CERTIFICATION PRACTICE STATEMENT

Nomor	**: MP-CA-001**
Revisi	**: 11**
Tanggal	**: 10 Agustus 2023**
Halaman	**: 69 halaman**
OID	**: 2.16.360.1.1.1.3.12.8.1**

PT SOLUSI IDENTITAS GLOBAL NET

OFFICE

Jl. Raya Lingkar Timur Km.1, Sidoarjo, Jawa Timur
Phone : (031) 8910919

FIND US HERE

www.esign.id
office@esign.id

Catatan :

- UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang diterbitkan **iOTENTIK/BSrE**

Dokumen ini disetujui secara elektronik.

Menyetujui,

Ditandatangani secara elektronik yang diterbitkan BSrE

Aries Kusdaryono

Direktur Tata Kelola Aplikasi Informatika
Kementerian Komunikasi dan Informatika
(selaku *Policy Authority* PSrE Induk)

Aries Handoko
Direktur

CATATAN PERUBAHAN DOKUMEN

REV No	TRACK No. / TANGGAL	DIUBAH OLEH	ALASAN PERUBAHAN DOKUMEN
01	82905	GRC Head	Mengubah penjelasan pada poin 1.1, 1.2, 1.3, 1.5, 2.1, 2.3, 3.2.4, 3.3.1, 3.4, 4.1.2, 4.7.6, 5.1.2, 5.2.1, 5.2.2, 5.3.2, 5.4.2, 6.2.9, 6.6.2, 6.6.3, 6.7, 6.8, 7.1, 8.7, 9.2, dan 9.3.1.
02	83423	GRC Head	Mengubah penjelasan pada poin 5.5.1, 8.7, 9.3.1, 9.7. Menghapus penjelasan OCSP responder pada poin 6.3.2. Menambahkan penjelasan tentang Pembatasan Tanggung Jawab Pemilik pada poin 9.8.3.
03	84795	GRC Officer	-Mengubah Poin 1.2 terkait penggunaan OID. -Mengubah Poin 1.3.2 terkait pelaksanaan audit terhadap RA. -Mengubah Poin 1.5 terkait penggunaan istilah Otoritas Kebijakan dan susunan PA PSrE e Sign. -Mengubah Poin 1.5.4 terkait persetujuan dari PSrE Induk. -Mengubah Poin 3.2.2 terkait persyaratan surat kuasa dengan kop atau email korporat. -Mengubah Poin 3.3.1 terkait layanan re-key. -Mengubah Poin 4.3.1 terkait verifikasi sumber permohonan sertifikat. -Mengubah Poin 4.5.1 terkait spesifikasi perangkat penyimpanan Kunci Privat Pemilik. -Menambah pernyataan pada Poin 5.1.1 terkait Pusat Pemulihan Bencana. -Menambah pernyataan pada Poin 5.3.2 terkait pemeriksaan latar belakang finansial. -Mengubah Poin 5.4.6, 5.5.4, dan 5.5.6 menjadi tidak ditentukan. -Mengubah Poin 6.1.6 terkait FIPS 186-4. -Mengubah Poin 6.2.10 terkait penghancuran kunci. -Mengubah Poin 7.1.2.1 terkait parameter keyUsage. -Mengubah Poin 10.2.2 dan 10.2.3 terkait OID.
04	6 April 2023	GRC Officer	-Menambah cover dan informasi dokumen. -Megubah halaman persetujuan untuk tanda

REV No	TRACK No. / TANGGAL	DIUBAH OLEH	ALASAN PERUBAHAN DOKUMEN
			tangan elektronik. -Menghapus kata “Pihak” pada penggunaan istilah Pihak Pengandal. -Menggunakan istilah “tidak ada ketentuan”. -Menghapus OID untuk Compliance dan AATL. -Penyesuaian dengan CP Induk versi 3.3.
05	12 April 2023	GRC Officer	-Menambahkan keterangan aplikasi web e Sign pada 4.1.2 poin b. -Mengubah 4.2.2 poin a, dengan menyertai alasan penolakan.
06	13 April 2023	GRC Officer	-Menambah pernyataan poin 4.7.1, terkait permohonan re-key untuk Sertifikat lama yang sudah dicabut, terkompromi, atau kedaluwarsa.
07	17 April 2023	GRC Officer	-Mengubah penyataan pada poin 9.4.2, bahwa PSrE e Sign tidak menyimpan informasi privat Pemohon yang ditolak. -Perbaikan tata cara pendaftaran pada poin 4.1.
08	26 Juni 2023	GRC Officer	-Menambah keadaan terjadinya pencabutan sertifikat pada poin 4.9.1. -Perubahan alamat URL OCSP pada poin 4.9.10. -Perubahan *DistributionPointName* CRL pada poin 7.1.2. -Perubahan *GeneralName* pada *AuthorityInfoAccess* poin 7.1.2. -Perubahan pada *accessLocation* pada *AuthorityInfoAccess* poin 7.1.2. -Perubahan link OCSP dan CRL pada poin 10.2.2. -Perubahan link OCSP dan CRL pada poin 10.2.3.
09	6 Juli 2023	GRC Officer	-Menambah identitas organisasi yang diperiksa pada poin 3.2.2. -Mengubah tahap pelaksanaan permohonan Sertifikat untuk organisasi/badan usaha/korporat pada poin 4.1.2. -Merubah tata bahasa terkait masa permohonan *re-key* pada poin 4.7.3. -Mengubah tampilan tabel pembangkitan pasangan kunci pada poin 6.1.1. -Menambah pernyataan terkait aktivasi Kunci Privat Pemilik pada poin 6.4.1.

REV No	TRACK No. / TANGGAL	DIUBAH OLEH	ALASAN PERUBAHAN DOKUMEN
			-Menambah pernyataan terkait konfigurasi sistem komputer PSrE e Sign pada poin 6.5.1. -Menghapus *subject* email untuk perorangan, individu terafiliasi perusahaan, dan segel elektronik pada poin 7.1.1. -Perubahan OID AuthorityInfoAccess ca Issuer URL pada poin 7.1.2. -Penambahan *subject alternative name email* pada poin 7.1.2. -Penambahan *subject alternative name email* pada poin 10.2.3.
10	2 Agustus 2023	GRC Officer	-Penghapusan atribut *Email* (E) pada poin 3.1.1. -Penghapusan atribut *Organization Name* (O) pada Perorangan dan Organisasi/Badan Usaha pada poin 3.1.1. -Penghapusan atribut *Organization Unit* (OU) pada Organisasi/Badan Usaha dan Personal Bagian dari Organisasi/Badan Usaha pada poin 3.1.1. -Penghapusan atribut *Organization Unit* (OU) pada *issuer name* untuk *Certificate Profile* PSrE e Sign dan Pemilik pada poin 7.1.1, 10.2.1, dan 10.2.3. -Penghapusan atribut *Organization Unit* (OU) pada *subject name* untuk *Certificate Profile* PSrE e Sign, Individu Terafiliasi Perusahaan, dan Segel Elektronik pada poin 7.1.1, 10.2.1, 10.2.2, dan 10.2.3. -Penghapusan atribut *Organization* (O) pada *subject name* untuk *Certificate Profile* Perorangan dan Segel Elektronik pada poin 7.1.1, 10.2.2, dan 10.2.3. -Konsistensi penggunaan *Common Name* (CN) dengan merek dagang e Sign.
11	10 Agustus 2023	GRC Officer	-Perubahan kalimat terkait Subject: OrganizationName pada poin 10.2.3. -Mengubah posisi Subject: AlternativeName berada di bawah Subject: CountryName pada poin 10.2.3.

DAFTAR ISI

BAB 1 PENGANTAR

PT Solusi Identitas Global Net melalui Departemen Teknologi Informasi adalah Penyelenggara Sertifikasi Elektronik (PSrE) yang beroperasi mengacu pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (untuk selanjutnya disebut "PSrE e Sign"). Sebagai perusahaan swasta, PSrE e Sign merupakan penyelenggara sertifikasi elektronik non-instansi yang menerbitkan Sertifikat kepada orang perseorangan (Warga Negara Indonesia/WNI) serta badan usaha, selain Aparatur Sipil Negara (ASN), Tentara Nasional Indonesia (TNI), dan Kepolisian Negara Republik Indonesia (Polri).

Dokumen *Certificate Practice Statement* (CPS) ini mendefinisikan kebijakan utama yang mengatur operasional PSrE e Sign. CPS menetapkan persyaratan bisnis, hukum, dan teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dan menyediakan layanan kepercayaan terkait untuk semua pemangku kepentingan. Persyaratan ini melindungi keamanan dan integritas PSrE e Sign dan terdiri atas seperangkat aturan yang berlaku secara konsisten di seluruh Indonesia, sehingga memberikan jaminan kepercayaan yang seragam di seluruh Infrastruktur Kunci Publik (IKP) Indonesia. CPS bukan merupakan perjanjian hukum antara PSrE e Sign dengan entitas yang terlibat dengan operasional e Sign seperti pemilik Sertifikat, Pengandal, dan partisipan lain, dimana perjanjian hukum yang dimaksud ditetapkan melalui perjanjian tersendiri.

Dokumen ini ditargetkan pada:

a. PSrE e Sign agar beroperasi sesuai dengan *Certificate Practice Statement* (CPS) dimana CPS tersebut selaras dan patuh terhadap ketentuan yang diatur dalam *Certificate Policy* (CP) PSrE Induk Indonesia.
b. Pemilik Sertifikat elektronik yang perlu memahami bagaimana proses autentikasi mereka dan apa kewajiban mereka sebagai pelanggan PSrE e Sign dan bagaimana mereka dilindungi oleh PSrE e Sign.
c. Pengandal yang perlu memahami fasilitas yang dimiliki oleh PSrE e Sign untuk mengelola Sertifikat elektronik sebelum dilakukan pengandalan.

Dengan mengikuti kerangka pembuatan CPS yakni sesuai format RFC 3647, beberapa judul sub bagian yang tidak berlaku ketentuannya atau belum ditentukan ketentuannya akan memiliki pernyataan "tidak ada ketentuan".

1.1. Ringkasan

CPS ini berlaku untuk semua Sertifikat elektronik yang diterbitkan oleh PSrE e Sign. Tujuan dari CPS ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan Sertifikat PSrE e Sign untuk menunjukkan kepatuhan terhadap peraturan perundang-undangan seperti Peraturan Menteri Kominfo No 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik. CPS ini disusun dengan menggunakan standar *Request for Comments* (RFC) 3647 tentang X.509 *Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework.*

CPS ini menetapkan tujuan, peran, tanggung jawab, dan praktik semua entitas yang terlibat dalam siklus hidup Sertifikat yang diterbitkan berdasarkan CPS ini. Dalam istilah sederhana, CPS menyatakan "apa yang harus dipatuhi", menetapkan kerangka aturan operasional untuk produk dan layanan.

CPS berisi ringkasan proses, prosedur, dan ketentuan umum yang berlaku sebagai acuan PSrE e Sign untuk mengelola Sertifikat elektronik yang telah diterbitkan.

Layanan yang diselenggarakan PSrE e Sign berdasarkan CPS ini adalah tanda tangan elektronik untuk *user* perorangan (Warga Negara Indonesia) dan personal dari badan usaha, serta segel elektronik untuk *user* badan usaha.

1.2. Nama Dokumen dan Identifikasi

Dokumen ini adalah *Certificate Practice Statement* (CPS) PSrE e Sign.

PSrE e Sign, sesuai kewenangannya, ditetapkan untuk memiliki *Object Identifier* (OID) dengan nomor identifikasi {joint-iso-itu-t(2) country(16) id(360) gov(1) kominfo(1) psre-induk(1) psre-Indonesia(3) psre-non-instansi(12) sign(8)}.

Berikut merupakan *Object Identifier* (OID) yang diterbitkan untuk e Sign dan turunannya:

OID e Sign	2.16.360.1.1.1.3.12.8
CPS	2.16.360.1.1.1.3.12.8.1

Selain OID untuk dokumen, berikut OID sesuai dengan ketentuan yang telah ditetapkan oleh Kementerian Komunikasi dan Informatika:

Individu WNI	2.16.360.1.1.1.5.1
Individu non-Instansi Online	2.16.360.1.1.1.5.1.2
Individu non-Instansi Online Level 2	2.16.360.1.1.1.5.1.2.2
Segel Elektronik	2.16.360.1.1.1.8
Badan Usaha	2.16.360.1.1.1.8.1

1.3. Partisipan Infrastruktur Kunci Publik (IKP)

1.3.1. Certification Authority (CA)/Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1. PSrE Induk Indonesia

PSrE Induk Indonesia adalah induk dari PSrE Indonesia (PSrE Berinduk) sebagaimana diatur dalam ketentuan peraturan perundang-undangan. PSrE Induk menerbitkan dan mencabut Sertifikat PSrE Indonesia (PSrE Instansi dan PSrE Non-Instansi) berdasarkan status Pengakuan yang diberikan oleh Kementerian Kominfo. PSrE Induk tidak menerbitkan sertifikat elektronik kepada Pemilik.

PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat Elektronik PSrE Indonesia, sebagaimana dirinci dalam CPS ini, termasuk:

a. Pengendalian terhadap proses pendaftaran;
b. Proses identifikasi dan autentikasi;
c. Proses penerbitan Sertifikat;
d. Publikasi Sertifikat;
e. Validasi Sertifikat;
f. Pencabutan Sertifikat; dan
g. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE Indonesia yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

1.3.1.2. PSrE Indonesia

PSrE Indonesia (PSrE Berinduk) adalah PSrE yang mendapatkan pengakuan dari Kementerian Komunikasi dan Informatika Republik Indonesia (Kementerian Kominfo) dengan berinduk kepada PSrE Induk yang diselenggarakan oleh Menteri Komunikasi dan Informatika Republik Indonesia

(Menteri Kominfo) yang Sertifikatnya telah ditandatangani oleh PSrE Induk. PSrE Indonesia menerbitkan Sertifikat kepada Pemilik. Ada 2 (dua) jenis PSrE Indonesia:

a. PSrE Instansi
   PSrE instansi adalah PSrE yang diselenggarakan oleh Instansi Penyelenggara Negara dan menerbitkan Sertifikat elektronik kepada entitas pemerintah.
b. PSrE Non-Instansi
   PSrE non-instansi adalah PSrE yang menerbitkan Sertifikat elektronik kepada entitas non-instansi. e Sign merupakan salah satu PSrE non-instansi yang memiliki kewenangan sesuai regulasi yang berlaku, diantaranya adalah sebagai berikut:
   - Melakukan pengendalian terhadap proses permohonan Sertifikat Pemilik;
   - Melakukan identifikasi dan autentikasi proses permohonan Sertifikat Pemilik;
   - Melakukan penerbitan Sertifikat Pemilik;
   - Melakukan penggantian kunci Pemilik;
   - Melakukan pencabutan Sertifikat Pemilik; dan
   - Melakukan pembuatan daftar Sertifikat Pemilik yang aktif dan yang dicabut.

   PSrE e Sign adalah PSrE Non Instansi yang menerbitkan Sertifikat elektronik, tanda tangan elektronik, segel elektronik untuk individu Warga Negara Indonesia dan organisasi yang berbadan hukum atau badan usaha di luar entitas pemerintah. PSrE e Sign tidak berinduk dan tidak menjadi induk bagi PSrE lain.

1.3.2. Otoritas Pendaftaran/*Registration Authority* (RA)

Registration Authority (RA) atau Otoritas Pendaftaran merupakan bagian dari PSrE e Sign dan PSrE e Sign menjalankan sendiri fungsi Otoritas Pendaftaran (RA) sebagai pengelola administrasi pendaftaran pemohon Sertifikat, pencabutan Sertifikat, penerbitan ulang, dan/atau perpanjangan Sertifikat. Dalam hal PSrE e Sign bertindak sebagai RA maka seluruh mekanisme administrasi seperti yang disebutkan di atas dikelola secara mandiri.

PSrE e Sign menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan identifikasi dan autentikasi Pemilik, permohonan Sertifikat, dan permohonan pencabutan Sertifikat sesuai dengan yang telah didefinisikan pada CPS dan dokumen terkait. PSrE e Sign melakukan audit terhadap RA (baik RA yang dilakukan sendiri maupun RA yang ditunjuk) untuk memastikan operasional RA sesuai dengan peraturan perundang-undangan dan CPS ini.

RA berkewajiban untuk melaksanakan fungsi-fungsi sebagai berikut:

a. Menyusun dan menjalankan prosedur pendaftaran untuk Pemohon Sertifikat;
b. Melakukan identifikasi dan autentikasi Pemohon Sertifikat;
c. Memulai atau meneruskan proses pencabutan Sertifikat; dan
d. Menyetujui atau menolak permohonan untuk memperbarui Sertifikat atau pembaruan kunci atas nama PSrE e Sign.

1.3.3. Pemilik

Pemilik (individu atau organisasi/badan hukum) adalah pihak yang identitasnya tertera dalam Sertifikat yang diterbitkan oleh PSrE dan sudah melalui proses verifikasi. Pemilik berarti subjek pemegang Sertifikat sekaligus entitas yang terikat dengan PSrE Indonesia penerbit Sertifikat. Sebelum dilakukan verifikasi identitas dan Sertifikat diterbitkan, entitas disebut sebagai Pemohon

1.3.4. Pengandal

Pengandal adalah entitas yang mempercayai informasi yang ada di dalam Sertifikat elektronik dan/atau tanda tangan elektronik yang diterbitkan oleh PSrE e Sign. Pengandal terlebih dahulu memeriksa respon dari *Certificate Revocation List* (CRL) atau *Online Certificate Status Protocol* (OCSP) PSrE e Sign yang sesuai sebelum memanfaatkan informasi yang ada dalam Sertifikat. Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama Pemilik dengan kunci publik. Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pengandal menggunakan informasi dalam Sertifikat untuk menentukan kecocokan penggunaan Sertifikat.

Pengandal menggunakan informasi dalam Sertifikat elektronik untuk:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi tanda tangan elektronik;
c. Memeriksa apakah Sertifikat elektronik termasuk dalam CRL dan/atau OCSP;
d. Penyetujuan atas batas tanggung jawab dan jaminan;

Pengandal meliputi lembaga keuangan/bank, perusahaan *e-commerce*, instansi penyelenggara negara dan entitas lain yang menggunakan tanda tangan elektronik di dalam layanannya.

1.3.5. Partisipan Lain

PSrE e Sign menentukan partisipan lain untuk bekerja sama menyelenggarakan layananannya dengan mendapat persetujuan dari Kementerian Kominfo.

1.3.5.1. Penyedia Layanan Pusat Data

Penyedia Layanan Pusat Data adalah pihak yang menyediakan layanan pusat data untuk operasional PSrE e Sign. Penyedia Layanan Pusat Data untuk PSrE e Sign menerapkan standar persyaratan keamanan informasi yang sesuai dan melaksanakan audit secara berkala.

1.4. Kegunaan Sertifikat

1.4.1. Penggunaan Sertifikat yang Semestinya

Sertifikat PSrE e Sign digunakan untuk menandatangani Sertifikat Pemilik, CRL, OCSP, dan Sertifikat penanda waktu, serta untuk verifikasi Sertifikat. Penggunaan Sertifikat Pemilik dibatasi sesuai *Key Usage* dan *Extended Key Usage* pada *Certificate Extension*. Sertifikat pemilik yang dikeluarkan PSrE e Sign digunakan untuk transaksi *digitalSignature* (tanda tangan elektronik) dan *nonRepudiation* (nirsangkal).

Sertifikat yang diterbitkan oleh PSrE e Sign adalah Sertifikat elektronik dengan level verifikasi identitas level 2 (dua) untuk individu/perorangan online dan level 3 (tiga) untuk badan usaha online sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Penggunaan yang tidak sesuai dapat berakibat pada hilangnya jaminan yang diberikan oleh PSrE e Sign kepada Pemilik Sertifikat dan Pengandal.

1.4.2. Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan sesuai CPS ini dilarang dipakai selain untuk penggunaan sebagaimana diatur pada Bagian 1.4.1.

1.5. Otoritas Kebijakan/*Policy Authority* (PA)

Policy Authority (PA) atau Otoritas Kebijakan adalah entitas yang ada di dalam PSrE e Sign. PA memiliki peran dan tanggung jawab sebagai berikut:

a. Menyusun, menetapkan, dan mengadministrasikan *Certificate Practice Statement* (CPS) PSrE e Sign;
b. Memastikan semua layanan, operasional, dan infrastruktur PSrE e Sign yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP lainnya yang memiliki tingkat verifikasi yang setara.

Policy Authority PSrE e Sign terdiri dari Direktur dan pihak-pihak yang ditunjuk, serta dibantu oleh *Policy Authority Officer* untuk melakukan kegiatan administratif PSrE e Sign.

1.5.1. Organisasi Pengelola Dokumen

Dokumen CPS dan dokumen terkait dikelola oleh PSrE e Sign dengan informasi berikut.

Policy Authority e Sign

PSrE e Sign – PT Solusi Identitas Global Net

Jalan Raya Lingkar Timur Km 1 Desa Banjarsari, Kecamatan Buduran Kabupaten Sidoarjo 61252

Email : tatakelola@esign.id

Telepon : 031-8910919

Fax : 031-8910928

Web : https://esign.id

1.5.2. Narahubung

Kontak yang dapat dihubungi dapat menggunakan informasi yang tertera pada poin 1.5.1

1.5.3. Personil yang Menentukan Kesesuaian CPS dengan Kebijakan

Policy Authority (PA) menentukan kesesuaian dan penerapan CPS ini berdasarkan CP induk Kementerian Kominfo dan hasil rekomendasi yang diterima oleh auditor independen ataupun ahli di bidang keamanan informasi.

1.5.4. Prosedur Persetujuan CPS

PSrE e Sign menyetujui CPS dan perubahan yang telah dibuat setelah mendapatkan persetujuan dari PSrE Induk. Perubahan CPS ini dilakukan setelah PSrE e Sign melakukan analisa kesesuaian dengan CP. PSrE e Sign akan menentukan apakah perubahan yang terjadi membutuhkan pemberitahuan kepada pihak yang berkepentingan dengan PSrE e Sign atau perubahan OID.

1.6. Definisi dan Akronim

Lihat pada Lampiran 1

BAB 2 TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI

2.1. Repositori

PSrE e Sign memelihara dokumen yang menunjang penyelenggaraan layanan PKI antara lain:

a. Sertifikat PSrE e Sign
b. CRL dan/atau status keaktifan Sertifikat
c. *Certificate Practice Statement* (CPS)
d. Perjanjian Pemilik
e. Perjanjian Pengandal
f. Kebijakan Privasi
g. Kebijakan Jaminan

2.2. Publikasi Informasi Sertifikat

PSrE e Sign mempublikasikan beberapa hal yang ada pada poin 2.1 dan dapat diakses publik melalui https://repository.esign.id.

2.3. Waktu atau Frekuensi Publikasi

a. CPS PSrE e Sign dan tiap perubahan dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui.
b. PSrE e Sign mempublikasikan data pencabutan Sertifikat (CRL) dalam waktu 30 (tiga puluh) menit setelah diperbarui. CRL diperbaharui sesuai penjelasan pada poin 4.9.7.

2.4. Kendali Akses pada Repositori

Informasi yang terdapat pada repositori publik merupakan informasi publik. PSrE e Sign memberikan akses *read-only*/hanya baca yang tidak dibatasi pada repositori publik ini. PSrE e Sign menerapkan kendali akses logis dan fisik untuk mencegah akses penulisan oleh pihak yang tidak berhak pada repositori tersebut. PSrE e Sign melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

BAB 3 IDENTIFIKASI DAN AUTENTIKASI

3.1. Penamaan

3.1.1. Tipe Nama

PSrE e Sign membuat dan menandatangani Sertifikat dengan subyek *Distinguished Name* (DN) yang tidak boleh kosong dan memenuhi standar ITU X.500. Berikut merupakan penjelasan DN Sertifikat yang diterbitkan PSrE e Sign.

a. *Common Name* (CN)
   Pada Sertifikat Pemilik perorangan/personil dari badan hukum yang diterbitkan oleh PSrE e Sign berisikan informasi nama lengkap pemegang Sertifikat. Sedangkan pada Sertifikat Pemilik organisasi/badan usaha berisikan informasi nama legal dari organisasi/badan usaha.

b. *Organization Name* (O)
   Pada Sertifikat Pemilik untuk personal bagian (terafiliasi) dari organisasi/badan usaha berisikan informasi nama legal dari organisasi/badan usaha.

c. *Organization Unit* (OU)
   Pada Sertifikat Pemilik perorangan berisikan informasi "personal".

d. *Country* (C)
   Pada Sertifikat Pemilik yang diterbitkan oleh PSrE e Sign berisikan negara kedudukan dari Pemilik Sertifikat.

DN	Keterangan	Perorangan	Organisasi/Badan Usaha	Personal Bagian dari Organisasi/Badan Usaha
CN	Common Name	nama lengkap pemegang Sertifikat	nama legal dari organisasi/badan usaha	nama lengkap pemegang Sertifikat
O	Organization Name	-	-	nama legal dari organisasi/badan usaha
OU	Organization Unit	Personal	-	-
C	Country	ID	ID	ID

3.1.2. Kebutuhan Nama yang Bermakna

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

Nama subjek dan penerbit yang terkandung dalam Sertifikat memiliki makna dalam arti bahwa PSrE e Sign memiliki bukti keterkaitan yang cukup antara nama dengan Pemilik. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh Pemilik yang sah atau perwakilan resmi dari Pemilik yang sah.

3.1.3. Anonimitas atau Pseudonimitas Pemilik

PSrE e Sign tidak menerbitkan Sertifikat anonim atau pseudonim.

3.1.4. Aturan Interpretasi Berbagai Bentuk Nama

Distinguished Name (DN) pada Sertifikat diinterpretasikan menggunakan standar X.500.

3.1.5. Keunikan Nama

Distinguished Name (DN) dalam Sertifikat yang diterbitkan merupakan karakter unik dan berdasarkan informasi yang disampaikan Pemilik pada saat melakukan permohonan Sertifikat elektronik kepada PSrE e Sign.

3.1.6. Pengakuan, Autentikasi, dan Peran Merek Dagang

Pemohon Sertifikat tidak diperbolehkan menggunakan nama atau konten yang melanggar hak kekayaan intelektual orang lain atau lembaga lain. PSrE e Sign tidak memverifikasi nama pemohon untuk penggunaan merek dagang. Hal tersebut merupakan tanggung jawab pemohon untuk memastikan penggunaan nama yang dipilih sah secara hukum. PSrE e Sign menolak permohonan penerbitan atau melakukan pencabutan Sertifikat yang menjadi bagian dari sengketa merek dagang. Tanggung jawab pemohon untuk memastikan penggunaan nama yang dipilih sah secara hukum.

3.2. Validasi Identitas Awal

3.2.1. Metode Pembuktian Kepemilikan Kunci Privat

Pasangan kunci Sertifikat Pemilik dibangkitkan dan disimpan oleh PSrE e Sign dimana kunci privatnya akan disimpan dan diamankan menggunakan modul kriptografis yang memenuhi persyaratan FIPS-140 level 2 dan hanya dapat diakses oleh Pemilik dengan minimal 2 (dua) faktor autentikasi.

3.2.2. Autentikasi dari Identitas Organisasi

Permohonan dari organisasi dibuat oleh pihak yang memiliki wewenang untuk mewakili organisasi tersebut. PSrE e Sign memeriksa identitas organisasi pemohon yaitu paling kurang:

a. Surat Permohonan yang memuat persetujuan untuk penerbitan Sertifikat Elektronik, yang diajukan oleh perwakilan organisasi yang secara sah memiliki kewenangan untuk bertindak mewakili organisasi tersebut;
b. Akta pendirian dan/atau akta perubahan terakhir dari organisasi;
c. Surat keputusan pengesahan organisasi;
d. Nomor Induk Berusaha (NIB) dari organisasi;
e. Nomor Pokok Wajib Pajak (NPWP) dari organisasi;
f. Salinan Kartu Tanda Penduduk (KTP) perwakilan organisasi yang memohonkan Sertifikat Elektronik;
g. Foto wajah perwakilan organisasi;
h. Nomor telepon seluler (ponsel)/*handphone* dari perwakilan organisasi;
i. Alamat *email* resmi dari perwakilan organisasi;
j. Jabatan (*role*) dari perwakilan organisasi;
k. Nomor telepon kantor organisasi;
l. *Email* resmi organisasi; dan
m. *Email* dari *sysadmin* yang ditunjuk oleh perwakilan organisasi

PsrE e Sign melakukan validasi atas identitas organisasi pemohon Sertifikat dengan:

a. Pemeriksaan data organisasi, perwakilan organisasi, dan surat keputusan pengesahan organisasi pada sistem instansi yang memiliki kewenangan untuk memberikan pengesahan organisasi sesuai ketentuan peraturan perundang-undangan (Kementerian Hukum dan HAM);
b. Pemeriksaan identitas perwakilan organisasi pada sistem pemerintahan yang mengelola administrasi kependudukan;
c. Data biometrik berupa swafoto dimana PSrE e Sign melakukan *liveness detection* untuk memastikan kebenaran/kesesuaian data dari perwakilan organisasi pemohon Sertifikat.

Di luar dokumen pendukung pengesahan badan hukum/badan usaha, perikatan antara organisasi yang menggunakan layanan PSrE e Sign akan dituangkan ke dalam Perjanjian Kerja Sama.

PSrE e Sign menyimpan dokumen dan catatan tentang jenis dan perincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari Sertifikat yang diterbitkan.

3.2.3. Autentikasi Identitas Individu

PSrE e Sign melakukan Identifikasi dan autentikasi identitas individu yang mengajukan permintaan Sertifikat. Untuk memastikan proses autentikasi identitas individu sesuai dengan ketentuan, Pemohon perlu menunjukkan :

a. Nama;
b. Nomor Induk Kependudukan (NIK);
c. Tanggal Lahir;
d. Salinan dokumen Kartu Tanda Penduduk (KTP);
e. Alamat email;
f. Nomor telepon; dan
g. Data biometrik berupa swafoto dimana PSrE e Sign melakukan *liveness detection* untuk memastikan kebenaran/kesesuaian data dan pemohon.

Terhadap proses autentikasi identitas individu, PSrE e Sign menerbitkan Sertifikat untuk Pemohon Sertifikat dengan klasifikasi Sertifikat level 2.

PSrE e Sign melakukan pemeriksaan, validasi, dan memastikan bahwa informasi yang tertera di dalam dokumen pendaftaran adalah valid dan autentik. PSrE e Sign melakukan pencocokan data, termasuk data biometrik berupa swafoto dengan basis data kependudukan yang dikelola oleh lembaga pemerintahan yang mengelola administrasi kependudukan.

PSrE e Sign menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk melakukan autentikasi identitas individu selama Sertifikat Pemilik aktif.

3.2.4. Informasi Pemilik yang Tidak Terverifikasi

PSrE e Sign tidak menerbitkan Sertifikat untuk pemohon yang informasinya tidak dapat diverifikasi pada poin 3.2.2 dan 3.2.3.

3.2.5. Validasi Otoritas

PSrE e Sign menggunakan mekanisme yang tepat dalam melakukan pemeriksaan terhadap keautentikan informasi pemohon. PSrE e Sign memastikan bahwa informasi yang diberikan oleh pemohon (baik individu maupun organisasi) akan dilakukan proses pemeriksaan sesuai dengan kegunaan informasi/dokumen tersebut.

3.2.6. Kriteria Inter-Operasi

Tidak ada ketentuan.

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

3.3.1. Identifikasi dan Autentikasi untuk Re-Key Rutin

Pemilik melakukan pengajuan permohonan penggantian kunci (*re-key*) sebelum masa berlaku Sertifikat berakhir. Terhadap permohonan penggantian kunci (*re-key*), PSrE e Sign akan menerbitkan pasangan kunci baru dengan masa validitas Sertifikat baru. PSrE e Sign memproses layanan

penggantian kunci (*re-key*) yang diawali dengan penandatanganan elektronik formulir permohonan *re-key* dengan sertifikat Pemilik/Pemohon *Re-Key* yang masih berlaku.

3.3.2. Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan

Setelah Sertifikat dicabut selain karena alasan pembaruan, Pemilik mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

3.4. Identifikasi dan Autentikasi dari Permintaan Pencabutan

Permohonan untuk mencabut Sertifikat diajukan oleh pemegang Sertifikat dengan cara menghubungi PSrE e Sign melalui saluran komunikasi *email* helpdesk@esign.id. Pemohon wajib membuktikan kepemilikan/penguasaan terhadap informasi data pemegang Sertifikat yang dimiliki oleh PSrE e Sign seperti *email* dan nomor telepon.

Untuk identifikasi dan autentikasi permintaan pencabutan dari pemilik Sertifikat personal bagian dari organisasi/badan usaha atau Sertifikat badan usaha maka dikoordinasikan oleh orang yang berwenang mewakili organisasi tersebut dengan menyebutkan alasan dari permintaan pencabutan.

Jika dibutuhkan PSrE e Sign meminta syarat tambahan untuk melakukan autentikasi permohonan pencabutan Sertifikat sesuai point 3.2.

BAB 4 PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT

Siklus hidup Sertifikat PSrE e Sign meliputi pendaftaran, penerbitan, perubahan, dan pencabutan Sertifikat. Untuk perubahan Sertifikat, terdapat 3 (tiga) metode, yaitu:

a. Pembaruan Sertifikat (*Certificate Renewal*), yaitu Sertifikat berisikan informasi dan kunci yang sama. PSrE e Sign tidak menyediakan layanan Pembaruan Sertifikat (*Certificate Renewal*).
b. Penggantian Kunci (*Certificate Re-Key*), yaitu Sertifikat berisikan informasi yang sama dan masa berlaku yang dapat berbeda. Perubahan terjadi pada kunci yang berasosiasi dengan Sertifikat. PSrE e Sign menyediakan layanan *Re-Key* Sertifikat dan dapat dilihat pada Bagian 4.7.
c. Modifikasi Sertifikat (*Certificate Modification*), yaitu Sertifikat berisikan kunci yang sama tetapi sebagian isi dari Sertifikat mengalami perubahan. PSrE e Sign tidak menyediakan layanan Modifikasi Sertifikat (*Certificate Modification*).

4.1. Permohonan Sertifikat

Untuk memperoleh Sertifikat dari PSrE e Sign, Pemohon melakukan hal-hal berikut:

a. Melakukan pendaftaran akun e Sign melalui website aplikasi e Sign pada alamat https://esign.id dengan mempersiapkan alamat *email* yang valid atau *email* organisasi yang resmi.
b. Memberikan informasi yang dibutuhkan oleh PSrE e Sign untuk dapat dilakukan verifikasi informasi dalam rangka permohonan penerbitan Sertifikat.
c. Memberikan persetujuan terhadap syarat dan ketentuan pada Perjanjian Pemilik, Kebijakan Jaminan, dan Kebijakan Privasi.

4.1.1. Siapa yang Dapat Mengajukan Sebuah Permohonan Sertifikat

Pihak-pihak yang dapat mengajukan permohonan Sertifikat PSrE e Sign adalah:

a. Organisasi yang berbadan hukum atau badan usaha untuk menjadi Pemilik kepada PSrE e Sign diajukan oleh orang yang berwenang mewakili organisasi tersebut;
b. Permohonan dari individu Warga Negara Indonesia (WNI) hanya dilakukan oleh individu tersebut atau oleh orang lain atau organisasi yang secara resmi memiliki kewenangan untuk mewakili Pemohon tersebut;

PSrE e Sign dan/atau RA yang ditunjuk oleh PSrE e Sign 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 e Sign bertanggung jawab atas pemeliharaan sistem dan proses autentikasi identitas Pemohon Sertifikat. Pemohon Sertifikat bertanggung jawab dalam memberikan informasi identitas yang benar dan lengkap, sehingga PSrE e Sign dan/atau RA yang ditunjuk oleh PSrE e Sign dapat melakukan verifikasi atas identitas tersebut.

Berikut merupakan proses pendaftaran bagi perorangan/individu hingga Pemohon menerima Sertifikat yang dilakukan melalui aplikasi web e Sign:

a. Pemohon mengakses aplikasi web e Sign dan memilih tautan untuk pendaftaran akun e Sign.
b. Pemohon melakukan pendaftaran dengan memberikan *username*, *password*, dan alamat *email* yang valid.
c. Pemohon mendapatkan notifikasi dari *email* terkait aktivasi akun aplikasi e Sign dan menekan tautan pada *email* tersebut sebagai verifikasi *email* dan aktivasi akun aplikasi e Sign.
d. Pemohon akan diarahkan pada halaman pengisian identitas diri dan verifikasi *liveness detection.*
e. Pada proses ini juga dilakukan verifikasi nomor telepon seluler (ponsel) Pemohon.

f. Pemohon yang telah melakukan pengisian identitas diri dan verifikasi *liveness detection*, akan diarahkan untuk membaca dan memberikan persetujuan terhadap syarat dan ketentuan pada Perjanjian Pemilik, Kebijakan Jaminan, dan Kebijakan Privasi.
g. Pemohon yang telah melakukan *submit* permohonan, akan mendapatkan notifikasi *email* bahwa permohonan sedang diproses oleh Registration Authority (RA).
h. Apabila RA telah memberikan persetujuan permohonan setelah memverifikasi seluruh identitas yang diberikan, Pemohon mendapatkan notifikasi bahwa permohonan telah diterima. Namun apabila RA membutuhkan verifikasi tambahan yang diakibatkan ketidakjelasan data yang diberikan, maka Pemohon mendapatkan notifikasi bahwa RA tidak dapat memverifikasi data dan jika diperlukan RA akan melakukan verifikasi tambahan dengan metode lain (misal verifikasi melalui *video call*).
i. Pemohon melakukan pembayaran sesuai metode dan nominal yang diinginkan.
j. Jika pembayaran diterima dan sukses, Pemohon mendapatkan informasi Sertifikat telah diterbitkan dan Pemohon menyetujui isi dari Sertifikat yang diterbitkan.
k. PSrE e Sign menyimpan informasi pribadi yang diberikan Pemohon secara aman.

Bagi Pemohon Sertifikat untuk organisasi/badan usaha/korporat, permohonan Sertifikat dilakukan dengan cara:

a. Perwakilan organisasi/badan usaha/korporat sebagai Pemohon Sertifikat telah terdaftar dalam sistem e Sign sebagai akun perorangan/individu dengan menggunakan email resmi organisasi/badan usaha/korporat dan memiliki Sertifikat yang masih aktif.
b. Pemohon Sertifikat organisasi/badan usaha/korporat menggunakan fitur menambah organisasi/badan usaha/korporat pada menu *Profile* pada aplikasi e Sign.
c. Pemohon Sertifikat organisasi/badan usaha/korporat mengisi data-data dan mengunggah dokumen-dokumen yang dibutuhkan untuk pendaftaran, serta mengisi data-data pihak dari organisasi/badan usaha/korporat yang ditunjuk sebagai *sysadmin*.
d. Pemohon Sertifikat organisasi/badan usaha/korporat menandatangani secara elektronik formulir permohonan Sertifikat dan *submit*.
e. RA mendapatkan notifikasi dari aplikasi RA Admin dan melakukan pemeriksaan kelengkapan permohonan Sertifikat organisasi/badan usaha/korporat.Apabila RA menemukan data dan/atau dokumen yang tidak sesuai/tidak lengkap, RA akan menyampaikan hal tersebut kepada Pemohon Sertifikat organisasi/badan usaha/korporat melalui *email*.
f. RA melakukan pemeriksaan kelengkapan dan verifikasi identitas organisasi/badan usaha/korporat dengan sistem pemerintahan yang secara peraturan ketentuan perundang-undangan memiliki kapasitas dalam menyediakan informasi identitas organisasi/badan usaha/korporat.
g. Apabila verifikasi identitas organisasi/badan usaha/korporat tidak ditemukan perbedaan dan sesuai, RA memberikan notifikasi melalui *email* kepada Pemohon bahwa verifikasi telah dilakukan dan menyampaikan informasi bahwa sistem e Sign untuk digunakan pada *environment* organisasi/badan usaha/korporat sedang disiapkan paling lama 1 x 24 jam.
h. RA memberikan panduan penggunaan aplikasi *web* e Sign kepada *sysadmin* atau Pemohon.
i. Apabila sistem e Sign yang digunakan pada lingkungan organisasi/badan usaha/korporat telah disiapkan, RA menyampaikan kepada Pemohon bahwa sistem dapat digunakan.
j. Administrator sistem e Sign melakukan pendaftaran bagi pegawai-pegawai yang akan menggunakan aplikasi e Sign.
k. Pegawai-pegawai organisasi/badan usaha/korporat yang menggunakan aplikasi *web* e Sign, harus melaksanakan pendaftaran perorangan/individu seperti pada bagian sebelumnya.

PSrE e Sign telah menyusun dokumen *user manual* untuk memberikan panduan kepada Pemohon terkait dengan proses pendaftaran. Adapun dokumen user manual tersebut disampaikan pada *website* https://esign.id/.

4.2. Pemrosesan Permohonan Sertifikat

4.2.1. Melaksanakan Fungsi Identifikasi dan Autentikasi

PSrE e Sign menggunakan data dan informasi yang diajukan pemohon untuk memvalidasi identitas Pemohon sebagaimana yang diatur pada sub bab 3.2 dari CPS ini.

4.2.2. Persetujuan atau Penolakan Permohonan Sertifikat

PSrE e Sign hanya memberikan persetujuan terhadap permohonan Sertifikat yang telah memenuhi syarat sesuai poin 4.1. Berikut merupakan hal-hal yang dilakukan PSrE e Sign jika permohonan penerbitan Sertifikat tidak sesuai dengan syarat pada poin 4.1:

a. Sistem e Sign memberikan notifikasi bahwa identitas yang diberikan tidak sesuai dengan hasil verifikasi dari sistem lembaga pemerintah yang berwenang menyelenggarakan administrasi kependudukan secara nasional.
b. Apabila verifikasi identitas gagal dilakukan selama 3 (tiga) kali berturut-turut, sistem e Sign akan mengunci akun Pemohon dan Pemohon dapat menyampaikan *email* permohonan pembukaan blokir ke helpdesk@esign.id.

4.2.3. Waktu untuk Memproses Permohonan Sertifikat

Semua pihak yang terlibat dalam proses permohonan Sertifikat melakukan usaha untuk memastikan permohonan Sertifikat diproses tepat waktu. Dalam hal permohonan Pemohon mengandung kesalahan, Pemohon akan mendapatkan notifikasi kegagalan verifikasi identitas dan/atau informasi bahwa akun pemohon terkunci langsung dari sistem aplikasi *web* e Sign. Apabila permohonan disetujui dan verifikasi sudah sesuai, sertifikat diterbitkan tidak lebih dari 1 x 24 jam (hari kerja).

4.3. Penerbitan Sertifikat

4.3.1. Tindakan PSrE Selama Penerbitan Sertifikat

PSrE e Sign melakukan hal-hal berikut selama proses penerbitan Sertifikat:

a. Memastikan identitas Pemohon sebagaimana diatur pada poin 3.2.2 dan 3.2.3;
b. Melakukan verifikasi otoritas Pemohon sebagaimana diatur pada poin 3.2.5;
c. Mempersiapkan dan menandatangani Sertifikat saat semua persyaratan telah terpenuhi;
d. Memastikan bahwa Pemilik menerima Sertifikat sebagaimana diatur pada poin 4.4;
e. Memastikan ketersediaan Sertifikat bagi Pemilik setelah Pemilik secara formal menyetujui kewajibannya sebagaimana diatur pada poin 9.6.3.

4.3.2. Pemberitahuan ke Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

PSrE e Sign memberitahu Pemilik selambat-lambatnya 1 x 24 jam (hari kerja) terkait persetujuan dan keberhasilan penerbitan Sertifikat melalui email atau media lainnya.

PSrE e Sign memberitahu Pemilik bahwa mereka tidak dapat menggunakan Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

4.4. Pernyataan Persetujuan Sertifikat

4.4.1. Sikap yang Dianggap Sebagai Menyetujui Sertifikat

Setelah PSrE e Sign melakukan pemberitahuan kepada Pemilik Sertifikat terkait persetujuan penerbitan Sertifikat, Pemilik Sertifikat dianggap menerima Sertifikat jika tidak ada keluhan dari Pemilik dalam jangka waktu 7 (tujuh) hari kerja sejak tanggal penerbitan Sertifikat.

Apabila Pemilik memiliki keluhan terhadap Sertifikat yang diterbitkan oleh PSrE e Sign, maka Pemilik dapat mengajukan permohonan pencabutan Sertifikat sesuai ketentuan pada poin 4.9.

4.4.2. Publikasi Sertifikat Oleh PSrE

PSrE e Sign mempublikasikan Sertifikat PSrE e Sign pada repositori seperti yang tercantum pada poin 2.2. PSrE e Sign tidak mempublikasikan Sertifikat Pemilik.

4.4.3. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.5. Penggunaan Pasangan Kunci dan Penggunaan Sertifikat

4.5.1. Penggunaan Kunci Privat dan Sertifikat oleh Pemilik

Pemilik menitipkan Kunci Privatnya kepada PSrE e Sign setelah pembangkitan Pasangan Kunci dan penerbitan Sertifikat dilakukan. Pemilik melindungi mekanisme autentikasi (*username*, *password*, dan OTP) yang digunakan untuk mengaktifkan Kunci Privatnya.

PSrE e Sign melindungi Kunci Privat Pemilik dengan menggunakan *Hardware Security Module* (HSM) berstandar FIPS 140-2 Level 2 dan Kunci Privat PSrE e Sign dengan menggunakan HSM berstandar FIPS 140-2 Level 3. PSrE e Sign melakukan segala upaya untuk melakukan pengamanan dan penyimpanan Kunci Privat pemegang Sertifikat sehingga dapat digunakan secara maksimal oleh pemegang Sertifikat untuk menjalankan layanan PSrE e Sign. Salah satu bentuk pengamanan Kunci Privat Pemilik adalah dengan menerapkan *Multifactor Authentication* (MFA) bagi Pemilik yang akan menggunakan Kunci Privatnya.

Pemilik dan PSrE e Sign hanya menggunakan Kunci Privatnya untuk tujuan yang sudah ditentukan sesuai dengan poin 1.4.1.

4.5.2. Penggunaan Kunci Publik dan Sertifikat oleh Pengandal

Dalam proses pengandalan Sertifikat yang diterbitkan oleh PSrE e Sign, Pengandal memberikan jaminan dan pernyataan sesuai dengan ketentuan yang diatur pada poin 9.6.4.

Pengandal mengakses *Public Key* Sertifikat PSrE e Sign melalui repositori milik PSrE e Sign.

Pengandal memeriksa Sertifikat sesuai dengan standar yang telah ditentukan oleh Pengandal. Pengandal bertanggung jawab atas risiko yang muncul selama mengandalkan Sertifikat yang diterbitkan oleh PSrE e Sign. Jika Pengandal membutuhkan tambahan jaminan, Pengandal menyampaikan kebutuhan tersebut kepada PSrE e Sign sebelum menggunakan Sertifikat.

4.6. Pembaruan Sertifikat

4.6.1. Kondisi untuk Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.2. Siapa yang Dapat Meminta Pembaruan

Tidak ada ketentuan.

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Tidak ada ketentuan.

4.6.5. Sikap yang Dianggap Sebagai Persetujuan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.6. Publikasi Pembaruan Sertifikat oleh PSrE

Tidak ada ketentuan.

4.6.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Pihak Lain

Tidak ada ketentuan.

4.7. *Re-Key* Sertifikat

Re-key adalah suatu kondisi dimana pemegang Sertifikat melakukan permohonan pengajuan Sertifikat baru untuk mengganti Sertifikat lamanya. Sertifikat baru yang diterbitkan memiliki 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 hasil *re-key* memiliki masa berlaku yang baru.

4.7.1. Ruang Lingkup Penggantian Kunci

Re-key dilakukan oleh Pemilik selama:

a. Sertifikat lama yang akan diganti belum dicabut, terkompromi, atau kedaluwarsa.
b. PSrE e Sign menerbitkan Sertifikat baru kepada Pemilik setelah Pemilik membangkitkan atau memberi persetujuan untuk pembangkitan Pasangan Kunci baru dan terasosiasi dengan Sertifikat tersebut; dan
c. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi.

Apabila Sertifikat lama sudah dicabut, terkompromi, atau kedaluwarsa, maka Pemilik dapat mengajukan permohonan baru sesuai ketentuan pada poin 4.1.

4.7.2. Pihak yang Dapat Meminta *Re-Key* Sertifikat

Pihak yang dapat meminta *re-key* adalah Pemilik Sertifikat Elektronik yang diterbitkan oleh PSrE e Sign.

4.7.3. Pemrosesan Permintaan *Re-Key* Sertifikat

Pemilik Sertifikat dapat mengajukan permohonan *re-key* mulai 30 hari sebelum tanggal kedaluwarsa Sertifikat sampai dengan tanggal kedaluwarsa Sertifikat melalui fitur *re-key* pada halaman *Profile* aplikasi web e Sign. Permohonan *re-key* yang diajukan Pemilik Sertifikat, akan diterima oleh RA dan akan ditindaklanjuti dengan mengirimkan formulir permohonan *re-key* kepada Pemohon melalui media *email*. Bagi pengguna organisasi/badan usaha/korporat, permohonan *re-key* yang diterima oleh RA, akan dikonfirmasi kembali oleh RA kepada Administrator Sistem e Sign organisasi/badan usaha/korporat pemohon *re-key* dan diikuti dengan pengiriman formulir permohonan *re-key* bagi pengguna organisasi/badan usaha/korporat. Pengguna yang mendapatkan formulir tersebut, harus mengisi sesuai dengan informasi yang sesuai dan ditanda tangan secara elektronik pada aplikasi *web* e Sign. Formulir yang telah ditanda tangan elektronik, dikirimkan kembali kepada RA melalui media *email*. RA akan melakukan verifikasi terhadap informasi yang diberikan. Apabila verifikasi sudah sesuai, RA akan melakukan proses *re-key* seperti yang dijelaskan pada poin 4.3.

4.7.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Pemberitahuan penerbitan Sertifikat dilakukan sebagaimana dinyatakan pada bagian 4.3.2.

4.7.5. Sikap yang Dianggap Sebagai Menerima Sertifikat yang di *Re-Key*

Pemegang Sertifikat dianggap telah menerima Sertifikat hasil permohonan *re-key* ketika telah memenuhi kondisi yang dijelaskan pada poin 4.4.1.

4.7.6. Publikasi Sertifikat yang di *Re-Key* oleh PSrE

PSrE e Sign mempublikasikan Sertifikat PSrE e Sign hasil *re-key* pada repositori seperti yang tercantum pada poin 4.4.2.

4.7.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Pihak Lain

Tidak ada ketentuan.

4.8. Modifikasi Sertifikat

PSrE e Sign tidak melakukan modifikasi Sertifikat. Apabila terjadi kesalahan dalam proses penerbitan Sertifikat (misalnya ejaan), maka Sertifikat akan dicabut dan pemegang Sertifikat mengajukan pengajuan baru sesuai dengan ketentuan pada poin 4.3.

4.9. Pencabutan dan Pembekuan Sertifikat

4.9.1. Keadaan untuk Pencabutan

PSrE e Sign melakukan pencabutan Sertifikat Pemilik dalam kondisi berikut:

a. Informasi yang berafiliasi dengan nama dalam Sertifikat menjadi tidak valid;
b. Informasi apa pun dalam Sertifikat menjadi tidak valid;
c. Pemilik Sertifikat secara sah terbukti melanggar ketentuan di dalam perjanjian Pemilik, CPS, atau kontrak yang telah disepakati;
d. Kunci privat diyakini telah terkompromi, hilang, dan/atau rusak;
e. Ketika Pemilik Sertifikat PSrE e Sign atau pihak yang berwenang (sesuai pada poin 4.9.2) mengajukan untuk dilakukan pencabutan Sertifikat;
f. PSrE e Sign berhenti beroperasi;
g. Pemilik sudah tidak bisa lagi menggunakan Sertifikat (misal: meninggal);
h. Terjadi perubahan standar industri, kebijakan pemerintah, dan/atau Peraturan Perundang-Undangan yang mengakibatkan berubahnya keabsahan sertifikat; dan/atau
i. Alasan lainnya yang menurut PSrE e Sign dibenarkan perlunya pelaksanaan pencabutan Sertifikat

Informasi pencabutan Sertifikat dimasukkan dalam CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut disertakan dalam semua publikasi baru tentang informasi status Sertifikat sampai masa berlaku Sertifikat berakhir.

4.9.2. Pihak yang Dapat Meminta Pencabutan

Pencabutan Sertifikat dilakukan oleh Pemilik, pihak lain yang dapat membuktikan adanya kuasa dari pemegang Sertifikat untuk melakukan pencabutan Sertifikat, atau pihak berwenang yang memiliki kewenangan hukum, ketentuan perundang-undangan, atau perintah pengadilan. PSrE e Sign membuka kemungkinan proses pencabutan dilakukan oleh Pihak Ketiga. Adapun kriteria pihak ketiga yang mengajukan permohonan pencabutan adalah sebagai berikut:

a. Memiliki kuasa dari pemegang Sertifikat untuk melakukan permohonan pencabutan Sertifikat; dan
b. Merupakan pihak ketiga yang sama ketika melakukan permohonan penerbitan Sertifikat pihak yang memberi kuasa.

Dalam hal kondisi yang ada pada poin 4.9.1 terpenuhi, PSrE e Sign melakukan pencabutan Sertifikat tanpa permohonan pencabutan dari pemegang Sertifikat.

4.9.3. Prosedur Permintaan Pencabutan

PSrE e Sign melakukan verifikasi identitas dan wewenang pihak yang melakukan pencabutan sebelum proses pencabutan. Validasi identitas pelanggan diperlukan sesuai dengan poin 3.4. Permintaan pencabutan Sertifikat oleh Pemilik menyerahkan bukti bahwa:

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Terdapat alasan relevan lain yang diberikan oleh Pemilik.

Permintaan pencabutan oleh pihak ketiga disertai dengan surat kuasa pencabutan Sertifikat. Disamping surat kuasa tersebut, pihak ketiga juga menunjukkan bukti bahwa:

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Pemilik sudah tidak terasosiasi dengan institusi yang bersangkutan.

Permintaan pencabutan dapat dilakukan oleh pihak berwenang yang telah diberikan kewenangan hukum, ketentuan perundangan atau perintah pengadilan. PSrE e Sign akan memeriksa:

a. Surat Penugasan dari pejabat instansi berwenang; dan
b. Surat Kuasa

Proses akan dilanjutkan setelah dipastikan bahwa pihak berwenang memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan kepada Pemilik Sertifikat

4.9.4. Masa Tenggang Permintaan Pencabutan

PSrE e Sign tidak mengatur tenggang waktu terkait permohonan pencabutan Sertifikat yang diajukan oleh Pemegang Sertifikat, pihak ketiga, maupun pihak berwenang.

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

4.9.5. Tenggat Waktu Dimana PSrE Harus Memproses Permintaan Pencabutan

PSrE e Sign melakukan proses pencabutan Sertifikat paling lama 1 x 24 jam setelah persyaratan yang dibutuhkan untuk permohonan pencabutan Sertifikat dipenuhi oleh Pemegang Sertifikat atau Pihak Ketiga.

Informasi pencabutan Sertifikat dimasukkan dalam CRL dan/atau ditambahkan pada responder OCSP.

4.9.6. Persyaratan Pemeriksaan *Pencabutan* bagi Pengandal

Pengandal memvalidasi setiap Sertifikat yang dilakukan pencabutan melalui CRL dan/atau OCSP yang diterbitkan oleh PSrE e Sign sebagaimana diakses melalui repositori dan atau *server* OCSP PSrE e Sign.

Frekuensi validasi Sertifikat pada CRL dan/atau OCSP milik PSrE e Sign ditentukan oleh Pengandal.

4.9.7. Frekuensi Penerbitan CRL

PSrE e Sign melakukan penerbitan CRL paling lama 24 (dua puluh empat) jam dan diakses melalui https://repository.esign.id/.

4.9.8. Latensi Maksimum CRL

PSrE e Sign mempublikasikan CRL dalam waktu 30 (tiga puluh) menit setelah penerbitan.

4.9.9. Ketersediaan Pemeriksaan Pencabutan/Status Secara Daring

Sertifikat Pemilik yang telah dicabut dipublikasikan oleh PSrE e Sign dan diverifikasi melalui layanan server OCSP dan CRL milik PSrE e Sign di repositori.

PSrE e Sign memberikan layanan validasi secara daring. Pengandal memanfaatkan fasilitas tersebut untuk memeriksa status pencabutan Sertifikat.

4.9.10. Persyaratan Pemeriksaan Pencabutan Secara Daring

PSrE e Sign mempublikasikan daftar responder OCSP melalui alamat URL http://signocsp.esign.id/ocsp/issuing yang dapat diakses sepanjang waktu dalam kondisi normal atau di luar waktu pemeliharaan (*maintenance*).

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. Keadaan untuk Pembekuan

Tidak ada ketentuan.

4.9.14. Siapa yang Dapat Meminta Pembekuan

Tidak ada ketentuan.

4.9.15. Prosedur Permintaan Pembekuan

Tidak ada ketentuan.

4.9.16. Batas Waktu Pembekuan

Tidak ada ketentuan.

4.10. Layanan Status Sertifikat

4.10.1. Karakteristik Operasional

PSrE e Sign menyediakan layanan pemeriksaan status Sertifikat publik melalui CRL dan OCSP.

4.10.2. Ketersediaan Layanan

Layanan CRL atau OCSP tersedia sepanjang waktu untuk memastikan validasi status Sertifikat Pemilik kecuali di waktu pemeliharaan (*maintenance*) yang ditentukan oleh PSrE e Sign.

4.10.3. Fitur Opsional

Tidak ada ketentuan.

4.11. Akhir Berlangganan

Masa kepemilikan Sertifikat berakhir ketika Sertifikat Pemilik kedaluwarsa atau ketika permohonan pencabutan Sertifikat Pemilik disetujui dan berhasil dilakukan.

4.12. Pemulihan dan Eskro Kunci

4.10.4. Kebijakan dan Praktik Pemulihan dan *Eskro* Kunci

PSrE e Sign tidak melakukan *eskro* Kunci Privat PSrE e Sign dan Kunci Privat Pemilik

4.10.5. Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi

Tidak ada ketentuan.

BAB 5 KENDALI FASILITAS, MANAJEMEN, DAN OPERASIONAL

5.1 Kendali Fisik

5.1.1. Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan PSrE e Sign ditempatkan dalam Pusat Data dan Pusat Pemulihan Bencana di wilayah Negara Kesatuan Republik Indonesia. Pusat Data dan Pusat Pemulihan Bencana tersebut dilengkapi dengan perlindungan keamanan fisik dan logis yang memadai untuk menjaga keamanan akses sistem PSrE sesuai dengan *trusted role* yang telah ditetapkan.

Sistem cadangan PSrE e Sign telah disiapkan di Pusat Pemulihan Bencana yang secara geografis berbeda dengan Pusat Data sehingga jika terjadi sesuatu dengan Pusat Data, Pusat pemulihan Bencana tidak terkena dampaknya.

PSrE e Sign mengukur risiko untuk menentukan jarak antara Pusat Data dan Pusat Pemulihan Bencana yang mempertimbangkan risiko terhadap keberlangsungan layanan PSrE e Sign.

5.1.2. Akses Fisik

Perangkat PSrE e Sign dilindungi dari akses yang tidak sah. Untuk dapat mengakses ke Pusat Data dan Pusat Pemulihan Bencana, personel PSrE e Sign diwajibkan untuk melakukan pendaftaran terlebih dahulu untuk memastikan kebutuhan untuk mengakses fisik pusat data. Gedung Pusat Data dan Pusat Pemulihan Bencana dijaga 24 (dua puluh empat) jam oleh *security*, CCTV, dan 8 (delapan) lapis perimeter keamanan, yaitu:

a. gerbang utama;
b. pos keamanan
c. *access door* utama
d. *access door* akses terbatas
e. *mantrap* utama
f. *access door* ke ruang *server*
g. pintu *cage* PSrE e Sign
h. rak *server*

Di samping akses fisik tersebut, PSrE e Sign memelihara dan memeriksa log akses secara berkala untuk memastikan bahwa personil yang mengakses Pusat Data dan Pusat Pemulihan Bencana PSrE e Sign adalah peran terpercaya.

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 dihafal atau dicatat dan disimpan dengan pengamanan yang setara dengan pengamanan yang disediakan modul kriptografis, dan tidak disimpan bersamaan dengan modul kriptografis.

Proses pemeriksaan keamanan fasilitas penyimpanan perangkat PSrE e Sign dilaksanakan jika fasilitas akan ditinggalkan tanpa adanya pengawasan. Setidaknya proses pemeriksaan memverifikasi hal-hal berikut:

a. Semua *security container* (misal: brankas) sudah diamankan atau terkunci;
b. Sistem keamanan fisik (misal: kunci pintu, pelindung ventilasi, kunci rak) berfungsi dengan baik;
c. Area diamankan dari akses yang tidak berhak.

PSrE e Sign menunjuk satu atau beberapa personel yang berperan dan bertanggung jawab untuk melakukan pemeriksaan tersebut. Pemeriksaan dibuktikan dengan log yang dapat dipertanggungjawabkan.

Jika fasilitas tidak ditempati setiap waktu, maka personel terakhir yang meninggalkan fasilitas membuat lembaran *sign-out* yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

5.1.3. Daya dan Penyejuk Udara

PSrE e Sign memastikan daya listrik dan cadangan yang cukup untuk mengunci masukan secara otomatis, menyelesaikan setiap tindakan yang tertunda, dan merekam status peralatan sebelum kekurangan daya atau AC yang menyebabkan *shutdown*. Sistem IKP dilengkapi daya cadangan yang cukup untuk beroperasi selama 3 x 24 jam. Pusat Data dan Pusat Pemulihan Bencana PSrE e Sign dilengkapi dengan sistem *air conditioning* pada *raised floor* terkendali.

5.1.4. Keterpaparan Air

PSrE e Sign memastikan Pusat Data dan Pusat Pemulihan Bencana berada di kawasan bebas banjir dan Peralatan PSrE e Sign dilindungi terhadap air dan diletakkan di atas tanah dengan *raised floor.*

5.1.5. Pencegahan dan Perlindungan dari Kebakaran

Peralatan PSrE e Sign ditempatkan di fasilitas dengan sistem deteksi dan pemadam kebakaran yang memadai seperti deteksi asap dan sistem pemadam kebakaran otomatis.

5.1.6. Penyimpanan Media

PSrE e Sign melindungi media penyimpanan dari kerusakan akibat pencurian, akses fisik yang tidak sah, dan kecelakaan (air, api, dan elektromagnetik). Media yang berisi informasi audit, arsip, atau backup diduplikasi dan disimpan di lokasi yang terpisah dari lokasi Pusat Data dan Pusat Pemulihan Bencana PSrE e Sign (*off-site backup*). Proses tersebut diatur secara internal melalui prosedur backup & restore dan prosedur pengarsipan.

5.1.7. Pembuangan Limbah

Semua salinan cetak yang tidak digunakan dan/atau bersifat rahasia dihancurkan sebelum dibuang sehingga tidak dapat dibentuk kembali. Pelaksanaan lebih rinci diatur pada Prosedur Pengarsipan PSrE e Sign.

Informasi sensitif yang terdapat pada perangkat yang sudah tidak digunakan dihancurkan hingga tidak dapat dipulihkan kembali sebelum dibuang atau diserahkan ke pihak lain. Pelaksanaan lebih rinci diatur pada Prosedur *IT Policy*, khususnya pada bagian keamanan perangkat keras.

Perangkat kriptografis yang mengalami kerusakan dan/atau tidak digunakan dihancurkan secara fisik pada lingkungan yang aman dan dipastikan perangkat kriptografis tidak dapat dirangkai kembali. Pelaksanaan lebih rinci diatur pada Instruksi Kerja Penghancuran Fisik *Hardware Security Modul* (HSM).

5.1.8. *Backup Off-Site*

PSrE e Sign melakukan *backup off-site* dan hasil *backup off-site* tersebut ditempatkan pada lokasi selain Pusat Data dan Pusat Pemulihan Bencana dengan mekanisme pengamanan yang setara dengan pengamanan pada operasional PSrE. Proses backup *off-site* dilakukan penyimpanan setiap 7 (tujuh) hari sekali sesuai yang dijelaskan pada prosedur *offline backup*.

5.2. Kendali Prosedur

5.2.1. Peran Terpercaya

Posisi untuk peran yang dipercaya (*trusted roles*) termasuk namun tidak terbatas pada:

a. **Manajer PsrE**
   Melakukan penetapan terkait kebutuhan bisnis dan kebijakan internal PSrE e Sign.
b. ***Policy Authority* (PA)**
   Menetapkan kebijakan PSrE e Sign.
c. ***Internal Auditor***
   Melakukan audit internal operasional PSrE.
d. ***Security Officer***
   Mengelola penerapan kebijakan dan praktik keamanan PSrE.
e. **Administrator Aplikasi PSrE**
   Melakukan operasional dan pemeliharaan sistem aplikasi PSrE.
f. **Administrator HSM**
   Melakukan operasional dan pemeliharaan HSM PSrE e Sign.
g. **Administrator Sistem Operasi**
   Melakukan operasional dan pemeliharaan sistem operasi di lingkungan PSrE e Sign.
h. **RA Administrator**
   Mengelola akses sistem *Registration Authority*, mengelola siklus pendaftaran pemohon hingga monitoring akun e Sign.
i. ***Cryptographic Materials Custodian***
   Menjaga perlengkapan seremoni pembangkitan kunci PSrE, aktivasi PSrE, dan inventaris *credential* fisik, serta memastikan keamanannya.
j. ***Key Shareholder***
   Memegang *credential* fisik untuk kuorum HSM.

Peran tersebut secara detail dijelaskan melalui dokumen internal PSrE e Sign.

5.2.2. Jumlah Orang yang Dibutuhkan untuk setiap Tugas

PSrE e Sign telah memetakan *trusted roles* yang akan menjalankan setiap proses bisnis yang ada. Terkait dengan faktor keamanan, pada beberapa proses bisnis PSrE e Sign dijalankan oleh lebih dari 1 (satu) orang dan untuk beberapa tugas berikut membutuhkan 2 (dua) orang atau lebih:

a. Pembangkitan kunci PSrE e Sign
b. Penandatanganan Sertifikat PSrE
c. Pencabutan Sertifikat PSrE
d. Pencadangan Kunci Privat PSrE e Sign

Proses yang membutuhkan kendali multipersonel seperti di atas, tidak boleh dilakukan oleh personel yang bertugas sebagai peran Auditor.

5.2.3. Identifikasi dan Autentikasi untuk Setiap Peran

PSrE e Sign memastikan seluruh pegawai dengan peran terpercaya telah diidentifikasi dan diautentikasi sesuai ketentuan Perusahaan serta mendapatkan mandat melalui Surat Penugasan.

Autentikasi *trusted roles* dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi tersebut 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 Memerlukan Pemisahan Tugas

PSrE e Sign memastikan Peran di bawah tidak boleh saling merangkap pada satu waktu:

a. *Policy Authority* dan administrator operasional
b. *Internal Auditor* dan semua peran lain
c. Pengembang aplikasi dan semua peran lain

5.3. Kendali Personil

5.3.1. Persyaratan Kualifikasi, Pengalaman, dan Penugasan

Setiap personil PSrE e Sign yang memiliki peran dan terpercaya dipilih berdasarkan keterampilan, pengalaman, kepercayaan, dan integritas sesuai dengan persyaratan sebagai berikut:

a. Bukti latar belakang yang diperlukan, kualifikasi, dan pengalaman yang diperlukan untuk secara efisien dan memadai dalam melaksanakan tanggung jawab pekerjaan mereka; dan
b. Surat Keterangan Catatan Kepolisian (SKCK).

Setiap personil PSrE e Sign yang ditunjuk sebagai *trusted roles*, diangkat secara resmi melalui surat penugasan dari Direktur.

5.3.2. Prosedur Pemeriksaan Latar Belakang

PSrE e Sign melakukan prosedur verifikasi identitas personil sekurang-kurangnya 5 (lima) tahun sekali (tentatif) yang meliputi:

a. Kontak Referensi Pekerjaan;
b. Pendidikan atau sertifikasi;
c. Identifikasi Kepegawaian (Kartu Pegawai) dan/atau Kependudukan (KTP);
d. Surat Keterangan Catatan Kepolisian (SKCK); dan
e. Informasi finansial dari sistem pemeriksaan finansial yang diakui di Negara Kesatuan Republik Indonesia.

Prosedur lebih rinci terkait pemeriksaan latar belakang personil PSrE e Sign tertuang dalam Prosedur *Background Checking* Calon Pegawai.

5.3.3. Persyaratan Pelatihan

Semua personil PSrE e Sign akan menerima pelatihan yang mencakup operasional PSrE e Sign, namun tidak terbatas pada hal-hal berikut:

a. Pelatihan operasional IKP (termasuk perangkat keras, perangkat lunak PSrE e Sign memberikan pelatihan keterampilan;
b. Prosedur operasional dan keamanan; dan
c. CPS yang berlaku.

PSrE e Sign melakukan evaluasi terhadap kecukupan kompetensi personil PSrE minimal 1 (satu) kali dalam setahun.

5.3.4. Frekuensi dan Persyaratan Pelatihan Ulang

PSrE e Sign akan memberikan pelatihan kepada personil yang mengisi posisi *Trusted Roles*/Peran terpercaya sebanyak yang dibutuhkan untuk memastikan personil tersebut mempertahankan tingkat kemampuan yang dipersyaratkan untuk melakukan tanggung jawab pekerjaan.

5.3.5. Frekuensi dan Urutan Rotasi Pekerjaan

PSrE e Sign memastikan bahwa dalam hal terjadi rotasi pegawai tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

5.3.6. Sanksi untuk Tindakan Tidak Terotorisasi

Sanksi terhadap personil yang melakukan tindakan yang tidak sah atau melanggar ketentuan pada CPS dan prosedur yang berlaku pada PSrE e Sign akan diberikan sanksi sesuai kebijakan PSrE e Sign. Pemberian sanksi akan berpengaruh terhadap *role* yang dimiliki oleh personil tersebut.

5.3.7. Persyaratan Kontraktor Independen

Pegawai kontrak yang digunakan PSrE e Sign untuk menjalankan proses bisnis mematuhi dan memenuhi persyaratan yang diatur dalam CPS ini dan dokumen Perusahaan yang terkait.

5.3.8. Dokumentasi yang Diberikan kepada Personel

PSrE e Sign telah menyediakan kepada para personilnya, dokumentasi untuk menjalankan proses bisnis sesuai seperti Manual Perusahaan, Prosedur Operasional, dan Instruksi Kerja yang sesuai dengan *Certificate Practice Statement* (CPS) ini.

5.4. Prosedur Log Audit

PSrE e Sign menyusun log audit untuk semua kejadian yang terkait dengan keamanan PSrE e Sign. Semua log audit keamanan, elektronik dan non elektronik, disimpan dan tersedia selama untuk kebutuhan operasional dan proses audit.

5.4.1. Jenis Kejadian yang Direkam

Log kejadian pengelolaan sertifikat yang terdapat pada sistem PSrE teridentifikasi dan terekam secara otomatis dengan menggunakan fitur dari sistem PSrE e Sign. Log pada PSrE e Sign menyimpan informasi dengan poin-poin sebagai berikut :

a. Tipe kejadian,
b. Nomor seri atau urutan rekaman,
c. Tanggal dan waktu terjadi rekaman,
d. Asal perekaman,
e. Indikator sukses atau gagal jika perlu, dan
f. Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut

Penunjuk waktu yang digunakan pada sistem PSrE e Sign disinkronkan dengan sumber waktu dengan ketelitian 1 (satu) menit.

5.4.2. Frekuensi Pemrosesan Log

PSrE e Sign melakukan peninjauan log sesuai dengan Prosedur Pencatatan Log. Pemeriksaan *log* bertujuan untuk memastikan setiap penyimpangan/anomali/peringatan yang diberikan oleh sistem PSrE e Sign. Di samping itu, pemeriksaan tersebut dilakukan untuk memastikan dan memverifikasi bahwa log tidak dirusak, diacak, dan tidak adanya jenis kehilangan yang lain.

5.4.3. Periode Retensi untuk Log Audit

Log audit PSrE e Sign disimpan dalam jangka waktu 1 (satu) tahun.

5.4.4. Proteksi Log Audit

Log audit dilindungi untuk mencegah perubahan dan mendeteksi gangguan serta untuk memastikan bahwa hanya individu dengan akses terpercaya yang berwenang yang mampu melakukan operasi apa pun tanpa memodifikasi integritasnya.

5.4.5. Prosedur Backup Log Audit

PSrE e Sign melakukan backup Log audit dan ringkasan audit setiap bulan. Media backup disimpan dalam suatu lokasi yang aman.

5.4.6. Sistem Pengumpulan Audit (Internal vs Eksternal)

Tidak ada ketentuan.

5.4.7. Pemberitahuan ke Subjek Penyebab Kejadian

Tidak ada ketentuan.

5.4.8. Asesmen Kerentanan

PSrE e Sign melakukan penilaian kerentanan dari sistem CA dan sistem RA atau komponen-komponennya secara berkala setiap 1 (satu) tahun sekali dan insidentil apabila dibutuhkan. Penilaian ini bertujuan untuk memastikan bahwa sistem yang dimiliki PSrE e Sign andal dari ancaman internal maupun eksternal yang berdampak pada kualitas layanan PSrE e Sign. Adapun ruang lingkup asesmen kerentanan yang dilakukan adalah namun tidak terbatas kepada penetration testing dan performance testing sesuai pada prosedur manajemen kerentanan yang telah ditetapkan PSrE e Sign.

PSrE e Sign melaksanakan *penetration testing* yang dilakukan pihak eksternal 1 (satu) kali setiap tahun dan kondisional untuk *penetration testing* yang dilakukan secara internal sesuai dengan kebutuhan.

5.5. Pengarsipan *Record*

5.5.1. Tipe *Record* yang Diarsipkan

PSrE e Sign melakukan penyimpanan rekaman/arsip berupa:

a. Siklus hidup operasi Sertifikat termasuk di dalamnya permohonan Sertifikat, permintaan pencabutan, dan permintaan *re-key*.
b. Semua Sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh PSrE e Sign yang tersedia pada repositori
c. Data konfigurasi sistem IKP
d. Dokumen CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini.
e. Data audit.
f. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI).
    1) Penunjukan dan pencabutan peran dan kewenangan;
    2) Akses pengunjung ke fasilitas PSrE e Sign;
    3) Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
    4) Deteksi dan tindakan terhadap insiden keamanan;
    5) Latihan keadaan darurat;
    6) Tindakan dan penilaian risiko;
    7) Perubahan aset, prosedur, dan tanggung jawab; dan
    8) Perubahan dokumentasi.

5.5.2. Periode Retensi Arsip

PSrE e Sign menyimpan catatan/arsip sebagaimana pada poin 5.5.1 setidaknya selama 5 (lima) tahun.

Perangkat lunak dan perangkat keras yang dibutuhkan untuk membaca catatan/arsip ini dipelihara selama masa retensi.

5.5.3. Perlindungan Arsip

Catatan yang diarsipkan oleh PSrE e Sign dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan yang diarsipkan dan aplikasi yang dibutuhkan untuk memproses arsip akan dipelihara dan dilindungi.

Muatan arsip tidak diungkap kecuali berdasarkan ketentuan pada poin 9.3 dan 9.4. Catatan dari transaksi individu diungkap berdasarkan permintaan dari Pemilik yang terlibat dalam transaksi atau berdasarkan permintaan dari agen pemilik yang dikenali oleh hukum.

5.5.4. Prosedur Backup Arsip

Tidak ada ketentuan.

5.5.5. Persyaratan Pemberian Penanda Waktu pada Rekaman Arsip

Rekaman arsip PSrE e Sign diberi stempel waktu (*time stamping*) ketika dibuat.

5.5.6. Sistem Pengumpulan Arsip (Internal vs Eksternal)

Tidak ada ketentuan.

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Permohonan untuk mengakses informasi di dalam arsip hanya boleh diberikan oleh pihak yang dipercayakan melalui *Trusted Roles. Trusted Roles* melakukan pemeriksaan terhadap sampel dari arsip sedikitnya 1 (satu) kali dalam setahun untuk memastikan integritas dari informasi rekaman dalam arsip.

Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh *trusted roles.*

5.6. Pergantian Kunci

Terkait dengan adanya potensi risiko terhadap bocornya kunci privat PSrE e Sign, kunci tersebut diganti dengan kunci baru yang digunakan dalam penandatanganan Sertifikat. Dalam hal telah diterbitkannya kunci baru PSrE e Sign, PSrE e Sign melakukan pemberitahuan kepada Pemilik Sertifikat dan Pengandal.

Sertifikat lama yang masih berlaku akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat pada Sertifikat lama tersebut kedaluwarsa.

Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka Kunci Privat lama disimpan dan dilindungi sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat lama habis masa berlakunya.

PSrE e Sign tidak membangkitkan (*generate*) Sertifikat Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat PSrE e Sign.Dengan demikian, pasangan kunci PSrE e Sign dibangkitkan lagi paling lambat pada saat Sertifikat PSrE e Sign kedaluwarsa dikurangi masa berlaku Sertifikat Pemilik.

5.7. Pemulihan Bencana dan Keadaan Terkompromi

5.7.1. Prosedur Penanganan Insiden dan Keadaan Terkompromi

PSrE e Sign telah memiliki serangkaian kebijakan dan prosedur yang berkaitan dengan manajemen insiden dan dikinikan secara berkala atau sesuai kebutuhan. Dalam hal terjadi insiden yang dapat mengganggu operasional PSrE e Sign, maka PSrE e Sign akan melakukan investigasi terkait dengan dampak yang ditimbulkan dari insiden tersebut. Penanganan insiden disesuaikan dengan dampak dan tingkat kerusakan yang dihasilkan. Jika dampak yang dihasilkan oleh insiden tersebut katastropik atau dalam keadaan yang terkompromi, maka PSrE e Sign akan melakukan pemberitahuan kepada Kementerian Komunikasi dan Informatika untuk menginformasikan kondisi dan pelaksanaan prosedur kunci privat PSrE e Sign terkompromi sesuai poin 5.7.3.

PSrE e Sign menginformasikan PSrE Induk apabila mengalami insiden, termasuk namun tidak terbatas pada:

a. Terdeteksinya atau adanya indikasi sistem PSrE e Sign terkompromi;

b. Adanya upaya untuk menembus sistem PSrE Indonesia, baik secara fisik maupun elektronik;
c. Serangan *Denial of Service* pada sistem PSrE e Sign;
d. 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 Indonesia segera memulihkan penerbitan CRL secepat mungkin; dan/atau
e. CRL dan/atau OCSP *responder* tidak dapat diakses oleh publik.

Semua sistem pencadangan/pemulihan diuji minimal setahun sekali

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

Ketika sumber daya komputer, perangkat lunak, dan/atau data rusak, PSrE e Sign akan melakukan hal berikut:

a. Menjalankan proses manajemen insiden yang berlaku di PSrE e Sign serta menyampaikan kondisi terkini ke PSrE induk;
b. Memastikan integritas sistem telah dipulihkan sebelum mengembalikan pada operasional normal dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup;
c. Mengoperasikan kembali PSrE e Sign dengan memberikan prioritas pada kemampuan untuk membangkitkan informasi status Sertifikat sesuai jadwal penerbitan CRL; dan
d. Bila kunci penandatanganan PSrE e Sign rusak, operasional PSrE e Sign segera dikembalikan secepat mungkin dengan memberikan prioritas ke restore pasangan kunci PSrE e Sign yang terdapat pada media backup.

Jika Pusat Data dan Pusat Pemulihan Bencana tidak dapat memulihkan kemampuan pencabutan Sertifikat dalam jangka waktu yang wajar, maka sistem PSrE e Sign akan diperlakukan sebagai PSrE e Sign terkompromi.

5.7.3. Prosedur Kunci Privat Entitas Terkompromi

Dalam hal kunci privat PSrE e Sign terkompromi, hilang, hancur, atau dicurigai terkompromi, maka PSrE e Sign akan memastikan informasi terkait dengan kejadian tersebut dan melakukan investigasi untuk memastikan penyebab dan dampak kerusakan yang dihasilkan. Hal tersebut digunakan untuk memutuskan tindak lanjut yang dilakukan, apakah perlu mencabut seluruh Sertifikat yang telah diterbitkan dan dan membangkitkan pasangan kunci PSrE e Sign yang baru. PSrE e Sign menyampaikan kepada PSrE Induk kondisi terkini terkait dengan dugaan atau kondisi kunci privat PSrE e Sign terkompromi.

Terkait dengan terjadinya kunci privat PSrE yang mengalami kompromi, hilang, hancur, atau dicurigai terkompromi, PSrE e Sign segera mengkomunikasikan kepada pemegang Sertifikat, pengandal dan PSrE Induk melalui media komunikasi PSrE e Sign serta melakukan pencabutan Sertifikat Pemilik yang terkait dengan Kunci Privat yang terkompromi tersebut.

PSrE e Sign menjadikan upaya penanggulangan kunci privat PSrE e Sign terkompromi, hilang, hancur, atau dicurigai terkompromi sebagai proses perbaikan berlanjut dan didokumentasikan melalui instruksi kerja manajemen insiden PSrE e Sign.

PSrE e Sign meminta penerbitan Sertifikat baru ke Menteri Komunikasi dan Informatika sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CP Induk.

PSrE e Sign membangkitkan Pasangan Kunci PSrE e Sign baru sesuai dengan prosedur yang ditetapkan dalam CPS.

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

5.7.4. Kapabilitas Keberlangsungan Bisnis Setelah Suatu Bencana

PSrE e Sign melakukan *mirroring system* sebagai *backup* layanan untuk memastikan layanan tetap berjalan ketika terjadi bencana, hal tersebut juga sebagai bagian dari rencana pemulihan bencana PSrE e Sign. PSrE e Sign memastikan rencana pemulihan bencana tersebut telah diuji, diverifikasi, dan terus-menerus diperbarui.

Layanan PSrE e Sign kembali pulih dalam kurun waktu paling lama 24 jam bila ada bencana.

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

5.8. Penutupan PSrE atau RA

Dalam hal terdapat situasi yang mengharuskan PSrE e Sign mengakhiri layanannya, berikut merupakan hal-hal yang dilakukan oleh PSrE e Sign:

a. Memberitahu Menteri Komunikasi dan Informatika dan/atau pihak berwenang lainnya terkait dengan penghentian penyelenggaraan layanan.
b. PSrE e Sign memberikan pemberitahuan melalui media komunikasi PSrE e Sign kepada para pihak seperti Pemilik Sertifikat, dan/atau pengandal terkait dengan status layanan ke pengguna yang terkena dampak;
c. PSrE eSign memastikan proses pencabutan semua Sertifikat pada saat penutupan dilakukan sampai selesai;
d. PSrE e Sign tetap mempertahankan arsip selama masa retensi arsip;
e. Memberi informasi status Sertifikat kepada Pemilik untuk tetap dapat diakses untuk jangka waktu 1 (satu) tahun setelah PSrE e Sign menghentikan layanan;
f. Tetap melakukan update CRL kepada Pemilik dan Pengandal;
g. Menyediakan dukungan berkelanjutan dan menjawab pertanyaan; dan
h. Melakukan penghancuran sistem IKP PSrE e Sign yang berisikan kunci privat PSrE e Sign dan kunci privat pemegang Sertifikat.

Selain hal-hal di atas, terdapat hak dan kewajiban yang masih tetap berlaku bagi para pihak sesuai dengan perjanjian yang telah disepakati sebelumnya.

Panduan lebih mendetail terkait penutupan PSrE e SIgn tercantum dalam Prosedur Penutupan PSrE e Sign.

BAB 6 KENDALI KEAMANAN TEKNIS

6.1. Pembangkitan dan Instalasi Pasangan Kunci

6.1.1. Pembangkitan Pasangan Kunci

Pembangkitan pasangan kunci PSrE e Sign dapat dilihat pada tabel di bawah ini.

Entitas	Level FIPS 140-2	Jenis Modul Kriptografis	Dibangkitkan Dalam Modul Kriptografis
PSrE Indonesia	3	Perangkat Keras	Ya
Time Stamp Authority	3	Perangkat Keras	Ya
OCSP Responder	3	Perangkat Keras	Ya
Pemilik untuk Tanda Tangan Elektronik	3	Perangkat Keras	Ya

6.1.2. Pengiriman Kunci Privat ke Pemilik

PSrE e Sign tidak melakukan pengiriman kunci privat kepada Pemilik Sertifikat.

6.1.3. Pengiriman Kunci Publik ke Penerbit Sertifikat

Tidak ada ketentuan

6.1.4. Pengiriman Kunci Publik PSrE e Sign kepada Pengandal

PSrE e Sign tidak secara langsung mengirimkan kunci publik PSrE e Sign kepada Pengandal, namun PSrE e Sign telah menyiapkan repository untuk Pengandal mengakses kunci publik tersebut. Adapun repository diakses melalui https://repository.esign.id/.

6.1.5. Ukuran Kunci

Sertifikat	Signing Algorithm	Encryption Algorithm	Panjang Kunci
PSrE e Sign	SHA-384	RSA	4096-bit
Pemilik Sertifikat	SHA-256	RSA	2048-bit

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

PSrE e Sign menggunakan algoritma RSA sebagai algoritma penandatanganan digital (digital signature algorithm), dimana RSA merupakan salah satu teknik pembangkitan, verifikasi, dan validasi yang sesuai standar FIPS 186-4 Digital Signature Standard (DSS).

6.1.7. Tujuan Penggunaan Kunci (pada field key usage X.509 v3)

Kunci privat PSrE e Sign dan Pemilik Sertifikat digunakan sesuai pada penjelasan poin 7.1.2.1 (*key usage*) dokumen ini.

6.2. Kendali Kunci Privat dan Kendali Teknis Modul Kriptografi

6.2.1. Kendali dan Standar Modul Kriptografi

PSrE e Sign menggunakan perangkat modul kriptografi yang memenuhi standar FIPS 140-2 Level 3 untuk membangkitkan Kunci Privat PSrE e Sign dan Kunci Privat Pemilik. Pada proses

penandatanganan, PSrE e Sign menggunakan perangkat modul kriptografi dengan standar yang sama.

6.2.2. Kendali Multipersonel (n dari m) Kunci Privat

PSrE e Sign mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa (n dari m) peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif. Adapun detil operasi kriptografis yang dilakukan mengacu pada poin 5.2.2 dokumen ini.

6.2.3. Eskro Kunci Privat

Kunci Privat PSrE e Sign dan Kunci Privat Pemilik tidak dieskro.

6.2.4. Cadangan (*Backup*) Kunci Privat

Kunci Privat PSrE e Sign di-*backup* dan disimpan secara aman dengan kendali multi personil untuk menjaga keberlangsungan layanan ketika terjadi gangguan. Adapun proses penyimpanan backup kunci privat tersebut dilakukan pada lokasi fisik yang berbeda.

Kunci Privat Pemilik di-*backup* selain melalui replikasi Pusat Data dan Pusat Pemulihan Bencana, juga dilakukan secara *offline-backup* yang dilakukan secara rutin setiap minggu dan berada di lokasi alternatif (*offsite-backup*).

6.2.5. Pengarsipan Kunci Privat

PSrE e Sign tidak mengarsipkan kunci privat, baik Kunci Privat PSrE e Sign maupun Kunci Privat Pemilik.

6.2.6. Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci Privat PSrE e Sign dan Pemilik dipindahkan dan disimpan dalam modul kriptografi dengan tujuan backup, keberlangsungan layanan atau dalam ruang lingkup pemulihan layanan. PSrE e Sign melakukan pemindahan kunci privat PSrE e Sign dengan melakukan enkripsi selama proses pemindahan. Di luar modul kriptografi, PSrE e Sign tidak melakukan pemindahan kunci privat tanpa proses enkripsi.

6.2.7. Penyimpanan Kunci Privat pada Modul Kriptografis

Kunci privat PSrE e Sign disimpan dalam modul kriptografis HSM berstandar FIPS 140-2 *Security Level* 3 dan kunci privat Pemilik disimpan dalam perangkat keras (Harddisk) berstandar FIPS 140-2 *Security Level* 2 dalam bentuk terenkripsi dan terlindungi kata sandi untuk menjamin keamanan dan menjaga kunci dari akses tidak sah. Adapun pengamanan Kunci Privat PSrE e Sign dan Pemilik diatur pada poin 4.5.1, 6.1.1.1, 6.1.1.2, dan 6.2.1.

6.2.8. Metode Pengaktifan Kunci Privat

Aktivasi operasi Kunci Privat PSrE e Sign dilakukan oleh personil yang berwenang dan memerlukan kendali multipersonel seperti yang dinyatakan dalam bagian 5.2.2. Kunci privat PSrE e Sign diaktifkan dengan mekanisme yang disediakan oleh penyedia modul kriptografi dan sesuai dengan standar keamanan seperti kendali fisik, kendali prosedur, dan kendali personel pada dokumen CPS ini.

Kunci Privat Pemilik akan aktif setelah Pemilik melakukan pembayaran atas biaya penggunaan layanan PSrE e Sign atau setelah RA melakukan persetujuan atas aktivasi akun korporat.

Pemilik bertanggung jawab untuk melindungi mekanisme autentikasi (*username*, *password*, dan OTP) yang digunakan untuk mengaktifkan Kunci Privatnya sesuai dengan kewajiban yang diatur dalam perjanjian pemilik atau kontrak berlangganan.

6.2.9. Metode Penonaktifan Kunci Privat

Modul kriptografis PSrE e Sign yang sudah diaktivasi dilakukan *monitoring* secara berkala sesuai prosedur pencatatan log. Dalam hal modul kriptografis akan dinonaktifkan, penonaktifan modul kriptografis PSrE e Sign dilakukan oleh peran terpercaya sesuai dengan prosedur penghancuran kunci yang dimiliki PSrE e Sign. Ketika PSrE e Sign tidak lagi beroperasi, maka Kunci Privat PSrE e Sign dihapus dari modul kriptografis.

Kunci Privat Pemilik dihancurkan setelah proses pencabutan (*revoke*) Sertifikat berhasil dilakukan atau saat Kunci Pemilik telah kedaluwarsa (*expired*). Pelaksanaan penghancuran Kunci Privat Pemilik dieksekusi menggunakan aplikasi e Sign. Proses ini tertuang dalam Prosedur Pengelolaan Kunci Pemilik.

6.2.10. Metode Penghancuran Kunci Privat

Dalam hal kunci privat PSrE e Sign tidak diperlukan lagi, personel yang termasuk dalam peran terpercaya melakukan *overwrite* kunci atau *factory reset* modul kriptografis bila pelaksanaan *overwrite* tidak berhasil. Apabila fungsi-fungsi atau perintah dalam modul kriptografis tidak dapat diakses, PSrE e Sign akan menghancurkan fisik modul kriptografis di lingkungan yang aman. Mekanisme penghancuran kunci privat PSrE e Sign dijelaskan pada prosedur penghancuran kunci PSrE e Sign dan akan dicatat dalam log sesuai ketentuan pencatatan log pada poin 5.4 dokumen ini.

Kunci Privat Pemilik dihancurkan setelah proses pencabutan Sertifikat telah berhasil dilakukan atau Kunci Privat Pemilik telah kedaluwarsa. Penghancuran Kunci Privat Pemilik dilakukan secara sistematis.

6.2.11. Peringkat Modul Kriptografi

Seperti diuraikan dalam bagian 6.2.1.

6.3. Aspek Lain dari Manajemen Pasangan Kunci

6.3.1. Pengarsipan Kunci Publik

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat. Adapun proses pengarsipan dilakukan selama 5 (lima) tahun. Rincian tentang pengarsipan diatur pada poin 5.5.

6.3.2. Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode penggunaan pasangan kunci berkaitan dengan periode operasional Sertifikat. Adapun jangka waktu operasional maksimum pasangan kunci yang ditetapkan untuk layanan PSrE e Sign adalah sebagai berikut:

Kunci	Jangka Waktu Operasional	Jenis Algoritma Kunci
PSrE e Sign	10 Tahun	4096 Bit Keys (RSA)
Sertifikat Pemilik	1 Tahun	2048 Bit Keys (RSA)
OCSP Responder	3 Tahun	2048 Bit Keys (RSA)
Time Stamp	3 Tahun	2048 Bit Keys (RSA)

6.4. Data Aktivasi

6.4.1. Pembangkitan dan Instalasi Data Aktivasi

Pembangkitan dan penggunaan data pengaktifan untuk mengaktifkan Kunci Privat PSrE e Sign dibuat pada saat *key ceremony*. Data pengaktifan dikelola dan disimpan secara aman oleh *trusted role*/peran terpercaya.

Pembangkitan Kunci Privat Pemilik terjadi setelah Pemilik melakukan pembayaran atas biaya layanan atau setelah RA menyetujui untuk pengaktifan akun korporat. Penggunaan data aktivasi Kunci Privat Pemilik dimasukkan oleh Pemilik saat aktivasi.

6.4.2. Perlindungan Data Aktivasi

Data pengaktifan PSrE e Sign dan Pemilik dilindungi oleh kombinasi mekanisme kontrol akses fisik dan teknologi kriptografi yang memadai. PSrE e Sign menyimpan data aktivasi dalam bentuk *smart card*/token fisik dengan perlindungan kata sandi.

6.4.3. Aspek Lain dari Data Aktivasi

Tidak ada ketentuan.

6.5. Kendali Keamanan Komputer

6.5.1. Persyaratan Teknis Keamanan Komputer Spesifik

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

a. Mewajibkan login terautentikasi bagi Peran Terpercaya;
b. Menyediakan kendali akses dengan kewenangan yang minimal;
c. Menyediakan kapabilitas audit keamanan (dilindungi integritasnya);
d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;
e. Menyediakan perlindungan mandiri untuk sistem operasi;
f. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
g. Mewajibkan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
h. Menyediakan perlindungan terhadap kode jahat (*malicious code*);
i. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
j. Mewajibkan pemeriksaan mandiri (*self-test*) terhadap layanan-layanan PSrE (contoh: pemeriksaan integritas audit log);

Sistem komputer PSrE e Sign dikonfigurasi dengan meminimalkan jumlah akun dan layanan jaringan yang diperlukan.

6.5.2. Peringkat Keamanan Komputer

Tidak Ada Ketentuan.

6.6. Kendali Teknis Siklus Hidup

6.6.1. Kendali Pengembangan Sistem

PSrE e Sign menetapkan kendali pengembangan sistem PSrE sebagai berikut:

a. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;
b. Proses pengadaan perangkat keras dan perangkat lunak dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen-komponen yang terdapat di dalam perangkat lunak dirusak.
c. Dalam hal pengembangan perangkat keras dan perangkat lunak dilakukan secara mandiri maka proses pengembangan dilakukan dalam sebuah lingkungan yang terkendali. Sedangkan untuk

perangkat keras dan perangkat lunak komersil dengan status siap-pakai, maka syarat pengembangan dilakukan dalam sebuah lingkungan yang terkendali dapat dikecualikan.

d. Perangkat keras dan perangkat lunak yang digunakan untuk aktivitas IKP didedikasikan dan tidak digunakan untuk kegiatan yang bukan bagian dari aktivitas IKP.
e. PSrE e Sign melakukan perawatan yang cukup untuk mencegah perangkat lunak yang berbahaya untuk dimuat ke perangkat. Perangkat keras dan perangkat lunak PSrE selalu di-scan untuk kode-kode berbahaya pada penggunaan pertama dan secara periodik.
f. Pembaruan perangkat keras dan perangkat lunak dibeli atau dikembangkan dengan cara yang sama dengan perangkat aslinya dan diinstal oleh personel yang terpercaya dan terlatih melalui langkah-langkah terdokumentasi.

PSrE e Sign memiliki mekanisme manajemen perubahan yang mencukupi untuk memfasilitasi pengembangan perangkat lunak.

6.6.2. Kendali Manajemen Keamanan

PSrE e Sign memiliki kebijakan dan prosedur manajemen perubahan untuk memastikan pengelolaan perubahan pada konfigurasi sistem IKP. kebijakan dan prosedur tersebut memastikan bahwa perubahan dilakukan oleh peran terpercaya.

6.6.3. Kendali Keamanan Siklus Hidup

PSrE e Sign melakukan pengawasan terhadap skema pemeliharaan untuk memastikan tingkat kepercayaan perangkat keras dan perangkat lunak yang telah dievaluasi keefektifannya melalui audit yang dilaksanakan secara berkala paling kurang 1 (satu) kali dalam setahun.

6.7. Kendali Keamanan Jaringan

PSrE e Sign menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa sistem PSrE terjaga dari serangan seperti namun tidak terbatas pada *denial of service* dan serangan intrusi. Adapun langkah-langkah yang dilakukan oleh PSrE e Sign tersebut termasuk namun tidak terbatas pada penggunaan firewall, pembatasan akses jaringan, memastikan port dan layanan jaringan yang tidak digunakan telah dimatikan, dan menggunakan sistem pengawasan jaringan.

6.8. Tanda Waktu

Semua komponen PSrE e Sign disinkronisasikan dengan sebuah layanan waktu (*Network Time Protocol* / NTP) untuk mejaga sinkronisasi waktu internal semua komponen PSrE. Adapun kegunaan dari NTP adalah untuk menentukan waktu pada saat proses:

a. Validitas waktu permulaan untuk Sertifikat PSrE e Sign;
b. Pencabutan Sertifikat e Sign;
c. Pembaruan CRL;
d. Penerbitan Sertifikat Pemilik; dan
e. Respon OCSP.

Proses pencocokan jam merupakan aktivitas yang dapat diaudit sebagaimana diatur pada poin 5.4.1 dokumen ini. PSrE e Sign mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

BAB 7 PROFIL OCSP, CRL, DAN SERTIFIKAT

7.1. Profil Sertifikat

Profil Sertifikat dan *Certificate Revocation List* (CRL) yang diterbitkan oleh PSrE e Sign sesuai dengan standar RFC 5280 "Infrastruktur Kunci Publik Internet X.509: *PKI Certificate and Certificate Revocation List (CRL) Profile*. PSrE e Sign melakukan reviu terhadap profil Sertifikat secara berkala minimal setahun sekali. Rincian aturan profil Sertifikat yang diterbitkan oleh PSrE e Sign mengacu ke Standar Interoperabilitas PSrE Indonesia yang dikeluarkan oleh Kementerian Komunikasi dan Informatika.

Profil Serfikat yang diterbitkan oleh PSrE e Sign dapat dilihat pada tabel pada poin 7.1.1 untuk *Basic Field* dan 7.1.2 untuk *Standard Extension Field* dengan kode penggunaan sebagai berikut:

a. **M** : *Mandatory*, wajib digunakan, harus;
b. **O** : *Optional*, dapat digunakan secara opsional dengan pertimbangan;
c. **X** : *Must Not*, tidak boleh digunakan;
d. **-** : *Not Stipulated*, tidak diatur;
e. **C** : *Critical*, kritikal;
f. **N** : *Noncritical*, tidak kritikal;

7.1.1. *Basic Field*

Field	Type	M	PSrE e Sign	Pemilik
Certificate (seq)				
tbsCertificate	TBSCertificate	M		
signatureAlgorithm	AlgorithmIdentifier	M		
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.12 SHA384WithRSA Encryption	1.2.840.113549.1.1.11 SHA256WithRSA Encryptio
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL
signatureValue	BIT STRING	M	Tanda tangan PSrE Induk	Tanda tangan PSrE Indonesia
TBSCertificate (seq)				
version	INTEGER{v1(0), v2(1), v3(3)}	M	Versi 3	Versi 3
serialNumber	INTEGER	M	Serial number sertifikat menyesuaikan dengan	Serial number sertifikat menyesuaikan dengan

Field	Type	M	PSrE e Sign	Pemilik
			RFC 5280	RFC 5280
signature	AlgorithmIdentifier	M		
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.12 SHA384WithRSA Encryption	1.2.840.113549.1.1.11 SHA256WithRSA Encryption
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL
issuer	Name	M	c=ID o=Kementerian Komunikasi dan Informatika cn=Root CA Indonesia DS {Issuance Number}	c=ID o=PT Solusi Identitas Global Net cn=e Sign CA Class 1 - G1
validity	Validity	M	10 Tahun	1 Tahun
Validity(seq)				
notBefore	UTCTime		Waktu mulai validitas	Waktu mulai validitas
notAfter	UTCTime		Waktu validitas berakhir	Waktu validitas berakhir
subject	Name	M	c=ID o=PT Solusi Identitas Global Net cn=e Sign CA Class 1 - G1	● Perorangan (*retail*) c=ID ou=Personal cn=(nama lengkap pemegang Sertifikat) ● Individu terafiliasi organisasi/badan usaha c=ID o=(nama organisasi/ badan usaha) cn=(nama lengkap pemegang Sertifikat)

Field	Type	M	PSrE e Sign	Pemilik
				● Segel elektronik c=ID cn=(nama organisasi/ badan usaha)
subjectPublicKeyInfo	SubjectPublicKeyInfo	M		
SubjectPublicKeyInfo (seq)				
algorithm	AlgorithmIdentifier			
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 4096)	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL
subjectPublicKey	BIT STRING		Kunci Publik PSrE Indonesia	Kunci Publik Pemilik
extensions	EXPLICIT Extensions	M		
Extensions (seq size (1...MAX))				
extension	EXTENSION			
EXTENSION (seq)				
extnID	OBJECT IDENTIFIER			
critical	BOOLEAN DEFAULT FALSE			
extnValue	OCTET STRING			

7.1.2. *Standard Extension Field*

Field	Type	OID	PSrE e Sign			Pemilik		
			M	C	Information	M	C	Information

Field	Type	OID	PSrE e Sign			Pemilik		
			M	C	Information	M	C	Information
AuthorityKeyIdentifier (seq)		**2.5.29.35**	M	N		M	N	
keyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik PSrE Induk			Hash SHA-1 160 bit dari kunci publik PSrE Induk
authorityCertIssuer	General Names							
authorityCert SerialNumber	INTEGER							
SubjectKeyIdentifier		**2.5.29.14**	M	N		M	N	
subjectKeyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik PSrE Indonesia			Hash SHA-1 160 bit dari kunci publik Pemilik
KeyUsage		**2.5.29.15**	M	C		M	C	
keyUsage	BIT STRING				keyCertSign (5), cRLSign (6) Nilai key usage (00001100)			digitalSignature, nonRepudiation
CertificatePolicies (seq size(1...MAX))		**2.5.29.32**	M	C		M	C	
policyInformation	Policy Information							
PolicyInformation (seq)								
policyIdentifier	OBJECT IDENTIFIER				Policy OID: 2.16.360.1.1.1.3.12.8 Notice:"OID esign"			Policy OID: 2.16.360.1.1.1.8.1 Notice: "Organisasi/Badan Usaha Policy OID: 2.16.360.1.1.1.5.1.2.2 Notice: "Individu Non-Instansi

Field	Type	OID	PSrE e Sign			Pemilik		
			M	C	Information	M	C	Information
								Online Level 2”
policyQualifiers	Sequence Size (1...MAX) Policy Qualifier Info							
SubjectAlternativeName		**2.5.29.17**						
subjectAlternative Name	General Names		O	N		O	N	• NIK Pemilik menggunakan Virtual ID (VID), sesuai ketentuan Subject Identification Method (SIM) sesuai RFC 4683 disimpan dalam bentuk otherName dari struktur GeneralName menggunakan SII Type=2.16.360.1.1.1.6.1 untuk tipe NIK. • *Email address* Pemilik sesuai RFC 5280 disimpan di *Subject Alternative Name extension* dengan mengikuti ketentuan rfc822Name.
IssuerAlternativeName		**2.5.29.18**						
issuerAlternative Name	General Names		O	N		O	N	
BasicConstraint (seq)		**2.5.29.19**						
cA	BOOLEAN		M	C	true	M	C	false

Field	Type	OID	PSrE e Sign			Pemilik		
			M	C	Information	M	C	Information
pathLenConstraint	INTEGER				0			
NameConstraint		**2.5.29.30**						
permittedSubtrees	General Subtrees		X	-		X	-	
excludedSubtrees	General Subtrees							
ExtendedKeyUsage (seq size (1...MAX))		**2.5.29.37**						
keyPurposeId	Object Identifier		X	-		O	N	
CRLDistributionPoints (seq size (1...MAX))		**2.5.29.31**	M	N		M	N	
DistributionPoir (seq)								
distributionPoint	Distribution PointName				http://signcrl.esign.id/crl/esignissuingca.crl http://signocsp.esign.id/ocsp/issuing https://repository.esign.id/certificate/3s1z10i77e620230623.cer			http://signcrl.esign.id/crl/esignissuingca.crl http://signocsp.esign.id/ocsp/issuing https://repository.esign.id/certificate/3s1z10i77e620230623.cer
reasons	Reason Flags							
cRLIssuer	General Names							
FreshestCRL		**2.5.29.46**						
freshestCRL	CRLDistribution Point		O	N		O	N	
AuthorityInfoAccess (seq siz (1..MAX))		**2.5.29.1**						
AccessDescription (seq)								
accessMethod	OBJECT IDENTI		X	-		X	-	1.3.6.1.5.5.7.48.1

Field	Type	OID	PSrE e Sign			Pemilik		
			M	C	Information	M	C	Information
	FIER							
accessLocation	General Name							http://signocsp.esign.id/ocsp/issuing
AccessDescription (seq)								
accessMethod	OBJECT IDENTIFIER		X	-		M	N	1.3.6.1.5.5.7.48.2
accessLocation	General Name		X	-				https://repository.esign.id/certificate/3s1z10i77e620230623.cer

7.2. Profil CRL

PSrE e Sign menggunakan CRL dan CRL *entry extension* RFC 5280.

7.2.1. Nomor Versi

PSrE e Sign menerbitkan CRL dengan format X.509 versi 2.

7.2.2. CRL dan Ekstensi CRL

PSrE e Sign menerbitkan dengan ekstensi sebagai berikut:

a. CRL number
b. Authority Key Identifier

7.3. Profil OCSP

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

7.3.1. Nomor Versi

PSrE e Sign menerbitkan respon OCSP versi 1.

7.3.2. Ekstensi OCSP

Tidak ada ketentuan.

BAB 8 AUDIT KEPATUHAN DAN PENILAIAN KELAIKAN LAINNYA

PSrE e Sign memiliki mekanisme Penilaian Kelaikan atau Audit Kepatuhan untuk memastikan ketentuan dalam CPS ini diterapkan. PSrE e Sign menjalani Penilaian Kelaikan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika Nomor 11 tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik.

8.1. Frekuensi atau Lingkup Penilaian

Untuk memastikan implementasi kebijakan yang terdapat dalam CPS PSrE e Sign ini sesuai dengan standar yang dikeluarkan oleh Kementerian Komunikasi dan Informatika (Kominfo) maka PSrE e Sign akan melakukan audit minimal 1 (satu) kali setahun dan menyampaikan laporan berkala minimal sekali setahun sebagaimana disyaratkan dalam peraturan perundang-undangan tentang penyelenggaraan sertifikasi elektronik dan sesuai dengan standar yang berlaku di industri. PSrE e Sign juga akan melakukan audit kepatuhan apabila terjadi perubahan yang signifikan terhadap dokumen CPS, prosedur, dan teknik yang diterapkan

8.2. Identitas/Kualifikasi Penilai

Auditor eksternal yang melakukan audit kepada PSrE e Sign merupakan pihak independen, kredibel, memiliki pemahaman dan pengalaman di bidang keamanan informasi serta IKP. Di samping kemampuan teknis tersebut, auditor eksternal juga telah diakui oleh Kominfo untuk sertifikasi melakukan audit kepatuhan yang dilakukan oleh Kominfo.

Kualifikasi auditor untuk melakukan audit sistem PSrE e Sign di antaranya :

a. Tidak memiliki konflik kepentingan terhadap PSrE e Sign;
b. Memiliki kemampuan untuk melakukan audit berdasarkan standar audit dalam ketentuan peraturan perundang-undangan termasuk pengetahuan terkait pemanfaatan layanan yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik, X.509 versi 3, PKI Certificate Policy and Certification Practices Framework, Undang-undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Kominfo terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik;
c. Memiliki kecakapan dalam memeriksa teknologi IKP, peralatan dan teknik keamanan informasi, audit keamanan informasi, dan penilaian pihak ketiga (*third-party attestation function*);
d. Memiliki sertifikasi sebagai auditor sistem informasi (CISA) atau IT Security Specialist, IKP spesialis, yang dapat memberikan masukan terkait *acceptable risks*, strategi mitigasi, dan *best practice* industri;
e. Menguasai beberapa keahlian tertentu, pengujian kompetensi, dan jaminan kualitas seperti penelaahan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional; dan
f. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

8.3. Hubungan Penilai dengan Entitas yang Dinilai

Auditor yang dipilih untuk melakukan audit merupakan auditor independen di luar PSrE e Sign dan memiliki hubungan kontrak yang jelas dengan PSrE e Sign serta mampu menjaga etika untuk memastikan ketidakberpihakan tersebut dan mampu melakukan penilaian secara profesional.

8.4. Topik Penilaian

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

Topik audit meliputi namun tidak terbatas pada implementasi/praktik bisnis CPS, integritas dari layanan operasional IKP dan hal lainnya yang tercantum dalam standar dari Kementerian Kominfo.
Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen PSrE e Sign.

8.5. Tindakan yang Diambil Akibat Ketidaksesuaian

Dalam hal auditor menemukan adanya ketidaksesuaian antara PSrE e Sign dirancang, dioperasikan, atau dipelihara dengan persyaratan CP Induk atau CPS PSrE e Sign yang berlaku, auditor mengambil langkah sebagai berikut:

a. Mencatat ketidaksesuaian tersebut;
b. Memberitahu PSrE e Sign;
c. Melaporkan ke PSrE Induk.

PSrE e Sign segera menentukan tindakan perbaikan lebih lanjut yang diperlukan agar sesuai dengan persyaratan CP Induk atau CPS PSrE e Sign dan/atau kontrak masing-masing.

8.6. Laporan Hasil Penilaian

Laporan hasil audit yang dilakukan oleh auditor independen diberikan kepada PSrE e Sign dimana kemudian akan disampaikan kepada PA untuk dilakukan perbaikan. Laporan hasil audit mengidentifikasi versi CP Induk dan CPS PSrE e Sign yang digunakan dalam penilaian. Hasil audit dikomunikasikan sesuai dengan poin 8.5.

8.7. Audit Internal

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan risiko gangguan pada proses bisnis PSrE e Sign. Audit internal dilakukan setidaknya setahun sekali terhadap sampel yang dipilih secara acak dari setidaknya 1 (satu) persen keseluruhan Sertifikat yang diterbitkan di tahun berjalan.

Audit internal dilakukan dengan memeriksa kesesuaian terhadap ketentuan peraturan perundang-undangan terkait PSrE e Sign.

BAB 9 BISNIS LAIN DAN MASALAH HUKUM

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

PSrE e Sign mengenakan biaya dalam penggunaan layanan e Sign yang dibebankan kepada Pengguna. Informasi biaya layanan penggunaan e Sign disampaikan saat proses pendaftaran.

9.1.2. Biaya Pengaksesan Sertifikat

Tidak ada ketentuan.

9.1.3. Biaya Pengaksesan Informasi Status atau Pencabutan

Tidak ada ketentuan.

9.1.4. Biaya Layanan Lainnya

PSrE e Sign dapat mengenakan biaya untuk biaya layanan lain yang belum diatur dalam CPS ini.

9.1.5. Kebijakan Pengembalian Biaya

PSrE e Sign tidak menyediakan fitur pengembalian biaya untuk layanan yang disediakan.

9.2. Tanggung Jawab Keuangan

9.2.1. Cakupan Asuransi

PSrE e Sign memiliki kebijakan jaminan untuk para Pemilik Sertifikat terkait dengan adanya kegagalan layanan, kesengajaan, dan/atau kelalaian kepada Pemilik Sertifikat sehingga PSrE e Sign tidak dapat memberikan layanan yang optimal**.** Kebijakan jaminan tersebut mengatur tentang poin-poin hak dan kewajiban PSrE e Sign dan Pemilik Sertifikat jika terdapat kegagalan layanan PSrE e Sign.

9.2.2. Aset Lainnya

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

9.2.3. Jaminan Asuransi atau Garansi untuk Pemilik

PSrE e Sign menyediakan garansi untuk para Pemilik Sertifikat. Ketentuan lebih lanjut diatur dalam kebijakan jaminan PSrE e Sign.

9.3. Kerahasiaan Informasi Bisnis

9.3.1. Cakupan Informasi Rahasia

PSrE e Sign memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Adapun daftar yang termasuk informasi rahasia, diantaranya adalah:

a. Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
b. Rekam jejak audit (*log audit*) dari sistem PSrE e Sign (beserta RA);
c. Data aktivasi pada saat pengaktifan Kunci Privat PSrE e Sign sebagaimana dijabarkan pada Bagian 6.4;
d. Dokumentasi bisnis proses PSrE e Sign termasuk dokumen *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* (BCP);
e. Laporan audit dari auditor internal atau auditor independen sebagaimana dijabarkan pada Bagian 8; dan
f. Hasil penilaian kerentanan.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, sebelum pengungkapan informasi di atas memerlukan persetujuan tertulis dari Pemilik.

9.3.2. Informasi yang Tidak dalam Cakupan Informasi yang Rahasia

Informasi yang tidak dikategorikan rahasia pada poin 9.3.1 dokumen CPS ini dianggap informasi publik.

9.3.3. Tanggung Jawab untuk Melindungi Informasi yang Rahasia

PSrE e Sign melindungi informasi rahasia sebagaimana pada poin 9.3.1 dengan menerapkan 3 (tiga) klasifikasi informasi, yaitu:

a. Rahasia (*confidential*), yaitu informasi data pribadi Pemilik. PSrE e Sign mengamankan dengan enkripsi, hanya dapat diakses oleh personel *trusted roles,* dan hanya dapat diakses dengan *Multifactor Authentication* (MFA);
b. Internal, yaitu informasi atau dokumen yang digunakan untuk kebutuhan internal PSrE e Sign, seperti dokumen kebijakan, prosedur, dan instruksi kerja; dan
c. Publik, yaitu informasi yang dapat diakses secara bebas oleh publik melalui website PSrE e Sign dan repositori PSrE e Sign.

Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:

a. Pelatihan atau peningkatan awareness;
b. Perjanjian kontrak pegawai; dan
c. NDA (*Non Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

9.4. Privasi Informasi Pribadi

9.4.1. Rencana Privasi

PSrE e Sign melindungi informasi pribadi yang tercantum dalam Kebijakan Privasi dan dipublikasikan ke dalam repositori.

Kebijakan Privasi PSrE e Sign menyesuaikan dengan ketentuan peraturan perundang-undangan Indonesia terkait perlindungan data pribadi dan informasi dan transaksi elektronik. Kebijakan Privasi PSrE e Sign mendokumentasikan informasi pribadi yang dikumpulkan, penyimpanan dan pemrosesan informasi pribadi, dan kondisi yang mengizinkan informasi tersebut diungkap.

PSrE e Sign memberikan akses atau layanan kepada Pemilik atau Pengandal untuk mengoreksi atau mengubah informasi pribadi atau organisasi melalui permintaan yang sah. Informasi tersebut hanya bisa diberikan setelah PSrE e Sign menjalankan langkah-langkah untuk mengidentifikasi identitas dari pihak yang meminta.

PSrE e Sign hanya mengumpulkan data yang diperlukan untuk pendaftaran dan sertifikasi dan hanya menggunakan untuk tujuan tersebut. PSrE e Sign tidak menggunakan data tersebut untuk kepentingan komersial apapun.

9.4.2. Informasi yang diperlakukan sebagai Privat

PSrE e Sign melindungi semua informasi pribadi Pemilik dari pengungkapan yang tidak sah. Baik informasi yang diberikan ketika pendaftaran maupun informasi yang digunakan ketika menggunakan layanan PSrE e Sign. Hal tersebut termasuk untuk informasi pribadi Pemilik Sertifikat yang Sertifikatnya diterbitkan oleh PSrE e Sign dan juga bagi yang permohonan Sertifikatnya ditolak. PSrE e Sign tidak menyimpan informasi pribadi Pemohon yang permohonan Sertifikatnya ditolak.

Informasi Pemilik dirilis atas persetujuan Pemilik terhadap Pengandal. Arsip yang dikelola oleh PSrE e Sign tidak boleh dirilis kecuali yang diizinkan sesuai poin 9.4.1.

9.4.3. Informasi yang Tidak Dianggap Privat

Informasi yang termasuk dalam poin 7 (Sertifikat dan CRL) CPS ini tidak dikenakan perlindungan sebagaimana pada poin 9.4.2.

9.4.4. Tanggung Jawab Melindungi Informasi Privat

PSrE e Sign bertanggung jawab menyimpan informasi pribadi sesuai dengan kebijakan privasi PSrE e Sign. Informasi yang disampaikan berupa elektronik maupun fisik. *Backup* informasi pribadi elektronik dienkripsi ketika dipindahkan ke media *backup*, dan informasi pribadi berbentuk fisik disimpan dalam lemari dengan akses *trusted roles* yang terbatas .

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 supaya dapat menggunakan informasi tersebut. PSrE e Sign mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Perjanjian Pemilik dan Kebijakan privasi yang didokumentasikan pada repositori.

9.4.6. Pengungkapan Berdasarkan Proses Peradilan atau Administratif

PSrE e Sign tidak mengungkap informasi pribadi kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, ketentuan peraturan perundang-undangan, atau perintah pengadilan.

9.4.7. Keadaan Pengungkapan Informasi Lainnya

Tidak ada ketentuan.

9.5. Hak Atas Kekayaan Intelektual

Semua hak kekayaan intelektual PSrE e Sign termasuk semua merek dagang dan hak cipta dari semua dokumen PSrE e Sign menjadi milik PSrE e Sign.

PSrE e Sign tidak melanggar hak kekayaan intelektual pihak lain.

9.6. Pernyataan dan Jaminan

9.6.1. Pernyataan dan Jaminan PSrE e Sign

PSrE e Sign menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

a. PSrE e Sign mematuhi ketentuan yang diatur dalam CP PSrE induk dan CPS ini;
b. PSrE e Sign menerbitkan dan memperbarui CRL secara berkala;
c. Seluruh Sertifikat yang diterbitkan memenuhi syarat yang diatur berdasarkan CPS ini dan hanya informasi yang telah diverifikasi yang ditampilkan di Sertifikat;
d. PSrE e Sign menampilkan informasi yang dapat diakses secara publik melalui repositori;
e. Kunci Privat PSrE terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;
f. Semua pernyataan yang disusun oleh PSrE e Sign dalam semua perjanjian yang diterapkan adalah benar dan akurat; dan
g. 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, sejauh yang ditentukan dalam CPS, bahwa:

a. Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat;

b. Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat; dan
c. Pemilik dikenakan kewajiban sebagaimana disebutkan dalam poin 9.6.3. Pemilik mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

9.6.3. Pernyataan dan Jaminan Pemilik Sertifikat

Pemilik Sertifikat menjamin bahwa:

a. Setiap Sertifikat Elektronik yang dibuat menggunakan Kunci Privat yang terkait dengan Kunci Publik yang ada di dalam Sertifikat adalah merupakan tanda tangan elektronik dari Pemilik dan Sertifikat Pemilik yang sudah disetujui, serta masih berlaku (belum dicabut atau kedaluwarsa) pada saat melakukan tanda tangan elektronik dibuat;
b. Kunci privat Pemilik disimpan dan diamankan oleh PSrE e Sign dan hanya Pemilik Sertifikat yang memiliki akses terhadap kunci privat tersebut;
c. Telah melakukan reviu dan verifikasi terhadap informasi dalam Sertifikat yang telah diterima untuk memastikan akurasi;
d. Semua informasi yang diberikan oleh Pemilik Sertifikat dan informasi yang berada di dalam Sertifikat adalah akurat;
e. Sertifikat Pemilik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
f. Segera:
    1) melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat Pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat;
    2) mengajukan permohonan untuk melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai di dalam Sertifikat Pemilik tersebut; dan
    3) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam Sertifikat Pemilik yang telah dicabut;
g. Menanggapi instruksi PSrE e Sign tentang *compromise* atau penyalahgunaan sertifikat Pemilik dalam kurun waktu empat puluh delapan (48) jam;
h. Menyetujui dan menerima bahwa PSrE e Sign diberikan kewenangan untuk segera melakukan pencabutan Sertifikat Pemilik jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam perjanjian Pemilik atau jika PSrE e Sign mene-mukan bahwa Sertifikat Pemilik tersebut digunakan untuk mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian malware; dan
i. Pemilik Sertifikat merupakan pengguna akhir dan bukan merupakan PSrE.

9.6.4. Pernyataan dan Jaminan Pengandal

Pihak yang mengandalkan Sertifikat PSrE e Sign menjamin bahwa:

a. Memiliki kemampuan teknis untuk menggunakan Sertifikat;
b. Apabila perwakilan dari Pengandal menggunakan suatu Sertifikat Pemilik, Pengandal memverifikasi informasi yang tercantum di dalam Sertifikat Pemilik sebelum digunakan dan menanggung akibat apa pun yang terjadi jika lalai dalam melakukan hal tersebut;
c. Melaporkan langsung kepada PSrE e Sign, jika Pengandal menyadari atau mencurigai bahwa telah terjadi compromise pada Kunci Privat;

d. Memiliki cukup informasi untuk membuat keputusan apakah bergantung atau tidak pada informasi dalam Sertifikat Pemilik, dan Pengandal menanggung konsekuensi hukum apabila tidak mematuhi kewajiban Pengandal yang ada pada CPS ini; dan
e. Mematuhi ketentuan yang ditetapkan di CPS dan Perjanjian Pengandal.

9.6.5. Pernyataan dan Jaminan Partisipan Lain

Tidak ada ketentuan.

9.7. Pelepasan Jaminan

PSrE e Sign tidak menjamin:

a. Kecuali untuk jaminan yang telah tercantum dalam CPS, kebijakan jaminan dan perjanjian kerja sama serta sepanjang diizinkan oleh hukum, PSrE e Sign mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu
b. Penyalahgunaan Sertifikat Pemilik yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (*Certificate Usage*);
c. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat;

9.8. Pembatasan Tanggung Jawab

9.8.1. Pembatasan Tanggung Jawab PSrE

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

a. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat Pemilik atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, kebijakan jaminan, perjanjian kerja sama, atau yang diatur dalam Sertifikat Pemilik itu sendiri,
b. Semua kerusakan yang disebabkan oleh *force majeure*,
c. Semua kerusakan yang disebabkan oleh malware (seperti *virus* atau *trojans*) di luar perangkat PSrE e Sign.

9.8.2. Pembatasan Tanggung Jawab RA

Dalam hal PSrE e Sign bekerja sama dengan RA, pembatasan tanggung jawab RA ditentukan dalam perjanjian kerja sama antara RA dan PSrE e Sign. Penjaminan yang dilakukan oleh RA terdapat pada poin 9.6.2.

9.8.3. Pembatasan Tanggung Jawab Pemilik

Pembatasan tanggung jawab dan kewajiban Pemilik ditetapkan dalam perjanjian pemilik. Adapun kewajiban dan tanggung jawab Pemilik adalah sebagai berikut:

a. Pemilik pada saat pendaftaran (Pemohon) wajib memberikan informasi yang akurat, lengkap, dan benar kepada PSrE e Sign. Pemilik berkewajiban untuk segera memperbarui informasi dan data pribadi apabila terjadi perubahan untuk menjaga keakuratan dan kelengkapan serta keandalan informasi dari waktu ke waktu.
b. Pemilik bertanggung jawab atas penggunaan Akun dan Sertifikat serta tidak memberikan atau mengungkapkannya kepada siapa pun.
c. Pemilik wajib menggunakan Sertifikat dengan tidak melanggar hukum maupun kewajiban yang disepakati dalam Perjanjian dengan PSrE e Sign maupun kebijakan-kebijakan PSrE e Sign.

9.9. Ganti Rugi

9.9.1. Ganti Rugi oleh PSrE

PSrE e Sign bertanggung jawab atas layanan yang diberikan kepada Pemilik. Terkait dengan kegagalan PSrE e Sign memberikan layanan sesuai yang dipersyaratkan pada CPS dan Perjanjian Pemilik, PSrE e Sign akan melakukan ganti rugi sesuai dengan dokumen kebijakan jaminan.

9.9.2. Ganti Rugi oleh Pemilik

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pemilik Sertifikat setuju untuk mengganti rugi dan membebaskan PSrE e Sign dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya, dan segala tuntutan yang diakibatkan oleh:

a. Pelanggaran yang dilakukan oleh Pemilik terhadap perjanjian pemilik atau kontrak, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
b. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik;
c. Penggunaan Sertifikat oleh Pemilik untuk melakukan perbuatan melawan hukum;
d. Kegagalan Pemilik untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu dan merugikan pihak manapun;
e. Kegagalan Pemilik untuk menggunakan sistem elektronik yang terpercaya, atau mengambil langkah-langkah yang wajar untuk mencegah kebocoran, kehilangan, pengungkapan, perubahan, atau penggunaan tidak sah Kunci Privat; atau
f. Penggunaan nama oleh Pemilik (termasuk namun tidak terbatas pada *common name*, nama *domain*, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

9.9.3. Ganti Rugi oleh Pengandal

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan PSrE e Sign dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya dan segala tuntutan yang diakibatkan oleh:

a. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pengandal, CPS ini, atau hukum yang berlaku;
b. Pengandal tidak memeriksa status Sertifikat untuk menentukan apakah Sertifikat tersebut sudah kedaluwarsa atau sudah dicabut.

9.10. Jangka Waktu dan Pengakhiran

9.10.1. Jangka Waktu

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut melalui media komunikasi PSrE e Sign.

9.10.2. Pengakhiran

Pada saat berakhirnya CPS ini maka:

a. Seluruh Sertifikat Pemilik yang diterbitkan dalam masa berlaku CPS ini tetap mengacu kepada CPS tersebut sampai dengan berakhirnya masa validitas dan Sertifikat Pemilik; dan
b. Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 (tiga puluh) hari kalender setelah dipublikasikan.

9.10.3. Dampak Pengakhiran dan Ketentuan yang tetap Berlaku

PSrE e Sign memberitahukan kondisi dan efek dari penghentian CPS melalui media komunikasi dan repositori PSrE e Sign.

PSrE e Sign tetap mematuhi aturan terkait perlindungan data dan arsip informasi meski CPS sudah tidak berlaku lagi.

9.11. Pemberitahuan Individu dan Komunikasi dengan Partisipan

PSrE e Sign menyediakan media komunikasi bagi para pihak terkait melalui email dan telepon. PSrE e Sign memberi tanggapan paling lama 20 (dua puluh) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke PSrE e Sign dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS.

9.12. Perubahan atau Amandemen

9.12.1. Prosedur untuk Perubahan atau Amandemen

Perubahan atas CPS PSrE e Sign dilakukan sesuai dengan prosedur pengelolaan publikasi informasi dimana setiap perubahan CPS PSrE e Sign mendapatkan persetujuan dari Policy Authority sebelum dipublikasikan melalui repositori.

Apabila terjadi perubahan besar atau signifikan dari CPS ini, PSrE e Sign akan menerbitkan pemberitahuan pada *website* PSrE e Sign, termasuk juga keterangan waktu CPS efektif berlaku.

9.12.2. Periode dan Mekanisme Pemberitahuan

PSrE e Sign memberitahukan di website jika terdapat perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika terjadi perubahan, CPS dipublikasikan pada *website* repositori PSrE e Sign paling lama 7 (tujuh) hari kerja sejak disahkan oleh Policy Authority.

9.12.3. Keadaan di mana OID Harus Diubah

Berikut merupakan keadaan yang menyebabkan perubahan OID antara lain:

a. Perubahan model bisnis PSrE e Sign, atau

b. Perubahan peraturan dari PSrE Induk.

Perubahan atau penambahan OID PSrE e Sign diimplementasikan setelah mendapatkan persetujuan dari Policy Authority PSrE Induk.

9.13. Ketentuan Penyelesaian Perselisihan/Sengketa

Jika ada perselisihan yang terkait dengan penafsiran atau implementasi dari CPS ini, maka para pihak menyelesaikan hal tersebut sesuai dengan perjanjian yang telah disepakati antara PSrE e Sign dengan Pemilik maupun antara PSrE e Sign dengan entitas lain.

Penyelesaian perselisihan diutamakan dilaksanakan secara musyawarah mufakat. Jika mufakat tidak tercapai, maka Pemilik atau entitas lain dengan PSrE e Sign bersepakat untuk menyelesaikan di Badan Arbitrase Nasional Indonesia (BANI) Surabaya mengikuti prosedur dan ketentuan arbitrase BANI.

9.14. Hukum yang Mengatur

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

9.15. Kepatuhan atas Hukum yang Berlaku

PSrE e Sign mematuhi hukum yang berlaku di Indonesia. Para Pihak (PSrE e Sign, Pemilik Sertifikat, Pengandal, dan rekanan) setuju untuk mematuhi peraturan perundang-undangan yang berlaku di Indonesia untuk penyediaan produk dan layanan yang dijelaskan dalam CPS ini. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait proses bisnis.

9.16. Kepatuhan yang belum diatur

9.16.1. Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2. Pengalihan Hak

Entitas yang beroperasi di bawah CPS ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari PSrE e Sign.

9.16.3. Keterpisahan

Jika terdapat ketentuan dari CPS ini, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CPS ini selanjutnya ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CPS ini 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 e Sign dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan PSrE e Sign dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak PSrE e Sign untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CPS ini. Segala hal terkait pelepasan hak dalam pengadilan disampaikan secara tertulis dan ditandatangani oleh PSrE e Sign.

9.16.5. Keadaan Memaksa

PSrE e Sign tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada di luar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga.

PSrE e Sign memiliki BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas PSrE e Sign.

9.17. Ketentuan Lain

9.17.1. Versi CPS yang memiliki kekuatan hukum

Versi Bahasa Indonesia dari CSP ini mengikat secara hukum. Jika dalam kesempatan lain terbit CPS dalam Bahasa Inggris, maka hal tersebut hanya untuk tujuan informasi.

BAB 10 LAMPIRAN 1

10.1 Definisi & Akronim

10.1.1 Definisi

Istilah	:	Definisi
Certificate Revocation List	:	Daftar terkini dari Sertifikat Elektronik yang dicabut yang dibuat dan ditandatangani secara digital oleh PSrE Indonesia yang menerbitkan Sertifikat dalam hal ini adalah PSrE e Sign.
Certificate Signing Request	:	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat.
Key Compromise	:	Kunci Privat dikatakan dikompromikan 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
Key Generation Ceremony	:	Sebuah prosedur di mana Pasangan Kunci dari PSrE atau RA dihasilkan, Kunci Privatnya ditransfer ke modul kriptografi, kunci privatnya dicadangkan, dan/atau kunci publiknya disertifikasi.
Kunci privat	:	Salah satu kunci dari sepasang kunci yang dirahasiakan Pemiliknya dan digunakan untuk membuat tanda tangan elektronik dan/atau melakukan deskripsi terhadap file elektronik yang dienkripsi dengan kunci publik yang sesuai.
Kunci publik	:	Salah satu kunci dari sepasang kunci yang dapat diungkapkan secara terbuka oleh pemegang kunci privat yang sesuai. Kunci ini digunakan untuk memverifikasi tanda tangan elektronik yang dibuat oleh pemegang kunci privat dan atau mengenkripsi pesan sehingga dapat dibuka oleh pemegang kunci privat yang sesuai.
OCSP *responder*	:	Aplikasi online yang dioperasikan di bawah kewenangan PSrE e Sign dan terhubung dengan repositori untuk memproses permintaan status Sertifikat
Online Certificate Status Protocol (OCSP)	:	Protokol pemeriksaan Sertifikat secara online bagi Pengandal yang berisi informasi mengenai status Sertifikat
Pemilik	:	Entitas yang diidentifikasi sebagai subjek dalam Sertifikat
Pemohon	:	Entitas yang memohon penerbitan Sertifikat
Perjanjian Pemilik Sertifikat	:	Perjanjian atau suatu fakta integritas yang mengatur penerbitan dan penggunaan Sertifikat oleh calon Pemilik Sertifikat. Calon Pemilik Sertifikat membaca dan menyetujui sebelum proses penerbitan.
PSrE e Sign	:	Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia non-instansi yang memiliki fungsi sebagai pihak yang layak dipercaya, yang memberikan dan

Istilah	:	Definisi
		mengaudit Sertifikat Elektronik.
PSrE induk Indonesia	:	PSrE Induk Indonesia dilaksanakan oleh Kementerian Komunikasi dan Informatika yang memiliki fungsi untuk memvalidasi Sertifikat CA di Indonesia secara *offline*.
RA/*Registration Authority*	:	Pihak yang menerima permohonan penerbitan Sertifikat elektronik dari calon Pemilik dan bertugas memverifikasi data dan kelengkapan berkas calon Pemilik.
Relying Party / Pengandal	:	Suatu entitas yang memanfaatkan atau mengandalkan informasi Sertifikat dan tanda cap waktu dari Sertifikat yang diterbitkan oleh PSrE e Sign .
Sepasang kunci	:	Kunci Privat yang terasosiasi dengan Kunci Publik
Sertifikat	:	Sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh PSrE Indonesia
Sertifikat Pemilik	:	Sertifikat elektronik yang diterbitkan oleh PSrE Indonesia

10.1.2 Akronim

- BCP : *Business Continuity Plan*
- CA : *Certificate Authority*
- CP : *Certificate Policy*
- CPS : *Certificate Practice Statement*
- CRL : *Certificate Revocation List*
- CSR : *Certificate Signing Request*
- FIPS : *Federal Information Processing Standard*
- HSM : *Hardware Security Module*
- IETF : *Internet Engineering Task Force*
- OCSP : *Online Certificate Status Protocol*
- OID : *Object Identifier*
- PKCS : *Public Key Cryptography Standard*
- PKI : *Public Key Infrastructure*
- RA : *Registration Authority*
- RFC : *Request for Comment* (pada IETF.org)
- SHA : *Secure Hashing Algorithm*
- SSL : *Secure Sockets Layer*
- TSA : *Time Stamping Authority*
- X.509 : Standar ITU-T untuk Sertifikat dan otentikasi

10.2 Profil Sertifikat

10.2.1 Sertifikat e Sign

Basic Certificate Field	***Value***
Signing Alghorithm	SHA-384 RSA Encryption
Issuer: CN	Root CA Indonesia DS {Issuance Number}
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	e Sign CA Class 1 - G1
Subject: OrganizationName	PT Solusi Identitas Global Net
Subject: CountryName	ID
Serial Number	Diberikan otomatis dari perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Key Usage	Critical=TRUE Digital Signature CRL sign Key certificate Sign
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.esign.id/crl/esignrootca.crl (dummy Root CA)
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Contraints	Critical=TRUE Subject Type=SUB CA Path Length Constraint=None
Public Key	RSA 4096 bits

10.2.2 Sertifikat Level 3 (segel elektronik)

Basic Certificate Field	***Value***
Signing Alghorithm	SHA-256 RSA Encryption
Issuer: CN	e Sign CA Class 1 - G1
Issuer: O	PT Solusi Identitas Global Net
Issuer: C	ID
Subject: CommonName	Nama legal dari organisasi/badan usaha
Subject: CountryName	ID
Serial Number	Diberikan otomatis dari perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Key Usage	Critical=TRUE Digital Signature Non-Repudiation
Extended Key Usage	Critical=FALSE
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://signcrl.esign.id/crl/esignissuingca.crl
Authority Information Access	Critical = FALSE http://signocsp.esign.id/ocsp/issuing
Certificate Policies	Critical=FALSE Policy OID: 2.16.360.1.1.1.3.12.8.1 URL: https://repository.esign.id Policy OID: : 2.16.360.1.1.1.3.12.8 Notice:"OID e Sign Policy OID: : 2.16.360.1.1.1.8.1 Notice:"Organisasi/badan usaha"
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Contraints	Critical=TRUE Subject Type=End Entity
Public Key	RSA 2048bits

10.2.3 Sertifikat Level 2 (tanda tangan elektronik)

Basic Certificate Field	***Value***
Signing Alghorithm	SHA-256 RSA Encryption
Issuer: CN	e Sign CA Class 1 - G1
Issuer: O	PT Solusi Identitas Global Net
Issuer: C	ID
Subject: CommonName	• Perorangan: Nama lengkap pemegang Sertifikat • Personal bagian dari organisasi/badan usaha: nama lengkap pemegang Sertifikat
Subject: OrganizationName	• Perorangan: Tidak menggunakan *field* OrganizationName • Personal bagian dari organisasi/badan usaha: nama legal dari organisasi/badan usaha
Subject: OrganizationUnit	• Perorangan: Personal • Personal bagian dari organisasi/badan usaha: Tidak menggunakan *field* OrganizationUnit
Subject: CountryName	ID
Subject: AlternativeName	• NIK (Nomor Induk Kependudukan) pemegang Sertifikat • *Email* pemegang Sertifikat (perorangan, individu terafiliasi perusahaan)
Serial Number	DIberikan otomatis dari perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Key Usage	Critical=TRUE Digital Signature Non-Repudiation
Extended Key Usage	Critical=FALSE
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://signcrl.esign.id/crl/esignissuingca.crl
Authority Information Access	Critical = FALSE http://signocsp.esign.id/ocsp/issuing
Certificate Policies	Critical=FALSE Policy OID: 2.16.360.1.1.1.3.12.8.1 URL: https://repository.esign.id Policy OID: 2.16.360.1.1.1.3.12.8 Notice:"OID esign" Policy OID: 2.16.360.1.1.1.5.1.2.2 Notice:"Individu Non-Instansi Online level 2
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Contraints	Critical=TRUE Subject Type=End Entity
Public Key	RSA 2048bits

PT SOLUSI IDENTITAS GLOBAL NET

OFFICE

Jl. Raya Lingkar Timur Km.1, Sidoarjo, Jawa Timur

Phone : (031) 8910919

FIND US HERE

www.esign.id

office@esign.id