PEDOMAN KEPALA BALAI SERTIFIKASI ELEKTRONIK

NOMOR 33 TAHUN 2022

TENTANG

KEBIJAKAN SERTIFIKAT (*CERTIFICATE POLICY*) DAN PERNYATAAN PRAKTIK SERTIFIKASI ELEKTRONIK (*CERTIFICATION PRACTICE STATEMENT*) *SECURE SOCKET LAYER* (SSL) BALAI SERTIFIKASI ELEKTRONIK *CERTIFICATION AUTHORITY* (BSrE CA)

Versi 1.0

Nomor dokumen	8 Tahun 2022
Tanggal pembuatan	20 Januari 2022
Tanggal Efektif	1 Februari 2022
Jadwal Reviu	1 Februari 2023
Klasifikasi	Biasa
Disahkan oleh	Ditandatangani secara elektronik oleh: KEPALA BALAI SERTIFIKASI ELEKTRONIK **Jonathan Gerhard T., S.ST** Penata Tk. I (III/d)

Lembar Catatan Review / Revisi

No.	Tanggal	Versi	Deskripsi	Oleh
1.	26 Juni 2022	1	Terbitan Pertama	*Policy Authority* BSrE

DAFTAR ISI

BAB I
PENGANTAR

1.1. Ringkasan

Dalam rangka mendukung pelaksanaan tugas dan fungsi Badan Siber dan Sandi Negara (BSSN) dalam upaya meningkatkan keamanan nasional di bidang siber dan sandi melalui pelayanan sertifikasi elektronik, BSSN membentuk Balai Sertifikasi Elektronik (BSrE) sebagai unit pelaksana teknis penyelenggara sertifikasi elektronik yang dinamakan BSrE CA. Tujuan penyelenggaraan layanan BSrE CA adalah untuk memenuhi aspek-aspek keamanan dengan derajat kepastian dan risiko tinggi atas informasi dan/atau dokumen elektronik yang dikelola, dipertukarkan dan disimpan pada sistem-sistem elektronik melalui pemanfaatan sertifikat elektronik. Cakupan aspek keamanan informasi pada pemanfaatan sertifikat elektronik meliputi kerahasiaan, autentikasi, integritas dan anti penyangkalan.

Dokumen ini adalah CP/CPS SSL yang berisi acuan teknis dalam penyelenggaraan sertifikasi elektronik BSrE CA. Dokumen CP/CPS SSL BSrE CA ini mengacu pada ketentuan-ketentuan dasar penyelenggaraan sertifikasi elektronik pada kerangka RFC 3647 dari IETF tentang Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework*, *Reference Certificate Policy* NIST IR 7924, EV SSL *Guidelines* v1.6.2, dan ketentuan mengenai identitas digital mengacu pada NIST 800-63-3. Regulasi dalam penyelenggaraan sistem dan transaksi elektronik di Indonesia yakni Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik, Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2019 tentang Organisasi dan Tata Kerja Balai Sertifikasi Elektronik.

1.2. Nama dan Identifikasi Dokumen CP/CPS SSL BSrE CA

Nama dokumen ini adalah CP/CPS SSL BSrE CA. OID dokumen ini adalah 2.16.360.1.1.1.3.11.2.0.2 dan versi dokumen ini adalah CP/CPS SSL BSrE CA Versi 1.0.

OID	Penggunaan
2.16.360.1.1.1.3.11.2	BSrE CA
2.16.360.1.1.1.3.11.2.0.2	CP/CPS SSL
2.16.360.1.1.1.3.11.2.1.1	Sertifikat SSL
2.16.360.1.1.1.3.11.2.1.2	Sertifikat EV SSL

1.3. Peserta dalam Infrastruktur Kunci Publik

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1 Penyelenggara Sertifikasi Elektronik (PSrE) Induk Indonesia

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

1.3.1.2 BSrE CA

BSrE CA merupakan Penyelenggara Sertifikasi Elektronik Berinduk Instansi yaitu PSrE yang menerbitkan sertifikat kepada Pemilik yang merupakan entitas pemerintah Indonesia. BSrE CA terdiri dari kumpulan perangkat keras, perangkat lunak, dan personil yang bertugas membuat, menandatangani, dan menerbitkan sertifikat elektronik untuk pemohon/ pemilik sertifikat elektronik. BSrE CA beroperasi sesuai dengan ketentuan perundang-undangan yang berlaku di Indonesia tentang Sertifikasi Elektronik. BSrE CA tidak boleh berinduk kepada PSrE lain dan tidak boleh menjadi induk bagi PSrE lainnya.

1.3.2 Otoritas Pendaftaran (RA)

Otoritas Pendaftaran yang selanjutnya disebut RA adalah personil yang bertanggung jawab melakukan pemeriksaan, penyetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan dan pencabutan sertifikat elektronik yang diajukan oleh pemilik (atau calon pemilik) sertifikat elektronik BSrE CA.

1.3.2.1 Fungsi dari RA

Tugas utama RA adalah:

a. Memproses setiap permintaan layanan penerbitan, pembaruan dan pencabutan sertifikat elektronik;
b. Melakukan proses identifikasi, autentikasi dan pemeriksaan terhadap kelengkapan bukti dan berkas milik entitas yang mengajukan permintaan layanan sertifikat elektronik.

1.3.2.2 Persyaratan khusus RA untuk Sertifikat EV SSL

Tidak ada ketentuan.

1.3.3 Pemilik Sertifikat Elektronik

Pemilik adalah pihak yang memohon dan berhasil mendapatkan Sertifikat Elektronik yang ditandatangani oleh BSrE CA. Entitas Pemilik berarti subjek pemilik Sertifikat Elektronik sekaligus entitas yang terikat dengan BSrE CA penerbit Sertifikat Elektronik. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat Elektronik, Pemilik disebut sebagai Pemohon.

1.3.4 Pengandal Sertifikat Elektronik

Pengandal adalah pihak yang mengandalkan (mempercayai) informasi yang ada dalam Sertifikat Elektronik dan/atau Tanda Tangan Elektronik yang diterbitkan oleh BSrE CA. Pengandal harus terlebih dahulu memeriksa respon dari CRL atau OCSP BSrE CA yang sesuai sebelum memanfaatkan informasi yang ada dalam sertifikat.

Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama Pemilik dengan kunci publik. Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat. Pengandal dapat menggunakan informasi dalam sertifikat untuk menentukan kecocokan penggunaan sertifikat. Pengandal menggunakan informasi dalam Sertifikat Elektronik untuk:

a. Memeriksa tujuan penggunaan sertifikat;
b. Melakukan verifikasi tanda tangan elektronik;
c. Memeriksa status pencabutan Sertifikat Elektronik termasuk di dalam CRL dan/atau OCSP; dan
d. Penyetujuan batas tanggung jawab dan jaminan

Pengandal dapat meliputi Bank, Perusahaan *e-Commerce*, Instansi Penyelenggara Negara dan entitas lain.

1.3.5 Partisipan Lain

BSrE CA dapat menentukan Partisipan lain yang berhubungan dengan operasional sertifikat.

1.3.5.1 Verifikator

Verifikator adalah personel yang bertanggung jawab melakukan proses verifikasi terhadap kelengkapan bukti dan berkas calon atau Pemilik Sertifikat Elektronik BSrE CA pada proses pendaftaran Sertifikat Elektronik.

1.3.5.2 Penyedia layanan pusat data

Penyedia layanan pusat data adalah pihak yang menyediakan layanan pusat data untuk operasional BSrE CA

1.4. Kegunaan Sertifikat Elektronik

Informasi yang diproses atau dilindungi menggunakan sertifikat elektronik yang diterbitkan oleh BSrE CA bervariasi ditinjau dari derajat kepentingan penggunaannya.

1.4.1 Penggunaan Sertifikat Elektronik

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

a. Autentikasi;

   Jenis Sertifikat yang disediakan adalah Sertifikat untuk otentikasi dua arah.

b. Tanda Tangan Elektronik & Non-Repudiasi;

   Jenis Sertifikat yang disediakan BSrE CA adalah Sertifikat Tanda Tangan Elektronik

c. Enkripsi;

   Layanan BSrE CA yang menggunakan enkripsi adalah pengiriman elektronik tercatat

Level Sertifikat	Level Verifikasi			Penggunaan		
	Verifikasi Rendah	Verifikasi Sedang	Verifikasi Tinggi	Autentikasi	Tanda Tangan Digital dan Nirsangkal	Enkripsi
Level 4			✓	✓	✓	✓

Pemilik Sertifikat Elektronik BSrE CA menggunakan verifikasi identitas level 4 yakni untuk verifikasi identitas dengan tingkat kepastian dan risiko tinggi. Verifikasi identitas dilakukan menggunakan kartu identitas dan data *biometric* yang dibandingkan dengan data identitas yang dimiliki oleh pemerintah.

1.4.2 Penggunaan Sertifikat yang Dilarang

Sertifikat elektronik yang telah diterbitkan oleh BSrE CA tidak boleh digunakan selain untuk keperluan yang tercantum pada poin 1.4.1 di atas.

1.5. Administrasi Kebijakan/PA

PA adalah entitas yang bertanggung jawab menentukan CP/CPS SSL BSrE CA telah sesuai dengan dokumen acuan dan dapat diterapkan untuk sistem-sistem elektronik instansi penyelenggara negara sebagai stakeholder dari BSrE. PA BSrE CA adalah kepala BSrE.

PA memiliki peran dan tanggung jawab sebagai berikut:

a. Menetapkan CP/CPS SSL;
b. Memastikan semua layanan, operasional dan infrastruktur BSrE CA yang didefinisikan dalam CP/CPS SSL telah dilakukan sesuai dengan persyaratan, representasi; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang kurang lebih setara.

1.5.1 Organisasi Pengelola Dokumen

CP, CPS, dan dokumen referensinya dikelola oleh:

Balai Sertifikasi Elektronik

Jl. Harsono RM No.mor 70, RT.2/RW.4, Ragunan, Kec. Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550

E-mail : info.bsre@bssn.go.id

1.5.2 Kontak yang Dapat Dihubungi

Kepala Balai Sertifikasi Elektronik

Telegram: t.me/infobsre

Email: info.bsre@bssn.go.id

1.5.3 Personil yang Menentukan Kesesuaian CP/CPS SSL dengan Kebijakan

PA BSrE CA menentukan kesesuaian konten CPS dan kesesuaian antara CPS dengan CP.

1.5.4 Prosedur Persetujuan CP/CPS SSL

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

1.6. Definisi dan Akronim

Lihat Lampiran A untuk tabel akronim dan definisi.

BAB II
PUBLIKASI DAN TANGGUNG JAWAB REPOSITORI

2.1 Repositori

BSrE CA bertanggung jawab memelihara repositori daring yang dipublikasikan pada suatu sistem repositori, yang dapat diakses publik. Sistem Repositori mempublikasikan informasi terkait sertifikat elektronik yang diterbitkan oleh BSrE, yaitu:

a. Sertifikat BSrE CA;
b. CRL*;*
c. CP/CPS SSL; dan
d. Dokumen kebijakan lainnya.

2.2 Publikasi Informasi Sertifikat Elektronik

Informasi terkait sertifikat elektronik yang diterbitkan oleh BSrE dapat diperoleh melalui website, dengan mengakses https://bsre.bssn.go.id/repository.

2.3 Periode Waktu Publikasi

Versi terbaru dari dokumen CP/CPS SSL BSrE CA tersedia dalam jangka waktu maksimum 7 hari sejak ditetapkan. BSrE CA mempublikasikan informasi CRL secara reguler dan terjadwal sebagaimana diatur dalam bagian 4.9.7.

2.4 Kendali Akses Pada Sistem Repositori

Informasi yang dipublikasikan pada repositori adalah informasi publik. Akses ke penyimpanan informasi di repositori bersifat *read-only* untuk publik. BSrE CA memberikan akses terbatas untuk pemutakhiran penyimpanan.

BAB III
IDENTIFIKASI DAN AUTENTIKASI

3.1 Penamaan

3.1.1 Tipe Nama

BSrE CA akan membuat dan menandatangani Sertifikat Elektronik dengan subyek nama yang berbeda / DN yang tidak boleh kosong dan memenuhi standar ITU X.500. Berikut tabel penjelasan DN BSrE CA dan DN pemilik sertifikat.

Tipe Sertifikat	*Distinguished Name*
Sertifikat CA	CN= BSrE CA SSL; O=Badan Siber dan Sandi Negara; C=ID
Sertifikat SSL	C=ID O={Nama Organisasi} CN={Nama Hostname} D={XXYYYYZZZZZZZZZZ_produk}
Sertifikat EV SSL	C=ID O={Nama Organisasi} CN={Nama Hostname} SERIALNUMBER={Nomor Akta Pendirian Instansi} BUSINESSCATEGORY={Private/Public} JURISDICTIONOFINCORPORATIONCOUNTRY=ID D={XXYYYYZZZZZZZZZZ_produk}

Catatan:

AMS ID = {XXYYYYZZZZZZZZZZ_produk}

XX = OID CA

Y = 4 Digit OID RA

Z = 10 Digit *random character* menggunakan *random generator*

3.1.2 Kebutuhan Nama yang Memiliki Arti

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

tersebut. Nama subjek yang digunakan dalam sertifikat elektronik merepresentasikan suatu pengenal yang tidak ambigu. Nama subjek yang digunakan memiliki arti agar dapat diidentifikasi bahwa sertifikat tersebut merepresentasikan subjek pemilik sertifikat elektronik.

3.1.3 Penggunaan Nama yang Anonim dan Pseudonimitas oleh Pemilik Sertifikat Elektronik

BSrE CA tidak menerbitkan sertifikat elektronik milik Pemilik Sertifikat Elektronik secara anonim atau pseudonim.

3.1.4 Aturan untuk Menginterpretasikan Jenis Penamaan Lainnya

DN dalam Sertifikat BSrE CA hanya mengacu pada ketentuan dalam standar ITU X.500.

3.1.5 Keunikan Nama

Semua DN adalah unik.

3.1.6 Penggunaan merk dagang dalam sertifikat elektronik

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. BSrE CA tidak perlu memverifikasi hak pemohon untuk penggunaan merek dagang. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih. BSrE CA dapat menolak permohonan atau melakukan pencabutan Sertifikat yang menjadi bagian dari konflik merek dagang.

3.2 Validasi Identitas

3.2.1 Metode untuk membuktikan kepemilikan Kunci Privat

Pasangan kunci dibangkitkan oleh pemilik. Metode yang digunakan untuk membuktikan kepemilikan kunci privat adalah PKCS #10 (CSR).

3.2.2 Autentikasi Identitas Organisasi

RA atau Verifikator harus melakukan pemeriksaan untuk setiap informasi identitas pemohon. Proses autentikasi identitas pemohon dapat dilakukan secara jarak jauh (*remote/online*) antara RA atau verifikator.

Pemohon wajib menyampaikan surat rekomendasi dari organisasi. Autentikasi identitas organisasi pemohon terdiri dari:

3.2.2.1 Identitas

RA akan memverifikasi identitas organisasi yang diajukan oleh pemohon. RA akan menetapkan apakah identitas, alamat, dan nama domain sesuai dengan informasi yang ada pada database pihak ketiga dan atau sumber terpercaya.

3.2.2.2 DBA/Tradename

Jika dalam informasi identitas termasuk juga DBA/Tradename, RA harus memverifikasi DBA/Tradename pemohon.

3.2.2.3 Verifikasi Negara

Verifikasi negara dilakukan pada tahap 3.2.2.1.

3.2.2.4 Validasi Otorisasi Domain

BSrE CA memvalidasi setiap FQDN menggunakan minimal satu cara/metode di bawah ini.

3.2.2.4.1 Validasi Kontak Domain

Tidak ada ketentuan.

3.2.2.4.2 Email, Fax, SMS dari Kontak Domain

Tidak ada ketentuan.

3.2.2.4.3 Nomor Telepon dari Kontak Domain

Tidak ada ketentuan.

3.2.2.4.4 Email ke Kontak Domain

Tidak ada ketentuan.

3.2.2.4.5 Dokumen Otorisasi Domain

Tidak ada ketentuan.

3.2.2.4.6 *Agreed-Upon Change to Website*

Tidak ada ketentuan.

3.2.2.4.7 Perubahan DNS

Tidak ada ketentuan.

3.2.2.4.8 Alamat IP

Mengonfirmasi kepemilikan Pemohon atas FQDN dengan memastikan bahwa pemohon memiliki Alamat IP yang berasal dari DNS Lookup, sesuai dengan ketentuan pada bagian 3.2.2.5.

Setelah FQDN divalidasi menggunakan metode ini, BSrE CA mungkin tidak menerbitkan Sertifikat untuk FQDN untuk tingkat domain di atasnya. Metode ini tidak

cocok untuk memvalidasi Nama Domain *Wildcard.*

3.2.2.4.9 *Test Certificate*

Tidak ada ketentuan.

3.2.2.4.10 TLS Menggunakan Nomor Acak

Tidak ada ketentuan.

3.2.2.4.11 *Any Other Method*

Tidak ada ketentuan.

3.2.2.4.12 *Validating Applicant as a Domain Contact*

Tidak ada ketentuan.

3.2.2.4.13 Email ke CAA DNS

Tidak ada ketentuan.

3.2.2.4.14 Email ke TXT DNS

Tidak ada ketentuan.

3.2.2.4.15 Kontak telepon ke Domain

Tidak ada ketentuan.

3.2.2.4.16 Kontak telepon TXT DNS Record

Tidak ada ketentuan.

3.2.2.4.17 Kontak telepon CAA DNS

Tidak ada ketentuan.

3.2.2.4.18 *Agreed-Upon Change to Website* V2

Mengkonfirmasi kepemilikan pemohon atas FQDN dengan memverifikasi bahwa pemohon dapat melakukan perubahan dengan menampilkan logo SSL BSrE pada halaman depan FQDN.

3.2.2.4.19 *Agreed Upon Change to Website* – ACME

Tidak ada ketentuan.

3.2.2.4.20 TLS Using ALPN

Tidak ada ketentuan.

3.2.2.5 Otentikasi dari Alamat IP

Bagian ini mendefinisikan proses dan prosedur untuk memvalidasi kepemilikan Pemohon atas Alamat IP yang tercantum dalam Sertifikat.

BSrE CA akan mengonfirmasi bahwa sebelum penerbitan, BSrE CA telah memvalidasi setiap Alamat IP yang tercantum dalam Sertifikat menggunakan setidaknya satu metode yang ditentukan di bagian ini.

3.2.2.5.1 *Agreed-Upon Change to Website*

Tidak ada ketentuan.

3.2.2.5.2 Email, Fax, SMS dari Kontak Domain

Tidak ada ketentuan.

3.2.2.5.3 *Lookup Reverse Address*

Mengkonfirmasi kepemilikan pemohon atas Alamat IP dengan mendapatkan nama domain yang terkait dengan alamat IP melalui *lookup reverse*-IP pada alamat IP

dan kemudian memverifikasi kepemilikan atas FQDN menggunakan metode pada bagian 3.2.2.4.

3.2.2.5.4 *Any Other Method*

Tidak ada ketentuan.

3.2.2.5.5 Nomor Telepon dari Kontak Domain

Tidak ada ketentuan.

3.2.2.5.6 Metode ACME “http-01” untuk Alamat IP

Tidak ada ketentuan.

3.2.2.5.7 Metode ACME “tls-alpn-01” untuk Alamat IP

Tidak ada ketentuan.

3.2.2.6 Validasi *Wildcard*

Memastikan FQDN memiliki tanda bintang berada di sebelah kiri dari nama domain, sebagai contoh *.bssn.go.id.

3.2.2.7 Akurasi Sumber Data

Sebelum menggunakan sumber data, RA harus mengevaluasi sumber data tersebut untuk realibilitas, akurasi dan ketahanan dari penambahan atau pemalsuan.

3.2.2.8 CAA Records

CAA records diatur ketentuannya pada poin 4.2.4.

3.2.2.9 Otentikasi Alamat Email

BSrE CA mengkonfirmasi kepemilikan pemohon atas alamat email menggunakan metode di bawah ini.

a. Mengirimkan URL termasuk nilai acak ke alamat email dan menerima link *acknowledgement,* kemudian masuk ke dalam URL tersebut.
b. Menggunakan proses validasi domain pada subbab 3.2.2.4 untuk menunjukkan kepemilikan atas FQDN. Ketika terverifikasi, RA dapat menyetujui penerbitan Sertifikat yang berisi alamat email untuk FQDN atau nama domain terkait.

3.2.2.10 Otentikasi *Registered Trademark*

Tidak ada ketentuan.

3.2.3 Autentikasi Identitas Individu

RA atau verifikator harus melakukan pemeriksaan untuk setiap informasi identitas individu yang mengajukan permohonan sertifikat elektronik. Proses autentikasi identitas individu dapat dilakukan secara jarak jauh (*remote/online*) antara RA atau verifikator dengan pemohon.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

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

3.2.5 Validasi Otoritas

Validasi otoritas melibatkan penentuan apakah seseorang memiliki hak khusus, hak, atau izin khusus, termasuk izin untuk bertindak atas nama organisasi untuk mendapatkan sertifikat.

Sertifikat yang mengandung afiliasi keorganisasian secara eksplisit atau implisit hanya dapat diterbitkan setelah memastikan bahwa Pemohon adalah benar memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan organisasinya.

3.2.6 Kriteria Inter Operasi

Kriteria interoperasi BSrE CA mengacu pada standar interoperabilitas yang diterbitkan oleh PSrE Induk.

3.3 Identifikasi dan Autentikasi untuk Permintaan Re-key Sertifikat Elektronik

Re-key Pemilik diperkenankan untuk mengajukan permohonan rekey sebelum sertifikat kedaluwarsa sesuai poin 4.7. BSrE CA dapat melakukan validasi ulang terhadap Pemohon sesuai poin 3.2.

3.3.1 Identifikasi dan Autentikasi untuk Re-Key Rutin

Sebelum masa berlaku Sertifikat berakhir, Pemilik dapat meminta penggantian kunci yang selanjutnya disebut re-key dan Pemilik harus diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau menggunakan proses pemeriksaan identitas awal sebagaimana diatur pada poin 3.2.

3.3.2 Identifikasi dan autentikasi untuk Re-Key setelah pencabutan

Jika suatu sertifikat elektronik telah dicabut, maka tidak dapat dilakukan pembaruan sertifikat elektronik. Pemilik Sertifikat Elektronik harus melakukan permohonan penerbitan ulang berdasarkan ketentuan BSrE CA.

3.3.3 Identifikasi dan Autentikasi untuk Permohonan Pencabutan Sertifikat Elektronik

RA harus melakukan identifikasi dan autentikasi permohonan dengan memeriksa hal-hal sebagai berikut:

a. Identitas pemilik sertifikat elektronik;
b. Tipe, nomor seri, dan informasi pada sertifikat elektronik; dan
c. Alasan pengajuan permohonan pencabutan. Apabila alasan pencabutan terjadi paling tidak satu dari kondisi-kondisi pada poin 4.7.1.

Proses pencabutan sertifikat elektronik dapat dilakukan secara tatap muka dengan RA atau secara jarak jauh (*remote/online*).

BAB IV
PERSYARATAN OPERASIONAL SIKLUS HIDUP SERTIFIKAT ELEKTRONIK

4.1 Permohonan Sertifikat Elektronik

4.1.1 Siapa yang Dapat Mengajukan Permohonan Sertifikat

BSrE menerbitkan sertifikat bagi pemohon warga negara Indonesia yang merupakan pegawai Instansi dan/atau Instansi. Pihak yang berhak mengajukan permohonan sertifikat elektronik adalah Individu yang mewakili sistem elektronik/aplikasi.

4.1.2 Proses Pendaftaran dan Tanggung Jawab

Seluruh proses komunikasi yang dilakukan pada proses pendaftaran dapat diautentikasi dan terlindungi dari ancaman-ancaman yang terkait modifikasi informasi secara tidak sah. Data yang dikomunikasikan terkait dengan informasi pribadi dilindungi baik yang melalui komunikasi elektronik maupun komunikasi non elektronik. Jika menggunakan komunikasi elektronik, maka digunakan mekanisme kriptografi dengan kekuatan pasangan Kunci Publik/Privat yang sepadan. Namun jika komunikasi menggunakan media non elektronik, tetap harus melindungi kerahasiaan dan keutuhan data.

Proses pendaftaran meliputi langkah-langkah sebagai berikut:

a. Pemohon atau calon pemilik sertifikat elektronik harus melengkapi berkas pendaftaran dan dokumen lain yang dibutuhkan, serta memberikan informasi yang akurat untuk melakukan pendaftaran sertifikat elektronik; dan
b. Pembuatan CSR menggunakan aplikasi pembuat file CSR dari BSrE CA.

4.2 Proses Permohonan Sertifikat Elektronik

4.2.1 Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi

Proses identifikasi dan autentikasi pemohon sertifikat elektronik dilakukan sesuai dengan ketentuan pada poin III.2 dan III.3.

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat Elektronik

RA atau BSrE memiliki wewenang untuk menyetujui atau menolak permohonan sertifikat elektronik. Apabila hasil proses identifikasi dan autentikasi dinyatakan sah, maka permohonan sertifikat elektronik harus disetujui dan diproses sesuai ketentuan. Namun apabila hasil proses identifikasi dan autentikasi dinyatakan tidak sah, maka permohonan sertifikat elektronik harus ditolak. Penolakan permohonan sertifikat elektronik dapat dilakukan karena sebab-sebab sebagai berikut:

a. Informasi dalam permohonan sertifikat elektronik tidak dapat diidentifikasi atau tidak autentik;
b. Pemohon sertifikat elektronik tidak melengkapi dokumen-dokumen sesuai dengan ketentuan;
c. Pemohon sertifikat elektronik tidak melakukan respon atas suatu pemberitahuan dari BSrE dalam jangka waktu tertentu; dan
d. Hal-hal lain yang berpotensi dapat merugikan pihak BSrE.

4.2.3 Waktu Proses Permohonan Sertifikat Elektronik

Tidak ada ketentuan batas waktu bagi Pemohon untuk melakukan permohonan sertifikat elektronik. BSrE CA memproses permohonan dan menerbitkan sertifikat elektronik dalam jangka waktu maksimal 3 hari kerja sejak permohonan diterima oleh RA atau BSrE.

4.2.4 CAA Records

Sebelum menerbitkan Sertifikat SSL atau Sertifikat EV SSL, BSrE CA memeriksa CAA *Records* untuk setiap DNS Name pada ekstensi subjectAltName dari Sertifikat SSL atau Sertifikat EV SSL, sesuai dengan RFC 8659.

Jika di dalam CAA *record* belum terdapat BSrE CA, maka sebelum Sertifikat SSL dan EV SSL diterbitkan, pemohon harus menambahkan BSrE CA pada CAA record.

Jika di dalam CAA *record* pemohon tidak menambahkan BSrE CA, dan Sertifikat SSL pada FQDN sudah terdaftar di CA lain, maka permohonan penerbitan Sertifikat SSL dan EV SSL akan ditolak.

4.3 Penerbitan Sertifikat Elektronik

4.3.1 Tindakan BSrE CA Selama Penerbitan Sertifikat

BSrE CA memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan semua field dan ekstensi telah diisi dengan benar.

BSrE CA mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membuat Sertifikat Pemohon. BSrE CA mempublikasikan Sertifikatnya ke suatu repositori sesuai dengan CP/CPS SSL terkait.

4.3.2 Pemberitahuan ke Pemilik oleh BSrE CA tentang Diterbitkannya Sertifikat

BSrE CA menginformasikan Pemilik dalam maksimum 5 (lima) hari kerja tentang berhasilnya penerbitan sertifikat melalui email.

4.4 Penerimaan Sertifikat

4.4.1 Sikap yang Dianggap Menerima Sertifikat

BSrE CA mendapatkan informasi bahwa sertifikat elektronik berhasil diterbitkan

Ketika tidak ada keluhan dari Pemilik dalam jangka waktu 7 (tujuh) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat.

4.4.2 Publikasi Sertifikat Elektronik oleh BSrE CA

Sebagaimana ditentukan pada poin 2.1, sertifikat elektronik milik BSrE CA dipublikasikan dalam sistem repositori yang dikelola BSrE CA.

Sertifikat elektronik yang diterbitkan oleh BSrE CA dipublikasikan sesuai dengan poin 2.2.

4.4.3 Pemberitahuan Penerbitan Sertifikat Elektronik oleh BSrE CA Kepada Entitas Lain

Tidak ada ketentuan.

4.5 Penggunaan Pasangan Kunci dan Sertifikat

4.5.1 Penggunaan Kunci Privat dan Sertifikat oleh Pemilik

Penggunaan kunci privat mengacu pada poin 9.6.3.

4.5.2 Penggunaan Kunci Publik dan Sertifikat Elektronik oleh Pengandal

Pengandal memvalidasi sertifikat elektronik yang sesuai dengan X.509 dan menggunakan aplikasi yang sudah ditentukan oleh BSrE CA serta PSrE Induk. BSrE CA menentukan penggunaan dan mekanisme keabsahan sertifikat elektronik (CRL dan OCSP) melalui ekstensi sertifikat elektronik yang diterbitkan oleh BSrE CA.

4.6 Pembaruan Sertifikat Elektronik

4.6.1 Kondisi Pembaruan Sertifikat Elektronik

Tidak ada ketentuan.

4.6.2 Pihak yang Dapat Mengajukan Pembaruan Sertifikat Elektronik

Tidak ada ketentuan.

4.6.3 Proses Permohonan Pembaruan Sertifikat Elektronik

Tidak ada ketentuan.

4.6.4 Pemberitahuan kepada Pemilik Sertifikat Elektronik

Tidak ada ketentuan.

4.6.5 Aturan Penerimaan Sertifikat Elektronik Setelah Pembaruan Sertifikat Elektronik

Tidak ada ketentuan.

4.6.6 Publikasi Setelah Pembaruan Sertifikat Elektronik oleh BSrE CA

Tidak ada ketentuan.

4.6.7 Pemberitahuan Pembaruan Sertifikat Elektronik Milik BSrE CA Kepada Pihak Lain

Tidak ada ketentuan.

4.7 Re-Key Sertifikat

Re-key merupakan pembuatan/penerbitan sertifikat baru dengan kunci publik, *serial number*, dan *key identifier* yang baru, sementara informasi lain terkait pemilik dalam sertifikat baru masih sama dengan sertifikat lama. Sertifikat baru dapat diisi masa berlaku yang baru, diisi

dengan tempat publikasi CRL yang baru, dan.atau ditandatangani dengan kunci yang baru.

4.7.1 Kondisi untuk Re-Key Sertifikat

BSrE CA melakukan re-key bagi pemilik sertifikat selama:

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

Apabila kunci privat pemilik terkompromi atau sertifikat kadaluarsa, pemilik dapat mengajukan permohonan baru sebagaimana diatur pada poin 4.1.

4.7.2 Pihak yang Dapat Meminta Sertifikasi dari Sebuah Kunci Publik yang Baru

Pemilik Sertifikat Elektronik atau perwakilan instansi, RA, dan BSrE CA dapat mengajukan pembaruan sertifikat elektronik jika dalam waktu 30 hari ke depan masa berlaku sertifikat elektroniknya akan habis.

4.7.3 Pemrosesan Permintaan Re-Key Sertifikat

Saat memproses permohonan penerbitan sertifikat elektronik melalui *re-key*, tanda tangan elektronik dari pihak yang mengajukan permohonan harus diperiksa keabsahannya sebelum permohonan penerbitan sertifikat elektronik tersebut diproses (sesuai poin 4.3).

Pembaruan sertifikat elektronik dimana masa berlaku sertifikat elektronik tersebut telah habis atau telah dicabut, maka Pemilik

Sertifikat Elektronik tersebut harus mengajukan permohonan sertifikat elektronik baru.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Setelah *re-key* Sertifikat berhasil dilakukan, maka BSrE CA akan memberitahukan Pemohon Sertifikat bahwa penerbitan Sertifikat telah berhasil dilakukan melalui media komunikasi yang ditentukan BSrE CA, selambatnya dalam jangka waktu 5 (lima) hari kerja.

4.7.5 Sikap yang dianggap sebagai Penerimaan Sertifikat *Re-key*

Pemililk Sertifikat dianggap telah menerima Sertifikat hasil *rekey* ketika pemberitahuan sebagaimana ditentukan pada poin 4.4.1 telah diterima oleh Pemilik Sertifikat.

4.7.6 Publikasi Sertifikat Re-key oleh BSrE CA

BSrE CA tidak melakukan publikasi sertifikat pemilik hasil re-key.

4.7.7 Pemberitahuan Sertifikat Re-key oleh BSrE CA

Tidak ada ketentuan.

4.8 Modifikasi Sertifikat

BSrE CA tidak mengizinkan modifikasi detil sertifikat. Apabila terjadi kesalahan dalam penerbitan Sertifikat, maka BSrE CA akan melakukan pencabutan Sertifikat dan menerbitkan Sertifikat baru yang sesuai dengan ketentuan yang diatur pada CP/CPS SSL ini.

4.8.1 Keadaan yang Menyebabkan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.2 Pihak yang Dapat Mengajukan Permohonan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3 Pemrosesan Permohonan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4 Pemberitahuan Sertifikat Baru ke Pemilik Sertifikat

Tidak ada ketentuan.

4.8.5 Sikap yang dianggap sebagai Penerimaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.6 Publikasi Sertifikat yang Dimodifikasi oleh BSrE CA

Tidak ada ketentuan.

4.8.7 Pemberitahuan Penerbitan Sertifikat oleh BSrE CA ke Pihak Lain

Tidak ada ketentuan.

4.9 Pencabutan Sertifikat Elektronik

4.9.1 Kondisi Pencabutan Sertifikat Elektronik

BSrE CA melakukan pencabutan sertifikat elektronik jika terjadi paling tidak satu dari kondisi-kondisi berikut:

a. Pemilik Sertifikat Elektronik meminta secara tertulis agar BSrE CA mencabut sertifikat.
b. Pemilik Sertifikat Elektronik memiliki pernyataan tertulis dan bukti-bukti bahwa secara sengaja atau tidak sengaja Kunci Privat miliknya telah hilang, telah dicuri, telah diketahui, atau telah disalahgunakan oleh pihak lain;
c. Pemilik Sertifikat Elektronik masih memiliki sertifikat elektronik dan kunci privat yang berelasi namun tidak

mengingat/lupa *passphrase* untuk mengakses sertifikat elektronik miliknya;

d. Sertifikat elektronik berisi informasi yang tidak sah dengan menyertakan bukti-bukti bahwa informasi tersebut merupakan informasi yang tidak sah;
e. Terdapat perubahan data identitas pada sertifikat elektronik yang berkaitan dengan data identitas pemilik sertifikat elektronik;
f. Pemilik Sertifikat Elektronik atau organisasi pemilik sertifikat elektronik tidak mematuhi CP BSrE CA dan/atau CPS BSrE CA dan/atau *subscriber agreement* dan/atau ketentuan yang ada dalam Perjanjian Kerja Sama;
g. Pemilik Sertifikat Elektronik atau organisasi pemilik sertifikat elektronik mengajukan permintaan kepada BSrE CA agar sertifikat elektronik miliknya/personilnya dibatalkan/dicabut untuk suatu alasan yang dapat dipertanggung jawabkan;
h. BSrE CA telah berhenti beroperasi;
i. BSrE CA mengetahui keadaan yang menunjukkan bahwa penggunaan Nama Domain atau alamat IP tidak diizinkan secara hukum (misalnya pengadilan atau arbiter telah mencabut hak Pendaftaran Nama Domain, perjanjian lisensi atau layanan Nama Domain telah berakhir, atau Pendaftar Nama Domain gagal memperpanjang Nama Domain); dan
j. BSrE CA diberitahu bahwa Sertifikat *Wildcard* telah digunakan untuk mengautentikasi Nama Domain yang sepenuhnya memenuhi syarat berinduk yang menyesatkan secara curang.

4.9.2 Pihak yang Dapat Meminta Pencabutan

Permintaan pencabutan sertifikat dapat dilakukan oleh:

a. Pemilik; dan

b. Pihak berwenang lainnya (sebagaimana didefinisikan dalam CP/CPS SSL).

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

4.9.3 Proses permintaan pencabutan sertifikat elektronik

BSrE CA memverifikasi identitas individu dan organisasi yang meminta pencabutan. Validasi identitas sesuai dengan poin 3.4. Permintaan pencabutan oleh entitas lain harus ada penyampaian bukti bahwa,

a. Kunci privat sertifikat telah terungkap;
b. Penggunaan sertifikat tersebut tidak sesuai dengan CP/CPS SSL; dan
c. Terdapat alasan relevan lain yang diberikan oleh pemilik.

Permintaan pencabutan sertifikat oleh pihak yang berwenang lainnya harus menyerahkan bukti bahwa:

1) Kunci Privat Sertifikat telah terungkap;
2) Penggunaan Sertifikat tidak sesuai dengan CP/CPS SSL, Perjanjian Pemilik/Kontrak Berlangganan, dan perjanjian lainnya; atau
3) Pemilik sudah tidak terasosiasi dengan institusi yang bersangkutan.

Proses permintaan pencabutan Sertifikat dijelaskan lebih rinci dalam CP, CPS, dan prosedur.

4.9.4 Masa Tenggang Permintaan Pencabutan Sertifikat Elektronik

BSrE CA tidak mengatur tenggang waktu untuk permintaan pencabutan Sertifikat yang diajukan oleh Pemilik Sertifikat atau pihak ketiga lainnya.

4.9.5 Jangka Waktu BSrE CA Memproses Permintaan Pencabutan

BSrE CA atau RA melakukan identifikasi dan autentikasi pemohonan pencabutan sertifikat elektronik selambat-lambatnya dalam waktu 3 (tiga) hari kerja setelah permohonan pencabutan sertifikat elektronik tersebut diajukan oleh pemohon.

4.9.6 Pemeriksaan Keberlakukan Sertifikat Elektronik oleh Pengandal

Jika Pengandal sertifikat elektronik tidak dapat memeriksa status keberlakukan suatu sertifikat elektronik menggunakan CRL terbaru dan/atau server OCSP, maka Pengandal tersebut harus menolak dan tidak melanjutkan penggunaan sertifikat elektronik.

4.9.7 Frekuensi Penerbitan CRL

CRL harus diperbarui dan dipublikasikan:

a. Untuk sertifikat Pemilik Sertifikat Elektronik, minimal sekali dalam 24 jam.
b. Dalam kasus kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat BSrE CA, maka CRL terbaru dipublikasi dalam waktu maksimal 24 jam semenjak stempel waktu (timestamp) pencabutan.

Untuk pencabutan Sertifikat Pemilik, waktu nextUpdate pada CRL BSrE CA paling lambat 48 (empat puluh delapan) jam setelah waktu penerbitan (*this Update time*). BSrE CA menjamin integritas CRL.

4.9.8 Latensi Maksimum CRL (bila berlaku)

BSrE CA mempublikasikan CRL dalam waktu 30 (tiga puluh) menit setelah penerbitan dan dapat diunduh dalam waktu 3 (tiga) detik. BSrE CA tidak menghapus entri pencabutan dalam CRL atau respons OCSP sampai setelah Tanggal Kedaluwarsa Sertifikat yang dicabut.

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status Daring

BSrE CA menyediakan layanan validasi daring menggunakan protokol OCSP yang memberikan waktu respons 10 detik atau kurang dalam kondisi operasi normal dengan menggunakan metode GET.

4.9.10 Persyaratan Pemeriksaan Pencabutan Daring

BSrE CA mengimplementasikan OCSP sesuai dengan standar IETF RFC 6960. Pembaruan informasi OCSP dilakukan setiap empat hari dan respon OCSP memiliki kadaluarsa selama 10 hari.

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus Re-key apabila *compromise*

Jika Kunci Privat BSrE CA terkompromi, maka seluruh sertifikat elektronik yang telah diterbitkan oleh BSrE CA dicabut.

4.9.13 Keadaan untuk Pembekuan

Tidak ada ketentuan.

4.9.14 Siapa yang Dapat Meminta Pembekuan

Tidak ada ketentuan

4.9.15 Prosedur Permintaan Pembekuan

Tidak ada ketentuan

4.9.16 Batas Waktu Pembekuan

Tidak ada ketentuan

4.10 Layanan Status Sertifikat

4.10.1 Karakteristik Operasional

Status keberlakuan sertifikat elektronik dapat diketahui berdasarkan informasi pada CRL dan/atau melalui OCSP.

4.10.2 Ketersediaan Layanan

BSrE CA melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status sertifikat.

4.10.3 Fitur Pilihan

Tidak ada ketentuan.

4.11 Akhir Berlangganan

Kepemilikan sertifikat elektronik oleh Pemilik Sertifikat Elektronik berakhir jika masa berlaku sertifikat elektronik tersebut telah habis atau jika sertifikat elektronik tersebut telah dicabut.

Pemilik dapat mengakhiri langganan dengan membiarkan sertifikatnya kadaluwarsa atau mencabut sertifikatnya tanpa meminta sertifikat yang baru.

4.12 Pemulihan dan Eskro Kunci

4.12.1 Kebijakan dan Praktik Eskro Kunci dan Pemulihan

a. BSrE CA tidak menitipkan kunci privat kepada pihak lain.

b. Kunci privat sertifikat pemilik tidak dititipkan kepada BSrE CA

4.12.2 Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ada ketentuan.

BAB V
FASILITAS, PENGELOLAAN DAN KENDALI OPERASIONAL

5.1 Kendali Fisik

5.1.1 Lokasi dan Konstruksi

Lokasi dan konstruksi bangunan yang menyimpan perangkat-perangkat sistem BSrE CA, berikut dengan perangkat-perangkat komputer untuk manajemen/ pengelolaan BSrE CA secara jarak jauh (*remote*), harus memenuhi kriteria sebagai tempat yang menyimpan informasi yang bernilai tinggi dan/atau informasi yang sangat sensitif. BSrE CA memastikan adanya perlindungan yang kuat terhadap upaya-upaya akses secara tidak sah pada setiap perangkat sistem BSrE CA dan informasi yang tersimpan di dalamnya (misal, menerapkan mekanisme penjagaan fisik, sensor untuk mendeteksi upaya penyusupan, dsb).

5.1.2 Akses fisik

Peralatan BSrE CA selalu terlindungi dari akses yang tidak resmi. Mekanisme keamanan fisik untuk BSrE CA telah diimplementasikan untuk:

a. Memastikan tidak ada akses tidak resmi ke perangkat keras
b. Menyimpan semua removable media yang berisi informasi teks yang sensitif dalam tempat penyimpanan yang aman.
c. Memonitor akses yang tidak berwenang baik secara manual maupun elektronik.
d. Memelihara dan memeriksa log akses secara berkala.

Semua operasional BSrE yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan setidaknya memiliki empat lapis keamanan 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 BSrE yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

5.1.3 Listrik dan AC

Fasilitas perangkat sistem BSrE CA dilengkapi perangkat pendukung yaitu pembangkit listrik yang menjamin ketersediaan listrik dan sistem pendingin udara yang mengontrol suhu dan kelembaban.

BSrE CA memiliki cadangan listrik yang cukup agar dapat menyelesaikan aktivitas proses sertifikasi elektronik, mencatat keadaan/status terakhir dari perangkat-perangkat yang aktif, sebelum terjadinya pemutusan daya listrik yang menyebabkan sistem non-aktif/mati. Komponen perangkat sistem BSrE CA yang kritikal (misal: *Certificate Validation System*) dilengkapi dengan sumber daya listrik yang tidak terganggu dan dapat beroperasi minimal selama 6 (enam) jam tanpa adanya sumber listrik utama agar layanan kritikal dapat selalu tersedia.

5.1.4 Keterpaparan Air

BSrE CA menempatkan perangkat sistem pada tempat yang tidak terpapar air.

5.1.5 Pencegahan dan Perlindungan Kebakaran

BSrE CA menempatkan perangkat sistem di fasilitas dengan sistem deteksi kebakaran dan sistem pemadaman kebakaran yang memadai.

5.1.6 Media Penyimpanan

Media penyimpanan yang digunakan oleh BSrE CA terlindungi dari kerusakan akibat kecelakaan (misal: air, api, elektromagnetik, dsb). Media penyimpanan yang tidak berkaitan secara langsung dengan proses sertifikasi elektronik (misal:

rekaman untuk audit, arsip, atau informasi cadangan) tersimpan pada lokasi yang terpisah dari lokasi utama.

Media penyimpanan yang berisi Kunci Privat milik BSrE CA dikelola dan disimpan dalam fasilitas penyimpanan yang aman dan dilengkapi kendali akses baik fisik maupun logik untuk membatasi akses terhadap personil yang tidak berwenang.

5.1.7 Pembuangan Limbah

BSrE CA memastikan setiap dokumen dan material yang bersifat sensitif dihancurkan sebelum dibuang. Media yang digunakan untuk mengumpulkan dan membawa informasi sensitif diubah sampai informasi tersebut tidak dapat dibaca sebelum dibuang. Sebelum dibuang, materiil dan peralatan kriptografi dihancurkan secara fisik atau di-*zeroized* (dikosongkan). Limbah selain yang disebutkan diatas, dibuang sesuai dengan persyaratan pembuangan limbah normal.

5.1.8 Backup Off-Site

BSrE CA secara rutin membuat informasi cadangan (*backup*) dari setiap sistem, informasi/catatan audit, dan informasi lain yang bersifat sensitif. Media *offsite backup* disimpan dalam fasilitas penyimpanan yang aman secara fisik. BSrE CA dapat melakukan pemulihan dari kejadian kegagalan sistem.

Data backup dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional BSrE CA.

5.2 Kendali Prosedur

5.2.1 Peran yang Dipercaya

BSrE CA memiliki daftar dan catatan tentang personil yang bertugas sebagai Peran Terpercaya, yang mencakup nama, informasi kontak, dan informasi lainnya yang diperlukan.

Peran terpercaya BSrE CA meliputi:

a. PA

   Pembuatan, revisi dan persetujuan CP/CPS SSL

b. Staff PA

   Membantu PA dalam menyiapkan dokumen CP/CPS SSL

c. Ketua Tim Operasional BSrE

   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan BSrE CA

d. Administrator Aplikasi CA

   Melakukan operasional dan maintenance aplikasi manajemen BSrE CA

e. DevOps *Engineer*

   Melakukan operasional dan maintenance terkait DevOps di BSrE

f. Administrator HSM

   Melakukan Operasional dan maintenance HSM BSrE CA.

g. *Network Engineer*

   Melakukan operasional dan maintenance jaringan sistem sertifikasi elektronik

h. RA

   Identifikasi dan Validasi identitas permohonan permintaan sertifikat

i. Staff RA

   Membantu RA dalam menyiapkan dokumen identifikasi dan validasi identitas

j. Developer

   Bertanggung jawab dalam mengembangkan aplikasi dan melakukan integrasi terkait dengan sistem PSrE

k. Repository

   Bertanggung jawab terhadap konten yang dipublikasikan pada repositori

l. *Key Custodian*

Mengelola penyimpanan dan pengamanan kunci

m. Internal Audit

Melakukan audit internal operasional BSrE CA

Penjelasan lebih detil dapat dilihat pada dokumen *trusted role*.

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 dua orang atau lebih:

a. Pembangkitan kunci BSrE CA
b. Pencabutan Sertifikat BSrE CA
c. Penandatanganan kunci BSrE CA
d. Pencadangan kunci privat BSrE CA

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran

Semua individu yang ditugaskan dalam Peran Terpercaya akan menerima Surat Perintah.

5.2.4 Peran yang Memerlukan Pemisahan Tugas

BSrE CA menerapkan pemisahan tugas baik berdasarkan perangkat BSrE CA, secara prosedural, maupun keduanya. Satu orang tidak boleh merangkap peran pada peran-peran berikut:

a. PA dan administrator operasional;
b. Auditor internal dan semua peran lain; dan
c. Pengembang aplikasi dan semua peran lain.

5.3 Kontrol Personil

5.3.1 Persyaratan Kualifikasi, Pengalaman dan Perizinan

Personil yang bertugas sebagai Peran Terpercaya adalah pegawai BSrE CA yang memiliki latar belakang, kualifikasi serta pengalaman dalam bidang keamanan informasi.

5.3.2 Prosedur Pemeriksaan Latar Belakang

Semua personil di BSrE CA telah menyelesaikan pemeriksaan latar belakang sesuai dengan aturan kepegawaian di lingkungan pemerintah.

5.3.3 Persyaratan Pelatihan

BSrE CA menjamin bahwa seluruh personil telah mendapatkan pelatihan yang dibutuhkan. Pelatihan tersebut meliputi 3 (tiga) hal yaitu: keamanan informasi, teknis operasional dan teknis prosedural. Pelatihan tersebut harus mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras, perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil PSrE harus dilakukan minimal 1 (satu) kali dalam setahun.

5.3.4 Frekuensi Pelatihan Ulang dan Persyaratannya

Personil yang bertugas sebagai Peran Terpercaya dalam BSrE CA akan selalu mendapatkan informasi terbaru tentang operasional BSrE CA. Setiap perubahan siginifikan terhadap operasional akan diikuti oleh program pelatihan yang terkait serta didokumentasikan dengan baik. BSrE akan mengevaluasi dan memperbaharui program pelatihannya minimal 1 (satu) tahun sekali.

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan

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

5.3.6 Sanksi untuk Aksi Legal di luar Kewenangan

BSrE CA akan mengambil tindakan tegas dan sanksi yang jelas berupa hukuman administratif dan disiplin bagi personil yang melakukan aksi melanggar ketentuan dan kebijakan didalam CP, CPS atau Prosedur operasional BSrE CA.

5.3.7 Persyaratan Kontraktor Independen

Apabila terdapat penyedia pihak ketiga/kontraktor yang terlibat dalam fungsi BSrE CA akan dikenakan aturan yang sama dengan personil BSSN sesuai 5.3.2.

5.3.8 Dokumentasi yang Disediakan untuk Personil

BSrE CA menjamin ketersediaan dokumen CP, CPS dan dokumen lain yang terkait dengan penyelenggaraan BSrE CA bagi personil- personilnya yang terlibat dalam operasional BSrE CA.

5.4 Prosedur Pencatatan untuk Audit

BSrE CA membuat berkas *log audit* untuk semua kejadian yang terkait dengan keamanan BSrE CA, VA, dan RA. 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, elektronik dan non elektronik, disimpan dan tersedia selama audit kepatuhan. *Log audit* keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai dengan poin 5.5.2.

5.4.1 Jenis kegiatan yang dicatat

BSrE CA mengaktifkan semua fitur audit keamanan dari sistem operasi BSrE CA dan RA, serta aplikasi BSrE CA, VA, dan RA yang dipersyaratkan oleh CPS ini. BSrE CA memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan *trusted role* dalam operasional BSrE CA 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 rekaman,
d. Sumber perekaman,
e. Indikator sukses atau gagal yang sesuai,
f. Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut

5.4.2 Frekuensi pemrosesan *audit log*

BSrE CA memastikan bahwa *audit log* diperiksa minimal 1 (satu) kali setiap bulan. BSrE CA menindaklanjuti setiap aktivitas yang mencurigakan atau tidak biasa berdasarkan insiden dalam sistem BSrE CA.

5.4.3 Masa retensi untuk *audit log*

BSrE CA menyimpan seluruh *audit log* dari sistem BSrE CA yang dihasilkan secara elektronik maupun yang dibuat manual untuk jangka waktu tidak kurang dari 12 (dua belas) bulan sejak *audit log* tersebut dibuat.

5.4.4 Perlindungan terhadap audit log

BSrE CA melindungi dengan sistem *audit log* elektronik dari pihak-pihak yang tidak berhak melihat, memodifikasi, menghapus atau gangguan lainnya.

5.4.5 Prosedur pembuatan audit log cadangan (*backup*)

BSrE CA mem-backup seluruh *log* sedikitnya sebulan sekali. Media backup disimpan dan diamankan di tempat terpisah.

5.4.6 Sistem pengumpulan audit (internal dan eksternal)

Sistem pengumpulan log audit dilakukan sejak sistem berjalan dan dimonitor secara internal BSrE CA.

5.4.7 Notifikasi kepada subjek penyebab kejadian

Tidak ditentukan.

5.4.8 Penilaian kerentanan

BSrE CA melakukan penilaian kerentanan (*vulnerability assessment*) secara rutin terhadap kendali keamanan yang telah dibuat oleh BSrE CA minimal 1 (satu) kali dalam 6 (enam) bulan.

5.5 Pengarsipan catatan

5.5.1 Jenis catatan yang diarsipkan

BSrE CA mengimplementasikan metode pencadangan untuk operasional BSrE CA yang terletak di Pusat Data. Minimal, data berikut harus disimpan pada arsip:

a. Siklus hidup sertifikat termasuk di dalamnya permohonan penerbitan, pembaruan, re-key, serta pencabutan sertifikat;
b. Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh BSrE CA;

c. Data konfigurasi sistem BSrE CA;
d. Dokumen CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.

5.5.2 Masa retensi untuk arsip

BSrE CA menyimpan catatan arsip mengenai kepemilikan sertifikat elektronik selama minimal 5 (lima) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.

5.5.3 Perlindungan terhadap dokumen arsip

BSrE CA melindungi dokumen arsip sehingga hanya pihak yang berwenang yang dapat memperoleh akses terhadap arsip tersebut. Setiap dokumen arsip dilindungi dari upaya pembacaan, pengubahan, atau penghapusan secara tidak sah dan upaya perusakan lainnya. Media penyimpanan dokumen arsip dan aplikasi yang diperlukan untuk memproses dokumen arsip harus dikelola untuk memastikan bahwa dokumen arsip tersebut dapat diakses selama masa retensi arsip yang telah ditentukan.

5.5.4 Prosedur pembuatan dokumen arsip cadangan

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

5.5.5 Penggunaan time-stamp pada setiap catatan (log)

Rekaman arsip BSrE CA diberi stempel waktu (timestamp) ketika mereka dibuat.

5.5.6 Sistem pengumpulan arsip

Sistem pengumpul arsip BSrE CA merupakan sistem internal, kecuali arsip RA yang berada diluar BSrE.

5.5.7 Prosedur untuk mendapatkan dan memeriksa informasi arsip

Penyimpanan media untuk informasi arsip BSrE CA diperiksa saat pembuatan. Secara berkala, sampel informasi yang diarsipkan diuji untuk memeriksa integritas dan keterbacaan informasinya.

Hanya pihak atau personil yang memiliki kewenangan yang dapat memperoleh akses ke suatu arsip. Integritas (keutuhan) informasi harus diperiksa kembali setelah arsip tersebut dikembalikan oleh personil yang telah mengakses dokumen arsip tersebut. Permintaan untuk mendapatkan dan memverifikasi informasi arsip dikoordinasikan oleh Ketua Tim.

5.6 Pergantian kunci

Untuk meminimalisir risiko terhadap bocornya Kunci Privat BSrE CA, kunci privat diubah secara berkala. Kunci tersebut akan diganti dengan kunci baru yang harus digunakan untuk penandatangan Sertifikat. BSrE CA akan melakukan pemberitahuan kepada Pemilik Sertifikat dan Pengandal dalam hal terjadi penggantian kunci baru BSrE CA tersebut.

5.7 Pemulihan Bencana dan Kondisi Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

Jika BSrE CA mendeteksi adanya percobaan peretasan terhadap sistem BSrE CA, maka BSrE CA melakukan investigasi untuk menentukan sifat dan tingkat kerusakan. Jika Kunci Privat milik BSrE CA diduga bocor, maka prosedur pencabutan seluruh sertifikat elektronik harus dilakukan. Jika

prosedur pencabutan sertifikat elektronik tidak dilakukan, lingkup potensi kerusakan harus dinilai untuk menentukan apakah sertifikat perlu dibangun kembali, hanya beberapa sertifikat harus ditarik, dan/atau kunci sertifikat perlu dinyatakan telah bocor.

Informasi cadangan terkait BSrE CA tersimpan di luar lokasi penyimpanan utama dan tersedia saat terjadi keadaan membahayakan atau bencana. Informasi cadangan tersebut minimal meliputi data permohonan sertifikat elektronik, *audit log* dan pangkalan data yang mencatat seluruh sertifikat elektronik yang telah dikeluarkan BSrE. Kunci Privat cadangan milik BSrE CA disimpan dan dikelola sesuai dengan ketentuan yang berlaku sebagaimana Kunci Privat utama.

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

Ketika sumber daya komputer, perangkat lunak, dan/atau data rusak, BSrE CA melakukan hal berikut:

a. Memberitahu PA atau PSrE Induk sesegera mungkin.
b. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.
c. Mengoperasikan kembali BSrE CA, dengan memprioritaskan kemampuan untuk membangkitkan informasi status sertifikat sesuai jadwal penerbitan CRL.
d. Bila kunci penandatanganan BSrE CA rusak, operasional BSrE CA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci BSrE CA baru.

5.7.3 Prosedur Kunci Privat Entitas Terkompromi

Jika Kunci Privat dari BSrE CA terkompromi, maka BSrE CA:

a. Memberitahu PA dan PSrE Induk sesegera mungkin agar dapat melakukan pencabutan Sertifikat;
b. Memberitahu semua Pemilik; dan
c. Mencabut Sertifikat Pemilik yang terkait dengan Kunci Privat yang terkompromi tersebut.

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana

Untuk memelihara integritas layanan BSrE CA, diimplementasikan backup data dan prosedur-prosedur pemulihan. BSrE CA membuat sebuah Rencana Pemulihan Bencana (Disaster Recovery Plan/DRP). DRP ditinjau ulang dan diuji secara berkala (minimal setahun sekali) dan diperbaharui jika dibutuhkan. Fasilitas Disaster Recovery Center BSrE CA tersedia bila fasilitas utama berhenti beroperasi.

BSrE CA harus menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbaharui. Layanan harus kembali pulih dalam kurun waktu 24 jam bila ada bencana.

5.8 Penghentian CA atau RA

Bila ada keadaan yang menyebabkan diakhirinya layanan BSrE CA dengan persetujuan dari PA dan PSrE Induk, BSrE CA akan memberitahu RA, pemilik, dan semua pengandal. Rencana aksi adalah sebagai berikut:

a. BSrE CA memberitahu ke RA, pemilik, dan semua pengandal bahwa status operasional BSrE CA dihentikan;
b. BSrE CA menyediakan dukungan berkelanjutan operasional hingga semua sertifikat pemilik kadaluarsa;
c. BSrE CA melakukan pencabutan seluruh sertifikat pemilik;

d. Menyimpan informasi BSrE CA dan Pemilik selama periode pemberitahuan untuk tujuan pengalihan tanggung jawab mengikuti ketentuan yang akan diberlakukan;

BAB 6
KENDALI KEAMANAN TEKNIS

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan pasangan kunci

a. Pembangkitan pasangan kunci BSrE CA

Material kunci kriptografi yang digunakan oleh BSrE CA untuk menandatangani sertifikat elektronik, CRL atau informasi status sertifikat elektronik harus dihasilkan dalam modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 3, atau sertifikasi lain yang ditetapkan dalam peraturan BSSN.

b. Pembangkitan pasangan kunci Setifikat SSL dan Sertifikat EV SSL

BSrE CA tidak membangkitkan pasangan kunci pemilik dan tidak menerima permohonan sertifikat menggunakan pasangan kunci yang sebelumnya dibangkitkan oleh BSrE CA.

6.1.2 Pengiriman Kunci Privat ke Pemilik Sertifikat Elektronik

Tidak ada ketentuan.

6.1.3 Pengiriman Kunci Publik ke Penerbit Sertifikat

CSR dari Pemilik Sertifikat Elektronik disampaikan kepada BSrE CA dengan menggunakan protokol keamanan HTTPS. Kunci Publik dalam bentuk X. 509 dikirimkan BSrE CA kepada Pemilik Sertifikat Elektronik dengan menggunakan protokol keamanan HTTPS.

6.1.4 Pengiriman Kunci Publik BSrE CA ke Pengandal

BSrE CA memastikan bahwa Pengandal menerima dan menyimpan sertifikat elektronik milik BSrE CA dengan cara

yang dapat dipercaya, dengan mengunduh sertifikat elektronik milik BSrE CA dari repository sesuai 2.1 yang diamankan menggunakan SSL.

6.1.5 Ukuran Kunci

Sertifikat	Panjang Kunci	Encryption Algorithm	Digest Algorithm
BSrE CA	4096 bit	RSA	SHA-256
Pemilik – Sertifikat SSL dan EV SSL	2048 bit	RSA	SHA-256

Panjang kunci dan periode penggunaan kunci dilakukan reviu secara periodik setiap tahun sesuai dengan kebijakan PSrE Induk.

6.1.6 Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Pembangkitan pasangan kunci BSrE Perangkat kriptografi sesuai standar FIPS 140-2 level 3.

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

Kunci BSrE CA digunakan untuk penandatanganan sertifikat (keyCertSign) dan penandatanganan CRL (cRLSign). Secara lebih lengkap akan dijelaskan pada bagian ekstensi Key Usage.

6.2 Pengamanan Kunci Privat dan Kendali Teknis Modul Kriptografi

6.2.1 Standar dan Kendali Modul Kriptografi

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

6.2.2 Kendali Multi Personil (n dari m) Kunci Privat

Privat BSrE CA telah mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi

kriptografis yang sensitif. Suatu jumlah minimum dari Secret Shares (m) dari sejumlah total Secret Shares yang dibuat dan didistribusikan untuk dipakai di modul kriptografis tertentu (n) diperlukan untuk mengaktifkan sebuah Kunci Privat BSrE CA yang disimpan di dalam modul

Angka ambang yang diperlukan untuk pembuatan kunci adalah 2 dari 4 (dimana n=2 dan m=4), aktivasi kunci penandatanganan adalah 2 dari 4, dan backup serta pemulihan kunci privat adalah 2 dari 4.

6.2.3 Eskro Kunci Privat

Kunci Privat BSrE CA dan pemilik tidak dititipkan.

6.2.4 *Backup* Kunci Privat

Kunci privat BSrE CA di-*backup* di bawah kendali multi-pihak yang sama dengan kunci privat asli. Paling tidak satu salinan dari kunci privat harus disimpan *off-site.* Semua salinan kunci privat BSrE CA dilindungi dengan cara yang sama dengan aslinya.

6.2.5 Arsip Kunci Privat

Jika pasangan kunci milik BSrE CA telah habis masa berlakunya maka pasangan kunci tersebut diarsipkan untuk masa retensi paling minimal selama 5 (lima) tahun sejak masa berlaku Kunci Privat tersebut habis.

BSrE tidak mengarsipkan Kunci Privat milik Pemilik Sertifikat Elektronik dan RA.

6.2.6 Pemindahan Kunci Privat ke/dari Modul Kriptografi

Kunci Privat milik BSrE CA dihasilkan di dalam dan tetap berada dalam perangkat kriptografi yang sama. Pasangan Kunci Publik/Privat milik BSrE CA dibuat salinannya untuk

cadangan keamanan. Pemindahan kunci dari perangkat keras modul kriptografi utama dilakukan secara langsung ke perangkat keras modul kriptografi cadangan dengan menggunakan mekanisme yang aman. Pasangan kunci BSrE CA tidak boleh disimpan dalam perangkat lunak, baik sementara ataupun permanen untuk tujuan apapun.

Proses pemindahan Kunci Privat ke/dari modul kriptografi harus dalam kondisi terenkripsi.

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografi

Material kunci kriptografi (Kunci Privat) yang digunakan oleh BSrE CA untuk menandatangani sertifikat elektronik, CRL atau informasi status sertifikat elektronik disimpan dalam pengamanan modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 3 dalam bentuk terenkripsi dan terlindungi oleh kata sandi, atau sertifikasi lain yang ditetapkan dalam peraturan BSSN.

Material kunci privat pemilik disimpan dalam pengamanan modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 2.

6.2.8 Metode Aktivasi Kunci Privat

Metode aktivasi Kunci Privat milik BSrE CA dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak sesuai kendali yang tercantum dalam poin 5.2.2.

6.2.9 Metode penonaktifan kunci privat

Kunci Privat milik seluruh pihak yang terlibat dalam BSrE CA secara otomatis tidak aktif pada saat peralatan kriptografi penyimpan Kunci Privat dinon-aktifkan/dimatikan.

6.2.10 Metode penghancuran kunci privat

Apabila dibutuhkan, seluruh pihak yang terlibat dalam BSrE CA melakukan penghancuran Kunci Privat milik BSrE CA dengan memastikan bahwa Kunci Privat tersebut tidak akan dapat direkonstruksi kembali. BSrE CA menggunakan mekanisme *zeroization* pada peralatan kriptografi beserta tindakan-tindakan lain yang dibutuhkan untuk memastikan penghancuran dari Kunci Privat BSrE CA.

6.3 Aspek-Aspek Lain Dalam Pengaturan Pasangan Kunci

6.3.1 Pengarsipan Kunci Publik

Kunci Publik setiap pihak dalam BSrE CA diarsipkan sebagai bagian dari proses pengarsipan sertifikat elektronik.

6.3.2 Periode operasional sertifikat elektronik dan periode penggunaan pasangan kunci

Periode operasi pasangan kunci ditentukan oleh periode operasional sertifikat elektronik yang sesuai. Jangka waktu operasional maksimum kunci ditentukan selama sepuluh (10) tahun untuk BSrE CA. Sementara untuk kunci Pemilik memiliki periode 2 tahun.

6.4 Data Aktivasi

6.4.1 Pembuatan dan Instalasi Data Aktivasi

Pembangkitan dan penggunaan data pengaktifan untuk mengaktifkan Kunci Privat BSrE CA dilakukan melalui upacara kunci.

Data aktivasi harus dibuat secara otomatis oleh HSM yang sesuai dan dikirimkan ke shareholder, dimana *shareholder* tersebut haruslah orang yang memiliki Peran Terpercaya.

6.4.2 Aktivasi Perlindungan Data

Data aktivasi untuk perangkat HSM dilindungi seperti yang diuraikan pada bagian 6.2.2. BSrE CA menyimpan data aktivasi dalam bentuk smartcard dengan perlindungan kata sandi.

Data aktivasi Kunci Privat PSrE BSrE CA hanya dikuasakan kepada Trusted Roles yang telah ditentukan.

6.4.3 Aspek Lain dari Aktivasi Data

Tidak ada ketentuan.

6.5 Kendali Keamanan Komputer

6.5.1 Persyaratan teknis keamanan komputer tertentu

BSrE CA memastikan bahwa sistem yang menjaga perangkat lunak BSrE CA dan file data aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem BSrE CA telah dikonfigurasi dan diperkuat keamanannya menggunakan praktik terbaik (*best practices*).

Fungsi-fungsi keamanan komputer dapat diberikan oleh sistem operasi, atau melalui kombinasi sistem operasi, perangkat lunak, dan pengamanan fisik, mencakup namun tidak terbatas pada fungsi berikut:

a. Memerlukan login terautentikasi untuk akses logikal;
b. Menyediakan kontrol akses terbatas;
c. Menyediakan kapabilitas audit keamanan;
d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;
e. Menyediakan perlindungan mandiri untuk sistem operasi.

6.5.2 Penilaian keamanan komputer

Tidak ada ketentuan

6.6 Kendali Teknis Siklus Hidup

6.6.1 Kendali pengembangan sistem

Diatur dalam pedoman pengembangan aplikasi sistem BSrE CA.

6.6.2 Kendali pengelolaan keamanan

Konfigurasi sistem BSrE CA serta modifikasi dan *upgrade* wajib didokumentasikan dan dikendalikan. BSrE CA menggunakan perangkat lunak untuk mendeteksi perubahan konfigurasi sistem manajemen BSrE CA. BSrE CA memiliki prosedur dan personil yang bertanggung jawab melakukan monitoring dan pemeriksaan sistem secara rutin.

6.6.3 Siklus hidup kendali keamanan.

BSrE CA melakukan pengawasan terhadap skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak dan secara berkala mengevaluasi keefektifannya melalui audit.

6.7 Kontrol Keamanan Jaringan

BSrE CA melakukan tindakan keamanan jaringan yang sesuai untuk memastikan keamanan dari tindakan DoS dan serangan intrusi. Langkah langkah tersebut termasuk penggunaan firewall dan router. BSrE CA mematikan port dan layanan jaringan yang tidak digunakan.

6.8 *Time stamping*

BSrE CA memastikan akurasi dari tanggal dan jam yang digunakan dalam proses *Time-Stamping*. Jam server *online* BSrE CA disinkronkan menggunakan *Network Time Protocol*. Waktu yang didapat dari layanan waktu diatas akan digunakan untuk menentukan waktu pada saat:

a. Validitas waktu berlakunya sertifikat elektronik milik BSrE CA
b. Pencabutan sertifikat elektronik milik BSrE CA
c. Pembaruan CRL, dan
d. Penerbitan, pembaruan, dan pencabutan sertifikat elektronik Pemilik Sertifikat Elektronik.

Prosedur secara elektronik atau manual dapat digunakan untuk mempertahankan akurasi waktu pada sistem. Setiap perubahan dari jam sistem harus dapat diaudit.

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

BAB VII

PROFIL SERTIFIKAT ELEKTRONIK, *CERTIFICATE REVOCATION LIST, & ONLINE CERTIFICATE STATUS PROTOCOL*

7.1 Profil Sertifikat Elektronik

Sertifikat elektronik X.509 versi 3 sesuai dengan RFC 5280. BSrE CA melakukan tinjauan terhadap profil sertifikat secara berkala minimal setahun sekali.

7.1.1 Nomor Versi

BSrE CA menerbitkan sertifikat X.509 v3.

7.1.2 *Certificate Extension*

BSrE CA memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

7.1.2.1 Penggunaan Kunci

Field	Sertifikat BSrE CA	Sertifikat SSL/EV SSL
Critical	True	True
digitalSignature	True	True
nonRepudiation	False	False
KeyEnchiperment	False	False
dataEnchiperment	False	False
Key Agreement	False	True
keyCertSign	False	False
cRLSign	True	False
enchiperOnly	False	False
dechiperOnly	False	False

7.1.2.2 *Certificate Policies Extension*

Ekstensi *certificate Policies* dari sertifikat X.509 Versi 3 diisi dengan identifier objek sesuai dengan bagian 7.1.6. *Field criticality* dari ekstensi ini diisi FALSE.

7.1.2.3 *Basic Constraint*

Ekstensi *Basic Constraints* sertifikat X.509 Versi 3 bagi sertifikat BSrE CA memiliki field CA yang diisi TRUE. Ekstensi *Basic Constraints* sertifikat Pemilik harus memiliki field CA yang diisi FALSE. Field criticality dari ekstensi ini harus diisi TRUE untuk sertifikat BSrE, tapi boleh diisi TRUE atau FALSE bagi sertifikat Pemilik.

7.1.2.4 *Extended Key Usage*

Secara baku, *Extended Key Usage* diatur sebagai suatu ekstensi non-critical. Sertifikat BSrE CA dapat memuat ekstensi *extended key usage* sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang BSrE CA terbitkan. Semua sertifikat Pemilik boleh mengandung sebuah ekstensi *extended key usage* sesuai tujuan penerbitan sertifikat, namun tidak boleh memuat nilai anyEKU.

7.1.2.5 CRL *Distribution Points*

Sertifikat X.509 Versi 3 diisi dengan suatu ektensi *cRLDistributionPoints* yang memuat URL yaitu lokasi dimana Pengandal dapat memperoleh CRL untuk memeriksa status sertifikat. *Field criticality* dari ekstensi ini harus diisi FALSE.

7.1.2.6 *Authority Key Identifier*

Sertifikat X.509 Versi 3 secara umum diisi dengan ekstensi *authorityKeyIdentifier*. Metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik dari BSrE CA, harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini harus diisi FALSE.

7.1.2.7 *Subject Key Identifier*

Bila ada dalam sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini harus diisi dengan FALSE dan metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik subjek sertifikat harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.

7.1.3 Identifier Objek Algoritma

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

CP: OID standar X.509v3 harus digunakan. Algoritma harus enkripsi RSA untuk kunci subjek dan SHA384 dengan enkripsi RSA untuk tanda tangan sertifikat.

SHA384 With RSA Encryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}

7.1.4 Format Nama

BSrE CA tidak menerbitkan sertifikat dengan nama domain yang berisi Reserved IP Address atau Nama Domain Internal.

7.1.5 Batasan Nama

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

7.1.6 Identifier Objek Kebijakan Sertifikat

OID CP yang tercantum di dalam sertifikat adalah sesuai dengan daftar OID pada poin 1.2.

7.1.7 *Usage of Policy Costraints Extension*

Tidak ditentukan.

7.1.8 *Policy Qualifiers Syntax and Semantics*

Tidak ditentukan.

7.1.9 *Processing Semantics for the Critical Certificate Policies Extension*

Tidak ditentukan.

7.2 Profil CRL

7.2.1 Nomor Versi

BSrE CA menerbitkan CRL dengan standar X.509 versi 2.

7.2.2 CRL dan Ekstensi Entri CRL

BSrE CA menggunakan CRL dan CRL entry extension sesuai RFC 5280.

7.3 Profil OCSP

BSrE mengoperasikan suatu responder OCSP yang sesuai dengan RFC 6960 atau RFC 5019.

7.3.1 Nomor Versi

BSrE menerbitkan responder OCSP versi 1.

7.3.2 Ekstensi OCSP

Ekstensi OCSP merujuk ke standar interoperabilitas PSrE Instansi.

BAB VIII
SISTEM AUDIT DAN PENILAIAN

BSrE CA menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Kementerian Komunikasi dan Informatika tentang Penyelenggaraan Sertifikasi Elektronik. BSrE CA diaudit untuk kepatuhan kepada Webtrust CA.

8.1 Frekuensi atau Keadaan Asesmen

BSrE CA diaudit secara periodik minimal 1 kali dalam 12 bulan untuk memastikan bahwa seluruh kegiatan operasional BSrE CA sesuai dengan yang ditetapkan dalam dokumen CP/CPS SSL. BSrE CA menindak lanjuti setiap hasil audit berdasarkan rekomendasi yang dibuat oleh Auditor. BSrE CA menjalani audit kepatuhan dan menyampaikan laporan berkala minimal sekali setahun yang dipersyaratkan oleh Kementerian Komunikasi dan Informatika.

8.2 Identitas/Kualifikasi Auditor

Auditor menunjukkan kompetensi pada bidang audit kepatuhan, dan benar-benar memahami persyaratan CP/CPS SSL ini. Auditor kepatuhan melakukan audit kepatuhan sebagai tanggung jawab utama. Auditor kepatuhan memiliki kualifikasi sebagai berikut:

a. Auditor dilaksanakan oleh tim asesmen independen yang *qualified*;
b. Auditor memiliki pengetahuan yang cukup tentang tanda tangan digital, sertifikat digital, X.509 versi 3 PKI *Certificate Policy and Certification Practices Framework*, serta Undang-Undang dan Peraturan di Indonesia terkait sistem dan transaksi elektronik, dan penyelenggaraan sertifikasi elektronik;
c. Auditor memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;

d. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah; dan
e. Auditor menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

8.3 Hubungan Auditor dengan Entitas yang Dinilai

BSrE CA memilih auditor / asesor yang independen.

8.4 Topik yang Dicakup oleh Asesmen

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

8.5 Tindakan yang Diambil sebagai Hasil dari Kekurangan

BSrE CA akan menyusun rencana tindakan perbaikan yang akan dilaksanakan untuk memperbaiki kekurangan yang tercatat berdasarkan masukan dari auditor.

Tindakan berikut harus dilakukan:

a. Auditor kepatuhan harus memberitahu BSrE CA tentang ketidaksesuaian; dan
b. Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian harus menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CPS dan kontrak yang sesuai, kemudian melanjutkan untuk melaksanakan pemberitahuan dan tindakan tersebut tanpa penundaan.

8.6 Komunikasi Hasil Audit

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada PA sebagaimana diatur dalam poin 8.1. Laporan tersebut harus mengidentifikasi versi CP/CPS SSL yang digunakan dalam asesmen. Selain itu, hasilnya harus dikomunikasikan seperti yang ditetapkan pada poin 8.5 di atas.

8.7 Audit Internal

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

BAB IX
ASPEK BISNIS DAN LEGAL

9.1 Biaya

9.1.1 Biaya layanan penerbitan atau pembaruan sertifikat elektronik

Seluruh proses/kegiatan yang berhubungan dengan permintaan, penerbitan dan pembaruan sertifikat elektronik tidak dikenakan biaya.

9.1.2 Biaya Pengaksesan Sertifikat

Seluruh proses/kegiatan yang berhubungan dengan akses terhadap sertifikat elektronik tidak dikenakan biaya.

9.1.3 Biaya Pengaksesan Informasi Pencabutan atau Status

Seluruh proses/kegiatan yang berhubungan dengan pencabutan sertifikat elektronik atau akses terhadap status keberlakuan sertifikat elektronik tidak dikenakan biaya.

9.1.4 Biaya layanan lainnya

Seluruh proses/kegiatan dalam konteks penerapan sertifikat elektronik BSrE CA tidak dikenakan biaya.

9.1.5 Kebijakan Pengembalian

Tidak ada ketentuan.

9.2 Tanggungjawab Keuangan

9.2.1 Cakupan Asuransi

Apabila terjadi compromise pada BSrE CA, BSSN dapat mengambil alih operasional BSrE CA. BSrE CA mematuhi persyaratan asuransi mengenai Penyelenggaraan Sertifikasi Elektronik sesuai dengan Peraturan Menteri yang terkait.

9.2.2 Aset Lainnya

Tidak ada ketentuan.

9.2.3 Jaminan Asuransi atau Garansi untuk Entitas Akhir

BSrE CA menyediakan kebijakan jaminan untuk para Pemilik sertifikat.

9.3 Kerahasiaan Informasi Bisnis

9.3.1 Ruang lingkup informasi rahasia

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

a. Informasi pribadi sebagaimana dijabarkan pada poin 9.4;
b. Kunci Privat Pemilik Sertifikat yang disimpan oleh BSrE CA, 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 BSrE CA;
f. Data aktivasi pada saat pengaktifan Kunci Privat BSrE CA sebagaimana dijabarkan pada poin 6.4;
g. Dokumentasi bisnis proses PSrE termasuk dokumen DRP dan BCP; dan
h. Laporan audit dari auditor independen sebagaimana dijabarkan pada poin 8.

9.3.2 Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia

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

9.3.3 Tanggungjawab untuk melindungi informasi rahasia

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

a. Pelatihan dan peningkatan awareness;
b. Perjanjian kontrak pegawai;
c. NDA dengan pegawai, pegawai *outsource*, dan rekanan.

9.4 Privasi Informasi Pribadi

9.4.1 Rencana privasi

BSrE CA melindungi informasi pribadi dalam kaitan dengan Kebijakan Privasi yang dipublikasikan pada website BSrE CA, https://bsre.bssn.go.id/repository.

9.4.2 Informasi yang Dianggap Pribadi

BSrE CA melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan Pemilik dengan persetujuan BSrE CA. Arsip yang dikelola oleh BSrE CA tidak boleh dirilis kecuali yang diizinkan pada poin 9.4.1.

9.4.3 Informasi tidak Dianggap Pribadi

Informasi yang termasuk dalam poin 7 (Informasi sertifikat, CRL, dan Profil OCSP) dari CP/CPS SSL ini tidak termasuk dalam poin 9.4.2.

9.4.4 Tanggungjawab perlindungan informasi pribadi

BSrE CA bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan dapat berbentuk digital maupun kertas. *Backup* informasi pribadi harus 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 supaya dapat menggunakan informasi tersebut. BSrE CA mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Perjanjian Pemilik Sertifikat Elektronik. Perjanjian Pemilik Sertifikat Elektronik juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh BSrE CA.

9.4.6 Pengungkapan Berdasarkan Proses Peradilan atau Administratif

BSrE CA tidak akan membuka informasi pribadi kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, aturan dan peraturan pemerintah, atau perintah pengadilan.

9.4.7 Keadaan Pengungkapan Informasi Lain

Tidak ada ketentuan.

9.5 Hak atas Kekayaan Intelektual

BSrE CA tidak boleh dengan sengaja melanggar hak kekayaan intelektual pihak lain. Semua hak kekayaan intelektual BSrE CA termasuk semua merek dagang dan hak cipta dari semua dokumen BSrE CA tetap menjadi milik tunggal dari BSrE CA.

9.6 Pernyataan dan Jaminan

9.6.1 Pernyataan dan Jaminan BSrE CA

BSrE CA menyatakan dan menjamin, sejauh yang ditentukan dalam CP/CPS SSL, bahwa:

a. BSrE CA mematuhi ketentuan yang diatur dalam CP/CPS SSL ini;
b. BSrE CA menerbitkan dan memperbarui CRL secara berkala;
c. Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP/CPS SSL ini;
d. BSrE CA akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

9.6.2 Pernyataan dan Jaminan RA

RA menyatakan dan menjamin, 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. BSrE CA mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP/CPS SSL ini serta perjanjian yang disetujui lainnya.

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat Elektronik

Pemilik Sertifikat menjamin bahwa:

a. Setiap sertifikat elektronik yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah merupakan tanda tangan elektronik pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan elektronik dibuat;

b. Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;
c. Sudah melakukan review terhadap informasi dari sertifikat;
d. Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;
e. Sertifikat elektronik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CP/CPS SSL ini;
f. Segera:
    1) Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat; dan
    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
    3) Menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat elektronik setelah sertifikat dicabut;
g. Akan menanggapi instruksi BSrE CA terkait compromise atau penyalahgunaan sertifikat elektronik dalam kurun waktu empat puluh delapan (48) jam;
h. Menyetujui dan menerima bahwa BSrE CA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika BSrE CA menemukan bahwa Sertifikat tersebut digunakan untuk

mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian *malware*;

i. Pemilik sertifikat adalah pengguna akhir dan bukan merupakan BSrE CA, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat elektronik untuk tujuan penandatangan sertifikat elektronik PSrE lain.
j. Sertifikat SSL dan EV SSL akan diinstall hanya pada server yang dapat diakses pada nama domain (subjectAltName(s)) yang terdapat pada Sertifikat.

9.6.4 Pernyataan dan Perjanjian Pengandal

Pengandal menjamin bahwa:

a. Memiliki kemampuan teknis untuk menggunakan sertifikat;
b. Apabila perwakilan dari Pengandal menggunakan suatu sertifikat yang diterbitkan oleh BSrE CA, 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 RA yang berwenang ataupun BSrE CA, jika Pengandal menyadari atau mencurigai bahwa telah terjadi compromise pada Kunci Privat;
d. Mewajibkan Pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hokum dari kegagalan memenuhi kewajiban Pengandal yang ada pada CP/CPS SSL ini;

e. Harus mematuhi ketentuan yang ditetapkan di CP/CPS SSL serta perjanjian lain yang terkait.

9.6.5 Pernyataan dan Jaminan dari Partisipan Lain

Tidak ada ketentuan.

9.7 Pelepasan Jaminan

BSrE CA membuat pernyataan dalam CP/CPS SSL bahwa mereka tidak menjamin:

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

9.8 Pembatasan Tanggung Jawab

9.8.1 Pembatasan Tanggung Jawab PSrE

BSrE tidak bertanggung jawab terhadap:

a. Kerugian yang diakibatkan oleh penggunaan sertifikat elektronik atau pasangan kunci yang tidak sesuai dengan yang ditetapkan dalam dokumen CP/CPS SSL ini;
b. Kerugian yang disebabkan oleh kondisi *force majeure*;
c. Kerugian yang disebabkan oleh kode yang tidak sah (*malicious code*) pada infrastruktur yang digunakan oleh Pemilik Sertifikat Elektronik;
d. Semua kerusakan yang disebabkan oleh malware (seperti virus atau Trojans) diluar perangkat BSrE CA.

9.8.2 Pembatasan Tanggung Jawab RA

Pembatasan tanggung jawab RA ditentukan dalam perjanjian dari BSrE CA kepada RA. Secara khusus, RA bertanggung jawab atas pendaftaran Pemilik.

9.9 Ganti Rugi

Penggantian kerugian diatur dalam perjanjian antar para pihak yang terlibat sebelum menggunakan layanan.

9.9.1 Ganti Rugi oleh BSrE CA

Kewajiban ganti rugi BSrE CA ditetapkan Perjanjian Pemilik Sertifikat, kebijakan terkait garansi, Perjanjian Pengandal atau perjanjian lainnya yang mengatur mengenai hal tersebut termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pemilik Sertifikat sepakat untuk mengganti rugi BSrE CA berikut dengan para pihak terkait terhadap kerugian, kerusakan, dan biaya, yang diakibatkan oleh:

a. *Any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional;*
b. Pelanggaran yang dilakukan oleh Pemilik Sertifikat terhadap Perjanjian Pemilik Sertifikat, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
c. Penggunaan Kunci Privat Pemilik Sertifikat yang tidak sah karena kelalaian Pemilik Sertifikat; atau

d. Penggunaan Sertifikat oleh Pemilik Sertifikat untuk kegiatan melawan hukum.

9.9.3 Ganti Rugi oleh Pengandal

BSrE CA menyertakan persyaratan ganti rugi untuk Pengandal dalam Perjanjian Pengandal.

9.10 Jangka Waktu dan Penghentian

9.10.1 Syarat

Dokumen CP/CPS SSL ini dan setiap perubahannya akan efektif berlaku setelah dipublikasikan dalam sistem repositori BSrE CA dan tetap berlaku sampai diganti dengan versi yang lebih baru.

9.10.2 Penghentian

Perubahan CP/CPS SSL ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 hari setelah dipublikasikan.

9.10.3 Efek Pengakhiran dan Keberlangsungan

BSrE CA mengkomunikasikan kondisi, dampak dari pengakhiran CPS, dan juga kondisi keberlangsungan dari Sertifikat yang masih berlaku melalui laman situs web BSrE CA atau repositori BSrE CA serta meski CPS sudah tidak berlaku lagi, aturan terkait pelindungan data dan arsip informasi tetap dipatuhi.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

BSrE CA menyediakan media komunikasi bagi para pihak terkait melalui publikasi pada laman, telepon, email, dan dokumen baik dalam bentuk elektronik maupun kertas. BSrE CA memberi tanggapan paling lama 20 (dua puluh) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke BSrE CA harus

dialamatkan sesuai dengan yang tercantum pada poin 1.5.2 pada CPS.

9.12 Amandemen

9.12.1 Prosedur untuk Amandemen

BSrE CA akan meninjau CP/CPS SSL ini setidaknya 1 (satu) kali setiap tahun. Perbaikan, pembaruan atau perubahan terhadap dokumen CP/CPS SSL ini harus dipublikasikan. Amandemen CP/CPS SSL dilakukan sesuai dengan prosedur persetujuan CP/CPS SSL.

9.12.2 Periode dan Mekanisme Pemberitahuan

BSrE CA menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CP/CPS SSL ini termasuk juga keterangan waktu ketika CP/CPS SSL efektif berlaku. Ketika terjadi perubahan CP/CPS SSL harus dipublish paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.

9.12.3 Kondisi dimana OID harus berubah

Jika Policy Authority memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, BSrE CA 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 CP/CPS SSL ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara BSrE CA dengan pemilik sertifikat.

9.14 Hukum yang Mengatur

CP/CPS SSL ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat BSrE CA ataupun produk/ layanan lainnya. Termasuk apabila sertifikat BSrE CA dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia. Para pihak, termasuk rekan BSrE CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

9.15 Kepatuhan atas Hukum yang Berlaku

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

9.16 Provisi Rupa-rupa

9.16.1 Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2 Pengalihan

Entitas yang beroperasi di bawah CP/CPS SSL ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari BSrE CA.

9.16.3 Keterpisahan

Jika terdapat ketentuan dari CP/CPS SSL ini, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CP/CPS SSL ini

selanjutnya akan ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CP/CPS SSL ini yang menjelaskan batasan tanggung jawab, dimaksudkan dapat dipisahkan dan bersifat independen dari ketentuan lain dan harus diberlakukan dengan sebagaimana harusnya.

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

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

9.16.5 Force *Majeure*

BSrE CA tidak bertanggung jawab atas kegagalan atau keterlambatan dalam kinerjanya dikarenakan penyebab yang berada di luar kendali yang wajar, termasuk namun tidak terbatas pada, bencana alam, tindakan otoritas sipil atau militer, kebakaran, wabah, banjir, gempa bumi, kerusuhan, keadaan perang, dan alasan di luar ketentuan hukum yang berlaku. BSrE CA wajib menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas BSrE CA.

9.17 Provisi Lain

Tidak ada ketentuan.

Ditetapkan di Jakarta

Pada tanggal

Ditandatangani secara elektronik oleh:
KEPALA BALAI SERTIFIKASI ELEKTRONIK

Jonathan Gerhard T., S.ST
Penata Tk. I (III/d)

Lampiran A

DEFINISI

a. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
b. Penyelenggara Sertifikasi Elektronik adalah badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik
c. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara sistem BSrE CA yang berada di bawah dan bertanggung jawab kepada Deputi Bidang Operasi Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara.
d. Balai Sertifikasi Elektronik *Certificate Authority* yang selanjutnya disebut BSrE CA adalah entitas yang berwenang untuk mengeluarkan, mengelola, mencabut, dan memperbarui Sertifikat dalam lingkup IKP yang dikelola oleh BSrE.
e. Otoritas Pendaftaran yang selanjutnya disebut RA yaitu unit yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon pemilik Sertifikat Elektronik BSrE CA.
f. Verifikator adalah personel pegawai tetap atau pegawai negeri sipil yang bertanggung jawab melakukan proses verifikasi terhadap kelengkapan bukti dan berkas calon atau Pemilik Sertifikat Elektronik BSrE CA pada proses pendaftaran Sertifikat Elektronik.
g. Pemilik Sertifikat Elektronik adalah pihak yang identitasnya tertera dalam Sertifikat Elektronik yang diterbitkan oleh BSrE dan sudah melalui proses verifikasi.
h. Institusi Pengguna Sertifikat Elektronik adalah lembaga/organisasi/badan hukum yang telah bekerja sama dengan

BSrE untuk pemanfaatan sertifikat elektronik bagi Pemilik Sertifikat Elektronik.

i. Pengandal adalah pihak yang mempercayai Sertifikat Elektronik dan Tanda Tangan Elektronik yang diterbitkan oleh BSrE dengan membuktikan keabsahan identitas dari pemilik sertifikat elektronik.
j. Auditor Kepatuhan adalah personel yang bertanggung jawab melakukan audit kesesuaian dan keamanan pada BSrE CA dan Otoritas Pendaftaran.
k. *Subject Distinguished Name* yang selanjutnya disebut Subject DN adalah informasi identitas Pemilik Sertifikat Elektronik yang tertera pada sertifikat elektronik.
l. Perangkat Pembuat Tanda Tangan Elektronik adalah Perangkat Lunak atau Perangkat Keras yang dikonfigurasi dan digunakan untuk membuat Tanda Tangan Elektronik.
m. Data Pembuatan Tanda Tangan Elektronik adalah kode pribadi, kode biometrik, kode kriptografi, dan/ atau kode yang dihasilkan dari pengubahan tanda tangan manual menjadi Tanda Tangan Elektronik, termasuk kode lain yang dihasilkan dari perkembangan Teknologi Informasi.
n. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan lnformasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
o. *Certificate Policy* yang selanjutnya disebut CP adalah ketentuan dan kebijakan yang mengatur semua pihak yang terkait dengan penggunaan sertifikat elektronik yang dikeluarkan oleh BSrE CA.
p. *Certificate Practice Statement* yang selanjutnya disebut CPS adalah pernyataan tentang bagaimana prosedur terkait penerbitan, penggunaan, pengaturan, penarikan dan pembaruan sertifikat elektronik oleh BSrE CA.
q. Pasangan Kunci adalah Kunci Privat dan Kunci Publik yang saling berasosiasi.

r. Kunci Privat adalah salah satu kunci dari pasangan kunci kriptografi yang hanya disimpan dan dirahasiakan oleh pengguna serta digunakan untuk melakukan tanda tangan elektronik atau untuk membuka (dekripsi) pesan yang disandi menggunakan Kunci Publik pada sertifikat elektronik.

s. Kunci Publik adalah salah satu kunci dari pasangan kunci kriptografi yang dimiliki oleh pihak tertentu dan dapat dipergunakan oleh pihak-pihak lain untuk melakukan pertukaran informasi secara aman dengan pemilik kunci tersebut.

t. Repositori adalah adalah sebuah basis data yang berisi informasi dan data yang berkaitan dengan sertifikasi elektronik. Repositori juga dapat disebut sebagai direktori.

u. Sertifikat SSL adalah sertifikat yang diterbitkan oleh BSrE CA untuk penggunaan pengamanan pada web server.

v. Sertifikat EV SSL adalah sertifikat SSL yang diterbitkan oleh BSrE CA dengan persyaratan EV SSL.

Akronim

ADN	Authorization Domain Name
BCP	Business Continuity Plans
CA	Certificate Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DRP	Disaster Recovery Plans
EV	Extended Validation
FQDN	Fully-Qualified Domain Name
IETF	Internet Engineering Task Force

ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standarization Sector
NDA	Non-Disclosure Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
RFC	Request for Comment (pada IETF.org)
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TSA	Time Stamping Authority
X.509	Standar ITU-T untuk sertifikat dan otentikasi sesuai kerangka mereka
URI	Uniform Resource Identifier