CA Digisign
Certificate Policy
Penyelenggara Sertifikat Elektronik (PSrE Terdaftar)
Versi : 1.4
OID : 2.16.360.1.1.1.12.2.1.1

6 Agustus 2019
Policy Authority

Fiki Arfiandi

Lembar Catatan Review/Revisi

Tanggal	Rev	Uraian	Oleh
1 Mei 2019	1.0	Initial Release	Manajer Kebijakan
6 Agustus 2019	1.1	Perubahan Judul CP, menjadi PSrE Terdaftar	PA
6 Agustus 2019	1.2	Penghapusan Point 1.4.1 (OID)	PA
6 Agustus 2019	1.3	Pengahapusan table 1.4.1	PA
6 Agustus 2019	1.4	Penghapusan point 5.5.1	PA

DAFTAR ISI

KENDALI KEAMANAN TEKNIS

- Pembangkitan dan Instalasi Pasangan Kunci
  - Pembangkitan Pasangan Kunci
    - Pembangkitan Pasangan Kunci CA
    - Pembangkitan Pasangan Kunci Pemilik
  - Pengiriman Kunci Privat ke Pemilik
  - Pengiriman Kunci Publik ke Penerbit Sertifikat 55
  - Pengiriman Kunci Publik PSrE kepada Pihak Pengandal
  - Ukuran Kunci
  - Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik
  - Tujuan Penggunaan Kunci (pada field key usage - X509 v3)
- Kendali Kunci Private dan Kendali Teknis Modul Kriptografi
  - Kendali dan Standar Modul Kriptografi 56
  - Kendali Multi Personil (n dari m) Kunci Privat
  - Penitipan Kunci Privat
  - Backup Kunci Privat
  - Pengarsipan Kunci Privat
  - Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi
  - Penyimpanan Kunci Privat pada Modul Kriptografis
  - Metode Pengaktifan Kunci Privat
  - Metode Penonaktifan Kunci Privat
  - Metode Penghancuran Kunci Privat
  - Pemeringkatan Modul Kriptografis
- Aspek Lain dari Manajemen Pasangan Kunci
  - Pengarsipan Kunci Publik
  - Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci
- Data Aktivasi
  - Pembuatan dan Instalasi Data Aktivasi
  - Aktivasi Perlindungan Data
  - Aspek Lain dari Aktivasi Data
- Kendali Keamanan Komputer
  - Persyaratan Teknis Keamanan Komputer Spesifik
  - Peringkat Keamanan Komputer
- Kendali Teknis Siklus Hidup
  - Kendali Pengembangan Sistem
  - Kendali Manajemen Keamanan
  - Kendali Keamanan Siklus Hidup
- Kendali Keamanan Jaringan
- Stempel Waktu

PROFIL OCSP, CRL, DAN SERTIFIKAT

- Profil Sertifikat
  - Nomor Versi

Keadaan Memaksa

Provisi Lain

Appendix A. Table of Acronyms and Definitions

1. PENGANTAR

Infrastruktur Kunci Publik (IKP) Indonesia adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikat Erlektronik (PSrE) Induk. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah nomor 82 Tahun 2012 tentang Penyelenggaraan 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 ini, “Certificate Policy Penyelenggara Sertifikasi Terdaftar” (CP PSrE Terdaftar) adalah kebijakan utama yang mengatur PSrE Terdaftar. CP menetapkan persyaratan bisnis, hukum, dan teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dalam IKP Indonesia dan menyediakan layanan kepercayaan terkait untuk semua peserta IKP Indonesia. Persyaratan ini melindungi keamanan dan integritas IKP Indonesia dan terdiri atas seperangkat aturan yang berlaku secara konsisten di seluruh Indonesia, sehingga memberikan jaminan kepercayaan yang seragam di seluruh IKP Indonesia. CP bukan merupakan perjanjian hukum antara PSrE Terdaftar dan rantai kepercayaannya; melainkan kewajiban kontraktual antara PSrE Terdaftar dengan Pemohon yang ditetapkan melalui perjanjian.

Dokumen ini ditargetkan pada:

- PSrE Induk yang harus beroperasi sesuai dengan Certificate Practice Statement (CPS) dimana CPS tersebut mengacu kepada persyaratan yang tertuang di dalam CP
- PSrE Berinduk yang perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai pelanggan PSrE Induk dan bagaimana mereka dilindungi oleh PSrE Induk
- Pihak Pengandal yang perlu memahami seberapa besar kepercayaan untuk dimasukkan ke dalam sertifikat Root CA Indonesia, atau tanda tangan digital menggunakan sertifikat itu

1.1 Ringkasan

CP ini berlaku untuk hierarki IKP Indonesia dari PSrE Terdaftar yang nantinya akan Tersertifikasi dan Berinduk dan semua Sertifikat Digital yang diterbitkan baik secara langsung melalui sistem PSrE Berinduk sendiri. Tujuan dari CP ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan sertifikat PSrE Terdaftar untuk menunjukkan kepatuhan terhadap akreditasi yang diterima industri formal. Selain itu, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan pengakuan atas tanda tangan elektronik yang digunakan untuk tujuan otentikasi atau nirsangkal. PSrE Berinduk beroperasi dalam lingkup bagian UU ITE saat memberikan layanannya.

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

CPS melengkapi CP ini dan menyatakan, “bagaimana PSrE Berinduk mematuhi CP”. CPS menyediakan Pemilik dengan ringkasan proses, prosedur, dan ketentuan umum yang berlaku bahwa PSrE Berinduk (yaitu entitas yang memberikan Sertifikat Digital kepada Pemilik) akan digunakan dalam membuat dan mengelola Sertifikat Digital tersebut. Demikian juga, PSrE Berinduk membuat CPS mereka sendiri yang berlaku untuk produk dan layanan yang mereka

tawarkan.

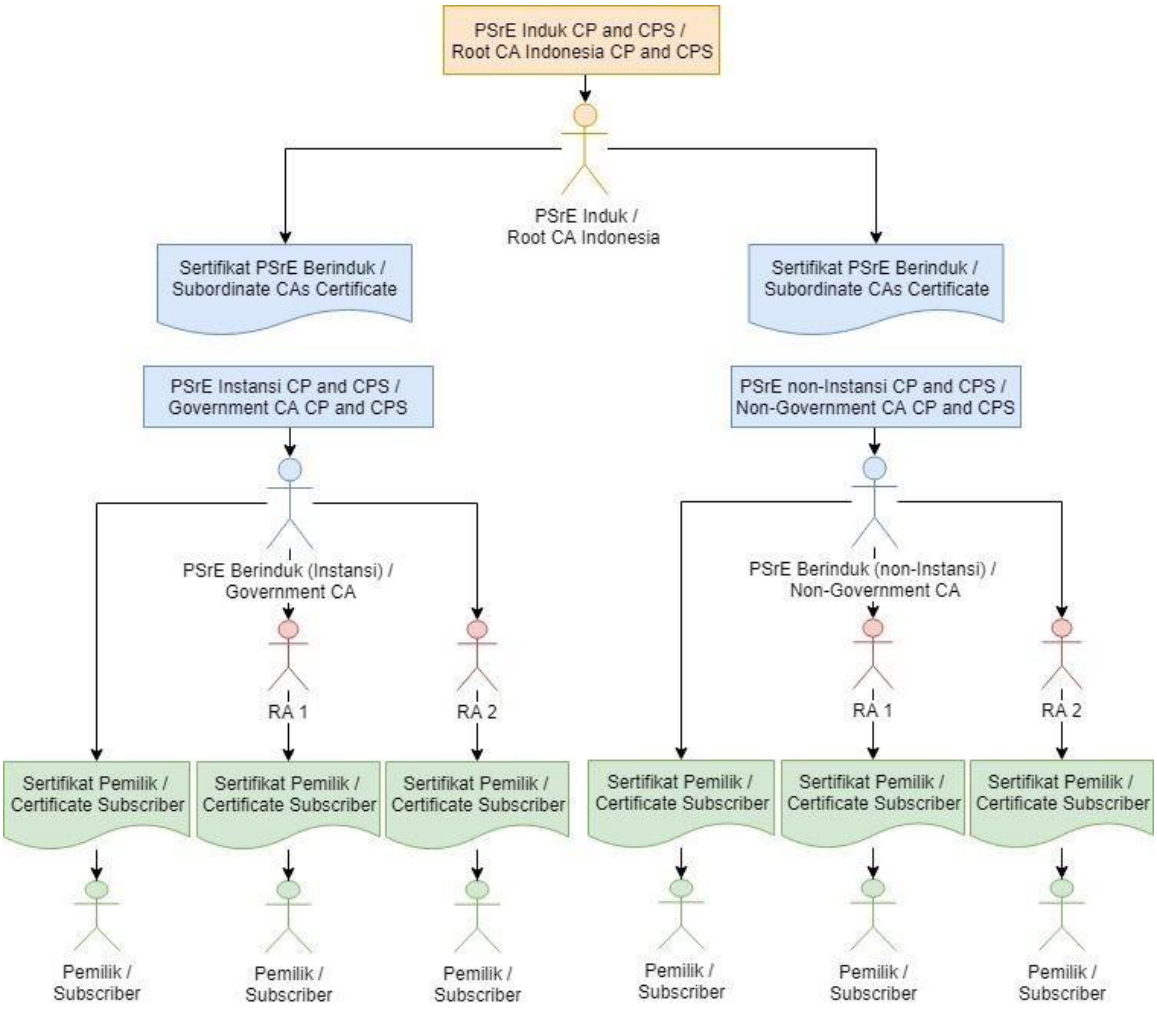

Diagram 1. Structure of the Indonesia PKI hierarchy of Root CA Indonesia

1.2 Identifikasi dan Nama Dokumen

Dokumen ini adalah dokumen CP (Certificate Policy) PSrE Terdaftar.(Digisign)

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

1. 2.16.360.1.1.1.12.2.1.1 (PSrE Terdaftar) (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 Digital PSrE Berinduk (PSrE Instansi maupun 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 CP 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 CP ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP ini.

1.3.1.2. PSrE Berinduk

PSrE Berinduk adalah PSrE 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 Non-Instansi)

PSrE Berinduk tidak boleh memiliki PSrE Berinduk di bawahnya.

1.3.2 Otoritas Pendaftaran (RA)

PSrE dapat menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan identifikasi dan autentikasi Pemilik, penerimaan permohonan dan pencabutan Sertifikat sesuai dengan yang telah didefinisikan pada CP dan dokumen terkait.

CA Digisign tidak menerapkan RA

1.3.2.1. Fungsi dari RA

RA berkewajiban untuk melaksanakan fungsi tertentu yang mengacu pada perjanjian RA, meliputi hal-hal sebagai 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
1.3.4 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.

1.3.5 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 Lists (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.

1.3.6 Partisipan Lain

PSrE menentukan Partisipan Lain yang berhubungan dengan operasional sertifikasi elektronik., yaitu penyedia layanan pusat data

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 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 jaminan rendah

b. Level 3: Sertifikat dengan Tingkat Jaminan Sedang

c. Level 4: Sertifikat dengan Tingkat Jaminan Tinggi

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

1.4.2 Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan oleh CA Digisign di bawah CP ini 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

CP dan dokumen referensinya dikelola oleh:

corpsec@digisign.id

Telepon : +62 21 31116109

1.5.2 Kontak

- Mailing Address / Alamat surat:
  Kepada PT. Solusi Net Internusa
  Jalan Jenderal Sudirman No 86 karet tengsin, tanaga abang Jakarta 10220
- Email : corpsec@diisign.id
- URL : https://www.digisign.id
- Telepon/phone : +62 21 31116109

1.5.3 Personil yang menentukan Kesesuaian CPS dengan Kebijakan

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

1.5.4 Prosedur Persetujuan CP & CPS

CA Digisign menyetujui CP/CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CP/CPS atau dengan mempublikasikan adendum. CA Digisign menentukan apakah perubahan atas CP ini membutuhkan pemberitahuan atau perubahan OID.

1.6 Definisi dan Akronim

Lihat Lampiran A untuk tabel akronim dan definisi.

2. TANGGUNGJAWAB PUBLIKASI DAN REPOSITORI

2.1 Repositori

CA Digisign bertanggung jawab memelihara repositori daring yang dapat diakses publik, berisi dokumen kebijakan, Sertifikat dari CA Digisign, dan CRL.

2.2 Publikasi Informasi Sertifikat

CA Digisign memelihara repositori yang dapat diakses melalui internet yang mempublikasikan Sertifikat dari CA Digisign, CRL terakhir, dokumen CP/CPS.

2.3 Waktu atau Frekuensi Publikasi

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

2.4 Kendali Akses pada Repositori

Informasi yang terpublikasi pada repositori adalah informasi publik. CA Digisign memberikan akses baca yang tidak dibatasi pada repositori dan harus menerapkan kendali 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. Tabel di bawah meringkas DN dari Sertifikat yang diterbitkan oleh CA Digisign di bawah CP ini.

3.1.2 Kebutuhan Nama yang Bermakna

Sertifikat yang diterbitkan sesuai dengan CP 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 resmi dari pemilik yang sah.

3.1.3 Anonimitas atau Pseudonimitas Pemilik

CA Digisign tidak menerbitkan sertifikat anonim atau pseudonim.

3.1.4 Aturan Interpretasi Berbagai Bentuk Nama

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

3.1.5 Keunikan Nama

Semua distinguished name (DN) harus unik di dalam ranah IKP Indonesia.

3.1.6 Pengakuan, Otentikasi, dan Peran Merek Dagang

Pemilik 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 Pemilik untuk memastikan penggunaan nama-nama pilihan yang sah. CA Digisign dapat menolak setiap permohonan atau melakukan pencabutan Sertifikat apapun yang menjadi bagian dari konflik merk 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 dari Identitas Organisasi

Permohonan dari organisasi untuk menjadi Pemilik harus dibuat oleh orang yang berwenang mewakili organisasi tersebut. dan menyertakan rincian tentang organisasi dan salinan surat-surat pendirian perusahaan yang dilegalisir.

CA Digisign memverifikasi identitas dan status kepegawaian dari individu yang membuat permohonan dan otoritasnya untuk menerima sertifikat untuk organisasi tersebut.

CA Digisign menyimpan dokumen dan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

3.2.3 Autentikasi dari Identitas Individu

Sebuah permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut.

CA Digisign menyimpan dokumen dan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi

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

3.2.5 Validasi Otoritas

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

3.2.6 Kriteria Inter-Operasi

Inter-Operasi IKP Indonesia tidak diizinkan.

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

3.3.1 Identifikasi dan Autentikasi untuk kegiatan Re-Key

Re-key tidak diterapkan

3.3.2 Identifikasi dan Autentikasi untuk Re-Key setelah Revokasi

Re-key tidak diterapkan

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan

Permintaan pencabutan harus selalu diautentikasi. Permintaan untuk mencabut Sertifikat dapat diautentikasi menggunakan Kunci Publik yang terhubung dengan Sertifikat, tanpa mempertimbangkan apakah Kunci Privat telah terkompromikan.

4. PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT

4.1 Permohonan Sertifikat

4.1.1 Siapa yang dapat mengajukan sebuah permohonan sertifikat

Pemohon individual dan Organisasi dapat mengajukan permohonan Sertifikat CA Digisign yang ditandatangani oleh CA Digisign,

4.1.2 Proses Pendaftaran dan TanggungJawab

CA Digisign memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat Pemohon harus memberikan informasi yang cukup sehingga memungkinkan CA Digisign untuk melakukan verifikasi atas identitas tersebut. CA Digisign melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses permohonan

Pemohon harus menyetujui kontrak berlangganan yang ditetapkan oleh CA Digisign sebelum melakukan pendaftaran

4.2 Pemrosesan Permohonan Sertifikat

4.2.1 Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi

Identifikasi dan autentikasi Pemilik harus memenuhi persyaratan yang ditentukan seperti yang tertera pada Bagian 3.2 dari CP ini. Untuk keterangan lebih rinci, harap mengacu pada CPS terkait.

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat

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

4.2.3 Waktu Pemrosesan Permohonan Sertifikat

Semua pihak yang terlibat dalam pemrosesan permohonan sertifikat harus melakukan usaha untuk memastikan permohonan sertifikat diproses tepat waktu.

4.3 Penerbitan Sertifikat

4.3.1 Tindakan CA Digisign Selama Penerbitan Sertifikat

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

4.3.2 Pemberitahuan ke Pemilik oleh CA Digisign tentang Diterbitkannya Sertifikat

CA Digisign memberitahu Pemilik dalam selang waktu yang wajar tentang berhasilnya penerbitan sertifikat sesuai dengan prosedur yang diatur dalam CPS terkait.

4.4 Penerimaan Sertifikat

4.4.1 Sikap Yang Dianggap Sebagai Menerima Sertifikat

CA Digisign memberitahu Pemilik bahwa mereka tidak dapat memakai Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

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

4.4.2 Publikasi Sertifikat Digisign

CA Digisign mempublikasikan Sertifikat dalam suatu repositori, sesuai dengan praktik publikasi sertifikat milik CA Digisign (sebagaimana didefinisikan dalam CPS), termasuk juga ketika menerbitkan informasi pencabutan terkait Sertifikat tersebut.

4.4.3 Pemberitahuan Penerbitan Sertifikat Digisign ke Entitas Lain

Tidak ada ketentuan.

4.5 Pasangan Kunci dan Penggunaan Sertifikat

4.5.1 Kunci Privat Pemilik dan Penggunaan Sertifikat

Semua Pemilik dan CA Digisign akan melindungi Kunci Privat mereka 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 patuh kepada X.509. CA Digisign menyatakan pembatasan penggunaan Sertifikat melalui ekstensi sertifikat dan harus menyatakan mekanisme untuk menentukan keabsahan sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan patuh kepada informasi ini sesuai dengan kewajiban mereka sebagai Pihak Pengandal.

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 Digisign 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 Dapat Meminta Pembaruan

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

Digisign.

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat

Suatu pembaruan sertifikat harus dilaksanakan dengan satu dari dua cara berikut:

- Proses pendaftaran awal sebagaimana diuraikan dalam bagian 3.2, atau
- Identifikasi dan autentikasi untuk re-key sebagaimana diuraikan dalam bagian 3.3, akan tetapi kunci lama juga dapat dipakai sebagai kunci baru.

4.6.4 Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Prosedur penerbitan sertifikat baru sebagaimana dinyatakan pada bagian 4.3.2.

4.6.5 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui

Pemilik dapat menerima sertifikat yang telah diperbarui sesuai dengan prosedur pendaftaran dan penerimaan sertifikat yang dinyatakan dalam bagian 4.4.1.

4.6.6 Publikasi Sertifikat yang Diperbarui oleh CA Digisign

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam bagian 4.4.2

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Lihat bagian 9.16.

4.7 Re-Key Sertifikat

4.7.1 Lingkup Re-Key Sertifikat

Penggantian kunci (re-key) sertifikat adalah penerbitan ulang suatu sertifikat yang memakai informasi subyek dan tanggal kadaluarsa yang sama (field “validTo”) namun dengan pasangan kunci yang baru.

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.2 Siapa yang Dapat Meminta Sertifikasi dari sebuah Kunci Publik Baru

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.3 Pemrosesan Permintaan Penggantian Kunci 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 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Kuncinya Digantikan

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.6 Publikasi Sertifikat yang Kuncinya Digantikan oleh CA Digisign

CA Digisign belum menerapkan penerbitan ulang kunci

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh CA Digisign ke Entitas Lain

Tidak ada aksi yang dilakukan untuk pemberitahuan atas entitas lain.

4.8 Modifikasi Sertifikat

Modifikasi detail sertifikat tidak diizinkan

4.8.1 Keadaan Bagi Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diizinkan.

4.8.2 Siapa yang Berhak Meminta Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.3 Pemrosesan Permintaan Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.4 Pemberitahuan tentang Penerbitan Sertifikat Baru ke Pemilik

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.5 Conduct Constituting Acceptance of Modified Certificate / Sikap yang Dianggap Sebagai Menerima Sertifikat yang Dimodifikasi

Modifikasi informasi sertifikat tidak diperbolehkan.

4.8.6 Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Modifikasi informasi sertifikat tidak diperbolehkan.

Modification of certificate information is not permitted.

4.8.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Modifikasi informasi sertifikat tidak diperbolehkan.

4.9 Pencabutan dan Pembekuan Sertifikat

4.9.1 Keadaan untuk Pencabutan

CA Digisign akan mencabut sertifikat Pemilik dalam keadaan berikut:

- Komponen informasi identifikasi atau afiliasi dari nama dalam sertifikat menjadi tidak valid.
- Informasi apapun dalam sertifikat menjadi tidak valid.
- Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya.
- Ada alasan untuk meyakini bahwa kunci privat telah dikompromikan/rusak.
- Pemilik atau pihak berwenang lainnya meminta sertifikatnya dicabut.
- CA Digisign berhenti beroperasi.

4.9.2 Siapa yang Dapat Meminta Pencabutan

Sertifikat dapat diminta untuk dicabut oleh Pemilik atau entitas lain yang dapat membuktikan terungkapnya kunci privat atau penyalahgunaan sertifikat sesuai dengan Kebijakan Sertifikat.

4.9.3 Prosedur Permintaan Pencabutan

CA Digisign memverifikasi identitas dan wewenang (untuk entitas penegak hukum) dari Pemilik yang mengajukan pencabutan sertifikat.

Permintaan pencabutan Sertifikat oleh entitas lain harus menyerahkan bukti bahwa:

a. privat key sertifikat telah terungkap, atau
b. penggunaan sertifikat tidak sesuai dengan Kebijakan Sertifikat, atau
c. pemilik sertifikat tidak memiliki hubungan dengan institusi

4.9.4 Masa Tenggang Permintaan Pencabutan

Tidak ada masa tenggang untuk pembatalan dalam kebijakan ini.

4.9.5 Waktu Dimana CA Digisign Harus Memproses Permintaan Pencabutan

CA Digisign memulai permintaan investigasi dalam satu (1) hari kerja kecuali dalam hal *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang cukup akan diproses sesegera mungkin.

4.9.6 Persyaratan Pemeriksaan Pencabutan bagi Pihak Pengandal

Pihak Pengandal harus memvalidasi sertifikat terhadap CRL terbaru melalui server CA

4.9.7 Frekuensi Penerbitan CRL

CRL CA Digisign diperbarui dan dipublikasi:

untuk sertifikat end-user/perangkat, setiap satu (1) hari.

4.9.8 Latensi Maksimum CRL

CA Digisign mempublikasikan CRL selambat lambatnya dalam waktu 30 (tiga puluh) Menit setelah penerbitan

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status Daring

CA Digisign memberikan layanan validasi daring, Jika validasi daring tersedia, diharapkan melakukan pengecekan menggunakan repositori yang disediakan.

4.9.10 Persyaratan Pemeriksaan Pencabutan Daring

Tidak ditentukan.

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ditentukan.

4.9.12 Kompromi Re-Key Persyaratan Khusus

Re-key tidak diterapkan

4.9.13 Keadaan untuk Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.14 Siapa yang Dapat Meminta Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.15 Prosedur Permintaan Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.16 Batas Waktu Pembekuan

Pembekuan sertifikat tidak disediakan.

4.10 Layanan Status Sertifikat

4.10.1 Karakteristik Operasional

Status sertifikat publik tersedia dari CRL di dalam repositori.

4.10.2 Ketersediaan Layanan

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

4.10.3 Fitur Opsional

Tidak ditentukan

4.11 Akhir Berlangganan

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

4.12 Pemulihan dan Penitipan Kunci

4.12.1 Kebijakan dan Praktik Pemulihan dan Penitipan Kunci

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

4.12.2 Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi

Tidak ditentukan.

5. FASILITAS, MANAJEMEN, DAN KENDALI OPERASI

5.1 Kendali Fisik

5.1.1 Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan CA Digisign maupun situs tempat workstation yang digunakan untuk mengelola CA Digisign.

5.1.2 Akses Fisik

Peralatan CA Digisign selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik untuk CA Digisign dilakukan untuk:

- Memastikan tidak ada akses ke perangkat keras tanpa izin
- Menyimpan semua media dan kertas yang berisi informasi teks polos yang sensitif dalam wadah yang aman.
- Memonitor, baik secara manual maupun elektronik, dari intrusi tanpa hak setiap saat.
- Memelihara dan secara berkala memeriksa 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 Daya dan Penyejuk Udara

CA Digisign memiliki daya cadangan yang cukup untuk mengunci masukan secara otomatis, menyelesaikan setiap tindakan yang tertunda, dan merekam status peralatan sebelum kekurangan daya atau AC menyebabkan shutdown. Repositori IKP harus dilengkapi Daya Tak Terputus dan Generator Listrik yang cukup untuk beroperasi saat tidak adanya daya komersial, untuk mendukung keberlangsungan operasional.

5.1.4 Pemaparan Air

Peralatan CA Digisign ditempatkan pada tempat yang tidak terpapar air. Paparan air untuk pencegahan kebakaran dan tindakan perlindungan (misalnya sistem sprinkler)

5.1.5 Pencegahan dan Perlindungan dari Kebakaran

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

5.1.6 Penyimpanan Media

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

Backup sistem dari CA Digisign, dimana backup tersebut cukup untuk memulihkan dari kegagalan sistem, harus dilakukan secara berkala, dan dijelaskan dalam CPS masing-masing. Backup dilakukan dan disimpan di luar lokasi tidak kurang dari sekali setiap tujuh (7) hari untuk CA Digisign. Setidaknya satu (1) salinan backup lengkap harus disimpan di lokasi di luar kantor (di lokasi yang terpisah dari peralatan CA Digisign). Hanya backup lengkap terbaru yang perlu dipertahankan. Data backup harus dilindungi dengan kendali fisik dan prosedural yang sepadan dengan operasional CA Digisign. Jarak minimal off-site backup adalah 50km.

5.2 Kendali Prosedur

5.2.1 Peran Terpercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

- Koordinator
  Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan CA Digisign
- Policy Authority
  Pembuatan, revisi dan persetujuan CP dan CPS
- 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 Dibutuhkan per Tugas

Untuk kegiatan yang memerlukan kendali multi-pihak, semua partisipan harus memegang peran terpercaya. Kendali multi-pihak harus tidak dicapai dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan tiga orang atau lebih:

- Pembangkitan kunci CA Digisign
- Penandatanganan Kunci CA Digisign
- Pencabutan Sertifikat
- CRL Generation

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran

Semua individu yang ditugaskan dalam peran terpercaya di CA Digisign diidentifikasi dan diautentikasi menggunakan akses control yang tepat

5.2.4 Peran yang Membutuhkan Pemisahan Tugas

Role yang ditidak boleh diperankan bersamaan adalah:

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

5.3 Kendali Personil Persyaratan Kualifikasi,Pengalaman, dan Clearance

Semua personil di CA Digisign Adalah warga negara Indonesia dan dipilih atas dasar keterampilan, pengalaman, kesetiaan, kepercayaan, dan integritas

5.3.1 Prosedur Pemeriksaan Latar Belakang

Semua personil di CA Digisign lulus pemeriksaan latar belakang. Lingkup pemeriksaan latar belakang mencakup area berikut:

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

- Catatan Kepolisian

5.3.2 Persyaratan Training

Semua personil CA Digisign dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan ini akan membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, dan prosedur terkait.

5.3.3 Frekuensi dan Persyaratan Training Ulang

CA Digisign memberikan penyegaran pelatihan dan pembaruan pada personilnya sejauh dan sesuai yang dibutuhkan untuk memastikan personil tersebut mempertahankan tingkat kemampuan yang dipersyaratkan untuk melakukan tanggung jawab pekerjaannya secara kompeten dan memuaskan.

5.3.4 Frekuensi dan Urutan Rotasi Pekerjaan

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

5.3.5 Sanksi untuk Tindakan Tidak Terotorisasi

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

5.3.6 Persyaratan Kontraktor Independen

Personel sub-kontraktor yang dipekerjakan untuk melakukan fungsi role yang berkaitan dengan operasional CA Digisign harus memenuhi persyaratan yang berlaku

5.3.7 Dokumentasi yang Diberikan kepada Personil

CA Digisign menyediakan kepada para personilnya Certificate Policy yang mereka gunakan, CPS, dan setiap undang-undang yang relevan, kebijakan, atau kontrak apapun. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) harus disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

5.4 Prosedur Log Audit

Berkas log audit dibuat 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 CA Digisign memastikan bahwa seluruh kegiatan yang berkaitan dari setiap tindakan Trusted Role dalam operasional CA Digisign. Seperti, type kejadian, tanggal dan waktu kejadian

5.4.2 Frekuensi Pemrosesan Log

Log audit ditinjau secara berkala. Tinjauan tersebut termasuk verifikasi bahwa log tersebut tidak dirusak atau hilang

5.4.3 Periode Retensi Log Audit

Log audit CA Digisign disimpan selama 1 (satu) tahun agar tersedia untuk pengendalian yang sah.

5.4.4 Proteksi Log Audit

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

5.4.5 Prosedur Backup Log Audit

Log audit CA Digisign di-backup. Media backup disimpan di tempat lokal pada 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 Digisign atau komponennya paling tidak sekali setahun.

5.5 Pengarsipan Record

5.5.1 Tipe Record yang Diarsipkan

Pencatatan arsip CA Digisign mencakup:

- Siklus hidup Sertifikat termasuk di dalamnya permohonan sertifikat, permintaan pencabutan sertifikat.
- Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh CA Digisign.
- Dokumen CP dan semua CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.

5.5.2 Periode Retensi Arsip

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

5.5.5 Kewajiban Pemberian Label Waktu pada Rekaman Arsip

Rekaman arsip CA Digisign diberi label waktu saat 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

Media peyimpanan informasi arsip CA Digisign diperiksa setelah dibuat. Secara berkala. Hanya yang diijinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada peran terpercaya.

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, maka Digisign akan memberitahu semua Pemilik yang mengandalkan Sertifikat CA Digisign bahwa telah terjadi perubahan.

5.7 Pemulihan Bencana dan Keadaan Terkompromi

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi

CA Digisign memiliki rencana tanggap darurat dan rencana pemulihan bencana.

Jika CA Digisign dicurigai telah terkompromi, CA Digisign akan melakukan Investigasi untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan harus dinilai untuk menentukan prosedur perbaikan yang tepat.

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

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

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

5.7.3 Prosedur Kunci Privat Entitas Terkompromi

Dalam kasus kehilangan kunci privat atau terkomprominya algoritma dan parameter yang digunakan untuk membangkitkan kunci privat dan sertifikat, semua sertifikat Pemilik/peranti yang terkait akan dicabut dan kunci-kunci serta sertifikat-sertifikat baru diterbitkan

Dalam kasus kehilangan kunci privat dari CA Digisign, semua Pemilik sertifikat akan diberitahu, semua sertifikat Pemilik yang diterbitkan dicabut, bersamaan dengan sertifikat milik CA Digisign.

Bila kunci privat CA Digisign, CA Digisign memberitahu PA dan Pihak Pengandal melalui

pengumuman publik. CA Digisign akan menghentikan layanan, memberitahu semua Pemilik, dilanjutkan 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 dimulai dengan suatu CA Digisign baru.

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana

CA Digisign harus menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbarui. 24 jam bila ada bencana.

5.8 Penutupan CA

Dalam kasus CA Digisign mengakhiri operasinya, mereka harus memberitahu ke PSrE Induk, PA, dan para Pemilik sebelum penutupan agar mematuhi Peraturan Pemerintah.

6. KENDALI KEAMANAN TEKNIS

6.1 Pembangkitan dan Instalasi Pasangan Kunci

6.1.1 Pembangkitan Pasangan Kunci

6.1.1.1. Pembangkitan Pasangan Kunci CA

Material kunci kriptografi yang digunakan oleh CA Digisign untuk menandatangani sertifikat, CRL atau informasi status harus dibuat di dalam modul kriptografi yang sesuai standar Pembangkitan pasangan kunci Pembangkitan Pasangan Kunci Pemilik Pembangkitan pasangan kunci pemilik dilakukan oleh CA Digisign dan disimpan oleh Digisign.

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 Digisign kepada Pihak Pengandal

Setiap sertifikat digital yang diterbitkan oleh CA Digisign berisi kunci publik. CA Digisign menyediakan mekanisme pengiriman secara digital (*digital delivery*) yang aman bagi semua sertifikat yang diterbitkan. Sebagai contoh, semua sertifikat dari setiap CA Digisign dipublikasikan melalui suatu situs web yang aman, yang identitasnya disertifikasi oleh penyedia SSL terpercaya.

Pada jangka waktu tertentu sebelum kunci publik CA Digisign kedaluwarsa, suatu pasangan kunci penandatanganan sertifikat yang baru akan dibangkitkan untuk menjaga operasional CA Digisign berjalan normal.

6.1.5 Ukuran Kunci

CA Digisign membuat sertifikat dan CRL di bawah policy ini harus menggunakan algoritma RSA dengan panjang kunci 2048 bit antara 4096 bit dan hash SHA-256 atau SHA-384 ketika membuat tanda tangan digital.

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 publik yang terikat pada suatu sertifikat harus disertifikasi, agar kunci publik tersebut bisa digunakan untuk autentikasi, penandatanganan, atau enkripsi, tapi tidak semua, kecuali yang sudah ditentukan oleh CA Digisign.

Kunci CA Digisign digunakan untuk penandatangan sertifikat dan CRL.

6.2 Kendali Kunci Private dan Kendali Teknis Modul Kriptografi

6.2.1 Kendali dan Standar Modul Kriptografi

CA Digisign menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 untuk operasional CA Digisign.

6.2.2 Kendali Multi Personil (n dari m) Kunci Privat

Semua kunci privat CA Digisign diakses melalui kendali multi-personil

6.2.3 Penitipan Kunci Privat

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

6.2.4 Backup Kunci Privat

Kunci privat CA Digisign 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.

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

6.2.10 Metode Penghancuran Kunci Privat

Ketika kunci privat CA Digisign tidak diperlukan lagi, para individu dalam peran terpercaya harus menghapus kunci privat dari Modul Kriptografis 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 operasional pasangan kunci didefinisikan oleh periode operasional dari sertifikat digital yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai sepuluh (10) tahun bagi CA Digisign, dan satu (1) tahun untuk sertifikat pengguna.

6.4 Data Aktivasi

6.4.1 Pembuatan dan Instalasi Data Aktivasi

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 Aktivasi Perlindungan Data

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

6.4.3 Aspek Lain dari Aktivasi Data

Tidak ditentukan.

6.5 Kendali Keamanan Komputer

6.5.1 Persyaratan Teknis Keamanan Komputer Spesifik

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

Ketika peralatan CA Digisign diwadahi dalam suatu platform terevaluasi dalam mendukung persyaratan penjaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak,

sistem operasi) harus, kalau mungkin, beroperasi dalam konfigurasi terevaluasi. Paling tidak, platform tersebut harus memakai versi yang sama dari sistem operasi komputer dengan yang menerima peringkat evaluasi.

Sistem komputer CA Digisign harus dikonfigurasi dengan akun yang diperlukan dan layanan jaringan yang minimum.

6.5.2 Peringkat Keamanan Komputer

Peringkat keamanan computer digisign telah memenuhi persyaratan keamanan yang tinggi

6.6 Kendali Teknis Siklus Hidup

6.6.1 Kendali 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 Kendali Manajemen Keamanan

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

6.6.3 Kendali Keamanan Siklus Hidup

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

6.7 Kendali Keamanan Jaringan

CA Digisign menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa mereka terjaga dari *denial of service* dan serangan intrusi.seperti penggunaan firewall dan router penyaring. Port jaringan dan layanan yang tidak dipakai harus dimatikan. Setiap perangkat lunak jaringan yang ada harus perlu bagi berfungsinya CA Digisign.

6.8 Stempel Waktu

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

- Validitas waktu permulaan untuk sebuah sertifikat CA Digisign
- Pencabutan sertifikat CA Digisign
- Pembaruan CRL, dan
- Penerbitan sertifikat pemilik dan entitas

7. PROFIL OCSP, CRL, DAN SERTIFIKAT

7.1 Profil Sertifikat

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

7.1.1 Version Number(s) / Nomor Versi

CA Digisign menerbitkan sertifikat X.509 v3 (mengisi versi field dengan integer “2”).

7.1.2 Ekstensi Sertifikat

CA Digisign memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

7.1.2.1. Key Usage / *Key Usage*

Sertifikat X.509 Versi 3 biasanya diisi sesuai dengan RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Field criticality dari ekstensi KeyUsage biasanya diisi TRUE.

7.1.2.2. Certificate Policies Extension / *Certificate Policies Extension*

Ekstensi certificatePolicies dari Sertifikat X.509 Versi 3 diisi dengan identifier objek dari CP ini sesuai dengan bagian 7.1.6 dan dengan kualifier kebijakan dari ekstensi ini harus diisi FALSE.

7.1.2.3. Basic Constraint / *Basic Constraint*

Ekstensi BasicConstraints Sertifikat X.509 Versi 3 harus memiliki field CA Digisign yang diisi TRUE. Ekstensi BasicConstraints Sertifikat Pengguna Akhir harus 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. Extended Key Usage / *Extended Key Usage*

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

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

7.1.2.5. CRL Distribution Points / *CRL Distribution Points*

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

URL harus patuh dengan persyaratan Mozilla yang tidak menyertakan protokol LDAP, dan mungkin muncul beberapa kali di dalam suatu ektensi cRLDistributionPoints.

7.1.2.6. Authority Key Identifier / *Authority Key Identifier*

Sertifikat X.509 Versi 3 biasanya diisi dengan ekstensi authorityKeyIdentifier. Metode untuk

menghasilkan keyIdentifier yang berbasis pada kunci publik dari CA Digisign, 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 / *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 Subyek Sertifikat harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.

7.1.3 Identifier Objek Algoritme

OID standar X.509v3 harus digunakan. Algoritma harus berupa enkripsi RSA untuk subject key dan SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.

7.1.4 Format Nama

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

7.1.5 Batasan Nama

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

7.1.6 Identifier Objek Kebijakan Sertifikat

Sertifikat yang diterbitkan di bawah CP ini menggunakan nomor OID Joint-ISO-ITU yang mengacu pada CA Digisign yang benar dan sesuai dengan Certificate Policy.

7.1.7 Penggunaan Ekstensi Kendala Kebijakan

Tidak ditentukan.

7.1.8 Sintaks dan Semantik Kualifier Kebijakan

Kualifikasi yang disesuaikan dengan peraturan dan fungsi dasar dari prnggunaan sertifikatnya

7.1.9 Processing Semantics for the Critical Certificate Policies Extension / Semantik Pemrosesan bagi Ekstensi Kebijakan Sertifikat Kritis

Tidak ditentukan.

7.2 Profil CRL

7.2.1 Nomor Versi

CA Digisign yang beroperasi di bawah CP ini harus menerbitkan CRL X.509 versi 2.

7.2.2 CRL dan Ekstensi Entri CRL

CA Digisign beroperasi di bawah CP ini harus menggunakan CRL dan CRL entry extension RFC 5280.

7.3 Profil OCSP

CA Digisign bisa mengoperasikan sebuah responder Online Certificate Status Protocol (OCSP) yang sesuai dengan RFC 6960 atau RFC 5019.

7.3.1 Nomor Versi

CA Digisign menerbitkan respon OCSP versi 1.

7.3.2 Ekstensi OCSP

Tidak ditentukan.

8. AUDIT KEPATUHAN DAN ASESMEN LAIN

CA Digisign menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika no 11/2018.

Semua kebijakan yang terdapat dalam CP 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 minimal sekali setahun, dan juga setiap setelah 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 ke Entitas yang Dinilai

CA Digisign memilih auditor / asesor yang independen.

8.4 Topik yang Dicakup oleh Asesmen

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

8.5 Tindakan yang Diambil sebagai Hasil dari Kekurangan

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

- Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.
- Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian harus menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CP dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan tersebut tanpa penundaan.

8.6 Komunikasi Hasil

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

8.7 Audit Internal

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

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 termasuk dalam hal penerbitan ulang sertifikat. Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat.

9.1.2 Biaya Pengaksesan Sertifikat

CA Digisign mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan.

9.1.3 Biaya Pengaksesan Informasi Status atau Pencabutan

CA Digisign mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau pencabutan sertifikat.

9.1.4 Biaya Layanan Lainnya

CA Digisign mengenakan biaya untuk mendapatkan layanan tambahan lainnya

9.1.5 Kebijakan Pengembalian Sertifikat

CA Digisign tidak menyediakan kebijakan pengembalian biaya

9.2 Tanggung Jawab Keuangan

9.2.1 Cakupan Asuransi

CA Digisign mematuhi persyaratan PM Kominfo Nomor 11 Tahun 2018 Pasal 12 huruf h.

CA Digisign menjamin kerugian akibat kegagalan verifikasi sertifikat pemilik

9.2.2 Jaminan Asuransi atau Garansi untuk Entitas Akhir

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;
- 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

CA 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 Informasi Pribadi“ yang dipublikasikan sesuai dengan ketentuan repositori

9.4.2 Informasi yang Dianggap Pribadi

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

9.4.3 Informasi tidak Dianggap Pribadi

Informasi yang termasuk dalam Bagian 7 (Sertifikat, CRL, Profil OCSP) dari CP ini tidak termasuk dalam Bagian 9.4.2.

9.4.4 Tanggung Jawab Melindungi Informasi Pribadi

CA Digisign bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan “Perlindungan Data Pribadi” secara aman. Informasi yang disimpan dapat berbentuk digital. 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.

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 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 Digisign

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

- CA Digisign mematuhi ketentuan yang diatur dalam CP ini,
- CA Digisign menerbitkan dan memperbarui CRL secara berkala,
- Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP ini,
- CA Digisign akan 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 Pemilik Sertifikat

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 CP 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 atau menjadi 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 terkait *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 CA Digisign lain.

9.6.4 Pernyataan dan Perjanjian Pihak Pengandal

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 CP ini,
- Harus mematuhi ketentuan yang ditetapkan di CP dan perjanjian lain yang terkait.

9.6.5 Pernyataan dan Jaminan Partisipan Lain

Tidak ditentukan.

9.7 Pelepasan Jaminan

CA 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 CP, 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.

9.8.2 Pembatasan Tanggung Jawab RA

RA tidak diterapkan

9.9 Ganti Rugi

9.9.1 Ganti Rugi oleh CA Digisign

Kewajiban ganti rugi CA Digisign ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat

CA Digisign menyertakan persyaratan ganti rugi untuk Pemilik Sertifikat dalam CPS dan dalam Kontrak Berlangganannya.

9.9.3 GantiRugi oleh Pihak Pengandal

CA Digisign menyertakan persyaratan ganti rugi untuk Pihak Pengandal dalam CPS.

9.10 Syarat dan Pengakhiran

9.10.1 Syarat

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

9.10.2 Pengakhiran

Perubahan CP 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 CP dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui laman atau repositori.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan

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. 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 CP ini termasuk juga keterangan waktu ketika CP efektif berlaku. Amandemen CP 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 CP ini termasuk juga keterangan waktu ketika CP efektif berlaku. Ketika terjadi perubahan, CP

harus dipublikasikan 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 / Ketentuan Penyelesaian Sengketa

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

9.14 Hukum yang Mengatur

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

Para pihak, termasuk partners CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

9.15 Kepatuhan atas Hukum yang Berlaku

CA Digisign mematuhi hukum yang berlaku di Indonesia. Para Pihak (termasuk CA Digisign, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi undang-undang dan regulasi ekspor yang berlaku di Indonesia

9.16 Ketentuan yang belum diatur

9.16.1 Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2 Pengalihan Hak

Entitas yang beroperasi dibawah CP ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari CA Digisign.

9.16.3 Keterpisahan

Jika terdapat ketentuan dari dari CP ini, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CP ini selanjutnya akan ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CP 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 PSrE 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 CP 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 CP 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 wajib 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

Istilah	Definisi
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

Istilah	Definisi
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 Applicant	Individu atau Badan Hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik atau PSrE Berinduk 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	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat

Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used
Certificate Revocation List Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh PSrE Berinduk yang menerbitkan Sertifikat 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	A unique alphanumeric or numeric identifier yang terdaftar di bawah standar International Organization for Standardization untuk objek atau kelas objek tertentu.

Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.
Online Certificate Status Protocol Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Kunci Privat Private Key	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key
Kunci Publik 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