iOTENTIK GOVERNMENT CERTIFICATION AUTHORITY	Nomor	:	KK-PSrE-002
	Versi	:	1.0
	Tanggal	:	9 Agustus 2019
	Hal	:	Certificate Practice Statement
	OID	:	2.16.360.1.1.1.11.1

Certification Practice Statement

Penyelenggara Sertifikasi Elektronik (PSrE)

Badan Pengkajian dan Penerapan Teknologi (iOTENTIK)

Versi 1.0

9 Agustus 2019

Digitally signed by iOTENTIK

Daftar Revisi

No.	Tanggal	Revisi	Keterangan	Oleh
1.	9 Agustus 2016	0.1	● Penambahan konten pada sub bab 3.1.1 dan 3.1.2 (klasifikasi pribadi/jabatan/unit organisasi untuk CN) ● Update materi sub bab 5.2.3 s.d 5.3.8	Marini Wulandari
2.	23 Februari 2018	0.2	● Sub bab 1.2 OID mengacu pada PSrE Induk Indonesia ● Penambahan konten pada sub bab 1.3.2 terkait RA internal dan RA eksternal ● Penambahan konten pada sub bab 1.4.1 terkait kegunaan sertifikat (SSL dan email encryption) ● Update url repositori publik iOTENTIK menjadi : http://bit.ly/crl-iOTENTIK ● Update waktu atau frkuensi publikasi sertifikat dan data pencabutan menjadi 1 hari kerja. ● Penambahan konten pada sub bab 3.1.1 email address pada DN Pemilik menjadi mandatory dan menambahkan atribut SN(serial number) dengan nilai : NIK:Key Usage : iOTENTIK: Versi ● Penambahan konten pada sub bab 4.1.1 yaitu : penggunaan layanan publik ● Upadte istilah renew sama dengan renew ● Penghapusan konten sub bab terkait re key dan modifikasi sertifikat.	Marini Wulandari

			● Update konten sub bab 4.9.7 frekuensi penerbitan CRL 1x24 jam dengan validasi 1 hari. ● Update konten pada subbab 5.2.1 terkait pembagian peran iOTENTIK : menyesuaikan dengan webtrust. ● Update konten pada sub bab 5.4.1 terkait aktivitas log sistem CA : menghapus indikasi keberhasilan atau kegagalan. ● Update konten pada sub bab 6.3.2 terkait periode operasional sertifikat. Untuk sertifikat CA iOTENTIK 10 tahun sedangkan periode operasional Pemilik sesuai kesepakatan minimal 1 tahun. ● Update konten pada sub bab 9.1.1 terkait biaya penerbitan dan perpanjangan sertifikat : Rp. 60.000	
3.	26 Februari 2018	0.3	● Penambahan penjelasan untuk penerbitan sertifikat layanan ● Penambahan contoh SN ● Perubahan persyaratan untuk penerbitan sertifikat untuk organisasi dan individu ● Perubahan proses pendaftaran permohonan sertifikat ● Mengganti istilah re-key menjadi renew ● Pengurangan sub bab mengenai penangguhan sertifikat dan pemulihan dan wasiat kunci	Marini Wulandari

4.	9 Agustus 2019	1.0	Revisi keseluruhan isi CPS menyesuaikan dengan CPS PSrE Induk	Marini Wulandari

Daftar Isi

1. Pendahuluan

1.1. Ringkasan

iOTENTIK BPPT 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, iOTENTIK merupakan penyelenggara instansi yang menerbitkan sertifikat kepada Aparatur Sipil Negara (ASN), TNI dan Polri.

Dokumen *Certificate Practice Statement* (CPS) ini mendefinisikan keseluruhan sistem iOTENTIK. Dokumen ini juga merupakan pernyataan publik dari praktik iOTENTIK dan berfungsi untuk memberitahukan kepada semua pihak yang terlibat akan peran dan tanggung jawab mereka di iOTENTIK. Menurut kerangka IETF PKIX RFC 3647 CPS, dokumen ini dibagi menjadi 9 (Sembilan) bagian yang mencakup praktik dan prosedur untuk mengidentifikasi permohonan sertifikat, daur hidup sertifikat seperti menerbitkan dan mencabut sertifikat, dan kontrol keamanan sesuai dengan RFC IETF PKIX terkait pengelolaan fisik, personil, komponen teknis dan operasional infrastruktur iOTENTIK. 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."

1.2. Nama Dokumen dan Identifikasi

Dokumen ini adalah *Certificate Practice Statement* iOTENTIK versi 1.1. *Object Identifier* (OID) yang digunakan untuk CP 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 dicabut

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

Registration Authority (RA) merupakan otoritas pendaftaran yang melakukan identifikasi dan autentikasi identitas calon pemilik sertifikat, memulai atau meneruskan proses permohonan

pencabutan sertifikat dan menyetujui permohonan pembaharuan dan perpanjangan sertifikat. Terdapat dua kategori RA yaitu internal dan eksternal. RA internal adalah bagian dari iOTENTIK yang memiliki peran sebagai Otoritas Pendaftaran. RA eksternal adalah mitra iOTENTIK yang berperan sebagai Otoritas Pendaftaran. RA internal dan eksternal masing-masing memiliki manajer RA (biasanya 1 orang) dan RA Operator (bisa lebih dari 1 orang). Untuk menjadi RA eksternal, wajib memenuhi persyaratan yang ditentukan oleh iOTENTIK dan menyetujui perjanjian RA yang ditetapkan oleh iOTENTIK.

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 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 diterbitkan oleh iOTENTIK dan terikat dengan Perjanjian Pemilik Sertifikat iOTENTIK. Subjek sertifikat adalah pihak yang disebutkan dalam sertifikat. Sebelum dilakukan verifikasi identitas dan penerbitan sertifikat, 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 List* (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 Elektronik untuk:

a. Memeriksa tujuan penggunaan sertifikat
b. Melakukan verifikasi tanda tangan elektronik
c. Memeriksa apakah Sertifikat Elektronik termasuk di dalam CRL
b. 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

1.3.5.1. Penyedia Layanan Pusat Data

Penyedia Layanan Pusat Data adalah kelompok kerja di Balai Jaringan Komunikasi dan Informasi yang menyediakan layanan Pusat Data untuk operasional iOTENTIK.

1.4. Penggunaan Sertifikat

1.4.1. Penggunaan Sertifikat yang Semestinya

Sertifikat elektronik dapat digunakan oleh pemilik untuk semua transaksi elektronik yang memerlukan: otentikasi yang sah, enkripsi, kontrol akses, tanda tangan elektronik, SSL dan enkripsi. Pemilik dapat menggunakan salah satu atau kombinasi dari beberapa macam kegunaan sertifikat.

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

a. Autentikasi;
b. Tanda Tangan Elektronik dan 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 Sertifikat 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 dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

1.5. Administrasi Kebijakan

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

- Menetapkan *Certificate Policy* (CP);
- Memastikan semua layanan, operasional, dan infrastruktur PSrE yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan
- Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki Tingkat Jaminan yang kurang lebih setara.

1.5.1. Organisasi Pengelola Dokumen

Dokumen CPS dan dokumen terkait dikelola oleh:

Telepon : 021-75791272 ext 3320

Email : iotentik@bppt.go.id

1.5.2. Kontak yang Dapat Dihubungi

- Alamat Surat:

  Kepada iOTENTIK

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

  Kawasan Puspiptek Tangerang Selatan 15314
- Email : iotentik@bppt.go.id
- URL : http://govca.id
- Telepon : 021-75791272 ext 3320
- Fax : 021-75791282

1.5.3. Personil yang Menentukan Kesesuaian CPS dengan Kebijakan

Policy Authority (PA) menentukan kesesuaian dan penerapan CPS ini berdasarkan hasil dan rekomendasi yang diterima oleh auditor independen ataupun ahli di bidang keamanan informasi. *Policy Authority* (PA) menyesuaikan CPS ini dengan CP dan CPS PSrE Induk Indonesia, yaitu Kementerian Komunikasi dan Informatika.

1.5.4. Prosedur Persetujuan CPS

iOTENTIK menyetujui CPS dan perubahan yang telah dibuat. Perubahan CPS ini dilakukan setelah iOTENTIK mengkaji kesesuaian dengan CP. iOTENTIK akan 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 Publik	:	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.
PSrE Induk Indonesia	:	PSrE Induk Indonesia 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. Tanggung Jawab Publikasi dan Repositori

2.1. Repositori

Admin Repositori harus mengoperasikan repositori di mana dokumen kebijakan, sertifikat dari iOTENTIK, CRL dipublikasikan.

2.2. Publikasi Informasi Sertifikat

iOTENTIK mengelola repositori yang dapat diakses melalui internet, tempat publikasi sertifikat elektronik dari iOTENTIK, sertifikat iOTENTIK, CRL terakhir, dokumen CP/CPS. Repositori sah /legal terletak di https://govca.id.

2.3. Waktu atau Frekuensi Publikasi

CPS ini dan tiap perubahan selanjutnya harus dapat diakses publik dalam tujuh (7) hari kalender setelah disetujui. iOTENTIK mempublikasikan sertifikat pemilik dan data pencabutan sertifikat dalam waktu 30 (tiga puluh) menit setelah diterbitkan. CRL diperbaharui sesuai dengan 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 penulisan oleh pihak yang tidak berhak pada repositori tersebut.

iOTENTIK akan 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 akan membuat dan menandatangani Sertifikat dengan subyek nama yang berbeda / *Distinguished Name* (DN) yang tidak boleh kosong dan memenuhi 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

iOTENTIK menggunakan DN untuk mengidentifikasi entitas (seperti : perorangan, jabatan, organisasi, dan layanan/server/perangkat/objek) yang merupakan subjek pemilik sertifikat dan penerbit sertifikat. Nama subjek dan penerbit yang terdapat pada sertifikat perlu diidentifikasi dengan benar sesuai dengan pemilik sertifikat yang sah dan penerbit sertifikat. Penamaan CN pada DN akan terdefinisi sesuai dengan kegunaaan sertifikatnya dan sebagai bukti keterkaitan dengan entitasnya.

3.1.3. Anonimitas atau Nama Samaran Pemilik

iOTENTIK tidak menerbitkan sertifikat anonim atau menggunakan nama samaran.

3.1.4. Aturan Interpretasi Berbagai Bentuk 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 Merek Dagang

Pemohon sertifikat dilarang menggunakan nama yang melanggar hak kekayaan intelektual orang lain. iOTENTIK tidak memverifikasi nama pemohon untuk penggunaan merek dagang. Hal tersebut merupakan tanggung jawab pemohon 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.

iOTENTIK dilarang mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. iOTENTIK tidak memverifikasi nama pemohon untuk penggunaan merek dagang. Hal tersebut merupakan tanggung jawab pemohon untuk memastikan penggunaan nama yang dipilih sah secara hukum. iOTENTIK dapat menolak setiap permohonan atau melakukan pencabutan sertifikat apa pun 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 sesuai dengan standar PKSCS #10 atau metode kriptografi yang sepadan.

1. Pemohon menyerahkan kunci publik
2. iOTENTIK mengenkripsi *challenge code* memakai kunci publik pemohon
3. Pemohon mendekripsi *challenge code* bersamaan dengan penyerahan CSR atau
4. Pemohon menyerahkan CSR secara *offline*

3.2.2. Autentikasi Identitas Organisasi

Permohonan dari organisasi harus dibuat oleh orang yang berwenang mewakili organisasi tersebut (lihat 3.2.5). Autentikasi identitas organisasi dapat dilihat pada prosedur penerbitan sertifikat mengenai persyaratan untuk mendapatkan sertifikat, di antaranya RA Operator memeriksa:

1. Dokumen yang menyatakan organisasi tersebut.
2. Pemegang sertifikat yang mendaftarkan organisasinya harus menyertakan :
    a. Kartu Pegawai dan/atau Kartu Tanda Penduduk
    b. Surat Permohonan Penerbitan Sertifikat Elektronik
    c. SK Penugasan
    d. Formulir Permohonan Penerbitan Sertifikat Elektronik

3.2.3. Autentikasi Identitas Individu

Identifikasi dan autentikasi identitas individu yang mengajukan permintaan sertifikat harus memenuhi persyaratan di bawah ini yang akan diperiksa oleh RA operator:

1. Kartu Pegawai dan/atau Kartu Tanda Penduduk
2. Surat Permohonan Penerbitan Sertifikat Elektronik yang ditandatangani oleh atasan langsung Pemohon
3. Formulir Permohonan Penerbitan Sertifikat Elektronik

3.2.4. Informasi Pemilik yang Tidak Terverifikasi

Informasi yang tidak diverifikasi meliputi informasi yang tidak disebutkan pada prosedur penerbitan sertifikat dan tidak boleh disertakan di dalam sertifikat.

3.2.5. Validasi Otoritas

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

Sertifikat yang mencantumkan afiliasi organisasi yang eksplisit atau implisit harus diterbitkan hanya setelah memastikan pemohon memiliki otoritas untuk bertindak atas nama organisasi dalam kapasitas yang dinyatakan dengan tegas.

iOTENTIK bertanggung jawab untuk memverifikasi dan mengautentikasi perwakilan resmi seorang ahli hukum dengan memeriksa SK Penugasan.

3.2.6. Kriteria Inter-operasi

Tidak berlaku.

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

Tidak ditetapkan.

3.3.1. Identifikasi dan Autentikasi untuk Re-Key Rutin

Tidak ditetapkan.

3.3.2. Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan

Tidak ditetapkan.

3.4. Identifikasi dan Autentikasi dari Permintaan Pencabutan

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 Jawabnya

Pemohon harus bertanggung jawab untuk memberikan informasi yang akurat dalam mengisi permohonan sertifikat. Proses pendaftaran permohonan sertifikat terbagi menjadi 2 (dua), yaitu:

1. Pendaftaran online dengan verifikasi offline (tatap muka)
2. Pendaftaran offline dengan verifikasi offline (tatap muka)

Secara umum, proses pendaftaran adalah sebagai berikut:

1. Mengajukan permohonan penerbitan sertifikat elektronik dengan menyertakan persyaratan yang ditentukan
2. Menyetujui Perjanjian Pemilik

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 CPS 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.

4.2.3. Waktu Pemrosesan Permohonan Sertifikat

Permohonan sertifikat yang diajukan harus segera diproses. Apabila permohonan tidak memenuhi persyaratan maka penolakan terhadap permohonan tersebut harus disampaikan secara tertulis. Untuk permohonan yang disetujui, sertifikatnya harus diterbitkan tidak lebih dari 30 (tiga puluh) hari kerja.

4.3. Penerbitan Sertifikat

4.3.1. Tindakan PSrE Selama Penerbitan Sertifikat

iOTENTIK memverifikasi 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. 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 maksimum 8 (delapan) hari kerja tentang berhasilnya penerbitan sertifikat melalui email atau media lainnya.

4.4. Penerimaan Sertifikat

4.4.1. Sikap yang Dianggap Menerima Sertifikat

iOTENTIK harus memeriksa semua informasi sertifikat dan menandatangani Berita Acara penerimaan sertifikat elektronik sebelum menggunakan sertifikat tersebut. Ketika tidak ada keluhan dari iOTENTIK dalam jangka waktu 30 (tiga puluh) hari kerja, iOTENTIK dianggap menerima semua informasi sertifikat. Untuk penerbitan sertifikat, iOTENTIK harus menyiapkan Berita Acara Penerimaan Sertifikat yang mengindikasikan dan mendokumentasikan penerimaan atas Sertifikat yang diterbitkan.

4.4.2. Publikasi Sertifikat Oleh PSrE

Sertifikat pemilik akan dipublikasikan di repositori seperti yang tercantum/tersebut pada bagian 2.2 setelah proses penerbitan sertifikat terjadi.

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 atau pengungkapan oleh pihak lain, untuk menghentikan penggunaan kunci privat setelah statusnya kedaluwarsa atau dicabut dan untuk menggunakan sertifikat sesuai dengan tujuannya. Pihak Pengandal harus menggunakan perangkat lunak yang sesuai dengan X.509.

4.5.2. Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

iOTENTIK harus menentukan pembatasan penggunaan sertifikat melalui sertifikat ekstensi dan harus menentukan mekanisme untuk menentukan validitas sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan mengikuti/mematuhi informasi ini sesuai dengan kewajibannya sebagai pihak pengandal.

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 dan minimal dengan waktu 30 hari sebelum masa berlaku sertifikat habis.

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat

Setelah pemilik mengajukan permohonan permintaan pembaruan, iOTENTIK akan memperpanjang sertifikat dengan menggunakan pendaftaran awal seperti dijelaskan pada bagian 3.2.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Prosedur penerbitan sertifikat baru yang sama juga diikuti, seperti yang dinyatakan pada bagian 4.3.2.

4.6.5. Melakukan Penerimaan Pembaruan Sertifikat

iOTENTIK harus menerima sertifikat baru setelah prosedur penerimaan sertifikat yang sama, seperti yang dinyatakan salam bagian 4.4.1.

4.6.6. Publikasi Pembaruan Sertifikat oleh PSrE

Sesuai sub bab 4.4.2. sertifikat pemilik dipublikasikan di repositori setelah proses penerbitan sertifikat.

4.6.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak Ditentukan.

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. Melaksanakan Penerimaan dari Penggantian Sertifikat

Tidak ada ketentuan.

4.7.6. Publikasi Sertifikat 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 Dapat Meminta Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3. Pemrosesan Permintaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Tidak ada ketentuan.

4.8.5. Melakukan Penerimaan dari Sertifikat yang Dimodifikasi

Tidak ada ketentuan.

4.8.6. Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Tidak ada ketentuan.

4.8.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan.

4.9. Pencabutan Sertifikat

4.9.1. Kondisi untuk Pencabutan

iOTENTIK harus mencabut sertifikat pemilik dalam keadaan berikut:

1. Komponen informasi identifikasi atau afiliasi dari nama dalam sertifikat menjadi tidak valid.
2. Informasi apa pun menjadi tidak valid.
3. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Pemilik.
4. Ada alasan untuk meyakini bahwa kunci privat telah dikompromikan/rusak.
5. Pemilik atau pihak berwenang lainnya meminta sertifikatnya dicabut.

Sertifikat harus dicabut bila ikatan antara subjek dan kunci publik subjek yang ditentukan dalam sertifikat tidak lagi dianggap valid. Bila ini terjadi, sertifikat terkait harus dicabut dan ditempatkan di CRL. Sertifikat yang dicabut harus disertakan pada semua publikasi baru pada informasi status sertifikat sampai sertifikat kedaluwarsa.

4.9.2. Siapa yang Dapat Meminta Pencabutan

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

4.9.3. Prosedur untuk Permintaan Pencabutan

Terdapat dua kondisi pencabutan sertifikat elektronik yaitu:

a) permintaan pencabutan oleh Pemilik atau pihak berwenang dengan keadaan yang ada dengan prosedur sebagai berikut :
   1. Pemilik atau entitas lain meminta pencabutan sertifikat dengan melampirkan persyaratan permintaan pencabutan sertifikat
   2. RA Operator memverifikasi permintaan pencabutan dari pemilik
   3. RA menyetujui permintaan pencabutan sertifikat
b) pencabutan sertifikat otomatis oleh iOTENTIK dengan alasan/kondisi:
   1. Sertifikat kedaluwarsa

4.9.4. Tenggang Waktu Permintaan Pencabutan

Tidak ada tenggang waktu yang diizinkan setelah permintaan pencabutan diverifikasi. iOTENTIK akan segera melakukan pencabutan sesuai dengan alasan keadaan yang ada untuk pencabutan sertifikat.

4.9.5. Jangka Waktu PSrE Harus Memroses Permintaan Pencabutan

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

4.9.6. Persyaratan Pemeriksaan untuk Pihak Pengandal

Pihak Pengandal harus memvalidasi setiap sertifikat dibandingkan CRL terbaru, yang berada di iOTENTIK. Pihak Pengandal harus memvalidasi sertifikat yang diajukan terhadap server OCSP iOTENTIK.

4.9.7. Frekuensi Penerbitan CRL

Frekuensi penerbitan CRL untuk pemilik harus dilakukan 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 harus disimpan pada lingkungan yang dilindungi untuk menjamin integritas dan autentikasinya.

4.9.8. Latensi Maksimum untuk CRL

iOTENTIK harus mempublikasikan data pencabutan sertifikat 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 daring 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 Keterpaparan 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. Status Layanan Sertifikat

4.10.1. Karakteristik Operasional

Informasi status sertifikat tersedia pada CRL dan OCSP.

4.10.2. Ketersediaan Layanan

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

4.10.3. Fitur Pilihan

Tidak ditentukan.

4.11. Akhir Berlangganan

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

4.12. Pemulihan dan Penitipan Kunci

4.12.1. Kebijakan dan Praktik Pemulihan dan Penitipan Kunci

Tidak ada ketentuan.

4.12.2. Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi

Tidak ada ketentuan.

5. Fasilitas, Manajemen / Pengelolaan dan Kendali Operasi

5.1 Kendali Fisik

5.1.1. Lokasi dan Konstruksi

Lokasi dan konstruksi dari fasilitas penempatan peralatan iOTENTIK **serta tempat kerja jarak jauh yang digunakan** untuk mengelola iOTENTIK sesuai dengan fasilitas yang digunakan untuk menampung informasi yang sensitif dan bernilai tinggi. Lokasi dan konstruksinya, jika dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjaga dan CCTV, telah memberikan perlindungan yang kuat terhadap akses yang tidak resmi ke peralatan dan arsip iOTENTIK.

Fasilitas penempatan peralatan iOTENTIK berada di pusat data Balai Jaringan Informasi dan Komunikasi (BJIK) BPPT yang beroperasi sesuai dengan kebijakan keamanan yang dirancang untuk mendeteksi, menghalangi, dan mencegah akses tidak sah pada pusat data sesuai dengan ISO 27001:2013.

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 yang telah diimplementasikan untuk:

- Memastikan tidak ada akses tidak resmi yang diizinkan ke perangkat keras
- Menyimpan semua media dan kertas yang dapat dilepas yang berisi informasi teks biasa yang sensitif dalam wadah yang aman.
- Monitor, baik secara manual maupun elektronik, untuk gangguan yang tidak sah setiap saat.
- Menjaga dan memeriksa secara berkala log akses.

Semua operasional 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 personil iOTENTIK yang memiliki otoritas yang bisa mengakses fasilitas tersebut

5.1.3. Listrik dan AC

iOTENTIK memiliki daya cadangan yang cukup untuk me- *lockout* secara otomatis, menyelesaikan beberapa hal/tindakan yang tertunda, dan mencatat keadaan peralatan sebelum kekurangan daya atau AC yang menyebabkan peralatan mati. Repositori IKP telah dilengkapi dengan UPS dan Generator Listrik yang cukup untuk pengoperasian minimal 6 (enam) jam tanpa adanya listrik/daya dari PLN, untuk mendukung kelangsungan operasi.

5.1.4. Keterpaparan Air

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

5.1.5. Pencegahan dan Perlindungan Kebakaran

Pusat data iOTENTIK dilengkapi dengan fasilitas perlindungan dan pencegahan dari bahaya api, menggunakan FM200. Sistem perlindungan dan pencegahan api sesuai dengan ISO 27001:2013.

5.1.6. Media Penyimpanan

iOTENTIK melindungi media penyimpanan dari kerusakan akibat pencurian, akses fisik yang tidak sah, dan kecelakaan (air, api, dan elektromagnetik). *Backup file* dilakukan setiap hari, *backup file* tersebut disimpan dan dikelola terpisah dengan lokasi primer fasilitas operasi data iOTENTIK.

5.1.7. Pembuangan Limbah

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

5.1.8. Backup *Off-Site*

iOTENTIK mengelola secara rutin (1x seminggu) untuk *back up* data yang penting dan dibutuhkan pada saat terjadinya kegagalan sistem. *Backup* dilakukan secara keseluruhan sistem iOTENTIK dan disimpan di luar lokasi iOTENTIK.

5.2. Kontrol Prosedur

5.2.1. Peran yang Dipercaya

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 pihak 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 iOTENTIK.

5.2.2. Jumlah Orang yang Diperlukan per/tiap Tugas

iOTENTIK mensyaratkan bahwa setidaknya dua orang yang bertindak dalam peran yang dipercaya. Hal ini untuk mengantisipasi ketika salah satu personil yang dibebankan pada peran yang dipercaya tidak dapat melaksanakan tugasnya pada kondisi yang mendesak. Kondisi tersebut dapat didukung dengan adanya SDM yang memadai.

Bila diperlukan kontrol dari banyak pihak, semua partisipan memegang jabatan yang terpercaya. Kontrol banyak pihak tidak dapat dicapai dengan menggunakan personil yang bertugas pada Auditor Internal kecuali fungsi audit. Tugas berikut membutuhkan 3 (tiga) orang:

- 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 Memerlukan Pemisahan Tugas

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 sebagai berikut:

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

5.3.2. Prosedur Pemeriksaan Latar Belakang

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

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

iOTENTIK akan menggunakan teknik investigasi pengganti yang diizinkan oleh hukum/undang-undang yang memberikan informasi serupa secara substansial, termasuk namun tidak terbatas untuk memperoleh pemeriksaan latar belakang yang dilakukan oleh instansi pemerintah yang berlaku.

5.3.3. Persyaratan Pelatihan

iOTENTIK memberikan pelatihan keterampilan kepada seluruh personil dalam rangka mendukung keberlangsungan sistem iOTENTIK. Pelatihan membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, prosedur terkait, undang – undang / hukum dan peraturan. Pelatihan yang diadakan oleh iOTENTIK berhubungan dengan fungsi dan kinerja pekerjaan seseorang yang mencakup dan tidak terbatas pada:

1. *Public Key Infrastructure* (PKI),
2. *Software version* yang digunakan iOTENTIK,
3. Autentikasi dan verifikasi kebijakan dan prosedur,
4. *Security principals and mechanisms.*

5.3.4. Frekuensi Pelatihan Ulang dan Persyaratan

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 yang Tidak Terotorisasi

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

5.3.7. Persyaratan Kontraktor Independen

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

5.3.8. Dokumentasi yang Disediakan untuk Personil

iOTENTIK memberikan dokumen pendukung bagi setiap personil baik dokumen teknik ataupun prosedural seperti CP, CPS, peraturan perundangan yang 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 dibangkitkan untuk semua kejadian yang terkait dengan keamanan iOTENTIK, 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*

iOTENTIK harus mengaktifkan semua kapabilitas audit keamanan dari sistem operasi iOTENTIK dan RA, serta aplikasi *Certification Authority*, yang dipersyaratkan oleh CP. Oleh karena itu, sebagian besar dari kejadian yang teridentifikasi dalam tabel harus direkam secara otomatis. iOTENTIK harus memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat disimpan sedemikian rupa sehingga dapat memastikan keterlacakan setiap tindakan *Trusted Role* dalam operasional iOTENTIK.

Setiap rekaman audit minimal harus memuat poin-poin sebagai berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian yang dapat diaudit):

- Tipe kejadian,
- Nomor seri atau urutan rekaman,
- Tanggal dan waktu terjadi rekaman,
- Asal perekaman,
- Indikator sukses atau gagal jika perlu,
- Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut

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, 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 untuk Log Audit

Log audit disimpan secara *on-site* sampai dilakukan peninjauan. Periode yang dilakukan untuk penyimpanan log audit yaitu 1 (satu) 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 lokal di lokasi yang aman. Salinan kedua dari log audit dikirim ke situs lain per buulan.

5.4.6. Sistem Pengumpulan Audit (Internal vs. Eksternal)

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 *Policy Authority (PA)* 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 tiap 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 kedaluawarsa) yang dikeluarkan oleh iOTENTIK. Berikut adalah beberapa jenis pencatatan arsip:

- Siklus hidup operasi sertifikat termasuk permohonan sertifikat, dan permintaan pencabutan.
- Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh iOTENTIK
- Data konfigurasi sistem IKP
- Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini.
- Data pendaftaran Pemilik sertifikat elektronik

5.5.2. Periode Retensi Arsip

iOTENTIK melakukan penyimpanan arsip dalam masa minimal 10 tahun. Aplikasi yang digunakan untuk membaca arsip ini harus dipertahankan dalam masa penyimpanan.

5.5.3. Perlindungan Arsip

iOTENTIK akan melindungi arsip dari segala bentuk modifikasi, penghapusan, atau gangguan yang tidak sesuai dengan prosedur dan aturan. Media yang memegang catatan arsip harus dipelihara dan dilindungi sesuai aturan dari CPS ini.

5.5.4. Prosedur Backup Arsip

Prosedur backup yang memadai dan teratur harus dilakukan agar jika terjadi kehilangan atau rusaknya arsip utama, satu set lengkap salinan cadangan yang ada di lokasi terpisah akan tersedia. *Record backup* arsip dinyatakan dalam Bagian 5.5.1 dalam media *backup*.

5.5.5. Persyaratan Record Stempel Waktu

Rekaman arsip iOTENTIK diberi stempel waktu ketika dibuat.

5.5.6. Sistem Pengumpulan Arsip (Internal dan Eksternal)

Pengumpulan arsip di iOTENTIK dilakukan oleh internal Iotentik.

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Media penyimpanan untuk informasi arsip iOTENTIK diperiksa saat pembuatan. Secara berkala beberapa informasi arsip diuji untuk memeriksa keberlanjutan integritas dan *readability* dari informasi. Hanya pihak iOTENTIK yang berwenang yang dapat mengakses arsip tersebut. Permintaan untuk memperoleh dan memverifikasi informasi arsip dikoordinasikan oleh Administrator Repositori.

5.6. Pergantian Kunci

Untuk meminimalkan risiko dari kondisi Kunci Privat iOTENTIK terkompromi, Kunci Privat dapat sering 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 iOTENTIK bahwa telah terjadi perubahan.

5.7. Pemulihan Bencana dan Keadaan Terkompromi

5.7.1. Prosedur Penanganan Insiden dan Keadaan Terkompromi

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

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

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

- Memberitahu PA sesegera mungkin.
- Memastikan integritas sistem telah direstorasi sebelum mengembalikan pada operasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.
- Mengoperasikan kembali iOTENTIK, memberikan prioritas pada kemampuan untuk membangkitkan informasi status sertifikat dalam skedul penerbitan CRL.

- Bila kunci penandatanganan iOTENTIK rusak, mengoperasikan kembali PSrE Induk Indonesia secepat mungkin, memberikan prioritas ke pembangkitan pasangan kunci baru penandatanganan iOTENTIK.

5.7.3. Prosedur Kunci Privat Entitas Terkompromi

iOTENTIK dapat membangkitkan pasangan kunci baru dan menandatangani sertifikat baru jika terjadi kerusakan fisik atau bencana pada semua salinan sertifikat PSrE. iOTENTIK akan mengambil tindakan yang tepat saat kunci privat dianggap membahayakan. Tindakan yang akan dilakukan iOTENTIK, yaitu :

a. Mengumpulkan informasi terkait kejadian tersebut.
b. Menyelidiki insiden tersebut dan menentukan tingkat serta ruang lingkup.
c. Memiliki tim help desk yang menentukan dan melaporkan tindakan atau strategi yang harus diambil untuk memperbaiki masalah dan mencegah terjadinya kembali.
d. Melakukan tindakan keamanan tambahan yang sesuai seperti menghubungi penegak hukum atau pihak yang berkepentingan lainnya.
e. Memberitahu entitas yang terkait dengan sertifikat sehingga mereka dapat mencabut sertifikat.
f. Kunci privat yang digunakan untuk *time stamp* dapat diinformasikan kepada Pemilik.
g. Membuat informasi tersedia yang digunakan untuk mengidentifikasi sertifikat dan *time stamp*.
h. Memantau sistem yang sedang berjalan, melanjutkan penyelidikan, memastikan bahwa data yang masih dicatat sebagai bukti dan membuat salinan forensik dari data yang dikumpulkan.
i. Menstabilkan sistem yang sedang berjalan dan menerapkan setiap perbaikan jangka pendek yang diperlukan untuk mengembalikan sistem ke keadaan operasi normal.
j. Mempersiapkan dan mengedarkan laporan insiden serta menganalisis penyebab insiden tersebut dan kemudian mendokumentasikan.
k. Hal ini dapat menjadikan masukkan yang dapat dipelajari ke dalam solusi jangka panjang dan rencana respon kejadian.

5.7.4. Kapasitas Keberlangsungan Bisnis Setelah Suatu Bencana

iOTENTIK harus mengembangkan sebuah Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP). DRP ditinjau ulang dan diuji secara berkala (minimal setahun sekali) dan diperbaiki dan diperbaharui jika dibutuhkan. Di fasilitas utama, iOTENTIK memelihara suatu sistem daring dan sistem *offline*. Fasilitas cadangan iOTENTIK tersedia bila fasilitas utama berhenti beroperasi.

5.8. Penutupan CA atau RA

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

- Memberitahu status layanan ke pengguna yang terkena dampak

- Mencabut semua sertifikat
- Menyimpan dalam jangka panjang informasi para pemilik mengikuti perioda yang dinyatakan di sini
- Menyediakan dukungan berkelanjutan dan menjawab pertanyaan
- Menangani dengan tepat pasangan kunci iOTENTIK dan perangkat keras yang terkait

6. Kendali Keamanan Teknis

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 dibuat di dalam modul kriptografis yang sesuai standar FIPS 140, atau standar lain yang setara. Kontrol multi-pihak dibutuhkan untuk pembangkitan pasangan kunci PSrE Induk Indonesia, 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 diikuti. Pemisahan peran yang tepat atas proses pembuatan kunci didokumentasikan di dalam dokumen internal iOTENTIK.

6.1.1.2. Pembangkitan Pasangan Kunci Pemilik

Pembangkitan pasangan kunci Pemilik harus dilakukan oleh Pemilik menggunakan aplikasi yang dikembangkan oleh 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.

Jika iOTENTIK membangkitkan kunci atas nama Pemilik pada HSM milik iOTENTIK, maka kunci privat harus disimpan secara aman di server iOTENTIK. Kunci privat dapat juga dikirim secara elektronik.

Dalam semua kasus, kunci privat harus dilindungi terhadap aktivasi, *compromise*, atau perubahahan selama proses pengiriman.

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) kepada iOTENTIK 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

iOTENTIK menyediakan mekanisme untuk penyampaian digital yang aman dari semua sertifikat yang memuat kunci publik, melalui repositori sesuai bagian 2.1 yang diamankan menggunakan SSL.

6.1.5. Ukuran Kunci

iOTENTIK membuat sertifikat dan CRL menggunakan algoritma RSA dengan panjang kunci 4096 bit dengan SHA versi 2 (SHA-256) ketika membuat tanda tangan elektronik.

Pemilik sertifikat harus menggunakan algoritma RSA dengan panjang kunci 2048 bit dan SHA versi 2 (SHA-256) ketika membuat tanda tangan elektronik.

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Tidak ada ketentuan.

6.1.7. Tujuan Penggunaan Kunci (pada field key usage X.509 v3)

Sertifikat iOTENTIK digunakan untuk menandatangani sertifikat Pemilik dan CRL.

6.2. Kontrol Kunci Privat dan Kontrol Teknis Modul Kriptografi

6.2.1. Kendali dan Standar Modul Kriptografi

iOTENTIK menggunakan *hardware cryptographic modules* yang berstandar FIPS 140-2 level 2 untuk mengenerate pasangan kunci dan menyimpan kunci privat iOTENTIK. (*Hardware Security Module*/HSM).

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

iOTENTIK akan menerapkan mekanisme teknis dan prosedural yang memerlukan partisipasi dan beberapa individu dipercaya untuk melakukan operasi sensitif terhadap operasional kriptografi iOTENTIK. iOTENTIK menggunakan *secret sharing* untuk membagi aktivasi data yang diperlukan untuk menggunakan kunci privat IOTENTIK menjadi bagian-bagian yang terpisah. *Secret sharing* dilakukan oleh orang terpercaya dan terlatih. Sejumlah orang (m) diciptakan dan didistribusikan untuk modul *hardware* kriptografi (n) yang diperlukan untuk mengaktifkan kunci privat yang akan dibagi sesuai kebutuhan.

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

6.2.3. Escrow Kunci Privat

Kunci privat iOTENTIK tidak boleh dititipkan (*escrow)* kepada pihak ketiga.

6.2.4. Backup Kunci Privat

Kunci Privat iOTENTIK di-*backup* pada modul kriptografi (HSM) dengan tujuan untuk pemulihan rutin dan pemulihan ketika terjadi bencana.

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

6.2.5. Pengarsipan Kunci Privat

iOTENTIK tidak mengarsipkan kunci privat.

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 pemindahan yang dipakai untuk mengenkripsi kunci privat harus ditangani dengan cara yang sama dengan kunci privat.

6.2.7. Penyimpanan Kunci Privat Pada Modul Kriptografi

Kunci privat iOTENTIK disimpan dalam modul kriptografi FIPS 140-2 dalam bentuk terenkripsi dan terlindungi 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 secara otomatis setelah *secret shares* dicabut dari modul kriptografi.

6.2.10. Metode Penghancuran Kunci Privat

Ketika kunci tanda tangan privat PSrE Induk 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 PSrE Induk 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

Kunci Publik diarsipkan sebagai bagian dari pengarsipan sertifikat.

6.3.2. Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Periode operasi pasangan kunci ditentukan oleh periode operasional sertifikat elektronik yang sesuai. Jangka waktu operasional maksimum kunci iOTENTIK ditentukan selama sepuluh (10) tahun.

6.4. Data Aktivasi

6.4.1. Aktivasi Generasi Data dan Instalasi

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

6.4.2. Perlindungan Data Aktivasi

Data aktivasi untuk perangkat HSM dilindungi seperti yang dijelaskan dalam Bagian 6.2.2 (Kunci Pribadi (n dari m) Kontrol Multi-Orang). iOTENTIK menyimpan data aktivasi dalam bentuk smart card dengan perlindungan kata sandi.

6.4.3. Aspek Lain Mengenai Data Aktivasi

Tidak ada ketentuan.

6.5. Kontrol Keamanan Komputer

6.5.1. Persyaratan Teknis Keamanan Komputer yang Spesifik / Khusus

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

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

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

Ketika peralatan PSrE di-*host* pada platform yang dievaluasi untuk mendukung persyaratan jaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak, sistem operasi) harus, bila memungkinkan, beroperasi dalam konfigurasi yang dievaluasi. Minimal, platform tersebut harus menggunakan versi yang sama dari sistem operasi komputer seperti yang menerima penilaian evaluasi. Sistem komputer iOTENTIK dikonfigurasi dengan minimum akun yang diperlukan, layanan jaringan.

6.5.2. Peringkat Keamanan Komputer

Tidak Ada Ketentuan.

6.6. Kontrol Teknis Siklus Hidup

6.6.1. Kontrol Pengembangan Sistem

Tidak ada ketentuan.

6.6.2. Kontrol Manajemen Keamanan

iOTENTIK menggunakan perangkat lunak untuk mendeteksi perubahan konfigurasi sistem manajemen PSrE. Untuk menjamin integritas perangkat keras, iOTENTIK menggunakan *anti-tempered bag*.

6.6.3. Kontrol 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. Kontrol Keamanan Jaringan

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

6.8. Stempel Waktu

Jam server *online* PSrE Induk Indonesia disinkronkan menggunakan *Network Time Protocol*. Waktu server offline disinkronkan secara manual.

7. Sertifikat, CRL dan Profil OCSP

7.1. Profil Sertifikat

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

7.1.1. Nomor Versi

iOTENTIK menerbitkan sertifikat X.509 v3 (isi kolom versi dengan bilangan bulat "2").

7.1.2. Ekstensi Sertifikat

iOTENTIK menggunakan ekstensi sertifikat yang mengikuti standar 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 pengidentifikasi objek untuk CP iOTENTIK sesuai dengan bagian CPS 7.1.6 (Pengidentifikasi Objek Kebijakan Sertifikat) dan dengan kualifikasi kebijakan yang ditetapkan dalam Bagian CP 7.1.8 (Sintaks Kualifikasi Kebijakan dan Semantik). Ekstensi Field Critical 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. Ekstensi field Critical 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 iOTENTIK X.509 versi 3 mencakup ekstensi cRLDistributionPoints yang berisi URL lokasi tempat Pihak Pengandal dapat memperoleh CRL untuk memeriksa status Penerbitan Sertifikat CA. Kekritisan ekstensi ini diisi FALSE.

7.1.2.6. Pengidentifikasi Kunci Otoritas

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

7.1.2.7. Pengidentifikasi Kunci Subjek

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

7.1.3. Pengidentifikasi Obyek Algoritma

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

OID standar X.509v3 harus digunakan. Algoritma harus enkripsi RSA untuk kunci subjek dan SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.

sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.1.4. Format Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1.

7.1.5. Batasan Nama

Sesuai konvensi penamaan dan batasan yang tercantum dalam bagian 3.1.

7.1.6. Pengidentifikasi Objek Kebijakan Sertifikat

OID adalah sebuah angka yang mengidentifikasi sebuah objek atau kebijakan. OID yang digunakan iOTENTIK dijelaskan pada sub bab 1.2 pada dokumen ini (Nama dan Identifikasi Dokumen).

7.1.7. Penggunaan Ekstensi Batasan Kebijakan

Tidak ada Ketentuan

7.1.8. Kualifikasi Kebijakan Sintaksis dan Semantik

Tidak ada Ketentuan.

7.1.9. Memproses Semantik untuk Ekstensi Kebijakan Sertifikat Kritis

Tidak ada Ketentuan.

7.2. Profil CRL

7.2.1. Nomor Versi

iOTENTIK menerbitkan CRL X.509 versi 2. CRL versi 2 dengan mematuhi persyaratan RFC 5280

7.2.2. Ekstensi Entry CRL dan CRL

iOTENTIK menggunakan ekstensi entry CRL dan CRL sesuai RFC 5280.

7.3. Profil OCSP

iOTENTIK mengoperasikan sebuah responder Online Certificate Status Proctocol (OCSP) yang sesuai dengan RFC 6960 dan RFC 5019.

7.3.1. Nomor Versi

Spesifikasi OCSP versi 1 didefinisikan oleh RFC 6960 dan didukung oleh versi 1 spesifikasi OCSP yang didefinisikan RFC 5019.

7.3.2. Ekstensi OCSP

Tidak ada ketentuan.

8. Audit Kepatuhan dan Penilaian Lainnya

iOTENTIK akan menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika no 11/2018. Semua kebijakan yang terdapat dalam CPS 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 yang tidak kurang dari sekali setahun dan setiap terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan.

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.

Kualifikasi auditor untuk melakukan audit sistem iOTENTIK di antaranya :

1. Auditor harus dilaksanakan oleh tim asesmen independen yang qualified .
2. Memiliki pengetahuan regulasi implementasi tanda tangan digital dan penyelenggara sertifikasi elektronik (CA) di antaranya UU ITE tahun 2008 dan PP PSTE tahun 2012
3. Memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
4. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah
5. Menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang

8.3. Hubungan Asesor dengan Badan yang Dinilai

Auditor yang menilai kepatuhan yang dilakukan oleh iOTENTIK dilakukan oleh lembaga independen.

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 iOTENTIK mengadopsi skema yang terbaru.

8.5. Tindakan yang Diambil sebagai Hasil dari Kekurangan

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

8.6. Komunikasi Hasil

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada *Policy Authority* sebagaimana diatur dalam bagian 8.1. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam asesmen.

8.7. Audit Internal

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

9. Bisnis Lain dan Masalah Hukum

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

iOTENTIK tidak mengenakan biaya dalam menerbitkan atau memperbarui 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;
- Kunci Privat Pemegang Sertifikat yang disimpan oleh iOTENTIK, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
- Catatan Permohonan Sertifikat;
- Hasil penilaian kerentanan;

- Rekam jejak audit (log audit) dari sistem iOTENTIK dan RA;
- Data aktivasi pada saat pengaktifan Kunci Privat iOTENTIK sebagaimana dijabarkan pada Bagian 6.4;
- Dokumentasi bisnis proses PSrE termasuk dokumen *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* (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 CPS 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 Privasi“ yang dipublikasikan dalam situs iOTENTIK, https://www.govca.id.

9.4.2. Informasi yang Dianggap Pribadi

iOTENTIK harus melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi Pemilik dapat dirilis atas permintaan Pemilik. 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 dan CRL) dari CPS ini tidak termasuk dalam Bagian 9.4.2.

9.4.4. Tanggung Jawab Melindungi Informasi Pribadi

iOTENTIK memperlakukan seluruh informasi yang diterima dari Pemohon yang biasanya tidak disediakan di sertifikat sebagai informasi rahasia. Hal ini diterapkan untuk para Pemohon baik yang Sertifikatnya berhasil diterbitkan begitu juga yang tidak berhasil diterbitkan dan ditolak. iOTENTIK melatih secara periodik seluruh staff begitu juga dengan seluruh pihak yang memiliki akses ke informasi mengenai asas kehati-hatian dan atensi yang harus ditaati.

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 Pengungkapan Informasi Lainnya

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 CPS, bahwa:

- iOTENTIK mematuhi ketentuan yang diatur dalam CPS ini,
- iOTENTIK menerbitkan dan memperbarui CRL secara berkala,
- Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini,
- 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 CPS, 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 CPS dan dituangkan dalam Perjanjian RA.

9.6.3. Pernyataan dan Jaminan Pemilik

Pemilik Sertifikat menjamin bahwa:

- Setiap sertifikat elektronik yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah

merupakan tanda tangan elektronik pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kedaluwarsa dan telah dicabut) saat tanda tangan elektronik 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 elektronik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
- Segera:
  a) melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat; dan
  b) mengajukan permohonan untuk melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam sertifikat tersebut
  c) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat elektronik setelah sertifikat dicabut;
- Akan menanggapi instruksi iOTENTIK tentang compromise atau penyalahgunaan sertifikat elektronik dalam kurun waktu empat puluh delapan (48) jam;
- menyetujui dan menerima bahwa iOTENTIK diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika iOTENTIK 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 Elektronik untuk tujuan penandatangan sertifikat elektronik 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 CPS ini,

- Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

9.6.5. Pernyataan dan Jaminan Partisipan Lain

Tidak ada ketentuan.

9.7. Pelepasan Jaminan

iOTENTIK harus membuat pernyataan dalam CPS bahwa iOTENTIK tidak menjamin:

1. 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,
2. Penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (*Certificate Usage*)
3. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau *testing* Sertifikat.

9.8. Pembatasan Tanggung Jawab

9.8.1. Pembatasan Tanggung Jawab PSrE

iOTENTIK tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat, termasuk:

1. Semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
2. Semua kerusakan yang disebabkan oleh *force majeure*,
3. 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

iOTENTIK tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.

9.10. Syarat dan Pengakhiran

9.10.1. Syarat

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

9.10.2. Pengakhiran

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

9.10.3. Efek Pengakhiran dan Keberlangsungan

iOTENTIK akan memberitahukan kondisi dan efek dari penghentian CPS melalui repositori iOTENTIK. Semua perjanjian yang berkaitan dengan Pemilik akan tetap efektif sampai sertifikat elektronik dicabut atau sampai dengan habis masa berlaku, bahkan jika CPS ini dihentikan.

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. iOTENTIK memberikan tanda terima yang valid sebagai bukti bagi pengirim. iOTENTIK memberi tanggapan paling lama dua puluh (20) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke iOTENTIK harus dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS.

9.12. Amandemen

9.12.1. Prosedur untuk Amandemen

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

9.12.2. Periode dan Mekanisme Pemberitahuan

iOTENTIK harus menerbitkan pemberitahuan di situs terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika terjadi perubahan CPS 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 CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari perjanjian yang disepakati antara iOTENTIK dengan Pemilik sertifikat.

9.14. Hukum yang Mengatur

CPS ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat iOTENTIK ataupun produk/ layanan

lainnya. Termasuk apabila sertifikat iOTENTIK dipakai untuk kebutuhan komersial di negara lain tetap menerapkan aturan hukum di Indonesia.

Para pihak, termasuk partner iOTENTIK, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan di atas.

9.15. Kepatuhan atas Hukum yang Berlaku

iOTENTIK mematuhi hukum yang berlaku di Indonesia. Ekspor berbagai jenis perangkat lunak tertentu yang digunakan dalam beberapa produk dan layanan manajemen Sertifikat publik iOTENTIK.

iOTENTIK dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang berwenang. Para Pihak (termasuk CA, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi undang-undang dan regulasi ekspor yang berlaku di Indonesia.

9.16. Provisi Rupa – Rupa

9.16.1. Seluruh Perjanjian

Tidak ada ketentuan.

9.16.2. Pengalihan

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

9.16.3. Keterpisahan

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

9.16.4. Penegakan Hukum (Biaya Pengacara dan Pengalihan Hak – Hak)

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

9.16.5. *Force Majure*

iOTENTIK tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS 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. iOTENTIK wajib menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas iOTENTIK.

9.17. Provisi Lain

Tidak ada ketentuan.