iOTENTIK GOVERNMENT CERTIFICATION AUTHORITY	Nomor	:	KK-PSrE-001
	Versi	:	1.0
	Tanggal	:	9 Agustus 2019
	Hal	:	Certificate Policy
	OID	:	2.16.360.1.1.1.11.1

Certificate Policy

Penyelenggara Sertifikasi Elektronik (PSrE)

Badan Pengkajian dan Penerapan Teknologi (iOTENTIK)

Version 1.0

9 Agustus 2019

Digitally signed by iOTENTIK

Daftar Revisi

No.	Tanggal	Revisi	Keterangan	Oleh
1	9 Agustus 2019	1.0	Initial	Marini Wulandari

Daftar Isi

1. Pendahuluan

Badan Pengkajian dan Penerapan Teknologi melalui Balai Jaringan Informasi dan Komunikasi adalah Penyelenggara Sertifikasi Elektronik (PSrE) yang beroperasi mengacu pada Peraturan Pemerintah Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, berikut dengan segala perubahannya yang mungkin timbul di kemudian hari (untuk selanjutnya disebut "iOTENTIK"). Sebagai instansi pemerintah, PSrE merupakan penyelenggara instansi yang menerbitkan sertifikat kepada Aparatur Sipil Negara (ASN), TNI dan Polri.

Dokumen *Certificate Policy* (CP) ini mendefinisikan kebijakan utama yang mengatur iOTENTIK. CP menetapkan persyaratan bisnis, hukum, dan teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dan menyediakan layanan kepercayaan terkait untuk semua pemangku kepentingan. Persyaratan ini melindungi keamanan dan integritas iOTENTIK 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 iOTENTIK dan rantai kepercayaannya (Pemilik, Pengandal dan Partisipan Lain); melainkan kewajiban kontraktual antara iOTENTIK dengan Pemilik, Pengandal dan Partisipan Lain yang ditetapkan melalui perjanjian.

Dokumen ini ditargetkan pada:

- iOTENTIK yang harus beroperasi sesuai dengan Certificate Practice Statement (CPS) dimana CPS tersebut mengacu kepada persyaratan yang tertuang di dalam CP
- Pemilik Sertifikat Elektronik yang perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai Pelanggan iOTENTIK dan bagaimana mereka dilindungi oleh iOTENTIK
- Pihak Pengandal yang perlu memahami seberapa besar kepercayaan untuk dimasukkan ke dalam sertifikat iOTENTIK, atau tanda tangan elektronik menggunakan sertifikat itu

Dengan mengikuti kerangka pembuatan CPS sesuai format RFC 3647, beberapa judul sub bagian yang tidak berlaku ketentuannya atau belum ditentukan ketentuannya akan memiliki pernyataan "Tidak berlaku", "Tidak ada ketentuan" atau "Tidak ditetapkan."

1.1. Ringkasan

CP ini berlaku untuk semua Sertifikat Elektronik yang diterbitkan oleh PSrE BPPT. Tujuan dari CP ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan sertifikat iOTENTIK untuk menunjukkan kepatuhan terhadap akreditasi dari Kementerian Komunikasi dan Informasi. 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.

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 iOTENTIK mematuhi CP”. CPS menyediakan Pemilik dengan ringkasan proses, prosedur, dan ketentuan umum yang berlaku bahwa iOTENTIK (yaitu entitas yang memberikan Sertifikat Elektronik kepada Pemilik) akan digunakan dalam membuat dan mengelola Sertifikat Elektronik tersebut. Demikian juga, iOTENTIK membuat CPS mereka sendiri yang berlaku untuk produk dan layanan yang mereka tawarkan.

1.2. Nama Dokumen dan Identifikasi

Dokumen ini adalah dokumen CP (Certificate Policy) PSrE iOTENTIK.

Object Identifier (OID) yang digunakan untuk CP (tidak termasuk *Extended Validation Certificate*) ini adalah 2.16.360.1.1.1.11.1.

1.3. Partisipan Infrastruktur Kunci Publik (IKP)

1.3.1. *Certification Authority* (CA) / Penyelenggara Sertifikasi Elektronik (PSrE)

iOTENTIK merupakan Penyelenggara Sertifikasi Elektronik (PSrE) untuk instansi yang memiliki kewenangan sesuai dengan Peraturan Pemerintah Nomor 82 Tahun 2012 adalah sebagai berikut:

a. Melakukan pengendalian terhadap proses pendaftaran
b. Melakukan identifikasi dan autentikasi
c. Melakukan penerbitan Sertifikat
d. Melakukan Publikasi Sertifikat
e. Melakukan pembaruan masa berlaku sertifikat
f. Melakukan pencabutan sertifikat
g. Melakukan pembuatan daftar sertifikat yang aktif dan yang dibekukan.
h. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE yang diterbitkan sesuai dengan CP ini dilaksanakan sesuai dengan persyaratan, representasi dan jaminan dari CP ini.

1.3.2. Otoritas Pendaftaran / *Registration Authority* (RA)

iOTENTIK 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.

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 memperbarui sertifikat atau pembaruan kunci atas nama iOTENTIK.

1.3.2.2. Persyaratan Khusus RA untuk Sertifikat EV SSL

Tidak ada ketentuan.

1.3.3. Pemilik Sertifikat

Pemilik adalah entitas yang memohon dan berhasil mendapatkan Sertifikat Elektronik yang ditandatangani serta diterbitkan oleh iOTENTIK. Entitas Pemilik merupakan subjek pemegang Sertifikat Elektronik sekaligus entitas yang terikat dengan Perjanjian Pemilik Sertifikat iOTENTIK. Subjek sertifikat adalah pihak yang disebutkan dalam sertifikat. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat Elektronik, entitas disebut Pemohon.

1.3.4. Pihak Pengandal

Pihak Pengandal adalah entitas yang mempercayai Sertifikat Elektronik dan Tanda Tangan Elektronik yang diterbitkan oleh iOTENTIK. Pihak Pengandal harus terlebih dahulu memeriksa respon dari *Certificate Revocation Lists* (CRL) atau *Online Certificate Status Protocol* (OCSP) iOTENTIK 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 elektronik
c. Memeriksa apakah Sertifikat Elektronik termasuk di dalam CRL
d. Penyetujuan batas tanggung jawab dan jaminan

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

1.3.5. Partisipan Lain

iOTENTIK dapat menentukan Partisipan Lain yang berhubungan dengan operasional sertifikasi elektronik.

1.4. Penggunaan Sertifikat

1.4.1. Penggunaan Sertifikat yang Semestinya

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

a. Autentikasi;
b. Tanda Tangan Elektronik & Non-Repudiasi; dan
c. Enkripsi.

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 3: Sertifikat dengan Tingkat Jaminan Sedang. Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap Data identitas yang dimiliki oleh pemerintah.
b. Level 4: Sertifikat dengan Tingkat Jaminan Tinggi. Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap data identitas yang dimiliki oleh pemerintah dan data biometrik.

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

Kelas Sertifikat	**Tingkat Jaminan**			**Penggunaan**		
	Jaminan Rendah	Jaminan Sedang	Jaminan Tinggi	Autentikasi	Tanda Tangan Elektronik	Enkripsi
Sertifikat Individu						
Level 3		✓		✓	✓	✓
Level 4			✓	✓	✓	✓
Sertifikat Organisasi						
Sertifikat Organisasi			✓		✓	✓

1.4.2. Pelarangan Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan iOTENTIK ini dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

1.5. Administrasi Kebijakan / *Policy Authority* (PA)

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

a. Menetapkan Certificate Policy (CP);
b. Memastikan semua layanan, operasional, dan infrastruktur PSrE 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 referensi terkait dikelola oleh:

Telepon : 021-75791272 ext 3320

Email : iotentik@bppt.go.id

1.5.2. Kontak yang Dapat Dihubungi

Alamat surat:

Kepada iOTENTIK BPPT – Penyelenggara Sertifikasi Elektronik (PSrE) Instansi

Balai Jaringan Informasi dan Komunikasi (BJIK)

Gedung Teknologi Informasi Komunikasi dan Elektronika (Gedung 254) Lantai 3

Kawasan Puspiptek Tangerang Selatan 15314

Telepon : 021-75791272 ext 3320

Fax : 021-75791282

Email : iotentik@bppt.go.id

1.5.3. Personil yang Menentukan Kesesuaian CP dengan Kebijakan

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

1.5.4. Prosedur Persetujuan CP & CPS

iOTENTIK menyetujui CP/CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CP/CPS atau dengan mempublikasikan adendum. iOTENTIK menentukan apakah perubahan yang terjadi membutuhkan pemberitahuan atau perubahan OID.

1.6. Definisi dan Akronim

1.6.1. Definisi

Pemohon	:	Entitas yang memohon penerbitan sertifikat
Sepasang kunci	:	Kunci Privat dan terasosiasi dengan Kunci Publik
OCSP Responder	:	Aplikasi online yang dioperasikan di bawah kewenangan iOTENTIK dan terhubung dengan repositori untuk memproses permintaan status sertifikat
Kunci Privat	:	Salah satu kunci dari sepasang kunci yang dirahasiakan pemiliknya dan digunakan untuk membuat tanda tangan elektronik dan/atau melakukan deskripsi terhadap file elektronik yang dienkripsi dengan kunci publik yang sesuai.
Kunci Public	:	Salah satu kunci dari sepasang kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Privat yang sesuai. Kunci ini digunakan untuk memverifikasi tanda tangan elektronik yang dibuat oleh pemegang Kunci Privat dan atau mengenkripsi pesan sehingga dapat dibuka oleh pemegang Kunci Privat yang sesuai.

Relying Party / Pihak Pengandal	:	Suatu entitas yang dapat memanfaatkan informasi sertifikat dan tanda cap waktu dari sertifikat yang diterbitkan oleh iOTENTIK.
Pemilik	:	Entitas yang diidentifikasi sebagai subjek dalam sertifikat
Perjanjian Pemilik Sertifikat	:	Perjanjian atau suatu pakta integritas yang mengatur penerbitan dan penggunaan sertifikat oleh calon pemilik sertifikat. Calon pemilik sertifikat harus membaca dan menyetujui sebelum proses penerbitan.
RA Operator	:	Pihak yang menerima permohonan penerbitan Sertifikat Elektronik dari calon pemilik dan bertugas memverifikasi data dan kelengkapan berkas calon pemilik.
iOTENTIK	:	Penyelenggara Sertifikasi Elektronik (PSrE) Instansi yang memiliki fungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat Elektronik.
Root CA / PSrE Induk	:	Root CA dilaksanakan oleh Kementerian Komunikasi dan Informatika yang memiliki fungsi untuk memvalidasi sertifikat CA di Indonesia secara offline.

1.6.2. Akronim

CPS	Certificate Practice Statement
CP	Certificate Policy
CA	Certificate Authority
CRL	Certificate Revocation List
CSR	Certificate Signing Request
OCSP	Online Certificate Status Protocol
OID	Object Identifier
HSM	Hardware Security Module
IANA	Internet Assigned Number Authority
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
IYU-T	ITU Telecommunication Standarization Sector

PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
RFC	Request for Comment (pada IETF.org)
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TSA	Time Stamping Authority
X.509	Standar ITU-T untuk sertifikat dan otentikasi sesuai kerangka mereka

2. Publikasi dan Tanggung Jawab Repositori

2.1. Repositori

iOTENTIK bertanggung jawab mengelola repositori daring yang dapat diakses publik terkait dokumen kebijakan, Sertifikat dari iOTENTIK, dan CRL.

2.2. Publikasi Informasi Sertifikat

iOTENTIK mengelola repositori publik yang dapat diakses melalui jaringan internet yang mempublikasikan Sertifikat dari PSrE Induk dan PSrE Berinduk, CRL terakhir, dokumen CP/CPS, dan dokumen lain yang berkaitan dengan operasionalnya.

2.3. Waktu atau Frekuensi Publikasi

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

iOTENTIK harus mempublikasikan sertifikat Pemilik dan data pencabutan sertifikat dalam waktu 30 (tiga puluh) Menit setelah penerbitan.

CRL diperbarui sesuai pengaturan pada bagian 4.9.7.

2.4. Kendali Akses pada Repositori

Informasi yang terdapat pada repositori ~~publik~~ merupakan informasi publik. iOTENTIK memberikan akses *read-only/*hanya bisa baca yang tidak dibatasi pada repositori publik ini. iOTENTIK menerapkan kendali akses logis dan fisik untuk mencegah akses penulisan oleh pihak yang tidak berhak pada repositori tersebut.

Informasi yang terpublikasi pada repositori adalah informasi publik. iOTENTIK akan 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.

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

3. Identifikasi dan Autentikasi

3.1. Penamaan

3.1.1. Tipe Nama

iOTENTIK menerbitkan sertifikat dengan subjek nama yang berbeda / *Distinguished Name* (DN) yang tidak boleh kosong sesuai dengan standar ITU X.500. Berikut tabel penjelasan DN PSrE iOTENTIK dan DN pemilik sertifikat.

a. DN PSrE iOTENTIK

Atribut		Nilai
Country (C) – Negara	:	Indonesia (ID)
Organization (O)-Organisasi	:	Badan Pengkajian dan Penerapan Teknologi (BPPT)
Organizational Unit (OU)- Unit Organisasi	:	Balai Jaringan Informasi dan Komunikasi (BJIK)
Common Name (CN)-Nama Subjek Sertifikat	:	iOTENTIK CA
Email Address (E)	:	iotentik@bppt.go.id

b. DN Pemilik Sertifikat

Atribut		Nilai
Country (C) – Negara	:	Indonesia (ID)
Organization (O)-Organisasi	:	Nama Organisasi
Organizational Unit (OU)- Unit Organisasi	:	Nama Organisasi Unit
State or Province (ST)-Provinsi	:	Tidak prioritas
Locality (L)-Alamat	:	Tidak Prioritas
Common Name (CN)-Nama Subjek Sertifikat	:	Nama subjek pemilik sertifikat (Untuk keperluan pribadi) dan penambahan CN ke-2 untuk keperluan Jabatan/Unit Organisasi. 1. Individu-pribadi/perorangan → CN1: Nama subjek Hukumnya

		2. Jabatan → CN1: Nama Jabatan, CN2; Nama subjek hukum pemegang jabatan 3. Unit Organisasi → CN1: Nama Unit Organisasi, CN2: nama subjek hukum yang mewakili organisasi 4. Layanan →CN1:nama objek/domain
Email Address (E)	:	Mandatory

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. Nama yang digunakan dalam Sertifikat harus mengidentifikasi orang atau objek tersebut.

Nama subjek dan penerbit yang terkandung dalam sertifikat HARUS bermakna dalam arti bahwa iOTENTIK memiliki bukti keterkaitan yang cukup antara nama dengan entitasnya. Untuk mencapai tujuan ini, penggunaan nama harus diotorisasi oleh pemilik yang sah atau perwakilan resmi dari pemilik yang sah.

3.1.3. Anonimitas atau Nama Samaran dari Pemilik

iOTENTIK tidak boleh menerbitkan sertifikat anonim atau menggunakan nama samaran (pseudonim).

3.1.4. Aturan Interpretasi Berbagai Jenis Nama

Distinguished Name (DN) pada sertifikat diinterpretasikan menggunakan standar X.500 dan sintaks ASN.1. (Lihat RFC 2253 dan RFC 2616). Informasi lebih lanjut bagaimana X.509 *Distingushed Name* pada sertifikat diinterpretasikan sebagai *Uniform Resource Identifier* dan referensi HTTP.

3.1.5. Keunikan Nama

iOTENTIK memastikan bahwa subjek DN Pemilik Sertifikat adalah unik pada domain iOTENTIK melalui prosedur pendaftaran pemilik sertifikat. Hal ini memungkinkan pemilik memiliki dua atau lebih sertifikat dengan subjek DN yang sama dari PSrE yang berbeda.

3.1.6. Pengakuan, Autentikasi, dan Peran Merk Dagang

Pemohon sertifikat dilarang mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual orang lain. iOTENTIK tidak perlu melakukan verifikasi hak pemohon untuk penggunaan merek dagang. Pemohon bertanggung jawab untuk memastikan penggunaan nama yang dipilih sah secara hukum. iOTENTIK dapat menolak permohonan penerbitan atau melakukan pencabutan Sertifikat yang menjadi bagian dari sengketa merek dagang.

3.2. Validasi Identitas Awal

3.2.1. Metode Pembuktian Kepemilikan Kunci Privat

Metode pembuktian kepemilikan Kunci Privat harus sesuai dengan standar PKSCS #10 (CSR) atau metode kriptografi yang sepadan.

Untuk Sertifikat Pemilik, pasangan kunci dapat dibangkitkan oleh iOTENTIK, dengan syarat bahwa Kunci Privat diamankan dengan menggunakan modul kriptografis yang memenuhi persyaratan FIPS-140 level 2 dan hanya dapat diakses oleh Pemilik, dengan minimal autentikasi dua faktor.

3.2.2. Autentikasi Identitas Organisasi

Permohonan dari organisasi untuk menjadi Pemilik harus dibuat oleh orang yang berwenang mewakili organisasi tersebut. Permohonan ini harus mengikuti persyaratan seperti yang tercantum dalam CPS milik iOTENTIK.

iOTENTIK harus memverifikasi identitas dan status kepegawaian dari individu yang membuat permohonan, serta otoritasnya untuk menerima sertifikat untuk organisasi tersebut.

iOTENTIK harus menyimpan dokumen dan catatan tentang jenis dan perincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

3.2.3. Autentikasi Identitas Individu

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

iOTENTIK harus menyimpan dokumen dan catatan tentang jenis dan perincian dari identifikasi yang digunakan untuk autentikasi bagi individu setidaknya selama masa berlaku dari sertifikat yang diterbitkan.

Autentikasi identitas individu pemohon sertifikat pemilik harus sesuai dengan Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018.

3.2.4. Informasi Pemilik yang Tidak Terverifikasi

Informasi yang tidak bisa diverifikasi (meliputi informasi yang tidak disebutkan pada prosedur penerbitan sertifikat) tidak boleh 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)

Tidak ditetapkan.

3.3.1. Identifikasi dan Autentikasi dari Penggantian Kunci Secara Rutin

Tidak ditetapkan.

3.3.2. Identifikasi dan Autentikasi dari Kunci Kembali setelah Pencabutan

Tidak ditetapkan.

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 perlu mempertimbangkan apakah Kunci Privat telah dikompromikan.

Dapat dilihat pada subbab 4.9.3, tentang Prosedur Permintaan Pencabutan

4. Persyaratan Operasional Siklus Sertifikat

4.1. Permohonan Sertifikat

4.1.1. Siapa yang Dapat Mengajukan Permohonan Sertifikat

Sebagai Penyelenggara Sertifikasi Elektronik (PSrE) Instansi, maka yang dapat mengajukan permohonan Sertifikat Elektronik ke iOTENTIK adalah: setiap Aparatur Sipil Negara (ASN). anggota TNI dan Polri.

4.1.2. Proses Pendaftaran dan Tanggung Jawab

iOTENTIK harus memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat di mana Sertifikat yang dimaksud menampilkan identitas kepada Pihak Pengandal atau Pemilik. Pemohon harus memberikan informasi yang cukup sehingga memungkinkan iOTENTIK dan RA untuk melakukan verifikasi atas identitas tersebut. iOTENTIK dan RA harus melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses permohonan.

Pemohon harus menyetujui Perjanjian Pemilik yang ditetapkan oleh iOTENTIK sebelum melakukan pendaftaran.

4.2. Pemrosesan Permohonan Sertifikat

4.2.1. Melaksanakan Fungsi Identifikasi dan Autentikasi

Setelah menerima permohonan sertifikat, CA dan RA melakukan fungsi identifikasi dan autentikasi dari pengajuan permohonan sertifikat sebagaimana yang diatur pada sub bab 3.2 dari CP ini.

4.2.2. Persetujuan atau Penolakan Permohonan Sertifikat

Persetujuan permohonan sertifikat dilakukan ketika persyaratan yang ditentukan sudah sesuai, serta calon pemilik mengajukan permohonan dengan data yang sesuai. Penolakan dapat terjadi ketika terdapat kekeliruan/kesalahan calon pemilik dalam mengisi inputan data dan juga tidak memenuhi persyaratan yang sudah ditentukan.

Setelah semua pemeriksaan identitas dan atribut Pemohon, konten aplikasi untuk sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap sertifikat atau permohonannya mengandung kesalahan, iOTENTIK 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 PSrE Selama Penerbitan Sertifikat

iOTENTIK melakukan verifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan semua *field* dan ekstensi telah diisi dengan benar.

iOTENTIK harus mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, selanjutnya menerbitkan Sertifikat, dan memberikan Sertifikat ke Pemohon. iOTENTIK harus mempublikasikan Sertifikat ke suatu repositori sesuai dengan CP ini dan CPS terkait. Semua ini harus dilaksanakan secara tepat waktu, yang diuraikan pada bagian 4.2.

4.3.2. Pemberitahuan Penerbitan Sertifikat Kepada Pemilik oleh PSrE

iOTENTIK 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 Menerima Sertifikat

iOTENTIK harus 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 tiga puluh (30) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat.

Untuk penerbitan Sertifikat, iOTENTIK harus menyiapkan prosedur penerimaan yang mengindikasikan dan mendokumentasikan penerimaan atas Sertifikat yang diterbitkan.

4.4.2. Publikasi Sertifikat Oleh PSrE

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

Semua sertifikat harus dipublikasikan dalam repositori, sesuai dengan bagian 2, segera setelah diterbitkan.

4.4.3. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.5. Pasangan Kunci dan Penggunaan Sertifikat

4.5.1. Pemilik Kunci Privat dan Penggunaan Sertifikat

Baik Pemilik maupun iOTENTIK bertanggung jawab untuk melindungi Kunci Privat mereka dari penggunaan yang tidak sah, menghentikan penggunaan Kunci Privat setelah statusnya kedaluwarsa atau dicabut dan menggunakan sertifikat sesuai dengan tujuannya.

4.5.2. Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

Pihak Pengandal harus menggunakan perangkat lunak yang patuh kepada X.509. PSrE harus 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.

Pihak Pengandal harus berhati-hati ketika mengandalkan sertifikat dan harus mempertimbangkan keseluruhan keadaan dan risiko kerugian sebelum mengandalkan sertifikat. Mengandalkan tanda tangan atau sertifikat elektronik yang belum diproses sesuai dengan standar yang berlaku dapat menyebabkan risiko bagi Pihak Pengandal. Pihak Pengandal hanya bertanggung jawab atas risiko semacam itu. Dari keadaan menunjukkan bahwa diperlukan jaminan tambahan, Pihak Pengandal harus mendapatkan jaminan tersebut sebelum menggunakan sertifikat.

4.6. Pembaruan Sertifikat

4.6.1. Kondisi untuk Pembaruan Sertifikat

Pembaruan sertifikat merupakan proses pembuatan sertifikat baru yang memiliki detail yang sama dengan sertifikat yang telah dikeluarkan sebelumnya namun dengan pasangan kunci yang berbeda. Proses pembaruan sertifikat sama dengan proses *renew,* dapat dilihat pada sub bab 4.7. iOTENTIK dapat memperbarui sertifikat selama:

- Sertifikat asli yang akan diperbarui belum dicabut
- Kunci publik dari sertifikat asli belum masuk daftar hitam karena alasan apa pun
- Semua perincian dalam sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan
- iOTENTIK dapat melakukan pembaruan sertifikat yang sudah pernah diperbarui sebelumnya

4.6.2. Siapa yang Dapat Meminta Pembaruan

Pemilik yang belum pernah dicabut sertifikatnya boleh meminta pembaruan Sertifikatnya ke iOTENTIK minimal dengan waktu 30 hari sebelum masa berlaku sertifikat habis.

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat

iOTENTIK harus melakukan identifikasi dan autentikasi terhadap permohonan permintaan pembaruan.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Prosedur penerbitan sertifikat baru sebagaimana dinyatakan pada bagian 4.3.2.

4.6.5. Melakukan Penerimaan Pembaruan Sertifikat

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 Pembaruan Sertifikat oleh PSrE

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam bagian 4.4.2.

4.6.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.7. Penggantian Kunci (Re-Key)

4.7.1. Ruang Lingkup Penggantian Kunci

Tidak ada ketentuan.

4.7.2. Siapa yang Dapat Meminta Sertifikasi Kunci Publik yang Baru

Tidak ada ketentuan.

4.7.3. Pemrosesan Permintaan Penggantian Kunci Sertifikat

Tidak ada ketentuan.

4.7.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.7.5. Melakukan Penerimaan dari Penggantian Sertifikat

Tidak ada ketentuan.

4.7.6. Publikasi Penggantian Kunci oleh PSrE

Tidak ada ketentuan.

4.7.7. Pemberitahuan Penerbitan Sertifikat yang Sudah Mengalami Penggantian Kunci oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.8. Modifikasi Sertifikat

4.8.1. Keadaan untuk Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.2. Siapa yang Berhak Meminta Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3. Pemrosesan Permintaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.8.5. Melakukan Penerimaan dari Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.6. Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Tidak ada ketentuan.

4.8.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.9. Pencabutan Sertifikat

4.9.1. Kondisi untuk Pencabutan

Keadaan sertifikat akan dicabut, di antaranya:

1. Komponen informasi identifikasi atau afiliasi dari nama dalam sertifikat menjadi tidak valid
2. Informasi apa pun dalam sertifikat selain yang disebutkan dalam poin 1 (satu) menjadi tidak valid
3. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam perjanjian pemilik
4. Ada alasan untuk meyakini bahwa Kunci Privat Pemilik telah dikompromikan / rusak
5. Pemilik atau pihak berwenang lainnya meminta sertifikatnya dicabut

Sertifikat harus dicabut ketika hubungan antara subyek dan kunci publiknya yang didefinisikan dalam sertifikat sudah tidak valid lagi. Ketika hal ini terjadi sertifikat seharusnya dicabut dan diletakkan pada CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status sertifikat sampai sertifikat kedaluwarsa.

4.9.2. Siapa yang bisa meminta Pencabutan

Sertifikat dapat diminta untuk dicabut oleh Pemilik atau pihak berwenang (yang dapat membuktikan kondisi pencabutan yang disebutkan pada sub bab 4.9.1 poin 1, 2 dan 5).

4.9.3. Prosedur untuk Permintaan Pencabutan

iOTENTIK harus memverifikasi identitas dan wewenang (untuk entitas penegak hukum) dari Pemilik yang mengajukan pencabutan sertifikat. Validitas identitas Pemilik dibutuhkan sesuai dengan bagian 3.4.

Permintaan pencabutan Sertifikat oleh entitas lain harus menyerahkan bukti bahwa:

a. Kunci Privat sertifikat telah terungkap, atau
b. Penggunaan sertifikat tidak sesuai dengan Kebijakan Sertifikat, atau
c. Pemilik sertifikat tidak memiliki hubungan dengan institusi

Langkah-langkah pada proses permintaan pencabutan sertifikat dijelaskan lebih rinci dalam CPS.

4.9.4. Tenggang Waktu Pencabutan Sertifikat

Tidak ada masa tenggang dalam permintaan pencabutan yang sudah diverifikasi. iOTENTIK akan segera melakukan pencabutan sesuai dengan alasan kondisi yang ada untuk pencabutan sertifikat.

4.9.5. Jangka Waktu PSrE Harus Memproses Permintaan Pencabutan

iOTENTIK harus 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. Pemeriksaan Persyaratan Pencabutan Bagi Pihak Pengandal

Pihak Pengandal harus memvalidasi sertifikat terhadap CRL terbaru melalui server PSrE.

Pihak Pengandal harus memvalidasi sertifikat terhadap server OCSP penerbit yang relevan.

4.9.7. Frekuensi Penerbitan CRL

CRL untuk pemilik harus diterbitkan dalam waktu 24 jam semenjak sertifikat dicabut. Jika sertifikat yang tercantum pada CRL kedaluwarsa, maka mungkin akan dihapus pada penerbitan CRL selanjutnya setelah sertifikat kedaluwarsa. CRL akan berdampak dalam waktu maksimum sepuluh (7) hari.

CRL harus disimpan pada lingkungan yang dilindungi untuk menjamin integritas dan keautentikannya.

4.9.8. Latensi Maksimum untuk CRL

iOTENTIK harus mempublikasikan CRL dalam waktu 30 (tiga puluh) Menit setelah penerbitan.

4.9.9. Ketersediaan Pemeriksaan Status/Pencabutan Secara Daring

iOTENTIK memberikan layanan pengecekan informasi status sertifikat secara online melalui OCSP. Pencabutan sertifikat perlu memeriksa OCSP terlebih dahulu sebelum dilakukan eksekusi pencabutan.

4.9.10. Persyaratan Pemeriksaan Pencabutan Secara Daring

iOTENTIK melakukan pemeriksaan pencabutan secara daring dengan cara:

1. Verifikasi surat permohonan pencabutan; dan
2. Verifikasi inputan security question.

4.9.11. Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12. Persyaratan Khusus Kompromi Penggantian Kunci (Re-Key Compromise)

Tidak ada ketentuan.

4.9.13. Keadaan untuk Pembekuan

Tidak ada ketentuan.

4.9.14. Siapa yang Dapat Meminta Pembekuan

Tidak ada ketentuan.

4.9.15. Prosedur Permintaan Pembekuan

Tidak ada ketentuan.

4.9.16. Batas Waktu Pembekuan

Tidak ada ketentuan.

4.10. Layanan Status Sertifikat

4.10.1. Karakteristik Operasional

Informasi status sertifikat tersedia pada CRL dan OCSP.

4.10.2. Ketersediaan Layanan

iOTENTIK harus melakukan semua tindakan yang diperlukan untuk menjamin ketersediaan layanan validasi status sertifikat.

4.10.3. Fitur Pilihan

Tidak ditentukan.

4.11. Akhir Masa Kepemilikan

Kepemilikan Sertifikat berakhir ketika sertifikat kedaluwarsa atau pemilik mengajukan permohonan pencabutan tanpa meminta sertifikat yang baru.

4.12. Pemulihan dan Penitipan Kunci

4.12.1. Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ditentukan.

4.12.2. Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ditentukan.

5. Fasilitas, Manajemen / Pengelolaan dan Kendali Operasi

5.1 Kendali Fisik

5.1.1. Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan iOTENTIK serta tempat-tempat yang digunakan untuk mengelola PSrE, harus konsisten dengan fasilitas yang digunakan untuk menampung informasi yang bernilai tinggi dan sensitif. Lokasi dan konstruksi situs, ketika dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjagaan dan sensor intrusi, harus memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan arsip iOTENTIK.

5.1.2. Akses Fisik

Perangkat iOTENTIK akan selalu dilindungi dari akses yang tidak sah. Mekanisme keamanan secara fisik pada iOTENTIK sesuai dengan ISO 27001:2013. Mekanisme keamanan fisik untuk iOTENTIK setidaknya harus 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 iOTENTIK yang sangat penting dan memiliki risiko 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 dari fasilitas organisasi yang lain, sehingga hanya pegawai iOTENTIK yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

5.1.3. Listrik dan AC

iOTENTIK harus memiliki daya listrik 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 UPS dan Generator Listrik yang cukup untuk beroperasi paling sedikit 6 (enam) jam saat tidak adanya daya komersial, untuk mendukung keberlangsungan operasional. Pusat data iOTENTIK dilengkapi dengan sistem *air conditioning* pada *raised floor*.

5.1.4. Keterpaparan Air

Peralatan iOTENTIK dipasang di tempat di mana tidak ada bahaya terpapar air. Paparan air untuk pencegahan kebakaran dan tindakan perlindungan (misalnya sistem *sprinkler*) dikecualikan dari persyaratan ini.

5.1.5. Pencegahan dan Perlindungan dari Kebakaran

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

5.1.6. Penyimpanan Media

iOTENTIK melindungi media penyimpanan dari kerusakan akibat kecelakaan dan akses fisik yang tidak sah. Media yang berisi informasi audit, arsip, atau cadangan harus diduplikasi dan disimpan setiap hari serta dikelola terpisah dari lokasi primer fasilitas operasi data iOTENTIK.

5.1.7. Pembuangan Limbah

Semua salinan cetak yang tidak perlu dan bersifat rahasia dihancurkan di tempat sebelum dibuang. Semua media elektronik harus dimusnahkan semua datanya agar tidak dapat dipulihkan kembali datanya.

5.1.8. Backup Off-Site

Backup sistem dari iOTENTIK, di mana *backup* tersebut cukup untuk memulihkan dari kegagalan sistem, harus dilakukan secara berkala, dan dijelaskan dalam CPS masing-masing.

Backup harus dilakukan dan disimpan di luar lokasi tidak kurang dari sekali setiap tujuh (7) hari. Setidaknya satu (1) salinan *backup* lengkap harus disimpan di lokasi di luar kantor (di lokasi yang terpisah dari peralatan PSrE). Hanya *backup* lengkap terbaru yang perlu dipertahankan. Data backup harus dilindungi dengan kendali fisik dan prosedural yang sepadan dengan operasional iOTENTIK. Jarak minimal off-site *backup* adalah 50km.

5.2. Kendali Prosedur

5.2.1. Peran Terpercaya

Personil yang bertindak dalam peran yang dipercaya yaitu pengelola sistem iOTENTIK. Semua personil yang terlibat dalam peran yang dipercaya harus pegawai tetap pada iOTENTIK dan bebas konflik yang memungkinkan merugikan iOTENTIK. Fungsi yang dilakukan dalam peran ini membentuk dasar kepercayaan untuk semua penggunaan sistem iOTENTIK. Peran dipercaya pada iOTENTIK, di antaranya:

a. **Manajer PSrE**
   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan PSrE
b. **Manajer Kebijakan**
   Melakukan pembuatan, revisi dan persetujuan CP dan CPS
c. **Internal Auditor**
   Melakukan audit internal operasional PSrE
d. **Key Manager**
   Melakukan pembangkitan dan pencabutan pasangan kunci
e. **CA Administrator**
   Mengelola akses sistem CA, siklus hidup sertifikat dan persetujuan pembuatan, dan pencabutan sertifikat

f. **RA Administrator**
   Mengelola akses sistem RA, LRA, persetujuan untuk identifikasi yang dilakukan Validation Specialist
g. **Validation Specialist**
   Melakukan identifikasi pemohon, verifikasi dokumen, dan verifikasi sertifikat
h. **Repository Administrator**
   Mengelola *web pages* dan publikasi
i. **Application Developer**
   Membangun CA/RA/OCSP dan sistem lain yang relevan
j. **Operator**
   Melakukan operasi sistem CA harian, sistem backup, dan pemulihan
k. **Third-Party Operator**
   Melakukan operasi sistem CA harian, sistem backup, dan pemulihan oleh pihdak ketiga yang dikontrak oleh CA/RA
l. **Maintenance Entity**
   Mengelola HSM, Server, Sistem Operasi, S/W dan lainnya

Peran Terpercaya lainnya bisa didefinisikan dalam dokumen lain, yang menjelaskan mengenai persyaratan peran-peran tersebut pada operasional PSrE.

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 iOTENTIK
- Pembuatan Sertifikat
- Pencabutan Sertifikat
- Pembuatan CRL

5.2.3. Identifikasi dan Autentikasi untuk Setiap Peran

Semua personil dengan peran yang dipercaya harus diverifikasi dan diidentifikasi sebelum melakukan fungsi keamanan dan menjalankan sistem iOTENTIK. Identifikasi identitas personil diperiksa melalui prosedur pemeriksaan latar belakang sesuai dengan sub bab 5.3.1.

5.2.4. Peran yang Membutuhkan Pemisahan Tugas

iOTENTIK telah mendefinisikan beberapa peran pada sub bab 5.2.1, di mana setiap personil tidak memiliki dua peran secara bersamaan. Namun saat ini iOTENTIK dalam pengembangannya mendefinisikan beberapa peran dan pada kondisi tertentu terdapat SDM yang memiliki dua peran secara bersamaan.

Peran yang tidak diperbolehkan diperankan bersamaan adalah:

- CA Administrator dan Key Manager
- Policy Authority dan administrator operasional

- Internal audit dan semua peran lain
- Pengembang aplikasi dan semua peran lain

5.3. Kendali Personil

5.3.1. Persyaratan Kualifikasi, Pengalaman dan Perizinan

Setiap personil iOTENTIK yang memiliki peran dan terpercaya dipilih berdasarkan keterampilan, pengalaman, loyalitas, kepercayaan, dan integritas sesuai dengan persyaratan, yaitu bukti latar belakang serta pengalaman kerja) demi melaksanakan tanggung jawab peran yang diberikan.

5.3.2. Prosedur Pemeriksaan Latar Belakang

iOTENTIK melakukan prosedur verifikasi identitas personil sekurang-kurangnya lima (5) tahun sekali (tentatif) yang meliputi:

1. Kontak Referensi Pekerjaan (SK Penugasan);
2. Pendidikan atau sertifikasi;
3. Identifikasi Kepegawaian dan/atau Identifikasi Kependudukan (KTP); dan
4. Penilaian Prestasi Kinerja Pegawai.

Prosedur pemeriksaan latar belakang harus dijelaskan pada CPS.

5.3.3. Persyaratan Pelatihan

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

Pelatihan tersebut harus mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras, perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP ini, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil iOTENTIK harus dilakukan minimal 1 (satu) kali dalam setahun.

5.3.4. Frekuensi dan Persyaratan Pelatihan Ulang

Personil harus menjaga tingkat keterampilan yang dimiliki dengan mengikuti pelatihan yang diadakan oleh iOTENTIK agar dapat mempertahankan tingkat kemahiran dalam tanggung jawab pekerjaan secara kompeten dan memuaskan. Frekuensi dalam mengikuti pelatihan minimal 1 (satu) kali dalam setahun untuk peningkatan kompetensi.

5.3.5. Frekuensi dan Urutan Rotasi Pekerjaan

iOTENTIK harus memastikan bahwa rotasi pekerjaan tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem

5.3.6. Sanksi untuk Tindakan Tidak Terotorisasi

Sanksi terhadap personil yang melakukan tindakan yang tidak sah atau melanggar ketentuan dan kebijakan di dalam CP, CPS maupun prosedur iOTENTIK akan diberikan sanksi administratif atau disiplin sesuai tingkatan tindakannya.

5.3.7. Persyaratan Kontraktor Independen

Personel sub-kontraktor yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional iOTENTIK harus memenuhi persyaratan yang berlaku yang ditetapkan dalam CP ini.

5.3.8. Dokumentasi yang Diberikan kepada Personil

iOTENTIK memberikan dokumen pendukung bagi setiap personil baik dokumen teknis ataupun prosedural seperti CP, CPS, peraturan perundangan terkait, kebijakan, kontrak yang relevan serta *user manual* agar setiap personil dapat menjalankan perannya yang sesuai dengan sistem iOTENTIK.

5.4. Prosedur Log Audit

Berkas log audit harus dibuat untuk semua kejadian yang terkait dengan keamanan PSrE, VA, dan RA. Bila memungkinkan, log audit keamanan harus dikumpulkan secara otomatis. Bila ini tidak mungkin, suatu buku log, kertas formulir, atau mekanisme fisik lain harus dipakai. Semua log audit keamanan, elektronik dan non elektronik, harus dipertahankan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini harus dipelihara sesuai dengan bagian 5.5.2.

5.4.1. Jenis Kejadian yang Direkam

iOTENTIK mencatat segala aktivitas log sistem CA dan TSA sebagai bukti keberlangsungan sistem. Kemampuan pencatatan dapat secara otomatis atau manual. Jika secara otomatis tidak dapat dilakukan, maka iOTENTIK secara prosedur manual akan melakukan pencatatan, yang meliputi:

a. Jenis aksi
b. Tanggal dan waktu aksi
c. Identitas operator atau sistem yang melakukan aksi

Semua jenis aksi disediakan untuk auditor pada saat akan melakukan audit, aksi yang akan diaudit, yaitu:

a. Security Audit
b. Authentication to System
c. Local Data Entry
d. Remote Data Entry
e. Data Export and Output
f. Key Generation
g. Private Key Load and Output
h. Trusted Public Key Entry, Deletion, and Storage
i. Secret Key Storage
j. Private and Secret Key Export
k. Certificate Registration
l. Certificate Revocation
m. Certificate Status Change Approval and Rejection
n. CA Configuration
o. Account Administration
p. Certificate Profile Management

q. *Revocation Profile Management*
r. *Certificate Revocation List Profile Management*
s. *Time Stamping*
t. *Miscellaneous*
u. *Configuration Changes*
v. *Physical Access /Site Security*
w. *Anomalies*

5.4.2. Frekuensi Pemrosesan Log

iOTENTIK akan melakukan audit log rutin tiap satu bulan sekali. Audit tersebut meliputi verifikasi log belum rusak, tidak ada diskontinuitas, dan tidak ada data yang hilang serta tidak ada segala bentuk penyimpangan dari log. Tindakan yang diambil sebagai hasil dari tinjauan audit log ini harus didokumentasikan.

5.4.3. Periode Retensi Log Audit

Log audit disimpan secara on-site sampai dilakukan peninjauan. Periode yang dilakukan untuk penyimpanan log audit yaitu 1 (tahun) tahun sebagai bahan yang sah terhadap monitoring sebelum ditransfer ke situs cadangan.

5.4.4. Proteksi Log Audit

iOTENTIK melakukan perlindungan terhadap sistem log audit. Perlindungan yang dimaksud, dilakukan untuk memastikan bahwa:

a. Hanya petugas yang berwenang yang dapat memasuki akses ke log.
b. Hanya petugas yang berwenang yang dapat mengarsipkan audit log.
c. Log audit tidak dimodifikasi oleh siapa pun.
d. Log audit terlindungi dari kerusakan sebelum akhir periode penyimpanan audit log yang kemudian ditransfer ke situs cadangan.
e. Lokasi *off site* situs penyimpanan iOTENTIK adalah lokasi yang aman yang terpisah dari lokasi di mana data dihasilkan.
f. iOTENTIK juga membuat log catatan waktu TSA bila diperlukan sebagai bahan pembuktian hukum bahwa waktu yang dikeluarkan TSA adalah benar dan pengoperasian TSA adalah benar. Log audit TSA ini dibuat untuk keperluan audit log.

5.4.5. Prosedur Backup Log Audit

iOTENTIK memiliki prosedur salinan log audit secara *off site* tiap satu bulan sekali. Media *backup* harus disimpan secara *local* di lokasi yang aman. Salinan kedua dari log audit harus diletakkan pada tempat yang lain setiap bulan.

5.4.6. Sistem Pengumpulan Audit (Internal vs External)

iOTENTIK akan melakukan sistem koleksi audit otomatis dimulai dari *startup* sistem dan berakhir pada sistem *shutdown*. Jika sistem koleksi audit otomatis gagal dan integritas sistem atau kerahasiaan informasi yang dilindungi berisiko, maka CA administrator sistem akan memberitahu ke

tim tata kelola untuk mempertimbangkan dalam penangguhan log audit CA atau operasi RA sampai dengan masalah tersebut diperbaiki.

5.4.7. Pemberitahuan ke Subyek Penyebab Kejadian

Tidak ditentukan.

5.4.8. Asesmen Kerentanan

iOTENTIK melakukan penilaian kerentanan dari sistem CA dan sistem RA atau komponen-komponennya setiap 1 (satu) tahun sekali dan apabila dibutuhkan.

5.5. Pengarsipan Rekaman

5.5.1. Tipe Rekaman yang Diarsipkan

Catatan arsip harus cukup rinci untuk menentukan operasional iOTENTIK yang benar dan validitas sertifikat apa pun (termasuk yang dicabut atau kedaluwarsa) yang dikeluarkan oleh iOTENTIK. Berikut adalah beberapa jenis data pencatatan arsip:

- Siklus hidup Sertifikat termasuk di dalamnya permohonan sertifikat, permintaan pencabutan sertifikat, dan permintaan re-key.
- Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh iOTENTIK.
- Data konfigurasi sistem IKP
- Dokumen CP dan semua CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.
- Data Pendaftaran Pemilik Sertifikat Elektronik

5.5.2. Periode Retensi Arsip

Catatan yang diarsipkan harus disimpan setidaknya selama 10 (sepuluh) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.

5.5.3. Perlindungan Arsip

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

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. CPS atau dokumen yang diacu harus menguraikan bagaimana rekaman arsip di-backup, dan bagaimana backup arsip dikelola.

5.5.5. Kewajiban Pemberian Label Waktu pada Rekaman Arsip

Rekaman arsip iOTENTIK harus diberi label waktu saat dibuat.

5.5.6. Sistem Pengumpulan Arsip (Internal dan Eksternal)

Informasi arsip dikumpulkan internal oleh iOTENTIK.

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Media penyimpanan informasi arsip CA diperiksa setelah dibuat. Secara berkala, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya yang diizinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh Administrator Repositori.

5.6. Pergantian Kunci

Untuk meminimalkan risiko dari kondisi Kunci Privat PSrE terkompromi, Kunci Privat diperbolehkan untuk 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 kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama harus disimpan dan dilindungi.

Apabila iOTENTIK memperbarui Kunci Privat dan dengan demikian menghasilkan kunci publik baru, iOTENTIK harus memberitahu semua Pemilik yang mengandalkan Sertifikat PSrE bahwa telah terjadi perubahan.

5.7. Pemulihan Bencana dan Keadaan Terkompromi

5.7.1. Prosedur Penanganan Insiden dan Keadaan Terkompromi

iOTENTIK harus memiliki rencana tanggap darurat dan rencana pemulihan bencana.

Jika suatu PSrE dicurigai telah terkompromi, penerbitan Sertifikat oleh PSrE tersebut harus dihentikan seketika. Investigasi independen oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan harus dinilai untuk menentukan prosedur perbaikan yang tepat. Jika Kunci Privat iOTENTIK dicurigai sudah terkompromi, prosedur pada Bagian 5.7.3 harus diikuti

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

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

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

Dalam kasus kehilangan Kunci Privat dari iOTENTIK, semua Pemilik dari iOTENTIK ini diberitahu, semua sertifikat Pemilik yang diterbitkan oleh iOTENTIK yang terkompromi tersebut dicabut, bersamaan dengan sertifikat milik iOTENTIK.

Bila Kunci Privat dari PSrE Induk hilang, PSrE Induk harus memberitahu PA dan Pihak Pengandal melalui pengumuman publik. iOTENTIK HARUS 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 PSrE baru dimulai dengan suatu PSrE Induk baru.

5.7.4. Kapabilitas Keberlangsungan Bisnis Setelah Suatu Bencana

iOTENTIK harus menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbarui. Suatu pemulihan layanan secara penuh harus terlaksana dalam 24 jam bila ada bencana.

5.8. Penutupan CA atau RA

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

6. Teknik Kontrol Keamanan

6.1. Pembangkitan dan Instalasi Pasangan Kunci

6.1.1. Pembangkitan Pasangan Kunci

6.1.1.1. Pembangkitan Pasangan Kunci iOTENTIK

Material kunci kriptografi yang digunakan oleh iOTENTIK untuk menandatangani sertifikat, CRL atau informasi status harus dibuat di dalam modul kriptografi yang sesuai standar FIPS 140, atau standar lain yang setara. Kendali multi-pihak dibutuhkan untuk pembangkitan pasangan kunci PSrE, seperti yang ditentukan pada bagian 6.2.2.

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

6.1.1.2. Pembangkitan Pasangan Kunci Pemilik

Pembangkitan pasangan kunci Pemilik harus dilakukan oleh Pemilik atau iOTENTIK. Jika. iOTENTIK membangkitkan pasangan kunci untuk Pemilik, persyaratan pengiriman pasangan kunci yang dinyatakan dalam bagian 6.1.2 juga harus dipenuhi dan iOTENTIK harus membangkitkan kunci dalam suatu perangkat keras kriptografis yang tervalidasi FIPS 140.

6.1.2. Pengiriman Kunci Privat ke Pemilik

Jika Pemilik membangkitkan sendiri pasangan kuncinya, maka tidak ada kebutuhan pengiriman Kunci Privat, dan bagian ini tidak berlaku. Bila iOTENTIK membangkitkan kunci atas nama Pemilik, maka Kunci Privat harus dikirimkan secara aman kepada Pemilik. Kunci Privat dapat dikirim secara elektronik atau dikirimkan pada modul kriptografi hardware. Dalam semua kasus persyaratan berikut harus dipenuhi:

- Kunci Privat harus dilindungi terhadap aktivasi, compromise, atau perubahan selama proses pengiriman.
- Subscriber harus memberikan pernyataan penerimaan Kunci Privat.
- PSrE harus menyimpan pernyataan penerimaan Pemilik atas Kunci Privat.

6.1.3. Pengiriman Kunci Publik ke Penerbit Sertifikat

Apabila pasangan kunci dibangkitkan oleh Pemilik, kunci publik dan identitas Pemilik harus dikirimkan dengan aman (misalnya menggunakan TLS dengan algoritma dan panjang kunci yang disetujui) pada PSrE untuk penerbitan sertifikat. Mekanisme pengiriman harus menyertakan identitas Pemilik yang telah diverifikasi dan ditandatangani menggunakan Kunci Privat pemilik.

6.1.4. Pengiriman Kunci Publik iOTENTIK kepada Pihak Pengandal

Setiap sertifikat elektronik yang diterbitkan oleh iOTENTIK berisi kunci publik. iOTENTIK harus menyediakan mekanisme pengiriman secara digital (*digital delivery*) yang aman bagi semua sertifikat yang diterbitkan. Sebagai contoh, semua sertifikat dari iOTENTIK dipublikasikan melalui suatu situs web yang aman, yang identitasnya disertifikasi oleh penyedia SSL terpercaya. Pada jangka waktu tertentu sebelum kunci publik iOTENTIK kedaluwarsa, suatu pasangan kunci penandatanganan sertifikat yang baru akan dibangkitkan untuk menjaga operasional iOTENTIK berjalan normal. Penjelasan tentang publikasi dan repositori sertifikat mengacu pada Bagian 2.1.

6.1.5. Ukuran Kunci

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

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Tidak ditentukan.

6.1.7. Tujuan Penggunaan Kunci (pada *field key usage* - X.509 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 iOTENTIK. Penggunaan sebuah kunci spesifik ditentukan oleh *key usage extension* dalam sertifikat X.509.

Kunci iOTENTIK digunakan untuk penandatanganan sertifikat dan CRL.

6.2. Kendali Kunci Privat dan Kendali Teknis Modul Kriptografi

6.2.1. Kendali dan Standar Modul Kriptografi

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

6.2.2. Kendali Multi Personil (n dari m) Kunci Privat

Semua Kunci Privat iOTENTIK harus diakses melalui kendali multi-personil seperti yang ditentukan pada Bagian 5.2.2 (Sejumlah orang dibutuhkan dalam setiap tugas) dari CP ini.

6.2.3. Penitipan Kunci Privat

Kunci Privat iOTENTIK tidak boleh diwasiatkan/dititipkan (*escrow*) kepada pihak ketiga.

6.2.4. Backup Kunci Privat

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

Pemilik dapat memilih untuk melakukan backup kunci mereka, tapi backup kunci harus berada di bawah kendali Pemilik.

6.2.5. Pengarsipan Kunci Privat

Kunci Privat iOTENTIK tidak boleh diarsipkan

6.2.6. Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

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

Bila sebuah Kunci Privat akan dipindahkan dari satu modul kriptografi ke yang lain, Kunci Privat harus dienkripsi selama pemindahan. Kunci yang dipakai untuk mengenkripsi Kunci Privat harus dilindungi dengan tingkat keamanan yang sama dengan Kunci Privat.

6.2.7. Penyimpanan Kunci Privat pada Modul Kriptografi

Kunci Privat PSrE harus disimpan pada modul kriptografi FIPS 140-2, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

6.2.8. Metode Pengaktifan Kunci Privat

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

6.2.9. Metode Penonaktifan Kunci Privat

Setelah dipakai, modul kriptografi harus dinonaktifkan oleh personil yang berwenang, misalkan melalui prosedur logout manual, atau secara otomatis setelah suatu selang waktu ketidak-aktifan sebagaimana didefinisikan dalam CPS yang berlaku.

6.2.10. Metode Penghancuran Kunci Privat

Ketika Kunci Privat iOTENTIK 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.

Kejadian penghancuran Kunci Privat iOTENTIK harus dicatat ke dalam barang bukti sesuai dengan bagian 5.4.

6.2.11. Pemeringkatan Modul Kriptografi

Seperti diuraikan dalam bagian 6.2.1.

6.3. Aspek Lain dari Manajemen Pasangan Kunci

6.3.1. Pengarsipan Kunci Publik

iOTENTIK membuat arsip kunci publik sesuai dengan sub bab 5.5.

6.3.2. Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasional sertifikat yang digunakan oleh iOTENTIK didefinisikan sebagai 10 (sepuluh) tahun. Periode operasional sertifikat yang diterbitkan untuk pemilik didefinisikan sesuai dengan kesepakatan kedua belah pihak dengan minimal 1 tahun.

Periode operasional pasangan kunci didefinisikan oleh periode operasional dari sertifikat digital yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai dua puluh (20) tahun bagi PSrE Induk, sepuluh (10) tahun bagi PSrE Berinduk, dan satu (1) tahun untuk sertifikat pengguna. Periode operasional harus didefinisikan menurut ukuran kunci dan perkembangan teknologi terkini di bidang kriptografi, sehingga tingkat terbaik untuk keamanan dan efisiensi penggunaan terjamin.

6.4. Data Aktivasi

6.4.1. Pembuatan dan Instalasi Data Aktivasi

Aktivasi data 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

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

6.4.3. Aspek Lain dari Aktivasi Data

Tidak ada ketentuan.

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. iOTENTIK harus 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 iOTENTIK 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 iOTENTIK harus dikonfigurasi dengan akun yang diperlukan dan layanan jaringan yang minimum.

6.5.2. Peringkat Keamanan Komputer

Tidak ada ketentuan.

6.6. Kendali Teknis Siklus Hidup

6.6.1. Kendali Pengembangan Sistem

Tidak ada ketentuan.

6.6.2. Kendali Manajemen Keamanan

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

6.6.3. Kendali Keamanan Siklus Hidup

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

6.7. Kendali Keamanan Jaringan

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

6.8. Stempel Waktu

Semua komponen iOTENTIK 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 *time stamp* tersendiri. Waktu yang didapat dari layanan waktu di atas akan digunakan untuk menentukan waktu pada saat:

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

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

7. Sertifikat, CRL dan Profil OCSP

7.1. Profil Sertifikat

Profil sertifikat mengikuti standar RFC 5280 "Internet X.509 *Public Key Infrastructure*: *Certificate and Certificate Revocation List* (CRL) *Profile*". iOTENTIK harus melakukan review terhadap profil sertifikat secara berkala minimal setahun sekali.

7.1.1. Nomor Versi

iOTENTIK harus menerbitkan sertifikat X.509 v3 (mengisi versi field dengan integer "2").

7.1.2. Ekstensi Sertifikat

iOTENTIK harus memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

7.1.2.1. Key Usage

keyUsage yang digunakan untuk sertifikat iOTENTIK dan Pemilik ditunjukan dalam table di bawah.

Field	iOTENTIK	Pemilik
Critical	True	True
digitalSignature	False	True
nonRepudiation	False	True
keyEncipherment	False	True
dataEncipherment	False	False
keyAgreement	False	False
keyCertSign	True	False
cRLSign	True	False
encipherOnly	False	False
decipherOnly	False	False

7.1.2.2. Perluasan Kebijakan Sertifikat

Ekstensi Kebijakan Sertifikat dari Sertifikat X.509 Versi 3 diisi dengan identifier objek dari CP ini sesuai dengan bagian 7.1.6 dan dengan kualifier kebijakan yang ditentukan dalam bagian 7.1.8. Field critical dari ekstensi ini harus diisi FALSE.

7.1.2.3. Batasan Dasar

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

7.1.2.4. Key Usage yang Diperluas

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

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

Semua sertifikat Pemilik harus mengandung sebuah ekstensi extended key usage untuk tujuan bahwa sertifikat tersebut telah diterbitkan untuk end-user, dan tidak boleh memuat nilai anyEKU.

7.1.2.5. Titik Distribusi CRL

Sertifikat X.509 Versi 3 diisi dengan suatu ekstensi cRLDistributionPoints yang memuat URL dari lokasi dimana Pihak Pengandal dapat memperoleh suatu CRL untuk memeriksa status Sertifikat. Field critical 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. Pengidentifikasian Kunci Otoritas

Sertifikat X.509 Versi 3 biasanya diisi dengan ekstensi authorityKeyIdentifier. Metode untuk menghasilkan keyIdentifier yang berbasis pada kunci publik dari PSrE Penerbit, harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280. Field critical dari ekstensi ini harus diisi FALSE.

7.1.2.7. Pengidentifikasian Kunci Subjek

Bila ada dalam Sertifikat X.509 Versi 3, field critical 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. Pengidentifikasian Objek Algoritma

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. Pengidentifikasi Objek Kebijakan Sertifikat

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

7.1.7. Penggunaan Ekstensi Batasan Kebijakan

Tidak ada Ketentuan

7.1.8. Kualifikasi Kebijakan Sintaks dan Semantik

Tidak ada Ketentuan

7.1.9. Pemrosesan Semantik bagi Ekstensi Kebijakan Sertifikat Kritis

Tidak ada Ketentuan

7.2. Profil CRL

7.2.1. Nomor Versi

iOTENTIK harus menerbitkan CRL X.509 versi 2.

7.2.2. CRL dan Ekstensi Entri CRL

iOTENTIK harus menggunakan CRL dan CRL entry extension RFC 5280.

7.3. Profil OCSP

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

7.3.1. Nomor Versi

iOTENTIK harus menerbitkan respon OCSP versi 1.

7.3.2. Ekstensi OCSP

Tidak ada Ketentuan.

8. Audit Kepatuhan dan Penilaian Lainnya

iOTENTIK harus menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018.

Semua kebijakan yang terdapat dalam CP ini mencakup semua bagian yang relevan dari standar IKP yang saat ini diterapkan untuk instansi pemerintah yang membutuhkan PSrE agar bisa beroperasi.

8.1. Frekuensi atau Keadaan Asesmen

iOTENTIK harus 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.

iOTENTIK harus menjalani audit kepatuhan dan menyampaikan laporan berkala minimal sekali setahun yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2018.

8.2. Identitas/Kualifikasi Asesor

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

Auditor kepatuhan harus memiliki kualifikasi sebagai berikut:

a. Auditor harus memiliki tim asesmen independen yang qualified;
b. Auditor harus memiliki pengetahuan yang cukup tentang tanda tangan digital, sertifikat digital, X.509 versi 3 PKI Certificate Policy and Certification Practices Framework, UU ITE, PP PSTE, Peraturan Menteri Komunikasi dan Informatika nomor 11 Tahun 2018;
c. memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
d. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah;
e. menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

8.3. Hubungan Asesor ke Entitas yang Dinilai

iOTENTIK harus memilih auditor / asesor yang independen dari iOTENTIK.

8.4. Topik yang Dicakup oleh Asesmen

Audit yang dilaksanakan harus memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema

audit. Sebuah skema audit akan berlaku pada tahun berikutnya setelah PSrE mengadopsi skema yang terbaru.

8.5. Tindakan yang Diambil sebagai Hasil dari Kekurangan

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

- Auditor kepatuhan harus memberitahu Kementerian Komunikasi dan Informatika 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 sebagaimana diatur dalam bagian 8.1. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam asesmen. Selain itu, hasilnya harus dikomunikasikan seperti yang ditetapkan pada bagian 8.5 di atas.

8.7. Audit Internal

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

9. Bisnis dan Hal Hukum Lainnya

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

iOTENTIK tidak mengenakan biaya dalam menerbitkan atau memperbaharui Sertifikat Pemilik.

9.1.2. Biaya Pengaksesan Sertifikat

iOTENTIK tidak mengenakan biaya untuk mengakses sertifikat publik.

9.1.3. Biaya Pengaksesan Informasi Status atau Pencabutan

iOTENTIK tidak mengenakan biaya untuk pencabutan sertifikat dan pengecekan validitas status sertifikat melalui CRL. iOTENTIK tidak mengenakan biaya pada Pemilik untuk mengetahui status informasi sertifikat melalui OCSP.

9.1.4. Biaya Layanan Lainnya

Biaya diperkenankan ketika ada biaya untuk mengintegrasikan pemanfaatan sertifikat elektronik dengan aplikasi yang digunakan oleh instansi pemerintah.. Biaya tersebut disesuaikan dengan Peraturan Presiden Nomor 51 Tahun 2018 tentang Jenis dan Tarif atas Jenis Penerimaan Negara Bukan Pajak yang berlaku di lingkungan Badan Pengkajian dan Penerapan Teknologi.

9.1.5. Kebijakan Pengembalian

Tidak ditentukan.

9.2. Tanggung Jawab Keuangan

9.2.1. Cakupan Asuransi

Tidak ditentukan.

9.2.2. Aset Lainnya

Tidak ditentukan.

9.2.3. Jaminan Asuransi atau Garansi untuk Entitas Akhir

Tidak ditentukan.

9.3. Kerahasiaan Informasi Bisnis

9.3.1. Cakupan Informasi Rahasia

iOTENTIK 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 PSrE dan RA;

- Data aktivasi pada saat pengaktifan Kunci Privat PSrE sebagaimana dijabarkan pada Bagian 6.4;
- Dokumentasi bisnis proses PSrE 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

iOTENTIK harus 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

iOTENTIK harus melindungi informasi pribadi dalam kaitan dengan "Kebijakan Informasi Pribadi" yang dipublikasikan sesuai dengan ketentuan repositori pada Bagian 2.1.

9.4.2. Informasi yang Dianggap Pribadi

iOTENTIK harus melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan Pemilik baik terhadap iOTENTIK maupun RA. Arsip yang dikelola oleh iOTENTIK tidak boleh dirilis kecuali yang diizinkan pada Bagian 9.4.1.

9.4.3. Informasi yang Tidak dianggap Pribadi

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

9.4.4. Tanggung Jawab untuk Melindungi Informasi Pribadi

iOTENTIK bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan "Perlindungan Data Pribadi" secara aman. Informasi yang disimpan dapat berbentuk digital maupun kertas. Backup informasi pribadi harus dienkripsi setiap akan dipindahkan ke media backup.

9.4.5. Catatan dan Persetujuan untuk Memakai Informasi Pribadi

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. iOTENTIK harus mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Perjanjian Pemilik. Perjanjian Pemilik juga mencakup persetujuan penggunaan informasi lain

yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh iOTENTIK.

9.4.6. Pengungkapan Berdasarkan Proses Peradilan atau Administratif

iOTENTIK tidak boleh membuka informasi pribadi kepada pihak ketiga mana pun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, aturan dan peraturan pemerintah, atau perintah pengadilan.

9.4.7. Keadaan Lainnya Pengungkapan Informasi

Tidak ada ketentuan.

9.5. Hak atas Kekayaan Intelektual

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

9.6. Pernyataan dan Jaminan

9.6.1. Pernyataan dan Jaminan iOTENTIK

iOTENTIK menyatakan dan menjamin, sejauh yang ditentukan dalam CP, bahwa:

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

9.6.2. Pernyataan dan Jaminan RA

RA menyatakan dan menjamin, sejauh yang ditentukan dalam CP, bahwa:

- Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat;
- Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat; dan
- PSrE mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP dan dituangkan dalam perjanjian RA.

9.6.3. Pernyataan dan Jaminan Pemilik

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 kedaluwarsa 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 instruksi PSrE terkait *compromise* atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;
- menyetujui dan menerima bahwa PSrE diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika PSrE menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian *malware*;
- Pemilik merupakan pengguna akhir dan bukan merupakan PSrE, 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 Pengandal

Pihak yang mengandalkan Sertifikat iOTENTIK menjamin bahwa:

- Memiliki kemampuan teknis untuk menggunakan sertifikat,
- Apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh iOTENTIK, pihak pengandal harus secara benar memverifikasi informasi yang tercantum di dalam sertifikat sebelum digunakan dan menanggung akibat apa pun yang terjadi jika lalai dalam melakukan hal tersebut,
- Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat
- 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

iOTENTIK harus membuat pernyataan dalam CPS bahwa iOTENTIK tidak menjamin:

- Kecuali untuk jaminan yang telah tercantum dalam CPS dan kontrak perjanjian dan sepanjang diizinkan oleh hukum, PSrE mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu,
- 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 iOTENTIK

iOTENTIK 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*; dan
- Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau Trojans) di luar perangkat iOTENTIK.

9.8.2. Pembatasan Tanggung Jawab RA

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan PSrE. Secara khusus, RA bertanggung jawab atas pendaftaran pemilik sertifikat.

9.9. Ganti Rugi

9.9.1. Ganti Rugi oleh PSrE

Kewajiban ganti rugi iOTENTIK harus ditetapkan dalam CPS, Perjanjian Pemilik, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

9.9.2. Ganti Rugi oleh Pemilik Sertifikat

iOTENTIK harus menyertakan persyaratan ganti rugi untuk Pemilik Sertifikat dalam CPS dan dalam Perjanjian Pemiliknya.

9.9.3. Ganti Rugi oleh Pihak Pengandal

iOTENTIK harus 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 PSrE 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

PSrE harus 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

iOTENTIK menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara digital, dalam bentuk kertas, atau email bersertifikat. PSrE memberikan tanda terima yang valid sebagai bukti bagi pengirim. iOTENTIK harus memberi tanggapan paling lama dua puluh (20) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke PSrE harus dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CP.

9.12. Amendmen

9.12.1. Prosedur untuk Amandemen

iOTENTIK harus menerbitkan pemberitahuan di situs 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

iOTENTIK harus menerbitkan pemberitahuan di situs 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 di mana OID Harus Diubah

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

9.13. Provisi Penyelesaian Ketidaksepahaman

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CP ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara PSrE 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 iOTENTIK ataupun produk/ layanan lainnya. Termasuk apabila sertifikat iOTENTIK dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia. Para pihak, termasuk partner CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan di atas.

9.15. Kepatuhan atas Hukum yang Berlaku

CP ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat iOTENTIK ataupun produk/ layanan lainnya. Termasuk apabila sertifikat iOTENTIK 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 di atas.

9.16. Ketentuan yang Belum Diatur

9.16.1. Seluruh Perjanjian

Tidak terdapat ketentuan

9.16.2. Pengalihan Hak

Entitas yang beroperasi di bawah CP ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari iOTENTIK.

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 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)

PSrE 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 PSrE 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 PSrE.

9.16.5. Force Majeure

PSrE tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CP ini, yang disebabkan oleh hal-hal yang berada di luar 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. PSrE wajib menyediakan BCP dan DRP dengan kendali yang

9.17. Provisi Lain

Tidak ada ketentuan.