Tata Cara Pengelolaan Sertifikat (*Certification Practice Statement*)

Privy

Versi 3.0

18 Agustus 2023

Jl. Kemang Raya 34L
Telp: 021-22715509
Email: Policy@privy.id
Website: www.privyca.id

Halaman Persetujuan *Policy Authority*

Dokumen ini disetujui secara elektronik sesuai pada waktu dan lokasi penandatanganannya.

Menyetujui,

Chief Executive Officer

Marshall Pribadi

Riwayat Perubahan

Versi	Tanggal	Deskripsi Riwayat dan Perubahan
1.0	-	Versi Perdana
1.1	22 Februari 2019	Penambahan untuk memenuhi persyaratan pengakuan sebagai Penyelenggara Sertifikasi Elektronik berinduk oleh Kominfo.
1.2	12 Januari 2021	Penambahan ketentuan RA Privy dan penyesuaian lainnya.
2.0	16 Juni 2021	Perubahan judul dokumen dan penyesuaian terhadap CP PSrE Induk Indonesia.
2.1	25 November 2021	Penambahan ketentuan tentang Inter-operasi, frekuensi pelatihan ulang, dan perubahan merek PrivyID menjadi Privy serta penyesuaian lainnya.
2.2	31 Januari 2023	Penambahan layanan Segel Elektronik dan identifikasi WNA. Penambahan persyaratan untuk penyesuaian terhadap CP Induk.
3.0	18 Agustus 2023	Penyesuaian terhadap ketentuan CP Induk berupa Perubahan OID, Kelas Sertifikat, Proses Validasi Identitas Awal, Arsip Dokumen, Perubahan Ketentuan Asuransi, Rencana Privasi.

Daftar Isi

1. Pengantar

1.1. Ringkasan

Privy atau PT Privy Identitas Digital merupakan badan hukum yang menjalankan usaha sebagai Penyelenggaraan Sertifikasi Elektronik ("PSrE") atau disebut juga dengan *Certificate Authority* ("CA"). Berdasarkan peraturan perundang-undangan yang diatur di Indonesia, Privy merupakan PSrE Non-Instansi.

Tata Cara Pelaksanaan Sertifikat PSrE/*Certificate Practice Statement* ("CPS") menguraikan persyaratan usaha, hukum, dan teknis yang mengatur mengenai Penyelenggara Sertifikasi Elektronik Privy oleh peserta di dalam Infrastruktur Kunci Publik/*Publik Key Infrastructure* ("PKI") Privy. CPS ini dibuat dengan memenuhi persyaratan formal yaitu konten, tata letak, dan format dari *Request for Comments* ("RFC") 3647 tentang X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework* yang dikeluarkan pada bulan November 2003 oleh Internet Engineering Task Force (IETF). CPS menguraikan praktik dan prosedur operasional PSrE Privy untuk memenuhi kriteria yang diatur oleh Kebijakan Sertifikat/*Certificate Policy* ("CP") dari Penyelenggara Sertifikasi Elektronik Induk Indonesia ("PSrE Induk").

Dokumen ini dibuat dengan asumsi bahwa pembaca telah memahami ketentuan yang diatur di dalam CP PSrE Induk, mengenal konsep Tanda Tangan Elektronik, sertifikat elektronik ("Sertifikat"), dan PKI secara umum. Apabila pembaca tidak mengenal konsep PKI, Pembaca dapat mengunduh CP PSrE Induk melalui https://www.rootca.id/.

Kecuali ditentukan lain, setiap penyebutan PSrE atau CA, adalah mengacu kepada PSrE Privy.

1.2. Identifikasi dan Nama Dokumen

Dokumen ini berjudul "**Tata Cara Pengelolaan Sertifikat (*Certificate Practice Statement*) v.3.0"** yang merupakan CPS dari PSrE Privy.

Privy, sesuai kewenangannya, ditetapkan untuk memiliki *Object Identifier* (OID) dengan nomor identifikasi joint-iso-itu-t(2) country(16) id(360) gov(1) kominfo(1) psre-induk(1) psre-Indonesia(3) psre-non-Instansi(12) privy(1).

Berikut merupakan OID untuk dokumen yang diterbitkan oleh Privy:

Sertifikat Non-Instansi	2.16.360.1.1.1.3.12
CPS	2.16.360.1.1.1.3.12.1.1

Selain OID untuk dokumen, berikut merupakan OID sesuai dengan ketentuan yang telah ditetapkan oleh Kementerian Komunikasi dan Informatika:

Compliance	2.16.360.1.1.1.9
AATL	2.16.360.1.1.1.9.1
SII Type	2.16.360.1.1.1.6
NIK	2.16.360.1.1.1.6.1
Peruntukan Sertifikat	2.16.360.1.1.1.7
Individu	2.16.360.1.1.1.7.1
Badan Usaha/Organisasi	2.16.360.1.1.1.7.2
Certificate Policies	2.16.360.1.1.1.5
Orang Individu Warga Negara Indonesia (WNI)	2.16.360.1.1.1.5.1
Individu non-Instansi Offline	2.16.360.1.1.1.5.1.1
Individu non-Instansi Offline Level 3	2.16.360.1.1.1.5.1.1.3
Individu non-Instansi Online	2.16.360.1.1.1.5.1.2
Individu non-Instansi Online Level 2	2.16.360.1.1.1.5.1.2.2
Orang Individu Warga Negara Asing (WNA)	2.16.360.1.1.1.5.2
Individu WNA Online	2.16.360.1.1.1.5.2.2
Individu WNA Online level 2	2.16.360.1.1.1.5.2.2.2
Individu WNA Online level 3	2.16.360.1.1.1.5.2.2.3

OID Segel Elektronik	2.16.360.1.1.1.8
Badan Usaha	2.16.360.1.1.1.8.1

Dokumen CPS tersedia secara umum pada https://repository.privyca.id.

1.3. Partisipan PKI

1.3.1. Penyelenggara Sertifikasi Elektronik

Penyelenggara Sertifikasi Elektronik (PSrE) /*Certificate Authority* (CA) adalah Badan Hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat, sesuai dengan apa yang diatur di dalam CPS ini. PSrE Privy berdasarkan CPS ini merupakan CA yang menjalankan fungsi *Publik Key Infrastructure* (PKI) Privy, yang termasuk namun tidak terbatas pada:

a. Operasional Siklus Sertifikat;
b. Pemrosesan Permohonan Sertifikat;
c. Penerbitan Sertifikat;
d. Penerimaan Sertifikat;
e. Penggunaan Sertifikat;
f. Pembaruan dan/atau Perpanjangan Sertifikat; dan
g. Pencabutan Sertifikat;

1.3.1.1. PSrE Induk

PSrE Induk adalah PSrE yang ditetapkan sebagai induk (*root*) PSrE Indonesia sebagaimana diatur di dalam peraturan perundang-undangan yang mengatur mengenai penyelenggaraan Sertifikasi Elektronik. PSrE Induk berperan dalam menandatangani dan mencabut Sertifikat PSrE yang berinduk dibawahnya. PSrE Induk dikelola oleh Kementerian Republik Indonesia yang berwenang menyelenggarakan fungsi PSrE Induk sesuai dengan ketentuan pada peraturan perundang-undangan. PSrE Induk tidak menerbitkan Sertifikat kepada Pemegang Sertifikat. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat

PSrE Indonesia, sebagaimana dirinci dalam CP PSrE Induk, termasuk namun tidak terbatas pada:

1. Pengendalian terhadap proses pendaftaran calon PSrE Indonesia;
2. Proses identifikasi dan autentikasi;
3. Proses penerbitan *self-sign* Sertifikat PSrE Induk;
4. Proses penerbitan Sertifikat PSrE Indonesia;
5. Proses penerbitan Daftar Pencabutan Sertifikat (*Certificate Revocation List*/CRLs);
6. Publikasi Sertifikat dan CRLs;
7. Validasi Sertifikat;
8. Pencabutan Sertifikat;
9. Membangun dan memelihara sistem PSrE Induk; dan
10. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE Induk yang diterbitkan sesuai dengan CP dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk.

1.3.1.2. PSrE Indonesia

PSrE Indonesia adalah PSrE yang telah mendapatkan pengakuan sebagai PSrE Berinduk dari Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, yang Sertifikatnya ditandatangani oleh PSrE Induk.

PSrE Indonesia tidak boleh menjadi induk bagi PSrE lainnya.

1.3.2. Otoritas Pendaftaran

Otoritas Pendaftaran/*Registration Authorities* (RA) merupakan pihak yang ditunjuk oleh PSrE Privy untuk menjalankan fungsi sebagai berikut:

a. Tunduk terhadap prosedur pendaftaran pemohon Sertifikat;

b. Identifikasi dan autentikasi Pemohon Sertifikat berdasarkan prosedur pendaftaran yang ditetapkan oleh PSrE Privy;
c. Memulai atau meneruskan permohonan untuk pencabutan Sertifikat kepada PSrE Privy; dan
d. Menyetujui permohonan penerbitan ulang atau perpanjangan Pemegang Sertifikat.

Dalam hal PSrE Privy bertindak secara langsung untuk menerima permohonan penerbitan Sertifikat dari Pemohon, maka PSrE Privy berperan sebagai RA bagi dirinya sendiri.

Kecuali disebutkan lain, RA yang tercantum dalam ketentuan ini adalah RA yang terikat dengan hubungan kontraktual dengan PSrE Privy. Oleh karena itu, seluruh ketentuan yang secara tegas menjelaskan mengenai peran RA di dalam CPS ini berlaku terhadap seluruh RA. PSrE Privy memiliki hak untuk melakukan audit atau pemeriksaan terhadap kesesuaian fungsi yang dijalankan oleh RA dengan CPS ini dan peraturan perundang-undangan yang berlaku.

1.3.3. Pengguna Akhir

Pengguna akhir dari PKI terdiri dari :

a. Pemohon/*Applicant* – Orang atau Badan Hukum yang telah mengajukan permohonan, namun belum mendapatkan Sertifikat.
b. Pemegang Sertifikat/*Subscriber* – Orang atau Badan Hukum yang telah berhasil memperoleh Sertifikat melalui permohonan kepada RA ataupun Privy.

1.3.4. Pengandal

Pengandal/*Relying Parties* adalah Orang atau Badan Hukum yang mempercayai Sertifikat dan/atau Tanda Tangan Elektronik yang diterbitkan oleh Privy. Pengandal terlebih dahulu memeriksa respon dari CRL atau OCSP yang sesuai sebelum memanfaatkan informasi yang tertera di dalam Sertifikat.

Pengandal mengandalkan keabsahan hubungan antara identitas Pemegang Sertifikat dengan kunci publik yang tercantum dalam Sertifikat. Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pengandal dapat menggunakan informasi di dalam Sertifikat untuk menentukan apakah suatu Sertifikat dapat diandalkan atau tidak.

Pengandal menggunakan informasi dalam Sertifikat untuk, antara lain:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi Tanda Tangan Elektronik;
c. Melakukan pemeriksaan (apakah Sertifikat ada pada daftar) pencabutan (CRL dan OCSP); dan
d. Penyetujuan atas batas tanggung jawab dan jaminan;

Setiap pihak, baik pelanggan maupun bukan pelanggan Privy, dapat mengandalkan Sertifikat yang diterbitkan oleh Privy. Namun siapapun yang mengandalkan Sertifikat yang diterbitkan oleh Privy tunduk pada ketentuan yang diatur dalam CPS ini dan juga Perjanjian Pengandal.

1.3.5. Partisipan Lain

Dalam menjalankan layanannya, PSrE Privy bekerja sama dengan partisipan lain yaitu pihak ketiga yang menyediakan layanan Pusat Data dan Pusat Data Pemulihan.

1.4. Kegunaan Sertifikat

Sertifikat memuat Tanda Tangan Elektronik Penerbit Sertifikat dan informasi mengenai identitas dan status subjek hukum Pemegang Sertifikat dalam suatu Transaksi Elektronik.

1.4.1. Penggunaan Sertifikat yang Dibolehkan

PSrE Privy menetapkan bahwa Layanan Sertifikat yang diterbitkan untuk Pengguna Akhir adalah hanya untuk melakukan **Tanda Tangan Digital dan Segel Elektronik**.

Tanda Tangan Digital merupakan jenis Tanda Tangan Elektronik yang digunakan untuk mendukung penandatangan melalui media elektronik dengan menggunakan metode kriptografi asimetris dan menggunakan Sertifikat untuk melakukan verifikasi antara pasangan Kunci Privat yang dikuasai oleh Pemegang Sertifikat dan Kunci Publik yang tertera di dalam Sertifikat.

Segel Elektronik adalah data elektronik yang dilekatkan, terasosiasi, atau terkait dengan Informasi Elektronik dan/atau Dokumen Elektronik untuk menjamin asal, integritas, dan keutuhan dari Informasi Elektronik dan/atau Dokumen Elektronik yang digunakan oleh Badan Usaha.

Sertifikat yang diterbitkan oleh PSrE Privy untuk Pemegang Sertifikat digunakan untuk transaksi dengan menggunakan Tanda Tangan Elektronik sehingga menjadi Tanda Tangan Digital, yang membutuhkan 3 (tiga) faktor berikut yang menjamin:

a. *Non-Repudiation*:
   Penandatangan tidak dapat menampik tanda tangan yang telah dibubuhkannya.
b. *Authentication*:
   Kepastian bahwa penanda tangan merupakan pihak yang benar-benar melakukan tanda tangan.
c. *Integrity*:
   Kepastian bahwa suatu informasi atau dokumen elektronik tidak mengalami perubahan.

Berdasarkan penjelasan tersebut, *Key Usage* yang diperbolehkan untuk Pemegang Sertifikat adalah *Digital Signature* dan *Non-Repudiation*.

Sertifikat yang diterbitkan oleh PSrE Privy adalah Sertifikat Elektronik dengan level verifikasi identitas level 2 dan 3 sesuai dengan peraturan perundang-undangan yang mengatur mengenai penyelenggaraan sertifikasi elektronik dengan deskripsi sebagai berikut:

a. Sertifikat Kelas 3
Sertifikat yang diterbitkan sesuai dengan level verifikasi identitas level 2 (Tingkat Kepastian Menengah); dan

b. Sertifikat Kelas 4
Sertifikat yang diterbitkan sesuai dengan level verifikasi identitas level 3 (Tingkat Kepastian Tinggi).

1.4.2. Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan oleh PSrE Privy hanya dapat digunakan untuk hal-hal yang diperbolehkan menurut ketentuan CPS ini dan peraturan perundang-undangan yang berlaku.

1.5. Administrasi Kebijakan

1.5.1. Organisasi Pengelola Dokumen

CPS ini dikelola oleh *Policy Authority* Privy (PA). CPS diubah sesuai dengan kebijakan yang ditentukan oleh PA. CPS ini juga berubah jika diperlukan penyesuaian dengan *Baseline Requirements* dari *CA Browser Forum, Webtrust Principles & Criteria for Certificate Authority*, *Adobe Approved Trusted List Technical Requirements,* dan/atau CP PSrE Induk.

PA terdiri dari *Chief Executive Officer* (Direktur Utama) dan pihak yang ditunjuk untuk mengepalai C-Level Unit di Privy.

PA dapat dihubungi melalui:
Policy Authority Privy
Jl. Kemang Raya No 34L
Telp: 021-22715509
Email: Policy@privy.id

1.5.2. Narahubung

Narahubung dapat menggunakan informasi yang tertera pada bagian 1.5.1.

1.5.3. Personil yang Menentukan Kesesuaian CPS dengan Kebijakan

PA Privy dibantu oleh Departemen yang mengurusi bagian hukum dan kepatuhan beserta dengan perwakilan yang ditunjuk oleh masing-masing divisi Privy yang terkait dengan PKI Privy dalam menentukan kesesuaian dan penerapan dari CPS ini.

1.5.4. Prosedur Persetujuan CPS

Perubahan terhadap CPS melalui persetujuan dari PA.

1.6. Definisi dan Akronim

Lihat Lampiran 2.

2. Tanggung Jawab Publikasi dan Repositori

2.1. Repositori

PSrE Privy menyediakan dan menjaga Repositori yang berisi dokumen yang menunjang penyelenggaraan layanan PKI yaitu:

a. *Publik Key Certificate* PSrE;
b. *CRL* dan/atau Status Keaktifan Sertifikat;
c. CPS;
d. Perjanjian Pemegang Sertifikat; dan
e. Perjanjian Pengandal.
f. Kebijakan Privasi; dan

g. Kebijakan Garansi.

2.2. Publikasi Informasi Sertifikat

Dokumen elektronik yang disebutkan di bagian 2.1. tersedia dan dapat diakses secara publik melalui URL https://repository.privyca.id. Dokumen tersebut hanya berlaku dan diakui oleh PSrE Privy apabila dokumen tercantum dan dapat diakses melalui Repositori Privy.

Dalam pelaksanaannya, PSrE Privy dapat menampilkan dokumen yang tercantum dalam Repositori tersebut dalam beberapa pilihan Bahasa. Khusus terhadap dokumen hukum, jika terdapat ketidaksesuaian antara satu bahasa dengan bahasa yang lain, maka dokumen berbahasa Indonesia yang berlaku.

2.3. Waktu atau Frekuensi Publikasi

Berikut merupakan waktu atau frekuensi publikasi untuk dokumen-dokumen yang tertera di dalam Repositori:

a. *Publik Key Certificate/* Sertifikat Kunci Publik PSrE
   Paling lambat 1 x 24 jam setelah pasangan kunci dibangkitkan.
b. *CRL* dan/atau Status Keaktifan Sertifikat
   Sebagaimana ditentukan pada bagian 4.9.7.
c. CPS
   Dalam kurun waktu 7 (tujuh) hari kerja setelah mendapat persetujuan dari PA. CPS akan ditinjau ulang setidaknya sekali dalam waktu satu tahun kalender. Jika tidak ada perubahan terhadap konten dari CPS tersebut, setidaknya akan dilakukan perubahan terhadap versi dan tanggal penerbitan dari CPS yang baru.

2.4. Kendali Akses pada Repositori

Dokumen yang tercantum dalam Repositori merupakan informasi publik yang dapat diakses oleh siapapun dalam bentuk dokumen *read-only.* PSrE Privy menerapkan kontrol keamanan secara logis dan fisik untuk mencegah pihak yang tidak berwenang untuk menambahkan, menghapus, atau mengubah dokumen di dalam Repositori.

3. Identifikasi dan Autentikasi

PSrE Privy sebagai CA dan/atau RA melakukan verifikasi dan autentikasi identitas dan/atau atribut lainnya dari Pemohon Sertifikat untuk menerbitkan Sertifikat.

3.1. Penamaan

3.1.1. Tipe Nama

Sertifikat yang diterbitkan oleh PSrE Privy sesuai dengan standar ITU X.500 *Distinguished Names*. Seluruh Sertifikat mengandung X.501 *distinguished name* dalam kolom *Subject Name*. Sertifikat yang diterbitkan oleh PSrE Privy menggunakan *Distinguished Name* (DN) untuk mendukung identifikasi dari Pemegang Sertifikat.

DN yang digunakan oleh PSrE Privy adalah sesuai dengan ketentuan yang diatur di dalam CP PSrE Induk. Adapun pengaturan parameter mengacu pada Standar Interoperabilitas PSrE Induk.

3.1.2. Kebutuhan Nama yang Bermakna

PSrE Privy menggunakan DN untuk mengidentifikasi suatu individu dan/atau Badan Hukum/Badan Usaha yang ditampilkan dalam kolom *Subject Name* dan kolom *Issuer Name.* Isi dari DN tersebut dapat berupa atribut sebagai berikut:

Atribut *Common Name* (CN) yang digunakan pada Sertifikat perorangan/individu adalah nama lengkap Pemegang Sertifikat ditambah dengan *Username* Privy, atau entitas yang mewakili Pemegang Sertifikat beserta *Username* Privy. Sedangkan untuk Badan Usaha/Badan Hukum adalah nama Badan Usaha/Badan Hukum tersebut sesuai pada dokumen legalitas milik Badan Usaha/Badan Hukum tersebut beserta *Username* Privy.

Atribut *Organization name* (O) merupakan nama Badan Hukum/Badan Usaha dimana Pemegang Sertifikat diidentifikasi sebagai bagian darinya.

Atribut *Organization Unit* (OU) merupakan nama divisi/departemen/unit dari Badan Hukum/Badan Usaha dimana Pemegang Sertifikat diidentifikasi sebagai bagian darinya. Dalam hal digunakan pada Sertifikat Organisasi/Badan Usaha maka akan diisi sebagai "Badan Usaha".

Atribut *Country* (C) merupakan negara dimana Pemegang Sertifikat menyatakan kedudukannya.

Informasi mengenai *Organisation name* dan *Organisation unit* tersebut hanya digunakan sebagai metode identifikasi pada Sertifikat dan tidak merepresentasikan kuasa atas Badan Hukum/Badan Usaha tersebut.

Khusus Sertifikat yang diterbitkan kepada Pemegang Sertifikat individu/perseorangan tanpa informasi yang merepresentasikan Badan Hukum/Badan Usaha apapun, maka Atribut *Organization name* akan diisi dengan nama entitas RA yang melakukan fungsi identifikasi dan autentikasi dari data Pemohon Sertifikat, dan *Organization Unit* akan diisi sebagai "Perorangan".

3.1.3. Anonimitas atau Pseudonimitas Pemegang Sertifikat

Privy tidak menerbitkan Sertifikat anonim atau pseudonim.

3.1.4. Aturan Interpretasi Berbagai Bentuk Nama

DN dalam Sertifikat diuraikan menggunakan standar X.500.

3.1.5. Keunikan Nama

DN dari setiap Sertifikat yang diterbitkan adalah unik dengan kriteria berdasarkan Kelas atau tipe dari Sertifikat yang diterbitkan. Apabila dibutuhkan, PSrE Privy dapat menambahkan informasi tambahan yang dicantumkan di dalam *Subject Distinguished Name* pada Sertifikat sebagai daya pembeda dalam hal terdapat 2 (dua) atau lebih Sertifikat yang seharusnya memiliki *Subject Name* yang sama.

3.1.6. Pengakuan, Autentikasi, dan Peran Merk Dagang

Pemohon tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE Privy tidak akan memverifikasi permohonan yang terkait dengan penggunaan merek dagang. Pemohon atau Pemegang Sertifikat berkewajiban dan bertanggungjawab untuk memastikan bahwa permohonan Sertifikat yang diajukan tidak melanggar hak kekayaan intelektual pihak lain.

3.2. Validasi Identitas Awal

PSrE Privy akan melakukan Identifikasi dan autentikasi Pemohon Sertifikat berdasarkan prosedur pendaftaran yang ditetapkan oleh PSrE Privy yang mengacu kepada Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk.

3.2.1. Metode Pembuktian Kepemilikan Kunci Privat

Pasangan Kunci yang telah dibangkitkan oleh Privy, Kunci Privatnya akan disimpan dan diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan *Federal Information Protection Standards* (FIPS)-140 level 2. Untuk pembuktian penguasaan Kunci Privat yang terasosiasi dengan Sertifikat Pemohon untuk proses penandatanganan menggunakan metode autentikasi yang ditentukan oleh PSrE Privy yang meliputi 2 dari 3 faktor autentikasi yaitu *Something you know, Something you have*, *Something you are*.

3.2.2. Autentikasi Identitas Organisasi

Jika suatu Sertifikat digunakan untuk mengidentifikasi suatu Badan Hukum/Badan Usaha maka pengajuan untuk mendapatkan Sertifikat tersebut hanya dapat diajukan oleh pihak yang berwenang untuk mewakili Badan Hukum/Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut.

PSrE Privy dan/atau RA akan memeriksa dokumen-dokumen milik Badan Hukum/Badan Usaha dan identitas pemohon sesuai autentikasi identitas individu yang diatur dalam bagian 3.2.3. Adapun pemeriksaan yang dilakukan meliputi:

a. Kartu Nomor Pokok Wajib Pajak (“NPWP”) Badan Hukum/Badan Usaha.
b. Akta pendirian dan/atau akta perubahan terakhir Badan Hukum/Badan Usaha;
c. Jabatan/wewenang dari perwakilan Pemohon;
d. Surat kuasa/surat penunjukan dari pihak yang berwenang untuk mewakili Badan Hukum/Badan Usaha (jika dibutuhkan);
e. Nomor ponsel perwakilan Badan Hukum/Badan Usaha;
f. Alamat surat elektronik perwakilan Badan Hukum/Badan Usaha;

PSrE Privy melakukan identifikasi dan autentikasi terhadap dokumen-dokumen yang diberikan oleh Badan Hukum/Badan Usaha untuk penerbitan Sertifikat. Adapun proses identifikasi dan autentikasi yang dilakukan adalah:

a. Pemeriksaan NPWP dengan Akta
b. Pemeriksaan Akta pendirian dan/atau akta perubahan terakhir Badan Hukum/Badan Usaha dengan membandingan informasi pada dokumen tersebut dengan informasi yang

diterima dari basis data Instansi berwenang yang memberikan pengesahan Badan Hukum/Badan Usaha sesuai dengan ketentuan perundang-undangan;

c. Pemeriksaan Data biometrik milik perwakilan dari Badan Hukum/Badan Usaha berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection;* dan
d. melakukan validasi, dan memastikan bahwa informasi yang tertera di dalam KTP milik perwakilan dari Badan Hukum/Badan Usaha adalah valid dan autentik diajukan oleh Pemohon dengan melakukan pencocokan data, termasuk data biometrik berupa swafoto, dengan basis data kependudukan yang dikelola oleh lembaga pemerintah yang menyelenggarakan administrasi kependudukan.

Dalam hal proses identifikasi dan autentikasi permohonan Sertifikat Badan Hukum/Badan Usaha telah berhasil, PSrE Privy akan menerbitkan Sertifikat Kelas 4 bagi Badan Hukum/Badan Usaha tersebut.

PSrE Privy menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi bagi organisasi setidaknya selama masa berlaku dari Sertifikat yang diterbitkan.

3.2.3. Autentikasi Identitas Individu/Perorangan

PSrE Privy dan/atau RA akan mengidentifikasi dan mengautentikasi permohonan Sertifikat yang diajukan oleh individu/perorangan berdasarkan kelas Sertifikat. PSrE Privy dapat menerbitkan Sertifikat untuk Pemohon Sertifikat dengan klasifikasi Sertifikat Kelas 3 dan Kelas 4.

Pemohon terdiri dari Warga Negara Indonesia (WNI) atau Warga Negara Asing (WNA). Berdasarkan ketentuan yang diatur oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik, untuk mendapatkan

Sertifikat, Pemohon dalam hal ini WNI, diwajibkan untuk menunjukkan, membuktikan, dan memberikan hal-hal berikut:

a. Formulir pendaftaran Sertifikat;
b. Salinan dokumen berupa Kartu Tanda Penduduk (KTP) yang dikeluarkan oleh Pemerintah Indonesia. PSrE Privy dan/atau RA dapat meminta dokumen-dokumen pendukung lainnya antara lain KK, SIM dan/atau Paspor sebagai dokumen pendukung proses identifikasi dan autentikasi permohonan Sertifikat jika diperlukan;
c. Alamat surat elektronik;
d. Nomor telepon (termasuk ponsel); dan
e. Data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection*.

Mekanisme *liveness detection* adalah mekanisme yang digunakan untuk mendeteksi apakah suatu objek merupakan objek hidup atau tidak. Untuk menghindari keraguan, beberapa mekanisme liveness detection adalah sebagai berikut:

a. *Active liveness detection,* dimana Privy dan/atau RA meminta Pemohon untuk mengedipkan mata, menggelengkan kepala, dan atau gerakan lainnya dalam proses verifikasi;
b. *Passive liveness detection,* dimana Privy dan/atau RA menggunakan algoritma tertentu dalam proses verifikasi sehingga sistem dapat mendeteksi apakah swafoto atau video wajah yang diberikan oleh Pemohon merupakan wajah orang hidup atau tidak;
c. *Remote Customer Onboarding,* dimana dengan menggunakan media *video conference*, verifikator akan menanyakan pertanyaan-pertanyaan dan/atau memberikan instruksi yang harus diikuti oleh Pemohon; dan/atau
d. Metode uji deteksi kehidupan lainnya.

PSrE Privy dan/atau RA berkewajiban untuk memeriksa, melakukan validasi, dan memastikan bahwa informasi yang

tertera di dalam KTP adalah valid dan autentik diajukan oleh Pemohon dengan melakukan pencocokan data, termasuk data biometrik berupa swafoto, dengan basis data kependudukan yang dikelola oleh lembaga pemerintah yang menyelenggarakan administrasi kependudukan.

Apabila pencocokan data identitas dilakukan oleh PSrE Privy dan/atau RA dengan melakukan pencocokan data pada basis data kependudukan yang ada di kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional maka Sertifikat yang diterbitkan adalah Sertifikat Kelas 3. Apabila pencocokan data identitas Pemohon dilakukan dengan menggunakan *E-KTP Reader* yang telah diaktivasi oleh pemerintah yang menyelenggarakan administrasi kependudukan, maka Sertifikat yang diterbitkan adalah Sertifikat Kelas 4.

Sementara untuk WNA, wajib memberikan:

a. Formulir pendaftaran Sertifikat;
b. Foto dokumen Paspor;
c. KTP atau Kartu Izin Tinggal Sementara (KITAS) yang dikeluarkan oleh Lembaga Kementrian Terkait;
d. Surat permohonan dari perusahaan yang ditandatangani oleh penanggung jawab perusahaan dimana Pemohon bekerja atau terafiliasi bagi yang tidak memiliki KTP;
e. Data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection;*
f. Nomor telepon; dan
g. Alamat surat elektronik.

Dalam hal proses verifikasi dokumen dan identitas berhasil, PSrE Privy akan menerbitkan Sertifikat Kelas 3 bagi WNA yang melampirkan KITAS sebagai dokumen identitas yang digunakan. Bagi WNA yang menggunakan KTP sebagai dokumen identitas

yang digunakan, maka dapat diterbitkan sertifikat kelas 4 oleh PSrE Privy.

PSrE Privy dan/atau RA juga harus memeriksa dan melakukan validasi terhadap informasi lainnya yang telah diterima dari Pemohon untuk mendeteksi kebenaran dan keasliannya serta mencari jika ada perubahan dan/atau pemalsuan terhadap informasi-informasi lainnya tersebut.

PSrE Privy menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi individu/perorangan setidaknya selama masa berlaku dari Sertifikat yang diterbitkan.

3.2.4. Informasi Pemegang Sertifikat yang Tidak Terverifikasi

PSrE Privy tidak menerbitkan Sertifikat untuk Pemohon Sertifikat yang informasinya tidak dapat diverifikasi dan diautentikasi sesuai bagian 3.2.3. diatas.

3.2.5. Validasi Otoritas

PSrE Privy dan/atau RA menggunakan upaya yang wajar dan andal untuk memeriksa keautentikan informasi Pemohon terhadap permohonan yang diajukan untuk Sertifikat yang dibuat dengan atas nama Badan Hukum/Badan Usaha.

3.2.6. Kriteria Inter-operasi

Tidak ada ketentuan.

3.3. Identifikasi dan Autentikasi untuk Permintaan *Re-key*

3.3.1. Identifikasi dan Autentikasi untuk *Re-key* Rutin

Pemegang Sertifikat dapat mengajukan permohonan pergantian kunci (*re-key*) dengan ketentuan bahwa PsrE Privy akan menerbitkan pasangan kunci baru dan menerbitkan Sertifikat baru, dengan masa validitas baru. PSrE Privy akan

meminta Pemegang Sertifikat untuk melakukan autentikasi pada proses permintaan *re-key*, sesuai dengan ketentuan yang disebutkan pada bagian 4.7.

3.3.2. Identifikasi dan Autentikasi untuk *Re-key* setelah Pencabutan

Ketentuan *re-key* sebagaimana disebutkan pada bagian 3.3.1 berlaku untuk Sertifikat yang telah dicabut atau habis masa berlakunya.

3.4. Identifikasi dan Autentikasi untuk Permohonan Pencabutan

Permohonan untuk mencabut Sertifikat dapat diajukan atas dasar risiko kebocoran kunci maupun alasan lainnya oleh Pemegang Sertifikat dengan menghubungi Privy melalui kontak yang tertera pada Situs dan membuktikan penguasaan terhadap informasi data Pemegang Sertifikat yang disimpan oleh Privy. Dalam hal permohonan pencabutan untuk Sertifikat Individu, maka PSrE Privy akan meminta data berupa *Username* Privy (PrivyID) dan alamat email. Dalam hal permohonan pencabutan dilakukan terhadap Sertifikat Badan Usaha maka PSrE Privy akan memastikan bahwa pihak yang melakukan permohonan adalah pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut. PSrE Privy akan melakukan verifikasi data dengan mengajukan beberapa pertanyaan. PSrE Privy dapat meminta syarat tambahan jika diperlukan untuk melakukan autentikasi permohonan pencabutan Sertifikat.

4. Persyaratan Operasional Siklus Sertifikat

4.1. Permohonan Sertifikat

4.1.1. Pihak yang dapat Mengajukan Permohonan Sertifikat

Pihak yang dapat mengajukan permohonan penerbitan Sertifikat adalah orang dan/atau Badan Hukum/Badan Usaha.

Orang yang dapat mengajukan permohonan penerbitan Sertifikat adalah warga negara Indonesia atau warga negara asing dan hanya dapat dilakukan oleh individu tersebut, sedangkan untuk Badan Hukum atau Badan Usaha harus terdaftar sebagai Badan Hukum atau Badan Usaha yang sah di Indonesia dan dilakukan oleh pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut.

4.1.2. Proses Pendaftaran dan Tanggung jawabnya

Berikut merupakan langkah yang harus dilakukan untuk memperoleh Sertifikat:

a. Mengirimkan formulir pendaftaran yang sudah diisi lengkap beserta dengan dokumen lain yang dibutuhkan sesuai dengan ketentuan pada bagian 3.2. kepada PSrE Privy dan/atau RA. Pemohon berkewajiban untuk memberikan data dan informasi yang tepat, benar, dan jelas;
b. Setuju terhadap Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, serta Kebijakan Privasi Privy yang berlaku;
c. Membayar biaya Sertifikat dan biaya penggunaannya (apabila berlaku);
d. Menunggu validasi serta verifikasi identitas dari PSrE Privy dan/atau RA; dan
e. Jika validasi dan verifikasi gagal dilakukan, PSrE Privy dan/atau RA dapat meminta data dan informasi tambahan kepada Pemohon.

Validasi dan verifikasi dilakukan berdasarkan permohonan kelas Sertifikat yang diajukan oleh Pemohon. Jika validasi dan verifikasi berhasil, Sertifikat kemudian diterbitkan.

Dalam rangka memproses penerbitan Sertifikat, RA memiliki tanggung jawab sebagai berikut:

a. Memeriksa formulir pendaftaran beserta dengan dokumen tambahan yang dikirimkan oleh Pemohon adalah benar, jelas

dan tepat, berikut dengan data dan informasi pendukungnya;

b. Memastikan bahwa jalur komunikasi yang digunakan antara Pemohon, RA, dan PSrE Privy untuk menghimpun dan menyalurkan informasi yang dibutuhkan untuk memenuhi kebutuhan pendaftaran adalah jalur komunikasi yang aman; dan
c. Mengirimkan informasi dan/atau dokumen yang dibutuhkan oleh PSrE Privy sebagaimana disebutkan pada bagian 3.2 untuk kebutuhan pemenuhan terhadap peraturan perundang-undangan.
d. Menyimpan informasi dan/atau dokumen yang telah diberikan oleh Pemohon dengan aman.

Setelah menerima permohonan penerbitan Sertifikat tersebut, PSrE Privy dan/atau RA akan menjalankan validasi dan verifikasi sebagaimana yang telah diatur di bagian 3.2. diatas. Dalam hal RA menerima permohonan penerbitan Sertifikat dan telah melakukan validasi dan verifikasi terhadap permohonan tersebut, maka RA akan melanjutkan permohonan penerbitan Sertifikat ke PSrE Privy.

Setelah pemeriksaan dan validasi dinyatakan berhasil oleh RA, maka PSrE Privy bertanggung jawab untuk menerbitkan Sertifikat Pemohon setelah seluruh syarat penerbitan Sertifikat lainnya terpenuhi dan menyimpan informasi terkait dengan proses pendaftaran Pemohon sebagaimana diatur di dalam peraturan perundang-undangan.

PSrE Privy dan/atau RA akan melakukan upaya yang wajar untuk memastikan bahwa Pemohon Sertifikat memberikan data dan informasi yang valid dan autentik. Pemohon Sertifikat harus melalui proses registrasi sebagaimana yang dicantumkan di dalam CPS ini sebelum permohonan penerbitan Sertifikat diterima. PsrE Privy dan/atau RA memiliki wewenang untuk

menolak permohonan penerbitan Sertifikat jika ada data dan informasi yang kurang dan/atau tidak benar. Sertifikat hanya dapat diterbitkan jika Pemohon menyetujui Perjanjian Pemegang Sertifikat dan Kebijakan Privasi.

4.2. Pemrosesan Permohonan Sertifikat

4.2.1. Melaksanakan fungsi Identifikasi dan Autentikasi

PsrE Privy dan/atau RA dapat menggunakan data dan informasi yang diajukan oleh Pemohon untuk mengautentikasi dan memeriksa identitas pemohon sebagaimana diatur dalam bagian 3.2. dari CPS ini.

4.2.2. Persetujuan atau Penolakan Permohonan Sertifikat

PsrE Privy dan/atau RA hanya akan memberikan persetujuan terhadap permohonan penerbitan Sertifikat apabila telah memenuhi kriteria yang disebutkan di bagian 4.1.

Dalam hal Pemohon tidak berhasil memenuhi kriteria tersebut maka Privy dan/atau RA memiliki kewenangan berikut:

a. Menolak permohonan penerbitan Sertifikat Pemohon; dan/atau
b. Meminta informasi tambahan kepada Pemohon agar dapat memenuhi kriteria yang dibutuhkan.

4.2.3. Waktu untuk Memproses Permohonan Sertifikat

PsrE Privy memastikan bahwa proses permohonan penerbitan Sertifikat dilakukan selambatnya dalam jangka waktu 3 x 24 jam setelah semua rincian dan dokumen yang diperlukan dari Pemohon diterima oleh PsrE Privy.

4.3. Penerbitan Sertifikat

Setelah menerima permohonan penerbitan Sertifikat, PsrE Privy harus menanggapi sesuai dengan persyaratan yang ditetapkan dalam CPS.

4.3.1. Tindakan PsrE Privy selama Penerbitan Sertifikat

Setelah menerima permohonan penerbitan Sertifikat, PSrE Privy melakukan tindakan-tindakan sebagai berikut:

a. Melakukan verifikasi dan validasi atas dokumen dan identitas yang diberikan oleh Pemohon atau melalui RA sebagaimana diatur dalam bagian 3.2.2 dan 3.2.3;
b. Dalam hal permohonan diajukan untuk Badan Hukum/Badan Usaha, PSrE Privy memverifikasi otoritas yang melakukan Permohonan sesuai dalam bagian 3.2.5;
c. Melakukan verifikasi sumber permohonan Sertifikat sebelum diterbitkan;
d. Mempersiapkan bahwa Pemegang Sertifikat menerima sertifikat sebagaimana diatur pada bagian 4.4;
e. Membuat Sertifikat tersedia bagi Pemegang Sertifikat setelah Pemegang Sertifikat menyetujui kewajibannya menurut CPS ini.

4.3.1.1. Tindakan RA selama Penerbitan Sertifikat

Setelah melakukan verifikasi dan validasi sebagaimana diatur dalam bagian 3.2.2, 3.2.3, dan 3.2.5, RA kemudian meneruskan permohonan penerbitan Sertifikat kepada PSrE Privy beserta dengan informasi pendaftaran Pemohon yang wajib disimpan oleh PSrE Privy sebagaimana dijelaskan pada bagian 4.1. RA wajib memastikan bahwa Pemegang Sertifikat menerima Sertifikat sebagaimana diatur dalam bagian 4.4.

4.3.1.2. Penerbitan Sertifikat Untuk Permohonan *Re-key* Sertifikat, dan Sertifikat Yang Habis Masa Berlakunya atau Telah Dicabut

Dalam hal Pemegang Sertifikat mengajukan permohonan *re-key* Sertifikat, atau suatu Sertifikat masa validitasnya berakhir atau telah dicabut, maka penerbitan Sertifikat baru dapat dilakukan tanpa melalui proses identifikasi dan

autentikasi sebagaimana diatur pada bagian 4.2.1 selama Pemegang Sertifikat berhasil melakukan mekanisme autentikasi yang ditentukan oleh PSrE Privy untuk penerbitan Sertifikat baru tersebut.

4.3.2. Pemberitahuan ke Pemegang Sertifikat oleh PSrE Privy tentang Penerbitan Sertifikat

Secara segera setelah Sertifikat diterbitkan, maka PSrE Privy memberitahu Pemohon Sertifikat bahwa permohonan Sertifikat telah disetujui melalui email dan/atau nomor telepon Pemohon yang terdaftar, paling lambat dalam jangka waktu 3 (tiga) jam.

4.4. Pernyataan Persetujuan

4.4.1. Sikap yang Dianggap sebagai Menyetujui Sertifikat

Pemohon dianggap telah menerima Sertifikat setelah pemberitahuan kepada Pemohon sesuai bagian 4.3.3.

Apabila dalam jangka waktu 7 (tujuh) hari kerja, Pemegang Sertifikat tidak menyampaikan keluhan terhadap informasi yang tertera pada Sertifikat, maka Pemegang Sertifikat dianggap telah menerima semua informasi yang tertera pada Sertifikat.

Apabila Pemegang Sertifikat memiliki keluhan terhadap informasi yang tertera pada Sertifikat, maka Pemegang Sertifikat dapat mengajukan permohonan pencabutan Sertifikat sesuai ketentuan yang diatur pada bagian 4.9. melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Privy.

4.4.2. Publikasi Sertifikat oleh PSrE Privy

PSrE Privy mempublikasikan Sertifikat PSrE Privy dalam Repositori yang dapat diakses melalui Situs Privy.

PSrE Privy tidak mempublikasikan Sertifikat Pengguna Akhir.

4.4.3. Pemberitahuan Sertifikat oleh PSrE Privy kepada Pihak Lain

RA dapat menerima pemberitahuan terhadap penerbitan suatu Sertifikat apabila RA terlibat dalam proses penerbitan Sertifikat tersebut.

4.5. Penggunaan Pasangan Kunci dan Sertifikat

4.5.1. Penggunaan Kunci Privat dan Sertifikat oleh Pemegang Sertifikat

Pemegang Sertifikat menitipkan Kunci Privatnya kepada PSrE Privy, sesuai dengan persetujuan berdasarkan Perjanjian Pemegang Sertifikat dengan PSrE Privy, maka PSrE Privy akan menyimpan Kunci Privat tersebut dengan menggunakan Hardware Security Module (HSM) dengan spesifikasi minimal FIPS 140-2 Level 2.

PSrE Privy melakukan upaya-upaya pengamanan dan penyimpanan dengan penuh kehati-hatian terhadap Kunci Privat Pemegang Sertifikat agar Kunci Privat tersebut hanya dapat digunakan oleh Pemegang Sertifikat. Pemegang Sertifikat harus melindungi parameter autentikasi yang digunakan untuk mengaktifkan Kunci Privatnya. Pemegang Sertifikat hanya memakai Kunci Privatnya untuk tujuan yang sudah ditentukan.

4.5.2. Penggunaan Kunci Publik dan Sertifikat oleh Pengandal

Dalam mengandalkan Sertifikat yang diterbitkan oleh PSrE Privy, Pengandal memberikan jaminan dan pernyataan sesuai ketentuan yang diatur pada 9.6.4.

Pengandal dapat mengakses *Public Key Certificate* Privy melalui Repositori Privy.

4.6. Pembaruan Sertifikat

PSrE Privy tidak melakukan Pembaruan Sertifikat.

4.6.1. Kondisi untuk Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.2. Pihak yang Dapat Mengajukan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.3. Pemrosesan Permohonan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemegang Sertifikat

Tidak ada ketentuan.

4.6.5. Sikap yang Dianggap sebagai Penerimaan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.6. Publikasi Pembaruan Sertifikat oleh Privy

Tidak ada ketentuan.

4.6.7. Pemberitahuan Pembaruan Sertifikat oleh Privy kepada Pihak Lain

Tidak ada ketentuan.

4.7. *Re-key* Sertifikat

Re-key merupakan proses dimana Pemegang Sertifikat mengajukan penerbitan Sertifikat baru untuk menggantikan Sertifikat lamanya yang akan menghasilkan pasangan kunci yang baru dan masa validitas yang baru.

4.7.1. Kondisi untuk *Re-key* Sertifikat

Re-key Sertifikat dapat dilakukan selama:

a. Sertifikat telah dicabut ataupun habis masa berlakunya; atau
b. Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam.

4.7.2. Pihak yang dapat Mengajukan *Re-key* Sertifikat

Pemegang Sertifikat dapat mengajukan *re-key* Sertifikat. Dalam hal pembaruan Sertifikat yang diajukan adalah untuk Sertifikat Badan Usaha, maka permohonan hanya dapat diajukan pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut dengan menghubungi Privy melalui kontak yang tertera pada Situs, lalu PSrE Privy akan melakukan verifikasi data dengan mengajukan beberapa pertanyaan untuk membuktikan wewenang pihak yang memohon pembaruan Sertifikat Badan Usaha tersebut.

4.7.3. Pemrosesan Permohonan *Re-key* Sertifikat

Prosedur *re-key* Sertifikat adalah sebagaimana ditentukan pada bagian 4.3 dan 3.3

4.7.4. Pemberitahuan Penerbitan *Re-key* Sertifikat ke Pemegang Sertifikat

Setelah *re-key* Sertifikat berhasil dilakukan, maka PSrE Privy akan memberitahukan Pemohon Sertifikat bahwa penerbitan Sertifikat telah berhasil dilakukan melalui *email* dan/atau nomor telepon Pemohon yang terdaftar, selambatnya dalam jangka waktu 3 (tiga) jam dengan merujuk ke bagian 4.3.2.

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

Pemegang Sertifikat dianggap telah menerima Sertifikat hasil *re-key* ketika pemberitahuan sebagaimana ditentukan pada bagian 4.7.4 telah diterima oleh Pemegang Sertifikat dengan merujuk ke bagian 4.4.1.

4.7.6. Publikasi *Re-key* Sertifikat oleh Privy

Privy tidak melakukan publikasi Sertifikat hasil *re-key*.

4.7.7. Pemberitahuan Sertifikat *Re-key* oleh Privy

Tidak ada ketentuan.

4.8. Modifikasi Sertifikat

PSrE Privy tidak melakukan Modifikasi Sertifikat. Apabila terjadi kesalahan dalam penerbitan Sertifikat, maka PSrE Privy melakukan pencabutan Sertifikat dan menerbitkan Sertifikat baru yang sesuai dengan ketentuan yang diatur pada CPS ini.

4.8.1. Keadaan yang Menyebabkan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.2. Pihak yang Dapat Mengajukan Permohonan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.3. Pemrosesan Permohonan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.4. Pemberitahuan Sertifikat Baru ke Pemegang Sertifikat

Tidak ada ketentuan.

4.8.5. Sikap yang dianggap sebagai Penerimaan Modifikasi Sertifikat

Tidak ada ketentuan.

4.8.6. Publikasi Sertifikat yang Dimodifikasi oleh PSrE Privy

Tidak ada ketentuan.

4.8.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE Privy ke Pihak Lain

Tidak ada ketentuan.

4.9. Pencabutan dan Pembekuan Sertifikat

4.9.1. Keadaan yang Menyebabkan Pencabutan Sertifikat

PSrE Privy melakukan pencabutan Sertifikat untuk hal-hal berikut ini:

a. Ketika Pemegang Sertifikat atau pihak ketiga lainnya yang berwenang mengajukan permohonan pencabutan Sertifikat;
b. Ketika kunci privat terkompromi, hilang, dan/atau rusak;
c. Ketika terjadi perubahan standar industri, kebijakan pemerintah, dan/atau peraturan perundang-undangan yang mempengaruhi keabsahan Sertifikat.
d. Ketika informasi yang tertera di dalam Sertifikat tidak akurat atau menyesatkan;
e. Ketika permohonan penerbitan Sertifikat dilakukan secara secara tidak sah;
f. Ketika penerbitan Sertifikat dilakukan secara tidak sesuai dengan ketentuan yang tercantum di dalam CPS;
g. Ketika Pemegang Sertifikat melanggar ketentuan yang tercantum di dalam CPS atau Perjanjian Pemegang Sertifikat;
h. Ketika Sertifikat Privy mengalami kebocoran;
i. Ketika Privy berhenti beroperasi;
j. Alasan lainnya yang menurut Privy dibenarkan untuk melakukan pencabutan Sertifikat; atau
k. Pemegang Sertifikat sudah tidak bisa lagi menggunakan Sertifikat.

4.9.2. Pihak yang dapat Mengajukan Pencabutan Sertifikat

Pencabutan Sertifikat hanya dapat dilakukan oleh subjek yang terkait dengan Sertifikat tersebut, dalam hal ini Pemegang Sertifikat, atau kuasanya, dapat mengajukan pencabutan Sertifikat untuk Sertifikatnya.

Pihak ketiga yang dapat mengajukan permohonan pencabutan harus dapat membuktikan wewenang tersebut berdasarkan kuasa dari Pemegang Sertifikat untuk melakukan pencabutan sertifikat.

Dalam hal ketentuan yang tercantum pada bagian 4.9.1. terpenuhi, maka PSrE Privy juga dapat melakukan Pencabutan Sertifikat tanpa permintaan pencabutan oleh Pemegang Sertifikat.

4.9.3. Prosedur Pengajuan Pencabutan Sertifikat

PSrE Privy memverifikasi identitas sebelum dilakukan pencabutan Sertifikat sebagaimana bagian bagian 3.4. Sertifikat yang telah dicabut masuk kedalam daftar CRL dan OCSP.

Dalam mengajukan permintaan pencabutan Sertifikat, Pemegang Sertifikat harus menyerahkan bukti yaitu:

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Terdapat alasan relevan lain yang diberikan oleh Pemegang Sertifikat.

Permintaan pencabutan Sertifikat oleh pihak ketiga harus disertai dengan kuasa pencabutan Sertifikat. Pihak ketiga juga harus menyerahkan bukti yaitu:

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Pemegang Sertifikat sudah tidak terasosiasi dengan pihak ketiga tersebut.

Setelah dilakukan pencabutan, Pemegang Sertifikat dapat mengajukan penerbitan Sertifikat Baru. Proses Penerbitan Sertifikat Baru akan mengikuti ketentuan pada bagian 4.1. hingga 4.4.

4.9.4. Tenggang Waktu Permohonan Pencabutan

PSrE Privy tidak mengatur tenggang waktu untuk permohonan pencabutan Sertifikat yang diajukan oleh Pemegang Sertifikat atau pihak ketiga lainnya. Pihak sebagaimana diatur pada bagian

4.9.2 harus meminta pencabutan segera setelah teridentifikasi adanya keperluan pencabutan.

4.9.5. Jangka Waktu PSrE Privy untuk Memproses Permohonan Pencabutan

PSrE Privy segera mencabut Sertifikat dalam jangka waktu 1 x 24 jam, setelah persyaratan pengajuan pencabutan Sertifikat sebagaimana tercantum pada bagian 4.9.3 berhasil dipenuhi.

4.9.6. Persyaratan Pemeriksaan Pencabutan bagi Pengandal

Pengandal harus memvalidasi setiap Sertifikat terhadap CRL dan/atau OCSP terbaru yang diterbitkan oleh PSrE Privy sebagaimana dapat diakses melalui Repositori dan/atau URL https://ocsp.privyca.id.

4.9.7. Frekuensi Penerbitan CRL

CRL diperbarui secara berkala dalam jangka waktu maksimal 1 x 24 jam dan dapat diakses melalui Repositori.

4.9.8. Latensi Maksimum untuk CRL

CRL dipublikasikan dalam jangka waktu 30 menit setelah CRL diperbarui.

4.9.9. Ketersediaan Pemeriksaan Pencabutan/Status secara Daring

PSrE Privy menyediakan layanan pengecekan informasi status Sertifikat melalui OCSP yang selalu tersedia pada URL https://ocsp.privyca.id, diluar waktu pemeliharaan yang ditentukan oleh PSrE Privy.

4.9.10. Persyaratan Pemeriksaan Pencabutan Secara Daring

Repositori PSrE Privy harus berisi dan mempublikasi daftar semua responder OCSP yang mereka operasikan. Jika OCSP diimplementasikan, semua layanan harus sesuai dengan standar *Internet Engineering Task Force* (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas.

4.9.11. Bentuk lain dari Pengumuman Pencabutan yang Disediakan

Tidak ada ketentuan.

4.9.12. Persyaratan Khusus Kebocoran Kunci

Tidak ada ketentuan.

4.9.13. Kondisi untuk Pembekuan Sertifikat

PSrE Privy tidak melakukan pembekuan Sertifikat.

4.9.14. Pihak yang dapat Mengajukan Permohonan Pembekuan

Tidak ada ketentuan.

4.9.15. Prosedur Permohonan Pembekuan

Tidak ada ketentuan.

4.9.16. Jangka waktu Masa Pembekuan

Tidak ada ketentuan.

4.10. Layanan Status Sertifikat

4.10.1. Karakteristik Operasional

PSrE Privy menyediakan layanan pemeriksaan informasi status Sertifikat melalui CRL atau OCSP.

4.10.2. Ketersediaan Layanan

Layanan CRL atau OCSP tersedia sepanjang waktu, diluar waktu pemeliharaan yang ditentukan oleh PSrE Privy.

4.10.3. Fitur Opsional

Tidak ada ketentuan.

4.11. Akhir Masa Berlangganan

Masa Kepemilikan Sertifikat berakhir ketika Sertifikat dicabut atau masa validitasnya berakhir. PSrE Privy memiliki prosedur untuk mengakhiri masa berlangganan.

4.12. Pemulihan dan Eskro Kunci

4.12.1. Kebijakan dan Praktik Pemulihan dan Eskro Kunci

Tidak ada ketentuan.

4.12.2. Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci

Tidak ada ketentuan.

5. Fasilitas, Manajemen, dan Kontrol Operasi

5.1. Kontrol Fisik

PSrE Privy melakukan kontrol terhadap keamanan Pusat Data sebagaimana diatur dalam CPS ini. "Pusat Data" mengacu kepada server yang ditempatkan melalui media penyimpanan yang menjalankan siklus operasi Sertifikat dan diletakan secara fisik dalam suatu lemari penyimpanan khusus.

5.1.1. Lokasi dan Konstruksi

Seluruh fasilitas komputasi yang digunakan untuk menjalankan Layanan PSrE Privy ditempatkan dalam Pusat Data dan Pusat Data Pemulihan di dalam wilayah Negara Kesatuan Republik Indonesia. Pusat Data tersebut dilengkapi dengan berbagai mekanisme keamanan baik secara logis dan fisik untuk menjaga agar *non-Trusted Roles* tidak dapat memiliki akses ke Pusat Data. Bangunan Pusat Data dibangun dengan kualitas premium. Pusat Data harus berada di lokasi yang ketika terjadi bencana alam baik pada Pusat Data, Pusat Data Pemulihan tidak ikut terkena dampaknya. Pusat Data Pemulihan PSrE Privy telah ditempatkan dengan mempertimbangkan availability layanan PSrE Privy.

5.1.2. Akses Fisik

Untuk mendapatkan akses masuk ke Pusat Data, maka harus dilakukan pendaftaran terlebih dahulu dan melalui penjagaan dengan setidaknya 4 (empat) lapis pengamanan antara lain akses yang dijaga 24 (dua puluh empat) jam oleh sekuriti, kamera pengawas, beberapa lapis pintu keamanan, akses masuk 3 (tiga) faktor autentikasi, dan kunci pengaman pada media penyimpanan. Hanya pihak tertentu yang termasuk pada *Trusted Roles* yang mendapat akses untuk masuk ke Pusat Data.

PSrE Privy melakukan review terhadap akses fisik setiap 1 x 24 jam.

Privy melakukan pengamanan fisik terhadap pengamanan Pusat Data dengan melakukan:

1. Memastikan tidak ada akses ke Pusat Data tanpa izin;
2. Menyimpan semua media yang berisi informasi teks yang bernilai tinggi dan sensitif dalam media yang aman;
3. Melakukan monitor terhadap akses ke Pusat Data;
4. Memelihara dan memeriksa log akses secara berkala; dan
5. Memastikan kendali akses ke modul kriptografis dan sistem komputer Privy minimal 2 (dua) orang.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat Privy dilaksanakan jika fasilitas ditinggalkan. Setidaknya proses pemeriksaan memverifikasi hal-hal sebagai berikut:

1. Semua security container sudah diamankan;
2. Sistem keamanan fisik berfungsi dengan baik; dan

Area diamankan dari akses yang tidak berhak;
Pemeriksaan dibuktikan dengan log yang dapat dipertanggungjawabkan. Jika fasilitas tidak ditempati setiap waktu, maka orang terakhir yang meninggalkan fasilitas membuat lembaran *sign-out* yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

5.1.3. Listrik dan Pendingin Ruangan

Fasilitas dan Pusat Data Privy dilengkapi dengan daya listrik yang tinggi dan didukung dengan cadangan listrik dari *Uninterrupted Power Supply* (UPS) dan generator listrik yang bekerja reaktif terhadap pemadaman listrik yang mampu bekerja selama minimal 6 jam saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

Pusat Data juga dilengkapi dengan menara (*tower*) pendingin ruangan yang menyesuaikan agar temperatur dan tingkat kelembaban ruangan terkendali untuk menjaga kinerja mesin dan peralatan Privy.

5.1.4. Keterpaparan Air

Pusat Data PSrE Privy berada di kawasan bebas banjir dan terletak tinggi diatas permukaan laut. Selain itu Pusat Data juga dilengkapi dengan alat pendeteksi kebocoran air dan *Environment Monitoring System* yang dapat mendeteksi tinggi kadar kelembapan udara.

5.1.5. Pencegahan dan Perlindungan Kebakaran

Pusat Data dilengkapi dengan sensor deteksi asap, dan sistem pemadam kebakaran otomatis.

5.1.6. Media Penyimpanan

Media penyimpanan disimpan dan dilindungi dari hal-hal yang dapat menyebabkan kerusakan, pencurian dan akses yang tidak berhak. Salinan yang digunakan sebagai cadangan terhadap media penyimpanan tersebut disimpan dan diamankan di lokasi yang terpisah dari Pusat Data.

5.1.7. Pembuangan Limbah

Seluruh dokumen dan perangkat keras yang sudah tidak digunakan dihancurkan dan dibuang dengan cara yang aman dan wajar agar perangkat tersebut tidak dapat digunakan lagi.

5.1.8. Cadangan *Off-site*

PSrE Privy menyiapkan sistem pencadangan yang cukup untuk digunakan dalam rangka pemulihan dari kegagalan sistem. Sistem pencadangan tersebut dilakukan dengan cara menyalin data yang yang ada pada Pusat Data dan Pusat Pemulihan Data secara manual ke sebuah media penyimpanan, untuk selanjutnya disimpan di lokasi yang aman dan berada di lokasi

yang terpisah dengan Pusat Data dan Pusat Pemulihan Data. Hanya sistem pencadangan yang disimpan terakhir yang digunakan untuk pemulihan.

5.1.9. Pusat Data Pemulihan

PSrE Privy memiliki Pusat Data Pemulihan di dalam wilayah Negara Kesatuan Republik Indonesia. Pusat Data Pemulihan merupakan fasilitas yang digunakan PSrE Privy untuk memulihkan infrastruktur atau layanan pasca bencana dan memiliki jarak tertentu dengan Pusat Data. Ketentuan pada bagian 5.1.1 – 5.1.8 juga berlaku terhadap Pusat Data Pemulihan.

5.2. Kontrol Prosedural

5.2.1. *Trusted Roles*

Posisi Peran Terpercaya (*Trusted Roles*) termasuk namun tidak terbatas pada:

a. Koordinator
b. *Policy Authority* (PA)
c. Staff PA
d. Administrator *Network*
e. Administrator Aplikasi
f. Administrator OS
g. Administrator HSM
h. Registration Authority (RA)
i. Staff RA
j. Registrasi
k. Key Custodian
l. Internal Audit

Peran tersebut secara detil dijelaskan melalui kebijakan internal perusahaan dan merupakan dokumen yang bersifat rahasia.

5.2.2. Jumlah Orang yang Diperlukan Setiap Tugas

PSrE Privy mensyaratkan setidaknya terdapat 2 (dua) orang ditambah dengan 2 (dua) orang cadangan yang mengisi posisi *Trusted Roles* untuk menjalankan setiap tindakan *Trusted Roles*. Adapun khusus untuk Koordinator dan PA terdiri dari 1 (satu) orang tanpa cadangan. PSrE Privy akan menggunakan prosedur tertentu untuk memastikan bahwa tindakan *Trusted Roles* tidak dapat dijalankan oleh 1 (satu) orang saja.

5.2.3. Identifikasi dan Autentikasi untuk Setiap Peran

Sebelum mengisi posisi *Trusted Roles*, maka individu akan diperiksa latar belakangnya sesuai dengan ketentuan pada bagian 5.3.1 dan 5.3.2 untuk memastikan bahwa *Trusted Roles* diisi oleh orang yang tepat. Autentikasi *Trusted Roles* dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi tersebut dilakukan berdasarkan identifikasi orang yang mengakses ruangan atau sistem dan hak akses yang diatur sesuai dengan peran dan tanggung jawab orang tersebut. Sebelum menjalankan tugas sebagai *Trusted Roles,* Privy akan menerbitkan surat penugasan bagi para individu terkait tersebut.

5.2.4. Peran yang Memerlukan Pemisahan Tugas

PSrE Privy memastikan bahwa 1 (satu) orang hanya dapat mengisi 1 (satu) peran *Trusted Roles* pada saat yang bersamaan untuk peran-peran berikut:

a. *Policy Authority* dan administrator operasional;
b. Internal audit dan semua peran lain; dan
c. Pengembang aplikasi dan semua peran lain.

5.3. Kontrol Personil

5.3.1. Persyaratan Kualifikasi, Pengalaman, dan Perizinan

Karyawan Privy tunduk pada pemeriksaan latar belakang dan pemeriksaan catatan kriminal yang dilakukan oleh Privy. Privy berdasarkan kebijaksanaannya memastikan karyawan Privy diisi oleh orang yang berpengalaman, terampil, terpercaya, dan

berintegritas. Untuk memastikan hal tersebut maka Privy melakukan pemeriksaan latar belakang, termasuk namun tidak terbatas, terhadap pemeriksaan identitas, latar belakang pendidikan, pekerjaan, kualifikasi, dan pengalaman, dan pemeriksaan catatan kriminal yang dibuktikan dengan SKCK dari Kepolisian Republik Indonesia.

5.3.2. Prosedur Pemeriksaan Latar Belakang

Diatur melalui bagian 5.3.1.

5.3.3. Persyaratan Pelatihan

Setiap orang yang diterima untuk mengisi posisi *Trusted Roles* menerima pelatihan yang mencakup, namun tidak terbatas, kepada hal-hal ini:

a. Konsep dasar mengenai PKI;
b. CP/CPS;
c. Internal *Standard Operational Procedure* (SOP) terkait dengan kegiatan operasional PKI;
d. Dokumentasi mengenai tata cara menggunakan sistem PKI;
e. Pemulihan bencana dan keberlangsungan bisnis; dan
f. Pemahaman mengenai pentingnya keamanan siber, terkhusus mengenai taktik *phishing* dan *social engineering*.

Evaluasi terhadap kecukupan kompetensi personil PSrE Privy dilakukan minimal 1 (satu) kali dalam setahun.

5.3.4. Frekuensi Pelatihan Ulang dan Persyaratannya

Karyawan yang mengisi posisi *Trusted Roles* memiliki keahlian dan kemampuan yang konsisten dengan perkembangan industri PKI. PSrE Privy melakukan pelatihan ulang secara rutin minimal setiap 1 (satu) kali dalam setahun. Dalam hal PSrE Privy mengubah kebijakan operasional PKI, maka PSrE Privy memberikan pelatihan sesuai dengan perubahan kebijakan yang diambil oleh PSrE Privy.

5.3.5. Frekuensi dan Urutan Rotasi Pekerjaan

PSrE Privy memastikan bahwa dalam hal terjadi perubahan atau rotasi pegawai, maka hal tersebut tidak berdampak negatif terhadap efektivitas operasional layanan atau keamanan sistem.

5.3.6. Sanksi terhadap Tindakan yang Tidak Sah

Karyawan yang tidak menjalankan perannya sesuai dengan CPS ini, baik secara di sengaja maupun tidak, akan menerima sanksi berdasarkan kebijakan PSrE Privy. Untuk karyawan yang berperan *sebagai Trusted Roles* dan tidak menjalankan perannya sesuai CPS ini, akan dikenakan sanksi berupa pencabutan dari fungsi *Trusted Roles* sampai ada peninjauan lebih lanjut dari manajemen perusahaan.

5.3.7. Persyaratan Kontraktor Independen

Kontraktor independent yang dipekerjakan untuk menjalankan fungsi *Trusted Roles* juga harus tunduk kepada ketentuan yang diatur di dalam CPS ini.

5.3.8. Dokumentasi yang Disediakan untuk Personil

Karyawan akan dibekali dengan dokumentasi pendukung yang dibutuhkan untuk menjalankan perannya sesuai dengan CPS ini.

5.4. Prosedur Log Audit

5.4.1. Jenis Peristiwa yang Direkam

Informasi yang akan disimpan di dalam log termasuk namun tidak terbatas kepada:

a. Jenis kejadian;
b. Nomor seri atau urutan rekaman;
c. Tanggal dan waktu kejadian;
d. Sumber perekaman;
e. Indikator sukses atau gagal yang sesuai; dan
f. Identitas dari entitas dan/atau operator yang menyebabkan kejadian.

PSrE Privy mengaktifkan semua fitur audit keamanan dari sistem operasi PSrE dan RA, serta aplikasi PSrE, Validasi Otoritas, dan RA yang dipersyaratkan oleh CPS ini. PSrE Privy harus memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan *Trusted Roles* dalam operasional PSrE Privy dapat dilacak. Waktu disinkronkan dengan otoritas sumber waktu dengan ketelitian paling lama 1 (satu) menit.

5.4.2. Frekuensi Pemrosesan Log

PSrE Privy melakukan pemeriksaan terhadap log yang sudah disimpan minimal 1 (satu) minggu sekali. Pemeriksaan tersebut dilakukan untuk memverifikasi bahwa log tersebut tidak dirusak, diacak, dan tidak adanya jenis kehilangan lain terhadap log.

Pemeriksaan dilanjutkan dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan yang muncul dalam log.

5.4.3. Masa Retensi untuk Log Audit

PSrE Privy menyimpan log audit dalam jangka waktu 1 (satu) tahun. Jangka waktu ini dapat berubah sewaktu-waktu sesuai dengan hukum yang berlaku.

5.4.4. Perlindungan Log Audit

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

5.4.5. Prosedur Pencadangan Log Audit

Log audit disalin untuk dicadangkan dengan mekanisme *Hot Backup*. Cadangan log tersebut disimpan secara terpisah dari Pusat Data.

5.4.6. Sistem Pengumpulan Audit (Internal atau Eksternal)

Proses log untuk audit berjalan secara otomatis sejak sistem dinyalakan dan sebaliknya berhenti jika sistem dimatikan. *Trusted Roles* dapat membuat log audit secara manual dan terpisah.

5.4.7. Pemberitahuan ke Subjek yang Menyebabkan Peristiwa

Tidak ada ketentuan.

5.4.8. Penilaian Kerentanan

PSrE Privy melakukan penilaian kerentanan, yang tidak terbatas hanya kepada *penetration testing, stress test dan load test*, secara berkala untuk memastikan bahwa sistem secara andal tanpa adanya ancaman secara internal dan eksternal yang dapat berdampak kepada sistem PSrE Privy. Penilaian kerentanan dilakukan paling tidak sekali setahun.

Hasil dari penilaian kerentanan menjadi informasi yang dirahasiakan dan digunakan untuk menjaga dan meningkatkan keamanan sistem PSrE Privy.

5.5. Pengarsipan Catatan

5.5.1. Jenis Catatan yang Diarsipkan

Berikut merupakan catatan yang disimpan dalam arsip:

a. Siklus hidup operasi Sertifikat termasuk permohonan Sertifikat, penolakan permohonan Sertifikat, dan permintaan pencabutan Sertifikat;
b. Semua Sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh PSrE Privy;
c. Log Audit;
d. Konfigurasi sistem PKI; dan
e. Dokumen yang tersedia di Repositori termasuk amandemen dan perubahannya.

f. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI):
   i. Penunjukkan dan pencabutan peran dan kewenangan;
   ii. Akses pengunjung ke fasilitas PsrE;
   iii. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
   iv. Deteksi dan tindakan terhadap insiden keamanan
   v. Latihan keadaan darurat;
   vi. Tindakan dan penilaian risiko;
   vii. Perubahan aset, prosedur dan tanggung jawab; dan
   viii. Perubahan dokumentasi.

5.5.2. Masa Retensi Arsip

PSrE Privy menyimpan arsip selama 5 (lima) tahun. Perangkat lunak dan perangkat keras yang dibutuhkan untuk membaca arsip dipelihara selama masa retensi.

5.5.3. Perlindungan Arsip

PSrE Privy menjaga agar arsip dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah dan memelihara arsip dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan tersebut.

5.5.4. Prosedur Pencadangan Arsip

Tidak ada ketentuan.

5.5.5. Persyaratan Stempel Waktu Pencatatan

Seluruh catatan diberikan stempel waktu (*time stamping*) secara otomatis sejak catatan tersebut terekam.

5.5.6. Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip dilakukan secara internal oleh Privy.

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Permohonan untuk memperoleh informasi di dalam arsip hanya dapat diberikan oleh pihak yang dipercayakan melalui *Trusted Roles.* Sedikitnya 1 (satu) kali dalam setahun, sampel dari arsip akan diperiksa oleh *Trusted Roles* yang bertanggung jawab terhadap hal tersebut untuk memeriksa integritas dari informasi yang terekam di dalam arsip.

5.6. Pergantian Kunci

Dalam hal terjadi hal yang membahayakan PKI Privy, untuk meminimalisir risiko terhadap bocornya Kunci Privat PSrE Privy, kunci tersebut diganti dengan kunci baru yang digunakan untuk penandatangan Sertifikat. PSrE Privy melakukan pemberitahuan kepada Pemegang Sertifikat dan Pengandal dalam hal terjadi penggantian kunci baru PSrE Privy tersebut.

Sertifikat PSrE Privy yang masih berlaku, akan tersedia untuk memverifikasi tanda tangan yang lama sampai semua Sertifikat yang ditandatangani oleh Kunci Privat PSrE Privy yang terkait tersebut juga sudah kedaluwarsa. Jika Kunci Privat PSrE Privy yang lama digunakan untuk menandatangani CRL, kunci yang lama harus disimpan dan dilindungi.

5.7. Pemulihan Bencana dan Kondisi Terkompromi.

5.7.1. Prosedur Penanganan Insiden dan Keadaan Terkompromi

Dalam hal terjadi hal yang membahayakan pelayanan PKI Privy, PSrE Privy segera melakukan investigasi sesuai prosedur yang telah ditentukan untuk memeriksa dan memperhitungkan dampak dari bahaya tersebut. Jika PKI Privy memang dalam keadaan bahaya atau dalam keadaan terkompromi yang menyebabkan Sertifikat yang diterbitkan oleh PSrE Privy harus dicabut, maka Sertifikat baru harus segera diterbitkan.

PSrE Privy akan menginformasikan kepada PSrE Induk dalam hal:

a. terjadi insiden serangan Denial of Service yang berdampak berhentinya pelayanan operasional Privy;

b. sistem PSrE Privy terkompromi;
c. adanya upaya untuk menembus sistem PSrE Privy baik secara fisik maupun elektronik yang yang berdampak berhentinya pelayanan operasional Privy;
d. Insiden yang mencegah atau menghambat penerbitan CRL dalam waktu 24 jam dari waktu yang ditentukan;
e. CRL dan/atau OCSP responder tidak dapat diakses oleh publik dikarenakan adanya insiden serangan seperti Denial of Service dan upaya menembus sistem Privy.

PSrE Privy juga memberikan laporan berkala kepada PSrE Induk terkait dengan insiden dan gangguan yang terjadi dalam kegiatan PSrE Privy.

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

Jika peralatan PKI Privy mengalami kerusakan atau berhenti berfungsi namun Kunci Privat masih tetap berfungsi dan tidak mengalami kerusakan, maka operasi PKI harus dengan segera dijalankan kembali dengan mengutamakan kemampuan sistem PKI untuk membangkitkan status informasi Sertifikat sesuai dengan rencana pemulihan bencana PSrE Privy.

Jika Pasangan Kunci PSrE Privy rusak, operasional PSrE Privy harus dilakukan kembali secepat mungkin dengan memberikan prioritas ke pembangkitan Pasangan Kunci Privy baru. PSrE Privy harus membangkitkan Pasangan Kunci PSrE baru sesuai dengan prosedur yang ditetapkan dalam CPS ini.

PSrE Privy melakukan pemberitahuan kepada PA sesegera mungkin apabila ketentuan dalam bagian ini terjadi.

5.7.3. Prosedur Kunci Privat Entitas Terkompromi

Dalam keadaan dimana Kunci Privat PSrE Privy terkompromi, hilang, hancur, atau dicurigai terkompromi, maka setelah dilakukan investigasi, PSrE Privy harus:

1. Segera memutuskan untuk mencabut seluruh Sertifikat yang telah diterbitkan dan membangkitkan Pasangan Kunci Privy yang baru;
2. Dengan segera akan memberikan pengumuman kepada Pemegang Sertifikat dan Pengandal melalui Situs Privy mengenai pencabutan Sertifikat yang disebabkan karena hal tersebut;
3. Menyelidiki penyebab kompromi atau kerugian dan Kembali yang harus diambil untuk mencegah kompromi tersebut terulang Kembali.

5.7.4. Kapabilitas Keberlangsungan Bisnis Setelah Suatu Bencana

PsrE Privy melakukan *mirroring system* sebagai cadangan layanan PKI di tempat yang terpisah dengan Pusat Data sebagai bagian dari rencana pemulihan bencana. Dalam hal layanan Privy terhentikan yang diakibatkan oleh musibah, maka PSrE Privy segera menjalankan layanan PKI-nya melalui cadangan layanan PKI tersebut, hingga Pusat Data pulih dan digunakan seperti semula paling lambat 24 (dua puluh empat) jam setelah terjadi bencana.

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan PSrE Privy rusak secara fisik dan semua salinan Kunci Privat PSrE Privy hancur, PSrE Privy harus meminta agar Sertifikatnya dicabut. PSrE Privy mengikuti ketentuan sebagaimana diatur pada bagian 5.7.3

5.8. Pengakhiran CA atau RA

Dalam hal PSrE Privy mengakhiri layanan-nya, maka:

a. PSrE Privy memberikan pemberitahuan melalui surat elektronik kepada para pihak yang terlibat dalam siklus operasional Sertifikat,

termasuk kepada PSrE Induk, Pemegang Sertifikat, Pengandal, dan RA;

b. Memastikan bahwa informasi status Sertifikat tetap dapat diakses untuk jangka waktu 1 (satu) tahun setelah pengakhiran layanan;
c. Menjamin agar proses pencabutan semua Sertifikat pada saat penutupan dilakukan sampai selesai;
d. Memastikan agar segala gangguan yang diakibatkan oleh penutupan Privy dapat diminimalisasi;
e. Mengirimkan informasi CRL terakhir kepada Pemegang Sertifikat dan Pengandal yang merupakan pengguna layanan Privy; dan
f. Menghancurkan sistem PKI Privy yang berisi Kunci Privat PSrE Privy dan Kunci Privat Pemegang Sertifikat.

Selain hal yang dikemukakan diatas, hak dan kewajiban yang berlaku bagi para pihak adalah sesuai dengan kesepakatan, sebagaimana telah disepakati dalam Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, Kebijakan Privasi Privy, dan/ atau perjanjian lainnya.

6. Kontrol Keamanan Teknis

6.1. Pembangkitan dan Instalasi Pasangan Kunci

6.1.1. Pembangkitan Pasangan Kunci

Pasangan Kunci PSrE Privy dibangkitkan melalui sistem PKI Privy, dan Kunci Privat PSrE Privy tidak boleh meninggalkan perangkat keras modul kriptografi (yang memenuhi persyaratan *Federal Information Protection Standards* (FIPS)-140-2 Level 3) yang terhubung dengan sistem tersebut.

Untuk Pasangan Kunci Pemegang Sertifikat yang dibangkitkan oleh Privy, Kunci Privatnya disimpan dan diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS-140-2 Level 2.

Dalam proses pembangkitan kunci, PSrE Privy menerapkan kendali multipersonel dan menyiapkan jejak audit yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. 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.

6.1.2. Pengiriman Kunci Privat Kepada Pemegang Sertifikat

Privy tidak melakukan pengiriman Kunci Privat kepada Pemegang Sertifikat.

6.1.3. Pengiriman Kunci Publik ke Privy

Pasangan Kunci Pemegang Sertifikat dibangkitkan oleh Privy sehingga Privy secara langsung menyimpan dan melekatkan Kunci Publik Pemegang Sertifikat pada Sertifikat Pemegang Sertifikat setelah penerbitan pasangan kunci Pemegang Sertifikat dilakukan oleh Privy.

6.1.4. Pengiriman Kunci Publik PsrE Privy ke Pengandal

Kunci Publik PSrE Privy tidak dikirim kepada Pengandal, namun Pengandal dapat mengakses Kunci Publik tersebut melalui Repositori PsrE Privy. Penjelasan tanggung jawab tentang publikasi dan repositori sertifikat mengacu pada bagian 2.1.

6.1.5. Ukuran Kunci

Sertifikat	*Digest Algorithm*	*Encryption Algorithm*	Panjang Kunci
Privy CA	SHA-256	RSA	4096-bit
End User	SHA-256	ECC	256-bit

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

Privy membangkitkan Pasangan Kunci PSrE Privy dengan menggunakan modul kriptografi sesuai standar FIPS 140-2 level 3 dan menggunakan suatu metode yang wajar untuk memvalidasi kesesuaian Kunci Publik yaitu FIPS 186-4. Privy melakukan pemeriksaan secara berkala untuk menguji ukuran

Kunci dan memastikan pemutakhiran berdasarkan standar keamanan industri dan persyaratan regulasi.

6.1.7. Tujuan Penggunaan Kunci (pada *field key usage* – X509 v3)

Kunci Privat PSrE Privy dan Pemegang Sertifikat digunakan sesuai dengan penjelasan yang disampaikan pada Profil Sertifikat sebagaimana dimaksud pada bagian 10.

6.2. Kendali Kunci Privat dan Kendali Modul Teknis Kriptografi

Untuk melindungi Kunci Privat PSrE Privy dari penyalahgunaan atau pengaksesan secara tidak sah, Privy melakukan upaya terbaik untuk:

a. Mengamankan semua akses dan kontrol pasangan kunci.
b. Mengimplementasikan prosedur yang mampu mencegah, menjaga, mengawasi dan melakukan mitigasi terhadap informasi rahasia dari akses tidak sah, perubahan tidak sah, kerusakan data, dan kebocoran informasi rahasia.

6.2.1. Kendali Kunci Privat dan Kendali Teknis Modul Kriptografi

Kunci Privat PSrE Privy dan Pemegang Sertifikat dibangkitkan oleh perangkat modul kriptografi yang memenuhi standar FIPS 140-2 Level 3. Untuk operasi penandatanganan, Privy juga menggunakan perangkat modul kriptografi dengan standar yang sama.

6.2.2. Kendali Multipersonel (n dari m) Kunci Privat

Privy menerapkan mekanisme teknis dan prosedur yang mensyaratkan partisipasi dari beberapa (m dari n) *Trusted Roles* untuk melakukan operasi dan fungsi kriptografi yang sensitif seperti namun tidak terbatas kepada akses dan pengaktifan Kunci Privat PSrE Privy.

6.2.3. Eskro Kunci Privat

Kunci Privat PSrE Privy tidak boleh dan tidak akan pernah dititipkan sebagaimana diatur dalam bagian 4.12.1.

6.2.4. Cadangan (*Backup*) Kunci Privat

Untuk menjaga keberlangsungan layanan, pasangan Kunci PSrE Privy dicadangkan dan disimpan secara aman dengan kendali multi personel yang sama dengan Pasangan Kunci asli.

Pasangan Kunci Pemegang Sertifikat disalin dan dijaga oleh Privy dengan usaha terbaik. Semua salinan Pasangan Kunci yang dibangkitkan dilindungi dengan standar dan mekanisme yang sama dengan Pasangan Kunci asli. Salinan Pasangan Kunci tersebut disimpan dalam lokasi fisik yang berbeda dari Pusat Data.

6.2.5. Pengarsipan Kunci Privat

Kunci Privat PSrE Privy dan Kunci Privat *Signing* Pemegang Sertifikat tidak diarsipkan.

6.2.6. Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci Privat PSrE Privy dibangkitkan dan disimpan dalam modul kriptografi. Jika ada penyalinan dengan tujuan kelangsungan dan pemulihan layanan, Kunci Privat akan disalin dalam keadaan terenkripsi ke modul kriptografi dengan standar/level keamanan yang sama. Di luar modul kriptografi, Kunci Privat PSrE Privy tidak akan pernah ditemukan dalam bentuk teks sederhana (*plaintext*). Dalam hal PSrE Privy mengetahui bahwa Kunci Privat disampaikan kepada orang atau entitas yang tidak berwenang, maka PSrE Privy akan mencabut semua Sertifikat yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.

6.2.7. Penyimpanan Kunci Privat pada Modul Kriptografi

Kunci Privat PSrE Privy disimpan pada modul kriptografi yang memenuhi standar FIPS 140-2 minimum level 3 dalam keadaan terenkripsi dan dilindungi oleh mekanisme teknis yang menjaga kunci dari akses tidak sah. Sedangkan untuk Kunci Privat

Pemegang Sertifikat disimpan pada modul kriptografi yang memenuhi standar FIPS 140-2 minimum level 2.

6.2.8. Metode Pengaktifan Kunci Privat

Kunci Privat PSrE Privy diaktifkan dengan mekanisme yang telah disediakan oleh penyedia modul kriptografi dan sesuai dengan prosedur dan standar keamanan informasi. Operasi pengaktifan Kunci Privat Privy melalui kendali multi personel yang telah dinyatakan dalam CPS di bagian 5.2.2.

Pengaktifan dan akses Kunci Privat Pemegang Sertifikat dilindungi dengan mekanisme keamanan yang dikendalikan, diawasi, dijaga, dan diatur oleh Privy. Pemegang Sertifikat bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemegang Sertifikat Privy.

6.2.9. Metode Penonaktifan Kunci Privat

Privy melakukan pengawasan terhadap modul kriptografis yang sudah diaktivasi dan memastikan modul kriptografis tidak ditinggal tanpa pengawasan dan tidak dapat diakses secara tidak sah. Dalam hal modul kriptografis harus dinonaktifkan, maka akan dilakukan oleh *Trusted Role(s)* terkait.

6.2.10. Metode Menghancurkan Kunci Privat

Trusted Role(s) menghancurkan Kunci Privat PSrE Privy ketika Kunci Privat tidak lagi diperlukan untuk kelangsungan layanan dengan cara menghapus atau menghancurkan Kunci Privat beserta dengan cadangannya sesuai dengan prosedur yang telah disediakan oleh penyedia modul kriptografi (termasuk diantaranya dengan cara *factory reset*) atau dengan cara menghancurkan fisik dari komponen perangkat keras Privy pada lingkungan fisik yang aman.

Kunci Privat Pemegang Sertifikat dihancurkan ketika Sertifikat atau Kunci Privat tidak lagi diperlukan. Hal ini dilakukan dengan mekanisme teknis tertentu yang dapat menjamin tidak ada kehilangan, pencurian, atau penggunaan tidak sah dari Kunci Privat maupun Sertifikat terkait.

Penghancuran Kunci Privat Privy dicatat dalam log sesuai ketentuan pencatatan log pada bagian 5.4.

6.2.11. Peringkat Modul Kriptografi

Sesuai dengan yang tercantum pada bagian 6.2.1.

6.3. Aspek Lain dari Manajemen Pasangan Kunci

6.3.1. Pengarsipan Kunci Publik

Privy mengarsipkan setiap Kunci Publik yang dibangkitkan minimal 5 (lima) tahun.

6.3.2. Masa Operasional Sertifikat dan Masa Penggunaan Pasangan Kunci

Periode operasi pasangan kunci ditentukan oleh periode operasional Sertifikat yang sesuai. Jangka waktu operasional maksimum pasangan kunci ditentukan sebagai berikut:

Jenis Sertifikat	Jangka Waktu Operasional
Privy CA Class 3	10 Tahun
Privy CA Class 4	10 Tahun
Sertifikat Kelas 3	1 Tahun
Sertifikat Kelas 4	1 Tahun
Time Stamp Authority	1 Tahun
OCSP Responder	1 Tahun

6.4. Data Aktivasi

6.4.1. Pembangkitan dan Instalasi Data Aktivasi

Pembangkitan dan penggunaan data pengaktifan untuk mengaktifkan Kunci Privat PSrE Privy dilakukan melalui upacara

kunci. Data pengaktifan dibangkitkan secara otomatis oleh modul kriptografi dengan menggunakan kartu pintar yang dilindungi oleh kata sandi yang kuat dan harus memenuhi kuorum yang telah ditentukan (n dari m). Kartu pintar diserahkan dan disimpan secara aman kepada *Trusted Roles* yang telah memenuhi kualifikasi yang telah ditentukan dan melalui pengecekan latar belakang.

6.4.2. Perlindungan Data Aktivasi

Data pengaktifan PSrE Privy dilindungi menggunakan mekanisme kontrol akses fisik dan teknologi kriptografi. Data pengaktifan disimpan dalam kartu pintar yang diserahkan kepada *Trusted Roles* dan telah memenuhi kualifikasi dan pengecekan latar belakang yang telah ditentukan.

6.4.3. Aspek Lain dari Data Aktivasi

Data aktivasi Kunci Privat PSrE Privy hanya dikuasakan kepada *Trusted Roles* yang telah ditentukan.

6.5. Kontrol Keamanan Komputer

6.5.1. Persyaratan Teknis Keamanan Komputer Spesifik

Privy memastikan premis dan perangkat keras yang menjaga komponen perangkat lunak Privy aman dari akses yang tidak sah. Privy melaksanakan mekanisme teknis dan prosedur yang memastikan keamanan informasi pada sistem Privy. Semua akses terhadap informasi terkait Privy tercatat dan memerlukan autentikasi identitas berdasarkan pembatasan kontrol akses layanan untuk setiap *Trusted Roles*. Semua akses menjadi catatan audit yang dilindungi untuk tujuan pencegahan dan penanggulangan risiko keamanan informasi.

Fungsi keamanan komputer berikut disediakan oleh kombinasi sistem operasi, perangkat lunak, dan perlindungan fisik yang mencakup namun tidak terbatas kepada:

a. Akses masuk menggunakan autentikasi identitas.

b. Memberikan akses kontrol berdasarkan dokumen kebijakan *user access matrix*.
c. Menyediakan kemampuan dan sumber daya untuk keperluan audit keamanan.
d. Menyediakan jalur dan mekanisme terpercaya untuk akses sistem dengan menggunakan kriptografi untuk sesi komunikasi dan keamanan basis data.
e. Menyediakan perlindungan mandiri untuk sistem operasi
f. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
g. Mewajibkan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
h. Menyediakan perlindungan terhadap kode jahat (*malicious code*);
i. Memberikan kemampuan untuk melakukan pemeriksaan terhadap standar dari perangkat lunak dan perangkat keras yang terpasang dengan standar yang telah ditetapkan melalui kebijakan internal perusahaan.
j. Memberikan kemampuan untuk menerapkan praktik keamanan terbaik industri seperti penggunaan kata sandi yang kuat, penggunaan jalur komunikasi yang terenkripsi, melakukan isolasi terhadap setiap proses domain, dan menyediakan kemampuan melindungi diri sendiri untuk sistem operasi.

Perangkat Privy beroperasi dengan konfigurasi yang telah dievaluasi untuk menjaga standar keamanan komputer.

6.5.2. Peringkat Keamanan Komputer

Privy memastikan bahwa untuk menjamin tingkat keamanan komputer yang digunakan oleh Privy, semua perangkat komputer telah memenuhi persyaratan keamanan FIPS 140-2 Level 1.

6.6. Kendali Teknis Siklus Hidup

6.6.1. Kendali Pengembangan Sistem

Privy melakukan kendali pengembangan sistem sebagai berikut:

1. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;
2. Pengadaan perangkat keras dan perangkat lunak telah dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen yang terdapat dalam perangkat lunak yang dirusak;
3. Pengembangan perangkat keras dan perangkat lunak telah dilakukan dalam sebuah lingkungan yang terkendali dan proses pengembangan didefinisikan dan didokumentasikan;
4. Perangkat keras dan perangkat lunak didedikasikan untuk pelaksanaan aktivitas KPI.
5. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya untuk dimuat ke perangkat. Privy telah melakukan scan secara berkala terhadap kode-kode berbahaya pada perangkat keras dan perangkat lunak; dan
6. Pembaruan perangkat keras dan perangkat lunak dibeli atau dikembangkan dengan cara yang sama dengan perangkat aslinya dan diinstal oleh personel yang terpercaya dan terlatih melalui langkah-langkah yang terdokumentasi.

Privy melakukan pengujian di lingkungan non-produksi terhadap perangkat lunak siap pakai maupun perangkat lunak yang dikembangkan sendiri yang digunakan untuk manajemen produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem atau komponennya telah melalui proses reviu Kontrol Manajemen Perubahan dan persetujuan pihak-pihak terkait.

6.6.2. Kendali Manajemen Keamanan

Segala perubahan pada konfigurasi sistem PKI milik Privy tercatat dan dikontrol oleh prosedur yang telah ditentukan. Prosedur ini mencakup pencegahan akses dan perubahan tidak sah. Semua perangkat yang disediakan oleh pihak ketiga yang

terpasang divalidasi bahwa terbebas dari segala perubahan di luar yang telah ditentukan.

6.6.3. Kendali Keamanan Siklus Hidup

Privy memastikan dan menjaga tingkat kepercayaan dan keamanan semua komponen perangkat lunak dan perangkat keras PKI secara berkala.

6.7. Kendali Keamanan Jaringan

Privy melakukan upaya yang wajar untuk melindungi jaringan semua komponen PKI pada Privy dari serangan seperti namun tidak terbatas pada *Denial of Service* (DoS), *Slowloris*, *Goloris* dan serangan intrusi. Upaya-upaya tersebut termasuk namun tidak terbatas pada penggunaan *firewall*, pembatasan dan penjaringan akses jaringan, dan memasang sistem pengawasan jaringan. Privy juga menggunakan jaringan aman terpercaya yang secara khusus yang telah disediakan untuk akses *remote* komponen PKI. Hanya perangkat lunak jaringan yang diperlukan untuk mengoperasikan layanan Privy yang diizinkan.

6.8. Stempel Waktu

Privy melakukan upaya yang wajar mengkonfigurasi dan menjaga sinkronisasi jam sistem internal semua komponen CA menggunakan *Network Time Protocol*.

Sistem ini digunakan sebagai stempel waktu untuk:

a. Validasi waktu awal penerbitan Sertifikat Induk CA;
b. Waktu pencabutan Sertifikat;
c. Penjadwalan penerbitan CRL; and
d. Validasi waktu penerbitan Sertifikat Pemegang Sertifikat.
e. Respon OCSP

Privy memeriksa dan memastikan bahwa seluruh sistem yang menggunakan stempel waktu tersinkronisasi dengan waktu yang disediakan oleh URL https://www.pool.ntp.org/zone/id. Pencocokan jam merupakan sebuah aktivitas yang dapat diaudit.

7. Profil Sertifikat, CRL, dan OCSP

7.1. Profil Sertifikat

Sertifikat dan *Certificate Revocation List* (CRL) yang diterbitkan oleh Privy tunduk terhadap standar dan spesifikasi yang tercantum pada IETF RFC 5280 Internet X.509 *PKI Certificate and Certificate Revocation List* (CRL) *Profile*.

Semua Sertifikat yang diterbitkan oleh Privy memiliki nomor serial dengan panjang setidaknya 64 bit dengan nilai yang lebih dari nol (0).

Lampiran 1 berisi profil Sertifikat untuk masing-masing klasifikasi Sertifikat yang diterbitkan oleh Privy.

Privy akan melakukan review terhadap profil Sertifikat secara berkala minimal 1 (satu) tahun sekali.

7.1.1. Nomor Versi

Privy menerbitkan semua Sertifikat dengan versi X.509 v3 (mengisi versi *field* dengan integer "2").

7.1.2. *Certificate Extensions*

Lihat Lampiran 1.

7.1.2.1. *Key Usage*

Lihat Lampiran 1.

7.1.2.2. *Certificate Policy Extension*

Lihat Lampiran 1.

7.1.2.3. *Basic Constraint*

Lihat Lampiran 1.

7.1.2.4. *Extended Key Usage*

Lihat Lampiran 1.

7.1.2.5. *CRL Distribution Points*

Lihat Lampiran 1.

7.1.2.6. *Authority Key Identifier*

Lihat Lampiran 1.

7.1.2.7. *Subject Key Identifier*

Lihat Lampiran 1.

7.1.3. *Algorithm-Object Identifiers*

Sertifikat yang diterbitkan oleh Privy menggunakan algoritma sebagai berikut:

Algoritma	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
prime256v1	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) curves(3) prime256v1(7) }

7.1.4. Format Nama

Setiap Sertifikat dengan bidang ini patuh terhadap format penamaan yang tercantum pada bagian 3.1.

7.1.5. Batasan nama

Setiap Sertifikat yang diterbitkan oleh Privy memiliki batasan penamaan sesuai dengan yang tercantum dalam bagian 3.1.

7.1.6. *Certificate Policy Object Identifier*

Privy menggunakan OID untuk CPS Privy sesuai dengan yang tercantum pada bagian 1.2.

7.1.7. Penggunaan Ekstensi Batasan Kebijakan

Tidak ada ketentuan.

7.1.8. Kualifikasi Kebijakan Sintaksis dan Semantik

Tidak ada ketentuan.

7.1.9. Pemrosesan Semantik untuk Ekstensi Kebijakan Sertifikat Kritis

Tidak ada ketentuan.

7.2. Profil CRL

Privy menerbitkan CRL dalam format X.509 versi 2 yang tunduk terhadap standar dan spesifikasi yang tercantum pada IETF RFC 5280.

7.2.1. Nomor-Versi

CRL yang diterbitkan memiliki bidang-bidang sebagai berikut:

a. *Issuer*: Subjek DN dari Privy.
b. *Version*: Versi dari CRL.
c. *Last update*: Tanggal penerbitan CRL.
d. *Next update*: Tanggal ekspektasi penerbitan CRL berikutnya.
e. *Signature algorithm*: Algoritma yang digunakan untuk penandaan CRL.

Untuk daftar Sertifikat yang telah dicabut oleh Privy yang tercantum pada CRL memiliki bidang-bidang sebagai berikut:

a. *Serial number*: Daftar nomor serial setiap Sertifikat yang dicabut.
b. *Revocation date*: Tanggal pencabutan setiap Sertifikat.

7.2.2. Ekstensi-CRL dan Catatan CRL

Privy menerbitkan CRL dengan ekstensi sebagai berikut:

a. *CRL number*: Nomor serial CRL.
b. *Authority Key Identifier*: 160-bit SHA-1 hash dari Kunci Publik Privy

7.3. Profil OCSP

Online Certificate Status Profile (OCSP) yang diatur oleh Privy patuh terhadap standar yang ada pada IETF RFC 6960 dan IETF RFC 5019.

7.3.1. Nomor Versi

Privy menerbitkan respon OCSP versi 1.

7.3.2. Ekstensi OCSP

Tidak ada ketentuan.

8. Audit Kepatuhan dan Penilaian Kelaikan Lainnya

8.1. Frekuensi atau Lingkup Penilaian

Implementasi dari CPS ini dijalankan dengan maksud untuk memenuhi kriteria dari standar yang dikeluarkan oleh Kementerian Komunikasi dan Informatika (Kominfo) dan juga standar industri internasional.

Privy diaudit minimal 1 (satu) kali setahun sebagaimana dipersyaratkan oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik dan juga diaudit sesuai kebutuhan standar industri lainnya seperti *Adobe Approved Trust List* atau *Webtrust for Certification Authorities.*

Privy juga mengirimkan laporan tahunan kepada Kementerian Komunikasi dan Informatika sesuai dengan ketentuan yang diatur di dalam peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik.

8.2. Identitas/kualifikasi Penilai

Audit eksternal dilakukan oleh Penilai Terkualifikasi yang independen, kredibel, memahami dan berpengalaman di bidang keamanan informasi dan PKI, diakui oleh Kominfo untuk sertifikasi dari Kominfo dan/atau diakui oleh AICPA/CICA sebagai penyelenggara jaminan sertifikasi dari *Webtrust* untuk sertifikasi *Webtrust*.

Secara spesifik, kriteria Penilai Terkualifikasi harus memiliki kualifikasi berikut:

a. Penilai harus memiliki tim asesmen independen yang qualified;
b. tidak memiliki konflik kepentingan terhadap PSrE Privy;
c. Penilai harus memiliki kemampuan untuk melakukan audit berdasarkan standar audit dalam ketentuan peraturan perundang-undangan termasuk pengetahuan terkait pemanfaatan layanan yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik Sertifikat, X.509 versi 3 *PKI Certificate Policy and Certification Practices Framework*, Undang-Undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Kominfo terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik;
d. Memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
e. Penilai harus memiliki bukti bahwa dirinya memenuhi kualifikasi penilai untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi seperti antara lain auditor sistem informasi (CISA) atau *IT Security specialist*, akreditasi, lisensi, atau asesmen lain yang sah;
f. Menguasai beberapa 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 professional ; dan
g. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

8.3. Hubungan Penilai dengan Entitas yang Dinilai

Penilai yang dipilih untuk melakukan audit merupakan penilai independen di luar Privy dan telah memiliki hubungan kontraktual dengan Privy dalam melakukan audit.

8.4. Topik Penilaian

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa PSrE Privy beroperasi sesuai dengan CP PSrE Induk yang berlaku dan ketentuan

peraturan perundang-undangan. Penilaian Kelaikan mencakup penilaian CPS Privy yang berlaku terhadap CP PSrE Induk, untuk menentukan bahwa CPS tersebut telah diimplementasikan dan ditegakkan. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen Privy.

8.5. Tindakan yang Diambil Akibat Ketidaksesuaian

Ketika Penilai kepatuhan menemukan adanya ketidaksesuaian antara bagaimana PSrE dirancang atau dioperasikan atau dipelihara terhadap CP PSrE Induk yang berlaku dan CPS ini maka:

a. Mencatat ketidaksesuaian tersebut
b. Penilai kepatuhan harus secara segera menyampaikan temuan tersebut kepada PA; dan
c. PA harus menentukan pemberitahuan atau tindakan perbaikan lebih lanjut mengenai hal-hal yang diperlukan sesuai dengan persyaratan CPS dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan perbaikan tersebut tanpa penundaan.

8.6. Laporan Hasil Penilaian

Laporan hasil penilaian termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh Privy dilaporkan kepada PA, dan Privy meneruskan laporan tersebut kepada pihak-pihak lain yang berkepentingan sesuai dengan kesepakatan di dalam perjanjian dan peraturan perundang-undangan yang berlaku.

8.7. Internal Audit

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan risiko gangguan pada proses bisnis PSrE Privy dengan frekuensi 1 (satu) tahun sekali. Audit internal ini juga dilakukan untuk memeriksa kesesuaian dengan peraturan perundang-undangan.

9. Bisnis Lain dan Masalah Hukum

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

Privy dapat mengenakan biaya berdasarkan penerbitan, penggunaan, dan/atau pembaruan Sertifikat.

9.1.2. Biaya Pengaksesan Sertifikat

Tidak ada ketentuan.

9.1.3. Biaya Pengaksesan Informasi Status atau Pencabutan

Tidak ada ketentuan.

9.1.4. Biaya Layanan Lainnya

Privy dapat mengenakan biaya untuk biaya lain yang belum diatur di CPS ini.

9.1.5. Kebijakan Pengembalian Biaya

Privy tidak mengatur kebijakan pengembalian biaya.

9.2. Tanggung Jawab Keuangan

9.2.1. Cakupan Asuransi

Privy memiliki *Cyber Edge Insurance Policy* dengan batas tanggungan sebesar USD 2.500.000 (Dua Juta Lima Ratus dolar Amerika Serikat) *dan Technology Professional Indemnity Insurance* dengan gabungan batas tanggungan sebesar USD 2.000.000 (Dua juta dolar Amerika Serikat).

9.2.2. Aset Lainnya

Privy menjamin kemampuan keuangan secara wajar dalam menjalankan operasionalnya sebagai PSrE.

9.2.3. Cakupan Asuransi atau Garansi untuk Pemegang Sertifikat

Privy menyediakan Jaminan Asuransi atau Garansi untuk para Pemegang Sertifikat yang diatur dalam dokumen Kebijakan Garansi pada Repositori Privy.

9.3. Kerahasiaan Informasi Bisnis

9.3.1. Cakupan Informasi Rahasia

Hal-hal berikut merupakan informasi rahasia dan mendapatkan perhatian khusus dari Privy:

a. Data Pribadi sebagaimana yang diatur dalam bagian 9.4
b. Kunci Privat Pemegang Sertifikat yang disimpan oleh Privy, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemegang Sertifikat;
c. Rekam jejak audit (audit *logs*) dari sistem PSrE Privy dan RA;
d. Data aktivasi pada saat pengaktifan Kunci Privat PSrE Privy sebagaimana dijabarkan pada bagian 6.4.;
e. Catatan permohonan Sertifikat;
f. Laporan Audit yang dibuat oleh Privy, atau Penilai eksternal maupun internal;
g. Hasil penilaian kerentanan; dan
h. Dokumentasi Proses Bisnis Privy diluar dari yang dipaparkan di CPS ini dan/atau Repositori, seperti *Disaster Recovery Plan* dan *Business Continuity Plans*.

9.3.2. Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia

Informasi lainnya yang tidak termasuk hal yang diatur diatas merupakan informasi publik.

Sertifikat dan informasi mengenai status Sertifikat termasuk kategori informasi publik.

9.3.3. Tanggung Jawab untuk Melindungi Informasi Rahasia

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

a. Pelatihan dan peningkatan *awareness*;
b. Perjanjian kontrak pegawai; dan
c. NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

9.4. Privasi Informasi Pribadi

9.4.1. Rencana Privasi

Privy melindungi data pribadi sesuai dengan ketentuan yang tercantum di dalam Ketentuan Penggunaan Layanan, Kebijakan Privasi, dan/atau Perjanjian Pemegang Sertifikat yang disesuaikan dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi dan informasi dan transaksi elektronik.

9.4.2. Informasi yang Dianggap Pribadi

Informasi yang dianggap pribadi adalah segala informasi tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Dalam hal Layanan Privy, semua informasi tentang Pemegang Sertifikat yang tidak tersedia secara umum melalui Sertifikat yang diterbitkan dianggap sebagai informasi data pribadi. Hal ini juga termasuk untuk data pribadi Pemegang Sertifikat yang Sertifikatnya berhasil diterbitkan dan juga bagi yang penerbitan Sertifikatnya ditolak. Untuk informasi data pribadi bagi calon Pemegang Sertifikat yang penerbitan Sertifikatnya ditolak, Privy akan menghapus informasi data pribadi tersebut paling lambat 30 (tiga puluh) hari kalender dari tanggal diterimanya informasi data pribadi tersebut apabila Pemohon tidak mengajukan kembali terkait dengan penerbitan Sertifikatnya tersebut. Privy hanya menyimpan nomor identitas kependudukan (NIK) calon Pemegang Sertifikat yang penerbitan Sertifikatnya ditolak disertai alasan penolakan.

Privy melindungi semua informasi identitas pribadi Pemegang Sertifikat dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan Pemegang Sertifikat baik terhadap Privy maupun RA. Arsip yang dikelola oleh Privy tidak boleh dirilis kecuali yang diizinkan pada bagian 9.4.1.

9.4.3. Informasi yang tidak Dianggap Pribadi

Informasi yang tidak masuk dalam kategori atau definisi informasi yang dianggap pribadi sebagaimana dijelaskan pada bagian 9.4.2 dan/atau informasi yang termasuk dalam bagian 7 (Sertifikat, CRL, Profil OCSP) dari CPS ini tidak dikenakan perlindungan sebagaimana dijelaskan pada bagian 9.4.2.

9.4.4. Tanggung Jawab Melindungi Informasi Pribadi

Privy bertanggung jawab untuk memproses dan menyimpan informasi pribadi sesuai dengan Kebijakan Privasi dan standar pelindungan yang diwajibkan dalam peraturan perundang-undangan yang berlaku terkait dengan pelindungan data pribadi. Informasi yang disimpan dapat berbentuk digital maupun fisik. *Backup* informasi pribadi harus dienkripsi setiap akan dipindahkan ke media *backup*.

9.4.5. Pemberitahuan dan Persetujuan untuk menggunakan Informasi Pribadi

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran diperlakukan sebagai informasi pribadi sehingga perlu persetujuan tertulis atau terekam dari Pemohon untuk Privy dapat menggunakan informasi tersebut. Privy mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam dokumen Kebijakan Privasi dan Perjanjian Pemegang Sertifikat sesuai dengan peraturan perundang-undangan yang berlaku terkait dengan pelindungan data pribadi. Penggunaan informasi Pribadi harus didasarkan pada pelaksanaan Perjanjian Pemegang Sertifikat atau Perjanjian Pengandal, atau dasar hukum lainnya, yang mengacu pada Kebijakan Privasi dan ketentuan peraturan perundang-undangan yang berlaku.

9.4.6. Pengungkapan Berdasarkan Proses Peradilan atau Administratif

Privy tidak boleh mengungkapkan informasi pribadi kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, aturan dan peraturan pemerintah, atau perintah pengadilan.

9.4.7. Keadaan Pengungkapan Informasi Lainnya

Tidak ada ketentuan.

9.5. Hak atas Kekayaan Intelektual

Privy memiliki dan menguasai hak kekayaan intelektual apapun, termasuk namun tidak terbatas pada paten, hak cipta, merek, rahasia dagang, atas Layanan Privy (termasuk namun tidak terbatas pada seluruh informasi, perangkat lunak, informasi, teks, huruf, angka, susunan warna, gambar, logo, nama, video dan audio, fitur, database, pemilihan dan pengaturan desain). Pemegang Sertifikat dan Pengandal tidak dapat menggunakan hak kekayaan intelektual Privy tanpa persetujuan tertulis terlebih dahulu dari Privy. Privy tidak akan melanggar hak kekayaan intelektual pihak lain.

9.6. Pernyataan dan Jaminan

9.6.1. Pernyataan dan Jaminan PSrE

Privy menyatakan dan menjamin, sejauh yang ditentukan dalam CPS ini, bahwa:

a. Privy mematuhi ketentuan yang diatur di dalam CP PSrE Induk dan CPS ini;
b. Privy menerbitkan dan memperbarui CRL sesuai ketentuan dalam CPS ini;
c. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini dan hanya informasi yang telah diverifikasi yang ditampilkan di Sertifikat;.
d. Privy menampilkan informasi yang dapat diakses secara publik melalui Repositorinya;
e. Kunci Privat Privy terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;

f. Semua pernyataan yang dibuat oleh Privy dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh Privy; dan
g. Setiap Pemegang Sertifikat telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemegang Sertifikat yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

9.6.2. Pernyataan dan Jaminan RA

RA menyatakan dan menjamin, sejauh yang ditentukan dalam CPS ini, bahwa:

a. Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang tidak menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat;
b. Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat;
c. Kegiatan registrasi yang dilakukan oleh RA adalah sesuai dengan CP PSrE Induk, CPS ini dan dituangkan di dalam perjanjian;dan
d. Pemegang Sertifikat dikenakan kewajiban sebagaimana disebutkan dalam bagian 9.6.3. Pemegang Sertifikat mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

9.6.3. Pernyataan dan Jaminan Pemegang Sertifikat

Privy mewajibkan Pemegang Sertifikat dan/atau Pemohon untuk menyetujui dokumen yang berisi persyaratan yang harus dipenuhi terkait perlindungan Kunci Privat dan penggunaan Sertifikat, sebelum Sertifikatnya diterbitkan. Pemegang Sertifikat dan/atau Pemohon menyetujui hal-hal sebagai berikut:

a. Setiap Tanda Tangan Digital yang dibuat dengan menggunakan Kunci Privat yang terkait dengan Kunci Publik

yang ada di dalam Sertifikat adalah Tanda Tangan Digital dari Pemegang Sertifikat dan Sertifikat sudah diterima dan valid (tidak kadaluarsa atau dicabut) saat tanda tangan dibubuhkan;

b. Kunci Privat Pemegang Sertifikat disimpan dan diamankan oleh Privy dan hanya Pemegang Sertifikat yang memiliki akses terhadap Kunci Privat tersebut;
c. Semua pernyataan yang dibuat oleh Pemegang Sertifikat saat proses permohonan pendaftaran adalah benar serta telah melakukan reviu dan verifikasi terhadap informasi yang terdapat pada Sertifikat;
d. Semua informasi yang diberikan oleh Pemegang Sertifikat dan informasi yang berada di dalam Sertifikat adalah benar;
e. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
f. Segera 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 yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat;
g. Segera 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;
h. Segera menghentikan penggunaan Kunci Privat yang terasosiasi dengan Kunci Publik yang Sertifikatnya dicabut;
i. Akan menanggapi instruksi Privy terkait keadaan terkompromi atau penyalahgunaan Sertifikat dalam kurun waktu 48 (empat puluh delapan) jam;
j. Menyetujui dan menerima bahwa Privy diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemegang Sertifikat melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Pemegang

Sertifikat, Syarat dan Ketentuan serta Kebijakan Privasi Privy, atau jika Privy menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising* , penipuan atau pendistribusian *malware*;

k. Pemegang Sertifikat merupakan Pengguna Akhir dan bukan merupakan PSrE, dan tidak menggunakan Kunci Privat yang kunci publiknya tercantum dalam Sertifikat untuk tujuan penandatangan Sertifikat PSrE lain.

9.6.4. Pernyataan dan Jaminan Pengandal

Dalam hal perwakilan dari Pengandal mengandalkan Sertifikat yang diterbitkan oleh Privy, Pengandal menjamin bahwa Pengandal:

a. Memiliki kemampuan teknis untuk menggunakan Sertifikat;
b. Akan selalu dan secara benar memverifikasi informasi yang tercantum di dalam Sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut;
c. Melaporkan langsung kepada PSrE Privy atau RA yang berwenang, jika Pengandal menyadari atau mencurigai bahwa telah terjadi Kunci Privat telah terkompromi;
d. Memiliki informasi yang cukup untuk membuat keputusan berdasarkan informasi sejauh mana Pengandal memilih mempercayai informasi yang tertera pada Sertifikat dan bertanggung jawab untuk memutuskan untuk mempercayai atau tidak informasi tersebut, serta akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pengandal yang ada pada CPS ini,
e. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

9.6.5. Pernyataan dan Jaminan Partisipan Lainnya

Tidak ada ketentuan.

9.7. Pelepasan Jaminan

Privy menyatakan bahwa:

a. Kecuali untuk jaminan yang telah tercantum di dalam CPS dan perjanjian lainnya dan sepanjang diizinkan oleh hukum, Privy mengabaikan semua jaminan atau kondisi lainnya, baik secara tersurat, tersirat, lisan atau tertulis, termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu;
b. Tidak menjamin Sertifikat yang penggunaannya tidak sesuai dengan peruntukannya; dan
c. Tidak menjamin keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam Sertifikat demo atau testing.

9.8. Pembatasan Tanggung Jawab

9.8.1. Pembatasan Tanggung Jawab Privy

Sepanjang Privy telah menjalankan persyaratan operasional siklus Sertifikat sesuai yang tercantum pada bagian 4 CPS ini, maka Privy tidak bertanggung jawab atas setiap akibat atau kerugian yang timbul akibat penggunaan Sertifikat tersebut, termasuk:

a. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat atau Pasangan Kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Pemegang Sertifikat, atau yang diatur dalam Sertifikat itu sendiri;
b. Semua kerusakan yang disebabkan oleh *force majeure*; dan/atau
c. Semua kerusakan yang disebabkan oleh *malware* (seperti *virus* atau *trojans*) di luar perangkat Privy.

9.8.2. Pembatasan Tanggung Jawab RA

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan Privy dan mengacu kepada ketentuan peraturan perundang-undangan. Secara khusus, RA bertanggung jawab atas pendaftaran Pemohon Sertifikat.

9.8.3. Pembatasan Tanggung Jawab Pemegang Sertifikat

Tanggung jawab Pemegang Sertifikat dan/atau batasannya diuraikan dalam kontrak berlangganan atau Perjanjian Pemegang Sertifikat, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak. Pemegang Sertifikat secara khusus bertanggung jawab atas kerugian yang disebabkan oleh kelalaian, pelanggaran kelaikan (*due diligence*) seperti memindahtangankan atau membuat dapat diaksesnya metode atau faktor autentikasi kepada orang lain ataupun tidak mencabut Sertifikatnya yang telah atau diduga terkompromi.

9.9. Ganti Rugi

9.9.1. Ganti Rugi oleh Privy

Privy tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.

Ketentuan ganti rugi lainnya oleh Privy ditentukan berdasarkan Perjanjian Pengandal atau Perjanjian Pemegang Sertifikat termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

9.9.2. Ganti Rugi oleh Pemegang Sertifikat

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

a. pelanggaran yang dilakukan oleh Pemegang Sertifikat terhadap Perjanjian Pemegang Sertifikat, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
b. penggunaan Kunci Privat Pemegang Sertifikat yang tidak sah karena kelalaian Pemegang Sertifikat;
c. penggunaan Sertifikat oleh Pemegang Sertifikat untuk kegiatan melawan hukum;

d. Kegagalan Pemegang Sertifikat untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu pihak manapun;
e. Kegagalan Pemegang Sertifikat untuk melindungi Kunci Privat, menggunakan sistem elektronik yang terpercaya, atau mengambil langkah-langkah yang wajar untuk mencegah kebocoran, kehilangan, pengungkapan, perubahan, atau penggunaan tidak sah Kunci Privat; dan/atau
f. Penggunaan nama oleh Pemegang Sertifikat (termasuk namun tidak terbatas pada *common name*, nama domain, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

9.9.3. Ganti Rugi oleh Pengandal

Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan Privy dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya dan segala tuntutan yang diakibatkan oleh:

a. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pengandal, CPS ini, atau hukum yang berlaku; dan
b. Pengandal tidak memeriksa status Sertifikat untuk menentukan apakah Sertifikat tersebut sudah kadaluwarsa atau sudah dicabut.

9.10. Jangka Waktu dan Pengakhiran

9.10.1. Jangka Waktu

CPS ini berlaku secara efektif setelah dipublikasikan melalui Repositori Privy dan tetap berlaku hingga pemberitahuan lebih lanjut oleh PSrE Privy melalui Situs Privy/Repositori Privy.

9.10.2. Pengakhiran

Pada saat berakhirnya CPS ini, maka seluruh Sertifikat yang terbit berdasarkan CPS tetap berlaku hingga berakhirnya masa validitas dari Sertifikat terakhir berdasarkan CPS tersebut.

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

9.10.3. Dampak dari Pengakhiran dan Ketentuan yang tetap Berlaku

Privy mengkomunikasikan kondisi akibat dari penghentian CPS dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit melalui laman atau Repositori.

9.11. Pemberitahuan Individu dan Komunikasi dengan Partisipan

Para pihak yang terlibat dalam CPS ini dapat mengirimkan pemberitahuan terkait dengan CPS ini kepada Privy melalui alamat dan media komunikasi yang dicantumkan pada Situs Privy dan/atau media komunikasi sebagaimana disebutkan pada bagian 1.5.1. Pemberitahuan dianggap telah diterima apabila pengirim menerima pernyataan penerimaan atau tanggapan tertulis dari Privy. Privy akan memberikan tanggapan atas permintaan yang diberikan paling lambat 20 (dua puluh) hari kerja dari diterimanya permintaan tersebut.

9.12. Amandemen

9.12.1. Prosedur Amandemen

Segala perubahan CPS ditinjau dan disetujui oleh *Policy Authority* Privy. Privy akan menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Amandemen CPS dilakukan sesuai dengan prosedur persetujuan CPS.

9.12.2. Periode dan Mekanisme Pemberitahuan

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

Setiap perubahan terhadap CPS akan dilakukan melalui pengumuman yang dilakukan oleh Privy kepada para pihak yang terkait. Pengumuman tersebut dapat dilakukan melalui informasi elektronik yang dikirim melalui surat elektronik atau pesan singkat melalui telepon genggam, dan juga dicantumkan dalam Situs yang akan menampilkan pengumuman tersebut selama 7x24 jam setelah pengumuman tersebut disampaikan.

9.12.3. Keadaan Dimana OID Harus Diubah

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

9.13. Prosedur Penyelesaian Sengketa

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara Privy dengan Pemegang Sertifikat atau dengan Pengandal.

9.14. Hukum Yang Berlaku

CPS ini diatur, ditafsirkan, dan dipahami sesuai dengan aturan hukum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat Privy ataupun produk/ layanan lainnya. Termasuk apabila Sertifikat yang diterbitkan oleh Privy dipakai untuk kebutuhan komersil atau kontrak di

negara lain, baik secara tersirat maupun tersurat menggunakan layanan Privy, tetap menerapkan aturan hukum di Indonesia.

Para pihak, termasuk *partners* CA, Pemegang Sertifikat, Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

9.15. Kepatuhan Terhadap Hukum yang Berlaku

Privy mematuhi semua persyaratan, hukum, dan ketentuan peraturan perundang-undangan Indonesia untuk penyediaan produk dan layanan yang dijelaskan dalam CPS ini. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.

9.16. Ketentuan yang Belum Diatur

9.16.1. Perjanjian Secara Keseluruhan

Privy secara kontraktual mewajibkan RA untuk mematuhi CPS ini dan semua panduan terkait termasuk namun tidak terbatas pada ketentuan yang terdapat di Repositori.

9.16.2. Pengalihan Hak atau Kewajiban

Ketentuan pengalihan hak dilakukan sesuai dengan ketentuan peraturan perundang-undangan yang berlaku atau pengumuman yang berkaitan dengan PSrE.

9.16.3. Keterpisahan

Jika terdapat ketentuan 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. Proses pembaruan CPS dijelaskan pada bagian 9.12.

9.16.4. Penegakan Hukum (Biaya Pengacara dan Pelepasan Hak)

Privy dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan Privy dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak Privy 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 Privy.

9.16.5. Keadaan Kahar

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

Privy menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Privy.

Sepanjang diperbolehkan oleh peraturan perundang-undangan, ketentuan mengenai keadaan kahar akan diatur secara lebih spesifik melalui Perjanjian Pemegang Sertifikat dan Perjanjian Pihak Pengandal.

9.17. Ketentuan Lain

9.17.1. Bahasa

Dalam hal CPS ini ditampilkan dalam beragam pilihan bahasa dan terdapat ketidaksesuaian antara satu bahasa dengan

bahasa yang lain, maka teks Bahasa Indonesia yang akan berlaku.

10. LAMPIRAN 1 – Profil Sertifikat

10.1. Sertifikat Privy CA Class 3

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	PrivyCA Class 3 – G2
Subject: OrganizationName	PT Privy Identitas Digital
Subject: CountryName	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=Certificate Authority, Path Length Constraint=None
Public Key	RSA 4096 bits

10.2. Sertifikat Privy CA Class 4

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	PrivyCA Class 4 – G2
Subject: OrganizationName	PT Privy Identitas Digital
Subject: CountryName	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=Certificate Authority, Path Length Constraint=None
Public Key	RSA 4096 bits

10.3. Sertifikat Kelas 3 (Subscriber Certificate)

10.3.1. Sertifikat Individu Non-Instansi Verifikasi Level 2 (Online)

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256dengan RSA Encryption
Issuer: CN	PrivyCA Class 3 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Opsional (Perorangan apabila diajukan perorangan)
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS3G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.3.12 Notice=”Sertifikat non-Instansi” OID : 2.16.360.1.1.1.5.1 Notice=”Individu Non-Instatansi Online Level 2” OID : 2.16.360.1.1.1.3.12.1 Notice=“Privy Identitas Digital”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.3.2. Sertifikat Individu Warga Negara Asing Verifikasi Level 2 (Online)

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256dengan RSA Encryption
Issuer: CN	PrivyCA Class 3 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Opsional (Perorangan apabila diajukan perorangan)
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS3G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.3.12 Notice=”Sertifikat non-Instansi” OID : 2.16.360.1.1.1.5.2.2.2 Notice=”Individu WNA Online level 2” OID : 2.16.360.1.1.1.3.12.1 Notice=“Privy Identitas Digital”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.4. Sertifikat Kelas 4 (Subscriber Certificate)

10.4.1. Sertifikat Individu Non-Instansi Verifikasi Level 3 (Offline)

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256dengan RSA Encryption
Issuer: CN	PrivyCA Class 4 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Opsional (Perorangan apabila diajukan perorangan)
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.3.12 Notice=”Sertifikat non-Instansi” OID : 2.16.360.1.1.1.5.1 Notice=”Individu non-Instansi Offline Level 3” OID : 2.16.360.1.1.1.3.12.1 Notice=“Privy Identitas Digital”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.4.2. Sertifikat Badan Usaha

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256dengan RSA Encryption
Issuer: CN	PrivyCA Class 4 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Badan Usaha/Badan Hukum (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Badan Usaha
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.3.12 Notice=”Sertifikat non-Instansi” OID : 2.16.360.1.1.1.8.1 Notice=”Badan Usaha” OID : 2.16.360.1.1.1.3.12.1 Notice=“Privy Identitas Digital”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.4.3. Sertifikat Individu Warga Negara Asing Verifikasi Level 3 (online)

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256dengan RSA Encryption
Issuer: CN	PrivyCA Class 4 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Opsional (Perorangan apabila diajukan perorangan)
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.3.12 Notice=”Sertifikat non-Instansi” OID : 2.16.360.1.1.1.5.2.2.3 Notice=”Individu WNA Online level 3” OID : 2.16.360.1.1.1.3.12.1 Notice=“Privy Identitas Digital”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

11. Lampiran 2 – Definisi dan Singkatan/Akronim

11.1. Definisi

Istilah	Definisi
Penilai Terkualifikasi	Orang atau Badan Hukum yang memenuhi persyaratan dalam CPS ini.
Badan Usaha/Badan Hukum	Perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
Data Elektronik	Data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi.
Informasi Elektronik	Satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
Dokumen Elektronik	Setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
Infrastruktur Kunci Publik/*Public Key Infrastructure* (“PKI”)	Serangkaian perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan

	Sertifikat dan kunci yang dapat dipercaya berdasarkan kriptografi Kunci Publik.
Kebijakan Privasi	Ketentuan mengenai cara PSrE Privy mengumpulkan, menggunakan, membagikan, memproses, dan mengamankan data pribadi pengguna layanan Privy, termasuk Pemegang Sertifikat. Kebijakan Privasi Privy tersedia di https://privy.id/id/kebijakan-privasi dan/atau pada Repositori.
Kebijakan Sertifikat/*Certificate Policy* ("CP")	Seperangkat aturan yang menunjukkan penerapan dari Sertifikat yang dinamai untuk komunitas tertentu dan/atau implementasi PKI dengan persyaratan keamanan umum. Kebijakan Sertifikat tersedia pada Repositori dan repositori yang dikelola oleh PSrE Induk yang saat ini tersedia pada https://www.rootca.id/.
Ketentuan Penggunaan Layanan	Ketentuan mengenai pengamanan dan penggunaan yang sesuai dari Sertifikat yang diterbitkan sesuai dengan dokumen ini (CPS) ini ketika Pemohon/Pemegang Sertifikat adalah PSrE atau afiliasi dari PSrE Privy. Ketentuan Penggunaan Layanan Privy tersedia di https://privy.id/id/ketentuan-penggunaan.
Kunci Privat	Kunci yang dirahasiakan oleh pemegang Pasangan Kunci yang digunakan untuk membuat Tanda Tangan Elektronik dan/atau mendekripsi catatan atau file elektronik yang dienkripsi dengan Kunci Publik yang sesuai.
Kunci Publik	Kunci yang dapat diungkapkan secara publik yang termuat dalam Sertifikat dan bersesuaian dengan Kunci Privat rahasia yang digunakan. Kunci Publik digunakan oleh Pengandal untuk memverifikasi Tanda Tangan Elektonik yang dibuat oleh Kunci Privat dan/atau untuk mengenkripsi pesan sehingga Kunci Publik hanya dapat didekripsi dengan menggunakan Kunci Privat yang sesuai.
Laporan Audit	Laporan dari Penilai Terkualifikasi yang menyatakan pendapat Penilai Terkualifikasi tentang apakah proses dan kontrol entitas

	memenuhi ketentuan wajib yang diatur pada dokumen ini (CPS).
Online Certificate Status Profile (“OCSP”)	Protocol pengecekan Sertifikat daring yang memungkinkan aplikasi perangkat lunak Pengandal untuk menentukan status Sertifikat yang diidentifikasi.
Otoritas Pendaftaran/*Registration Authority* (“RA”)	Pihak yang atas nama CA menjalankan fungsi identifikasi dan autentikasi terhadap permohonan Sertifikat, baik memulai dan meneruskan permohonan untuk pencabutan Sertifikat kepada CA, dan meminta untuk dilakukan penerbitan ulang atau perpanjangan Sertifikat.
Pasangan Kunci	Kunci Privat dan Kunci Publik terkait.
Pemegang Sertifikat/*Subscriber*	Orang atau Badan Hukum yang telah berhasil memperoleh Sertifikat baik melalui RA ataupun Privy.
Pemohon/A*pplicant*	Orang atau Badan Hukum yang telah mengajukan permohonan, namun belum mendapatkan Sertifikat.
Penyelenggara Sertifikasi Elektronik (“PSrE”)/*Certification Authority* (“CA”)	Badan Hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat.
Penyelenggara Sertifikasi Elektronik Induk (“PSrE Induk”)/*Root CA*	Penyelenggara Sertifikasi Elektronik tingkat atas yang Sertifikat Induk-nya didistribusikan oleh Aplikasi Perangkat Lunak dan menandatangani Sertifikat CA dibawahnya.
Pengidentifikasian Objek Kebijakan/*Object Identifier* (“OID”)	Merupakan set nomor yang secara unik menunjuk kepada sebuah objek atau kebijakan yang diatur dalam CPS.
Perjanjian Pemegang Sertifikat	Perjanjian antara CA dan Pemohon/Pemegang Sertifikat yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pemegang Sertifikat Privy tersedia di Repositori.
Perjanjian Pengandal	Pejanjian antara CA dan Pengandal yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pengandal Privy tersedia di Repositori.
Pengandal	Orang atau Badan Hukum yang mempercayai Sertifikat dan/atau Tanda Tangan Digital yang diterbitkan oleh CA.

Repositori	Database online yang berisi dokumen tata kelola PKI yang diungkapkan secara publik (seperti CP/CPS) dan informasi status Sertifikat, baik dalam bentuk respon CRL atau OCSP. Repositori Privy pada tautan https://repository.privyca.id/.
Sertifikat Elektronik ("Sertifikat")	Sertifikat yang bersifat elektronik dan memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
Sertifikat Induk/*Root Certificate*	Sertifikat yang diterbitkan dan ditandatangani sendiri oleh Root CA untuk mengidentifikasi dirinya dan untuk memfasilitasi sertifikasi Sertifikat yang dikeluarkan oleh *Subordinate CA*.
Situs	berarti segala URL yang menggunakan domain dengan alamat www.privy.id dan/atau www.privyca.id atau situs lain yang dinyatakan oleh Privy dari waktu ke waktu.
Status Keaktifan Sertifikat / *Certificate Revocation List* ("CRL")	Berisi daftar dengan penanda waktu dari Sertifikat yang dicabut yang di perbaharui secara berkala yang dibuat dan ditandatangani secara elektronik oleh CA/PSrE yang menerbitkan Sertifikat.
Subjek	Berarti perseorangan, Badan Hukum/Badan Usaha yang diidentifikasi dalam Sertifikat sebagai Subjek.
Penyelenggara Sertifikasi Elektronik Berinduk ("PSrE Indonesia") / *Subordinate CA* ("Sub-CA")	CA yang Sertifikatnya ditandatangani oleh *Root CA*, atau *Subordinate CA* lainnya.
Tanda Tangan Elektronik	Tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
Tata Cara Pelaksanaan Sertifikat PSrE/*Certificate Practice Statement* ("CPS")	Satu dari beberapa dokumen yang membentuk kerangka kerja tata kelola di mana Sertifikat dibuat, diterbitkan, dikelola dan digunakan.

Warm Backup	Metode pencadangan data yang dilakukan dengan menyalin data pada Pusat data ke lokasi cadangan *off-site* secara *real time*.

11.2. Singkatan/Akronim

Akronim	Arti
AICPA	American Institute of Certified Public Accountants
C	Country
CA	Certification Authority/Penyelenggara Sertifikasi Elektronik
CICA	Canadian Institute of Chartered Accountants
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certification Revocation List
DN	Distinguished Name
DoS	Denial of Services
EDI	Electronic Data Interchange
FIPS	Federal Information Protection Standards
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
KTP	Kartu Tanda Penduduk
NIB	Nomor Induk Berusaha
NIK	Nomor Induk Kependudukan
NPWP	Nomor Pokok Wajib Pajak
O	Organization Name
OU	Organization Unit
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PKI	Public Key Infrastructure
PSrE	Penyelenggara Sertifikasi Elektronik
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SIUP	Surat Izin Usaha Perdagangan
SIM	Surat Izin Mengemudi
SK	Surat Keputusan
SOP	Strandard Operational Procedure
Sub-CA	Subordinate Certification Authority

RA	Registration Authority / Otoritas Pendaftaran
UPS	Uninterrupted Power Supply (UPS)
URL	Uniform Resource Locator