Certification Practice Statement (“CPS”)

Penyelenggara Sertifikasi Elektronik (“PSrE”)

Berinduk Indonesia

PT Djelas Tandatangan Bersama (“DTB”)

Nomor	IT-SOP-58-00
Versi	1.0
Tanggal	22 Februari 2021
OID	2.16.360.1.1.1.3.12.7.0.2.1
Jenis Dokumen	Publik

22 Februari 2021
Policy Authority

Aidil Chendramata

Keterangan Revisi Dokumen

Revisi	Tgl.	Penjelasan perubahan	Dibuat oleh
1.0	**22-02-2021**	**Edisi perdana**	**Policy Authority Officer**

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 dibawah PSrE Induk (Kemenkominfo).

Dokumen *Certification Practice Statement* (CPS) DTB ini mendefinisikan persyaratan prosedural dan operasional yang dianut oleh DTB saat menerbitkan dan mengelola objek yang ditandatangani secara digital dalam lingkungan IKP Indonesia.

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.

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 untuk Individu	2.16.360.1.1.1.7.1
OID Sertifikat Level 4	2.16.360.1.1.1.4.4

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 mencabut Sertifikat Digiital 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:

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

1.3.1.2. PSrE Berinduk

DTB adalah PSrE dengan status pengakuan berinduk yang Sertifikatnya telah ditandatangani oleh PSrE Induk. 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, baik pendaftaran awal maupun perpanjangan. DTB menjalankan fungsi RA sendiri dan tidak menggunakan pihak luar.

1.3.2.1 Fungsi dari RA

DTA sebagai RA berkewajiban untuk melaksanakan fungsi sebagai berikut:

a. Memverifikasi dan mengautentikasi data indentitas Pemilik maupun Pemohon berdasarkan prosedur pendaftaran yang ditetapkan oleh DTB;
b. Memulai atau meneruskan proses permohonan pembuatan Sertifikat;

c. Memulai atau meneruskan proses permohonan pencabutan Sertifikat; dan
d. Menyetujui permohonan penerbitan ulang atau perpanjangan Pemilik Sertifikat.

DTB tidak menggunakan RA eksternal.

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.

1.3.4 Pihak Pengandal

Pihak pengandal adalah entitas yang mempercayai Sertifikat dan tanda tangan digital yang diterbitkan oleh DTB (Pihak Pengandal). Pihak 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.

Pihak Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama Pemilik dengan Kunci Publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pihak Pengandal dapat menggunakan informasi dalam Sertifikat untuk menentukan kesesuaian penggunaan dan tujuan Sertifikat. Pihak 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.

Pihak 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

Penyedia Layanan Pusat Data adalah Pihak Ketiga yang menyediakan layanan Pusat Data untuk operasional 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 elektronik; dan
b. Nirsangkal;

DTB hanya menyediakan level verifikasi level 4: Sertifikat dengan Level Verifikasi Tinggi, 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 Pihak Pengandal.

Certificate Class	**Level Verifikasi**			**Penggunaan**		
	Verifikasi Rendah	**Verifikasi Sedang**	**Verifikasi Tinggi**	**Autentikasi**	**Tanda Tangan Digital & Nirsangkal**	**Enkripsi**
Sertifikat Individu						
Level 4			✓		✓	

1.4.2 Penggunaan Sertifikat yang Dilarang

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

1.5 Administrasi Kebijakan

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

a. Menetapkan Certificate Policy (CP) / 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; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang kurang lebih setara.

1.5.1 Organisasi Pengelola Dokumen

CPS dan dokumen referensinya dikelola oleh:

- Alamat Surel : info@djelas.id

- Telepon : +62 21 2271-8863

1.5.2 Kontak yang Dapat Dihubungi

- Alamat surat : Jln. Bangka Raya No. 21
  Kel. Pela Mampang, Kec. Mampang Prapatan
  Jakarta Selatan
- Alamat Surel : info@Djelas.id
- URL : 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

DTB menyetujui CPS dan segala amandemen/perubahannya. Amandemen/perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum. 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 termasuk namun tidak terbatas pada kebijakan, Sertifikat, dan CRL. Repositori daring dapat diakses secara publik di https://repository.djelas.id.

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 Pasal 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>,EMAILADDRESS=<email>, O=personal,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 Pihak 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. DTB tidak perlu memverifikasi hak Pemohon untuk penggunaan merek dagang. 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 kriptografis 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 elektronik.

3.2.2 Autentikasi Identitas Organisasi

Tidak ada ketentuan

3.2.3 Autentikasi Identitas Individu/Perorangan

Permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut.

DTB menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi setidaknya untuk selama masa berlaku dari Sertifikat yang diterbitkan.

Autentikasi identitas individu pemohon Sertifikat harus sesuai dengan Peraturan Menteri Komunikasi dan Informatika terkait Penyelenggara Sertifikasi Elektronik.

Identifikasi dan Autentikasi Identitas Individu yang mengajukan permintaan Sertifikat DTB:

a. Mengumpulkan salinan Kartu Tanda Penduduk resmi yang dikeluarkan oleh pemerintah;
b. Memasukkan informasi data diri seperti NIK, nama lengkap, tempat lahir, tanggal lahir, alamat surel dan nomer seluler;
c. Melakukan proses verifikasi biometrik melalui kamera web Pemilik dan divalidasi dengan data administrasi kependudukan;
d. DTB melakukan verifikasi dan validasi data pemohon dengan data kependudukan pemerintah. Data yang divalidasi adalah NIK, nama, tempat lahir, tanggal lahir dan foto selfie;
e. Konfirmasi untuk aktifasi akun dikirim ke alamat surel yang didaftarkan; dan
f. DTB menyimpan data Pemilik selama 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 Pasal 3.2.3 diatas.

3.2.5 Validasi Otoritas

Tidak ada ketentuan

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*) atau setelah Sertifikat dicabut (*revoke*), 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 Pasal 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 Pemilik oleh penegak hukum dilakukan melalui prosedur pencabutan Sertifikat. DTB wajib melakukan verifikasi manual terhadap permintaan pencabutan Sertifikat.

Permintaan pencabutan Sertifikat dapat dimohonkan oleh Pemilik melalui situs https://cp.djelas.id dengan antarmuka sistem DTB.

4. PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT

4.1 Permohonan Sertifikat

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

4.1.1 Siapa yang Dapat Mengajukan Permohonan Sertifikat

Pemohon yang dapat mengajukan permohonan sertifikat adalah sebagai berikut:

a. Warga Negara Indonesia;
b. Memiliki identitas diri (ektp);
c. Terverifikasi menggunakan verifikasi biometrik dibandingkan dengan data kependudukan pemerintah;
d. Individu yang berasal dari non-Instansi; dan
e. Individu yang merupakan Aparatur Sipil Negara (ASN) dan mendaftar untuk kepentingan pribadi, tidak diperbolehkan mendaftar menggunakan surel instansi pemerintahan.

4.1.2 Proses Pendaftaran dan Tanggung Jawabnya

Pemohon Sertifikat bertanggung jawab untuk memberikan informasi yang akurat dalam mengisi permohonan Sertifikat.

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

a. Mengisi data diri sesuai bidang formulir di antarmuka halaman pendaftaran sistem DTB;
b. Mengunggah salinan Kartu Tanda Penduduk;
c. Melakukan verifikasi biometrik dengan menggunakan *liveness detection*, DTB akan mengambil gambar Pemohon pada saat verifikasi biometrik;
d. Menyetujui *subscriber agreement*, kebijakan privasi, dan kebijakan jaminan dengan cara mencentang kotak persetujuan pada saat proses pendaftaran;
e. DTB melakukan verifikasi data calon Pemilik yang diberikan saat pendaftaran untuk dibandingkan dengan data penduduk pemerintah. Data yang dibandingkan adalah NIK, nama, tempat lahir, tanggal lahir dan foto selfie;
f. Jika verifikasi gagal, maka calon Pemilik dapat mengulangi dengan memberikan data yang benar tanpa batas;

g. Jika verifikasi berhasil, maka Pemohon berhasil menjadi Pemilik akun DTB dan dapat melakukan permohonan pembuatan Sertifikat; dan
h. Melakukan pembayaran sesuai dengan struktur harga yang disepakati oleh Pemohon

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

Pemohon harus memberikan informasi yang cukup sehingga memungkinkan DTB untuk melakukan verifikasi atas identitas tersebut.

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 Pasal 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 gagall 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.

4.3 Penerbitan Sertifikat

4.3.1 Tindakan P S r E selama Penerbitan

DTB mengautentikasi dan memverifikasi Permohonan Sertifikat, memastikan bahwa Pemohon sertifikat merupakan individu yang data dirinya benar dan sesuai dengan yang berada di

catatan kependudukan resmi pemerintah. Sebelum dapat mengakhiri proses registrasi, Pemilik harus memberikan persetujuan terhadap *Subscriber Agreement* yang menandakan bahwa Pemilik telah menyetujui ketentuan penerbitan sertifikat, (termasuk ketentuan terkait tanggung jawab Pemilik atas validasi, kebenaran dan akurasi informasi yang diberikan) Kebijakan Privasi dan Kebijakan Jaminan.

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 kami kirim kepada Pemilik sertifikat, Pemilik sertifikat dianggap telah memahami dan menerima setiap informasi yang terkandung dalam sertifikat.

4.4 Penerimaan Sertifikat

4.4.1 Sikap yang Dianggap Menerima Sertifikat

1. Pemilik dianggap telah menerima Sertifikat yang terbit melalui sistem DTB apabila;

    a. Pemilik menyetujui penerbitan Sertifikat. Dengan menyetujui penerbitan Sertifikat, Pemilik dianggap telah memeriksa dan menyetujui bahwa informasi yang terkandung dalam Sertifikat adalah sesuai dengan informasi yang diberikan Pemilik; dan
    b. Pemilik tidak memberikan tanggapan atas notifikasi surel sebagaimana dimaksud dalam Pasal 4.3.2 dalam jangka waktu 7 hari.

2. Pemilik Sertifikat harus memeriksa informasi yang terkandung dalam Sertifikat adalah sesuai dengan informasi yang diberikan Pemilik dengan cara mengunduh dari antarmuka sistem DTB.

4.4.2 Publikasi Sertifikat oleh DTB

Setiap Sertifikat Pemilik dapat diunduh melalui antarmuka sistem DTB.

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

4.4.3 Pemberitahuan Penerbitan Sertifikat oleh DTB ke Entitas Lain

Tidak ada ketentuan.

4.5 Pasangan Kunci dan Penggunaan Sertifikat

4.5.1 Kunci Privat Pemilik dan Penggunaan Sertifikat

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

4.5.2 Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

Pihak Pengandal harus menggunakan perangkat lunak yang patuh kepada X.509. DTB menyatakan batasan penggunaan Sertifikat melalui ekstensi sertifikat dan harus menyatakan

mekanisme untuk menentukan keabsahan Sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan patuh kepada informasi ini sesuai dengan kewajiban mereka sebagai Pihak Pengandal.

Pihak 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 Pihak Pengandal. Pihak Pengandal bertanggung jawab atas risiko tersebut. Jika keadaan menunjukkan bahwa diperlukan jaminan tambahan, Pihak Pengandal harus mendapatkan jaminan tersebut sebelum menggunakan Sertifikat.

4.6 Pembaruan Sertifikat

4.6.1 Kondisi untuk Pembaruan Sertifikat

Pembaruan Sertifikat didefinisikan sebagai pembuatan Sertifikat baru yang memiliki rincian yang sama dengan Sertifikat yang telah diterbitkan sebelumnya namun dengan pasangan kunci yang berbeda dan berisikan tanggal yang baru pada *field* '*Not After'* dan '*Not Before'*. Pemilik dapat memperbarui Sertifikat selama:

a. Sertifikat yang aktif masa berlakunya akan berakhir dalam waktu kurang dari 6 bulan;
b. Kunci Publik dari Sertfikat asli belum masuk daftar hitam karena alasan apa pun;
c. Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan; atau
d. DTB dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya.

4.6.2 Siapa yang Boleh Meminta Pembaruan

Pemilik yang belum pernah dicabut sertifikatnya dapat meminta pembaruan Sertifikatnya.

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat

Perpanjangan sertifikat harus dilakukan dengan menggunakan proses pendaftaran awal seperti yang dijelaskan pada Pasal 3.2.

4.6.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Prosedur penerbitan sertifikat baru dilakukan seperti yang dinyatakan pada Pasal 4.3.2.

4.6.5 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui

Ketentuan terkait penerimaan sertifikat yang diperbarui sebagaimana diatur dalam 4.4.1 di atas

4.6.6 Publikasi Pembaruan/Perpanjangan Sertifikat oleh PSrE

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam Pasal 4.4.2

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada tindakan yang diambil untuk pemberitahuan entitas lain selain yang tercantum dalam Pasal 9.16

4.7 Re-Key Sertifikat

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

4.7.1 Kondisi untuk Re-Key Sertifikat

Re-key (penggantian kunci) Sertifikat adalah penerbitan ulang suatu sertifikat yang menggunakan informasi subyek dan tanggal kadaluarsa yang sama (field “validTo”) namun dengan pasangan kunci yang baru.

DTB dapat melakukan re-key selama:

a. Sertifikat yang aktif/belum pernah dicabut; dan

b. Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun.

Pemilik dapat memperbarui Sertifikat 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

a. Pemilik yang sertifikatnya telah habis masa berlaku; atau
b. Pemilik yang sertifikatnya dicabut.

4.7.3 Pemrosesan Permintaan Re-Key Sertifikat

Re-key Sertifikat harus dilakukan dengan menggunakan proses pendaftaran awal seperti yang dijelaskan pada Pasal 3.2.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Prosedur Penerbitan Sertifikat baru dilakukan seperti yang dinyatakan pada Pasal 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 Pasal 4.4.1.

4.7.6 Publikasi Sertifikat Re-Key oleh PSrE

Sertifikat Pemilik tidak DTB publikasikan.

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh DTB ke Entitas Lain

Tidak ada tindakan yang diambil untuk pemberitahuan entitas lain selain yang tercantum dalam Pasal 9.16

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 Pasal 4.3.

4.8.1 Kondisi untuk Modifikasi Sertifikat

Modifikasi informasi Sertifikat tidak diizinkan.

4.8.2 Siapa yang Dapat Meminta Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3 Pemrosesan Permintaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.8.5 Melakukan Penerimaan Sertifikat yang Dimodifikasi

Tidak ada ketentuan.

4.8.6 Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Tidak ada ketentuan.

4.8.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Kondisi 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; dan
f. DTB berhenti beroperasi.

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

Sertifikat dapat dicabut atas permintaan Pemilik atau penegak hukum (yang dapat membuktikan pemaparan atau penyalahgunaan sertifikat sesuai dengan Kebijakan Sertifikat).

4.9.3 Prosedur Permintaan Pencabutan

Pemilik Sertifikat dapat mencabut sertifikatnya sendiri melalui sistem yang disediakan oleh DTB.

Untuk melakukan pencabutan Sertifikat, Pemilik melewati tahap verifikasi pada saat:

a. Log in ke dalam akun Pemilik pada situs DTB.
b. Verifikasi biometrik pada saat melakukan pencabutan Sertifikat sehingga Pemilik Sertifikat tidak perlu melakukan permintaan khusus untuk pencabutan sertifikat ke DTB.
c. Memilih alasan pencabutan Sertifikat.

Setelah pencabutan Sertifikat berhasil dilakukan, Pemilik akan menerima surel terkait aktifitas pencabutan Sertifikat.

Untuk permintaan pencabutan Serifikat Pemilik oleh penegak hukum (yang dapat membuktikan pemaparan atau penyalahgunaan sertifikat sesuai dengan Kebijakan Sertifikat), DTB akan memverifikasi identitas dan wewenang pemohon pencabutan, validitas identitas dibutuhkan sesuai dengan Pasal 3.4. Permintaan pencabutan oleh penegak hukum harus memiliki bukti bahwa:

a. Kunci Privat Sertifikat telah terpapar/terungkap; atau
b. Penggunaan Sertifikat tersebut tidak sesuai dengan Kebijakan Sertifikat.

4.9.4 Tenggang Waktu Permintaan Pencabutan

Untuk permintaan pencabutan dari penegak hukum, DTB akan mencabut Sertifikat Pemilik dalam waktu paling lambat 1 jam setelah verifikasi identitas permohonan pencabutan Sertifikat berhasil dilakukan.

Untuk pencabutan langsung oleh Pemilik Sertifikat melalui *menu* antarmuka sistem DTB. Sertifikat akan dicabut secara langsung setelah identitas Pemilik terverifikasi dan tervalidasi melalui verifikasi biometrik dengan menggunakan *liveness detection*.

4.9.5 Jangka Waktu PSrE Harus Memproses Permintaan Pencabutan

DTB memulai permintaan investigasi paling lama dalam waktu 1 hari kerja kecuali dalam hal *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang cukup akan diproses sesegera mungkin.

4.9.6 Persyaratan Pemeriksaan untuk Pihak Pengandal

Pihak Pengandal harus memvalidasi Sertifikat terhadap CRL terbaru melalui server DTB.

Pihak Pengandal harus memvalidasi Sertifikat terhadap server OCSP milik DTB.

4.9.7 Frekuensi Penerbitan CRL (bila berlaku)

CRL harus diperbaharui dan dipublikasi:

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.

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 Online/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 Online

Tidak ada ketentuan.

4.9.11 Bentuk Lain Pengumuman Pencabutan

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus Keterpaparan Re-Key

Jika Sertifikat Pemilik terpapar/terungkap, Sertifikat yang aktif akan dicabut dan langkah selanjutnya mengacu kepada Pasal 4.7.

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 untuk Permintaan Pembekuan

Tidak ada ketentuan.

4.9.16 Pembatasan pada Masa Pembekuan

Tidak ada ketentuan.

4.10 Layanan Status Sertifikat

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. SLA DTB untuk ketersediaan layanan validasi status Sertifikat adalah 99,5%.

4.10.3 Fitur Pilihan

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 Escrow Kunci

4.12.1 Kebijakan dan Praktik Escrow Kunci dan Pemulihan

DTB tidak menitipkan Kunci Privat DTB ke pihak lain. DTB mengelola pasangan kunci Pemilik Sertifikat. Kunci Privat dilindungi dengan menggunakan standard FIPS 140-2 level 3.

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, harus memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan catatan DTB.

5.1.2 Akses Fisik

Peralatan DTB selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik untuk DTB setidaknya harus 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; dan
d. Memelihara dan memeriksa log akses secara berkala.

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.

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 ditempatkan di lokasi terpisah dan harus disimpan agar terlindungi dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau cadangan diduplikasi dan disimpan di lokasi yang terpisah dari DTB.

5.1.7 Pembuangan Limbah

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

5.1.8 Backup Off-Site

Sistem *backup* DTB dilakukan secara berkala dan mampu memulihkan sistem ketika terjadi kegagalan. *Backup* harus dilakukan dan hasil backup tersebut disimpan di lokasi terpisah minimal sekali dalam 7 hari untuk DTB. Setidaknya 1 salinan *backup* lengkap harus disimpan di lokasi terpisah (di lokasi yang terpisah dari perangkat DTB). Hanya *backup* lengkap terkini yang perlu disimpan. Data *backup* harus dilindungi dengan pengamanan fisik dan prosedur

yang setara dengan pengamanan pada operasional DTB. Jarak minimal *off-site backup* adalah 50 km.

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 VA
   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem VA.

g. Administrator HSM
   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem HSM.

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

i. Administrator Operator
   Melakukan *backup* harian dan memantau kapasitas ketersediaan dan insiden.

j. Web Admin Repositori
   Bertanggung jawab atas pembaharuan repositori DTB.

k. Key Manager
   Bertanggung jawab atas pengelolaan inventaris kunci dan token DTB.

l. Internal Auditor
   Bertanggung jawab atas proses audit internal dan monitoring DTB.

m. Developer
   Bertanggung jawab atas pengembangan aplikasi dan sistem DTB.

Peran terpercaya lainnya bisa 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 multi-pihak, semua partisipan harus memegang peran terpercaya. Kendali multi-pihak tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. 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 diidentifikasi dan diautentikasi menggunakan surat penugasan.

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 harus 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.

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 harus 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 harus 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 harus memenuhi persyaratan yang berlaku yang ditetapkan dalam Pasal 5.3.1, Pasal 5.3.2 dan Pasal 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.

5.4 Prosedur Log Audit

Berkas log audit harus 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 Pasal 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.

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.

5.4.5 Prosedur Backup Log Audit

Log audit DTB di-*backup* sedikitnya sebulan sekali. Media *backup* harus disimpan secara lokal pada lokasi yang aman. Salinan kedua dari log audit harus diletakkan pada tempat terpisah setiap bulan.

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 setahun.

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 pendaftaran Pemilik.

5.5.2 Periode Retensi Arsip

Catatan yang diarsipkan harus disimpan setidaknya selama 5 tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi. Sertifikat DTB yang sudah habis masa berlakunya wajib 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.

5.5.4 Prosedur Backup Arsip

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

Record backup arsip yang dikelola DTB disamakan dengan arsip seperti Pasal 5.5.1.

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.

Apabila DTB memperbarui Kunci Privat dan dengan demikian menghasilkan Kunci Publik baru, DTB 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 harus dihentikan segera. Investigasi independent oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan harus diperiksa untuk menentukan prosedur perbaikan yang tepat. Jika Kunci Privat DTB dicurigai sudah bocor, prosedur pada Pasal 5.7.3 harus diikuti.

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 menentukan seberapa 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*.

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.

Bila Kunci Privat dari PSrE Induk hilang, PSrE Induk harus memberitahu PA dan Pihak Pengandal melalui pengumuman publik. DTB HARUS menghentikan layanan, memberitahu semua Pemilik dari semua DTB, dilanjutkan dengan pencabutan semua Sertifikat, menerbitkan suatu CRL akhir, dan memberitahu kontak-kontak keamanan yang relevan. Lalu Infrastruktur Kunci Publik akan disiapkan lagi dengan DTB baru dimulai dengan suatu PSrE Induk baru.

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.

5.8 Penutupan CA atau RA

Dalam kasus DTB mengakhiri operasinya, DTB memberitahukan Kemenkominfo, PA, 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

6.1.1.1 Pembangkitan Pasangan Kunci CA

Material kunci kriptografi yang digunakan oleh DTB untuk menandatangani Sertifikat, CRL atau informasi status harus dibuat di dalam modul kriptografis yang sesuai standar FIPS 140-2 level 3, atau standar lain yang setara. Kendali multi-pihak dibutuhkan untuk pembangkitan pasangan kunci DTB seperti yang ditentukan pada Pasal 6.2.2.

Pembangkitan pasangan kunci DTB harus menghasilkan jejak audit yang dapat diverifikasi yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. Dokumentasi prosedur harus cukup rinci untuk menunjukkan bahwa pemisahan peran yang tepat digunakan. Pihak ketiga yang independen harus memvalidasi pelaksanaan prosedur pembangkitan kunci baik dengan menyaksikan pembangkitan kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci.

6.1.1.2 Pembangkitan Pasangan Kunci Pemilik

Pembangkitan pasangan kunci pemilik dilakukan oleh DTB dalam suatu modul kriptografi yang sesuai dengan standar FIPS 140-2 level 3.

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 Pihak Pengandal

Pihak Pengandal dapat mengunduh Kunci Publik DTB melalui repositori DTB sebagaimana tercantum pada Pasal 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.

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 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 menggunakan modul kriptografi yang sudah sesuai standard FIPS 140-2 level 3 untuk operasional DTB.

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 Pasal 5.2.2.

6.2.3 Escrow Kunci Privat

Kunci Privat DTB tidak dititipkan.

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.

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 Pasal5.2.2.

Aktivasi Kunci Privat Pemilik dilakukan oleh DTB.

6.2.9 Metode Penonaktifan Kunci Privat

Setelah dipakai, Kunci Private Pemilik Kembali dienkripsi dan dinonaktifkan oleh DTB.

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 Pasal 5.4.

6.2.11 Pemeringkatan Modul Kriptografis

Seperti diuraikan dalam Pasal 6.2.1.

6.3 Aspek Lain dari Manajemen Pasangan Kunci

6.3.1 Pengarsipan Kunci Publik

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasional pasangan kunci didefinisikan oleh periode operasional dari Sertifikat yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai 10 tahun bagi DTB, dan 1 tahun untuk Pemilik. Periode operasional harus 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

Aktivasi data dibuat secara otomatis oleh HSM yang cocok dan dikirimkan ke shareholder, dimana shareholder tersebut haruslah orang yang memiliki Peran Terpercaya.

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. Menyediakan *Discretionary Access Control;*
c. Menyediakan kapabilitas audit keamanan;
d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data; atau
e. Menyediakan perlindungan mandiri untuk sistem operasi.

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 Stempel 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, dan
d. Penerbitan Sertifikat Pemilik

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 harus 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. *Certificate Policies Extension*

Ekstensi Kebijakan Sertifikat dari Sertifikat X.509 versi 3 diisi dengan pengidentifikasi objek untuk CP DTB sesuai dengan Pasal CPS 7.1.6 (Pengidentifikasi Obyek Kebijakan Sertifikat) dan dengan kualifikasi kebijakan yang ditetapkan dalam Pasal 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 harus memiliki field CA yang diisi FALSE. Field criticality dari ekstensi ini harus 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 harus digunakan. Algoritma harus 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 Pasal 3.1

7.1.5 Batasan Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam Pasal 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 CP/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 RFC 5280 dan ekstensi entri CRL.

7.3 Profil OCSP

Online Certificate Status Profile (OCSP) yang diatur oleh DTB patuh terhadap standar yang ada pada IETF RFC 6960 dan IETF 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 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 auditor independen untuk melaksanakan audit terhadap kepatuhan DTB berdasarkan CP dan CPS DTB. Auditor juga akan mengaudit sistem RA, CA dan VA DTB.

DTB tunduk pada Peraturan Menteri Komunikasi dan Informatika tentang Penyelenggaraan Sertifikasi Elektronik. DTB akan di audit secara berkala oleh Kemenkominfo / auditor yang ditunjuk oleh Kemenkominfo.

8.1 Frekuensi atau Keadaan Asesmen

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 prosedur dan teknik yang diterapkan.

DTB juga *comply* untuk laporan secara berkala.

8.2 Identitas/Kualifikasi Asesor

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

Auditor kepatuhan memiliki kualifikasi sebagai berikut:

a. Audit dilaksanakan oleh tim asesmen independen yang *qualified*;

b. Auditor memiliki pengetahuan yang cukup tentang tanda tangan digital, Sertifikat, X.509 versi 3 PKI Certificate Policy and Certification Practices Framework, UU ITE, PP PSTE, Peraturan Menteri Komunikasi dan Informatika tentang penyelenggara sertifikasi elektronik;
c. Auditor memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
d. Auditor memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah;
e. Auditor menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

8.3 Hubungan Asesor ke Entitas yang Dinilai

DTB memilih auditor / penilai yang independen dari DTB. Internal Auditor DTB juga dapat memberikan masukan yang akan dipertimbangkan oleh DTB.

8.4 Topik yang Dicakup oleh Asesmen

Audit yang dilaksanakan memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema audit akan berlaku pada tahun berikutnya setelah DTB mengadopsi skema yang terbaru. Audit yang dilaksanakan harus mengikuti standar industry, mencakup kepatuhan DTB dalam pelaksanaan usahanya, dan mengevaluasi integritas operasi IKP DTB. Audit harus dapat memverifikasi bahwa DTB telah mematuhi dokumen CPS ini.

8.5 Tindakan yang Diambil sebagai Hasil dari Kekurangan

Ketika auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana DTB dirancang atau dioperasikan atau dipelihara terhadap persyaratan CP atau CPS yang berlaku, tindakan berikut harus dilakukan:

a. Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.
b. Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian harus 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 Komunikasi Hasil

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan terhadap komponen, diberikan kepada PA sebagaimana diatur dalam Pasal 8.2. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam penilaian.

DTB mengkomunikasikan hasil audit kepada manajemen dan staff internal yang bersangkutan dan melakukan perbaikan

8.7 Audit Internal

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

9. BISNIS LAIN DAN MASALAH HUKUM

9.1 Biaya

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat

DTB mengenakan biaya administrasi dalam menerbitkan atau memperbaharui Sertifikat termasuk dalam hal penerbitan ulang Sertifikat yang mengacu pada Permen Kemenkominfo.

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 tambahan untuk layanan penandatanganan digital.

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

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, kesengajaan, dan/atau kelalaian kepada orang, badan usaha, atau Instansi karena kegagalannya 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).

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 Pasal 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 auditor independen sebagaimana dijabarkan pada Pasal 8.0; dan
i. Kunci Privat DTB.

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 sesuai Pasal 2.1.

9.4.2 Informasi yang Dianggap Pribadi

DTB melindungi semua informasi identitas Pemilik Sertifikat dari pengungkapan yang tidak sah. 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 Pasal 9.4.1.

9.4.3 Informasi yang tidak Dianggap Pribadi

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

9.4.4 Tanggung Jawab Melindungi Informasi Pribadi

DTB bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan dapat berbentuk digital maupun kertas. *Backup* informasi pribadi dienkripsi setiap akan dipindahkan ke media *backup*.

9.4.5 Catatan dan Persetujuan untuk memakai Informasi Pribadi

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon. DTB mengakomodir semua ketentuan terkait penggunaan informasi pribadi 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 pribadi 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.

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; dan
d. DTB akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

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 Pihak yang Mengandalkan

Pihak yang mengandalkan Sertifikat DTB menjamin bahwa:

a. Memiliki kemampuan teknis untuk memverifikasi Sertifikat;

b. Apabila perwakilan dari pihak Pengandal menggunakan suatu Sertifikat yang diterbitkan oleh DTB, pihak 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 pihak Pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat;
d. Mewajibkan Pihak 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 Pihak Pengandal yang ada pada CPS ini; dan
e. Harus mematuhi ketentuan yang ditetapkan di CPS dan Perjanjian Pihak 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 Pasal 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 tidka 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 CP ini.

9.9 Ganti Rugi

9.9.1 Ganti Rugi oleh DTB

Kewajiban ganti rugi DTB harus ditetapkan dalam CPS, *Subscriber Agreement*, Kebijakan Jaminan atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat

Diatur dalam *Subscriber Agreement.*

9.9.3 Ganti Rugi oleh Pihak Pengandal

Diatur dalam Perjanjian Pihak Pengandal

9.10 Syarat dan Pengakhiran

9.10.1 Syarat

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

9.10.2 Pengakhiran

Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 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.

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 Pasal 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.

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 hukum di Indonesia.

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

9.15 Kepatuhan atas Hukum yang Berlaku

DTB mematuhi hukum yang berlaku di Indonesia. Ekspor berbagai jenis perangkat lunak tertentu yang digunakan dalam berberapa produk dan layanan manajemen Sertifikat publik DTB dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang berwenang. Para Pihak (termasuk DTB, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi Undang-Undang dan regulasi yang berlaku di Indonesia

9.16 Ketentuan yang Belum Diatur

9.16.1 Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2 Pengalihan

Entitas yang beroperasi dibawah CPS ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari DTB.

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 wajib 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	Penyelenggara Sertifikasi Elektronik
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DTB	PT Djelas Tandatangan Bersama
FIPS	(US Government) Federal Information Processing Standards
OCSP	Online Certificate Status Protocol
OID	Object Identifier
IKP	Infrastruktur Kunci Publik
RA	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 elektronik 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	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 Certification Practice Statement	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat. 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 Pihak 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 were encrypted with the corresponding Public Key.

Kunci Publik	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.
Public Key	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.