Téken pake Téken Aja!

By Djelas Tandatangan Bersama

Certification Practice Statement (“CPS”)

Penyelenggara Sertifikasi Elektronik (“PSrE”)

Berinduk Indonesia

PT Djelas Tandatangan Bersama (“DTB”)

Nomor	MGT-KEB-02-4.0
Versi	4.0
Tanggal	08 Agustus 2023
OID	2.16.360.1.1.1.3.12.7.0.2.1
Jenis Dokumen	Publik

08 Agustus 2023
Policy Authority

Aidil Chendramata

Keterangan Revisi Dokumen

Revisi	Tanggal	Penjelasan perubahan	Dibuat oleh
1.0	**22-02-2021**	**Edisi perdana**	**Policy Authority Officer**
2.0	**02-08-2021**	• **Penambahan ketentuan penerbitan Sertifikat Elektronik untuk Warga Negara Asing dan pencabutan Sertifikat Elektronik untuk Pihak Ketiga**	**Policy Authority Officer**
3.0	**28-10-2022**	• **Review Berkala** • **Perubahan Logo** • **Penambahan pada poin 1.2, OID untuk e-Stamp** • **Pembaruan pada poin 1.3, Otoritas Pendaftaran (RA),** • **Fungsi RA, Pemilik Sertfikat dan Penyedia Layanan Data Center** • **Penambahan pada poin 1.4.2, Penggunaan Sertifikat yang Dilarang** • **Penambahan pada poin 3.1, Tipe Nama Sertifikat dan Anonimitas atau Pseudonimitas Pemilik** • **Pembaruan pada poin 3.2, Autentikasi dari Identitas Organisasi, Autentikasi dari Identitas Individu** • **Pembaruan pada poin 3.3.1, Identifikasi dan Autentikasi untuk kegiatan Re-Key Rutin** • **Penambahan dan Perubahan pada poin 4.1, Subjek yang dapat mengajukan permohonan Sertifikat, Proses Pendaftaran dan Tanggung Jawab** • **Pembaruan pada poin 4.4.2, Publikasi Sertfikat oleh DTB** **Pembaruan pada poin 4.5.1, Pemilik Kunci dan Pengguna Sertifikat** • **Pembaruan pada poin 5.2.1, Peran yang Dipercaya**	**Policy Authority Officer**

4.0	08-08-2023	• **Review Berkala** • **Penambahan pada poin 1.1.** • **Penambahan pada poin 1.2 terkait UID** • **Pembaruan pada poin 1.3.1, PSrE Induk berubah menjadi PSrE Indonesia dan Definisi RA** • **Pembaruan pada poin 1.4.1, Autentikasi, Digital Signature, Data Encipherment** • **Penambahan pada poin 1.5.1, CPS dan Dokumen referensi terkait kontak dan alamat** • **Pembaruaan poin 2.1, Repositori** • **Penambahan poin 3.1.1, Certificate profile** • **Penambahan poin 3.2.2, Posisi Perwakilan Badan Usaha** • **Penambahan poin 4, Renewal, re-key, dan modification** • **Penambahan poin 4.1.1, Pihak yang dapat mengajukan permohonan penerbitan Sertifikat** • **Penambahan poin 4.1.2, Pemohon dapat memberikan informasi yang benar** • **Pembaruan 4.2.3, DTB akan menerbitkan Sertifikat Pemilik tidak lebih dari 60 menit** • **Penambahan 4.3.1, Tindakan PSrE selama penerbitan** • **Penambahan 4.3.2, DTB memberitahu Pemilik dalam maksimum 1x24 jam** • **Penambahan 4.4.1, Pemilik harus mengkonfirmasi persetujuan Sertifikat** • **Penambahan 4.6, PT. Djelas Tandatangan Bersama tidak melakukan Pembaruan Sertifikat** • **Penambahan 4.7, Penerbitan ulang Sertifikat dengan penggantian kunci (re-key)** • **Penambahan 4.7.2, Pemilik dapat melakukan re-key sertifikatnya** • **Penambahan poin 4.7.3, PSrE harus mengikuti prosedur** • **Penambahan poin 4.7.4, Prosedur DTB melakukan pemberitahuan Penerbitan Sertifikat** • **Penambahan 4.7.6, Sertifikat re-key dipublikasikan sesuai ketentuan** • **Penambahan 4.7.7, Tidak ada tindakan yang diambil untuk pemberitahuan entitas lain** • **Penambahan poin 4.8, Modifikasi detil sertifikat tidak diperbolehkan** • **Penambahan poin 4.9.1, Kunci hilang dan pemilik** • **Perubahan poin 4.9.2, DTB sendiri apakah bisa mencabut** • **Pembaruan poin 4.9.3, Instansi, PT Djelas diseragamkan menjadi PT DTB** • **Perubahan Poin 4.9.4, Tenggang waktu pencabutan** • **Pembaruan 4.9.5, The time within which CA must process the revocation request** • **Pembaruan 4.9.10, Repositori PSrE Indonesia mempublikasi semua responder OCSP** • **Pembaruan poin 4.9.12, Apabila Kunci bocor selain ke tindakan**	**Policy Authority Officer**

		pembukuan atau revoke • **Penambahan point 4.12, Kunci Privat Pemilik** • **Penambahan 5.1.1, Sistem cadangan PSrE di data center** • **Pembaruan poin 5.1.2, Membutuhkan kendali akses fisik dua orang** • **Pembaruan poin 5.1.6, Disimpan di kantor DTB (technically sudah terpisah dari DC dan DRC)** • **Pembaruan dan penambahan poin 5.1.7, Dokumen yang mengandung informasi sensitif harus dihancurkan** • **Pembaruan dan penambahan poin 5.1.8, Lokasi off-site backup** • **Penambahan poin 5.2.1, Cryptographic ke custodian dan security officer** • **Penambahan poin 5.2.2, Backup kunci privat DTB multipersonal** • **Penambahan poin 5.2.3, Individu yang ditugaskan dalam Peran Terpercaya harus merupakan karyawan** • **Pembaruan poin 5.2.4, Dokumen lain yang mengatur segregation of duties** • **Pembaruan poin 5.3.2, Dokumen prosedur background check** • **Penambahan poin 5.3.3, Catatan pelatihan semua personel PSrE** • **Pembaruan poin 5.3.4, Kata "harus" dihapus** • **Pembaruan poin 5.3.5, Kata "harus" dihapus** • **Pembaruan poin 5.3.8, Dokumen menunjang tugas dan tanggung jawab bagi setiap peran** • **Pembaruan dan penambahan poin 5.4.1, Waktu disinkronkan dengan otoritas sumber waktu dengan 1 (satu) menit** • **Penambahan poin 5.4.4, Sistem dapat menimpa (overwrite) log audit setelah log audit** • **Penambahan pada poin 5.4.5, di brankas yang sama** • **Penambahan poin 5.48, Uji penetrasi ke sistem PSrE harus dilakukan minimal 1 (satu) tahun sekali** • **Penambahan poin 5.5.1, Tipe Record yang Diarsipkan** • **Pembaruan poin 5.5.2, Kata "wajib" dan "harus" dihapus** • **Penambahan poin 5.5.3, Muatan arsip** • **Pembaruan poin 5.5.4, Tata cara untuk backup arsip** • **Penambahan poin 5.6, Pembuatan Sertifikat yang melebihi masa berlaku** • **Pembaruan dan penambahan poin 5.7.1** • **Penambahan poin 5.7.2** • **Pembaruan dan penambahan poin 5.7.3, DTB memberitahu Menteri terkait pencabutan Sertifikat** • **Penambahan poin 5.7.4, terkait bencana yang mengakibatkan semua fasilitas dan peralatan rusak** • **Penambahan poin 6.1.1, Daftar pembangkitan kunci entitas terdiri dari CA, TSA, OCSP** • **Penambahan poin 6.1.2, Pengiriman Kunci Privat ke Pemilik** • **Penambahan poin 6.1.5, SHA yang digunakan sesuai dengan standar interoperebulutas**	

		• **Penambahan poin 6.1.7, Kunci pemilik digunakan untuk apa saja** • **Penambahan poin 6.2.1, Pembangkitan kunci pemilik** • **Penambahan poin 6.2.3, Ditambah tentang kunci pemilik** • **Pembaruan poin 6.2.4, Backup dibawah kendali Pemilik sudah ada di Kebijakan Privacy** • **Pembaruan poin 6.2.5, Layanan kunci private pemilik untuk enkripsi** • **Pembaruan poin 6.2.9, Di nonaktifkan oleh personel yang berwenang** • **Penambahan pin 6.3.1, Kunci Publik selama 5 (lima) tahun** • **Pembaruan poin 6.3.2, hapus kata harus** • **Pembaruan 6.4.1, Pembuatan dan Instalasi Data Aktivasi** • **Penambahan poin 7.1, Rincian aturan profil** • **Penambahan poin 7.2.2, CRL DTB mematuhi Standar Interoperabilitas .** • **Penambahan poin 7.3, DTB mengoperasikan Online Certificate Status Protocol** • **Pembaruan poin 8, Audit Kepatuhan dan Penilaian Kelaikan Lainnya** • **Pembaruan poin 8.1, Frekuensi atau Lingkup Penilaian** • **Pembaruan dan penambahan poin 8.2, Auditor disesuaikan menjadi "Penilai"** • **Pembaruan dan penambahan 8.3, Hubungan Penilai dengan Entitas yang Dinilai** • **Pembaruan dan penambahan poin 8.4, Topik Penilaian bertujuan untuk memverifikasi** • **Pembaruan dan penambahan poin 8.5, Tindakan yang diambil akibat ketidaksesuaian** • **Pembaruan dan penambahan poin 8.6, Laporan Hasil Penilaian** • **Penambahan poin 8.7, DTB memantau kepatuhannya terhadap CP induk** • **Pembaruan poin 9.1.4, Biaya tambahan untuk layanan TTE** • **Pembaruan poin 9.2, DTB menjamin kerugian kepada Instansi** • **Pembaruan 9.3, Diwajibkan hukum atau perintah pengadilan** • **Pembaruan 9.4, Informasi yang diperlakukan sebagai Privat** • **Penambahan poin 9.5, Hak atas Kekayaan Intelektual** • **Pembaruan poin 9.6, Kunci Privat DTB terlindungi dan tidak dapat diakses** • **Penambahan poin 9.8, Kontrak Pemilik Sertifikat** • **Pembaruan poin 9.8.2 Penulisan CP diganti dengan CPS** • **Pembaruan poin 9.9.1, Ganti Rugi oleh DTB** • **Penambahan poin 9.9.2, Ganti Rugi oeh Pemilik** • **Pembaruan poin 9.9.3, Ganti Rugi oleh Pengandal** • **Pembaruan poin 9.10, Jangka Waktu dan Pengakhiran** • **Pembaruan poin 9.10.1, Jangka Waktu** • **Pembaruan 9.10.2 tentang Pengakhiran** • **Pembaruan 9.10.3, aturan terkait pelindungan data dan arsip Informasi** • **Pembaruan poin 9.11, Bunyi ketentuan Pemberitahuan Individu** • **Penambahan poin 9.12, Diatur dalam SOP Manajemen Perubahan** • **Pembaruan poin 9.12.2 Tambahkan link url repositori DTB**	

		• **Pembaruan 9.12.3, Keadaan Dimana OID Harus Diubah** • **Pembaruan poin 9.13, Dokumen dan kebijakan DTB** • **Pembaruan poin 9.14, Hukum Yang Mengatur** • **Pembaruan poin 9.15, Kepatuhan atas Hukum Yang Berlaku** • **Pembaruan 9.16.1, Ketentuan Kewajiban RA** • **Pembaruan 9.16.2, Pengalihan hak** • **Pembaruan 9.16.5, Hapus kata "wajib"**	

DAFTAR ISI

1. PENGANTAR

1.1 Ringkasan

Infrastruktur Kunci Publik (IKP) Indonesia adalah hirarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikasi Elektronik (PSrE) Induk. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PT Djelas Tandatangan Bersama (DTB) adalah PSrE berinduk non-Instansi yang menerbitkan Sertifikat di bawah PSrE Induk (Kemenkominfo).

Dokumen *Certification Practice Statement* (CPS) DTB ini menjelaskan Penyelenggaraan Sertifikasi Elektronik oleh DTB dan menetapkan persyaratan bisnis, hukum serta teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat Pemilik dalam Infrastruktur Kunci Publik (IKP) DTB.

CPS ini sesuai dengan standar *Request for Comments* 3647 (RFC 3647) dari *Internet Engineering Task Force* (IETF) tentang *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework* dan CPS ini mengacu kepada *Certificate Policy* (CP) PSrE Induk yang diterbitkan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo).

Dokumen ini ditujukan kepada:

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

1.2 Identifikasi dan Nama Dokumen

Dokumen ini adalah Dokumen CPS *(Certification Practice Statement)* DTB.

Object Identifier (OID) yang digunakan untuk CPS (tidak termasuk *Extended Validation Certificate*) ini adalah:

Digitally Signed Object	Object Identifier (OID)
OID non-Instansi DTB	2.16.360.1.1.1.3.12.7
OID Dokumen CPS DTB	2.16.360.1.1.1.3.12.7.0.2.1

OID Sertifikat Verifikasi Level 4	2.16.360.1.1.1.4.4
OID Individu WNA Online level 2	2.16.360.1.1.1.5.2.2.2
OID Individu WNA Online level 3	2.16.360.1.1.1.5.2.2.3
OID SII Type	2.16.360.1.1.1.6
OID NIK	2.16.360.1.1.1.6.1
OID Sertifikat untuk Individu	2.16.360.1.1.1.7.1
OID Sertifikat Badan Usaha	2.16.360.1.1.1.7.2
OID AATL	2.16.360.1.1.1.9.1

1.3 Partisipan IKP

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1 PSrE Induk Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia. PSrE Induk menerbitkan dan/atau mencabut Sertifikat Digital PSrE Berinduk (DTB) berdasarkan status Pengakuan yang diberikan oleh Kemenkominfo. PSrE Induk tidak menerbitkan Sertifikat kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat DTB, sebagaimana dirinci dalam CPS ini, termasuk namun tidak terbatas pada:

a. Pengendalian terhadap proses pendaftaran;
b. Proses identifikasi dan autentikasi;
c. Proses penerbitan self-sign Sertifikat;
d. Proses penerbitan Sertifikat;
e. Proses penerbitan Daftar Pencabutan Sertifikat (Certificate Revocation List/CRLs);
f. Publikasi Sertifikat dan CRLs;
g. Validasi Sertifikat;
h. Pencabutan Sertifikat;
i. Membangun dan memelihara sistem DTB; dan
j. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan DTB yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.
k.

1.3.1.2. PSrE Indonesia

DTB adalah PSrE dengan status pengakuan berinduk yang Sertifikatnya telah ditandatangani oleh PSrE Indonesia. DTB menerbitkan Sertifikat kepada Pemilik Sertifikat.

DTB adalah PSrE non-Instansi yaitu PSrE yang menerbitkan Sertifikat kepada entitas selain Pemerintah.

DTB tidak boleh berinduk kepada PSrE lain dan tidak boleh menjadi induk bagi PSrE lainnya.

1.3.2 Otoritas Pendaftaran (RA)

DTB sebagai penyedia RA (*Registration Authority*) bertanggung jawab dan bertindak secara langsung untuk memverifikasi identitas Pemilik maupun Pemohon dan menerima permintaan pencabutan dan penandatanganan Sertifikat. DTB menjalankan fungsi RA sendiri dan tidak menggunakan pihak luar.

1.3.2.1 Fungsi dari RA

RA berkewajiban untuk melaksanakan fungsi sebagai berikut:

a. Tunduk kepada Prosedur Penerbitan Sertifikat Elektronik;
b. Identifikasi dan autentikasi data Pemilik maupun Pemohon berdasarkan prosedur pendaftaran;
c. Memulai atau meneruskan proses permohonan pembuatan Sertifikat;
d. Memulai atau meneruskan proses permohonan pencabutan Sertifikat; dan
e. Menyetujui permohonan penerbitan ulang atau perpanjangan Pemilik Sertifikat.

1.3.2.2 Persyaratan khusus RA untuk Sertifikat EV SSL

Tidak ada ketentuan.

1.3.3 Pemilik

Pemilik adalah entitas yang memohon dan berhasil mendapatkan Sertifikat yang ditandatangani oleh DTB. Entitas Pemilik berarti subjek pemegang Sertifikat entitas yang terikat dengan DTB sebagai penerbit Sertifikat. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat, Pemegang disebut sebagai Pemohon.

DTB menerbitkan Sertifikat kepada perseorangan non-Instansi untuk Warga Negara Indonesia, Warga Negara Asing (WNA) dan Badan Usaha.

1.3.4 Pengandal

pengandal adalah entitas yang mempercayai Sertifikat dan tanda tangan digital yang diterbitkan oleh DTB (pengandal). pengandal harus terlebih dahulu memeriksa respon dari *Certificate Revocation Lists* (CRL) atau *Online Certificate Status Protocol* (OCSP) DTB 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 dapat menggunakan informasi dalam Sertifikat untuk menentukan kesesuaian penggunaan dan tujuan Sertifikat. pengandal menggunakan informasi dalam Sertifikat untuk:

a. Memeriksa tujuan penggunaan Sertifikat;

b. Melakukan verifikasi tanda tangan digital

c. Memeriksa apakah Sertifikat termasuk di dalam CRL

d. Penyetujuan batas tanggung jawab dan jaminan.

pengandal dapat meliputi Bank, Perusahaan *e-commerce*, Instansi Penyelenggara Negara dan entitas lain yang menggunakan tanda tangan digital di dalam layanannya.

1.3.5 Partisipan Lain

1.3.5.1 Penyedia Layanan Pusat Data (*Data Center*)

Penyedia Layanan Pusat Data adalah pihak ketiga yang menyediakan layanan Pusat Data untuk operasional PSrE DTB.

1.4 Kegunaan Sertifikat

1.4.1 Penggunaan Sertifikat yang Semestinya

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

a. Tanda tangan digital; dan

b. Segel Elektronik

DTB menyediakan level verifikasi identitas level 3, yang mana verifikasi identitas dilakukan menggunakan kartu identitas dan data biometrik yang dibandingkan dengan data identitas yang dimiliki oleh Pemerintah.

Penggunaan yang tidak sesuai dapat berakibat pada hilangnya jaminan yang diberikan oleh DTB kepada Pemilik Sertifikat dan pengandal.

Certificate Class	**Level Verifikasi**			**Penggunaan**		
	Verifikasi Rendah	**Verifikasi Sedang**	**Verifikasi Tinggi**	**Autentikasi**	**Tanda Tangan Digital dan Segel Elektronik**	**Enkripsi**

Sertifikat Individu						
Level 4			✓		✓	

1.4.2 Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan DTB dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam bagian 1.4.1.

1.5 Administrasi Kebijakan

Policy Authority (PA) / Administrasi Kebijakan adalah pihak yang ada di dalam DTB. PA memiliki peran dan tanggung jawab sebagai berikut:

a. Menetapkan *Certificate Policy* (CP) dan/atau *Certification Practice Statement* (CPS);
b. Memastikan semua layanan, operasional, dan infrastruktur DTB yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang kurang lebih setara.

1.5.1 Organisasi Pengelola Dokumen

CPS ini dan dokumen referensi lainnya dikelola oleh *Policy Authority* (PA) DTB.

1.5.2 Kontak yang Dapat Dihubungi

- Alamat Surat : *Policy Authority* (PA)
  PT. Djelas Tandatangan Bersama
  Jln. Bangka Raya No. 21
  Kel. Pela Mampang, Kec. Mampang Prapatan
  Jakarta Selatan
- Alamat Surel : info@djelas.id
- Website : https://www.djelas.id
- Telepon/phone : +62 21 2271-8863

1.5.3 Personil yang menentukan Kesesuaian CPS dengan Kebijakan

PA DTB menentukan kesesuaian konten CPS dan kesesuaian antara CPS dengan CP.

1.5.4 Prosedur Persetujuan CPS

PA DTB menyetujui CPS dan segala amandemen/perubahannya. Amandemen/perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum. PA DTB menentukan apakah amandeman/perubahan ke CPS ini memerlukan pemberitahuan atau perubahan OID.

Perubahan CPS akan diinformasikan di https://www.djelas.id/.

1.6 Definisi dan Akronim

Lihat Lampiran A untuk tabel akronim dan definisi.

2. TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI

2.1 Repositori

DTB bertanggung jawab memelihara repositori daring yang berisikan dokumen-dokumen yang menunjang layanan Penyelenggaraan sertifikasi elektronik seperti antara lain :

a. CPS DTB;
b. Kebijakan privasi;
c. Kebijakan jaminan;
d. Panduan pengamanan kata sandi untuk pemilik Sertifikat;
e. Panduan tanda tangan elektronik;
f. Panduan verifikasi tanda tangan elektronik tersertifikasi dan verifikasi Sertifikat elektronik;
g. Perjanjian pengandal;
h. Perjanjian pelanggan; dan
i. Struktur harga.

2.2 Publikasi Informasi Sertifikat

DTB memelihara repositori yang dapat diakses melalui https://repository.djelas.id/ tempat publikasi Sertifikat DTB, CRL terakhir, dokumen CP/CPS.

2.3 Waktu atau Frekuensi Publikasi

CPS ini dan tiap perubahan selanjutnya dapat diakses publik dalam 7 hari kalender setelah disetujui.

DTB mempublikasikan Sertifikat Pemilik dan data pencabutan Sertifikat 30 menit setelah diterbitkan. CRL diperbaharui sesuai dengan Bagian 4.9.7.

2.4 Kendali Akses pada Repositori

Informasi yang dipublikasikan pada repositori adalah informasi publik. DTB memberikan akses baca yang tidak dibatasi pada repositorinya dan menerapkan kontrol logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.

DTB melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

3. IDENTIFIKASI DAN AUTENTIKASI

3.1 Penamaan

3.1.1 Tipe Nama

DTB membuat dan menandatangani Sertifikat dengan subyek *Distinguished Name* (DN) yang non-null dan mematuhi standar ITU-T X.500. Tabel di bawah meringkas DN dari Sertifikat yang diterbitkan oleh DTB berdasarkan CPS.

Tipe Sertifikat	*Distinguished Name*
Sertifikat PSrE (DTB)	CN=DTB CA, O=<PT Djelas Tandatangan Bersama>, C=ID
Sertifikat Pemilik	CN=<nama orang>, O=personal, UID=<tekenid pemilik>, C=ID
Sertifikat E-Seal	CN=<namaperusahaan>, C=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 harus mengidentifikasi orang atau objek tersebut.

Nama subjek dan penerbit yang terkandung dalam Sertifikat HARUS bermakna dalam arti bahwa DTB memiliki bukti cukup yang menunjukkan keterkaitan antara nama dengan entitasnya. Untuk mencapai tujuan ini, penggunaan nama harus diotorisasi oleh Pemilik yang sah atau perwakilan legal dari Pemilik yang sah.

3.1.3 Anonimitas atau Pseudonimitas Pemilik

DTB tidak boleh menerbitkan Sertifikat anonim atau pseudonim.

3.1.4 Aturan Interpretasi Berbagai Bentuk Nama

DN dalam Sertifikat diinterpretasikan menggunakan standar X.500.

3.1.5 Keunikan Nama

DN diisi dengan informasi pada saat pendaftaran. Semua DN di Sertifikat perorangan harus sesuai dengan data yang dimasukkan Pemilik. Pemilik bertanggung jawab penuh terhadap ketepatan dan akurasi pemilihan DN. Nama yang tertera di dalam Sertifikat harus sesuai dengan yang tertera di e-KTP.

3.1.6 Pengakuan, Autentikasi, dan Peran Merek Dagang

Pemohon Sertifikat tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih pemohon Sertifikat.

DTB dapat menolak permohonan atau melakukan pencabutan Sertifikat yang menjadi bagian dari konflik merek dagang.

3.2 Validasi Identitas Awal

3.2.1 Pembuktian Kepemilikan *Private Key*

Metode untuk membuktikan kepemilikan Kunci Privat harus PKCS#10 (CSR), atau permintaan lain yang ekuivalen secara kriptografi (permintaan ditandatangani secara digital dengan Kunci Privat).

Untuk Sertifikat pemilik, pasangan kunci dapat dibangkitkan oleh DTB, dengan syarat bahwa Kunci Privat diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS 140-2 level 3 dan hanya dapat diakses oleh Pemilik dengan minimal dua faktor autentikasi.
Pembuktian kepemilikan Kunci Privat Pemilik dengan cara verifikasi biometrik dilakukan pada saat melakukan tandatangan digital.

3.2.2 Autentikasi Identitas Organisasi

Permohonan untuk mendapatkan Sertifikat yang mengidentifikasi suatu badan hukum/badan usaha *(E-Seal) hanya dapat* dibuat oleh pihak yang berwenang mewakili organisasi tersebut. Permohonan untuk memiliki *E-Seal* diajukan melalui *RA* dengan memenuhi persyaratan sebagai berikut:

1. Surat permohonan yang memuat persetujuan untuk penerbitan Sertifikat Elektronik yang diajukan oleh perwakilan Badan Usaha yang secara sah memiliki kewenangan untuk bertindak mewakili Badan

Usaha tersebut;

2. Akta pendirian Badan Usaha dan/atau akta perubahan terakhir Badan Usaha;
3. Surat keputusan pengesahan Badan Usaha;
4. Salinan kartu identitas (KTP) perwakilan Badan Usaha yang memohonkan Sertifikat Elektronik;
5. Foto wajah perwakilan Badan Usaha;
6. Nomor handphone perwakilan Badan Usaha; dan
7. Alamat email resmi perwakilan Badan Usaha.

Mekanisme verifikasi data pemohon badan hukum/badan usaha yaitu:

a. Melakukan verifikasi terhadap penanggung jawab atau perwakilan yang ditunjuk organisasi atau pemimpin organisasi;

b. Melakukan pengecekan kelengkapan dokumen perusahaan lainnya dengan metode tatap muka dengan metode online yang direkam dengan membawa atau menunjukan dokumen asli untuk di verifikasi; dan

d. Melakukan verifikasi Akta Pendirian Perusahaan dan Akta Perubahan terakhir melalui legalisir dari Notaris.

Dalam hal data Badan Usaha tidak tercantum dalam basis data Instansi yang berwenang memberikan pengesahan Badan Usaha sesuai dengan ketentuan peraturan perundang-undangan, melampirkan surat/dokumen penunjukan Perwakilan Badan Usaha.

DTB menyimpan data Pemilik selama minimal 5 (lima) tahun.

3.2.3 Autentikasi Identitas Individu/Perorangan

Identifikasi dan Autentikasi Identitas Individu yang mengajukan permintaan Sertifikat DTB dilakukan sebagai berikut:

I. Untuk Warga Negara Indonesia;
   a. Mengajukan permohonan untuk menjadi Pemilik Sertifikat Elektronik;
   b. Mengumpulkan salinan Kartu Tanda Penduduk resmi yang dikeluarkan oleh pemerintah;
   c. Memasukkan informasi data diri seperti NIK, nama lengkap, tempat lahir, tanggal lahir, alamat surel dan nomer seluler;
   d. Melakukan proses verifikasi biometrik melalui kamera web Pemilik dan divalidasi dengan data administrasi kependudukan;
   e. DTB melakukan verifikasi dan validasi data pemohon dengan data kependudukan

pemerintah. Data yang divalidasi adalah NIK, nama, tempat lahir, tanggal lahir dan foto selfie;

f. Konfirmasi untuk aktivasi akun dikirim ke alamat surel yang didaftarkan; dan
g. DTB menyimpan data Pemilik selama minimal 5 tahun.

II. Persyaratan untuk WNA yang tinggal di Indonesia:
   a. Surat permohonan yang memuat persetujuan oleh user untuk penerbitan Sertifikat elektronik dan pernyataan keaslian bukti identitas;
   b. KTP Elektronik atau Paspor dan Kartu izin tinggal sementara (KITAS) bagi yang tidak memiliki KTP Elektronik;
   c. Foto wajah;
   d. Nomor handphone; dan
   e. Email.
   f. Melakukan Liveness
   g. Konfirmasi untuk aktivasi akun dikirim ke alamat surel yang didaftarkan; dan
   h. DTB menyimpan data Pemilik selama minimal 5 tahun.

III. Persyaratan untuk WNA yang tinggal di luar negara Indonesia:
   a. Surat permohonan yang memuat persetujuan oleh user untuk penerbitan Sertifikat elektronik dan pernyataan keaslian bukti identitas;
   b. Kartu Identitas yang dikeluarkan dari Negara Pemohon atau Sertifikat Elektronik yang dikeluarkan pemerintah Negara Pemohon dan Salinan identitas yang dipakai untuk menerbitkan identitas Sertifikat Elektronik tersebut (Sertifikat Digital).
   c. Paspor;
   d. Bukti alamat surat menyurat;
   e. Foto wajah;
   f. Nomor handphone; dan
   g. Email.
   h. Melakukan Liveness Detection
   i. Konfirmasi untuk aktivasi akun dikirim ke alamat surel yang didaftarkan; dan
   j. DTB menyimpan data Pemilik selama minimal 5 tahun.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

Informasi yang tidak bisa diverifikasi tidak boleh disertakan di dalam Sertifikat.

DTB tidak akan menerbitkan Sertifikat dari Pemohon yang informasinya tidak dapat diverifikasi sesuai bagian 3.2.3 diatas.

3.2.5 Validasi Otoritas

Sertifikat yang mengandung afiliasi Badan Usaha atau Instansi secara eksplisit atau implisit hanya dapat diterbitkan setelah memastikan bahwa Pemohon adalah benar memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan oleh Badan Usaha atau Instansi tersebut.

3.2.6 Kriteria Inter-operasi

Tidak ada ketentuan.

3.3 Identifikasi dan Autentikasi untuk Permintaan Re-Key

3.3.1 Identifikasi dan Autentikasi untuk Re-Key Rutin

Jika Pemilik bersedia terus menggunakan layanan DTB pada saat Sertifikat Pemilik habis masa pakainya (*expire*d) atau setelah Sertifikat dicabut (*revoked*), Pemilik bisa mengulang proses pembuatan Sertifikat dengan melalui verifikasi dan validasi ulang menggunakan verifikasi biometrik.

3.3.2 Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan

Setelah Sertifikat dicabut, Pemilik harus mengulang proses pendaftaran seperti yang dijelaskan pada bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan

Permintaan pencabutan harus selalu diverifikasi dan diautentikasi.

Permintaan pencabutan Sertifikat, dapat diajukan oleh Pemilik, Pihak ketiga yang diberi kuasa oleh Pemilik dengan melampirkan kuasa pencabutan Sertifikat dan/atau oleh Penegak hukum melalui prosedur pencabutan Sertifikat. DTB dapat meminta syarat tambahan jika diperlukan untuk melakukan autentikasi permohonan pencabutan Sertifikat.

Permintaan pencabutan Sertifikat dapat dimohonkan oleh Pemilik dengan menghubungi DTB melalui email ke support@djelas.id.

4. PERSYARATAN OPERASIONAL SIKLUS Sertifikat

Siklus hidup Sertifikat meliputi pendaftaran, penerbitan, perubahan, dan pencabutan Sertifikat. Untuk perubahan Sertifikat terdiri atas 3 macam cara, yaitu:

1. Pembaruan Sertifikat (*Certificate Renewal*): Sertifikat berisikan informasi dan kunci yang sama. Perubahan

terletak pada masa berlaku Sertifikat. Pengaturan lebih lengkap dibahas pada Bagian 4.6.

2. Penggantian kunci (*Certificate Re-key*): Sertifikat berisikan informasi yang sama dan masa berlaku yang dapat berbeda. Perubahan terletak pada kunci yang berasosiasi dengan Sertifikat. Pengaturan lebih lengkap dibahas pada Bagian 4.7.
3. Perubahan Sertifikat (*Certificate Modification)*: Sertifikat berisikan kunci yang sama namun sebagian isi Sertifikat berubah. Pengaturan lebih lengkap dibahas pada Bagian 4.8.

4.1 Permohonan Sertifikat

Berikut adalah ketentuan-ketentuan terkait permohonan Sertifikat yang berlaku bagi Pemohon.

4.1.1 Siapa yang Dapat Mengajukan Permohonan Sertifikat

Pihak yang dapat mengajukan permohonan penerbitan Sertifikat adalah:

a. WNI yang berafiliasi dengan Badan Hukum atau Badan Usaha
b. WNA yang berafiliasi dengan Badan Hukum atau Badan Usaha
c. Badan Hukum atau Badan Usaha yang terdaftar sebagai Badan Hukum atau Badan Usaha yang sah di Indonesia.

4.1.2 Proses Pendaftaran dan Tanggung Jawab

Pemohon harus bertanggung jawab dalam memberikan informasi yang benar dan lengkap sehingga memungkinkan DTB dan/atau RA melakukan verifikasi atas identitas tersebut.

Secara umum, proses pendaftaran terdiri dari langkah-langkah berikut (tidak harus berurutan):

a. Mengisi data diri sesuai formulir pada antarmuka halaman pendaftaran sistem RA;
b. Mengunggah salinan Kartu Tanda Penduduk;
c. Pemohon harus melakukan verifikasi biometrik melalui liveness detection;
d. Menyetujui *Subscriber Agreement*, kebijakan privasi, dan kebijakan jaminan dengan cara mencentang kotak persetujuan pada saat proses pendaftaran;
e. RA melakukan verifikasi data calon Pemilik yang diberikan saat pendaftaran untuk dibandingkan dengan data penduduk pemerintah. Data yang dibandingkan adalah NIK, nama, tanggal lahir dan foto selfie;
f. Jika verifikasi gagal, maka calon Pemilik dapat mengulangi dengan memberikan data yang benar;
g. Jika verifikasi berhasil, maka Pemohon berhasil menjadi Pemilik akun DTB;
h. Selanjutnya RA dapat mengajukan permohonan pembuatan Sertifikat setelah melakukan konfirmasi pada link yang dikirimkan melalui email ke Pemohon;
i. Melakukan pembayaran sesuai dengan struktur harga yang disepakati oleh Pemohon; dan

j. Khusus Warga Negara Asing, Pemohon harus mengajukan permohonan kepada DTB dengan menyertakan persetujuan penerbitan Sertifikat, jaminan keaslian dokumen identitas, salinan Paspor, swa foto, email, nomor telepon selular dan KITAS atau KITAP (sebagaimana diatur pada poin 3.2.3).

DTB bertanggung jawab dalam memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua Sertifikat dimana Sertifikat yang dimaksud menampilkan identitas kepada pengandal atau Pemilik.

DTB bertanggung jawab dalam melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh Pemohon selama proses pendaftaran.

4.2 Pemrosesan Permohonan Sertifikat

4.2.1 Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi

Identifikasi dan autentikasi Pemilik harus memenuhi persyaratan yang ditentukan seperti yang tertera pada Bagian 3.2 dari CPS ini.

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat

Setelah semua informasi identitas telah diverifikasi maka Pemohon dapat membuat Sertifikat dengan menggunakan data identitas tersebut. Apabila terdapat kegagalan verifikasi identitas maka Sertifikat tidak dapat diterbitkan. Jika tidak ada masalah, permohonan disetujui.

DTB menolak permintaan pendaftaran yang validasi persyaratannya tidak lengkap, termasuk untuk alasan berikut:

a. Data diri yang dimasukkan tidak sesuai dengan hasil verifikasi; atau
b. Verifikasi biometrik gagal / Pemilik tidak terverifikasi

Untuk alasan gagal verifikasi, Pemilik dapat mengulangi prosesnya dengan memperbaiki data dukung yang diberikan.

4.2.3 Waktu Pemrosesan Permohonan Sertifikat

DTB akan menerbitkan Sertifikat Pemilik tidak lebih dari 60 menit setelah semua proses verifikasi selesai dan berhasil. Khusus untuk permohonan yang diajukan secara manual oleh Warga Negara Asing, DTB akan menerbitkan Sertifikat Pemilik tidak lebih dari 3 hari setelah semua proses verifikasi selesai dan berhasil.

4.3 Penerbitan Sertifikat

4.3.1 Tindakan PSrE selama Penerbitan Sertifikat

DTB harus melakukan tindakan-tindakan sebagai berikut:

1. Memastikan identitas Pemohon sebagaimana diatur pada Bagian 3.2.2 dan 3.2.3;
2. Memverifikasi otoritas Pemohon sebagaimana diatur pada Bagian 3.2.5;
3. Mempersiapkan dan menandatangani Sertifikat saat semua persyaratan telah dipenuhi;
4. Memastikan bahwa Pemilik menerima Sertifikat sebagaimana diatur pada Bagian 4.4;
5. Membuat Sertifikat tersedia bagi Pemilik setelah Pemilik secara formal menyetujui kewajibannya sebagaimana diatur pada Bagian 9.6.3.

4.3.2 Pemberitahuan ke Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

DTB memberitahu Pemilik dalam maksimum 1x24 jam tentang berhasilnya penerbitan Sertifikat melalui email. Apabila dalam jangka waktu 7 hari tidak terdapat tanggapan atas notifikasi email yang di kirim kepada Pemilik, Pemilik dianggap telah memahami dan menerima setiap informasi yang terkandung dalam Sertifikat. Khusus untuk Warga Negara Asing, pemberitahuan penerbitan Sertifikat disampaikan melalui *email* dalam maksimum 1x24 jam setelah Sertifikat berhasil diterbitkan.

4.4 Penerimaan Sertifikat

4.4.1 Sikap yang Dianggap Sebagai Menyetujui Sertifikat

Pemilik harus melakukan pemeriksaan atas semua informasi dalam Sertifikat dan menyetujui informasi yang terkandung dalam Sertifikat sebelum menggunakan Sertifikat tersebut. Ketika tidak ada keluhan dari Pemilik dalam jangka waktu 7 (tujuh) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat.

4.4.2 Publikasi Sertifikat oleh DTB

Setiap Sertifikat Pemilik dapat diunduh melalui antarmuka sistem DTB.

Sertifikat DTB dipublikasikan di repositori sebagaimana tercantum dalam Bagian 2.1 di atas.

4.4.3 Pemberitahuan Penerbitan Sertifikat oleh DTB ke Entitas Lain

Tidak ada ketentuan.

4.5 Penggunaan Pasangan Kunci dan Sertifikat

4.5.1 Penggunaan Kunci Privat dan Sertifikat oleh Pemilik

Penggunaan Kunci Privat Pemilik harus disertai dengan OTP atau data biometrik Pemilik. DTB melindungi Kunci Privat Pemilik dengan menggunakan *Hardware Security Module* (HSM) dan mendeteksi setiap perubahan. Pemilik harus memakai Kunci Privat dan Sertifikatnya hanya untuk tujuan yang sudah ditentukan.

4.5.2 Penggunaan Kunci Publik dan Sertifikat oleh Pengandal

Pengandal harus menggunakan perangkat lunak yang sesuai dengan X.509. DTB menyatakan batasan penggunaan Sertifikat melalui ekstensi Sertifikat dan harus menyatakan mekanisme untuk menentukan keabsahan Sertifikat (CRL dan OCSP). pengandal harus memproses dan patuh kepada informasi ini sesuai dengan kewajiban mereka sebagai pengandal.

Pengandal harus berhati-hati ketika mengandalkan Sertifikat dan harus mempertimbangkan keseluruhan keadaan dan risiko kerugian sebelum mengandalkan Sertifikat. Mengandalkan tanda tangan digital atau Sertifikat yang belum diproses sesuai dengan standar yang berlaku dapat menyebabkan risiko bagi pengandal. Pengandal bertanggung jawab atas risiko tersebut.

4.6 Pembaruan Sertifikat

PT. Djelas Tandatangan Bersama tidak melakukan Pembaruan Sertifikat.

4.7 Re-Key Sertifikat

4.7.1 Kondisi untuk Re-Key Sertifikat

Penerbitan ulang Sertifikat dengan penggantian kunci (*re-key*) adalah pembuatan/penerbitan Sertifikat baru dengan Kunci Publik, *serial number*, dan *key identifier* yang baru, sementara informasi pribadi Pemilik yang terverifikasi dalam Sertifikat baru masih sama dengan Sertifikat lama. Sertifikat baru dapat diisi masa berlaku yang baru, diisi dengan tempat publikasi CRL yang baru, dan/atau ditandatangani dengan kunci yang baru.

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

Pemilik dapat melakukan re-key selama :

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

Apabila Kunci Privat Pemilik terkompromi atau Sertifikat kedaluwarsa atau dicabut, maka Pemilik dapat mengajukan permohonan baru sebagaimana diatur pada Bagian 4.1.

Pemilik dapat melakukan re-key selama Sertifikat yang aktif masa berlakunya akan berakhir dalam waktu kurang dari 6 bulan.

4.7.2 Siapa yang Dapat Meminta Sertifikasi Public Key yang Baru

Pemilik dapat menghubungi DTB untuk melakukan re-key Sertifikat.

4.7.3 Pemrosesan Permintaan Re-Key Sertifikat

DTB mengikuti prosedur sebagaimana diatur pada Bagian 3.3 dan 4.3. DTB dapat menggunakan masa berlaku Sertifikat baru yang sama seperti masa berlaku Sertifikat sebelumnya.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

DTB melakukan pemberitahuan Penerbitan Sertifikat baru seperti yang dinyatakan pada Bagian 4.3.2.

4.7.5 Melaksanakan Penerimaan Sertifikat Re-Key

Pemilik harus menerima Sertifikat dengan kunci baru, mengikuti prosedur penerimaan yang sama, sebagaimana diuraikan dalam Bagian 4.4.1.

4.7.6 Publikasi Sertifikat Re-Key oleh PSrE

Sertifikat re-key dipublikasikan sesuai ketentuan diatur pada Bagian 4.4.2.

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh DTB ke Entitas Lain

Tidak ada tindakan yang diambil untuk pemberitahuan ke entitas lain.

4.8 Modifikasi Sertifikat

Modifikasi detil Sertifikat tidak diperbolehkan. Apabila terjadi kesalahan selama penerbitan Sertifikat (misalnya, ejaan), Sertifikat akan di-revoke/dicabut dan dilanjutkan dengan proses penerbitan, seperti yang dijelaskan pada Bagian 4.3.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Keadaan untuk Pencabutan

DTB akan mencabut Sertifikat Pemilik dengan alasan atau keadaan sebagai berikut:

a. Komponen informasi yang berafiliasi dengan nama dalam Sertifikat menjadi tidak valid;
b. Informasi apapun dalam Sertifikat menjadi tidak valid;
c. Pemilik terbukti melanggar ketentuan dalam kontrak berlangganannya;

d. Ada alasan untuk meyakini bahwa Kunci Privat telah *compromised*/rusak;

e. Pemilik atau pihak berwenang lainnya (sebagaimana didefinisikan dalam CPS) meminta Sertifikatnya dicabut;

f. DTB berhenti beroperasi;

g. Alasan lainnya yang menurut DTB dibenarkan untuk melakukan pencabutan Sertifikat;

h. Kunci hilang; dan

i. Pemilik sudah tidak bisa lagi menggunakan Sertifikat (misal: meninggal - salinan Sertifikat kematian harus ditunjukkan ke DTB).

Sertifikat harus dicabut ketika hubungan antara subyek dan Kunci Publiknya yang didefinisikan dalam Sertifikat sudah tidak valid lagi. Ketika hal tersebut terjadi Sertifikat harus dicabut dan dimasukkan dalam CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status Sertifikat sampai masa berlaku Sertifikat berakhir.

4.9.2 Siapa yang Dapat Meminta Pencabutan

Pencabutan Sertifikat dapat dilakukan oleh subjek yang terkait dengan Sertifikat dalam hal ini, antara lain :

1. Pemilik Sertifikat;
2. Pihak ketiga yang sama, yang atas kuasanya mengajukan permohonan penerbitan Sertifikat Pemilik dengan melampirkan kuasa pencabutan Sertifikat; atau
3. Penegak hukum yang dapat membuktikan penyalahgunaan Sertifikat sebagaimana didefinisikan dalam CPS.

Dalam hal ketentuan yang tercantum pada bagian 4.9.1. terpenuhi, maka DTB juga dapat melakukan Pencabutan Sertifikat tanpa permintaan pencabutan oleh Pemilik Sertifikat.

4.9.3 Prosedur Permintaan Pencabutan

Pemilik Sertifikat dapat mencabut Sertifikatnya dengan cara sebagai berikut :

1. Pemilik mengajukan permohonan Sertifikat pada DTB melalui email support@djelas.id.
2. Setelah identitas entitas lain tervalidasi, pencabutan Sertifikat akan dilaksanakan oleh DTB dalam jangka waktu 1 jam.
3. Proses pencabutan Sertifikat dilaksanakan oleh Admin Front End atas persetujuan CISO;
4. Setelah pencabutan Sertifikat berhasil dilakukan, Pemilik akan menerima surel terkait aktifitas pencabutan Sertifikat.

Prosedur Pencabutan Sertifikat oleh Pihak ketiga atau Penegak Hukum

1. Pemohon mengajukan permohonan Sertifikat pada DTB melalui email support@djelas.id.
2. DTB memverifikasi identitas dan wewenang yang meminta pencabutan Sertifikat;
3. Validasi identitas dapat dilakukan melalui pengecekan surat tugas;
4. Permintaan pencabutan Sertifikat harus menyampaian bukti bahwa:
    - Keterangan identitas dan kewenangan pihak terkait yang relevan dengan permohonan pencabutan Sertifikat elektronik;
    - Surat perintah pencabutan Sertifikat elektronik (bagi penegak hukum);
    - Keterangan kunci privat Sertifikat telah terpapar; atau
    - Penggunaan Sertifikat tersebut tidak sesuai dengan Kebijakan Sertifikasi.
5. Setelah identitas entitas tervalidasi, pencabutan Sertifikat akan dilaksanakan oleh DTB dalam jangka waktu 1 jam.
6. Proses pencabutan Sertifikat dilaksanakan oleh Admin Front End atas persetujuan CISO;
7. Setelah pencabutan Sertifikat berhasil dilakukan, Pemilik akan menerima surel terkait aktifitas pencabutan Sertifikat.

4.9.4 Tenggang Waktu Permintaan Pencabutan

DTB tidak mengatur tenggang waktu untuk permohonan pencabutan Sertifikat yang diajukan oleh

Pemegang Sertifikat atau pihak ketiga lainnya.

4.9.5 Jangka Waktu DTB Harus Memproses Permintaan Pencabutan

DTB akan segera mencabut Sertifikat dalam waktu 1 hari kerja, setelah persyaratan pengajuan pencabutan Sertifikat sebagaimana tercantum pada bagian 4.9.3 berhasil dipenuhi.

4.9.6 Persyaratan Pemeriksaan Pencabutan untuk Pengandal

Pengandal harus memvalidasi Sertifikat terhadap CRL dan/atau OCSP terbaru yang diterbitkan server DTB.

4.9.7 Frekuensi Penerbitan CRL (bila berlaku)

CRL diperbaharui dan dipublikasi secara berkala :

a. Untuk Sertifikat Pemilik/perangkat, paling sedikit setiap 1 hari. CRL akan berdampak dalam waktu maksimum 26 jam; dan

b. Untuk Sertifikat DTB, sedikitnya setiap 6 bulan. CRL akan berdampak dalam waktu maksimum 6 bulan.

Dalam hal kebocoran Kunci Privat atau insiden keamanan penting lainnya, contohnya pencabutan Sertifikat DTB, CRL terbaru harus HARUS dipublikasikan dalam waktu 26 jam semenjak waktu pencabutan sesuai dengan stemple waktu (*timestamp*).

CRL harus diamankan untuk menjamin integritas dan keautentikannya dan dapat diakses melalui *Repository* https://repository.djelas.id

4.9.8 Latensi Maksimum untuk CRL (bila berlaku)

DTB mempublikasikan CRL paling lama 30 menit setelah penerbitan.

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status secara Daring

Sertifikat yang dicabut, ditandatangani dan dipublikasikan oleh DTB dapat diverifikasi melalui layanan OCSP yang disediakan oleh DTB.

4.9.10 Persyaratan Pemeriksaan Pencabutan secara Daring

Tidak ada ketentuan.

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus terkait Kebocoran Kunci

Tidak ada ketentuan.

4.9.13 Kondisi untuk Pembekuan

Pembekuan Sertifikat tidak disediakan.

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

Tidak ada ketentuan.

4.10.1 Karakteristik Operasional

Status Sertifikat tersedia di CRL yang terdapat pada repositori dan OCSP.

4.10.2 Ketersediaan Layanan

DTB melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status Sertifikat.

4.10.3 Fitur Opsional

Tidak ada ketentuan.

4.11 Akhir Berlangganan

Pemilik dapat menghentikan layanan / penghentian berlangganan jasa DTB dengan cara mencabut Sertifikat, tidak memperpanjang Sertifikat yang akan segera berakhir masa berlakunya atau jasa DTB sudah tidak lagi tersedia.

4.12 Pemulihan dan Eskro Kunci

4.12.1 Kebijakan dan Praktik Eskro Kunci dan Pemulihan

Kunci Privat DTB dan Kunci Privat Pemilik yang terasosiasi dengan Sertifikat yang berisi key usage digital Signature tidak dieskrokan.

4.12.2 Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ada ketentuan.

5. FASILITAS, MANAJEMEN/PENGELOLAAN, DAN KENDALI OPERASI

5.1 Kendali Fisik

5.1.1 Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan DTB maupun lokasi tempat kerja yang digunakan untuk mengelola DTB, harus sama dengan lokasi fasilitas yang digunakan untuk menampung informasi yang bernilai tinggi dan sensitif. Lokasi dan konstruksi tempat kerja, ketika dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjagaan dan sensor intrusi, memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan catatan DTB.

Sistem cadangan DTB disiapkan di data center (DC) cadangannya (yaitu DC yang difungsikan sebagai DRC/*Disaster Recovery Center*), dan mampu memulihkan layanan sistem ketika terjadi kegagalan di DC utama. DRC berada di lokasi yang ketika terjadi bencana alam dalam DC utama, DRC tidak ikut terkena dampaknya. Lokasi fisik DC dan DRC berada di Indonesia. DTB mengukur risiko untuk menentukan jarak antara DC dan DRC yang mempertimbangkan *availability* layanan DTB.

5.1.2 Akses Fisik

Peralatan DTB selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik untuk DTB setidaknya dilakukan untuk:

a. Memastikan tidak ada akses tidak resmi ke perangkat keras;
b. Menyimpan semua *removable media* yang berisi informasi teks yang sensitif dalam tempat penyimpanan yang aman;
c. Memonitor akses yang tidak berwenang baik secara manual maupun elektronik;
d. Memelihara dan memeriksa log akses secara berkala; dan
e. Membutuhkan kendali akses fisik dua orang untuk modul kriptografis dan sistem komputer DTB.

Semua operasional DTB yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan setidaknya memiliki pengamanan berlapis untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif. Fasilitas tersebut harus terpisah secara fisik terpisah dari fasilitas organisasi yang lain, sehingga hanya pegawai DTB yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

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

Data untuk aktivasi diingat atau dicatat dan disimpan dengan pengamanan yang setara dengan pengamanan yang disediakan modul kriptografis, dan tidak boleh disimpan bersama modul kriptografis.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat DTB wajib dilaksanakan jika fasilitas akan ditinggalkan. Setidaknya proses pemeriksaan memverifikasi hal-hal berikut:

1. Untuk DTB yang offline, semua perangkat selain repositori IKP harus dimatikan;
2. Semua security container (misal: lemari besi) sudah diamankan (dikunci);

3. Sistem keamanan fisik (misalnya kunci pintu, pelindung ventilasi) berfungsi dengan baik; dan
4. Area diamankan dari akses yang tidak berhak.

DTB menunjuk satu atau beberapa staf yang berperan dan bertanggung jawab untuk melakukan pemeriksaan tersebut. Pemeriksaan tersebut dibuktikan dengan log yang dapat dipertanggungjawabkan. Jika fasilitas tidak ditempati setiap waktu, maka orang terakhir yang meninggalkan fasilitas harus membuat lembaran *sign-out* yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

5.1.3 Listrik dan AC

DTB memiliki daya listrik cadangan yang cukup ketika listrik utama mati, dan menyelesaikan setiap aksi yang tertunda, dan merekam status perangkat sebelum kekurangan daya atau AC yang menyebabkan *shutdown*. Sistem IKP harus dilengkapi Daya Tak Terputus dan Generator Listrik yang cukup untuk beroperasi paling sedikit 6 (enam) jam saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

5.1.4 Keterpaparan Air

Peralatan DTB ditempatkan pada tempat yang tidak terpapar air. Paparan air untuk pencegahan kebakaran dan tindakan perlindungan (misalnya sistem sprinkler) dikecualikan dari persyaratan ini.

5.1.5 Pencegahan dan Perlindungan Kebakaran

Peralatan DTB ditempatkan di fasilitas dengan sistem deteksi kebakaran dan sistem pemadaman kebakaran yang memadai.

5.1.6 Media Penyimpanan

Media *Backup* dari DTB disimpan di lokasi terpisah dari DC dan DRC diletakan di dalam Brankas kantor DTB, Jl. Bangka Nomor 21, Jakarta. Media backup terlindungi dari kerusakan akibat kecelakaan (air,

api dan elektromagnetik), pencurian, dan akses yang tidak sah.

5.1.7 Pembuangan Limbah

Semua informasi sensitif yang terdapat pada barang yang sudah tidak digunakan dihancurkan sebelum dibuang.

Dokumen yang mengandung informasi sensitif harus dihancurkan sampai tidak dapat direkontruksi kembali. Seluruh perangkat kriptografi yang sudah tidak digunakan harus dihancurkan fisiknya sampai tidak dapat digunakan kembali sebelum dibuang.

Tata cara pembuangan limbah diatur dalam Prosedur Pembuangan Peralatan.

5.1.8 Backup Off-Site

Sistem *backup* DTB dilakukan secara berkala dan mampu memulihkan sistem ketika terjadi kegagalan. *Backup* dilakukan minimal sekali dalam 1 bulan dan hasil backup disimpan diruangan khusus pada safe box perbankan, di lokasi terpisah dari DC dan DRC. Data *backup* dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional DTB.

5.2 Kontrol Prosedur

5.2.1 Peran yang Dipercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

a. Koordinator

   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan DTB.

b. Policy Authority (PA)

   Bertanggung jawab atas persetujuan CP dan CPS.

c. Policy Authority Officer (PAO)

   Bertanggung jawab atas pembuatan, revisi CP dan CPS.

d. Administrator CA

   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem CA.

e. Administrator RA

   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem RA.

f. Administrator Frontend

   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem Frontend.

g. Administrator VA

   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem VA.

h. Administrator HSM

   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem HSM.

i. Administrator Network

   Bertanggung jawab atas instalasi, konfigurasi dan pemeliharaan sistem operasi dan jaringan.

j. Administrator System

   Melakukan *backup* harian dan memantau kapasitas ketersediaan dan insiden.

k. Web Admin Repositori
   Bertanggung jawab atas pembaharuan repositori DTB.
l. Key Manager
   Bertanggung jawab atas pengelolaan inventaris kunci dan token DTB.
m. Internal Penilai
   Bertanggung jawab atas proses audit internal dan monitoring DTB.
n. Developer
   Bertanggung jawab atas pengembangan aplikasi dan sistem DTB.

Peran terpercaya lainnya didefinisikan dalam dokumen lain, yang menjelaskan mengenai persyaratan peran-peran tersebut pada operasional DTB.

5.2.2 Jumlah Orang yang Diperlukan per/tiap Tugas

Untuk kegiatan yang memerlukan kendali multipersonel, semua partisipan harus memegang peran terpercaya. Kendali multipersonel tidak boleh dilakukan dengan melibatkan personel yang bertugas dalam peran Penilai. Tugas berikut memerlukan tiga orang atau lebih:

a. Pembangkitan kunci DTB;
b. Penandatanganan Sertifikat DTB; dan
c. Pencabutan Sertifikat DTB.

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran

Semua individu yang ditugaskan dalam Peran Terpercaya harus merupakan karyawan dari DTB yang sudah melalui proses pemeriksaan latar belakang sesuai Bagian 5.3.2.

Autentikasi Peran Terpercaya 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

Satu orang tidak boleh merangkap peran pada peran-peran berikut:

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

5.3 Kontrol Personil

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan Perizinan

Semua personil DTB harus warga negara Indonesia dan telah dipilih atas dasar 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. Bukti catatan kriminal yang bersih.

5.3.2 Prosedur Pemeriksaan Latar Belakang

Semua personil di DTB harus lulus pemeriksaan latar belakang. Ruang lingkup pemeriksaan latar belakang mencakup area berikut yang mencakup paling tidak dalam dua (2) tahun terakhir:

a. Pendidikan atau sertifikasi;
b. Identifikasi Kependudukan (KTP);
c. Catatan Kepolisian;
d. Pengalaman / referensi kerja; dan
e. Rekening Bank.

DTB akan menggunakan teknik investigasi pengganti yang diizinkan oleh hukum/undang-undang yang memberikan informasi serupa secara substansial, termasuk namun tidak terbatas untuk memperoleh pemeriksaan latar belakang yang dilakukan oleh instansi pemerintah yang berlaku.

5.3.3 Persyaratan Pelatihan

Semua personil DTB dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan semacam itu membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, prosedur terkait, undang-undang/hukum dan peraturan. DTB harus menyimpan catatan pelatihan semua personel DTB.

Pelatihan juga mencakup operasional DTB, topologi jaringan DTB, administrasi aplikasi CA – RA – VA, alur proses aplikasi DTB, sistem monitoring DTB (termasuk perangkat keras, perangkat lunak dan sistem operasi DTB), SMKI, prosedur operasional dan keamanan, CPS ini, dan CP yang berlaku. Evaluasi terhadap kecukupan kompetensi personil DTB harus dilakukan minimal 1 kali dalam setahun.

5.3.4 Frekuensi dan Pelatihan Ulang dan Persyaratanya

DTB memberikan pelatihan ulang yang sifatnya memberi penyegaran dan memutakhirkan kemampuan para personilnya sesuai tingkatan dan frekuensi pelatihan yang dibutuhkan. Hal ini

dilakukan untuk memastikan bahwa personil tersebut mempertahankan kompetensi yang dipersyaratkan untuk melakukan tugas dan tanggung jawab pekerjaan secara memuaskan.

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan

DTB memastikan bahwa perubahan pegawai tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

5.3.6 Sanksi untuk Tindakan yang Tidak Terotorisasi

Sanksi disiplin yang sesuai berlaku pada personel yang melanggar ketentuan dan kebijakan dalam CP, CPS, atau prosedur operasional DTB.

5.3.7 Persyaratan Kontraktor Independen

Pegawai kontrak yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional DTB memenuhi persyaratan yang berlaku yang ditetapkan dalam Bagian 5.3.1, Bagian 5.3.2 dan Bagian 5.3.3 di atas.

5.3.8 Dokumentasi yang Diberikan kepada Personil

DTB menyediakan sejumlah dokumen kepada para personilnya. Dokumen tersebut antara lain CP, CPS, peraturan, kebijakan, dan kontrak yang relevan. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) juga harus disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

DTB menyediakan dokumen yang memadai untuk menunjang tugas dan tanggung jawab bagi setiap peran, dan harus disediakan bagi personel yang melaksanakan peran tersebut.

5.4 Prosedur Log Audit

Berkas log audit dibuat untuk semua kejadian yang terkait dengan keamanan untuk pengelolaan sistem *life cycle* Sertifikat dan kunci (CA). Bila memungkinkan, log audit keamanan dikumpulkan secara otomatis. Bila tidak mungkin, dapat menggunakan buku log, kertas formulir, atau mekanisme fisik lain. Semua log audit keamanan, baik elektronik dan non elektronik, harus disimpan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini harus dipelihara sesuai dengan bagian 5.5.2.

5.4.1 Jenis Kejadian yang Direkam

DTB mengaktifkan semua fitur audit keamanan dari sistem operasi serta aplikasi DTB yang dipersyaratkan oleh CPS ini. Oleh karena itu, sebagian besar dari kejadian yang teridentifikasi harus

direkam secara otomatis. DTB memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan *trusted roles* dalam operasional DTB dapat dilacak.

Setiap record audit, minimal harus memuat poin-poin sebagai berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian yang dapat diaudit):

a. Jenis kejadian;
b. Nomor seri atau urutan rekaman;
c. Tanggal dan waktu terjadi kejadian;
d. Sumber perekaman;
e. Indikator sukses atau gagal yang sesuai; dan
f. Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut.

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

5.4.2 Frekuensi Pemrosesan Log

Log audit harus ditinjau minimal sebulan sekali. Peninjauan tersebut termasuk melakukan verifikasi bahwa log tersebut tidak dirusak, tidak diacak, dan tidak adanya jenis kehilangan lain terhadap data audit, dan kemudian secara singkat memeriksa semua entri log, dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan yang muncul dalam log.

Tindakan yang diambil sebagai hasil dari peninjauan ini didokumentasikan.

5.4.3 Perioda Retensi untuk Log Audit

Log audit DTB disimpan selama 1 tahun agar tersedia untuk pengendalian yang sah. Jangka waktu ini dapat berubah sewaktu-waktu sesuai dengan hukum yang berlaku.

Jejak audit untuk pengelolaan Sertifikat terkait data Pemilik disimpan 5 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. Sistem dapat menimpa (overwrite) log audit setelah log audit tersebut di *backup* dan diarsipkan.

5.4.5 Prosedur Backup Log Audit

Log audit DTB di-*backup* dengan mekanisme *Hot Backup* setiap hari. Backup log tersebut disimpan secara terpisah dari pusat data.

5.4.6 Sistem Pengumpulan Audit (Internal vs Eksternal)

DTB mengumpulkan log audit termaksud namun tidak terbatas pada log berikut ini:

a. Aplikasi;
b. Database;
c. OS;
d. Jaringan;
e. Firewall;
f. *Fingerprint*;
g. CCTV;
h. IDS -IPS;
i. Akses Penyedia Pusat Data;
j. Akses brankas;
k. Ruang khusus;
l. Buku tamu; dan
m. Media penyimpanan (SAN Storage, NAS).

5.4.7 Pemberitahuan ke Subyek Penyebab Kejadian

Tidak ditentukan.

5.4.8 Asesmen Kerentanan

DTB melakukan penilaian akan kerentanan sistem DTB atau komponennya paling tidak sekali dalam seminggu. Uji penetrasi ke sistem DTB dilakukan minimal 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem DTB.

5.5 Pengarsipan Record

5.5.1 Tipe Record yang Diarsipkan

Catatan arsip DTB cukup rinci untuk menentukan kesesuaian operasional DTB dan validitas Sertifikat yang dikeluarkan oleh DTB (termasuk yang dicabut atau kadaluarsa). Minimal, data berikut dicatat pada arsip:

a. Siklus hidup operasi Sertifikat termasuk permohonan Sertifikat dan permintaan pencabutan dan permintaan pembaruan;
b. Semua Sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh DTB;
c. Data konfigurasi sistem IKP;
d. Dokumen CP dan semua CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen tersebut; dan
e. Data audit.

f. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI):

- Penunjukkan dan pencabutan peran dan kewenangan;
- Akses pengunjung ke fasilitas PSrE;
- Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
- Deteksi dan tindakan terhadap insiden keamanan;
- Latihan keadaan darurat;
- Tindakan dan penilaian risiko;
- Perubahan aset, prosedur, dan tanggung jawab; dan
- Perubahan dokumentasi.

5.5.2 Periode Retensi Arsip

Catatan yang diarsipkan disimpan setidaknya selama 5 (lima) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini dipelihara selama masa retensi. Sertifikat DTB yang sudah habis masa berlakunya diarsipkan secara permanen.

5.5.3 Perlindungan Arsip

Catatan yang diarsipkan dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan arsip dan aplikasi yang dibutuhkan untuk memproses catatan arsip akan dipelihara dan dilindungi sesuai peraturan yang ditentukan dalam CP dan dalam CPS yang berlaku.

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

5.5.4 Prosedur Backup Arsip

Prosedur *backup* yang memadai dan teratur dilakukan agar jika terjadi kehilangan atau rusaknya arsip utama, satu set lengkap salinan cadangan yang ada di lokasi terpisah tersedia.

Record backup arsip yang dikelola DTB disamakan dengan arsip seperti Bagian 5.5.1. Tata cara untuk backup arsip diatur dalam Prosedur Pengarsipan Backup.

5.5.5 Persyaratan Record Stempel Waktu

Rekaman arsip DTB diberi stempel waktu (*timestamp*) saat dibuat.

5.5.6 Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip di DTB dilakukan oleh internal DTB.

5.5.7 Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Media penyimpanan informasi arsip DTB diperiksa setelah dibuat. Secara berkala, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya DTB, peran terpercaya (*trusted roles*) dan pihak-pihak lain yang berwenang yang diijinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada peran terpercaya.

5.6 Pergantian Kunci

Kunci Privat DTB diubah secara berkala setiap 10 tahun. Setelah Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat yang lama, namun masih berlaku, akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat pada Sertifikat lama tersebut kadaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama tetap harus disimpan dan dilindungi.

Tabel penjelesan Kunci DTB dan masa berlakunya dijelaskan pada bagian 6.3.2.

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

Apabila DTB memperbarui Kunci Privat yang menghasilkan Kunci Publik baru, DTB akan memberitahu semua Pemilik yang mengandalkan Sertifikat DTB tersebut bahwa telah terjadi perubahan.

5.7 Pemulihan Bencana dan Keadaan Kondisi Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

DTB memiliki rencana tanggap darurat (*Business Continuity Plan*) dan rencana pemulihan bencana (*Disaster Recovery Plan*).

DTB menangani bencana dan insiden *compromise* sesuai dengan prosedur penanganan bencana untuk meminimalkan dampak dari peristiwa seperti itu. Jika Kunci Privat DTB dicurigai telah bocor, penerbitan Sertifikat oleh DTB dihentikan segera. Investigasi independent oleh pihak ketiga dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan diperiksa untuk menentukan prosedur perbaikan yang tepat. Jika Kunci Privat DTB dicurigai sudah bocor, prosedur pada Bagian 5.7.3 harus diikuti.

DTB harus menginformasikan Kemenkominfo apabila mengalami insiden, termasuk namun tidak terbatas pada:

1. Terdeteksinya atau adanya indikasi sistem DTB terkompromi;
2. Adanya upaya untuk menembus sistem DTB, baik secara fisik maupun elektronik;
3. Serangan Denial of Service pada sistem DTB;
4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam field “next update” pada CRLnya yang valid saat ini. DTB harus segera memulihkan penerbitan CRL secepat mungkin; dan/atau
5. CRL dan/atau OCSP responder tidak dapat diakses oleh publik.

Prosedur diperbarui secara berkala sesuai kebutuhan. 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, DTB melakukan hal berikut:

a. Memberitahu PSrE Induk sesegera mungkin sesuai dengan prosedur penanganan insiden;
b. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukanseberapa banyak kehilangan data sejak posisi terakhir backup;
c. Mengoperasikan kembali sistem DTB, dengan memprioritaskan kemampuan untuk membangkitkan informasi status Sertifikat sesuai jadwal penerbitan CRL; atau
d. Bila kunci penandatanganan DTB rusak, operasional DTB harus dilakukan kembali secepat mungkin, dengan memberikan prioritas ke *restore* pasangan kunci DTB yang terdapat pada media *backup*.

Jika kemampuan DTB untuk membangkitkan informasi status Sertifikat tidak bisa dipulihkan dalam jangka waktu yang wajar, DTB harus menentukan apakah perlu untuk meminta pencabutan Sertifikat miliknya kepada Kemenkominfo.

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

5.7.3 Prosedur Kunci Privat EntitasTerkompromi

Dalam kasus kehilangan Kunci Privat atau bocornya algoritma dan parameter yang digunakan untuk

membangkitkan Kunci Privat dan Sertifikat, semua Sertifikat Pemilik/peranti yang terkait dicabut oleh DTB dan kunci-kunci serta Sertifikat-Sertifikat baru diterbitkan tanpa menghentikan layanan.

Dalam kasus kehilangan Kunci Privat dari DTB, semua Pemilik dari DTB diberitahu, semua Sertifikat Pemilik yang diterbitkan oleh DTB yang terkompromi tersebut dicabut, begitu pula dengan Sertifikat milik DTB.

DTB memberitahu Menteri sesegeera mungkin agar dapat melakukan pencabutan Sertifikat. DTB meminta penerbitan Sertifikat baru ke Menteri sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CPS.

DTB membangkitkan Pasangan Kunci DTB baru sesuai dengan prosedur yang ditetapkan dalam CPS. Penerbitan ulang Kunci Privat Pemilik akibat terkompromi dapat dilakukan Pemilik dengan mengajukan permohonan Sertifikat sebagaimana diatur pada Bagian 4.1.

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

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana

DTB memiliki rencana keberlangsungan bisnis dan rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbaharui. Layanan kembali pulih dalam kurun waktu 24 jam bila ada bencana.

Rencana pemulihan bencana DTB ditinjau ulang dan diuji secara berkala (minimal 6 bulan sekali) dan diperbaharui jika dibutuhkan.

Fasilitas *Disaster Recovery Center* DTB tersedia bila fasilitas utama berhenti beroperasi.

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan DTB rusak secara fisik dan semua salinan kunci penandatanganan milik DTB hancur, DTB harus meminta agar Sertifikatnya dicabut. DTB harus mengikuti ketentuan sebagaimana diatur pada bagian 5.7.3.

5.8 Penutupan CA atau RA

Dalam kasus DTB mengakhiri operasinya, DTB memberitahukan Kemenkominfo, Policy Authority, dan para Pemilik Sertifikat sebelum penutupan dilakukan sesuai dengan ketentuan Peraturan perundang-undangan.

a. DTB akan mengirimkan pemberitahuan melalui surat elektronik kepada Kemenkominfo, para pihak yang terlibat dalam siklus operasional Sertifikat, termasuk kepada Pemilik Sertifikat;
b. Memastikan bahwa informasi status Sertifikat tetap dapat diakses sampai masa berlaku

Sertifikat Pemilik berakhir; dan

c. Menghancurkan sistem PKI DTB yang berisi Kunci Privat DTB.

DTB memberikan kompensasi sebagaimana diatur dalam Kebijakan Jaminan.

6 KENDALI KEAMANAN TEKNIS

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan Pasangan Kunci

Tabel berikut berisi persyaratan pembangkitan Pasangan Kunci untuk berbagai entitas.

Entitas	FIPS 140-2 Level	Perangkat Keras atau Perangkat Lunak (Modul Kriptografis)	Dibangkitkan di dalam Modul Kriptografis
CA	3	Perangkat Keras	Ya
Time Stamp Authority	3	Perangkat Keras	Ya
OCSP Responder	3	Perangkat Keras	Ya
Pemilik untuk TTE	3	Perangkat Keras	Ya
Pemilik untuk Enkripsi	3	Perangkat Keras	Ya

Pembangkitkan Pasangan Kunci DTB membutuhkan kendali multipersonel sebagaimana diatur pada Bagian 6.2.2.

6.1.2 Pengiriman Kunci Privat ke Pemilik

DTB membangkitkan sendiri pasangan kunci milik DTB sehingga tidak memerlukan pengiriman Kunci Privat.

DTB membangkitkan pasangan kunci atas nama Pemilik, namun DTB tidak memberikan Kunci Privat kepada Pemilik sehingga tidak ada pengiriman Kunci Privat ke Pemilik.

6.1.3 Pengiriman Kunci Publik ke Penerbit Sertifikat

DTB tidak mengirimkan Kunci Publik. Pemilik dapat mengunduh Kunci Publik dan Sertifikat melalui antarmuka Sistem DTB.

6.1.4 Pengiriman Kunci Publik PSrE kepada Pengandal

Pengandal dapat mengunduh Kunci Publik DTB melalui repositori DTB sebagaimana tercantum pada bagian 2.1.

Pada jangka waktu tertentu sebelum kunci publik DTB kadaluwarsa, suatu pasangan kunci

penandatanganan Sertifikat yang baru akan dibangkitkan supaya DTB tetap bisa beroperasi secara normal.

6.1.5 Ukuran Kunci

DTB membuat Pasangan Kunci dengan menggunakan algoritma RSA dengan panjang kunci 2048 bit untuk kunci Pemilik dan 4096 bit untuk kunci DTB. (ditambah SHA berapa yang digunakan sesuai dengan standar interoperabilutas)

Sertifikat	Encryption Algorithm	Panjang Kunci
DTB	RSA	4096 bit
Pemilik	RSA	2048 bit

6.1.6 Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Tidak ditentukan.

6.1.7 Tujuan Penggunaan Kunci (pada field key usage - X509 v3)

Kunci yang terikat dengan Sertifikat Pemilik digunakan hanya untuk pemanfaatan tandatangan digital. Kunci DTB digunakan untuk penandatangan Sertifikat dan CRL.

6.2 Kontrol Kunci Private dan Kontrol Teknis Modul Kriptografi

6.2.1 Kendali dan Standar Modul Kriptografi

DTB menjamin semua sistem untuk menandatangani Sertifikat dan CRL atau menerbitkan respon OCSP menggunakan perangkat FIPS 140-2 Level 3 sebagai tingkat minimum perlindungan kriptografis.

Untuk Pemilik, Pasangan Kunci dibangkitkan oleh DTB menggunakan Kunci Privat yang dibangkitkan dan dikelola menggunakan modul kriptografis yang memenuhi persyaratan FIPS 140-2 Level 3 dan hanya dapat diakses oleh Pemilik dengan menerapkan kombinasi paling sedikit 2 (dua) faktor autentikasi.

6.2.2 Kendali Multi Personil (n dari m) Kunci Privat

Semua Kunci Privat DTB harus diakses melalui kendali multi-personil seperti yang ditentukan pada Bagian 5.2.2.

Modul kriptografi yang memuat seluruh kunci penandatanganan, tidak boleh diaktivasi hanya oleh 1 (satu) orang. Kunci penandatanganan harus di-*backup* dengan melalui kendali multipersonel.

6.2.3 Eskro Kunci Privat

Kunci Privat DTB tidak dititipkan.

Kunci Privat Pemilik disimpan dan diamankan didalam sistem DTB.

6.2.4 Backup Kunci Privat

Kunci Privat DTB di-*backup* di bawah kendali multi-pihak yang sama dengan kunci tanda tangan asli. Paling tidak satu salinan dari Kunci Privat disimpan *off-site*. Semua salinan Kunci Privat DTB dilindungi dengan cara yang sama dengan aslinya.

Backup pasangan Kunci Pemilik disimpan di *Disaster Recovery Center* (DRC).

6.2.5 Pengarsipan Kunci Privat

Kunci Privat DTB tidak diarsipkan. Kunci Privat Pemilik diarsipkan.

6.2.6 Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci Privat DTB dapat diekspor dari modul kriptografi hanya untuk melaksanakan prosedur *backup* kunci DTB. Kunci Privat DTB tidak pernah sekalipun berada dalam bentuk *plain text* di luar modul kriptografi.

Bila sebuah Kunci Privat akan dipindahkan dari satu modul kriptografi ke yang lain, Kunci Privat dienkripsi selama pemindahan. Token yang dipakai untuk mengenkripsi Kunci Privat ditangani dengan cara yang sama dengan Kunci Privat.

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografis

Kunci Privat DTB disimpan pada modul kriptografi tersertifikasi FIPS 140-2 level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

6.2.8 Metode Pengaktifan Kunci Privat

Aktivasi operasi Kunci Privat DTB dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak seperti yang dinyatakan dalam bagian 5.2.2.

Aktivasi Kunci Privat Pemilik dilakukan oleh DTB.

6.2.9 Metode Penonaktifan Kunci Privat

Setelah dipakai, Kunci Private Pemilik Kembali dienkripsi dan dinonaktifkan oleh personel yang berwenang.

6.2.10 Metode Penghancuran Kunci Privat

Ketika Kunci Privat DTB tidak diperlukan lagi, para individu dalam peran terpercaya menghancurkan Kunci Privat dari HSM dan *backup*-nya dengan menimpa Kunci Privat atau menginisialisasi modul dengan fungsi *factory reset* dari modul kriptografi.

Kejadian penghancuran Kunci Privat DTB dicatat di dalam barang bukti sesuai dengan bagian 5.4.

6.2.11 Pemeringkatan Modul Kriptografis

Seperti diuraikan dalam Bagian 6.2.1.

6.3 Aspek Lain dari Manajemen Pasangan Kunci

6.3.1 Pengarsipan Kunci Publik

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

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasional pasangan kunci didefinisikan oleh periode operasional dari Sertifikat yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai 10 tahun bagi DTB, dan 2 (dua) tahun untuk Pemilik. Periode operasional didefinisikan menurut ukuran kunci dan perkembangan teknologi terkini di bidang kriptografi, sehingga tingkat terbaik untuk keamanan dan efisiensi penggunaan terjamin.

6.4 Data Aktivasi

6.4.1 Pembuatan dan Instalasi Data Aktivasi

Pembangkitan dan penggunaan data aktivasi DTB untuk mengaktifkan Kunci Privat PSrE dibuat pada saat *key ceremony*. Aktivasi data dibuat secara otomatis oleh HSM yang sesuai. Dalam pengaktivan data aktivasi, Kunci Privat dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan.

6.4.2 Perlindungan Data Aktivasi

Aktivasi data DTB dilindungi dari pengungkapan kerahasiaan, perlindungan diberikan melalui kombinasi antara kriptografi dan mekanisme kendali akses fisik. Aktivasi data DTB disimpan dalam token fisik.

6.4.3 Aspek Lain mengenai Data Aktivasi

Tidak ada ketentuan.

6.5 Kontrol Keamanan Komputer

6.5.1 Persyaratan Teknis Keamanan Komputer yang Spesifik/Khusus

Fungsi-fungsi keamanan komputer berikut dapat disediakan oleh sistem operasi, atau melalui suatu kombinasi dari sistem operasi, perangkat lunak, dan perlindungan fisik. DTB menyertakan fungsionalitas berikut:

a. Membutuhkan *login* terautentikasi;
b. Memberikan akses control berdasarkan dokumen kebijakan *User Access Matrix;*
c. Menyediakan kapabilitas audit keamanan;
d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;
e. Menyediakan perlindungan mandiri untuk sistem operasi;
f. Penggunaan kebijakan kata sandi yang kuat;
g. Penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
h. Menyediakan perlindungan dari kode jahat;
i. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
j. Pemeriksaan mandiri terhadap layanan PSrE.

Ketika peralatan DTB diwadahi dalam suatu platform terevaluasi dalam mendukung persyaratan penjaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak, sistem operasi) beroperasi dalam konfigurasi terevaluasi. Paling tidak, platform tersebut memakai versi yang sama dari sistem operasi komputer dengan yang menerima peringkat evaluasi.

Sistem komputer DTB dikonfigurasi dengan meminimalisir jumlah akun dan layanan jaringan yang diperlukan.

6.5.2 Peringkat Keamanan Komputer

Tidak ada ketentuan.

6.6 Kontrol Teknis Siklus Hidup

6.6.1 Kontrol Pengembangan Sistem

Tidak ada ketentuan.

6.6.2 Kontrol Manajemen Keamanan

Konfigurasi dari sistem DTB serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen DTB. Ada mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi milik DTB.

6.6.3 Kontrol Keamanan Siklus Hidup

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

6.7 Kontrol Keamanan Jaringan

DTB menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa sistem terjaga dari *denial of service* dan serangan intrusi. Langkah-langkah sedemikian termasuk penggunaan *firewall* dan *router* penyaring. *Port* jaringan dan layanan yang tidak dipakai dimatikan.

6.8 Tanda Waktu

Semua komponen DTB secara berkala disinkronisasikan dengan sebuah layanan waktu, seperti contohnya layanan *atomic clock* atau *Network Time Protocol* (NTP). Sebuah otoritas khusus untuk menyediakan waktu yang terpercaya juga bisa digunakan jika perlu, misalnya dengan membentuk sebuah otoritas *timestamp* tersendiri. Waktu yang didapat dari layanan waktu di atas akan digunakan untuk menentukan waktu pada saat:

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

Prosedur elektronik atau manual bisa digunakan untuk tetap mempertahankan akurasi waktu pada sistem. Pencocokan jam merupakan sebuah aktivitas yang dapat diaudit.

7 Sertifikat, CRL, DAN PROFIL OCSP

7.1 Profil Sertifikat

Profile Sertifikat mengikuti standar RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”. DTB melakukan *review* terhadap profil Sertifikat secara berkala minimal setahun sekali.

7.1.1 Nomor Versi

DTB menerbitkan Sertifikat X.509 versi 3 (mengisi versi filed dengan integer “2”).

7.1.2 Ekstensi Sertifikat

DTB memakai ekstensi Sertifikat standar yang mematuhi RFC 5280.

7.1.2.1 Key Usage / Penggunaan Kunci

KeyUsage yang digunakan untuk DTB ditunjukan dalam tabel di bawah.

Field	Subordinate CA	Pemilik Sertifikat
Critical	True	True
digitalSignature	False	True
nonRepudiation	False	True
keyEncipherment	False	False
dataEncipherment	False	False
keyAgreement	False	False
keyCertSign	True	false
cRLSign	True	false
encipherOnly	false	false
decipherOnly	false	false

7.1.2.2. Ekstensi Kebijakan Sertifikat

Ekstensi Kebijakan Sertifikat dari Sertifikat X.509 versi 3 diisi dengan pengidentifikasi objek untuk sesuai dengan bagian CPS 7.1.6 (Pengidentifikasi Obyek Kebijakan Sertifikat) dan dengan kualifikasi kebijakan yang ditetapkan dalam bagian CPS 7.1.8 (Sintaks Kualifikasi Kebijakan dan Semantik). Bidang kritikalitas ekstensi ini disetel ke FALSE.

7.1.2.3. Basic Constraint

Ekstensi BasicConstraints Sertifikat X.509 Versi 3 bagi Sertifikat DTB harus memiliki field CA yang diisi TRUE. dan Ekstensi BasicConstraints Sertifikat Pemilik memiliki field CA yang diisi FALSE. Field criticality dari ekstensi ini diisi TRUE untuk Sertifikat DTB, tapi boleh diisi TRUE atau FALSE bagi Sertifikat Pemilik.

7.1.2.4. Extended Key Usage

Secara baku, ExtendedKeyUsage diatur sebagai suatu ekstensi non-kritikal. Sertifikat DTB dapat memuat ekstensi ExtendedKeyUsage sebagai suatu bentuk dari pembatasan teknis pada penggunaan Sertifikat-Sertifikat yang mereka terbitkan. Semua Sertifikat Pemilik harus mengandung sebuah ekstensi extended key usage untuk tujuan bahwa Sertifikat tersebut telah diterbitkan untuk end-user, dan tidak boleh memuat nilai anyEKU.

7.1.2.5. CRL Distribution Points

Sertifikat DTB mencakup ekstensi cRLDistributionPoints yang berisikan URL lokasi CRL untuk pemeriksaan status Sertifikat. Kekritisan ekstensi ini disetel ke FALSE.

7.1.2.6. Authority Key Identifier

Ketika penerbit Sertifikat mengandung ekstensi Pengidentifikasi Kunci Subyek, Pengidentifikasi Kunci Otoritas terdiri dari 160-bit SHA-1 hash dari Kunci Publik dari DTB. Bidang kritikalitas ekstensi ini disetel ke FALSE.

7.1.2.7 *Subject Key Identifier*

Subject key Identifier adalah dimana DTB mengisi versi X.509 Menerbitkan Sertifikat Pemilik dengan ekstensi subjectKeyIdentifier, keyIdentifier berdasarkan Kunci Publik dari subjek Sertifikat dihasilkan sesuai dengan salah satu metode yang dijelaskan dalam RFC 5280. Dimana ekstensi ini digunakan, bidang kekritisan dari ekstensi ini disetel ke FALSE.

7.1.3 Algorithm Object Identifier

Pengidentifikasi objek algoritma kriptografi diisi sesuai dengan standar dan rekomendasi RFC 5280.

OID standar X.509v3 digunakan. Algoritma enkripsi RSA untuk kunci subjek dan SHA256 dengan enkripsi RSA untuk tanda tangan Sertifikat. **sha256withRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.1.4 Format Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1.

7.1.5 Batasan Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1.

7.1.6 Pengidentifikasi Objek Kebijakan Sertifikat

Pengidentifikasi objek kebijakan (OID) merupakan set nomor yang secara unik menunjuk kepada sebuah objek atau kebijakan yang diatur dalam CPS. Bidang kritikalitas ekstensi ini disetel ke FALSE.

7.1.7 Penggunaan Ekstensi Batasan Kebijakan

Tidak ada ketentuan.

7.1.8 Kualifikasi Kebijakan Sintaksis dan Semantik

Tidak Ada ketentuan.

7.1.9 Memproses Semantik untuk Ekstensi Kebijakan Sertifikat Kritis

Tidak ada ketentuan.

7.2 Profil CRL

7.2.1 Nomor Versi

DTB menerbitkan CRL X.509 versi 2.

7.2.2 Ekstensi Entry CRL dan CRL

DTB menggunakan CRL dan CRL *entry extension* RFC 5280.

7.3 Profil OCSP

DTB mengoperasikan *Online Certificate Status Protocol responder* (responder OCSP) mengacu ke Standar Interoperabilitas PSrE Indonesia RCF 5019.

7.3.1 Nomor Versi

DTB menerbitkan respon OCSP versi 1.

7.3.2 Ekstensi OCSP

Tidak ada ketentuan.

8 AUDIT KEPATUHAN DAN PENILAIAN KELAIKAN LAINNYA

Semua kebijakan yang terdapat dalam CPS ini mencakup semua bagian yang relevan dari standar IKP yang saat ini diterapkan untuk berbagai macam industri IKP vertikal, dimana industri-industri tersebut membutuhkan DTB agar bisa beroperasi.

DTB akan menunjuk Penilai independen untuk melaksanakan audit terhadap kepatuhan DTB berdasarkan CP PSrE Induk dan CPS DTB. Penilai juga akan mengaudit sistem RA, CA dan VA DTB.

DTB tunduk pada Peraturan Menteri Komunikasi dan Informatika Nomor 11 tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik. DTB akan diaudit secara berkala oleh Kemenkominfo /

Penilai yang ditunjuk oleh Kemenkominfo.

8.1 Frekuensi atau Lingkup Penilaian

DTB menjalani audit kepatuhan berkala dalam jangka waktu minimal 1 tahun sekali, terhadap skema yang telah ditetapkan yang tidak kurang dari sekali setahun dan setiap terjadi perubahan yang signifikan terhadap CPS, prosedur dan teknik yang diterapkan. DTB juga menyampaikan laporan secara berkala.

8.2 Identitas/Kualifikasi Penilai

Penilai menunjukkan kompetensi pada bidang audit kepatuhan, dan benar-benar memahami persyaratan CP ini. Penilai kepatuhan melakukan audit kepatuhan sebagai tanggung jawab utama.

Penilai memiliki kualifikasi sebagai berikut:

a. Tidak memiliki Konflik kepentingan terhadap PSrE Indonesia;
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 Eelktronik, Segel Elektronik, X.509 versi 3 PKI *Certificate Policy and Certification Practices Framework*, Undang-Undang tentang tentang Informasi dan Transaksi Elektronik, dan Peraturan Menteri Kominfo terkait Tatat Kelola Penyelenggaraan Sertifikasi Elektronik;
c. Memiliki kecakapan dalam memeriksa keamanan teknologi IKP, peralatan dan teknik keamanan informasi, aufdit keamanan informasi, dan penilaian pihak ketiga (*third-party attestation function*).
d. Memiliki sertifikasi sebagai Penilai sistem informasi (CISA) atau IT Security spesialis, IKP Spesialis, yang dapat memberikan masukan terkait *acceptable risks*, startegi 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

Penilai atau Penilai Independen dari DTB atau secara organisasional terpisah dari DTB sehingga memberikan evaluasi independen yang tidak memihak. Untuk memastikan independensi dan objektivitas, Penilai dipastikan tidak melayani DTB dalam mengembangkan atau memelihara fasilitas dan / atau CPS. Kominfo memastikan apakah Penilai memenuhi persyaratan ini.

Selain larangan konflik kepentingan di atas dalam melaksanakan penilaian, Penilai harus memliki

hubungan kontrak yang jelas untuk menjaga indepensi / ketidakperpihakan. Penilai harus mempertahankan standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan pelaksanaan penilaian profesional yang independen, dengan tunduk pada ketentuan peraturan perundang-undangan.

8.4 Topik Penilaian

Penilaian kelaikan bertujuan untuk memverifikasi bahwa DTB beroperasi sesuai dengan CP PSrE Induk yang berlaku dan ketentuan peraturan perundang-undangan. Penilaian kelaikan mencakup penilaian CPS DTB yang berlaku terhadap CP PSrE Induk, menentukan bahwa CPS tersebut telah diimplementasikan dan ditegakkan.

Penialaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen DTB. Penilaian dilaksanakan untuk memenuhi persyaratan dari skema audit yang digunakan dalam penilaian. Persyaratan tersebut dapat berubah seiring dengan pembaruan skema audit. Skema audit baru diberlakukan paling lama 1 (satu) tahun setelah dipublikasikan.

8.5 Tindakan yang Diambil Akibat Ketidaksesuaian

Ketika Penilai menemukan adanya ketidaksesuaian antara bagaimana PSrE dirancang atau dioperasikan atau dipelihara terhadap CP atau CPS yang berlaku, tindakan berikut harus dilakukan:

a. Mencatat ketidaksesuaian tersebut;
b. Penilai kepatuhan segera menyampaikan temuan tersebut kepada PA;
c. PA menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CPS dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan tersebut tanpa penundaan.

8.6 Laporan Hasil Penilaian

Laporan Penilaian Kelaikan, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh DTB, diberikan kepada PA. Laporan tersebut mengidentifikasi versi CP PSrE dan CPS DTB yang digunakan dalam penilaian. Selain itu, hasilnya dikomunikasikan sebagaimana diatur pada bagian 8.5.

8.7 Audit Internal

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan resiko gangguan pada proses bisnis.

DTB memantau kepatuhannya terhadap CP induk, CPS ini, dan ketentuan peraturan perundang-undangan dan secara ketat mengontrol kualitas layanan dengan melakukan audit mandiri setidaknya 1 (satu) kali dalam setahun terhadap sampel yang dipilih secara acak dari setidaknya 1 persen dari

keseluruhan Sertifikat yang diterbitkan.

9 BISNIS LAIN DAN MASALAH HUKUM

9.1 Biaya

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat

DTB mengenakan biaya administrasi dalam menerbitkan atau memperbarui Sertifikat termasuk dalam hal penerbitan ulang Sertifikat yang mengacu pada Permen Kemenkominfo No.11 Tahun 2022.

Detail biaya dapat dilihat di https://repository.djelas.id/doc/struktur-harga.pdf.

9.1.2 Biaya Pengaksesan Sertifikat

DTB tidak mengenakan biaya administrasi kepada Pemilik untuk mengakses repositori DTB.

9.1.3 Biaya Pengaksesan Informasi Pencabutan atau Status

DTB tidak mengenakan biaya kepada Pemilik untuk mengakses daftar pencabutan atau verifikasi status.

9.1.4 Biaya Layanan Lainnya

DTB mengenakan biaya sebagaimana dapat dilihat di https://repository.djelas.id/doc/struktur-harga.pdf dan biaya tambahan lainnya jika ada.

9.1.5 Kebijakan Pengembalian

DTB tidak menyediakan pengembalian biaya Sertifikat. Bagi Pemilik Sertifikat yang mengajukan permohonan kebijakan pengembalian, semua Sertifikatnya dicabut.

9.2 Tanggung Jawab Keuangan

9.2.1 Cakupan Asuransi

DTB menjamin kerugian akibat kegagalan layanan Penyelenggaraan Sertifikasi Elektronik, yang disengaja dan/atau kelalaian DTB kepada orang atau badan usaha dalam mematuhi kewajiban sebagai PSrE sesuai dengan ketentuan perundang-undangan yang diatur dalam dokumen Kebijakan Jaminan.

9.2.2 Aset Lainnya

DTB menjamin bahwa DTB memiliki sumber modal usaha yang cukup untuk menjalankan kegiatan

operasionalnya dan menjalankan fungsinya.

9.2.3 Jaminan Asuransi atau Garansi untuk Entitas Akhir

Batasan tanggung jawab DTB kepada Pemilik Sertifikat atas setiap perselisihan yang timbul dari atau sehubungan dengan layanan DTB atau penggunaan Situs oleh Pemilik Sertifikat, terlepas dari forum penyelesaian perselisihan atau terlepas dari tuntutan berasal dari perbuatan melawan hukum, wanprestasi atau lain sebagainya, tidak akan melebihi Rp. 1.000.000 (satu juta Rupiah) dalam setiap perselisihan atau tuntutan.

9.3 Kerahasiaan Informasi Bisnis

9.3.1 Cakupan Informasi Rahasia

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

a. Informasi pribadi sebagaimana dijabarkan pada bagian 9.4;
b. Kunci Privat Pemilik Sertifikat yang disimpan oleh DTB, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
c. Catatan Permohonan Sertifikat;
d. Hasil penilaian kerentanan;
e. Rekam jejak audit (*audit logs*) dari sistem DTB;
f. Data aktivasi pada saat pengaktifan Kunci Privat DTB sebagaimana dijabarkan pada bagian 6.4;
g. Dokumentasi bisnis proses DTB termasuk dokumen *Disaster Recovery Plans* (DRP) *and Business Continuity Plans* (BCP);
h. Laporan audit dari Penilai independen sebagaimana dijabarkan pada bagian 8.0 ;
i. Kunci Privat DTB; dan
j. Kecuali diwajibkan oleh hukum atau perintah pengadilan, sebelum pengungkapan informasi Pemilik, DTB akan meminta persetujuan tertulis dari Pemilik.

9.3.2 Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia

Informasi yang tidak dikategorikan rahasia dalam dokumen CPS dianggap informasi publik. Sertifikat dan informasi mengenai status Sertifikat termasuk kategori informasi publik.

9.3.3 Tanggung Jawab untuk Melindungi Informasi yang Rahasia

DTB melindungi informasi rahasia. 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

DTB melindungi informasi pribadi dalam kaitan dengan Kebijakan Privasi yang dipublikasikan dalam *repositori* DTB pada Bagian 2.1.

9.4.2 Informasi yang Diperlakukan sebagai Privat

DTB melindungi semua informasi identitas Pemohon dan Pemilik Sertifikat dari pengungkapan yang tidak sah. DTB akan menghapus informasi privat Pemohon yang ditolak. Informasi Pemilik Sertifikat dapat dirilis atas persetujuan Pemilik Sertifikat atau sebagaimana diatur oleh hukum yang berlaku. Arsip yang dikelola oleh DTB tidak boleh dirilis kecuali yang diizinkan pada Bagian 9.4.1.

9.4.3 Informasi yang tidak Dianggap Privat

Informasi yang termasuk dalam bagian 7 (Sertifikat, CRL, dan OCSP) dari CPS ini tidak termasuk pada Bagian 9.4.2.

9.4.4 Tanggung Jawab Melindungi Informasi Privat

DTB bertanggung jawab untuk menyimpan informasi privat sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan dapat berbentuk fisik ataupun elektronik. *Backup* informasi privat dienkripsi setiap akan dipindahkan ke media *backup*.

9.4.5 Pemberitahuan dan Persetujuan untuk menggunakan Informasi Privat

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon. DTB mengakomodir semua ketentuan terkait penggunaan informasi privat ke dalam Kebijakan Privasi dan *Subscriber Agreement*. Kebijakan Privasi dan *Subscriber Agreement* juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh DTB.

9.4.6 Pengungkapan Berdasarkan Proses Peradilan atau Administratif

DTB dapat mengungkapkan data privat dalam rangka memenuhi ketentuan hukum dan peraturan perundang-undangan, dalam rangka proses penegakan hukum atau pengambilan tindakan

pencegahan lebih lanjut sehubungan dengan kegiatan yang tidak berwenang, dugaan tindak pidana atau pelanggaran hukum atau peraturan perundang-undangan.

9.4.7 Keadaan Pengungkapan Informasi Lain

Tidak ada ketentuan.

9.5 Hak atas Kekayaan Intelektual

Semua hak kekayaan intelektual DTB termasuk semua merek dagang dan hak cipta dari semua dokumen DTB tetap menjadi milik tunggal dari DTB.

DTB tidak akan dengan sengaja melanggar hak kekayaan intelektual seperti hak cipta, paten, merek dagang, atau rahasia dagang pihak ketiga. DTB mematuhi pembatasan hukum pada penggunaan materi sehubungan dengan hak kekayaan intelektual, dang penggunaan produk lunak berbayar.

9.6 Pernyataan dan Jaminan

9.6.1 Pernyataan dan Jaminan PSrE

DTB menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

a. DTB mematuhi ketentuan yang diatur dalam CPS ini;
b. DTB menerbitkan dan memperbarui CRL secara berkala;
c. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini;
d. DTB akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.
e. Kunci Privat DTB terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang; dan
f. Hanya informasi yang diverifikasi yang dapat muncul dalam Sertifikat.

9.6.2 Pernyataan dan Jaminan RA

DTB tidak menggunakan external RA. DTB sebagai 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,
c. DTB menjamin bahwa kegiatan registrasi dilakukan sesuai dengan CPS.

9.6.3 Pernyataan dan Jaminan Pelanggan/Pengguna

Pemilik Sertifikat menjamin bahwa:

a. Data yang terkandung dalam Sertifikat sudah sesuai;

b. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada di dalam CP ini;

c. 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 atau menjadi tidak sesuai di dalam Sertifikat tersebut; atau
3. Menghentikan penggunaan Kunci Privat yang Kunci Publiknya tercantum dalam CRL.

d. Akan menanggapi instruksi terkait *compromise* atau penyalahgunaan Sertifikat dalam kurun waktu empat puluh delapan (48) jam;

e. Menyetujui dan menerima bahwa DTB diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam *Subscriber Agreement* atau jika DTB menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phishing*, penipuan atau pendistribusian *malware*;

f. Pemilik Sertifikat adalah pengguna akhir dan bukan merupakan PSrE;

g. Setiap Sertifikat yang dibuat menggunakan Kunci Privat serta berkorespondensi dengan Kunci Publik yang tercantum pada Sertifikat adalah merupakan tanda tangan digital Pemilik dan Sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan digital dibuat;

h. Kunci Privat Pemilik Sertifikat disimpan dan diamankan oleh DTB dan hanya Pemilik Sertifikat yang memiliki akses terhadap Kunci Privat tersebut; dan

i. Sudah melakukan review terhadap informasi dari Sertifikat.

9.6.4 Pernyataan dan Jaminan Pengandal

Pengandal Sertifikat DTB menjamin bahwa:

a. Memiliki kemampuan teknis untuk memverifikasi Sertifikat;

b. Apabila perwakilan dari Pengandal menggunakan suatu Sertifikat yang diterbitkan oleh DTB, Pengandal harus secara benar memverifikasi informasi yang tercantum di dalam Sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut;

c. Melaporkan langsung kepada DTB, jika Pengandal menyadari atau mencurigai bahwa telah terjadi

compromise pada Kunci Privat;

d. Mewajibkan Pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pengandal yang ada pada CPS ini; dan

e. Mematuhi ketentuan yang ditetapkan di CPS dan Perjanjian Pengandal.

9.6.5 Pernyataan dan Jaminan dari Partisipan Lain

Tidak ada ketentuan.

9.7 Pelepasan Jaminan

DTB tidak menjamin:

a. Penyalahgunaan Sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (*Certificate Usage*);
b. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat; dan
c. Selain jaminan yang telah tercantum dalam Kebijakan Jaminan dan sepanjang diizinkan oleh hukum, DTB mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu.

9.8 Pembatasan Tanggung Jawab

9.8.1 Pembatasan Tanggung Jawab PSrE

DTB tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat, termasuk:

a. Semua kerusakan yang diakibatkan dari penggunaan Sertifikat atau pasangan kunci dengan cara

   lain selain didefinisikan dalam CPS, kontrak Pemilik Sertifikat, atau yang diatur dalam Sertifikat itu sendiri;
b. Semua kerusakan yang disebabkan oleh *force majeure*; dan
c. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau *Trojans*) di luar perangkat

   DTB.

9.8.2 Pembatasan Tanggung Jawab RA

DTB sebagai RA tidak bertanggung jawab atas setiap akibat atau kerugian, baik secara langsung

maupun tidak langsung, yang dapat timbul, termasuk namun tidak terbatas pada hal-hal yang disebabkan karena kesalahan Pemilik yaitu

a. Kehilangan data;
b. Kehilangan pendapatan, keuntungan, atau pemasukan lainnya; dan/atau
c. Kehilangan, kerusakan atau kerugian yang timbul dari penggunaan informasi atau data pribadi yang tidak sesuai, akurat dan/atau valid, yang diberikan oleh Pemilik kepada DTB dalam penggunaan layanan DTB berdasarkan CPS ini.

9.9 Ganti Rugi

9.9.1 Ganti Rugi oleh DTB

Ketentuan ganti rugi DTB ditetapkan dalam CPS, Perjanjian Pemilik atau Perjanjian Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat. Kewajiban ganti rugi sesuai dengan ketentuan peraturan perundang-undangan.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat

Pemilik Sertifikat menyetujui untuk melindungi, mengganti rugi dan membebaskan DTB dari dan terhadap setiap dan seluruh klaim dan kerugian, tanggung jawab, biaya dan pengeluaran (termasuk namun tidak terbatas pada klaim dan kerugian, tanggung jawab, biaya dan pengeluaran dari pihak ketiga) yang diderita atau ditanggung oleh DTB yang timbul dari atau sehubungan dengan, baik secara langsung maupun tidak langsung terkait: (a) penyalahgunaan dalam hal pengaksesan yang Anda atas Situs DTB (b) pelanggaran atas Perjanjian oleh Anda atau Pemilik Yang Berwenang; (c) pelanggaran atas hak kekayaan intelektual atau hak lainnya oleh Anda dan/atau Pemilik yang Berwenang; (d) setiap data yang Anda berikan untuk diproses oleh Layanan DTB; atau (e) setiap produk atau jasa yang Anda beli atau dapatkan sehubungan dengan Layanan DTB.

9.9.3 Ganti Rugi oleh Pengandal

Pengandal menyetujui untuk melindungi, mengganti rugi dan membebaskan DTB dari dan terhadap setiap dan seluruh klaim dan kerugian, tanggung jawab, biaya dan pengeluaran (termasuk namun tidak terbatas pada klaim dan kerugian, tanggung jawab, biaya dan pengeluaran dari pihak ketiga) yang diderita atau ditanggung oleh DTB yang timbul dari atau sehubungan dengan, baik secara langsung maupun tidak langsung: (a) penyalahgunaan dalam hal pengaksesan atau penggunaan Anda atas Situs; (b) pelanggaran atas Perjanjian oleh Anda atau Pihak Pengandal Yang Berwenang; (c) pelanggaran atas hak kekayaan intelektual atau hak lainnya oleh Anda; (d) setiap data yang Anda berikan untuk diproses oleh Layanan DTB; atau (e) setiap produk atau jasa yang Anda beli atau dapatkan sehubungan dengan Layanan DTB.

9.10 Jangka Waktu dan Pengakhiran

9.10.1 Jangka Waktu

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh DTB melalui website atau repositori.

9.10.2 Pengakhiran

CPS ini dapat diubah dan akan tetap berlaku sampai digantikan oleh CPS versi terbaru, yang ditandai dengan perubahan dengan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 (tiga puluh) hari setelah dipublikasikan.

9.10.3 Efek Pengakhiran dan Keberlangsungan

DTB mengkomunikasikan efek dari pengakhiran dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit melalui laman atau repositori.

Meski CPS sudah tidak berlaku lagi, aturan terkait pelindungan data dan arsip informasi tetap dipatuhi.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

DTB menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara elektronik, dalam bentuk kertas, atau email berSertifikat. DTB memberikan tanda terima yang valid sebagai bukti pengiriman. DTB memberi tanggapan paling lama 20 hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke DTB dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2.

9.12 Amandemen

9.12.1 Prosedur untuk Amandemen

DTB menerbitkan pemberitahuan di Website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku.

9.12.2 Periode dan Mekanisme Pemberitahuan

DTB menerbitkan pemberitahuan di Website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika terjadi perubahan CPS dipublish paling lama 7 hari kerja sejak tanggal ditandatangani.

9.12.3 Keadaan Dimana OID Harus Diubah

Jika Policy Authority PSrE Induk Indonesia memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, DTB akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

Jika Policy Authority PSrE Indonesia menambah atau mengubah OID dibawah kebijakan OID PSrE Indonesia, maka PSrE Indonesia akan menginformasikan kepada Policy Authority Induk sebelum OID tersebut diimplementasikan.

9.13 Provisi Penyelesaian Ketidaksepahaman

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara DTB dengan Pemilik Sertifikat.

9.14 Hukum yang Mengatur

CPS ini diatur, ditafsirkan, dan dipahami sesuai dengan aturan hkum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama , terlepas dari lokasi domisili ata lokasi penggunaan Sertifikat DTB ataupun produk / layanan yang lainnya. Termasuk apabila Sertifikat DTB digunakan untuk kebutuhan komersial atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan DTB, tetap menerapkan aturan hukum yang berlaku di Indonesia.

Para pihak, termasuk rekan-rekan DTB, Pemilik, maupun pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

9.15 Kepatuhan atas Hukum yang Berlaku

DTB mematuhi semua persyaratan, hukum dan ketentuan 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 operasi praktik bisnis.

9.16 Ketentuan yang Belum Diatur

9.16.1 Seluruh Perjanjian

DTB secara kontraktual mewajibkan RA yang terlibat dalam penerbitan Sertifikat, untuk mematuhi CPS ini dan semua panduan yang terkait.

9.16.2 Pengalihan Hak

Ketentuan pengalihan hak sesuai dengan ketentuan peraturan perundang-undangan atau pengumuman yang berkaitan dengan CPS.

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 akan 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 Pengalihan Hak-hak)

DTB dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan DTB dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak DTB 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 DTB.

9.16.5 Keadaan Memaksa

DTB tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam melaksanakan CPS, yang disebabkan oleh hal-hal yang berada diluar 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. DTB menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas DTB.

9.17 Provisi Lain

Tidak ada ketentuan

10 APPENDIX A. TABLE OF ACRONYMS AND DEFINITIONS

11 Tabel Akronim

Istilah / Term	Definisi / Definition
PSrE CA	Penyelenggara Sertifikasi Elektronik Certification Authority
CP CP	Certificate Policy Certificate Policy
CPS CPS	Certification Practice Statement Certification Practice Statement
CRL CRL	Certificate Revocation List Certificate Revocation List
DTB	PT Djelas Tandatangan Bersama
FIPS FIPS	(US Government) Federal Information Processing Standards (US Government) Federal Information Processing Standards
OCSP OCSP	Online Certificate Status Protocol Online Certificate Status Protocol
OID OID	Object Identifier Object Identifier
IKP PKI	Infrastruktur Kunci Publik Public Key Infrastructure
RA RA	Registration Authority Registration Authority
RFC	Request for Comment
VA	Validation Authority

12 Definisi / Definitions

Istilah / Term	Definisi / Definition
IKP Indonesia Indonesia PKI	Seperangkat perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan, dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan Sertifikat dan kunci yang dapat dipercaya berdasarkan pada kriptografi Infrastruktur Kunci Publik sesuai peraturan Indonesia. A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Infrastructure cryptography according to Indonesian regulations.
PSrE CA	Entitas yang berwenang untuk mengeluarkan, mengelola, mencabut, dan memperbarui Sertifikat dalam lingkup IKP Indonesia. An entity authorized to issue, manage, revoke, and renew Certificates within the Indonesia PKI.
PSrE Induk Root CA Indonesia	Entitas legal yang memiliki otoritas Sertifikasi tingkat teratas yang menandatangani Sertifikat DTB dalam rantai IKP Indonesia. The top-level Certification Authority that signs DTB Certificates in the Indonesian PKI chain.
PSrE Berinduk atau DTB Subordinate CA	Entitas legal yang Sertifikatnya ditandatangani oleh PSrE Induk dan bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Pemilik. Legal entity whose Certificate is signed by the Root CA and is responsible for the creation, issuance, revocation, and management of Subscriber's Certificates.
PSrE Instansi *Government CA*	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi. *Subordinate CA whose responsible for the creation, issuance, revocation, and management of Government Certificates.*

PSrE non-Instansi Non-Government CA	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat non-Instansi. Subordinate CA whose responsible for the creation, issuance, revocation, and management of Non-Government Certificates.
Pemohon Applicant	Individu atau Badan Hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik. The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.
Pemilik Subscriber	Individu yang merupakan subjek dari Sertifikat, telah diterbitkan Sertifikatnya. A person who is the Subject of, and has been issued, a Certificate.
Sertifikat Certificate	Sertifikat adalah Sertifikat yang bersifat elektronik yang memuat tanda tangan digital dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik. Certificate is an electronic certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions.
Sertifikat PSrE Induk Root CA Indonesia Certificate	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PSrE Induk untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh DTB. The self-signed Certificate issued by Root CA Indonesia to identify itself and to facilitate verification of Certificates issued by DTB.
Sertifikat DTB Subordinate's Certificate	Sertifikat yang dikeluarkan oleh PSrE Induk Indonesia. The Certificate issued by Root CA Indonesia.

Sertifikat Pemilik Subscriber's Certificate	Sertifikat yang dikeluarkan oleh DTB. Certificate issued by DTB.
Kebijakan Sertifikat Certificate Policies	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum. A set of rules that indicates the applicability of a named Certificate to a PKI implementation with common security requirements.
Pernyataan Kebijakan Sertifikasi	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat.
Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.
Certificate Revocation List Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh DTB yang menerbitkan Sertifikat. A regularly updated list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.
Certificate Signing Request Certificate Signing Request	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat. A message conveying a request to have a Certificate issued.
Kompromi Compromise	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif. A violation of a security policy that results in loss of control over sensitive information.

Extended Validation Certificate Extended Validation Certificate	Sertifikat yang berisi informasi yang ditentukan dalam Pedoman EV dan yang telah divalidasi sesuai dengan Pedoman tersebut. A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
Kebocoran Kunci 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. A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Upacara Pembangkitan Kunci Key Generation Ceremony	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan, kunci privasinya ditransfer ke modul kriptografi, Kunci Privatnya dicadangkan, dan/atau Kunci Publiknya disertifikasi. A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Object Identifier Object Identifier	Sebuah tanda pengenal alfanumerik atau numerik yang terdaftar di bawah standar yang berlaku terhadap objek atau kelas objek tertentu yang diterbitkan oleh Organisasi Standardisasi Internasional (*International Organization for Standardization*). A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

Online Certificate Status Protocol Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi pengandal yang berisi informasi mengenai status Sertifikat. An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.
Kunci Privat Private Key	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait. The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that
Kunci Publik Public Key	Kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Pribadi terkait dan yang digunakan oleh Pihak yang Mengandalkan untuk memverifikasi Tanda Tangan Digital yang dibuat dengan Kunci Pribadi dan / atau untuk mengenkripsi pesan Pemiliknya sehingga dapat didekripsi hanya dengan Kunci Publik yang sesuai. The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.