Kebijakan Sertifikat (*Certificate Policy*) /
Tata Cara Pengelolaan Sertifikat
(*Certificate Practice Statement*)

PrivyID

Versi 1.2

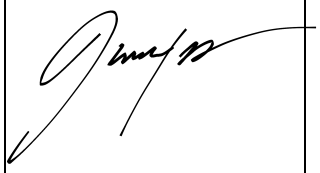
12 Januari 2021

Jl. Kemang Raya No 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	Chief Technology Officer	Chief Information Security and Compliance
		
Marshall Pribadi	Guritno Adi Saputra	Krishna Chandra

VP Legal and Compliance
Digitally signed by: HARZY RANDHANI I. (. Signed By: 
Harzy Randhani Irdham

Riwayat Perubahan

Issue	Date	Changes to this Revision
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 PrivyID dan penyesuaian lainnya.

Daftar Isi

1. Pengantar

1.1. Ringkasan

PrivyID atau PT Privy Identitas Digital merupakan badan hukum yang menjalankan usaha sebagai Penyelenggaraan Sertifikasi Elektronik (PSrE) atau disebut juga dengan *Certificate Authority* (CA).

Kebijakan Sertifikat/*Certificate Policy* ("CP") dan Tata Cara Pelaksanaan Sertifikat PSrE/*Certificate Practice Statement* ("CPS"), yang selanjutnya disingkat menjadi CP/CPS, menguraikan persyaratan usaha, hukum, dan teknis yang mengatur mengenai Penyelenggara Sertifikasi Elektronik PrivyID oleh peserta dalam Infrastruktur Kunci Publik/*Publik Key Infrastructure* ("PKI") PrivyID. CP/CPS ini memenuhi persyaratan formal yaitu konten, tata letak dan format dari Internet Engineering Task Force (IETF) RFC 3647 yang dikeluarkan pada bulan November 2003.

Dokumen ini dibuat dengan asumsi bahwa pembaca telah mengenal konsep tanda tangan elektronik, sertifikat elektronik ("Sertifikat"), dan PKI secara umum. Apabila pembaca tidak mengenal konsep PKI, pembaca dapat menghubungi Kementerian Komunikasi dan Informatika Republik Indonesia untuk memperoleh gambaran mengenai PKI, termasuk orientasi mengenai konsep kunci seperti tanda tangan elektronik, pasangan kunci asimetris, penyelenggara sertifikasi, penyelenggara pendaftaran, pernyataan kebijakan dan praktik, serta aspek dan pertimbangan usaha terkait PKI.

1.2. Nama Dokumen dan Identifikasi

Dokumen ini merupakan CP/CPS dari PrivyID. *Object Identifier* (OID) untuk PrivyID adalah iso(1) identified-organization(3) dod(6) internet(1) privat(4) enterprise(1) PT PrivyID Identitas Digital (52554).

1.3. Partisipan PKI

1.3.1. Penyelenggara Sertifikasi Elektronik

Penyelenggara Sertifikasi Elektronik/*Certificate Authority* (CA) adalah pihak ketiga terpercaya berbentuk badan hukum, yang berfungsi sebagai pihak yang menerbitkan dan mengaudit Sertifikat Elektronik (Sertifikat), sesuai dengan apa yang diatur didalam CP/CPS ini. PrivyID dalam hal ini menjalankan fungsi yang berhubungan dengan fungsi *Publik Key Infrastructure* (PKI) seperti:

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

1.3.2. Otoritas Pendaftaran

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

a. Tunduk terhadap prosedur pendaftaran pemohon Sertifikat;
b. identifikasi dan autentikasi Pemohon Sertifikat berdasarkan prosedur pendaftaran yang ditetapkan oleh PrivyID;
c. memulai atau meneruskan permohonan untuk pencabutan Sertifikat kepada PrivyID; dan
d. menyetujui permohonan penerbitan ulang atau perpanjangan Pemegang Sertifikat.

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

Kecuali disebutkan lain, RA yang tercantum dalam ketentuan ini adalah RA yang terikat dengan hubungan kontraktual dengan

PrivyID. Oleh karena itu, seluruh ketentuan yang secara tegas menjelaskan mengenai peran RA di dalam CP/CPS ini berlaku terhadap seluruh RA. Privy memiliki hak untuk melakukan audit atau pemeriksaan terhadap kesesuaian fungsi yang dijalankan oleh RA dengan CP/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 Elektronik.
b. Pemegang Sertifikat/*Subscriber* – Orang atau Badan Hukum yang telah berhasil memperoleh Sertifikat Elektronik baik melalui RA ataupun PrivyID.

1.3.4. Pihak Pengandal

Pihak Pengandal/*Relying Parties* adalah Orang atau Badan Hukum yang mempercayai Sertifikat dan/atau tanda tangan digital yang diterbitkan oleh CA. Pihak Pengandal harus terlebih dahulu memeriksa respon dari CRL atau OCSP yang sesuai sebelum memanfaatkan informasi yang ada dalam sertifikat.

Pihak Pengandal mengandalkan keabsahan hubungan antara identitas dari Pemegang Sertifikat dengan kunci public yang tercantum dalam Sertifikat tersebut. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat. Pihak Pengandal dapat menggunakan informasi dalam sertifikat untuk menentukan kecocokan penggunaan sertifikat.

Pihak Pengandal menggunakan informasi dalam sertifikat untuk, antara lain:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi Tanda Tangan Digital;

c. Melakukan pemeriksaan (apakah sertifikat ada pada daftar) pencabutan;
d. Penyetujuan atas batas tanggung jawab dan jaminan;

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

1.3.5. Partisipan Lain

Tidak ada ketentuan.

1.4. Penggunaan Sertifikat

Sertifikat Elektronik memuat Tanda Tangan Elektronik dan identitas yang menunjukan status subjek hukum para pihak dalam Transaksi Elektronik.

1.4.1. Penggunaan Sertifikat yang Dibolehkan

PrivyID menetapkan bahwa Sertifikat yang diterbitkan adalah hanya untuk melakukan **Tanda Tangan Digital**.

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

Sertifikat yang diterbitkan oleh PrivyID untuk Pemegang Sertifikat digunakan untuk transaksi dengan menggunakan Tanda Tangan Elektronik sehingga menjadi Tanda Tangan Digital, yang membutuhkan 3 faktor berikut yang menjamin:
a. *Non-Repudiation*:

Penandatangan tidak dapat menampik tanda tangan yang telah dibubuhkannya.

b. *Authentication*:
Kepastian untuk suatu entitas bahwa entitas lain adalah siapa dirinya mengaku.

c. *Integrity*:
Kepastian bahwa suatu informasi atau dokumen elektronik tidak mengalami perubahan.

Untuk mengakomodir ketiga faktor yang disampaikan diatas dengan menggunakan Tanda Tangan Digital, maka PrivyID menetapkan bahwa seluruh Sertifikat yang diterbitkan untuk Pemegang Sertifikat memiliki klasifikasi Sertifikat *Class 1*.

1.4.2. Penggunaan Sertifikat yang Dilarang

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

1.5. Kebijakan Administrasi

1.5.1. Organisasi Pengelola Dokumen

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

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

PA PrivyID dapat dihubungi melalui:
Policy Authority PrivyID
Jl. Kemang Raya No 34L

Telp: 021-22715509
Email: Policy@privy.id
Website: www.privyca.id

1.5.2. Narahubung

Narahubung dapat menggunakan informasi yang tertera diatas.

1.5.3. Pihak yang Menentukan Kesesuaian CP/CPS dengan Kebijakan

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

1.5.4. Prosedur Persetujuan CP/CPS

Setiap perubahan terhadap CP/CPS harus melalui persetujuan dari PA PrivyID.

1.6. Definisi dan Akronim

Tidak ada ketentuan.

2. Tanggung Jawab Publikasi dan Repositori

2.1. Repositori

PrivyID menyediakan dan menjaga repositori yang berisi dokumen yang menunjang penyelenggaraan layanan PKI, antara lain:

a. *Publik Key Certificate*
b. *CRL* dan/atau Status Keaktifan Sertifikat Elektronik
c. CP/CPS
d. Perjanjian Pemegang Sertifikat
e. Perjanjian Pihak Pengandal

PrivyID memiliki hak untuk tidak menerbitkan dokumen sifatnya rahasia, seperti namun tidak terbatas pada prosedur operasi standar, kontrol keamanan, kontrol operasional, dan prosedur keamanan internal.

2.2. Publikasi Informasi Sertifikat

Dokumen yang berlaku dan diakui oleh PrivyID adalah dokumen yang bertandatangan elektronik, tercantum, dan dapat diakses melalui repositori.

Dalam pelaksanaanya, PrivyID dapat menampilkan dokumen yang tercantum dalam repositori tersebut dalam beberapa pilihan Bahasa. Dalam hal dokumen legal, maka jika terdapat ketidaksesuaian antara satu bahasa dengan bahasa yang lain, maka dokumen Berbahasa Indonesia yang akan berlaku.

2.3. Waktu atau Frekuensi Publikasi

Berikut merupakan waktu atau frekuensi publikasi untuk dokumen-dokumen yang tertera didalam repository:

a. *Publik Key Certificate/* Sertifikat Kunci Publik
   Sesegera mungkin setelah pasangan kunci dibangkitkan.
b. *CRL* dan/atau Status Keaktifan Sertifikat Elektronik
   Sesegera mungkin setelah CRL diterbitkan.
c. CP/CPS

Dalam kurun waktu 7 hari setelah mendapat persetujuan dari PA. CP/CPS akan ditinjau ulang setidaknya sekali dalam waktu satu tahun kalender. Jika tidak ada perubahan terhadap konten dari CP/CPS tersebut, setidaknya akan dilakukan perubahan terhadap versi dan tanggal penerbitan dari CP/CPS yang baru.

d. Perjanjian Pemegang Sertifikat
   Dalam kurun waktu 7 hari setelah mendapat persetujuan PA
e. Perjanjian Pihak Pengandal
   Dalam kurun waktu 7 hari setelah mendapat persetujuan PA.

2.4. Kendali Akses pada Repositori

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

3. Identifikasi dan Autentikasi

PrivyID sebagai CA dan/atau RA melakukan verifikasi dan otentikasi identitas dan/atau atribut lainnya dari Pemohon sertifikat untuk menerbitkan Sertifikat Elektronik.

3.1. Penamaan

3.1.1. Tipe Nama

Sertifikat Elektronik yang diterbitkan oleh PrivyID sesuai dengan standar ITU X500 *Distinguished Names*. Seluruh Sertifikat Elektronik harus mengandung X.501 *distinguished name* dalam kolom *Subject Name*. Sertifikat Elektronik yang diterbitkan oleh PrivyID harus menggunakan *Distinguished Name* (DN) untuk mendukung identifikasi dari Pemegang Sertifikat.

3.1.2. Kebutuhan Nama yang Bermakna

PrivyID menggunakan DN untuk mengidentifikasi suatu individu dan/atau badan hukum/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 adalah nama lengkap Pemegang Sertifikat ditambah dengan *Username* PrivyID, atau entitas yang mewakili Pemegang Sertifikat beserta *Username* PrivyID.

Atribut *Organization name* (O) merupakan nama badan hukum/usaha dimana Pemegang Sertifikat diidentifikasi sebagai bagian darinya.

Atribut *Organization unit* (OU) merupakan nama divisi/departemen/unit dari badan hukum/usaha dimana Pemegang Sertifikat diidentifikasi sebagai bagian darinya.

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/usaha tersebut.

Khusus Sertifikat yang diterbitkan kepada Pemegang Sertifikat individu/perseorangan tanpa informasi yang merepresentasikan badan hukum/badan usaha apapun, maka Atribut Organization name dan Organization unit akan diisi sebagai “PrivyID RA” dan “Perorangan”.

3.1.3. Anonimitas atau Pseudonimitas Pemilik

Tidak diatur

3.1.4. Aturan untuk Menginterpretasi Bentuk Nama

Tidak diatur

3.1.5. Keunikan Nama

DN dari setiap Sertifikat Elektronik yang diterbitkan akan menjadi unik, karena CN dari kolom *Subject Name* akan berisi nama lengkap Pemegang Sertifikat dan *username* PrivyID yang hanya akan diterbitkan untuk satu individu berdasarkan Nomor Induk Kependudukan.

3.1.6. Pengakuan, Otentikasi, dan Peran Merk Dagang

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

3.2. Validasi Awal Identitas

PrivyID akan melakukan identifikasi terhadap setiap permohonan penerbitan Sertifikat.

3.2.1. Metode Pembuktian Kepemilikan Kunci Privat

Metode yang digunakan untuk membuktikan kepemilikan Kunci Privat Pemegang Sertifikat adalah melalui Akun PrivyID.

3.2.2. Otentikasi Identitas Organisasi

Jika suatu Sertifikat digunakan untuk mengidentifikasi suatu badan hukum/badan usaha maka pengajuan untuk mendapatkan Sertifikat tersebut hanya dapat dilakukan oleh pihak yang berwenang untuk mewakili badan hukum/badan usaha tersebut.

PrivyID akan memeriksa identitas (KTP) dan jabatan/wewenang dari Pemohon, surat kuasa (jika ada), dokumen pendukung pengesahan Badan Hukum/Badan Usaha (termasuk namun tidak terbatas kepada SIUP, SK Kementerian, NPWP, dan perubahan anggaran dasar terakhir).

PrivyID menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi bagi organisasi.

3.2.3. Otentikasi Identitas Individu/Perorangan

PrivyID dan/atau RA akan mengidentifikasi dan mengautentikasi permohonan Sertifikat yang diajukan oleh individu/perorangan berdasarkan kelas Sertifikat. Saat ini PrivyID hanya menerbitkan Sertifikat untuk Pemohon Sertifikat dengan klasifikasi Sertifikat Kelas 1.

Berdasarkan ketentuan yang diatur oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik, untuk mendapatkan Sertifikat, Pemohon diwajibkan untuk menunjukan, membuktikan, dan memberikan hal-hal berikut:

1. salinan dokumen berupa Kartu Tanda Penduduk (KTP) yang dikeluarkan oleh Pemerintah Indonesia. SIM dan Paspor dapat digunakan sebagai dokumen pengganti atau pendukung jika diminta oleh PrivyID dan/atau RA;
2. Alamat surat elektronik;
3. Nomor telepon (termasuk ponsel); dan
4. Data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection* atau mekanisme lain yang setara.

PrivyID 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.

PrivyID 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.

PrivyID menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi individu/perorangan.

3.2.4. Informasi Pemegang Sertifikat yang Tidak Terverifikasi

PrivyID tidak menerbitkan Sertifikat untuk Pemohon Sertifikat yang tidak dapat diverifikasi.

3.2.5. Validasi Otoritas

PrivyID dan/atau RA akan menggunakan upaya yang wajar dan andal untuk memeriksa keotentikan informasi Pemohon

terhadap permohonan yang diajukan untuk Sertifikat yang dibuat dengan atas nama badan hukum.

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

PrivyID tidak melakukan proses *Re-key*.

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

Tidak ada ketentuan.

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

Tidak ada ketentuan.

3.4. Identifikasi dan Otentikasi untuk Permohonan Pencabutan

Permohonan untuk mencabut Sertifikat dapat diajukan oleh Pemegang Sertifikat dengan menghubungi PrivyID dan membuktikan penguasaan terhadap informasi data Pemilik yang disimpan oleh PrivyID, seperti alamat email dan nomor ponsel.

4. Persyaratan Operasional Siklus Sertifikat

4.1. Permohonan Sertifikat

Untuk memperoleh Sertifikat, Pemohon harus melakukan hal sebagai berikut:

a. Pendaftaran permohonan dapat dilakukan dengan mengisi formulir pendaftaran pada platform PrivyID dan/atau RA.
b. Pemohon memberikan data dan informasi yang dibutuhkan oleh PrivyID dan/atau RA untuk keperluan validasi. Pemohon berkewajiban untuk memberikan data dan informasi yang tepat, benar, dan jelas.
c. Pemohon memberikan persetujuan terhadap Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, dan Kebijakan Privasi PrivyID.

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

PrivyID dan/atau RA akan melakukan upaya yang wajar untuk memastikan bahwa Pemohon Sertifikat memberikan data dan informasi yang benar. Pemohon Sertifikat harus melalui proses registrasi sebagaimana yang dicantumkan didalam CP/CPS ini sebelum permohonan penerbitan Sertifikat Elektroniknya diterima. PrivyID dan/atau RA memiliki wewenang untuk menolak permohonan penerbitan Sertifikat Elektronik jika ada data dan informasi yang kurang dan/atau tidak benar.

4.1.1. Pihak yang dapat Mengajukan Permohonan Sertifikat

Pihak yang dapat mengajukan Permohonan penerbitan Sertifikat adalah Orang dan Badan Hukum atau Badan Usaha.

Orang yang dapat mengajukan permohonan penerbitan Sertifikat adalah Orang yang telah memiliki KTP, sedangkan untuk Badan Hukum atau Badan Usaha harus terdaftar sebagai Badan Hukum atau Badan Usaha yang sah di Indonesia.

4.1.2. Proses Pendaftaran dan Tanggungjawabnya

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 Pasal 3.2. kepada PrivyID dan/atau RA;
b. Setuju terhadap Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, serta Kebijakan Privasi PrivyID yang berlaku;
c. Membayar biaya Sertifikat dan biaya penggunaannya (apabila berlaku);
d. Menunggu validasi serta verifikasi identitas dari PrivyID dan/atau RA; dan
e. Jika validasi dan verifikasi gagal dilakukan, PrivyID 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 PrivyID 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 PrivyID yaitu berupa salinan KTP, alamat surat elektronik, nomor telepon, dan swafoto untuk kebutuhan pemenuhan terhadap peraturan perundang-undangan.

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

4.2. Pemrosesan Permohonan Sertifikat

4.2.1. Melaksanakan fungsi Identifikasi dan Otentikasi

PrivyID dan/atau RA dapat menggunakan data dan informasi yang diajukan oleh Pemohon untuk memvalidasi Identitas pemohon sebagaimana diatur dalam Pasal 3.2. dari CP/CPS ini.

4.2.2. Persetujuan atau Penolakan Permohonan Sertifikat

PrivyID dan/atau RA hanya kan memberikan persetujuan terhadap Permohonan penerbitan Sertifikat apabila telah memenuhi kriteria yang disebutkan di pasal 4.1.

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

d. menolak Permohonan penerbitan Sertifikat tersebut;
e. meminta informasi tambahan kepada Pemohon agar dapat memenuhi kriteria yang dibutuhkan.

4.2.3. Waktu untuk Memproses Permohonan Sertifikat

PrivyID memastikan bahwa proses Permohonan penerbitan Sertifikat dilakukan dalam jangka waktu yang wajar.

4.3. Penerbitan Sertifikat

4.3.1. Tindakan RA selama Penerbitan Sertifikat

Setelah melakukan verifikasi dan validasi, RA kemudian meneruskan permohonan penerbitan Sertifikat kepada PrivyID.

4.3.2. Tindakan CA selama Penerbitan Sertifikat

Setelah menerima permohonan penerbitan Sertifikat yang telah diverifikasi dan divalidasi, baik secara langsung melalui Pemohon maupun melalui RA, maka PrivyID secara segera membangkitkan pasangan kunci yang terasosiasi kepada Pemohon dan menerbitkan Sertifikat melalui sistem PKI. Seluruh proses Penerbitan Kunci, Manajemen Kunci, Permohonan Sertifikat, dan Penerbitan Sertifikat harus dilakukan melalui sistem PKI.

Dalam hal Permohonan diteruskan oleh RA maka apabila menurut PrivyID diperlukan, maka PrivyID dapat melakukan verifikasi dan validasi ulang terhadap informasi yang telah diteruskan tersebut sebelum membangkitkan pasangan kunci.

Setelah Penerbitan Sertifikat, Sertifikat milik Pemohon akan tersimpan bersama dengan dokumen ditandatangani secara elektronik oleh Pemegang Sertifikat.

4.3.3. Pemberitahuan ke Pemegang Sertifikat oleh PrivyID tentang Penerbitan Sertifikat

Setelah Sertifikat Elektronik di terbitkan, maka PrivyID akan memberitahu Pemohon Sertifikat bahwa Permohonan Sertifikat disetujui melalui email dan/atau nomor ponsel Pemohon yang terdaftar.

4.4. Penerimaan Sertifikat

4.4.1. Sikap yang Dianggap sebagai Penerimaan Sertifikat

Pemohon dianggap telah menerima Sertifikat Elektronik setelah pemberitahuan kepada pemohon sesuai pasal 4.3.3.

4.4.2. Publikasi Sertifikat oleh PrivyID

PrivyID mempublikasikan Sertifikat PrivyID dalam repositori yang dapat diakses melalui situs PrivyID. PrivyID mempublikasikan Sertifikat Pengguna Akhir dengan mengirimkannya kepada Pemegang Sertifikat.

4.4.3. Pemberitahuan Sertifikat oleh PrivyID kepada Pihak Lain

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

4.5. Pasangan Kunci dan Penggunaan Sertifikat

4.5.1. Kunci Privat Pemegang Sertifikat dan Penggunaan Sertifikat

PrivyID akan mengamankan Kunci Privat Pemegang Sertifikat sesuai dengan persetujuan berdasarkan Perjanjian Pemegang Sertifikat dengan PrivyID.

PrivyID 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.

4.5.2. Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

Tidak ada ketentuan.

4.6. Pembaruan Sertifikat

PrivyID akan melakukan Pembaruan Sertifikat secara otomatis.

4.6.1. Keadaan yang Menyebabkan Pembaruan Sertifikat

Pembaruan Sertifikat akan terjadi secara otomatis ketika masa validitas dari Sertifikat telah berakhir.

4.6.2. Pihak yang Dapat Mengajukan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.3. Pemrosesan Permohonan Pembaruan Sertifikat

Pembaruan Sertifikat akan terjadi secara otomatis ketika Pemegang Sertifikat melakukan autentikasi melalui PrivyID setelah masa validitas Sertifikat berakhir.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

PrivyID akan melakukan pemberitahuan penerbitan Sertifikat baru kepada Pemegang Sertifikat melalui e-mail dan/atau nomor ponsel Pemegang Sertifikat yang terdaftar.

4.6.5. Sikap yang Dianggap sebagai Penerimaan Pembaruan Sertifikat

Tidak ada ketentuan.

4.6.6. Publikasi Pembaruan Sertifikat oleh PrivyID

Tidak ada ketentuan.

4.6.7. Pemberitahuan Pembaruan Sertifikat oleh PrivyID kepada Pihak Lain

Tidak ada ketentuan.

4.7. Sertifikat *Re-key*

PrivyID tidak melakukan Sertifikat *Re-key.*

4.7.1. Keadaan yang Menyebabkan Sertifikat *Re-key*

Tidak ada ketentuan.

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

Tidak ada ketentuan.

4.7.3. Pemrosesan Permohonan Sertifikat *Re-key*

Tidak ada ketentuan.

4.7.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemegang Sertifikat

Tidak ada ketentuan.

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

Tidak ada ketentuan.

4.7.6. Publikasi Sertifikasi *Re-key* oleh PrivyID

Tidak ada ketentuan.

4.7.7. Pemberitahuan Sertifikat *Re-key* oleh PrivyID

Tidak ada ketentuan.

4.8. Modifikasi Sertifikat

Tidak ada ketentuan.

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 PrivyID

Tidak ada ketentuan.

4.8.7. Pemberitahuan Penerbitan Sertifikat oleh PrivyID ke Pihak Lain

Tidak ada ketentuan.

4.9. Pencabutan Sertifikat dan Penangguhan

4.9.1. Keadaan yang Menyebabkan Pencabutan Sertifikat

PrivyID melakukan pencabutan Sertifikat untuk hal-hal berikut ini:

f. Ketika Pemegang Sertifikat mengajukan permohonan pencabutan Sertifikat;
g. Ketika kunci privat terkompromi, hilang, dan/atau rusak;
h. Ketika informasi yang tertera didalam Sertifikat tidak akurat atau menyesatkan;
i. Ketika permohonan penerbitan Sertifikat dilakukan secara secara tidak sah;
j. Ketika penerbitan Sertifikat dilakukan secara tidak sesuai dengan ketentuan yang tercantum didalam CP/CPS;
k. Ketika Pemegang Sertifikat melanggar ketentuan yang tercantum didalam CP/CPS atau Perjanjian Pemegang Sertifikat;
l. Ketika Sertifikat PrivyID mengalami kebocoran;
m. Ketika PrivyID berhenti beroperasi;
n. Dan alasan lainnya yang menurut PrivyID dibenarkan untuk melakukan pencabutan Sertifikat.

4.9.2. Pihak yang dapat Mengajukan Pencabutan Sertifikat

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

Dalam hal ketentuan yang tercantum pada pasal 4.1. terpenuhi, maka PrivyID juga dapat melakukan Pencabutan Sertifikat tanpa permintaan Pemegang Sertifikat.

4.9.3. Prosedur Pengajuan Pencabutan Sertifikat

PrivyID akan memverifikasi identitas sebelum dilakukan pencabutan Sertifikat. Sertifikat yang telah dicabut akan masuk kedalam daftar CRL dan OCSP. Setelah dilakukan pencabutan, Pemegang Sertifikat dapat mengajukan penerbitan Sertifikat Baru. Proses Penerbitan Sertifikat Baru akan mengikuti ketentuan pada pasal 4.2. hingga 4.4.

4.9.4. Tenggang Waktu Permohonan Pencabutan

PrivyID akan segera mencabut sertifikat setelah verifikasi identitas terhadap permohonan pencabutan Sertifikat berhasil.

4.9.5. Jangka Waktu PrivyID untuk Memproses Permohonan Pencabutan

Tidak ada ketentuan.

4.9.6. Persyaratan Pemeriksaan untuk Pihak Pengandal

Pihak Pengandal harus memvalidasi setiap Sertifikat terhadap CRL dan/atau OCSP terbaru yang diterbitkan oleh PrivyID.

4.9.7. Frekuensi Penerbitan CRL

CRL akan diperbarui secara berkala setiap hari dan dapat diakses melalui repositori.

4.9.8. Latensi Maksimum untuk CRL

Tidak ada ketentuan.

4.9.9. Ketersediaan Pemeriksaan Pencabutan/Status secara daring

PrivyID menyediakan layanan pengecekan informasi status Sertifikat melalui OCSP yang selalu tersedia, diluar waktu pemeliharaan yang ditentukan oleh PrivyID.

4.9.10. Persyaratan Pemeriksaan Pencabutan Secara Online

Tidak ada ketentuan.

4.9.11. Bentuk lain dari Pengumuman Pencabutan yang Disediakan

Tidak ada ketentuan.

4.9.12. Persyaratan Khusus Kompromisasi *Re-key*

Jika Kunci Privat PrivyID terkompromisasi, maka seluruh Sertifikat yang diterbitkan oleh PrivyID harus dicabut.

Jika Kunci Privat Pemegang Sertifikat terkompromisasi, maka Sertifikat terkait dicabut sesuai dengan prosedur didalam CP/CPS ini.

4.9.13. Keadaan yang Menyebabkan Penangguhan Sertifikat

Tidak ada ketentuan.

4.9.14. Pihak yang dapat Mengajukan Permohonan Penangguhan

Tidak ada ketentuan.

4.9.15. Prosedur Permohonan Penangguhan

Tidak ada ketentuan.

4.9.16. Jangka waktu Masa Penangguhan

Tidak ada ketentuan.

4.10. Layanan Status Sertifikat

4.10.1. Karakteristik Operasional

PrivyID 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 PrivyID.

4.10.3. Fitur Pilihan

Tidak ada ketentuan.

4.11. Akhir Masa Berlangganan

Masa Kepemilikan Sertifikat berakhir ketika Sertifikat Elektronik dicabut atau masa validitasnya berakhir.

4.12. Escrow Kunci dan Pemulihan

4.12.1. Kebijakan dan Praktik Escrow Kunci dan Pemulihan

Tidak ada ketentuan.

4.12.2. Kebijakan dan Praktik Enkapsulasi Kunci dan Pemulihan Kunci

Tidak ada ketentuan.

5. Fasilitas, Manajemen, dan Kontrol Operasi

5.1. Kontrol Fisik

PrivyID melakukan kontrol terhadap keamanan Pusat Data sebagaimana diatur dalam CP/CPS ini. Pusat Data dalam hal ini mengacu kepada server yang ditempatkan melalui media penyimpanan yang menjalankan siklus operasi sertifikat digital dan diletakan secara fisik dalam suatu lemari penyimpanan khusus.

5.1.1. Lokasi dan Konstruksi

Seluruh fasilitas komputasi yang digunakan untuk menjalankan layanan PrivyID ditempatkan dalam Pusat Data didalam 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.

5.1.2. Akses Fisik

Akses untuk masuk ke Pusat Data harus mendaftar terlebih dahulu dan melalui penjagaan yang dijaga 24 (dua puluh empat) jam oleh sekuriti, kamera pengawas, beberapa lapis pintu keamanan, akses masuk 3 faktor otentikasi, dan kunci pengaman pada media penyimpanan. Hanya pihak tertentu yang termasuk pada *Trusted Roles* yang mendapat akses untuk masuk ke pusat data.

5.1.3. Listrik dan Pendingin Ruangan

Pusat Data PrivyID 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.

Pusat Data juga dilengkapi dengan tower pendingin ruangan yang menyesuaikan agar temperatur dan tingkat kelembapan

ruangan terkendali untuk menjaga kinerja mesin dan peralatan PrivyID.

5.1.4. Keterpaparan Air

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

5.1.5. Pencegahan dan Perlindungan Kebakaran

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

5.1.6. Media Penyimpanan

Media penyimpanan disimpan dan dilindungi dari hal-hal yang dapat menyebabkan kerusakan. 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 perangkat keras yang sudah tidak digunakan akan dihancurkan dan dibuang dengan cara yang aman dan wajar agar perangkat tersebut tidak dapat digunakan lagi.

5.1.8. Cadangan *Off-site*

PrivyID menyiapkan sistem pencadangan yang cukup untuk digunakan dalam rangka pemulihan dari kegagalan sistem. Sistem pencadangan tersebut dilakukan secara langsung dan disimpan di lokasi yang aman dan berada di lokasi yang terpisah dengan Pusat Data. Hanya sistem pencadangan yang disimpan terakhir yang akan digunakan untuk pemulihan.

5.2. Kontrol Prosedural

5.2.1. Trusted Roles

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

a. *Network Officer*
b. *Security Officer*
c. *System Auditor*
d. *Registration Officer*

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

5.2.2. Jumlah Orang yang Diperlukan Setiap Tugas

PrivyID mensyaratkan setidaknya terdapat 1 (satu) orang ditambah dengan 2 (dua) orang cadangan yang mengisi posisi *Trusted Roles* untuk menjalankan setiap tindakan *Trusted Roles*. PrivyID akan menggunakan prosedur tertentu untuk memastikan bahwa tindakan *Trusted Roles* tidak dapat dijalankan oleh 1 (satu) orang saja.

5.2.3. Identifikasi dan Otentikasi untuk Setiap Peran

Sebelum mengisi posisi *Trusted Roles*, maka individu akan diperiksa latar belakangnya sesuai dengan ketentuan pada pasal 5.3.1 dan 5.3.2 untuk memastikan bahwa *Trusted Roles* diisi oleh orang yang tepat.

5.2.4. Peran yang Memerlukan Pemisahan Tugas

PrivyID memastikan bahwa 1 (satu) orang hanya dapat mengisi 1 (satu) peran *Trusted Roles* pada saat yang bersamaan.

5.3. Kontrol Personil

5.3.1. Persyaratan Kualifikasi, Pengalaman, dan Perizinan

Setiap karyawan yang terlibat dalam kegiatan operasional PKI harus tunduk pada pemeriksaan latar belakang dan pemeriksaan catatan criminal yang dilakukan oleh PrivyID. PrivyID berdasarkan kebijaksanaannya akan memastikan bahwa posisi *Trusted Roles* diisi oleh orang yang berpengalaman,

terampil, terpercaya, dan berintegritas. Untuk memastikan hal tersebut maka PrivyID akan 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 pasal 5.3.1.

5.3.3. Persyaratan Pelatihan

Setiap orang yang diterima untuk mengisi posisi *Trusted Roles* akan 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. Pemahaman mengenai pentingnya keamanan siber, terkhusus mengenai taktik *phishing* dan *social engineering*.

5.3.4. Frekuensi Pelatihan Ulang dan Persyaratannya

Karyawan yang mengisi posisi *Trusted Roles* harus memiliki keahlian dan kemampuan yang konsisten dengan perkembangan industri PKI. Dalam hal PrivyID mengubah kebijakan operasional PKI, maka PrivyID akan memberikan pelatihan sesuai dengan perubahan kebijakan yang diambil oleh PrivyID.

5.3.5. Frekuensi dan Urutan Rotasi Pekerjaan

Tidak ada ketentuan.

5.3.6. Sanksi terhadap Tindakan yang Tidak Sah

Karyawan yang tidak menjalankan perannya sesuai dengan CP/CPS ini, baik secara di sengaja maupun tidak, akan menerima sanksi berdasarkan kebijakan perusahaan. Karyawan yang dikenakan sanksi tersebut akan dicabut 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 didalam CP/CPS ini.

5.3.8. Dokumentasi yang Disediakan untuk Personil

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

5.4. Prosedur Log Audit

5.4.1. Jenis Peristiwa yang Direkam

Informasi yang akan disimpan didalam log termasuk namun tidak terbatas kepada:

a. Aktifitas Pengguna sistem;
b. Identitas Pemegang Sertifikat;
c. Tanggal Sertifikat diterbitkan dan dicabut;
d. Waktu penerbitan CRL;
e. Waktu otentikasi; dan
f. Aktifitas terkait penggunaan repositori.

5.4.2. Frekuensi Pemrosesan Log

PrivyID menentukan waktu secara wajar untuk melakukan review terhadap Log yang sudah disimpan.

5.4.3. Masa Retensi untuk Log Audit

PrivyID akan menyimpan Log audit dalam jangka waktu 10 tahun.

5.4.4. Perlindungan Log Audit

Catatan yang tersimpan dalam log akan dibuat sedemikian rupa sehingga tidak dapat dihapus atau diubah. Hanya *Trusted Roles* yang memiliki akses terhadap Log audit.

5.4.5. Prosedur Pencadangan Log Audit

Log audit akan disalin untuk dicadangankan. Cadangan log tersebut akan disimpan secara terpisah dari Pusat Data.

5.4.6. Sistem Pengumpulan Audit (Internal atau Eksternal)

Proses log untuk audit akan 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

PrivyID akan melakukan penilaian kerentanan, yang tidak terbatas pada *penetration pesting, 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 PrivyID. Hasil dari penilaian kerentanan menjadi informasi yag dirahasiakan dan akan digunakan untuk menjaga dan meningkatkan keamanan sistem PrivyID.

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

b. Log Audit
c. Konfigurasi sistem PKI
d. Dokumen yang tersedia di repository termasuk amandemen dan perubahannya

5.5.2. Masa Retensi Arsip

PrivyID menyimpan catatan didalam arsip selama 10 tahun.

5.5.3. Perlindungan Arsip

Arsip disimpan dan diamankan di lokasi yang berbeda dari Pusat Data.

5.5.4. Prosedur Pencadangan Arsip

Tidak ada ketentuan.

5.5.5. Persyaratan Stempel Waktu Pencatatan

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

5.5.6. Sistem Pengumpulan Arsip (Internal atau Ekternal)

Pengumpulan arsip akan dilakukan secara internal oleh PrivyID.

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Permohonan untuk memperoleh informasi didalam arsip hanya dapat diberikan oleh pihak yang dipercayakan melalui *Trusted Roles.* Secara berkala sampel dari arsip akan diperiksa oleh *Trusted Roles* yang bertanggung jawab terhadap hal tersebut untuk memeriksa integritas dari informasi yang terekam didalam arsip.

5.6. Pergantian Kunci

5.6.1. Pemulihan Bencana dan Kondisi Terkompromi.

Untuk meminimalisir risiko terhadap bocornya Kunci Privat PrivyID, kunci tersebut akan diganti dengan kunci baru yang harus digunakan untuk penandatangan Sertifikat.

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

5.6.2. Prosedur Penanganan Insiden dan Keadaan Terkompromi

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

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

Jika peralatan PKI PrivyID 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 PrivyID.

5.6.4. Prosedur Kunci Privat Entitas Terkompromi

Dalam keadaan dimana Kunci Privat PrivyID terkompromisasi, hilang, hancur, atau dicurigai terkompromisasi, maka setelah dilakukan investigasi, PrivyID harus segera memutuskan untuk mencabut seluruh Sertifikat yang telah diterbitkan dan

membangkitkan pasangan kunci PrivyID yang baru. PrivyID dengan segera akan memberikan pengumuman kepada Pemegang Sertifikat mengenai pencabutan Sertifikat yang disebabkan karena hal tersebut.

5.6.5. Kapabilitas Keberlangsungan Bisnis Setelah Suatu Bencana

PrivyID melakukan *mirroring system* sebagai cadangan layanan PKI di tempat yang terpisah dengan Pusat Data sebagai bagian dari rencana pemulihan bencana. Dalam hal layanan PrivyID terhentikan yang diakibatkan oleh musibah, maka PrivyID akan segera menjalankan layanan PKI-nya melalui cadangan layanan PKI tersebut, hingga Pusat Data pulih dan digunakan seperti semula.

5.7. Pengakhiran CA atau RA

Dalam hal PrivyID mengakhiri layanan-nya, maka:

a. PrivyID akan memberikan pemberitahuan melalui surat elektronik kepada para pihak yang terlibat dalam siklus operasional sertifikat, termasuk kepada Pemegang Sertifikat, Pihak Pengandal, dan Otoritas Pendaftaran;
b. Memastikan bahwa informasi status Sertifikat tetap dapat diakses untuk beberapa jangka waktu setelah pengakhiran layanan;
c. Mengirimkan informasi CRL terakhir kepada Pemegang Sertifikat dan Pihak Pengandal yang merupakan pengguna layanan PrivyID; dan
d. Menghancurkan sistem PKI PrivyID yang berisi Kunci Privat PrivyID.

6. Kontrol Keamanan Teknis

6.1. Pembangkitan dan Instalasi Pasangan Kunci

6.1.1. Pembangkitan Pasangan Kunci

Pasangan kunci PrivyID harus dibangkitkan melalui sistem PKI, dan Kunci Privat PrivyID tidak boleh meninggalkan perangkat keras modul kriptografi yang terhubung dengan sistem tersebut.

6.1.2. Pengiriman Kunci Privat Kepada Pemegang Sertifikat

Pemilik Sertifikat tidak memiliki akses secara langsung terhadap Kunci Privat Pemegang Sertifikat. Kunci Privat dijaga dan digunakan dengan layanan tanda tangan PrivyID.

6.1.3. Pengiriman Kunci Publik ke PrivyID

PrivyID secara langsung menyimpan dan menempelkan Kunci Publik di Sertifikat Elektronik Pemegang Sertifikat setelah penerbitan pasangan kunci dilakukan oleh PrivyID.

6.1.4. Pengiriman Kunci Publik PrivyID ke Pihak Pengandal

Tidak ada ketentuan.

6.1.5. Ukuran Kunci

PrivyID menggunakan kunci Rivest–Shamir–Adleman (RSA) 4096-bit untuk Kunci Induk PrivyID dan RSA 2048-bit untuk Kunci Sub-CA PrivyID dan Kunci Pengguna Akhir. PrivyID menggunakan *Secure Hash Algorithm* versi-2 (SHA-256) untuk menandatangani Sertifikat yang diterbitkannya.

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

PrivyID membangkitkan pasangan kunci sesuai dengan FIPS 140-2 level 3 dan menggunakan suatu metode yang wajar untuk memvalidasi kesesuaian Kunci Publik yang dipersembahkan oleh Pemegang Sertifikat. Untuk Kunci yang telah diuji dan diketahui memiliki kekuatan keamanan yang lemah akan di tolak pada saat persembahan.

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

Kunci PrivyID akan digunakan untuk menandatangani CRL dan menandatangani Sertifikat yang diterbitkan oleh PrivyID.

6.2. Perlindungan Kunci Privat dan Kontrol Modul Teknis Kriptografi

Untuk melindungi Kunci Privat dari semua sertifikat yang diterbitkan, PrivyID akan 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. Standar Modul Kriptografi dan Kontrol

PrivyID harus dibangkitkan oleh perangkat modul kriptografi yang memenuhi standar Federation Information Protection Standards (FIPS) 140-2 Level 3. Untuk operasi penandatanganan, PrivyID juga menggunakan perangkat modul kriptografi dengan standar yang sama.

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

PrivyID 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 PrivyID.

6.2.3. *Escrow* Kunci Privat

Kunci Privat PrivyID tidak akan pernah dititipkan. PrivyID menyimpan dan menjaga Kunci Privat Pemegang Sertifikat.

6.2.4. Cadangan Kunci Privat

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

kunci Pemegang akan disalin dan dijaga oleh PrivyID dengan usaha terbaik. Semua salinan pasangan kunci yang dibangkitkan dilindungi dengan standar dan mekanisme yang sama dengan pasangan kunci asli. Salinan pasangan kunci tersebut akan disimpan dalam lokasi fisik yang berbeda dari Pusat Data.

6.2.5. Pengarsipan Kunci Privat

Lihat kembali 6.2.4.

6.2.6. Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografis

Kunci privat PrivyID 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 yang sejenis. Di luar modul kriptografi, Kunci Privat PrivyID tidak akan pernah ditemukan dalam bentuk teks sederhana (*plaintext*).

6.2.7. Penyimpanan Kunci Privat pada Modul Kriptografis

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

6.2.8. Metode Pengaktifan Kunci Privat

Kunci privat PrivyID diaktifkan dengan mekanisme yang telah disediakan oleh penyedia modul kriptografi dan sesuai dengan prosedur dan standar keamanan informasi. Operasi pengaktifan Kunci Privat PrivyID harus melalui kendali multi personel yang telah dinyatakan dalam CPS.

Pengaktifan dan akses Kunci Privat Pemegang Sertifikat dilindungi dengan mekanisme keamanan yang dikendalikan, diawasi, dijaga, dan diatur oleh PrivyID.

6.2.9. Metode Penonaktifan Kunci Privat

Ketika dalam keadaan tidak digunakan, Kunci Privat PrivyID dinonaktifkan oleh *Trusted Roles* melalui prosedur yang sesuai dengan spesifikasi penyedia modul kriptografi.

6.2.10. Metode Menghancurkan Kunci Privat

Trusted role akan menghancurkan Kunci Privat PrivyID ketika Kunci Privat tidak lagi diperlukan untuk kelangsungan layanan dengan cara menghapus Kunci Privat pada modul kriptografi sesuai dengan prosedur yang telah disediakan oleh penyedia modul kriptografi atau dengan cara menghancurkan fisik dari komponen perangkat keras PrivyID.

Kunci privat Pemegang Sertifikat akan 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.

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

PrivyID mengarsipkan setiap Kunci Publik yang dibangkitkan.

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 selama dua puluh (20) tahun untuk masa Sertifikat Induk PrivyID, sepuluh tahun (10) untuk masa Sertifikat Sub-CA PrivyID, dan satu (1) tahun untuk Pemegang Sertifikat.

6.4. Data Aktivasi

6.4.1. Pembangkitan Data Aktivasi dan Instalasi

Pembangkitan dan penggunaan data pengaktifan PrivyID dilakukan pada Upacara Kunci. Data pengaktifan akan 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 akan 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 PrivyID 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

Untuk dapat mengakses dan menggunakan Sertifikat, Pemegang harus melakukan otentikasi melalui platform yang ditentukan oleh PrivyID.

6.5. Kontrol Keamanan Komputer

6.5.1. Persyaratan Teknis Keamanan Komputer Spesifik

PrivyID memastikan premis dan perangkat keras yang menjaga komponen perangkat lunak PrivyID aman dari akses yang tidak sah. PrivyID melaksanakan mekanisme teknis dan prosedur yang memastikan keamanan informasi pada sistem PrivyID. Semua akses terhadap informasi terkait PrivyID tercatat dan memerlukan otentikasi identitas berdasarkan pembatasan kontrol akses layanan untuk setiap *Trusted Roles*. Semua akses akan menjadi catatan audit yang dilindungi untuk tujuan pencegahan dan penaggulangan 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 kebijakan least privileged.
c. Menyediakan kemampuan dan sumber daya untuk keperluan audit keamanan.
d. Menyediakan jalur dan mekanisme terpercaya untuk akses sistem.
e. Memberikan kemampuan untuk melakukan pemeriksaan terhadap standar dari perangkat lunak dan perangkat keras yang terpasang dengan standar yang telah ditetapkan melalui kebijakan internal perusahaan.
f. 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 PrivyID beroperasi dengan konfigurasi yang telah dievaluasi untuk menjaga standar keamanan komputer.

6.5.2. Peringkat Keamanan Komputer

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

6.6. Siklus Kontrol Teknis

Semua komponen PKI milik PrivyID harus melalui siklus kontrol teknis sebagai berikut:

a. Pengadaan perangkat keras dan perangkat lunak akan melalui prosedur tertentu yang memastikan perangkat terbebas dari segala perubahan yang tidak sah.

b. Upaya yang wajar akan dilakukan untuk mencegah dan mengatasi akses perangkat lunak berbahaya ke dalam ekosistem perangkat PrivyID.
c. Semua personil yang memiliki akses ke dalam sistem PrivyID harus melalui pengecekan kualifikasi dan latar belakang sesuai yang telah ditentukan.
d. Semua aspek terkait pengelolaan komponen PrivyID diatur dan diawasi dengan mekanisme yang telah ditentukan oleh PrivyID untuk menjamin keamanan informasi beserta penanggulangan terhadap risiko yang ada.

6.6.1. Kontrol Pengembangan Sistem

Tidak ada ketentuan.

6.6.2. Kontrol Manajemen Keamanan

Segala perubahan pada konfigurasi sistem PKI milik PrivyID 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 akan divalidasi terbebas dari segala perubahan diluar yang telah ditentukan.

6.6.3. Siklus Kontrol Keamanan

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

6.7. Kontrol Keamanan Jaringan

PrivyID akan melakukan upaya yang wajar untuk melindungi jaringan semua komponen PKI pada PrivyID dari serangan seperti namun tidak terbatas pada *Denial of Service* (DoS), Slow Loris, Go Loris dan serangan intrusi. Upaya-upaya tersebut termasuk namun tidak terbatas pada penggunaan *firewall*, pembatasan dan penjaringan akses jaringan, dan memasang sistem pengawasan jaringan. PrivyID juga menggunakan jaringan aman terpercaya yang

secara khusus yang telah disediakan untuk akses *remote* komponen PKI.

6.8. Stempel Waktu

PrivyID akan melakukan upaya yang wajar mengkonfigurasi dan menjaga sinkronisasi jam sistem internal semua komponen CA menggunakan *Network Time Protocol*. Sistem ini akan 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 Pengguna.

7. Profil Sertifikat, CRL, dan OCSP

7.1. Profil Sertifikat

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

Semua Sertifikat yang diterbitkan oleh PrivyID 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 PrivyID.

7.1.1. Nomor Versi

PrivyID menerbitkan semua Sertifikat dengan versi X.509 *version 3 Certificates*.

7.1.2. *Certificate Extentions*

Lihat Lampiran 1.

7.1.2.1. *Key Usage*

Lihat Lampiran 1.

7.1.2.2. *Certificate Policy Extention*

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*

Setiap Sertifikat yang diterbitkan oleh PrivyID mencakup algoritma penanda yang sesuai standar dan format IETF RFC 5280.

7.1.4. Format Nama

Setiap Sertifikat yang diterbitkan oleh PrivyID yang mencakup formulir nama akan patuh terhadap standar IETF RFC 5280. Setiap Sertifikat dengan bidang ini akan patuh terhadap konvensi penamaan dan batasan yang tercantum dalam bagian 3.1.

7.1.5. Batasan nama

Setiap Sertifikat yang diterbitkan oleh PrivyID akan memiliki batasan nama sesuai dengan yang tercantum dalam bagian 3.1.

7.1.6. *Certificate Policy Object Identifier*

Pengidentifikasi objek kebijakan (OID) merupakan set nomor yang secara unik menunjuk kepada sebuah objek atau kebijakan yang diatur dalam CP/CPS. Bidang kritikalitas ekstensi ini disetel ke FALSE.

7.1.7. Penggunaan Ekstensi Batasan Kebijakan

Tidak ada ketentuan.

7.1.8. Kualifikasi Kebijakan Sintaksis dan Semantik

PrivyID menerbitkan Sertifikat yang dapat mencakup kualifikasi kebijakan dan teks yang sesuai untuk menentukan tujuan penggunaan sertifikat.

7.1.9. Pemrosesan Semantik untuk Ekstensi Kebijakan Sertifikat Kritis

Tidak ada ketentuan.

7.2. Profil CRL

7.2.1. Nomor Versi

CRL yang diterbitkan oleh PrivyID patuh terhadap standar IETF RF 5280 dengan format X.509 *version 2*. CRL yang diterbitkan memiliki bidang-bidang sebagai berikut:

a. *Issuer*: Subjek DN dari PrivyID.
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 PrivyID 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

PrivyID menerbitkan CRL dengan ekstensi sebagai berikut:

a. *CRL number*: Nomor serial CRL.
b. *Authority Key Identifier*: 160-bit SHA-1 hash dari Kunci Publik PrivyID
c. *Issuing Distribution Point*: Alamat tautan untuk mengunduh CRL.

7.3. Profil OCSP

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

PrivyID mengeluarkan 1 versi untuk respon OCSP dengan bidang sebagai berikut:

a. *Version*: Versi dari OCSP.
b. *Requestor list*: Informasi unik dari Sertifikat target seperti *serial number*, *hash algorithm*, *issuer name hash*, dan *issuer key hash*.
c. *Request extensions*: Jika permintaan yang dikirimkan ke tautan OCSP responder memiliki bidang nonce, maka respon balik akan memiliki nilai nonce yang sama.
d. *Response status*: Status balikan dari tautan OCSP *responder*.
e. *Certificate status*: Status dari Sertifikat target.
f. *This update*: Tanda waktu dari respon balik OCSP responder.
g. *Reason*: Sebab dari status Sertifikat, hanya jika ada.
h. *Revocation time*: Tanda waktu pencabutan Sertifikat, hanya jika ada.

7.3.1. Nomor Versi

Tidak ada ketentuan.

7.3.2. Ekstensi OCSP

Tidak ada ketentuan.

8. Audit Kepatuhan dan Penilaian Lainnya

8.1. Frekuensi atau Keadaan Penilaian

Implementasi dari CP/CPS ini dijalankan dengan maksud untuk memenuhi kriteria dari standar yang dikeluarkan oleh Kementerian Komunikasi dan Informatika (Kominfo) dan juga standar industri internasional. Oleh karena itu, PrivyID akan diaudit oleh Kementerian Kominfo dan juga diaudit tahunan untuk memenuhi standar terakhir dari *Webtrust for Certification Authorities.*

8.2. Identitas/kualifikasi Asesor

Audit eksternal akan dilakukan oleh auditor 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.

8.3. Hubungan Asesor dengan Badan yang Dinilai

Auditor yang dipilih untuk melakukan audit merupakan auditor independen diluar PrivyID.

8.4. Topik Penilaian

Ruang lingkup audit akan meliputi, namun tidak terbatas pada, pengungkapan praktik bisnis yang tertulis pada CP/CPS, integritas dari layanan operasional PKI, kepatuhan operasional terhadap CP/CPS, dan hal lainnya yang tercantum dalam standar dari Kementerian Kominfo dan Webtrust.

8.5. Tindakan yang Diambil Sebagai Akibat dari Kekurangan

PrivyID akan menyusun rencana perbaikan sebagai tindakan perbaikan terhadap terhadap kekurangan yang tercatat berdasarkan hasil audit.

8.6. Komunikasi Hasil

Laporan hasil audit akan dilaporkan kepada PA untuk dianalisis lebih lanjut dan untuk memutuskan rencana perbaikan apa yang harus dilakukan terhadap hasil audit tersebut.

9. Bisnis Lain dan Masalah Hukum

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

PrivyID dapat mengenakan biaya untuk penerbitan dan pembaruan Sertifikat Elektronik.

9.1.2. Biaya Akses Sertifikat

Tidak ada ketentuan.

9.1.3. Biaya Akses Pencabutan atau Status Informasi

Tidak ada ketentuan.

9.1.4. Biaya untuk Layanan Lainnya

PrivyID dapat mengenakan biaya untuk biaya lain yang belum diatur di CP/CPS ini.

9.1.5. Kebijakan Pengembalian

Tidak ada ketentuan.

9.2. Tanggung Jawab Keuangan

9.2.1. Cakupan Asuransi

PrivyID memiliki *Cyber Edge Insurance Policy* dengan gabungan batas tanggungan sebesar USD 2.000.000. (Dua Juta dolar Amerika Serikat).

9.2.2. Aset Lainnya

PrivyID menjamin bahwa PrivyID memiliki sumber kapital yang cukup untuk menjalankan kegiatan operasionalnya dan menjalankan fungsinya.

9.2.3. Jaminan Asuransi atau Garansi untuk Entitas Akhir

PrivyID memberikan jaminan kepada Pemegang Sertifikat sebagaimana diatur dalam Kebijakan Jaminan yang dapat diakses pada situs PrivyID.

9.3. Kerahasiaan Informasi Bisnis

9.3.1. Cakupan Informasi Rahasia

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

a. Data Pribadi sebagai mana yang diatur dalam Pasal 9.4,
b. Kunci Privat Pemegang Sertifikat yang disimpan oleh PrivyID, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemegang Sertifikat,
c. Catatan Permohonan Sertifikat,
d. Laporan Audit yang dibuat oleh PrivyID, atau auditor eksternal maupun internal, dan
e. Hasil penilaian kerentanan, dan
f. Dokumentasi Proses Bisnis PrivyID diluar dari yang dipaparkan di CP/CPS ini dan/atau repositori, seperti *Disaster Recovery Plan* dan *Business Continuity Plans*

9.3.2. Informasi yang Dikecualikan dari Cakupan Informasi Rahasia

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

9.3.3. Tanggung Jawab untuk Melindungi Informasi Rahasia

PrivyID menjaga informasi rahasia melalui prosedur operasi standar, pelatihan, dan implementasi khusus mengenai informasi rahasia yang dilakukan oleh pegawai PrivyID dan juga pihak terkait lainnya.

9.4. Privasi Informasi Pribadi

9.4.1. Rencana Privasi

PrivyID melindungi data pribadi sesuai dengan ketentuan yang tercantum didalam Kebijakan Privasi dan juga Ketentuan

Penggunaan Layanan PrivyID yang disesuaikan dengan ketentuan peraturan perundang-undangan.

9.4.2. Informasi yang Dianggap Data Pribadi

Semua informasi tentang Pemegang Sertifikat yang tidak tersedia secara umum melalui Sertifikat Elektronik 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.

9.4.3. Informasi yang Dianggap Bukan Data Pribadi

Informasi di dalam Sertifikat dan CRL tidak dianggap sebagai informasi data pribadi.

9.4.4. Tanggung Jawab Melindungi Informasi Data Pribadi

Informasi data pribadi harus dilindungi dari akses tidak sah dan pihak ketiga tanpa persetujuan dari pemilik data pribadi.

9.4.5. Pemberitahuan dan Persetujuan Penggunaan Data Pribadi

Kecuali dinyatakan lain dalam CP/CPS ini, Kebijakan Data Pribadi atau perjanjian lainnya, informasi data pribadi tidak akan digunakan tanpa persetujuan dari pemilik data pribadi.

9.4.6. Pengungkapan Berdasarkan Proses Administratif atau Peradilan

PrivyID dapat mengungkapkan data pribadi dalam rangka memenuhi ketentuan hukum dan peraturan perundang-undangan, dalam rangka proses penegakan hukum atau pengambilan tindakan pencegahan lebih lanjut sehubungan dengan kegiatan yang tidak berwenang, dugaan tindak pidana atau pelanggaran hukum atau peraturan perundang-undangan.

9.4.7. Keadaan Pengungkapan Informasi Lainnya

Tidak ada ketentuan.

9.4.8. Hak atas Kekayaan Intelektual

PrivyID memiliki dan menguasai hak kekayaan intelektual apapun, termasuk namun tidak terbatas pada paten, hak cipta, merek, rahasia dagang, atas Layanan PrivyID (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 Pihak Pengandal tidak dapat menggunakan hak kekayaan intelektual PrivyID tanpa persetujuan tertulis terlebih dahulu dari PrivyID.

9.5. Pernyataan dan Jaminan

9.5.1. Pernyataan dan Jaminan CA

PrivyID menyatakan dan menjamin, sejauh yang ditentukan dalam CP/CPS ini, bahwa:

a. PrivyID mematuhi ketentuan yang diatur didalam CP/CPS ini.
b. PrivyID akan menerbitkan dan memperbarui CRL secara berkala.
c. Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP/CPS ini.
d. PrivyID akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

9.5.2. Pernyataan dan Jaminan RA

RA menyatakan dan menjamin, sejauh yang ditentukan dalam CP/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; dan

c. Kegiatan registrasi yang dilakukan oleh RA adalah sesuai dengan CP/CPS ini dan dituangkan di dalam perjanjian.

9.5.3. Pernyataan dan Jaminan Pemegang Sertifikat

Pemegang Sertifikat menjamin bahwa:

a. Setiap tanda tangan digital yang dibuat dengan menggunakan Kunci Privat yang terkait dengan Kunci Publik yang ada di dalam sertifikat digital adalah tanda tangan digital dari Pemegang Sertifikat dan Sertifikat sudah diterima dan valid (tidak kadaluarsa atau dicabut) saat tanda tangan digunakan,
b. Kunci privat akan diamankan oleh PrivyID 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,
d. Semua informasi yang diberikan oleh Pemegang Sertifikat dan informasi yang berada di dalam sertifikat adalah benar,
e. Sertifikat Digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CP/CPS ini, dan
f. Pemegang sertifikat adalah pengguna akhir dan bukan merupakan CA, dan tidak menggunakan Kunci Privat yang terkait dengan Kunci Publik yang tercantum dalam Sertifikat Digital untuk tujuan penanda tangan digital sertifikat (atau format lain dari Kunci Publik yang tersertifikasi) atau CRL sebagai sebuah CA lain.

9.5.4. Pernyataan dan Jaminan Pihak Pengandal

Dalam hal perwakilan dari Pihak Pengandal menggunakan suatu Sertifikat yang diterbitkan oleh PrivyID, Pihak Pengandal harus secara benar memverifikasi informasi yang tercantum didalam sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut.

9.5.5. Pernyataan dan Jaminan Partisipan Lainnya

Tidak ada ketentuan.

9.6. Pelepasan Jaminan

Sepanjang yang diizinkan oleh hukum, PrivyID melepaskan semua jaminan baik tersurat maupun tersirat termasuk jaminan barang dagangan, dan/atau kesesuaian untuk tujuan tertentu.

9.7. Pembatasan Tanggung Jawab

Sepanjang PrivyID telah menjalankan siklus operasional Sertifikat sesuai dengan yang tercantum dalam CP/CPS ini, maka PrivyID tidak bertanggung jawab atas setiap akibat atau kerugian yang timbul akibat penggunaan Sertifikat tersebut, termasuk namun tidak terbatas pada kehilangan keuntungan dan kehilangan data.

9.8. Ganti Rugi

9.8.1. Ganti Rugi oleh PrivyID

PrivyID tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.

9.8.2. Ganti Rugi oleh Pemegang Sertifikat

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pemegang Sertifikat sepakat untuk mengganti rugi PrivyID berikut dengan para pihak terkait terhadap kerugian, kerusakan, dan biaya, yang diakibatkan oleh (i) pelanggaran yang dilakukan oleh Pemegang Sertifikat terhadap Perjanjian Pemegang Sertifikat, CP/CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja, (ii) penggunaan Kunci Privat Pemegang Sertifikat yang tidak sah karena kelalaian Pemegang Sertifikat, atau (iii) penggunaan Sertifikat oleh Pemegang Sertifikat untuk kegiatan melawan hukum.

9.8.3. Ganti Rugi oleh Pihak Pengandal

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pihak Pengandal sepakat untuk mengganti rugi PrivyID berikut

dengan para pihak terkait terhadap kerugian, kerusakan, dan biaya, yang diakibatkan oleh (i) pelanggaran yang dilakukan oleh Pihak Pengandal terhadap Perjanjian Pihak Pengandal, CP/CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja, dan (ii) kegagalan dalam memeriksa respon dari status CRL atau OCSP Sertifikat sebelum penggunaannya.

9.9. Jangka Waktu dan Pengakhiran

9.9.1. Jangka Waktu

CP/CPS ini berlaku secara efektif setelah diterbitkan melalui repositori PrivyID dan akan tetap berlaku hingga berakhirnya masa validitas dari Sertifikat terakhir yang diterbitkan berdasarkan CP/CPS tersebut.

9.9.2. Pengakhiran

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

9.9.3. Dampak dari Pengakhiran dan Ketentuan yang tetap Berlaku

CP/CPS yang berakhir harus segera digantikan dengan CP/CPS yang baru. Untuk hal-hal yang berubah dari CP/CPS sebelumnya, akan disampaikan oleh CP/CPS baru.

9.10. Pemberitahuan Individu dan Komunikasi dengan Partisipan

Setiap pengumuman yang dilakukan oleh PrivyID kepada para pihak yang terkait akan dilakukan melalui informasi elektronik yang ditandatangani secara digital, melalui bentuk tertulis diatas kertas, dan melalui informasi yang tercantum dalam situs yang akan ditampilkan selama 7x24 jam setelah pengumuman disampaikan.

9.11. Amandemen

9.11.1. Prosedur Amandemen

Seluruh perubahan terhadap CP/CPS harus melalui persetujuan dari PA.

9.11.2. Masa dan Mekanisme Perubahan

PrivyID memiliki hak untuk mengubah CP/CPS tanpa melakukan pengumuman kepada pihak terkait. CP/CPS yang mengalami perubahan harus diterbitkan di repositori dalam kurun waktu 7 (tujuh) hari.

9.11.3. Keadaan Dimana OID Harus Diubah

Tidak ada ketentuan.

9.12. Prosedur Penyelesaian Sengketa

Prosedur penanganan penyelesaian sengketa akan diatur secara spesifik melalui Perjanjian Pemegang Sertifikat dan Perjanjian Pihak Pengandal.

9.13. Hukum Yang Berlaku

CP/CPS ini diatur dan ditafsirkan berdasarkan hukum Negara Republik Indonesia.

9.14. Kepatuhan Terhadap Hukum yang Berlaku

PrivyID tunduk kepada hukum yang berlaku di Negara Republik Indonesia.

9.15. Ketentuan yang Belum Diatur

9.15.1. Perjanjian Secara Keseluruhan

Setiap RA terikat secara kontraktual dengan PrivyID untuk memastikan kepatuhan dan kesesuaian fungsi RA dengan CP/CPS, berikut dengan standar industri lain yang dibutuhkan namun belum tercantum pada CP/CPS.

9.15.2. Pengalihan Hak atau Kewajiban

RA dan Pihak Pengandal tidak boleh mengalihkan hak atau kewajiban mereka berdasarkan CP/CPS ini, baik untuk

menjalankan hukum atau lainnya, tanpa persetujuan tertulis dari PrivyID. Segala bentuk upaya pengalihan tanpa persetujuan PrivyID adalah dapat dibatalkan.

9.15.3. Keterpisahan

Dalam hal sebagian dari ketentuan ini tidak dapat dijalankan karena sebab apapun, maka ketentuan lain yang tersisa tidaklah batal dan akan terus berlaku dengan kekuatan penuh.

9.15.4. Penegakan Hukum (Biaya Pengacara dan Pengabaian Hak)

PrivyID dapat mengajukan ganti rugi dan biaya pengacara dari para pihak terhadap kerusakan, kerugian, dan biaya yang diakibatkan atas perilaku pihak tersebut.

9.15.5. Keadaan Kahar

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

9.16. Ketentuan Lain

Tidak ada ketentuan.

10. LAMPIRAN 1 – Profil Sertifikat

10.1. Sertifikat Root Privy CA

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-512 dengan RSA Encryption
Issuer: CN	Root CA Privy CA - G1
Issuer: O	PrivyCA
Issuer: C	ID
Subject: CommonName	Root CA Privy CA - G1
Subject: OrganizationName	PrivyCA
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 20 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Sign Certificate (CA), Sign CRL
Extended Key Usage	N/A
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
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 PrivyID CA Class 1

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-512 dengan RSA Encryption
Issuer: CN	Root CA Privy CA - G1
Issuer: O	PrivyCA
Issuer: C	ID
Subject: CommonName	Privy CA Class 1 - G1
Subject: OrganizationName	PrivyCA
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, Key Cert Sign, CRL Sign
Extended Key Usage	Critical=TRUE OCSP Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE URI = http://167.99.68.164:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=C=ID,%20O=PrivyCA,%20CN=Root%20CA%20Privy%20CA%20-%20G1 CRL Issuer: cn=Root CA Privy CA - G1 o=PrivyCA c=ID
Authority Information access	Critical=FALSE Access Method=OCSP, URI = http://167.99.68.164:8080/ejbca/publicweb/status/ocsp
Certificate Policies	Critical=FALSE Policy OID: 2.5.29.32.0 URL: https://repository.privyca.id/
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=CA, Path Length Constraint=None
Public Key	RSA 2048 bits

10.3. Sertifikat Kelas 1 (Subscriber Certificate)

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Privy CA Class 1 – G1
Issuer: O	Privy CA
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username PrivyID)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Opsional (Perorangan apabila diajukan perorangan)
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 1 (satu) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE URI = http://167.99.68.164:8080/ejbca/publicweb/webdist/certdist?cmd=crl&issuer=CN=Privy%20CA%20Class%201%20-%20G1,O=PrivyCA,C=ID CRL Issuer: c=ID o=PrivyCA cn=Privy CA Class 1 - G1
Authority Information access	Critical=FALSE Access Method=OCSP URI = http://167.99.68.164:8080/status/ocsp
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	RSA 2048 bits