikan dalam Perjanjian Pemilik Sertifikat, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak.

Pemilik secara khusus bertanggung jawab atas kerugian yang disebabkan oleh pelanggaran kelaikan (*due diligence*), seperti memindahtangankan token kepada orang lain ataupun tidak mencabut Sertifikatnya yang terkompromi.

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 Pengandal

Kebijakan ganti rugi oleh Pengandal mengacu pada dokumen Perjanjian 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.

Setiap perubahan efektif berlaku setelah dokumen CPS dipublikasikan. Dalam hal terdapat perubahan CP PSrE Induk, dokumen Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan lainnya yang berdampak pada OID PSrE TILAKA, maka OID dalam CPS tetap berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan dengan ketentuan CP PSrE Induk, Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan terkini lainnya.

9.10.3 Dampak Pengakhiran dan Ketentuan yang tetap Berlaku

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

Aturan terkait pelindungan data dan arsip informasi tetap dipatuhi walaupun CPS sudah tidak berlaku lagi.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

PSrE TILAKA menyediakan media komunikasi bagi para pihak terkait melalui *email* atau telepon. PSrE TILAKA 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 Perubahan atau Amandemen

9.12.1 Prosedur untuk Perubahan atau Amandemen

Segala perubahan CPS ditinjau dan disetujui oleh PA PSrE Induk. Perubahan CPS dilakukan sesuai dengan prosedur persetujuan CPS.

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 kerja sejak tanggal ditandatangani melalui Repositori dan diberitahukan melalui *email* kepada Pemilik.

9.12.3 Keadaan Dimana OID Harus Diubah

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

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

9.13 Ketentuan Penyelesaian Perselisihan/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 tetap diterapkan. Para pihak, termasuk PSrE TILAKA, rekanan, Pemilik, dan 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 Pengandal sepakat untuk mematuhi peraturan perundang-undangan dan regulasi yang berlaku di Indonesia. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.

9.16 Ketentuan yang Belum Diatur

9.16.1 Seluruh Perjanjian

PSrE TILAKA secara kontraktual mewajibkan semua PSrE TILAKA yang terlibat dalam penerbitan Sertifikat untuk mematuhi CP PSrE Induk dan semua panduan yang terkait.

9.16.2 Pengalihan Hak

Seluruh entitas yang beroperasi di bawah CPS tidak dapat 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 dilaksanakan, maka bagian CPS selanjutnya ditafsirkan sedemikian rupa sehingga 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 Pelepasan Hak)

PSrE TILAKA 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.

PSrE TILAKA menyediakan *Business Continuity Management* (BCM) dengan kendali yang wajar sesuai dengan kapabilitas PSrE TILAKA.

9.17 Provisi Lain

Tidak ada ketentuan.

9.18 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
Kemenkomdigi	Kementerian Komunikasi dan Digital
KITAP	Kartu Izin Tinggal Tetap
KITAS	Kartu Izin Tinggal Sementara
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.
Badan Usaha	Setiap badan hukum yang didirikan sesuai ketentuan peraturan perundang-undangan yang berlaku.
Channel	Perwakilan dari Pelanggan Korporasi atau Pelanggan Personal yang menggunakan Layanan Tanda Tangan Elektronik Tilaka melalui *Application Programming Interface* (API).
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.

Istilah	Definisi
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.
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. Dalam hal PSrE TILAKA melakukan hubungan kontraktual dengan RA eksternal untuk menjalankan fungsi sebagai RA, PSrE TILAKA berpedoman pada CPS dan prosedur yang berlaku di PSrE TILAKA.
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 Sertifikat Pemilik. Terhadap Pelanggan Korporasi, subjek dari Sertifikat Pemilik adalah

Istilah	Definisi
	pengurus, pengawas, dan/atau pekerja atau pihak lain yang memiliki hubungan kontraktual dengan pihak tersebut.
Pemilik	Pemilik untuk Sertifikat orang perseorangan/individu adalah WNI dan WNA yang bertindak baik untuk kepentingan dirinya sendiri maupun untuk entitas yang terafiliasi dengan badan usaha. Dalam hal ini, Pemilik berada dalam ruang lingkup Pelanggan dan merupakan subjek dari Sertifikat Pemilik.
Pemohon	WNI dan WNA 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 Pengandal	Perjanjian antara PSrE TILAKA dan Pengandal yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pengandal tersedia di Repositori.
Perjanjian Kerja Sama	Perjanjian antara PSrE TILAKA dan Pelanggan yang menentukan hak dan tanggung jawab para 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 Kemenkomdigi.
PSrE Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi.

Istilah	Definisi
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 Policy (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 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 Pengandal yang berisi informasi mengenai status Sertifikat.