CA Digisign
Certificate Practice Statement
Penyelenggara Sertifikat Elektronik (PSrE Terdaftar)
Versi : 1.3
OID : 2.16.360.1.1.1.12.2.1.2

6 Agustus 2019
Policy Authority

Fiki Arfiandi

Lembar Catatan Review/Revisi

Tanggal	Rev	Uraian	Oleh
18 Juli 2019	1.0	Initial Release	PA Authority
6 Agustus 2019	1.1	Perubahan Judul CPS, menjadi PSrE Terdaftar	PA
6 Agustus 2019	1.2	Penghapusan point 2.3.2 huruf a “termasuk aparatur sipil negara, TNI”	PA
6 Agustus 2019	1.3	Penghapusan point 2.3.2 huruf b	PA

DAFTAR ISI

1. PENGANTAR

1.1 Ringkasan

Infrastruktur Kunci Publik (IKP) Indonesia adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikat Elektronik (PSrE) Induk. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah nomor 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik. PSrE di bawah PSrE Induk terdiri atas 2 (dua) jenis PSrE yaitu PSrE Instansi Penyelenggara Negara (PSrE Instansi) dan PSrE non-Instansi Penyelenggara Negara (PSrE non-Instansi). PSrE Instansi menerbitkan sertifikat untuk entitas Pemerintah (Government to Government dan Government to Government Employee). PSrE non-Instansi menerbitkan sertifikat untuk entitas non-Pemerintah.

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

CPS ini sesuai dengan standar Request for Comments 3647 (RFC 3647) dari Internet Engineering Task Force (IETF) tentang Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework.

1.2 Identifikasi dan Nama Dokumen

Dokumen ini adalah Dokumen CPS (Certification Practice Statement) PSrE Terdafar (Digisign)
Object Identifier (OID) yang digunakan untuk CPS (tidak termasuk Extended Validation Certificate) ini adalah:

1. 2.16.360.1.1.1.12.2.1.2 (PSrE Terdaftar Non-Instansi) (Digisign)

1.3 Partisipan IKP

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1 PSrE Induk Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia. PSrE Induk menerbitkan dan mencabut Sertifikat Digiital PSrE Berinduk (PSrE Instansi dan PSrE Non-Instansi) berdasarkan status Pengakuan yang diberikan oleh Kemenkominfo. PSrE Induk tidak menerbitkan Sertifikat Digital kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat Digital PSrE Berinduk, sebagaimana dirinci dalam CPS ini, termasuk:

- Pengendalian terhadap proses pendaftaran
- Proses identifikasi dan autentikasi
- Proses penerbitan Sertifikat
- Publikasi Sertifikat
- Pencabutan Sertifikat, dan
- Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE berinduk yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

1.3.1.2 PSrE Berinduk

PSrE Berinduk adalah PSrE yang tersertifikasi dan Sertifikat Digitalnya ditandatangani oleh PSrE

Induk. PSrE Berinduk akan menerbitkan Sertifikat Digital kepada Pemilik. Ada 2 (dua) jenis PSrE Berinduk:

- PSrE Instansi
  PSrE Instansi adalah PSrE yang diselenggarakan oleh Instansi Penyelenggara Negara dan menerbitkan Sertifikat Digital kepada entitas Pemerintah.
- PSrE Non-Instansi
  PSrE Non-Instansi adalah PSrE yang menerbitkan Sertifikat Digital kepada entitas selain Pemerintah. (CA Digisign adalah salah satu PSrE Terdaftar Non-Instansi)

CA Digisign tidak memiliki PSrE Berinduk dibawahnya

1.3.2 Otoritas Pendaftaran (RA)

PSrE Berinduk menjalankan sendiri fungsi Otoritas Pendaftaran (RA). Pemohon melakukan permintaan penandatanganan Sertifikat Digital (*Certificate Signing Request*) ke PSrE Berinduk

CA Digisign tidak menerapkan RA

1.3.2.1 Function of Registration Authorities / Fungsi dari RA

RA berkewajiban untuk melaksanakan fungsi tertentu yang mengacu pada perjanjian RA, meliputi hal-hal seperti berikut:

a. menyusun prosedur pendaftaran untuk Pemohon sertifikat;
b. melakukan identifikasi dan otentikasi Pemohon sertifikat;
c. memulai atau meneruskan proses permohonan pembatalan sertifikat; dan
d. menyetujui permohonan untuk memperbaharui sertifikat atau pembaharuan kunci atas nama PSrE

CA Digisign tidak menerapkan RA

1.3.2.2 Persyaratan khusus RA untuk Sertifikat EV SSL

Tidak diterapkan

1.3.3 Subscribers / Pemilik

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

CA Digisign boleh menerbitkan Sertifikat kepada semua Pemilik.

1.3.4 Relying Parties / Pihak Pengandal

Pihak Pengandal adalah entitas yang mempercayai Sertifikat Digital dan Tanda Tangan Digital yang diterbitkan oleh PSrE Berinduk. Pihak Pengandal harus terlebih dahulu memeriksa respon dari Certificate Revocation List (CRL) atau Online Certificate Status Protocol (OCSP) PSrE Berinduk yang sesuai sebelum memanfaatkan informasi yang ada dalam sertifikat.

Pihak Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama Pemilik

dengan kunci publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat. Pihak Pengandal dapat menggunakan informasi dalam sertifikat untuk menentukan kecocokan penggunaan sertifikat. Pihak Pengandal menggunakan informasi dalam Sertifikat Digital untuk:

a. Memeriksa tujuan penggunaan sertifikat
b. Melakukan verifikasi tanda tangan digital
c. Memeriksa apakah Sertifikat Digital termasuk di dalam CRL
d. Penyetujuan batas tanggung jawab dan jaminan

Pihak Pengandal meliputi Bank, Perusahaan e-Commerce, Instansi Penyelenggara Negara dan entitas lain yang menggunakan tanda tangan elektronik di dalam layanannya.

1.3.5 Partisipan Lain

1.3.5.1 Penyedia Layanan Pusat Data

Penyedia Layanan Pusat Data adalah Pihak Ketiga yang menyediakan layanan Pusat Data untuk operasional CA Digisign

1.4 Kegunaan Sertifikat

1.4.1 Penggunaan Sertifikat yang Semestinya

Penggunaan Sertifikat Pemilik dibatasi sesuai *Key Usage* dan *Extended Key Usage* pada *Certificate Extension.* Sertifikat CA Digisign hanya dapat digunakan untuk menerbitkan Sertifikat Digital untuk transaksi Tanda Tangan Elektronik

Pemilik Sertifikat dapat memilih Tingkat Jaminan yang sesuai sebagai identitas yang akan mereka tunjukkan kepada Pihak Pengandal. Tingkatan Jaminan yang dimaksud dibedakan menjadi Kelas Sertifikat sebagai berikut:

a. Level 2: Sertifikat dengan Tingkat Jaminan rendah
   OID (2.16.360.1.1.1.12.2.2.2)
b. Level 3: Sertifikat dengan Tingkat Jaminan Sedang
   OID (2.16.360.1.1.1.12.2.2.3)
c. Level 4: Sertifikat dengan Tingkat Jaminan Tinggi
   OID (2.16.360.1.1.1.12.2.2.4)

Penggunaan yang tidak sesuai dapat berakibat pada hilangnya jaminan yang diberikan oleh CA Digisign kepada Pemilik Sertifikat dan Pihak Pengandal.

Certificate Class	**Tingkat Jaminan / Assurance Level**			**Penggunaan / Usage**		
	Jaminan Rendah / Low Assurance	**Jaminan Sedang / Medium Assurance**	**Jaminan Tinggi / High Assurance**	**Autentikasi / Authentication**	**Tanda Tangan Digital / Digital Signature**	**Enkripsi / Encryption**
Sertifikat Individu / Individual Certificates						
Level 2	✓				✓	✓

Level 3		✓		✓	✓	✓
Level 4			✓	✓	✓	✓
Sertifikat Organisasi / Organizational Certificate			✓		✓	✓

1.4.2 Prohibited Certificate Uses / Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan oleh CA Digisign dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

1.5 Administrasi Kebijakan

Policy Authority (PA) CA Digisign memiliki peran dan tanggung jawab sebagai berikut:

a. Menetapkan *Certificate Policy* (CP)

b. Memastikan semua layanan, operasional dan infrastruktur CA Digisign yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan

c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki Tingkat Jaminan yang kurang lebih setara.

1.5.1 Organisasi Pengelola Dokumen

CPS dan dokumen referensinya dikelola oleh:

corpsec@digisign.id

Telepon : +62 21 31116109

1.5.2 Kontak yang Dapat Dihubungi

- Alamat surat:

  Digisign, PT. Solusi Net Internusa,
  Gedung Sahid Sudirman Center Lt.
  55 Jl. Jenderal Suidrman No 86 karet
  Tengsin Tanah Abang Jakarta 10220

- Email : corpsec@digisign.id
- URL : https://www.digisign.id
- Telepon/phone : +62 21 31116109

1.5.3 Personil yang Menentukan Kesesuaian CPS dengan Kebijakan

Policy Authority (PA) CA Digisign menentukan kesesuaian konten CPS dan kesesuaian antara CPS dengan CP.

1.5.4 Prosedur Persetujuan CPS

CA Digisign menyetujui CPS dan segala amandemen/perubahannya. Amandemen/perubahan

dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum. CA Digisign menentukan apakah amandeman/perubahan ke CP ini memerlukan pemberitahuan atau perubahan OID.

1.6 Definisi dan Akronim

PSrE Penyelenggara Sertifikasi Elektronik

PA Policy Authority

CRL Certificate Revocation List

2. TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI

2.1 Repositori

CA Digisign mengoperasikan repositori di mana dokumen kebijakan, sertifikat dari CA Digisign, CRL dipublikasikan.

2.2. Publikasi Informasi Sertifikat

CA Digisign memelihara repositori yang dapat diakses melalui internet, tempat publikasi sertifikat digital dari sertifikat CA Digisign, CRL terakhir, dokumen CP/CPS. Repositori sah/legal CA Digisign terletak di https://repository.digisign.id

2.3. Waktu atau Frekuensi Publikasi

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

2.4. Kendali Akses pada Repositori

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

3. IDENTIFIKASI DAN AUTENTIKASI

3.1 Penamaan

3.1.1 Tipe Nama

CA Digisign membuat dan menandatangani sertifikat dengan subyek Distinguished Name (DN) yang non-null dan mematuhi standar ITU X.500.

3.1.2 Kebutuhan Nama yang Bermakna

Sertifikat yang diterbitkan sesuai dengan CPS ini bermakna hanya jika nama-nama yang muncul dalam Sertifikat dapat dipahami dan digunakan oleh Pihak Pengandal.

penggunaan nama harus diotorisasi oleh pemilik yang sah atau perwakilan legal dari pemilik yang sah.

3.1.3 Anonimitas atau Pseudonimitas Pemilik

CA Digisign tidak menerbitkan sertifikat pemilik yang anonim atau pseudonim.

3.1.4 Aturan Interpretasi Berbagai Bentuk Nama

Distinguished Name (DN) dalam sertifikat diinterpretasikan dengan menggunakan standar X.500.

3.1.5 Keunikan Nama

Distinguished Names (DN) dalam sertifikat harus unik di dalam ranah IKP Indonesia.

3.1.6 Pengakuan, Otentikasi, dan Peran Merek Dagang

Pemohon tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. CA Digisign tidak perlu memverifikasi hak pemohon untuk penggunaan merek dagang. Merupakan tanggung jawab Pemohon untuk memastikan penggunaan nama-nama pilihan yang sah.

CA Digisign dapat menolak setiap permohonan atau melakukan pencabutan sertifikat apapun yang menjadi bagian dari sengketa merek dagang.

3.2 Validasi Identitas Awal

3.2.1 Pembuktian Kepemilikan Private Key

Pembuktian kepemilikan private key ada di akun Digisign

3.2.2 Autentikasi Identitas Organisasi

Permohonan dari organisasi harus dibuat oleh orang yang berwenang mewakili organisasi tersebut (lihat 3.2.5).

CA Digisign menyimpan catatan jenis dan perincian identifikasi yang digunakan untuk otentikasi organisasi setidaknya selama masa berlaku sertifikat yang dikeluarkan.

Persyaratan identifikasi dan autentikasi untuk organisasi:

Permohonan untuk memiliki Sertifikat Elektronik harus memenuhi persyaratan sebagai berikut:

a. menyerahkan asli surat permohonan yang dibuat dan ditandatangani oleh pemohon orang perseorangan, dan warga negara asing; dan

b. memperlihatkan asli dan menyerahkan salinan kepada CA Digisign
    a. kartu tanda penduduk yang memiliki nomor induk kependudukan untuk pemohon orang perseorangan;
    b. paspor, kartu izin tinggal terbatas, atau kartu izin tinggal tetap untuk warga negara asing;
    c. Akta pendirian dan/atau akta perubahan terakhir organisasi dan/atau badan usaha.

3.2.3 Autentikasi Identitas Individu/Perorangan

Identifikasi dan Otentikasi Identitas Individu sebagai perwakilan organisasi yang mengajukan permintaan sertifikat CA Digisign adalah :

a. Menunjukkan dan mengumpulkan salinan Identitas resmi yang dikeluarkan oleh pemerintah

b. Menunjukkan dan mengumpulkan salinan identitas yang dikeluarkan oleh perusahaan

Identifikasi dan Otentikasi Identitas Individu untuk yang mengajukan permintaan sertifikat pemilik Sebuah permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut, Identifikasi dan Otentikasi Identitas Individu sebagai perwakilan organisasi yang mengajukan permintaan sertifikat organisasi ke CA Digisign

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

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

3.2.5 Validasi Otoritas

CA Digisign bertanggung jawab untuk memverifikasi dan mengautentikasi perwakilan resmi seorang ahli hukum dengan memeriksa dokumen berikut (sebutkan):

- Surat Penunjukan Perwakilan Resmi
- Surat pengacara

3.2.6 Kriteria Inter-operasi

Inter-Operasi IKP Indonesia tidak diizinkan.

3.3 Identifikasi dan Autentikasi untuk Permintaan Re-Key

3.3.1 Identifikasi dan Autentikasi untuk Re-Key Rutin

Re-key tidak diterapkan

3.3.2 Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan

Re-key tidak diterapkan

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan

Permintaan pencabutan harus selalu diautentikasi. Permintaan untuk mencabut Sertifikat dapat diautentikasi dengan menggunakan Kunci Publik yang terkait Sertifikat tersebut, terlepas dari apakah Kunci Pribadi-nya telah rusak.

4. PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT

4.1 Permohonan Sertifikat

4.1.1 Siapa yang Dapat Mengajukan Permohonan Sertifikat

Pemohon Sertifikat individual maupun organisasi dapat mengajukan permohonan sertifikat CA yang ditandatangani oleh CA Digisign

4.1.2 Proses Pendaftaran dan Tanggung Jawabnya

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

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

a. Pembangkitan pasangan kunci yang sesuai menggunakan *platform* yang layak dan aman;
b. Pembangkitan *Certificate Signing Request* (CSR) dengan menggunakan perangkat yang sesuai dan aman;
c. Mengajukan permohonan Sertifikat;

4.2 Pemrosesan Permohonan Sertifikat

4.2.1 Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi

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

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat

Setelah semua pemeriksaan identitas dan atribut pemohon, konten permohonan untuk sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap sertifikat atau permohonannya terdapat kesalahan, CA Digisign menolak permohonan tersebut. Apabila tidak ada masalah, permohonan disetujui.

CA Digisign dapat menolak permintaan pendaftaran yang validasi persyaratannya tidak lengkap.

termasuk untuk alasan berikut;

a. CA Digisign dapat menolak permintaan pendaftaran berdasarkan pada potensi rusaknya merek CA Digisign
b. CA Digisign juga dapat menolak permohonan sertifikat dari pemohon yang sebelumnya melanggar kebijakan CA Digisign

CA Digisign tidak wajib untuk memberikan alasan kepada pemohon terkait permohonan permintaan sertifikat.

4.2.3 Waktu Pemrosesan Permohonan Sertifikat

Semua pihak yang terlibat dalam proses permohonan sertifikat harus melakukan usaha untuk memastikan permohonan sertifikat diproses tepat waktu. Pemohon juga akan mendapatkan informasi penolakan.

Sertifikat harus diterbitkan dan ditolak tidak lebih dari 8 (delapan) hari kerja semenjak disetujuinya berkas pendaftaran.

4.3 Penerbitan Sertifikat

4.3.1 Tindakan Digisign selama Penerbitan Sertifikat

CA Digisign memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa. CA Digisign juga mengautentikasi Permohonan Sertifikat

4.3.2 Pemberitahuan ke Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

CA Digisign segera memberitahu Pemilik tentang berhasilnya penerbitan sertifikat melalui email.

4.4 Penerimaan Sertifikat

4.4.1 Sikap yang Dianggap Menerima Sertifikat

Pemilik harus memeriksa semua informasi sertifikat dan menandatangani formulir penerimaan

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

4.4.2 Publikasi Sertifikat oleh CA Digisign

CA Digisign mempublikasikan sertifikat pada satu repositori

4.4.3 Pemberitahuan Penerbitan Sertifikat oleh Digisign ke Entitas Lain

Tidak ada ketentuan.

4.5 Pasangan Kunci dan Penggunaan Sertifikat

4.5.1 Pemilik Kunci Privat dan Penggunaan Sertifikat

CA Digisign akan melindungi Kunci Private atau bila pemilik memiliki system operasi yang sesuai untuk melindungi Kunci Privat mereka dengan menggunakan *hardware security module* dari penggunaan tanpa izin atau pengungkapan oleh pihak lain, dan harus memakai Kunci Privat mereka hanya untuk tujuan yang sudah ditentukan.

4.5.2 Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

Pihak Pengandal harus menggunakan perangkat lunak yang sesuai dengan X.509. CA Digisign menentukan pembatasan penggunaan sertifikat melalui sertifikat ekstensi dan harus menentukan mekanisme untuk menentukan validitas sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan mengikuti/mematuhi informasi ini sesuai dengan kewajibannya sebagai pihak pengandal.

4.6 Pembaruan Sertifikat

4.6.1 Kondisi untuk Pembaruan Sertifikat

Pembaruan Sertifikat didefinisikan sebagai pembuatan Sertifikat baru yang memiliki detail yang sama dengan Sertifikat yang telah dikeluarkan sebelumnya namun dengan pasangan kunci yang berbeda dan bertanggal 'Not After' yang baru. CA Digisign mendukung pembaruan harus mengidentifikasi produk dan layanan di mana pembaruan dapat diterima. CA dapat memperbarui Sertifikat selama:

- Sertifikat asli yang akan diperbarui belum dicabut;
- Kunci Publik dari Sertifikat asli belum masuk daftar hitam karena alasan apa pun; dan
- Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan.
- CA Digisign dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya.

4.6.2 Siapa yang Boleh Meminta Pembaruan

Pemilik yang belum pernah dicabut sertifikatnya boleh meminta pembaruan Sertifikatnya ke CA Digisign.

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat

Perpanjangan sertifikat harus dicapai dengan menggunakan proses pendaftaran awal

4.6.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Prosedur penerbitan sertifikat baru yang sama juga diikuti

4.6.5 Melakukan Penerimaan Pembaruan/Perpanjangan Sertifikat

Pemilik harus menerima sertifikat baru setelah prosedur penerimaan dan penerimaan sertifikat yang sama

4.6.6 Publikasi Pembaruan/Perpanjangan Sertifikat oleh CA Digisign

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam bagian 4.4.2

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh CA Digisign ke Entitas Lain

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

4.7 Re-Key Sertifikat

Re-Key sertifikat adalah penerbitan ulang sertifikat menggunakan informasi subyek dan tanggal kadaluarsa yang sama (bidang "validTo") namun dengan pasangan kunci yang baru.

4.7.1 Kondisi untuk Re-Key Sertifikat

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.2 Siapa yang Dapat Meminta Sertifikasi Public Key yang Baru

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.3 Pemrosesan Permintaan Re-Key Sertifikat

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.5 Melaksanakan Penerimaan Sertifikat Re-Key

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.6 Publikasi Sertifikat Re-Key oleh Digisign

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada tindakan yang diambil untuk pemberitahuan ke entitas lain.

4.8 Modifikasi Sertifikat

Modifikasi detil sertifikat tidak diperbolehkan.

4.8.1 Kondisi untuk Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.2 Siapa yang Dapat Meminta Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.3 Pemrosesan Permintaan Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.5 Melakukan Penerimaan Sertifikat yang Dimodifikasi

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.6 Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.7 Pemberitahuan Penerbitan Sertifikat oleh Digisign ke Entitas Lain

Modifikasi informasi sertifikat tidak diperbolehkan.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Kondisi untuk Pencabutan

CA Digisign mencabut sertifikat Pemilik dalam keadaan berikut:

- Mengidentifikasi informasi atau komponen afiliasi dari setiap nama dalam sertifikat yang menjadikannya tidak valid.
- Semua informasi dalam sertifikat menjadi tidak valid.
- Pemilik dapat ditunjukkan telah melanggar ketentuan Peraturan Perundang-undangan.
- Ada alasan untuk percaya bahwa kunci privat telah dikompromikan/rusak.
- Pemilik atau pihak berwenang lainnya (sesuai ketentuan Peraturan Perundang-undangan) meminta agar sertifikatnya dicabut.
- Penghentian Operasional CA Digisign

Sertifikat harus dicabut bila ikatan antara subjek dan kunci publik subjek yang ditentukan dalam sertifikat tidak lagi dianggap valid.

4.9.2 Siapa yang Dapat Meminta Pencabutan

Sertifikat tersebut dapat diminta dicabut oleh Pemilik atau oleh entitas lain (yang dapat membuktikan pemaparan atau penyalahgunaan sertifikat sesuai dengan Kebijakan Sertifikasi).

4.9.3 Prosedur Permintaan Pencabutan

CA Digisign memverifikasi identitas dan wewenang (untuk entitas penegak hukum) yang meminta

pencabutan.

Permintaan pembatalan oleh entitas lain harus ada penyampaian bukti bahwa,

a. kunci privat sertifikat telah terpapar, atau
b. penggunaan sertifikat tersebut tidak sesuai dengan Kebijakan Sertifikasi atau
c. hubungan pemilik sertifikat dengan institusi tidak ada

4.9.4 Tenggang Waktu Permintaan Pencabutan

Tidak ada tenggang waktu yang diizinkan setelah permintaan pencabutan diverifikasi. CA Digisign akan mencabut sertifikat segera setelah cukup praktis mengikuti verifikasi permintaan pencabutan.

4.9.5 Jangka Waktu Digisign Memroses Permintaan Pencabutan

CA Digisign memulai investigasi permintaan pencabutan dalam satu (1) hari kerja kecuali dari kasus *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang memadai akan segera diproses.

4.9.6 Persyaratan Pemeriksaan untuk Pihak Pengandal

Pihak Pengandal harus memvalidasi setiap sertifikat dibandingkan CRL terbaru, yang berada di CA Digisign.

4.9.7 Frekuensi Penerbitan CRL

CRL akan diperbarui dan dipublikasikan setiap hari secara berkala

4.9.8 Latensi Maksimum untuk CRL

CA Digisign mempublikasikan data pencabutan sertifikat selambat lambatnya dalam waktu 30 (tiga puluh) menit setelah penerbitan.

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status secara Online/Daring

CA Digisign menyediakan layanan validasi online. informasi status sertifikat lainnya tersedia melalui repositori berbasis web CA Digisign Repository.

https://repository.digisign.id

4.9.10 Persyaratan Pemeriksaan Pencabutan secara Online

Tidak ada ketentuan.

4.9.11 Bentuk Lain Pengumuman Pencabutan

Tidak ada ketentuan.

4.9.12 Persyaratan Khusus Keterpaparan Re-Key

Re-key tidak diterapkan

4.9.13 Kondisi untuk Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.14 Siapa yang Dapat Meminta Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.15 Prosedur untuk Permintaan Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.16 Pembatasan pada Masa Pembekuan

Pembekuan sertifikat tidak disediakan.

4.10 Layanan Status Sertifikat

4.10.1 Karakteristik Operasional

Status sertifikat publik tersedia dari CRL di repositorinya.

4.10.2 Ketersediaan Layanan

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

4.10.3 Fitur Pilihan

Tidak ada ketentuan.

4.11 Akhir Berlangganan

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

4.12 Pemulihan dan Escrow Kunci

4.12.1 Kebijakan dan Praktik Escrow Kunci dan Pemulihan

Kunci privat CA Digisign tidak dititipkan. Penitipan pasangan kunci pengguna akhir dilindungi dengan sistem keamanan tingkat tinggi.

4.12.2 Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ada ketentuan.

5. FASILITAS, MANAJEMEN/PENGELOLAAN, DAN KENDALI OPERASI

5.1 Kendali Fisik

5.1.1 Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan CA Digisign serta juga tempat-tempat yang menampung workstation jarak jauh yang digunakan untuk mengelola CA Digisign

5.1.2 Akses Fisik

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

- Memastikan tidak ada akses tidak resmi yang diizinkan ke perangkat keras
- Menyimpan semua media dan kertas yang dapat dilepas yang berisi informasi teks biasa

yang sensitif dalam wadah yang aman.

- Monitor, baik secara manual maupun elektronik, untuk gangguan yang tidak sah setiap saat.
- Menjaga dan memeriksa secara berkala log akses.

Semua operasional CA Digisign yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan memiliki setidaknya 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 CA Digisign yang memiliki otoritas yang bisa mengakses fasilitas tersebut

5.1.3 Listrik dan AC

CA Digisign memiliki daya cadangan yang cukup untuk me-*lockout* secara otomatis, menyelesaikan beberapa hal/tindakan yang tertunda, dan mencatat keadaan peralatan sebelum kekurangan daya atau AC yang menyebabkan peralatan mati. Repositori IKP telah dilengkapi dengan Uninterrupted Power dan Generator Listrik yang cukup untuk pengoperasian tanpa adanya listrik/daya dari PLN, untuk mendukung kelangsungan operasi.

5.1.4 Keterpaparan Air

Peralatan CA Digisign dilindungi terhadap air dan diletakkan di atas tanah dengan *raised floor.*

5.1.5 Pencegahan dan Perlindungan Kebakaran

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

5.1.6 Media Penyimpanan

Media CA Digisign disimpan sehingga bisa melindunginya dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau *backup* diduplikasi dan disimpan di lokasi yang terpisah dari lokasi CA Digisign

5.1.7 Pembuangan Limbah

Bahan limbah yang mengandung informasi sensitif harus dihancurkan informasi yang ada di dalamnya sebelum dibuang.

5.1.8 Off-Site Backup / Backup Off-Site

Backup semua sistem dari CA Digisign yang cukup untuk pulih dari kegagalan sistem, telah dilakukan pada jadwal berkala dan disimpan di lokasi yang aman dan offsite (di lokasi yang terpisah dari peralatan CA Digisign.

5.2 Kontrol Prosedur

5.2.1 Peran yang Dipercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

- Koordinator
  Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan CA Digisign
- Policy Authority (PA)
  Pembuatan, revisi dan persetujuan CP dan CPS
- Staff PA

Membantu PA dalam menyiapkan dokumen dan Kebijakan CA Digisign

- Administrator Aplikasi
  Melakukan operasional dan maintenance aplikasi manajemen CA Digisign
- Adminstrator OS
  Melakukan operasional dan maintenance Sistem Operasi CA Digisign
- Admin Perangkat Kriptografi
  Melakukan Operasional dan maintenance Perangkat kriptografi CA Digisign.
- Registrasi
  Identifikasi dan Validasi identitas permohonan permintaan sertifikat
- Internal Audit
  Melakukan audit internal operasional CA Digisign

5.2.2 Jumlah Orang yang Diperlukan per/tiap Tugas

Bila diperlukan kontrol dari banyak pihak, semua partisipan memegang jabatan yang terpercaya. Kontrol banyak pihak tidak dapat dicapai dengan menggunakan personil yang bertugas pada Auditor Internal kecuali fungsi audit. Tugas berikut membutuhkan personil cadangan:

- Pembangkitan kunci
- Pembuatan Sertifikat
- Pencabutan Sertifikat
- Pembuatan CRL

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran

Semua individu diminta untuk mengidentifikasi dan mengotentikasi dirinya sendiri dengan control aksesnya.

5.2.4 Peran yang Memerlukan Pemisahan Tugas

Peran yang tidak diperankan bersamaan adalah:

- Policy Authority dan administrator operasional
- Internal audit dan semua peran lain
- Pengembang aplikasi dan semua peran lain

5.3 Kontrol Personil

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan Perizinan

Semua personil di CA Digisign adalah warga negara Indonesia dan telah dipilih atas dasar keterampilan, pengalaman, kesetiaan, kepercayaan, dan integritas sesuai dengan persyaratan sebagai berikut:

1. Bukti latar belakang yang diperlukan, kualifikasi dan pengalaman yang diperlukan untuk secara efisien dan memadai dalam melaksanakan tanggung jawab pekerjaan mereka; dan
2. Bukti catatan kriminal yang bersih.

5.3.2 Prosedur Pemeriksaan Latar Belakang

Semua personil di CA Digisign telah menyelesaikan pemeriksaan latar belakang. Ruang lingkup pemeriksaan latar belakang mencakup area berikut yang cakupannya:

- Kontak Referensi Pekerjaan
- Pendidikan atau sertifikasi
- Identifikasi Kependudukan (KTP)
- Catatan Kepolisian

5.3.3 Persyaratan Pelatihan

Semua personil CA Digisign dilatih untuk menjalankan tugasnya. Pelatihan semacam itu membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, prosedur terkait, undang-undang/hukum dan peraturan.

5.3.4 Frekuensi Pelatihan Ulang dan Persyaratannya

CA Digisign memberikan pelatihan ulang dan pembaruan kepada personilnya sesuai yang dibutuhkan untuk memastikan personil tersebut mempertahankan tingkat kemampuan yang dipersyaratkan untuk melakukan tanggung jawab pekerjaan mereka secara kompeten dan memuaskan

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan

CA Digisign memastikan bahwa perubahan staf tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

5.3.6 Sanksi untuk Tindakan yang Tidak Terotorisasi

Sanksi disipliner yang sesuai diberikan pada personil yang melanggar ketentuan dan kebijakan didalam CP, CPS atau Prosedur operasional CA Digisign

5.3.7 Persyaratan Kontraktor Independen

Personil sub kontraktor yang dipekerjakan untuk melaksanakan fungsi-fungsi yang terkait dengan operasi CA Digisign harus memenuhi persyaratan yang berlaku yang diatur dalam CPS ini.

5.3.8 Dokumentasi yang Disediakan untuk Personil

CA Digisign telah membuat tersedia bagi personilnya, Certificate Policy (Kebijakan Sertifikat) yang mereka dukung, CPS, dan undang-undang yang relevan, kebijakan, atau kontrak yang relevan. Dokumen teknis, operasi, dan administratif lain (mis. Panduan Administrasi, Manual Pengguna, dsb) telah disediakan agar personil yang terpercaya dapat melaksanakan kewajiban mereka.

5.4 Prosedur Log Audit

Berkas log audit harus disimpan untuk semua kejadian yang terkait dengan keamanan CA Digisign.

5.4.1 Jenis Kejadian yang Direkam

CA Digisign mengaktifkan semua kapabilitas audit keamanan dari sistem operasi CA Digisign, serta aplikasi Certification Authority CA Digisign memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat disimpan sedemikian rupa sehingga dapat memastikan keterlacakan setiap tindakan Trusted Role dalam operasional CA Digisign. Seperti, type kejadian dan tanggal serta waktu kejadian

5.4.2 Frekuensi Pemrosesan Log

Log audit ditinjau secara berkala, termasuk verifikasi bahwa log tidak rusak atau hilang

5.4.3 Perioda Retensi untuk Log Audit

Log audit CA Digisign dipertahankan selama satu (1) tahun agar tersedia bagi sebarang kendali yang patuh hukum.

5.4.4 Proteksi Log Audit

Log Audit dilindungi untuk mencegah perubahan dan mendeteksi gangguan serta untuk memastikan bahwa hanya individu denga n akses tepercaya yang berwenang yang mampu melakukan operasi apa pun tanpa memodifikasi integritasnya.

5.4.5 Prosedur Backup Log Audit

Log audit dan ringkasan audit di-backup. Media backup disimpan secara lokal dalam suatu lokasi yang aman.

5.4.6 Sistem Pengumpulan Audit (Internal vs Eksternal)

Sistem pengumpulan log audit adalah internal ke sistem CA Digisign.

5.4.7 Pemberitahuan ke Subyek Penyebab Kejadian

Ketika suatu kejadian dilog oleh sistem maka tidak ada pemberitahuan yang dipersyaratkan untuk diberikan ke individu, organisasi, peranti, atau aplikasi yang menyebabkan kejadian tersebut.

5.4.8 Asesmen Kerentanan

CA Digisign mengases kerentanan sistem CA atau komponennya paling tidak sekali setahun.

5.5 Pengarsipan Record

5.5.1 Tipe Record yang Diarsipkan

Catatan arsip CA Digisign mencakup:

- Siklus hidup operasi sertifikat termasuk permohonan sertifikat, dan permintaan pencabutan.
- Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh CA Digisign
- Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini.
- Data pendaftaran Pemohon

5.5.2 Periode Retensi Arsip

Catatan yang diarsipkan harus disimpan setidaknya selama 7 (tujuh) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.

5.5.3 Perlindungan Arsip

Catatan yang diarsipkan dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah.

5.5.4 Prosedur Backup Arsip

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

5.5.5 Persyaratan Record Stempel Waktu

Rekaman arsip CA Digisign diberi stempel waktu ketika mereka dibuat.

5.5.6 Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip di CA Digisign dilakukan oleh internal CA Digisign

5.5.7 Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Penyimpanan media untuk informasi arsip CA Digisign diperiksa saat pembuatan. Secara berkala,. Hanya peran tepercaya, dan orang-orang resmi lainnya yang diizinkan untuk mengakses arsip.

5.6 Pergantian Kunci

Untuk meminimalkan risiko dari kondisi Kunci Privat CA Digisign terkompromi, Kunci Privat dapat diubah. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat yang lama, namun masih berlaku, akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat terkait kadaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama harus disimpan dan dilindungi.
Apabila CA Digisign memperbarui kunci privat dan dengan demikian menghasilkan kunci publik baru, CA Digisign akan memberitahu semua Pemilik yang mengandalkan Sertifikat CA Digisign bahwa telah terjadi perubahan.

5.7 Pemulihan Bencana dan Kondisi Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

CA Digisign menangani bencana dan insiden *compromise* sesuai dengan prosedur penanganan bencana untuk meminimalkan dampak dari peristiwa seperti itu.

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

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

- Memberitahu PA sesegera mungkin.
- Memastikan integritas sistem telah direstorasi sebelum mengembalikan pada operasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.
- Mengoperasikan kembali CA Digisign, memberikan prioritas pada kemampuan untuk membangkitkan informasi status sertifikat dalam skedul penerbitan CRL.
- Bila kunci penandatanganan CA Digisign rusak, mengoperasikan kembali CA Digisign secepat mungkin, memberikan prioritas ke pembangkitan pasangan kunci baru penandatanganan CA Digisign.

5.7.3 Prosedur Kunci Privat Entitas Terkompromi

Bila kunci privat CA Digisign hilang atau *compromise*, CA Digisign memberitahu PSrE Induk, PA dan Pihak Pengandal melalui pengumuman publik. CA Digisign akan menghentikan layanan, memberitahu semua Pemilik melanjutkan dengan pencabutan semua sertifikat, menerbitkan suatu CRL akhir, dan memberitahu kontak-kontak keamanan yang relevan. Lalu Infrastruktur Kunci Publik akan disiapkan lagi dengan CA Digisign baru

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana

Untuk memelihara integritas layanan CA Digisign, diimplementasikan backup data dan prosedur-prosedur pemulihan. Seperti Rencana Pemulihan Bencana (Disaster Recovery Plan/DRP). DRP ditinjau ulang dan diuji secara berkala (minimal setahun sekali) dan diperbaiki dan diperbaharui jika dibutuhkan

5.8 Penutupan CA

Bila ada keadaan yang menyebabkan diakhirinya layanan CA Digisign dengan persetujuan dari Otoritas Kebijakan, CA Digisign akan memberitahu CA Induk, pemilik, dan semua pengandal. Rencana aksi adalah sebagai berikut:

- Memberitahu status layanan ke pengguna yang terkena dampak
- Menyimpan dalam jangka panjang informasi CA Digisign dan para pemilik mengikuti perioda yang dinyatakan di sini
- Menyediakan dukungan berkelanjutan dan menjawab pertanyaan
- Menangani dengan tepat pasangan kunci CA Digisign dan perangkat keras yang terkait

6. KENDALI KEAMANAN TEKNIS

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan Pasangan Kunci

Material kunci kriptografi yang digunakan oleh CA Digisign untuk menandatangani sertifikat, CRL, atau informasi status dibuat di dalam modul kriptografis yang sesuai standar FIPS 140

6.1.2 Pengiriman Kunci Privat ke Pemilik

Kunci private pemilik tidak dikirimkan ke pemilik

6.1.3 Pengiriman Kunci Publik ke Penerbit Sertifikat

Kunci publik didapatkan dari proses pembangkitan pasanagn kunci yang dijelaskan pada poin 6.1.1

6.1.4 Pengiriman Kunci Publik CA kepada Pihak Pengandal

CA Digisign menyediakan mekanisme untuk penyampaian digital yang aman dari semua sertifikat yang memuat kunci public yang diamankan menggunakan SSL.

6.1.5 Ukuran Kunci

CA Digisign membuat dan memakai Kunci RSA 4096-bit dengan Secure Hash Algorithm versi 2 (SHA-256) untuk menandatangani Sertifikat dan CRL yang diterbitkannya.

6.1.6 Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Pembangkitan pasangan kunci akan menghasilkan pasangan kunci yang sesuai dengan

FIPS 186

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

Kunci-kunci CA Digisign dipakai untuk penandatanganan sertifikat (keyCertSign) dan penandatanganan CRL (cRLSign).

6.2 Kontrol Kunci Private dan Kontrol Teknis Modul Kriptografi

6.2.1 Kendali dan Standar Modul Kriptografi

CA Digisign menggunakan modul kriptografi yang sudah sesuai standard FIPS 140-2.

6.2.2 Kendali Multi Personil (n dari m) Kunci Privat

CA Digisign mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif. Suatu jumlah minimum dari *Secret Shares* (n) dari sejumlah total *Secret Shares* yang dibuat dan didistribusikan untuk dipakai di modul kriptografis tertentu (m) diperlukan untuk mengaktifkan sebuah kunci privat CA Digisign yang disimpan di dalam modul.

Angka ambang yang diperlukan untuk pembuatan kunci adalah 5 dari 10 (dimana n=5 dan m=10), aktivasi kunci penandatanganan adalah 5 dari 10, dan backup serta pemulihan kunci privat adalah 2 dari 4.

6.2.3 Escrow Kunci Privat

Kunci privat CA Digisign tidak boleh pernah dititipkan (escrow). Pasangan kunci pemilik disimpan

oleh Digisign

6.2.4 Backup Kunci Privat

Kunci privat CA Digisign harus di-backup di bawah kendali multi-pihak yang sama dengan kunci tanda tangan asli.

6.2.5 Pengarsipan Kunci Privat

Kunci privat CA Digisign tidak boleh diarsipkan. CA

6.2.6 Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci privat CA Digisign boleh diekspor dari modul kriptografis hanya untuk melaksanakan prosedur backup kunci CA Digisign. kunci privat harus dienkripsi selama pemindahan

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografis

Kunci privat CA Digisign harus disimpan pada modul kriptografis FIPS 140-2, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

6.2.8 Metode Pengaktifan Kunci Privat

Aktivasi operasi kunci privat CA Digisign dilakukan oleh personil yang berwenang

6.2.9 Metode Penonaktifan Kunci Privat

Setelah dipakai, modul kriptografis harus dinonaktifkan oleh personil yang berwenang secara

otomatis setelah secret shares dicabut dari modul kriptografi.

6.2.10 Metode Penghancuran Kunci Privat

Ketika kunci tanda tangan privat CA Digisign tidak diperlukan lagi, para individu dalam peran terpercaya harus menghapus kunci privat dari Modul Kriptografi dan backupnya dengan menimpa kunci privat atau menginisialisasi modul dengan fungsi *factory reset* dari Modul Kriptografi.

6.2.11 Pemeringkatan Modul Kriptografis

Seperti diuraikan dalam bagian 6.2.1.

6.3 Aspek Lain dari Manajemen Pasangan Kunci

6.3.1 Pengarsipan Kunci Publik

Kunci publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasi pasangan kunci ditentukan oleh periode operasional sertifikat digital yang sesuai. Jangka waktu operasional maksimum kunci ditentukan selamasepuluh (10) tahun untuk CA Digisign.

6.4 Data Aktivasi

6.4.1 Aktivasi Generasi Data dan Instalasi

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

6.4.2 Perlindungan Data Aktivasi

Data aktivasi untuk perangkat HSM dilindungi CA Digisign menyimpan data aktivasi dalam bentuk *smart card* dengan perlindungan kata sandi.

6.4.3 Aspek Lain mengenai Data Aktivasi

Tidak ada ketentuan.

6.5 Kontrol Keamanan Komputer

6.5.1 Persyaratan Teknis Keamanan Komputer yang Spesifik/Khusus

CA Digisign memastikan bahwa sistem yang menjaga perangkat lunak CA Digisign dan file data aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem CA Digisign telah dikonfigurasi dan dikeraskan/dikuatkan menggunakan praktik terbaik industri. Semua sistem operasi membutuhkan identifikasi dan otentikasi untuk login yang diotentikasi. Ini memberikan kontrol akses discretionary, pembatasan kontrol akses ke layanan berdasarkan identitas yang diotentikasi, kemampuan audit keamanan, dan catatan audit yang dilindungi untuk berbagi sumber daya, perlindungan diri, dan isolasi proses.

Server CA Digisign yang terkait dengan kunci penandatanganan pribadi dioperasikan offline.

CP: Fungsi keamanan komputer berikut mungkin disediakan oleh sistem operasi, atau melalui kombinasi sistem operasi, perangkat lunak, dan perlindungan fisik. CA Digisign mencakup fungsi berikut:

- Membutuhkan login terautentikasi
- Menyediakan Discretionary Access Control
- Menyediakan kapabilitas audit keamanan
- Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data
- Menyediakan perlindungan mandiri untuk sistem operasi

6.5.2 Peringkat Keamanan Komputer

Peringkat keamanan computer digisign telah memenuhi persyaratan keamanan yang tinggi

6.6 Kontrol Teknis Siklus Hidup

6.6.1 Kontrol Pengembangan Sistem

Seluruh perangkat peralatan dan fasilitas Digisign disesuaikan dengan spesifikasi dengan tingkat keamanan yang tinggi, setiap penambahan dan perubahan harus melalui mekanisme prosedural, pengawasan dari berbagai ancaman dilakukan dengan pembatasan akses control disetiap peran

6.6.2 Kontrol Manajemen Keamanan

Konfigurasi dari sistem CA Digisign serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen CA Digisign.

6.6.3 Kontrol Keamanan Siklus Hidup

CA Digisign melakukan pengawasan terhadap kebutuhan skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak

6.7 Kontrol Keamanan Jaringan

CA Digisign menggunakan tindakan keamanan jaringan yang sesuai untuk memastikannya dijaga dari DoS dan serangan intrusi. Langkah-langkah tersebut termasuk penggunaan firewall dan menyaring router. Port dan layanan jaringan yang tidak digunakan telah dimatikan. Perangkat lunak jaringan apa pun diperlukan untuk memfungsikan CA Digisign

6.8 Stempel Waktu

Jam server online CA Digisign disinkronkan menggunakan Network Time Protocol. Waktu server offline disinkronkan secara manual.

7. SERTIFIKAT, CRL, DAN PROFIL OCSP

7.1 Profil Sertifikat

Profil sertifikat menurut RFC 5280 "Infrastruktur Kunci Publik Internet X.509: Daftar Sertifikat Pencabutan Sertifikat (CRL) Profil" yang digunakan.

7.1.1 Nomor Versi

CA Digisign menerbitkan sertifikat X.509 v3 (isi kolom versi dengan bilangan bulat “2”).

7.1.2 Ekstensi Sertifikat

CA Digisign menggunakan ekstensi sertifikat standar yang sesuai dengan RFC 5280.

7.1.2.1 Penggunaan Kunci

keyUsage yang digunakan untuk Sertifikat CA Digisign ditunjukan dalam tabel dibawah.

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

7.1.2.2 Perluasan Kebijakan Sertifikat

Ekstensi Kebijakan Sertifikat dari Sertifikat X.509 versi 3 diisi dengan pengidentifikasi objek untuk CP CA Digisign sesuai dengan bagian CPS 7.1.6 (Pengidentifikasi Obyek Kebijakan Sertifikat) dan dengan kualifikasi kebijakan yang ditetapkan Bidang kritikalitas ekstensi ini harus disetel ke FALSE.

7.1.2.3 Batasan Dasar

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

7.1.2.4 Penggunaan Kunci yang Diperluas

Secara baku, ExtendedKeyUsage diatur sebagai suatu ekstensi non-kritikal.

Sertifikat CA Digisign memuat ekstensi ExtendedKeyUsage sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang mereka terbitkan.

7.1.2.5 Titik Distribusi CRL

Sertifikat CA Digisign X.509 versi 3 mencakup ekstensi cRLDistributionPoints yang berisi URL lokasi tempat Pihak Relying dapat memperoleh CRL untuk memeriksa status Penerbitan Sertifikat CA Digisign. Kekritisan ekstensi ini disetel ke FALSE.

7.1.2.6 Pengidentifikasi Kunci Otoritas

CA Digisign umumnya mengisi ekstensi Pengidentifikasi Kunci Otoritas dari X.509 Versi 3 yang menerbitkan Sertifikat CA Digisign. Ketika penerbit sertifikat mengandung ekstensi Pengidentifikasi Kunci Subyek, Pengidentifikasi Kunci Otoritas terdiri dari 160-bit SHA-1 hash dari kunci publik dari CA Digisign Bidang kritikalitas ekstensi ini disetel ke FALSE.

7.1.2.7 Pengidentifikasi Kunci Subjek

Dimana CA Digisign mengisi X.509 version Menerbitkan Sertifikat CA Digisign dengan ekstensi subjectKeyIdentifier, keyIdentifier berdasarkan kunci publik dari subjek sertifikat dihasilkan sesuai dengan salah satu metode yang dijelaskan dalam RFC 5280. Di mana ekstensi ini digunakan, bidang kekritisan dari ekstensi ini disetel ke FALSE.

7.1.3 Pengidentifikasi Obyek 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 SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.

7.1.4 Format Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1

7.1.5 Batasan Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1

7.1.6 Pengidentifikasi Objek Kebijakan Sertifikat

CP OID yang menggabungkan CPS ini ke dalam sertifikat tertentu dengan referensi tercantum dalam Bagian 1.2 (Nama dan Identifikasi Dokumen).

7.1.7 Penggunaan Ekstensi Batasan Kebijakan

Tidak ada ketentuan.

7.1.8 Kualifikasi Kebijakan Sintaksis dan Semantik

Kualifikasi yang disesuaikan dengan peraturan dan fungsi dasar dari penggunaan sertifikatnya

7.1.9 Memproses Semantik untuk Ekstensi Kebijakan Sertifikat Kritis

Tidak ada ketentuan.

7.2 Profil CRL

7.2.1 Nomor Versi

CA Digisign menerbitkan CRL X.509 versi 2.

7.2.2 Ekstensi Entry CRL dan CRL CA Digisign menggunakan CRL RFC

5280 dan ekstensi entri CRL.

7.2.3 CA Digisign uses RFC 5280 CRL and CRL entry extension.

7.3 Profil OCSP

7.3.1 Nomor Versi

CA Digisign menerbitkan respon OCSP versi 1.

7.3.2 Ekstensi OCSP

Tidak ada ketentuan.

8. AUDIT KEPATUHAN DAN PENILAIAN LAINNYA

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

8.1 Frekuensi atau Keadaan Asesmen

CA Digisign menjalani audit kepatuhan berkala terhadap skema yang telah ditetapkan yang tidak kurang dari sekali setahun dan setiap terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan.

8.2 Identitas/Kualifikasi Asesor

Auditor menunjukkan kompetensi pada bidang audit kepatuhan, dan harus benar-benar memahami persyaratan CPS ini.

8.3 Hubungan Asesor dengan Badan yang Dinilai

CA Digisign memilih auditor / asesor yang independen.

8.4 Topik yang Dicakup oleh Asesmen

Audit yang dilaksanakan harus memenuhi kebutuhan dan didesuaikan dengan skema audit yang digunakan dalam asesmen.

8.5 Tindakan yang Diambil sebagai Hasil dari Kekurangan

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

8.6 Komunikasi Hasil

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada Policy Authority

9. BISNIS LAIN DAN MASALAH HUKUM

9.1 Biaya

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat

CA Digisign mengenakan biaya administrasi dalam menerbitkan atau memperbaharui Sertifikat Pemilik termasuk dalam hal penerbitan ulang sertifikat yang mengacu pada PM Kominfo Nomor 11 Tahun 2018.

9.1.2 Biaya Pengaksesan Sertifikat

CA Digisign mengenakan biaya administrasi kepada Pemilik dan Pihak Pengandal untuk mengakses repositori CA Digisign

9.1.3 Biaya Pengaksesan Informasi Pencabutan atau Status

CA Digisign dapat mengenakan biaya kepada Pemilik dan Pihak Pengandal untuk mengakses daftar pencabutan atau status informasi.

9.1.4 Biaya Layanan Lainnya

CA Digisign dapat mengenakan biaya untuk layanan tambahan lainnya

9.1.5 Kebijakan Pengembalian

CA Digisign tidak menyediakan kebijakan pengembalian biaya.

9.2 Tanggung Jawab Keuangan

9.2.1 Cakupan Asuransi

CA Digisign menjamin kerugian akibat kegagalan verifikasi sertifikat pemilik, sesuai dengan Peraturan Menteri No 11 tahun 2018 Pasal 12 huruf h

9.2.2 Jaminan Asuransi atau Garansi untuk Entitas Akhir

CA Digisign menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik sertifikat.

9.3 Kerahasiaan Informasi Bisnis

9.3.1 Cakupan Informasi Rahasia

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

- Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
- Kunci Privat Pemegang Sertifikat yang disimpan oleh CA Digisign, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
- Catatan Permohonan Sertifikat;
- Hasil penilaian kerentanan;
- Rekam jejak audit (*audit logs*) dari sistem CA Digisign
- Data aktivasi pada saat pengaktifan Kunci Privat CA Digisign sebagaimana dijabarkan pada Bagian 6.4;
- Dokumentasi bisnis proses CA Digisign termasuk dokumen Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); dan
- Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0.

9.3.2 Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia

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

9.3.3 Tanggung Jawab untuk Melindungi Informasi yang Rahasia

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

- Pelatihan atau peningkatan *awareness*
- Perjanjian kontrak pegawai
- NDA (*Non Disclosure Agreement*) dengan pegawai, pegawai outsource, dan rekanan

9.4 Privasi Informasi Pribadi

9.4.1 Rencana Privasi

CA Digisign melindungi informasi pribadi dalam kaitan dengan “Kebijakan Privasi “yang dipublikasikan dalam *web site* CA Digisign, https://repository.digisign.id

9.4.2 Informasi yang Dianggap Pribadi

CA Digisign melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi Pemilik dapat dirilis atas permintaan Pemilik.

9.4.3 Informasi yang tidak Dianggap Pribadi

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

9.4.4 Tanggung Jawab Melindungi Informasi Pribadi

CA Digisign memperlakukan seluruh informasi yang diterima dari Pendaftar yang biasanya tidak

disediakan di sertifikat sebagai informasi rahasia. Hal ini diterapkan untuk para Pendaftar baik yang Sertifikatnya berhasil diterbitkan begitu juga yang tidak berhasil diterbitkan dan ditolak.

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.

9.4.6 Pengungkapan Berdasarkan Proses Peradilan atau Administratif

CA Digisign tidak boleh 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 Intellectual Property Rights / Hak atas Kekayaan Intelektual

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

9.6 Pernyataan dan Jaminan

9.6.1 Pernyataan dan Jaminan CA

CA Digisign menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

- CA Digisign mematuhi ketentuan yang diatur dalam CPS ini,
- CA Digisign menerbitkan dan memperbarui CRL secara berkala,
- Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini,
- CA Digisign menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

9.6.2 Pernyataan dan Jaminan RA

CA Digisign tidak menerapkan RA

9.6.3 Pernyataan dan Jaminan Pelanggan/Pengguna

Pemilik Sertifikat menjamin bahwa:

- Setiap sertifikat digital yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah merupakan tanda tangan digital pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan digital dibuat;
- Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;
- Sudah melakukan review terhadap informasi dari sertifikat;
- Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di

dalam sertifikat adalah benar;

- Sertifikat Digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
- segera:
    - (a) 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
    - (b) mengajukan permohonan untuk melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai ataumenjadi tidak sesuai di dalam sertifikat tersebut
    - (c) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut;
- Akan menanggapi permohonan pemilik Digisign tentang *compromise* atau penyalahgunaan sertifikat digital;
- menyetujui dan menerima bahwa CA Digisign diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika CA Digisign menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware;*
- pengguna akhir dan bukan merupakan CA Digisign, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat Digital untuk tujuan penandatangan sertifikat digital PSrE lain.

9.6.4 Pernyataan dan Jaminan Pihak yang Mengandalkan

Pihak yang mengandalkan Sertifikat CA Digisign menjamin bahwa:

- Memliki kemampuan teknis untuk menggunakan sertifikat,
- apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh CA Digisign, pihak pengandal harus secara benar memverifikasi informasi yang tercantum di dalam sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut,
- mewajibkan Pihak Pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pihak Pengandal yang ada pada CPS ini,
- Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

9.6.5 Pernyataan dan Jaminan dari Partisipan Lain

Tidak ada ketentuan.

9.7 Pelepasan Jaminan

Digisign membuat pernyataan dalam CPS bahwa CA Digisign tidak menjamin:

- Kecuali untuk jaminan yang telah tercantum dalam CPS, kontrak perjanjian, term and condition subscriber dan relying party dan sepanjang diizinkan oleh hukum, CA Digisign mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan

tertentu,

- penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Certificate Usage)
- 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 CA Digisign

CA Digisign tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat, termasuk:

- semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
- semua kerusakan yang disebabkan oleh force majeure,
- semua kerusakan yang disebabkan oleh malware (seperti virus atau Trojans) diluar perangkat CA Digisign

9.9 Ganti Rugi

CA Digisign tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.

9.10 Syarat dan Pengakhiran

9.10.1 Syarat

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh CA Digisign melalui laman atau repositorinya.

9.10.2 Pengakhiran

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

9.10.3 Efek Pengakhiran dan Keberlangsungan

CA Digisign mengkomunikasikan kondisi, akibat dari penghentian CPS, dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui laman atau repositori.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

CA Digisign menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara digital, dalam bentuk kertas, atau email bersertifikat. CA Digisign memberikan tanda terima yang valid sebagai bukti bagi pengirim. CA Digisign harus memberi tanggapan paling lama dua puluh (20) hari kerja melalui media komunikasi yang sama.

9.12 Amandemen

9.12.1 Prosedur untuk Amandemen

CA Digisign menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Amandemen CPS dilakukan sesuai dengan prosedur persetujuan CP/CPS.

9.12.2 Periode dan Mekanisme Pemberitahuan

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

9.12.3 Keadaan Dimana OID Harus Diubah

Jika Policy Authority memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, CA Digisign akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

9.13 Provisi Penyelesaian Ketidaksepahaman

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

9.14 Hukum yang Mengatur

CPS ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat CA Digisign ataupun produk/ layanan lainnya. Termasuk apabila sertifikat CA Digisign dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia.

9.15 Kepatuhan atas Hukum yang Berlaku

CA Digisign mematuhi hukum yang berlaku di Indonesia. Para Pihak (termasuk CA, Pemilik, dan Pihak 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 dibawah CPS ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari CA Digisign.

9.16.3 Keterpisahan

Jika terdapat ketentuan dari dari CPS ini, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CPS ini selanjutnya akan ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CPS ini yang menjelaskan batasan tanggung jawab, dimaksudkan dapat dipisahkan dan bersifat independen dari ketentuan lain dan harus diberlakukan dengan sebagaimana harusnya.

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

CA Digisign dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang

terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan CA Digisign dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak CA Digisign untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CPS ini. Segala hal terkait pelepasan hak dalam pengadilan harus disampaikan secara tertulis dan ditandatangani oleh CA Digisign.

9.16.5 Keadaan Memaksa

CA Digisign tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada diluar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga. CA Digisign menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas CA Digisign.

9.17 Provisi Lain

Tidak ada ketentuan

APPENDIX A. TABLE OF ACRONYMS AND DEFINITIONS

Tabel Akronim / Table of Acronyms

Istilah / Term	Definisi / Definition
PSrE	Penyelenggara Sertifikasi Elektronik
CA	Certification Authority
CP	Certificate Policy
CP	Certificate Policy
CPS	Certification Practice Statement
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRL	Certificate Revocation List
EV	Extended Validation
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standards
FIPS	(US Government) Federal Information Processing Standards
OCSP	Online Certificate Status Protocol
OCSP	Online Certificate Status Protocol

OID	Object Identifier
OID	Object Identifier
IKP	Infrastruktur Kunci Publik
PKI	Public Key Infrastructure
RA	Registration Authority
RA	Registration Authority
RFC	Request For Comment
RFC	Request For Comment
VA	Validation Authority
VA	Validation Authority

Definisi / Definitions

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

Applicant	The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber or Subordinate CA.
Pemilik Subscriber	Individu yang merupakan subjek dari Sertifikat, telah diterbitkan Sertifikatnya A person who is the Subject of, and has been issued, a Certificate
Sertifikat Certificate	Sertifikat adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik Certificate is an electronic certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions
Sertifikat PSrE Induk Root CA Indonesia Certificate	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PSrE Induk untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh PSrE Berinduk The self-signed Certificate issued by Root CA Indonesia to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs
Sertifikat PSrE Berinduk Subordinate's Certificate	Sertifikat yang dikeluarkan oleh PSrE Induk The Certificate issued by Root CA Indonesia
Sertifikat Pemilik Subscriber's Certificate	Sertifikat yang dikeluarkan oleh PSrE Berinduk The Certificate issued by Subordinate CA
Certificate Policies Certificate Policies	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum. A set of rules that indicates the applicability of a named Certificate to a PKI implementation with common security requirements.
Certification Practice Statement Certification Practice Statement	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat One of several documents forming the governance framework in which Certificates are created, issued, managed, and used
Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh PSrE Berinduk yang menerbitkan Sertifikat

Certificate Revocation List	A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates
Certificate Signing Request Certificate Signing Request	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat A message conveying a request to have a Certificate issued
Kompromi Compromise	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif A violation of a security policy that results in loss of control over sensitive information
Extended Validation Certificate Extended Validation Certificate	Sertifikat digital yang berisi informasi yang ditentukan dalam Pedoman EV dan yang telah divalidasi sesuai dengan Pedoman tersebut A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines
Key Compromise Key Compromise	Kunci Privat dikatakan dikompromikan jika nilainya telah diungkapkan kepada orang yang tidak berkepentingan, orang yang tidak sah memiliki akses ke sana, atau ada praktek teknis yang memungkinkan orang yang tidak berwenang mendapatkan nilainya A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value
Key Generation Ceremony Key Generation Ceremony	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan, kunci privasinya ditransfer ke modul kriptografi, kunci privatnya dicadangkan, dan/atau kunci publiknya disertifikasi A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified
Object Identifier Object Identifier	A unique alphanumeric or numeric identifier yang terdaftar di bawah standar International Organization for Standardization untuk objek atau kelas objek tertentu. A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
Online Certificate Status Protocol Online Certificate	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat An online Certificate-checking protocol for providing Relying Parties with

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