Certification Practice Statement (CPS)

Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia

PT Digital Tandatangan Asli (DTA)

Nomor	**IT-SOP-49-2.6**
Versi	**2.6**
Tanggal	**5 Juni 2024**
OID	**2.16.360.1.1.1.3.12.6.0.2.1**
Jenis Dokumen	**Kebijakan**
Klasifikasi	**Publik**

Ditandatangani secara elektronik oleh
Robert Rompas
pada 10/06/2024 09:15

Aries Kusdaryono
Policy Authority PSrE Induk

Robert Rompas
Policy Authority DTA

Keterangan Revisi Dokumen

Status Perubahan Dokumen				
Versi	**Reviu/Revisi** **Tanggal**	**Catatan / Perubahan**	**Dibuat oleh**	**Disetujui oleh**
00	30-11-2021	Edisi Perdana	Policy Authority Officer	Policy Authority
1.1	04-04-2022	• Perubahan Penomoran Dokumen • Perubahan Logo dalam Dokumen • Perubahan Format Penomoran Dokumen. Dari format 00,01,02 menjadi 1.0,1.1,1.2 • Perubahan Alamat Website DTA • Perubahan Alamat Kantor DTA • Perubahan Nomor Telfon kontak yang dapat dihubungi. Dari 081280853907 menjadi 02125981386 • Perubahan Subyek Distinguished Name (DN) untuk Sertifikat Pemilik	Policy Authority Officer	Policy Authority
1.2	13-10-2022	• Penambahan ketentuan terkait pendaftaran dan verifikasi untuk WNI Tatap Muka level 2 dan WNA yang tinggal di Indonesia Tatap Muka level 2 • Perubahan terkait CP	Policy Authority Officer	Policy Authority
1.3	17-05-2023	Perubahan Format persetujuan Manajemen	Policy Authority Officer	Policy Authority
2.0	04-09-2023	• Penyesuaian dengan o Peraturan Menteri Kominfo No 11 tahun 2022 o CP PSrE Induk o CPS PSrE Induk	Policy Authority Officer	Policy Authority
2.1	10-09-2023	• Penambahan penjelasan terkait persetujuan Sertifikat yang diterbitkan • Perbaikan Diagram Heirarki	Policy Authority Officer	Policy Authority
2.2	09-11-2023	Perbaikan untuk Temuan Audit Kominfo	Policy Authority Officer	Policy Authority
2.3	01-02-2024	Perubahan kolom keterangan revisi dokumen	Policy Authority Officer	Policy Authority
2.4	08-02-2024	Perbaikan untuk Temuan Audit Kominfo Catatan Kerja 7 Februari 2024	Policy Authority Officer	Policy Authority
2.5	13-02-2024	• Perbaikan penjelasan pada bagian 5.5.2 terkait Arsip	Policy Authority Officer	Policy Authority
2.6	05-06-2024	Penambahan penanda tangan Dokumen CPS	Policy Authority Officer	Policy Authority

DAFTAR ISI

1. PENGANTAR

Infrastruktur Kunci Publik (IKP) Indonesia adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikasi Elektronik (PSrE) Induk. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PT Digital Tandatangan Asli (DTA) adalah PSrE Indonesia (PSrE Berinduk) non-Instansi yang menerbitkan Sertifikat dibawah PSrE Induk (Kemenkominfo). Sebagai PSrE non-instansi, DTA menerbitkan sertifikat kepada pihak swasta Warga Negara Indonesia, Warga Negara Asing yang tinggal di indonesia dan untuk Badan Usaha untuk kepentingan transaksi eletronik pihak swasta.

Dokumen *Certification Practice Statement* (CPS) DTA ini mendefinisikan persyaratan prosedural dan operasional yang dianut oleh DTA saat menerbitkan dan mengelola objek yang ditandatangani secara digital dalam lingkungan IKP Indonesia. Layanan yang diberikan DTA adalah penerbitan, pencabutan, penerbitan ulang Sertifikat untuk Pemilik dan Tandatangan Digital untuk dokumen Pdf.

Dokumen ini ditunjukan kepada:

1. PT Digital Tandatangan Indonesia (DTA) agar beroperasi sesuai dengan *Certification Practice Statement* (CPS) dimana CPS DTA mengacu pada persyaratan yang diatur di dalam CP PSrE Induk.
2. Pemilik Sertifikat yang perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai pemegang sertifikat yang diterbitkan oleh PT Digital Tandatangan Asli (DTA) dan bagaimana mereka dilindungi oleh PT Digital Tandatangan Asli (DTA).
3. Pengandal yang perlu memahami seberapa besar tingkat kepercayaan terhadap Sertifikat Pemilik atau tanda tangan elektronik tersertifkasi (tanda tangan digital) dan layanan yang memanfaatkan sertifikat elektronik lain yang menjadi bagian dari rantai kepercayaan (*trust chain)* Sertifikat PT Digital Tandatangan Asli (DTA).

1.1. Ringkasan

CPS ini berlaku untuk hierarki IKP Indonesia dari PSrE Induk (diperlihatkan dalam Diagram) dan semua Sertifikat yang diterbitkan secara langsung melalui sistem PT Digital Tandatangan Asli (DTA). Tujuan dari CPS ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan Sertifikat PT Digital Tandatangan Asli untuk menunjukan kepatuhan terhadap akreditasi yang diterima industri formal, seperti *WebTrust*. Selain itu Undang-Undang Republik Indonesia Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan pengakuan atas tanda tangan elektronik yang digunakan untuk tujuan autentikasi, verifikasi, dan nirsangkal. PT Digital Tandatangan Asli (DTA) beroperasi dalam lingkup bagian UU ITE saat memberikan layanannya.

CPS ini menetapkan tujuan, peran, tanggung jawab, dan praktek semua entitas yang terlibat dalam siklus hidup Sertifikat yang diterbitkan berdasarkan CPS ini. Dalam istilah sederhana, CPS menyatakan”praktik dan prosedur yang dilakukan”, yaitu menetapkan prosedur sesuai kerangka aturan operasional untuk produk dan layanan.

CPS merupakan penjelasan yang menyatakan cara PT Digital Tandatangan Asli (DTA) dalam mematuhi CP PSrE Induk. CPS PT Digital Tandatangan Asli (DTA) berisi ringkasan proses, prosedur, dan ketentuan umum yang dilakukan oleh PT Digital Tandatangan Asli (DTA) untuk memenuhi CP PSrE Induk. Ringkasan proses, prosedur, dan ketentuan umum tersebut digunakan

oleh PT Digital Tandatangan Asli (DTA) dalam menerbitkan dan memelihara Sertifikat PT Digital Tandatangan Asli (DTA).

CPS ini mengacu kepada CP PSrE Induk (Kominfo) dan standar Request for Comments 3647 (RFC 3647) dari Internet Engineering Task Force (IETF) tentang Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework.

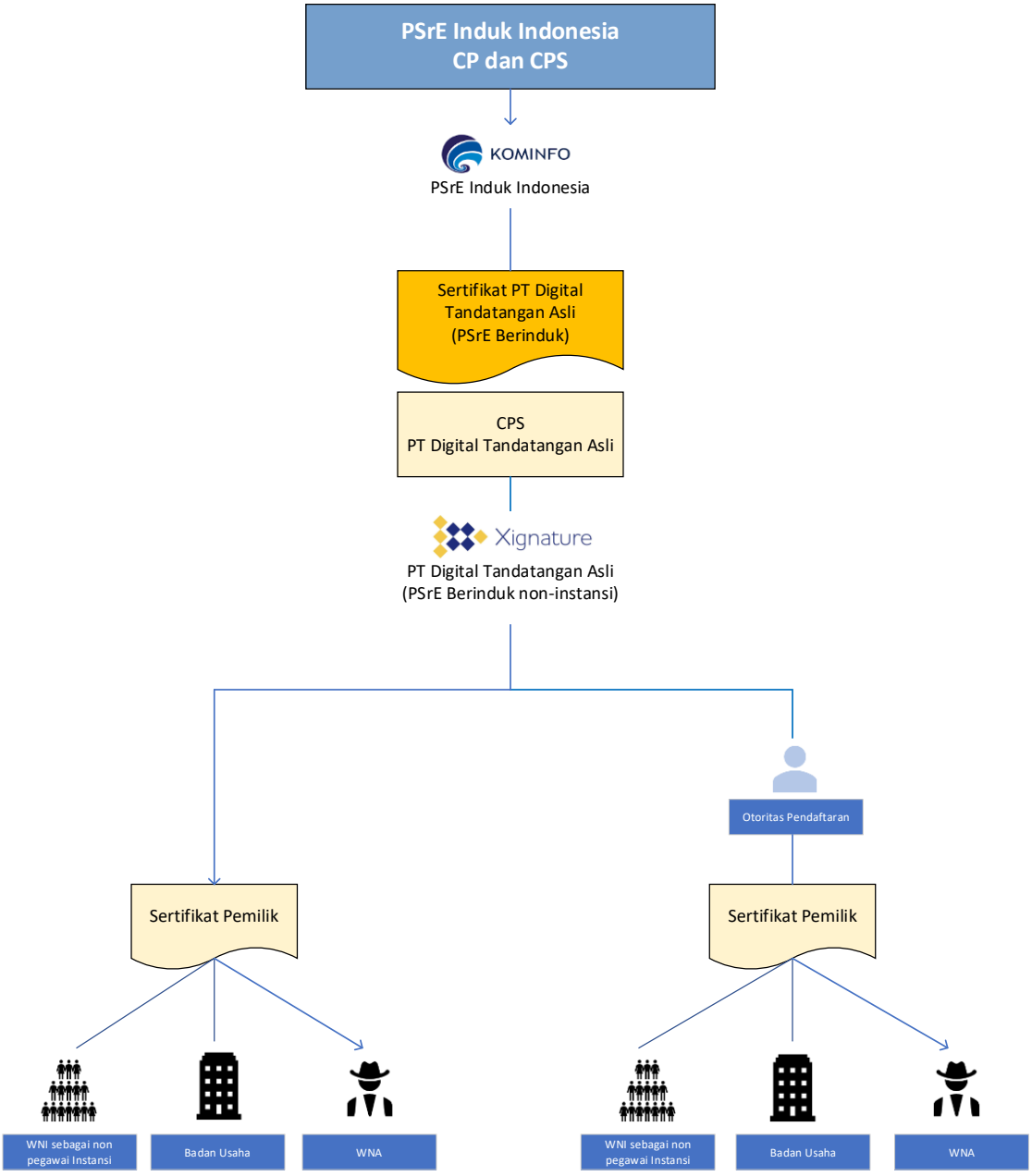

Diagram 1. Struktur Hierarki IKP PT Digital Tandatangan Asli

Sebagai pelengkap CPS, PT Digital Tandatangan Asli (DTA) mengelola dokumen kebijakan terkait beberapa hal, antara lain:

1. Prosedur pemulihan bencana dan keberlangsungan bisnis;
2. Kebijakan keamanan;
3. Kebijakan Personil PT Digital Tandatangan Asli;
4. Prosedur Manajemen Kunci;

5. Kebijakan Privasi.

1.2. Identifikasi dan Nama Dokumen

Dokumen ini adalah Dokumen CPS *(Certification Practice Statement)* DTA.

Object Identifier (OID) yang digunakan untuk CPS (tidak termasuk *Extended Validation Certificate*) DTA adalah:

[Sebelum - Peraturan Menteri Kominfo Nomor 11 Tahun 2022]

Sertifikat pemilik yang diterbitkan sebelum CPS ini dipublikasikan masih menggunakan OID seperti yang tercantum pada tabel di bawah ini, yang berlaku paling lama sampai 1 (satu) tahun sejak CPS dipublikasikan.

1. DTAEndUser
   - OID in Certificate Profile:

CPS	2.16.360.1.1.1.3.12.6.0.2.1
OID PSrE Indonesia Non-Instansi	2.16.360.1.1.1.3.12
PT Digital Tandatangan Asli (DTA)	2.16.360.1.1.1.3.12.6
OID untuk Level 4 *	2.16.360.1.1.1.4.4
Orang perseorangan/Individu	2.16.360.1.1.1.7.1
NIK (OID SII Type)	2.16.360.1.1.1.6.1

   * Sesuai Peraturan Menteri Kominfo Nomor 11 tahun 2018 tentang Penyelenggaraan Sertifikasi Elektronik (PM 11/2018).

[Sesudah - Peraturan Menteri Kominfo Nomor 11 Tahun 2022]

1. DTAEndUserWNIOnline (WNI - Individu Online)
   - OID in Certificate Profile:

CPS	2.16.360.1.1.1.3.12.6.0.2.1
PT Digital Tandatangan Asli (DTA)	2.16.360.1.1.1.3.12.6
Individu non-Instansi Online Level 2	2.16.360.1.1.1.5.1.2.2
NIK (OID SII Type)	2.16.360.1.1.1.6.1

2. DTAEndUserWNIOffline (WNI - Individu Offline)
   - OID in Certificate Profile:

CPS	2.16.360.1.1.1.3.12.6.0.2.1
PT Digital Tandatangan Asli (DTA)	2.16.360.1.1.1.3.12.6
Individu non-Instansi Offline Level 2	2.16.360.1.1.1.5.1.1.2
NIK (OID SII Type)	2.16.360.1.1.1.6.1

3. DTAEndUserSeal (Stamp/Seal - Badan Usaha)
   - OID in Certificate Profile:

CPS	2.16.360.1.1.1.3.12.6.0.2.1
PT Digital Tandatangan Asli (DTA)	2.16.360.1.1.1.3.12.6
Badan Usaha (Segel El)	2.16.360.1.1.1.8.1

4. DTAEndUserWNAOffline (WNA - Individu Offline)
   - OID in Certificate Profile:

CPS	2.16.360.1.1.1.3.12.6.0.2.1
PT Digital Tandatangan Asli (DTA)	2.16.360.1.1.1.3.12.6
WNA Offline Level 2	2.16.360.1.1.1.5.2.1.2
NIK (OID SII Type)	2.16.360.1.1.1.6.1

1.3. Partisipan IKP

1.3.1. Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1. PSrE Induk Indonesia

PSrE Induk adalah PSrE Induk dari IKP Indonesia. PSrE Induk menerbitkan dan/atau mencabut Sertifikat PSrE Indonesia (DTA) berdasarkan status Pengakuan yang diberikan oleh Kominfo. PSrE Induk tidak menerbitkan Sertifikat kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat DTA, sebagaimana dirinci dalam CPS ini, termasuk namun tidak terbatas pada:

a. Pengendalian terhadap proses pendaftaran;
b. Proses identifikasi dan autentikasi;
c. Proses penerbitan self-sign Sertifikat;
d. Proses penerbitan Sertifikat PT Digital Tandatangan Asli (DTA);
e. Proses Penerbitan Daftar Pencabutan Sertifkat (*Certificate Revocation List*/CRLs);
f. Publikasi Sertifikat dan CRLs;
g. Validasi Sertifikat;
h. Pencabutan Sertifikat; dan
i. Membangun dan memelihara sistem PT Digital Tandatangan Asli (DTA);
j. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan DTA yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk.

1.3.1.2. PSrE Indonesia

DTA adalah PSrE yang mendapatkan pengakuan dari Menteri Komunikasi dan Informatika (Menteri) dengan berinduk kepada PSrE Induk yang diselenggarakan oleh Menteri yang Sertifikatnya telah ditandatangani oleh PSrE Induk. DTA menerbitkan Sertifikat kepada Pemilik Sertifikat sebagaimana digambarkan pada Diagram 1 diatas.

DTA adalah PSrE non-Instansi yaitu PSrE yang menerbitkan Sertifikat kepada WNI non instansi dan Badan Usaha.

DTA membuat dan memelihara CPS serta memastikan bahwa semua aspek layanan DTA, operasi, dan infrastruktur dilakukan sesuai dengan CP PSrE Induk

DTA tidak berinduk kepada PSrE lain dan tidak menjadi induk bagi PSrE lainnya.

1.3.2. Otoritas Pendaftaran (RA)

Registration Authority (RA) bertanggung jawab dan bertindak secara langsung melakukan, penerimaan permohonan, pendaftaran, identifikasi, autentifikasi dan pencabutan Sertifikat sesuai dengan yang telah didefinisikan dalam CPS dan dokumen terkait.

DTA dapat menunjuk RA tertentu untuk melakukan penerimaan permohonan. Dalam hal DTA bertindak secara langsung untuk menerima permohonan penerbitan Sertifikat dari Pemohon maka DTA berperan sebagai RA bagi dirinya sendiri.

PT Digital Tandatangan Asli harus melaksanakan audit terhadap RA yang ditunjuk. Audit yang dilakukan terhadap RA tersebut paling sedikit memeriksa keamanan dan kesesuaian fungsi berdasarkan ketentuan peraturan perundang-undangan dan CPS ini. PT Digital Tandatangan Asli (DTA) dalam melakukan wewenang memeriksa kebenaran identitas perpanjangan masa berlaku, dan pencabutan Sertifkat dapat dilakukan dengan bekerja sama dengan pihak ketiga misalnya notaris dan/atau pihal lain sebagai RA. Kerja sama dengan RA tidak melepaskan tanggung jawab PT Digital Tandatangan Asli (DTA) sesuai dengan ketentuan peratura perundang-undangan.

RA PT Digital Tandatangan Asli (DTA) berkewajiban untuk melaksanakan fungsi sebagai berikut:

a. Menyusun dan melaksanakan prosedur penerimaan pendaftaran Pemohon Sertifikat Elektronik;
b. Menerima pendaftaran Sertifikat dan memproses permohonan pencabutan Sertifikat,
c. Melakukan identifikasi dan autentikasi Pemohon berdasarkan Prosedur Penerbitan Sertifikat Elektronik yang ditetapkan oleh DTA; dan
d. menyetujui permohonan untuk Pembuatan Kunci Ulang (*Re-Key*) Sertifikat, atas nama PSrE.

Dalam hal DTA menunjuk pihak ketiga sebagai RA, fungsi di atas tercantum dalam perjanjian kerja sama antara DTA dengan RA pihak ketiga.

1.3.3. Pemilik

Pemilik adalah pihak yang identitasnya tertera dalam Sertifikat yang diterbitkan oleh DTA dan sudah melalui proses verifikasi. Entitas Pemilik berarti subjek pemegang Sertifikat sekaligus entitas yang terikat dengan DTA sebagai penerbit Sertifikat. Sebelum dilakukan verifikasi identitas dan Sertifikat diterbitkan, Entitas disebut sebagai Pemohon.

Pemilik adalah pihak yang namanya tertera sebagai subjek pada Sertifikat yang menegaskan bahwa dia menggunakan kunci dan Sertifikat sesuai dengan CPS.

DTA menerbitkan Sertifikat kepada perseorangan non-Instansi untuk Warga Negara Indonesia dan Warga Negara Asing yang tinggal di Indonesia.

1.3.4. Pengandal

Pengandal adalah pihak yang mengandalkan (mempercayai) informasi yang ada dalam Sertifikat dan/atau tanda tangan elektronik tersertifikasi dan/atau layanan yang memanfaatkan Sertifkat lainnya yang diverifikasi menggunakan Sertifkat tersebut.

Pengandal terlebih dahulu memeriksa respon dari *Certificate Revocation Lists* (CRL) dan/atau *Online Certificate Status Protocol* (OCSP) DTA sebelum memanfaatkan informasi yang ada dalam Sertifikat.

Pengandal bertanggung jawab untuk melakukan pengecekan informasi di dalam Sertifikat. Pengandal menggunakan informasi dalam Sertifikat untuk menentukan kesesuaian penggunaan dan tujuan Sertifikat. Pengandal menggunakan informasi dalam Sertifikat untuk:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi tanda tangan digital dan layanan lain yang menggunakan Sertifkat;
c. Memeriksa status pencabutan Sertifikat (*revocation)* menggunakan CRL dan/atau OCSP; dan
d. Penyetujuan batas tanggung jawab dan jaminan.

Pengandal meliputi Bank, Perusahaan *e-commerce*, Instansi Penyelenggara Negara dan entitas lain yang menggunakan tanda tangan digital di dalam layanannya.

1.3.5. Partisipan Lain

Partisipan Lain adalah Penyelengara Sistem Elektronik yang bekerja sama dengan PT Digital Tandatangan Asli (DTA) dalam penyelenggaraan sebagian infrastruktur atau layanan terkait Penyelenggaraan Sertifkat Elektronik. PT Digital Tandatangan Asli (DTA) menentukan Partisipan Lain yang berhubungan dengan Penyelenggaraan Sertifkat Elektronik. Dalam hal DTA bekerjasama dengan Partisiapan Lain untuk menyelenggarakan layanan, DTA mendapat persetujuan dari Kominfo.

1.3.5.1. Penyedia Layanan Pusat Data

Penyedia Layanan Pusat Data adalah Pihak Ketiga yang menyediakan layanan Pusat Data dan Pusat Pemulihan bencana untuk operasional DTA.

1.4. Kegunaan Sertifikat

1.4.1. Penggunaan Sertifikat yang Semestinya

Sertifikat PT Digital Tandatangan Asli (DTA) hanya digunakan untuk menandatangani Sertifikat Pemilik, CRL, OCSP, dan Sertifikat penanda waktu, serta untuk verifikasi Sertifikat.

Penggunaan Sertifikat Pemilik dibatasi sesuai Key Usage dan Extended Key Usage pada Certificate Extension. Sertifikat PT Digital Tandatangan Asli (DTA) dapat digunakan untuk menerbitkan Sertifikat Pemilik untuk transaksi yang memerlukan:
1. Tanda Tangan Elektronik; dan
2. Nirsangkal.

DTA menyediakan level verifikasi:
a. Level verifikasi WNI Online Level 2, yaitu Sertifikat dengan level verifikasi online identitas level 2 dengan tingkat jaminan menengah, dimana verifikasi identitas dilakukan dengan menggunakan Kartu Tanda Penduduk dan data biometrik yang dibandingkan dengan basis data kependudukan yang dikelola oleh lembaga Pemerintah yang menyelenggarakan administrasi kependudukan sesuai dengan peraturan perundang-undangan yang dikeluarkan oleh Kominfo;
b. Level verifikasi WNI Tatap Muka level 2, yaitu Sertifikat dengan level verifikasi Tatap Muka identitas level 2 dengan tingkat jaminan menengah;

c. Level verifikasi Badan Usaha Tatap Muka level 3, yaitu Sertifikat dengan level verifikasi Tatap Muka identitas level 3 dengan tingkat jaminan tinggi;
d. Level verifikasi WNA yang tinggal di Indonesia Tatap Muka level 2, yaitu Sertifikat dengan level verifikasi Tatap Muka identitas level 2 dengan tingkat jaminan menengah.

Sertifikat yang diterbitkan oleh DTA adalah Sertifikat dengan level verifikasi identitas yang sesuai dengan peraturan perundang-undangan yang mengatur mengenai penyelenggaraan sertifikasi elektronik. Penggunaan Sertifikat yang tidak sesuai, dapat berakibat pada hilangnya jaminan atau garansi yang diberikan oleh DTA kepada Pemilik Sertifikat dan Pengandal.

1.4.2. Penggunaan Sertifikat yang Dilarang

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

1.5. Administrasi Kebijakan

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

a. Menetapkan Certification Practice Statement (CPS);
b. Memastikan semua layanan, operasional, dan infrastruktur DTA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, pernyataan, dan jaminan dari CP PSrE Induk; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP lainnya yang memiliki level verifikasi yang kurang lebih setara.

1.5.1. Organisasi Pengelola Dokumen

CPS dan dokumen referensinya dikelola oleh *Policy Authority* PT Digital Tandatangan Asli (DTA).

1.5.2. Kontak yang Dapat Dihubungi

Policy Authority PT Digital Tandatangan Asli (DTA) dapat dihubungi melalui:

- Alamat Surat : Genarali Tower, Gran Rubina Business Park Lantai 20, Unit B, Jl HR. Rasuna Said Kav. C-22, Jakarta Selatan 12940
- Alamat Surel : support@xignature.co.id
- URL : https://www.xignature.co.id
- Telepon/Phone : 021-25981386

1.5.3. Personil yang menentukan Kesesuaian CPS dengan Kebijakan

Policy Authority (PA) DTA menentukan kesesuaian konten CPS.

1.5.4. Prosedur Persetujuan CPS

Perubahan CPS PT Digital Tandatangan Asli (DTA) mengacu pada dokumen Panduan CP PSrE Induk.

Policy Authority (PA) DTA menyetujui CPS DTA dan segala perubahannya setelah mendapat persetujuan dari PA PSrE Induk.

Perubahan CPS diinformasikan di https://repository.xignature.co.id/.

1.6. Definisi dan Akronim

Lihat Lampiran A untuk tabel akronim dan definisi.

2. TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI

DTA melaksanakan prosedur yang mengatur ketentuan tentang tanggung jawab publikasi dan repository.

2.1. Repositori

DTA memelihara repositori daring yang berisikan dokumen-dokumen kebijakan yang dapat diakses secara publik.

Policy Authority Officer menyediakan dokumen untuk Administrator Web Repository agar dipublikasi di repository DTA atas persetujuan Policy Authority.

Dokumen – dokumen yang terdapat dalam repositori DTA:
1. Certification Practice Statement (CPS)
2. Kebijakan Jaminan
3. Kebijakan Privasi
4. Panduan Pengamanan Kata Sandi Untuk Pemilik
5. Panduan Tandatangan Elektronik
6. Panduan Verifikasi Tanda Tangan Elektronik Tersertifikasi dan Verifikasi Sertifikat Elektronik
7. Perjanjian Pengandal
8. Perjanjian Pemilik Sertifikat
9. Sertifikat DTA
10. CRL

2.2. Publikasi Informasi Sertifikat

DTA mempublikasikan Dokumen kebijakan yang tertuang di Bagian 2.1 dalam repositori yang dapat diakses melalui https://repository.xignature.co.id/.

2.3. Waktu atau Frekuensi Publikasi

DTA mempublikasikan versi terkini dari dokumen elektronik berikut di Repositori:
1. Sertifikat DTA dipublikasikan segera stelah penerbitan Sertifikat.
2. Dokumen CPS. Jika pembaruan diperlukan, versi terbaru CPS tersebut akan dipublikasikan segera setelah disetujui. CPS dapat diakses publik dalam waktu paling lama 7 (tujuh) hari kerja setelah disetujui.

DTA mempublikasikan informasi CRL secara reguler dan terjadwal sebagaimana diatur dalam Bagian 4.9.7.

2.4. Kendali Akses pada Repositori

Informasi yang terpublikasi pada Repositori adalah informasi publik. DTA memberikan akses baca yang tidak dibatasi pada Repositori dan menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada Repositori tersebut.

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

3. IDENTIFIKASI DAN AUTENTIKASI

3.1. Penamaan

3.1.1. Tipe Nama

DTA men-generate (membangkitkan) dan menandatangani Sertifikat dengan subjek *Distinguished Name* (DN) yang non-null dan mematuhi standar ITU-T X.500.

Pengaturan parameter Sertifikat mengacu pada Standar Interoperabilitas PSrE Indonesia.

3.1.2. Kebutuhan Nama yang Bermakna

Sertifikat yang diterbitkan sesuai dengan CPS ini bermakna hanya jika nama-nama yang muncul dalam Sertifikat dapat dipahami dan digunakan oleh Pengandal. Nama yang digunakan dalam Sertifikat mampu mengidentifikasi orang atau objek tersebut.

Nama subjek dan penerbit yang terkandung dalam Sertifikat bermakna dalam arti bahwa DTA memiliki cukup bukti yang menunjukkan keterkaitan antara nama dengan Pemilik. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh Pemilik yang sah atau perwakilan legal dari Pemilik yang sah.

3.1.3. Anonimitas atau Pseudonimitas Pemilik

DTA tidak menerbitkan Sertifikat anonim atau pseudonim.

3.1.4. Aturan Interpretasi Berbagai Bentuk Nama

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

3.1.5. Keunikan Nama

Distinguished Name (DN) diisi dengan informasi pada saat pendaftaran. Semua DN di Sertifikat perorangan sesuai dengan data yang dimasukkan Pemilik dan bersifat unik. Pemilik bertanggung jawab penuh terhadap ketepatan dan akurasi pemilihan DN. Nama yang tertera di dalam Sertifikat sesuai dengan yang tertera di e-KTP.

3.1.6. Pengakuan, Autentikasi, dan Peran Merek Dagang

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

DTA memastikan keabsahan penggunaan dari nama yang dipilih dengan memeriksa salinan akta pendirian perusahaan beserta perubahannya.

3.2. Validasi Identitas Awal

3.2.1. Metode Pembuktian Kepemilikan Kunci Privat

Metode untuk membuktikan kepemilikan Kunci Privat menggunakan PKCS#10 (CSR).

Pasangan Kunci yang telah dibangkitkan oleh DTA, Kunci Privatnya disimpan dan diamankan dengan menggunakan modul kriptografis yang memenuhi persyaratan Federal Information Protection Standards (FIPS)-140 level 3 dan hanya dapat diakses oleh Pemilik dengan minimal dua faktor autentikasi yaitu password dan biometrik.

3.2.2. Autentikasi dari Identitas Organisasi

Permohonan Organisasi untuk menjadi Pemilik diajukan oleh orang yang berwenang mewakili Organisasi tersebut.

DTA menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi selama masa berlaku dari Sertifikat yang diterbitkan.

Autentikasi identitas pemohon Sertifkat Organisasi sesuai dengan Peraturan Menteri Komunikasi dan Informatika terkait penyelenggara Sertifikasi Elektronik.

Identifikasi dan Autentikasi Identitas Perwakilan Organisasi yang mengajukan permintaan Sertifikat DTA:

Data yang digunakan untuk identifikasi:

a. Surat permohonan persetujuan penerbitan Sertifikat Elektronik yang diajukan oleh perwakilan Badan Usaha;
b. Akta Pendirian Badan Usaha dan/atau Akta Perubahan terakhir Badan Usaha;
c. Surat Keputusan pengesahan Badan Usaha;
d. Salinan Kartu Identitas (KTP) perwakilan Badan Usaha;
e. Foto wajah perwakilan Badan Usaha;
f. Nomor Handphone perwakilan Badan Usaha; dan
g. Alamat email resmi perwakilan Badan Usaha;

DTA wajib melakukan proses verfikasi dengan:

1. Data biometrik berupa swafoto dibandingkan dengan basis data kependudukan yang dikelola oleh lembaga Pemerintah yang menyelenggarakan administrasi kependudukan sesuai dengan peraturan perundang-undangan yang dikeluarkan oleh kominfo;
2. Memeriksa, melakukan validasi bahwa informasi yang terdapat dalam KTP valid dan benar. DTA melakukan verifikasi data pemohon dengan data kependudukan Pemerintah. Data yang diverifikasi adalah NIK, Nama, tanggal lahir dan biometrik wajah;
3. Konfirmasi untuk aktifasi akun dikirim ke alamat surel yang didaftarkan.

Dalam hal proses identifikasi dan autentikasi permohonan Sertifikat Badan Usaha telah berhasil, DTA akan menerbitkan Sertifikat bagi Badan Usaha tersebut.

3.2.3. Autentikasi Identitas Individu

Permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut.

DTA menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi setidaknya untuk selama masa berlaku dari Sertifikat yang diterbitkan.

Autentikasi identitas individu pemohon Sertifikat sesuai dengan Peraturan Menteri Komunikasi dan Informatika terkait Penyelenggara Sertifikasi Elektronik.

Identifikasi dan Autentikasi Identitas Individu yang mengajukan permintaan Sertifikat DTA:

Warga Negara Indonesia:

Data yang digunakan untuk Identifikasi:
a. Salinan Kartu Tanda Penduduk resmi yang dikeluarkan oleh pemerintah;
b. Memasukkan informasi data diri seperti NIK, nama lengkap, tanggal lahir, alamat surel.
c. Data biometrik berupa swafoto yang telah diuji oleh deteksi kehidupan dengan menggunakan mekanisme *liveness detection*.

DTA melakukan proses verifikasi dengan:
a. Data biometrik berupa swafoto dibandingkan dengan basis data kependudukan yang dikelola oleh lembaga Pemerintah yang menyelenggarakan administrasi kependudukan sesuai dengan peraturan perundang-undangan yang dikeluarkan oleh Kemenkominfo;
b. Memeriksa, melakukan validasi bahwa informasi yang terdapat dalam KTP valid dan benar. DTA melakukan verifikasi data pemohon dengan data kependudukan pemerintah. Data yang diverifikasi adalah NIK, nama, tanggal lahir dan biometrik wajah;
c. Konfirmasi untuk aktifasi akun dikirim ke alamat surel yang didaftarkan.

Warga Negara Asing yang tinggal di Indonesia:

Data yang digunakan untuk Identifikasi:
a. Salinan Paspor, KITAP atau KITAS yang dikeluarkan oleh Pemerintah;
b. Surat Jaminan dari Perusahaan yang ditandatangani oleh Penanggung Jawab Perusahaan;
c. Memasukkan informasi data diri seperti Nomor Paspor, Nomor KITAP/KITAS, nama lengkap, tanggal lahir, nomor Handphone dan alamat surel;
b. Foto Wajah.

DTA wajib melakukan proses verifikasi dengan:
a. Melakukan verifikasi tatap muka atau dengan media online melalui zoom atau skype dengan membawa atau menunjukan Dokumen asli untuk diverifikasi;
b. Memeriksa, melakukan validasi bahwa informasi yang terdapat dalam Paspor / KITAP / KITAS valid dan benar. DTA melakukan verifikasi data pemohon dengan data kependudukan pemerintah. Data yang diverifikasi adalah Nomor paspor / KITAP / KITAS, nama, tanggal lahir dan biometrik wajah;
c. Konfirmasi untuk aktifasi akun dikirim ke alamat surel yang didaftarkan.

DTA memeriksa dan melakukan validasi terhadap informasi lainnya yang telah diterima dari Pemohon untuk mendeteksi kebenarannya.

Dalam hal proses identifikasi dan autentikasi permohonan Sertifikat Individu telah berhasil, DTA akan menerbitkan Sertifikat bagi Individu tersebut.

3.2.4. Informasi Pemilik yang Tidak Terverifikasi

Informasi yang tidak bisa diverifikasi tidak disertakan di dalam Sertifikat.

DTA tidak akan menerbitkan Sertifikat dari Pemohon yang informasinya tidak dapat diverifikasi sesuai Bagian 3.2.3 diatas.

3.2.5. Validasi Otoritas

Permohonan Sertifikat yang diajukan dengan atas nama Badan Hukum/Usaha, DTA memastikan Pemohon memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan oleh badan Hukum/Usaha tersebut.

3.2.6. Kriteria Inter-operasi

DTA mengikuti Standar Interoperabilitas PSrE Indonesia dalam rangka melakukan interoperasi antar PSrE Indonesia.

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

3.3.1. Identifikasi dan Autentikasi untuk Re-Key Rutin

Jika Pemilik bersedia terus menggunakan layanan DTA pada saat Sertifikat Pemilik sudah masuk masa 1 bulan sebelum habis masa berlakunya (expire), Pemilik bisa mengulang proses pembuatan Sertifikat dengan melalui verifikasi ulang menggunakan verifikasi biometrik seperti yang diatur dalam Bagian 3.2.

3.3.2. Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan

Setelah Sertifikat dicabut, Pemilik mengulang proses validasi identitas seperti yang dijelaskan pada Bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

3.4. Identifikasi dan Autentikasi untuk Permintaan Pencabutan

Permintaan pencabutan selalu diverifikasi dan diautentikasi tanpa mempertimbangkan apakah Kunci Privat telah terkompromikan (*compromised*).

Permintaan pencabutan Sertifikat Pemilik oleh aparat penegak hukum dilakukan melalui prosedur pencabutan Sertifikat. DTA melakukan verifikasi tatap muka terhadap permintaan pencabutan Sertifikat.

Permintaan pencabutan Sertifikat dapat dimohonkan oleh Pemilik melalui situs https://my.xignature.co.id/ dengan antarmuka sistem DTA.

4. PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT

4.1. Permohonan Sertifikat

4.1.1. Siapa yang dapat Mengajukan Permohonan Sertifikat

Pemohon yang dapat mengajukan permohonan Sertifikat adalah sebagai berikut:
a. Warga Negara Indonesia;
b. Warga Negara Asing yang tinggal di Indonesia;
c. Badan Usaha yang permohonannya diajukan oleh orang yang berwenang mewakili Badan Usaha tersebut.

4.1.2. Proses Pendaftaran dan Tanggung Jawab

Pemohon Sertifikat bertanggung jawab untuk memberikan informasi yang akurat dalam mengisi permohonan Sertifikat sehingga memungkinkan DTA untuk melakukan verifikasi atas identitas Pemohon.

Secara umum, proses pendaftaran terdiri dari langkah-langkah berikut:
a. Menyetujui Perjanjian Pemilik Sertifikat dan kebijakan privasi dengan cara mencentang kotak persetujuan pada saat proses pendaftaran;
b. Mengisi email, no hp dan password sesuai formulir di antarmuka halaman pendaftaran sistem DTA;
c. Mengunggah salinan Kartu Tanda Penduduk;
d. Mengisi data diri sesuai formulir di antarmuka halaman pendaftaran sistem DTA;
e. Melakukan verifikasi data diri yang sudah di isi dengan melakukan centang pada data yang telah diisi;
f. Melakukan verifikasi liveness detection dengan DTA akan mengambil gambar Pemohon pada saat proses liveness detection dan mengirimkan data yang telah disertakan;
g. Pemohon melakukan aktivasi akun;
h. Setelah akun Pemohon telah aktif dan berhasil masuk, pemilik akun DTA dapat melakukan aktivasi nomor handphone;
i. DTA melakukan verifikasi data Pemohon yang diberikan saat pendaftaran dengan menggunakan verifikasi biometrik untuk dibandingkan dengan data penduduk pemerintah. Data yang dibandingkan adalah NIK, nama, tanggal lahir dan biometrik wajah;
j. Pemilik akun melakukan pembayaran untuk proses penerbitan Sertifikat Elektronik;
k. DTA melakukan verifikasi data Pemohon yang diberikan saat pendaftaran untuk dibandingkan dengan data penduduk pemerintah. Data yang dibandingkan adalah NIK, nama, tanggal lahir dan biometrik wajah;
l. Jika verifikasi gagal, maka Pemohon dapat mengulangi dengan memberikan data yang benar tanpa batas; dan
m. Jika verifikasi berhasil, maka Pemohon berhasil membuat digital certificate.

DTA bertanggung jawab:
a. Memeriksa seluruh persyaratan yang dikirimkan oleh pemohon adalah valid dan benar.
b. Memelihara sistem dan proses agar mampu mengautentikasi identitas Pemohon untuk Penerbitan Sertifikat.
c. Memastikan bahwa jalur komunikasi yang digunakan antara pemohon dan DTA dalam menerima dan mengirimkan informasi yang dibutuhkan untuk memenuhi proses pendaftaran adalah jalur komunikasi yang aman.
d. Menyimpan dengan aman informasi yang diberikan oleh Pemohon.

Pemohon harus memberikan informasi yang benar sehingga memungkinkan PSrE DTA untuk melakukan verifikasi atas identitas tersebut.

4.2. Pemrosesan Permohonan Sertifikat

4.2.1. Melaksanakan Fungsi Identifikasi dan Autentikasi

DTA mengindentifikasi dan mengautentikasi Pemilik untuk memenuhi persyaratan yang ditentukan Bagian 3.2 dari CPS ini.

4.2.2. Persetujuan atau Penolakan Permohonan Sertifikat

DTA dan/atau RA hanya akan memberikan persetujuan terhadap permohonan penerbitan Sertifikat apabila telah memenuhi kriteria yang disebutkan pada Bagian 4.1.

Dalam hal Pemohon tidak memenuhi kriteria tersebut, maka DTA dan/atau RA memiliki kewenangan berikut:
1. Menolak permohonan penerbitan Sertifikat; atau
2. Meminta informasi tambahan kepada Pemohon agar dapat memenuhi persyaratan.

4.2.3. Waktu Pemrosesan Permohonan Sertifikat

DTA akan menerbitkan Sertifikat Pemilik tidak lebih dari 60 menit setelah semua proses verifikasi selesai dan berhasil.

4.3. Penerbitan Sertifikat

4.3.1. Tindakan PSrE selama Penerbitan Sertifikat

DTA melakukan tindakan-tindakan sebagai berikut:
1. Melakukan verifikasi dan validasi atas dokumen dan identitas yang diberikan oleh pemohon sebagaimana diatur pada Bagian 3.2.2 dan 3.2.3;
2. Permohonan yang diajukan untuk Badan Hukum/Usaha, DTA memverifikasi otoritas yang melakukan sebagaimana diatur pada Bagian 3.2.5;
3. Mempersiapkan dan menandatangani Sertifikat saat semua persyaratan telah dipenuhi;
4. Memastikan bahwa Pemilik menerima Sertifikat sebagaimana diatur pada Bagian 4.4;
5. Membuat Sertifikat tersedia bagi Pemili setelah Pemilik menyetujui kewajibannya sebagaimana diatur pada Bagian 9.6.3.

4.3.2. Pemberitahuan ke Pemilik oleh PSrE tentang Diterbitkannya Sertifikat

DTA memberitahu Pemilik dalam waktu maksimum 1x24 jam tentang berhasilnya penerbitan Sertifikat melalui email yang telah didaftarkan.

4.4. Penerimaan Sertifikat

4.4.1. Sikap yang Dianggap Menerima Sertifikat

Pemilik dianggap telah menerima Sertifikat yang terbit melalui sistem DTA apabila:

a. Pemilik tidak memberikan tanggapan melalui surel ke support@xignature.co.id sesuai yang tertuang dalam notifikasi surel sebagaimana dimaksud dalam Bagian 4.3.2 dalam jangka waktu paling lama 7 (tujuh) hari kerja, atau

b. Pemilik telah menggunakan Sertifikat untuk Tanda Tangan Digital.

DTA memiliki prosedur yang mengindikasikan dan mendokumentasikan persetujuan atas Sertifikat yang diterbitkan.

4.4.2. Publikasi Sertifikat oleh DTA

Setiap Sertifikat Pemilik diunduh melalui antarmuka sistem DTA.

Sertifikat PSrE Induk dan Sertifikat DTA dipublikasikan di repositori sebagaimana tercantum dalam Bagian 2.1 di atas.

4.4.3. Pemberitahuan Penerbitan Sertifikat oleh DTA ke Entitas Lain

Tidak ada ketentuan.

4.5. Penggunaan Pasangan Kunci dan Sertifikat

4.5.1. Penggunaan Kunci Privat dan Sertifikat oleh Pemilik

DTA melindungi Kunci Privat Pemilik dengan menggunakan Hardware Security Module (HSM) dengan spesifikasi FIPS 140-2 Level 3.

DTA melakukan upaya-upaya pengamanan dan penyimpanan dengan penuh kehati-hatian terhadap Kunci Privat Pemilik agar Kunci Privat tersebut hanya dapat digunakan oleh Pemilik dan dilindungi dari penggunaan tanpa izin.

Pemilik memakai Kunci Privat dan Sertifikatnya hanya untuk tujuan yang sudah ditentukan.

4.5.2. Kunci Publik Pengandal dan Penggunaan Sertifikat

Pengandal menggunakan perangkat lunak yang patuh kepada X.509. DTA menyatakan batasan penggunaan Sertifikat melalui ekstensi Sertifikat dan menyatakan mekanisme untuk menentukan keabsahan Sertifikat (CRL dan OCSP). Pengandal menjalankan dan patuh kepada ketentuan ini sesuai dengan kewajiban mereka sebagai Pengandal.

Pengandal berhati-hati ketika mengandalkan Sertifikat dan mempertimbangkan keseluruhan keadaan dan risiko kerugian sebelum mengandalkan Sertifikat. Mengandalkan Sertifikat yang belum diperiksa sesuai dengan standar yang berlaku dapat menyebabkan risiko bagi Pengandal. Pengandal bertanggung jawab atas risiko tersebut. Jika keadaan menunjukkan bahwa diperlukan jaminan tambahan, Pengandal mendapatkan jaminan tersebut sebelum menggunakan Sertifikat.

4.6. Pembaruan Sertifikat

4.6.1. Kondisi untuk Pembaruan Sertifikat

DTA tidak mendukung prosedur pembaruan sertifikat.

4.6.2. Siapa yang Dapat Meminta Pembaruan

Tidak ada ketentuan

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat

Tidak ada ketentuan

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Tidak ada ketentuan

4.6.5. Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui

Tidak ada ketentuan

4.6.6. Publikasi Sertifikat yang Diperbarui oleh PSrE

Tidak ada ketentuan

4.6.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ada ketentuan

4.7. Re-Key Sertifikat

Pemilik dapat mengulang proses pembuatan Sertifikat dengan melalui verifikasi dan validasi ulang menggunakan verifikasi biometrik.

4.7.1. Kondisi Re-Key Sertifikat

Re-key (penggantian kunci) Sertifikat adalah penerbitan suatu sertifikat baru dengan tanggal kadaluarsa yang baru (field “validTo”) dan pasangan kunci yang baru.

DTA dapat melakukan re-key selama:

a. Sertifikat yang lama akan diganti belum dicabut, terkompromi, atau kedaluwarsa dan sudah masuk masa 1 bulan sebelum habis masa berlakunya (expire); dan
b. Seluruh rincian yang terkait dengan Sertifikat masih akurat dan tidak membutuhkan validasi baru atau tambahan informasi baru.

Apabila Kunci Privat Pemilik atau PSrE Indonesia terkompromi atau Sertifikat kedaluwarsa atau dicabut, maka Pemilik dapat mengajukan permohonan baru sebagaimana diatur pada Bagian 4.1.

4.7.2. Siapa yang Dapat Meminta Sertifikasi dari sebuah Kunci Public Baru

Pemilik Sertifikat dapat melakukan pengajuan Re-Key Sertifikat.

4.7.3. Pemrosesan Permintaan Re-Key Sertifikat

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

4.7.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik

Setelah Re-Key Sertifikat berhasil dilakukan, maka DTA memberitahukan penerbitan Sertifikat telah berhasil dilakukan seperti yang dinyatakan pada Bagian 4.3.2.

4.7.5. Sikap yang Dianggap Sebagai Menerima Sertifikat Re-Key

Pemilik Sertifikat dianggap telah menerima Sertifikat hasil Re-key, sebagaimana dinyatakan pada Bagian 4.4.1.

4.7.6. Publikasi Sertifikat yang di Re-Key oleh PSrE

Sertifikat Re-key dipublikasikan sebagaimana dinyatakan pada Bagian 4.4.2

4.7.7. Pemberitahuan Penerbitan Sertifikat oleh DTA ke Entitas Lain

Tidak ada ketentuan.

4.8. Modifikasi Sertifikat

DTA tidak melakukan Modifikasi detil Sertifikat. Apabila terjadi kesalahan selama penerbitan Sertifikat, maka DTA akan melakukan pencabutan Sertifikat dan menerbitkan Sertifikat baru sesuai dengan ketentuan pada CPS ini.

4.9. Pencabutan dan Pembekuan Sertifikat

4.9.1. Kondisi untuk Pencabutan

DTA akan mencabut Sertifikat Pemilik dengan alasan atau kondisi sebagai berikut:

a. Komponen informasi yang berafiliasi dengan nama dalam Sertifikat menjadi tidak valid;
b. Informasi apapun dalam Sertifikat menjadi tidak valid;
c. Pemilik terbukti melanggar ketentuan dalam kontrak berlangganannya;
d. Ada alasan untuk meyakini bahwa Kunci Privat terkompromi, rusak, dan/atau hilang;
e. Pemilik atau pihak berwenang lainnya (sebagaimana didefinisikan dalam CPS) meminta Sertifikatnya dicabut;
f. Ketika terjadi perubahan standar, kebijakan pemerintah atau ketentuan perundang-undangan yang berlaku yang mempengaruhi keabsahan Sertifikat;
g. DTA berhenti beroperasi.

Informasi pencabutan Sertifkat dimasukkan dalam CRL dan OCSP. Sertifikat yang dicabut disertakan dalam semua publikasi baru tentang informasi status Sertifikat sampai masa berlaku Sertifikat berakhir.

4.9.2. Siapa yang Dapat Meminta Pencabutan

Permintaan penbutan Sertifikat dilakukan oleh:
1. Pemilik, atau
2. Pihak lainnya yang diberikan kewenangan oleh hukum, ketentuan peraturan perundang-undangan, atau perintah pengadilan.

Dalam hal ketentuan yang tercantum pada Bagian 4.9.1 terpenuhi, DTA dapat melakukan pencabutan Sertifikat tanpa permintaan pencabutan dari Pemilik Sertifikat.

4.9.3. Prosedur Permintaan Pencabutan

Pemilik Sertifikat dapat mencabut Sertifikatnya sendiri melalui sistem yang disediakan oleh DTA.

Untuk melakukan pencabutan Sertifikat, Pemilik melewati tahap verifikasi pada saat:

a. Login ke dalam akun Pemilik pada situs DTA;
b. DTA akan memverifikasi identitas biometrik Pemilik sebelum dilakukan pencabutan Sertifikat; dan
c. Memilih alasan pencabutan Sertifikat.

Setelah pencabutan Sertifikat berhasil dilakukan, Pemilik akan menerima surel terkait aktifitas pencabutan Sertifikat.

DTA memverifikasi identitas dan wewenang pihak yang meminta pencabutan Sertifikat. Validasi identitas dan wewenang pihak yang meminta pencabutan dibutuhkan sebagaimana diatur pada Bagian 3.2 dan 3.4.

Permintaan pencabutan Sertifikat oleh Pemilik harus menyerahkan bukti bahwa:
1. Kunci Privat Sertifikat telah terungkap;
2. Penggunaan Sertifikat tidak sesuai dengan CPS, Perjanjian Pemilik Sertifikat/Kontrak Berlangganan dan/atau Perjanjian lainnya;
3. Terdapat alasan relevan lain yang diberikan oleh pemilik.

Permintaan pencabutan oleh pihak yang berwenang harus memiliki bukti bahwa:

1. Kunci privat Sertifikat telah terpapar/terungkap; atau
2. Penggunaan Sertifikat tidak sesuai dengan CPS, Perjanjian Pemilik Sertifikat/Kontrak Berlangganan dan/atau Perjanjian lainnya;
3. Terdapat alasan relevan lain yang diberikan oleh pihak yang berwenang.

4.9.4. Tenggang Waktu Permintaan Pencabutan

Tidak ada tenggang waktu setelah permintaan pencabutan diterima. Pihak sebagaimana diatur pada bagian 4.9.2 harus meminta pencabutan segera setelah teridentifikasi adanya keperluan pencabutan.

4.9.5. Tenggat Waktu Dimana PSrE Harus Memproses Permintaan Pencabutan

Untuk permintaan pencabutan dari aparat penegak hukum, DTA akan mencabut Sertifikat Pemilik dalam waktu paling lambat 1 (satu) jam setelah persyaratan pengajuan pencabutan Sertifikat sebagaimana Bagian 4.9.3 berhasil diverifikasi.

Untuk pencabutan langsung oleh Pemilik Sertifikat melalui *fitur* antarmuka sistem DTA, Sertifikat akan dihapus secara langsung setelah identitas Pemilik terbukti valid dan benar melalui verifikasi biometrik dengan menggunakan *liveness detection*.

4.9.6. Persyaratan Pemeriksaan Pencabutan bagi Pengandal

Pengandal harus memvalidasi setiap Sertifikat terhadap CRL dan/atau OCSP terbaru melalui repository DTA dam melakukan pemeriksaan masa berlaku Sertifikat, Certification Practice Statement, batasan key usage dan status Sertifikat.

4.9.7. Frekuensi Penerbitan CRL

CRL dipublikasikan sesuai ketentuan berikut:

Kondisi	Publikasi CRL
Rutin	• Sertifikat Pemilik maksimal 26 (dua puluh enam) jam • Sertifikat DTA maksimal 6 (enam) bulan
Kunci Privat hilang atau terkompromi	Maksimal 24 (dua puluh empat) jam setelah DTA menerima notifikasi Kunci Privat hilang atau terkompromi
DTA terkompromi atau insiden keamanan lainnya	Sesegera mungkin, tidak lebih dari 24 (dua puluh empat) jam setelah DTA menerima notifikasi kompromi

Dalam hal kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat DTA, CRL terbaru dipublikasikan dalam waktu 24 (dua puluh empat) jam semenjak waktu pencabutan sesuai dengan stempel waktu (*timestamp*).

CRL harus diamankan untuk menjamin integritasnya.

4.9.8. Latensi Maksimum CRL

DTA mempublikasikan CRL paling lama 30 (tiga puluh) menit setelah penerbitan.

4.9.9. Ketersediaan Pemeriksaan Pencabutan/Status Daring

Sertifikat yang dicabut, ditandatangani dan dipublikasikan oleh DTA dapat diverifikasi melalui layanan OCSP yang disediakan oleh DTA.

4.9.10. Persyaratan Pemeriksaan Pencabutan Daring

Tidak ada ketentuan.

4.9.11. Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ada ketentuan.

4.9.12. Persyaratan Khusus terkait Kebocoran Kunci

Jika Sertifikat Pemilik terpapar atau terjadi kebocoran, Sertifikat yang aktif akan dicabut dan langkah selanjutnya mengacu kepada Bagian 4.7.

4.9.13. Kondisi untuk Pembekuan

Pembekuan sertifikat tidak disediakan.

4.9.14. Siapa yang Dapat Meminta Pembekuan

Tidak ada ketentuan.

4.9.15. Prosedur untuk Permintaan Pembekuan

Tidak ada ketentuan.

4.9.16. Pembatasan pada Masa Pembekuan

Tidak ada ketentuan.

4.10. Layanan Status Sertifikat

4.10.1. Karakteristik Operasional

Status Sertifikat tersedia melalui CRL yang terdapat pada repositori dan/atau OCSP.

4.10.2. Ketersediaan Layanan

DTA melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status sertifikat agar tersedia sepanjang waktu, diluar waktu pemeliharaan yang ditentukan oleh DTA.

4.10.3. Fitur Opsional

Tidak ada ketentuan.

4.11. Akhir Berlangganan

Pemilik dapat mengakhiri langganan atau tidak melanjutkan jasa langganan DTA dengan cara mencabut Sertifikat, tidak memperpanjang Sertifikat yang telah kedaluwarsa, atau jasa DTA sudah tidak tersedia lagi.

Akun Pemilik akan tetap aktif walaupun Pemilik tidak memperpanjang Sertifikat yang telah kedaluwarsa.

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 Sesi

Tidak ada ketentuan.

5. KENDALI FASILITAS, MANAJEMEN, DAN OPERASIONAL

5.1. Kendali Fisik

5.1.1. Lokasi dan Konstruksi

Seluruh fasilitas penempatan peralatan DTA yang digunakan untuk mengelola PSrE DTA ditempatkan dalam Data Center (DC) dan Disaster Recovery Center (DRC) yang berada di Indonesia.

Fasilitas layanan DTA dilengkapi dengan mekanisme keamanan untuk menjaga agar non-Trusted Roles tidak dapat memiliki akses ke fasilitas layanan DTA.

Data Center (DC) dan Disaster Recovery Center (DRC) DTA ditempatkan dengan mempertimbangkan availability layanan PSrE DTA.

5.1.2. Akses Fisik

Akses untuk masuk ke Data Center DTA harus didaftarkan lebih dahulu dan melalui penjagaan 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 pengamanan pada media penyimpanan. Hanya pihak-pihak yang termasuk dalam *Trusted Role* yang dapat mengakses masuk ke Data Center.

Peralatan yang digunakan oleh DTA selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik yang dilakukan oleh DTA antara lain:

a. Memastikan tidak ada akses tidak resmi ke perangkat keras.
b. Menyimpan semua *removable media* yang berisi informasi yang sensitif dalam tempat penyimpanan yang aman.
c. Memonitor akses yang tidak berwenang baik secara manual maupun elektronik.
d. Memelihara dan memeriksa log akses secara berkala.
e. Membutuhkan kendali akses fisik dua orang untuk modul kriptografis dan sistem komputer DTA.

Ketika tidak digunakan, modul kriptografis yang *removable* dinonaktifkan sebelum disimpan. Informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografis ditempatkan pada tempat penyimpanan yang aman.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat DTA dilaksanakan sebelum personel DTA meninggalkan fasilitas tersebut. Proses pemeriksaan memastikan hal-hal sebagai berikut:

1. Semua security container (misalnya lemari besi) sudah terkunci;
2. Sistem keamanan fisik (misalnya kunci pintu, pelindung ventilasi) berfungsi dengan baik; dan
3. Area diamankan dari akses yang tidak berhak.

DTA menunjuk personel-personel yang berperan dan bertanggung jawab untuk melakukan pemeriksaan. 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. Daya dan Penyejuk Udara

DTA memiliki daya listrik memadai yang cukup ketika listrik utama mati, menyelesaikan setiap tindakan yang tertunda, dan merekam status perangkat sebelum kekurangan daya atau AC yang menyebabkan shutdown. Fasilitas dilengkapi daya tak terputus dan generator listrik yang cukup untuk beroperasi paling sedikit 6 (enam) jam saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

5.1.4. Keterpaparan Air

Peralatan DTA ditempatkan pada tempat yang tidak terpapar air.

5.1.5. Pencegahan dan Perlindungan dari Kebakaran

Peralatan DTA ditempatkan di fasilitas dengan sistem pendeteksi kebakaran dan sistem pemadaman kebakaran yang memadai.

5.1.6. Penyimpanan Media

Media dari DTA ditempatkan di lokasi terpisah dan disimpan agar terlindungi dari kerusakan yang tidak disengaja (air, api, dan elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau cadangan diduplikasi dan disimpan di lokasi yang terpisah dari layanan DTA.

5.1.7. Pembuangan Limbah

Dokumen yang mengandung informasi sensitif dihancurkan sampai tidak dapat direkonstruksi kembali.

Semua informasi sensitif yang terdapat pada barang yang sudah tidak digunakan dihancurkan sebelum dibuang.

Seluruh perangkat kriptografis yang sudah tidak digunakan dihancurkan fisiknya sampai tidak dapat digunakan kembali sebelum dibuang.

Tata cara pembuangan limbah diatur dalam Prosedur Pemusnahan Media.

5.1.8. Backup Off-Site

DTA melakukan Backup off-site dan hasil backup offsite disimpan di luar lokasi DC dan DRC minimal sekali dalam 1 (satu) bulan. Data Backup off-site DTA dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional DTA.

5.2. Kendali Prosedur

5.2.1. Peran Terpercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

a. Manager Operating PSrE
   Melakukan penetapan terkait kebutuhan bisnis dan kebijakan internal DTA.
b. Policy Authority (PA)
   Menetapkan kebijakan DTA.
c. Policy Authority Officer (PAO)
   Bertanggung jawab atas pembuatan, revisi Dokumen Kebijakan DTA.
d. Application PSrE Administrator
   Melakukan operasional dan pemeliharaan sistem aplikasi PSrE.
e. Application Support
   Bertanggung jawab atas konfigurasi dan pemeliharaan sistem PSrE.
f. Network Administrator
   Bertanggung jawab atas instalasi, konfigurasi dan pemeliharaan sistem operasi dan jaringan.
g. Administrator Operating System
   Melakukan *backup* harian dan memantau kapasitas ketersediaan dan insiden.
h. Cryptographic Materials Custodian
   Bertanggung jawab atas pengelolaan inventaris kunci dan token DTA.
i. Internal Auditor
   Bertanggung jawab atas proses audit internal dan monitoring DTA.
j. IT Developer
   Bertanggung jawab atas pengembangan aplikasi dan sistem DTA.
k. Security Officer
   Bertanggung jawab terhadap aspek keamanan di sistem dan perimeter DTA.

Peran terpercaya lainnya didefinisikan dalam dokumen lain, yang menjelaskan mengenai persyaratan peran-peran tersebut pada operasional DTA.

5.2.2. Jumlah Orang yang Dibutuhkan untuk setiap Tugas

Untuk kegiatan yang memerlukan kendali multi personel, semua pihak yang terlibat memegang Peran Terpercaya. Kendali multi personel tidak melibatkan personel yang bertugas dalam peran Auditor. Tugas berikut yang memerlukan 2 (dua) orang atau lebih:

a. Pembangkitan kunci DTA; dan
b. Pencadangan Kunci Privat DTA.

5.2.3. Identifikasi dan Autentikasi untuk Setiap Peran

Semua individu yang ditugaskan dalam Peran Terpercaya merupakan pegawai DTA yang sudah melalui proses pemeriksaan latar belakang sesuai Bagian 5.3.2. Sebelum menjalankan tugas, Peran Terpercaya diberikan mandat melalui Surat Penugasan.

Autentikasi Peran Terpercaya 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.

5.2.4. Peran yang Membutuhkan Pemisahan Tugas

DTA menerapkan pemisahan tugas berdasarkan perangkat PSrE dan/atau secara prosedural.

Tidak ada satu orang yang merangkap peran pada peran-peran berikut:

a. Policy Authority dan Operational Administrator;
b. Internal audit dan semua peran lain;
c. Pengembang aplikasi dan semua peran lain.

Ketentuan mengenai pemisahan tugas Peran Terpercaya lebih lanjut diatur dalam Asset Register Personil (Daftar Peran Terpercaya).

5.3. Kendali Personel

5.3.1. Persyaratan Kualifikasi, Pengalaman, dan Penugasan

Semua personel DTA warga negara Indonesia dan telah dipilih atas dasar keterampilan, pengalaman, terpercaya, dan integritas sesuai dengan persyaratan sebagai berikut:

a. Bukti latar belakang yang diperlukan, kualifikasi yang diperoleh melalui pendidikan, pelatihan formal dan pengalaman yang diperlukan untuk secara efisien dan memadai dalam melaksanakan tanggung jawab pekerjaan mereka; dan
b. Bukti catatan kriminal yang bersih yang dibuktikan dengan SKCK.

5.3.2. Prosedur Pemeriksaan Latar Belakang

Semua personel di DTA lulus pemeriksaan latar belakang. Ruang lingkup pemeriksaan latar belakang mencakup area berikut yang mencakup paling tidak dalam dua (2) tahun terakhir:

a. Pendidikan atau sertifikasi;
b. Identifikasi kependudukan (KTP);
c. Surat Keterangan Catatan Kepolisian;
d. Pengalaman / Referensi kerja;
e. Informasi finansial dari sistem pengecekan finansial yang dikeluarkan oleh otoritas yang berwenang.

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

5.3.3. Persyaratan Pelatihan

Semua personel DTA diberikan pelatihan yang sesuai untuk menjalankan tugasnya. Pelatihan tersebut paling sedikit mencakup topik-topik sebagai berikut:

1. Mekanisme dan prinsip keamanan operasional DTA;
2. Seluruh versi perangkat lunak, perangkat keras, dan sistem operasi dalam lingkup IKP yang digunakan dalam sistem DTA;
3. Seluruh kewajiban masing-masing personel terkait operasional DTA;
4. Prosedur pemulihan bencana dan keberlangsungan bisnis; dan
5. CPS DTA yang berlaku.

DTA menyimpan catatan pelatihan semua personel DTA. Evaluasi terhadap kecukupan kompetensi personel DTA dilakukan minimal 1 (satu) kali dalam setahun.

5.3.4. Frekuensi dan Persyaratan Pelatihan Ulang

DTA memberikan pelatihan ulang yang sifatnya memberi penyegaran dan memutakhiran kemampuan para personelnya dan sosialisasi awareness keamanan informasi, dengan frekuensi 2 (dua) kali setahun atau lebih jika dibutuhkan. Hal ini dilakukan untuk memastikan bahwa personel DTA mempertahankan kompetensi yang dipersyaratkan untuk melakukan tugas dan tanggung jawab pekerjaan secara memuaskan.

5.3.5. Frekuensi dan Urutan Rotasi Pekerjaan

DTA memastikan bahwa perubahan pegawai tidak memengaruhi efektivitas operasional layanan atau keamanan sistem.

5.3.6. Sanksi untuk Tindakan yang Tidak Terotorisasi

Sanksi disiplin diberlakukan kepada personel yang melanggar ketentuan dan kebijakan dalam CPS atau prosedur operasional DTA.

5.3.7. Persyaratan Kontraktor Independen

Pegawai kontrak yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional DTA memenuhi persyaratan yang berlaku yang ditetapkan dalam Bagian 5.3.1, Bagian 5.3.2 dan Bagian 5.3.3 di atas.

5.3.8. Dokumentasi yang Diberikan kepada Personil

DTA menyediakan sejumlah dokumen kepada para personelnya. Dokumen tersebut antara lain CPS, peraturan, kebijakan, dan kontrak yang relevan. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) juga disediakan agar personel Peran Terpercaya dapat menjalankan tugasnya.

DTA menyediakan repository internal yang memuat seluruh dokumen yang diperlukan oleh para personel untuk menunjang tugas dan kewajibannya.

5.4. Prosedur Log Audit

Berkas log audit dibuat untuk semua kejadian yang terkait dengan keamanan sistem DTA. Log audit keamanan dikumpulkan secara otomatis dan manual. Log yang dikumpulkan dengan cara manual dilakukan dengan menggunakan buku log, kertas formulir, atau mekanisme fisik lain. Semua log audit keamanan, baik elektronik dan non elektronik, dijaga dan tersedia untuk audit. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai dengan Bagian 5.5.2.

5.4.1. Jenis Kejadian yang Direkam

DTA mengaktifkan fitur audit keamanan dari sistem operasi serta aplikasi DTA yang dipersyaratkan oleh CPS ini. DTA memastikan bahwa seluruh kejadian yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan Peran Terpercaya dalam operasional DTA dapat dilacak.

Setiap rekaman kejadian yang diperlukan untuk audit, minimal memuat poin-poin sebagai berikut:

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

Waktu disinkronkan dengan otoritas sumber waktu dengan ketelitian paling lama 1 (satu) menit. Kejadian penghancuran Kunci Privat DTA diatur dalam Bagian 6.2.10.

5.4.2. Frekuensi Pemrosesan Log

Log audit ditinjau minimal sekali dalam sebulan. Peninjauan tersebut termasuk melakukan verifikasi bahwa log tersebut tidak dirusak, tidak ada diskontinuitas data, dan tidak adanya jenis kehilangan lain terhadap data audit. Pemeriksaan dilanjutkan dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan yang muncul dalam log.

Tindakan yang diambil sebagai hasil dari peninjauan ini didokumentasikan.

5.4.3. Periode Retensi Log Audit

Log audit DTA disimpan selama 1 (satu) tahun agar tersedia untuk pengendalian yang sah. Jangka waktu ini dapat berubah sewaktu-waktu sesuai dengan hukum yang berlaku.

5.4.4. Proteksi Log Audit

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

Setelah audit log di-backup, sistem menimpa (overwrite) log audit tersebut dengan log audit yang baru.

5.4.5. Prosedur Backup Log Audit

Log audit DTA di-backup sebulan sekali. Salinan dari log audit disimpan secara lokal dalam suatu lokasi terpisah yang aman setiap bulan.

5.4.6. Sistem Pengumpulan Audit (Internal vs Eksternal)

DTA mengumpulkan log audit termaksud namun tidak terbatas pada log berikut ini:

a. Aplikasi;
b. Database;
c. OS;
d. Jaringan;
e. Firewall;
f. *Fingerprint;*
g. CCTV;
h. IDS -IPS;
i. Akses Penyedia Pusat Data;
j. Akses brankas;
k. Ruang khusus;
l. Buku tamu; dan
m. Media penyimpanan (SAN Storage, NAS).

5.4.7. Pemberitahuan ke Subyek Penyebab Kejadian

Tidak ada ketentuan.

5.4.8. Asesmen Kerentanan

DTA melaksanakan asesmen kerentanan sistem atau komponennya setiap 1 (satu) minggu sekali atau ketika terjadi perubahan signifikan pada sistem DTA. Dalam hal terdapat temuan pada saat asesmen kerentanan, DTA memperbaiki temuan tersebut.

DTA melakukan uji penetrasi ke sistem dilakukan minimal 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem DTA. Dilakukan oleh pihak independen dan didokumentasikan.

5.5. Pengarsipan Record

5.5.1. Tipe Record yang Diarsipkan

Catatan DTA yang disimpan dalam arsip untuk mementukan kesesuaian operasional DTA dan validitas Sertifikat yang dikeluarkan oleh DTA, termasuk pada Sertifikat pemilik yang telah dicabut

atau yang telah melewati batas jangka waktu Sertfikat. Data yang diarsipkan adalah sebagai berikut:

1. Siklus hidup operasi Sertifikat termasuk permohonan Sertifikat, penolakan permohonan Sertifikat, dan permintaan pencabutan Sertifikat;
2. Semua Sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh DTA;
3. Log Audit;
4. Konfigurasi sistem PKI;
5. Dokumen yang tersedia di Repositori termasuk amandemen dan perubahannya; dan
6. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI):
    a. Penunjukan dan pencabutan peran dan kewenangan;
    b. Akses pengunjung ke fasilitas PSrE;
    c. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
    d. Deteksi dan tindakan terhadap insiden keamanan;
    e. Latihan keadaan darurat;
    f. Tindakan dan penilaian risiko;
    g. Perubahan aset, prosedur dan tanggung jawab; dan
    h. Perubahan dokumentasi.

5.5.2. Periode Retensi Arsip

Arsip disimpan selama 5 tahun. Khusus Sertifikat DTA yang sudah habis masa berlakunya, diarsipkan secara permanen. Perangkat lunak dan perangkat keras yang dibutuhkan untuk membaca arsip ini dipelihara selama masa retensi.

5.5.3. Perlindungan Arsip

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

Muatan arsip tidak diungkap kecuali berdasarkan ketentuan pada Bagian 9.3 dan 9.4.

5.5.4. Prosedur Backup Arsip

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

Record backup arsip yang dikelola DTA disamakan dengan arsip seperti Bagian 5.5.1.

5.5.5. Persyaratan Pemberian Penanda Waktu pada Rekaman Arsip

Rekaman arsip DTA memiliki stempel waktu (*timestamp*).

5.5.6. Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip di DTA dilakukan oleh internal DTA

5.5.7. Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip

Media penyimpanan informasi arsip DTA diperiksa setelah dibuat. Setiap 6 (enam) bulan, sampel dari informasi arsip diuji untuk memeriksa integritas dan keterbacaan informasi. Hanya DTA, Peran Terpercaya (*trusted roles*) dan pihak-pihak lain yang berwenang yang diizinkan yang dapat

mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh Peran Terpercaya.

5.6. Pergantian Kunci

Kunci Privat DTA diubah secara berkala setiap 10 (sepuluh) tahun untuk meminimalisir risiko kebocoran. Setelah Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat.

Sertifikat yang lama, namun masih berlaku, akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat pada sertifikat lama tersebut kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka Kunci Privat lama tetap disimpan dan dilindungi sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat lama habis masa berlakunya.

Tabel penjelasan Kunci DTA dan masa berlakunya dijelaskan pada bagian 6.3.2.

Ketika DTA memperbarui Kunci Privat dan dengan demikian menghasilkan Kunci Publik baru, DTA memberitahu semua Pemilik yang mengandalkan Sertifikat DTA tersebut bahwa telah terjadi perubahan.

Pasangan kunci DTA akan diperbarui paling lambat pada saat Sertifikat DTA kedaluwarsa dikurangi masa berlaku Sertifikat Pemilik.

5.7. Pemulihan Bencana dan Keadaan Terkompromi

5.7.1. Prosedur Penanganan Insiden dan Keadaan Terkompromi

DTA memiliki rencana penanganan insiden (*Business Continuity Plan*) dan rencana pemulihan bencana (*Disaster Recovery Plan*).

DTA menangani bencana dan insiden *compromise* sesuai dengan prosedur penanganan bencana untuk meminimalkan dampak dari peristiwa seperti itu. Jika Kunci Privat DTA dicurigai telah terkompromi, penerbitan Sertifikat oleh DTA segera dihentikan. Investigasi independent oleh pihak ketiga dilakukan untuk menentukan sifat dan tingkat kerusakan. Cakupan potensi kerusakan diperiksa untuk menentukan prosedur perbaikan yang tepat.

Jika Kunci Privat DTA dicurigai sudah terkompromi, ketentuan sebagaimana diatur pada Bagian 5.7.3 diikuti.

DTA menginformasikan PSrE Induk apabila mengalami insiden, termasuk namun tidak terbatas pada:

1. Terdeteksinya atau adanya indikasi sistem DTA terkompromi;
2. Adanya upaya untuk menembus sistem DTA, baik secara fisik maupun elektronik;
3. Serangan *Denial of Service* pada sistem DTA;
4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam *field* “next update” pada CRL DTA. DTA segera memulihkan penerbitan CRL secepat mungkin; dan/atau
5. CRL dan/atau OCSP responder tidak dapat diakses oleh publik.

Prosedur DTA direviu 1 (satu) tahun sekali, perubahan dilakukan berdasarkan hasil reviu tersebut atau jika diperlukan perubahan.

Semua sistem pencadangan/pemulihan diuji minimal setahun sekali.

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

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

1. Memberitahu PSrE Induk sesegera mungkin sesuai dengan prosedur penanganan insiden;
2. Jika Kunci Privat masih tetap berfungsi dan tidak mengalami kerusakan, maka:
   a. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup;
   b. Mengoperasikan kembali sistem DTA, dengan memprioritaskan kemampuan untuk membangkitkan informasi status sertifikat sesuai jadwal penerbitan CRL;
      - Jika kemampuan untuk membangkitkan informasi status sertifikat tidak beroperasi atau rusak, DTA memulihkan kemampuan untuk membangkitkan informasi status sertifikat sesegera mungkin sesuai dengan prosedur yang ditetapkan dalam CPS DTA. Jika kemampuan DTA untuk membangkitkan informasi status sertifikat tidak bisa dipulihkan dalam jangka waktu yang wajar, DTA menentukan apakah perlu untuk meminta pencabutan Sertifikat miliknya kepada PSrE Induk.
3. Bila kunci penandatanganan DTA rusak, operasional DTA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan Pasangan Kunci DTA yang baru. DTA membangkitkan Kunci tersebut sesuai dengan prosedur yang sudah ditetapkan dalam CPS.

Jika DC dan DRC tidak dapat memulihkan kemampuan pencabutan Sertifikat dalam jangka waktu yang wajar, maka sistem DTA akan diperlakukan sebagai PSrE terkompromi.

5.7.3. Prosedur Kunci Privat EntitasTerkompromi

Dalam kasus kehilangan Kunci Privat atau terjadi kebocoran/kompromi terhadap parameter yang digunakan untuk membangkitkan Kunci Privat dan Sertifikat, semua Sertifikat yang terkait dicabut oleh DTA dan semua kunci serta Sertifikat baru diterbitkan tanpa menghentikan layanan.

Jika Kunci Privat dari DTA terkompromi, hilang, atau terindikasi terkompromi, maka DTA:
1. Memberitahu Menteri (PSrE Induk) segera mungkin agar dapat melakukan pencabutan Sertifkat;
2. Memberitahu semua Pemilik Sertifikat dari DTA; dan
3. Mencabut Sertifikat Pemilik yang terkompromi tersebut.

DTA meminta penerbitan Sertifikat baru ke PSrE Induk sesuai dengan proses registrasi awal.

DTA membangkitkan Pasangan Kunci baru sesuai dengan prosedur yang ditetapkan dalam CPS.

Penerbitan ulang Kunci Privat Pemilik akibat terkompromi dilakukan Pemilik dengan mengajukan permohonan Sertifikat sebagaimana diatur pada Bagian 4.1.

DTA menyelidiki penyebab kompromi atau kerugian dan tindakan yang harus diambil untuk mencegah kompromi tersebut terulang kembali.

5.7.4. Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana

DTA memiliki rencana keberlangsungan bisnis dan rencana pemulihan bencana yang telah diuji, ditinjau ulang, dan diperbaiki secara berkala. Layanan kembali pulih dalam kurun waktu 24 (dua puluh empat) jam bila ada bencana.

Rencana pemulihan bencana DTA ditinjau ulang dan diuji secara berkala (minimal 1 tahun sekali) dan diperbaharui jika dibutuhkan. Fasilitas *Disaster Recovery Center* DTA tersedia bila fasilitas utama berhenti beroperasi.

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan DTA rusak secara fisik dan semua salinan Kunci penandatangan milik DTA hancur, DTA meminta kepada PSrE Induk agar Sertifikatnya dicabut. DTA mengikuti ketentuan sebagaimana diatur pada Bagian 5.7.3.

5.8. Penutupan PSrE atau RA

Dalam hal DTA menghentikan penyelenggaraan layanannya, DTA akan mengirimkan pemberitahuan melalui surat elektronik kepada para pihak yang terlibat dalam siklus operasional Sertifikat, termasuk kepada PSrE Induk, Pemilik Sertifikat, dan Pengandal.

DTA memiliki prosedur penutupan PSrE memuat hal-hal berikut:

1. Memberitahu Menteri (PSrE Induk) segera mungkin agar dapat melakukan pencabutan Sertifkat;
2. Memberitahu status layanan DTA ke pengguna yang terkena dampak;
3. Menyimpan rekaman arsip DTA dalam jangka panjang mengikuti periode pengarsipan;
4. Mencabut Sertifikat DTA dan Sertifikat Pemilik
5. Menyediakan informasi status Sertifikat agar tetap dapat diakses sampai masa berlaku Sertifikat Pemilik kedaluwarsa; dan
6. Menghancurkan sistem PKI DTA yang berisi Kunci Privat DTA dan Pemilik.

DTA memberikan kompensasi sebagaimana diatur dalam Kebijakan Jaminan.

6. KENDALI KEAMANAN TEKNIS

6.1. Pembangkitan dan Instalasi Pasangan Kunci

6.1.1. Pembangkitan Pasangan Kunci

Tabel berikut berisi persyaratan pembangkitan Pasangan Kunci.

Entitas	FIPS 140-2 Level	Perangkat Keras atau Perangkat Lunak	Dibangkitkan di dalam Modul Entitas
DTA	3	Perangkat Keras	Ya
Time Stamp Authority	3	Perangkat Keras	Ya
OCSP Responder	3	Perangkat Keras	Ya
Pemilik untuk TTE	3	Perangkat Keras	Ya

Kendali multi-pihak dibutuhkan untuk pembangkitan pasangan kunci DTA seperti yang ditentukan pada Bagian 6.2.2.

Pembangkitan Pasangan Kunci DTA menghasilkan jejak audit yang dapat diverifikasi yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. Dokumentasi prosedur cukup rinci untuk menunjukkan bahwa pemisahan peran yang tepat telah dilakukan. Pihak ketiga yang independen 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 ke Pemilik

DTA membangkitkan sendiri Pasangan Kunci milik DTA sehingga tidak memerlukan pengiriman Kunci Privat.

DTA membangkitkan pasangan kunci atas nama Pemilik, namun DTA tidak memberikan Kunci Privat kepada Pemilik sehingga tidak ada pengiriman Kunci Privat ke Pemilik. Kunci Privat Pemilik hanya disimpan di DTA.

6.1.3. Pengiriman Kunci Publik ke Penerbit Sertifikat

DTA tidak mengirimkan Kunci Publik. Pemilik dapat mengunduh Kunci Publik dan Sertifikat melalui antarmuka Sistem DTA di https://my.xignature.co.id/.

6.1.4. Pengiriman Kunci Publik PSrE kepada Pengandal

Pengandal dapat mengunduh Kunci Publik DTA melalui repositori DTA sebagaimana tercantum pada Bagian 2.2.

Pada jangka waktu tertentu sebelum kunci publik DTA kadaluwarsa, suatu pasangan kunci penandatanganan sertifikat yang baru akan dibangkitkan supaya DTA tetap bisa beroperasi secara normal. Kunci Publik DTA berlaku selama 10 tahun.

6.1.5. Ukuran Kunci

DTA membuat Pasangan Kunci dengan menggunakan algoritma RSA dengan panjang kunci 2048 bit untuk kunci Pemilik dan 4096 bit untuk kunci DTA. DTA menggunakan HASH SHA 256.

6.1.6. Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik

DTA membangkitkan dan memvalidasi Kunci Publik dengan parameter sesuai FIPS 186-4.

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

Kunci DTA digunakan untuk penandatangan Sertifikat dan CRL. Penggunaan sebuah kunci spesifik ditentukan oleh key usage extension dalam sertifikat X.509. Kunci pemilik digunakan untuk digital signing dan non repudiation.

6.2. Kendali Kunci Privat dan Kendali Teknis Modul Kriptografis

6.2.1. Kendali dan Standar Modul Kriptografi

DTA menggunakan perangkat FIPS 140-2 level 3 untuk sistem penandatanganan Sertifikat dan CRL. Untuk pembangkitan dan penandatanganan, Kunci Privat Pemilik Sertifikat menggunakan perangkat modul kriptografi yang memenuhi standar FIPS 140-2 level 3.

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

Semua Kunci Privat DTA diakses melalui kendali multi-personel seperti yang ditentukan pada Bagian 5.2.2.

Modul kriptografi yang memuat seluruh Kunci penandatanganan DTA diaktivasi atau diakses lebih dari 1 (satu) orang. Kunci penandatanganan DTA di-backup melalui kendali multipersonel. Akses ke Kunci penandatanganan DTA yang di-backup untuk pemulihan bencana dilakukan melalui kendali multipersonel. Nama-nama pihak yang terlibat dalam kendali multi personel dicatat dalam sebuah daftar yang tersedia untuk pemeriksaan Audit.

6.2.3. Eskro Kunci Privat

Kunci Privat DTA tidak dititipkan. Kunci Privat Pemilik disimpan dan diamankan di sistem DTA.

Kunci Pemilik yang dapat dieskro hanya digunakan untuk dekripsi, pengamanan Kunci yang dieskro diperlakukan setara seperti ketika kunci dibangkitakan.

6.2.4. Cadangan (*Backup*) Kunci Privat

Kunci Privat DTA di-backup, dilindungi dan disimpan secara aman dengan kendali multi personal yang sama dengan Kunci Privat Utama.
Satu salinan Kunci Privat disimpan dalam lokasi fisik yang berbeda dari pusat data.

Kunci Privat Pemilik disimpan dan di-backup secara aman, *Backup* pasangan Kunci Pemilik disimpan di *Disaster Recovery Center* (DRC). Pemilik telah menyetujui untuk dilakukan backup pasangan kunci pemilik pada dokumen Kebijakan Privasi.

Semua backup Kunci Publik Pemilik dicatat dan dilindungi dengan cara yang sama dengan pada saat Kunci Publik dibangkitkan.

6.2.5. Pengarsipan Kunci Privat

Kunci Privat DTA dan Kunci Privat Pemilik tidak diarsipkan.

6.2.6. Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci Privat DTA dibangkitkan, diaktifkan dan disimpan dalam modul kriptografi. Ketika Kunci Privat DTA berada diluar modul kriptografis (baik untuk keperluan penyimpanan maupun pemindahan), Kunci Privat dalam bentuk terenkripsi. Kunci Privat DTA tidak pernah sekalipun berada dalam bentuk plaintext di luar modul kriptografis. Kunci Privat DTA di-backup sesuai dengan ketentuan pada Bagian 6.2.4.

Ketika DTA mengetahui bahwa Kunci Privat Pemilik telah disampaikan kepada orang atau entitas yang tidak berwenang dan berafiliasi dengan Subscriber tersebut, maka DTA mencabut semua Sertifikat yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.

6.2.7. Penyimpanan Kunci Privat pada Modul Kriptografis

DTA menyimpan Kunci Privatnya dalam perangkat FIPS 140-2 level 3, dalam bentuk terenkripsi dan terlindungi oleh mekanisme *key-shared* dan kata sandi.

Kunci Privat Pemilik sama proteksinya dengan Kunci Privat DTA disimpan dalam perangkat FIPS-2 level 3, karena dibangkitkan dari perangkat yang sama dengan Kunci Privat DTA.

6.2.8. Metode Pengaktifan Kunci Privat

Pengaktifan Kunci Privat DTA dilakukan oleh personel yang berwenang dan memerlukan kendali multipersonel sebagaimana diatur pada Bagian 5.2.2.

DTA bertanggung jawab untuk mengaktifkan Kunci Privat sesuai dengan petunjuk dan dokumentasi yang disediakan oleh penyedia modul kriptografis.

Pengaktifan dan akses Kunci Privat Pemilik dilindungi dengan mekanisme password. Pemilik Sertifikat bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemilik Sertifikat.

6.2.9. Metode Penonaktifan Kunci Privat

Modul kriptografis yang sudah diaktivasi tidak ditinggalkan tanpa pengawasan atau dapat diakses secara tidak sah. Penonaktifan operasi Kunci Privat DTA dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak seperti yang dinyatakan dalam Pasal 5.2.2.

DTA tidak menyerahkan Kunci Privat kepada Pemilik Sertifikat.

Ketika DTA tidak lagi beroperasi Kunci Privat DTA dihapus dari modul kriptografis.

6.2.10. Metode Penghancuran Kunci Privat

Kunci Privat DTA dihancurkan oleh para individu dalam Peran Terpercaya ketika Kunci Privat tidak diperlukan lagi atau ketika Sertifikat yang terkait dengan Kunci Privat tersebut telah dicabut atau kadaluwarsa. Penghancuran Kunci Privat dan salinannya dilakukan dengan menimpa (overwrite) Kunci Privat atau menginisialisasi modul dengan fungsi factory reset dari modul kriptografis sehingga tidak ada lagi informasi yang digunakan untuk memulihkan Kunci Privat. Jika fungsi-fungsi atau perintah dalam modul kriptografis tidak dapat diakses untuk menghancurkan kunci yang ada di dalam modul kriptografis tersebut, maka modul kriptografis tersebut harus dihancurkan secara fisik. Proses penghancuran dilakukan pada lingkungan fisik yang aman.

DTA mengatur prosedur penghancuran Kunci Privat Pemilik.

6.2.11. Pemeringkatan Modul Kriptografis

Sesuai dengan ketentuan yang diatur 6.2.1.

6.3. Aspek Lain dari Manajemen Pasangan Kunci

6.3.1. Pengarsipan Kunci Publik

Semua Kunci Publik yang digunakan untuk tujuan verifikasi diarsipkan permanen sebagai satu kesatuan dari Sertifikat yang diterbitkan. Rincian tentang pengarsipan diatur pada Bagian 5.5.

Sertifikat DTA yang sudah habis masa berlakunya diarsipkan secara permanen.

6.3.2. Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci

Tabel berikut berisi umur Sertifikat dan Kunci Privat DTA:

Kunci	Algoritma					
	2048 Bit Keys (RSA)		Prime256v1 (ECC)		4096 (RSA)	
	Kunci Privat	Sertifikat	Kunci Privat	Sertifikat	Kunci Privat	Sertifikat
DTA	n/a	n/a	n/a	n/a	10 tahun / 10 years	10 tahun / 10 years
Time Stamp Authority	3 tahun / 3 years	3 tahun / 3 years	n/a	n/a	n/a	n/a
OCSP Responder	3 tahun / 3 years	3 tahun / 3 years	n/a	n/a	n/a	n/a
Pemilik untuk TTE	1 tahun / 1 years	1 tahun / 1 years	n/a	n/a	n/a	n/a
Pemilik untuk Enkripsi	n/a	n/a	n/a	n/a	n/a	n/a

6.4. Data Aktivasi

6.4.1. Pembangkitan dan Instalasi Data Aktivasi

Pembangkitan dan penggunaan data pengaktifan untuk mengaktifkan Kunci Privat DTA dilakukan melalui upacara kunci (merujuk pada Bagian 6.1.1).
Data aktivasi untuk mengaktifkan Kunci Privat dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan.

Penggunaan data aktivasi Kunci Privat Pemilik dimasukkan oleh Pemilik saat aktivasi.

6.4.2. Perlindungan Data Aktivasi

Data aktivasi Kunci Privat DTA dilindungi dari pengungkapan kerahasiaan melalui kombinasi antara kriptografi dan mekanisme kendali akses fisik. Data aktivasi Kunci Privat DTA disimpan dalam token fisik.

Token fisik diakses menggunakan kata sandi tertulis. Tulisan tersebut diamankan pada tingkat yang setara dengan pengamanan modul kriptografis dan tidak disimpan bersama dengan modul kriptografis.

Setelah mengalami kegagalan login sebanyak jumlah yang ditentukan, disediakan kemampuan untuk mengunci sementara akun tersebut.

Pemilik Sertifikat diwajibkan selalu menjaga kerahasiaan data aktivasi.

6.4.3. Aspek Lain mengenai Data Aktivasi

Tidak ada ketentuan.

6.5. Kendali Keamanan Komputer

6.5.1. Persyaratan Teknis Keamanan Komputer Spesifik

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

a. Mewajibkan login terautentikasi bagi Peran Terpercaya;
b. Menyediakan kendali akses dengan kewenangan yang minimal;
c. Menyediakan kapabilitas audit keamanan (dilindungi integritasnya);
d. Memerlukan penggunaan 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. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
j. Mewajibkan pemeriksaan mandiri (self-test) terhadap layanan-layanan DTA.

DTA membatasi jumlah aplikasi yang diinstal pada tiap perangkat untuk mengurangi risiko keamanan. Aplikasi tersebut ditingkatkan keamanannya berdasarkan instruksi yang disediakan

oleh penyedia aplikasi. Selain itu, pemutakhiran keamanan aplikasi tersebut direviu secara rutin untuk memastikan agar tidak ada kerentanan yang terekspos.

Efektivitas kendali keamanan komputer dianalisis melalui penilaian risiko yang dilaksanakan oleh DTA dalam konteks sertifikasi ISO 27001, dan kendali keamanan diaudit setiap 3 (tiga) bulan (lihat Bagian 6.6.2).

6.5.2. Peringkat Keamanan Komputer

Tidak ada ketentuan.

6.6. Kendali Teknis Siklus Hidup

6.6.1. Kendali Pengembangan Sistem

Kendali pengembangan sistem DTA adalah sebagai berikut:

1. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;
2. Pengadaan perangkat keras dan perangkat lunak dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen-komponen yang terdapat dalam perangkat lunak dirusak;
3. Pengembangan perangkat keras dan perangkat lunak dilakukan dalam sebuah lingkungan yang terkendali, dan proses pengembangan didefinisikan dan didokumentasikan. Syarat ini tidak berlaku bagi perangkat lunak maupun perangkat keras komersil siap-pakai yang dibeli;
4. Perangkat keras dan perangkat lunak didedikasikan untuk melaksanakan aktivitas IKP. Tidak ada aplikasi lain, perangkat lunak, koneksi jaringan, atau komponen perangkat lunak yang diinstall yang bukan bagian dari operasional IKP;
5. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya dimuat ke perangkat. Perangkat keras dan perangkat lunak DTA selalu di-scan untuk kode-kode berbahaya pada penggunaan pertama dan secara periodik; 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.

Perangkat lunak siap pakai maupun perangkat lunak yang dikembangkan sendiri oleh DTA yang digunakan untuk manajemen Sertifikat, sepenuhnya diuji di lingkungan non-produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem atau komponennya melalui proses reviu Kontrol Manajemen Perubahan dan persetujuan.

6.6.2. Kendali Manajemen Keamanan

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

Metodologi manajemen konfigurasi resmi digunakan untuk instalasi dan pemeliharaan sistem DTA. Perangkat lunak DTA, ketika dimuat pertama kali, diverifikasi bahwa perangkat lunak tersebut benar berasal dari penyedia, tanpa modifikasi, dan benar merupakan versi yang ingin digunakan.

DTA memiliki prosedur dan jadwal untuk memantau dan mengontrol sistem, serta memelihara prosedur dan jadwal tersebut. Personel DTA bertanggung jawab melakukan pemeriksaan dan pemantauan sistem secara rutin. Sebagai tambahan untuk pemantauan secara manual, proses otomatis dapat diimplementasikan untuk memberikan informasi kepada Peran Terpercaya yang

bersangkutan ketika terjadi aktivitas yang tidak wajar pada sistem. Perubahan sistem diproses melalui kontrol manajemen keamanan.

6.6.3. Kendali Keamanan Siklus Hidup

DTA melakukan pengawasan dan pemeliharaan untuk mempertahankan tingkat kepercayaan dan keamanan komponen perangkat keras dan perangkat lunak dan secara berkala mengevaluasi keefektifannya melalui audit.

6.7. Kendali Keamanan Jaringan

DTA menerapkan konfigurasi keamanan jaringan yang sesuai untuk memastikan bahwa sistem terlindungi dari serangan seperti namun tidak terbatas pada *denial of service* (*DoS*) dan serangan intrusi. Pengamanan yang dilakukan termasuk penggunaan *firewall,* pembatasan port jaringan dan pembatasan akses server.

6.8. Tanda Waktu

Semua komponen DTA secara berkala disinkronisasikan dengan layanan *Network Time Protocol* (NTP). Waktu yang didapat dari layanan waktu di atas digunakan untuk menentukan waktu pada saat:

a. Validitas waktu permulaan untuk penerbitan Sertifikat DTA;
b. Pencabutan Sertifikat DTA;
c. OCSP;
d. Pembaruan CRL; dan
e. Penerbitan Sertifikat Pemilik.

DTA mensinkronisasi waktu dengan: time.nist.gov, pool.ntp.org dan BMKG.

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

7. PROFIL OCSP, CRL, DAN SERTIFIKAT

7.1. Profil Sertifikat

Profil Sertifikat mengikuti standar RFC 5280 "Internet X.509 *Public Key Infrastructure*: *Certificate and Certificate Revocation List* (CRL) *Profile*". DTA melakukan review terhadap profil Sertifikat secara berkala minimal satu tahun sekali.

Profil Sertifikat DTA mematuhi Standar Interoperabilitas PSrE Indonesia.

Profil Sertifikat untuk masing-masing klasifikasi Sertifikat yang diterbitkanlan oleh DTA terdapat dalam lampiran 1.

7.2. Profil CRL

Profil CRL DTA mematuhi Standar Interoperabilitas PSrE Indonesia.

DTA menggunakan CRL dan CRL entry extension sesuai RFC 5280.

7.3. Profil OCSP

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

8. AUDIT KEPATUHAN DAN PENILAIAN KELAIKAN LAINNYA

DTA tunduk pada Peraturan Menteri Komunikasi dan Informatika tentang Penyelenggaraan Sertifikasi Elektronik. DTA akan diaudit secara berkala oleh Kemenkominfo / auditor yang ditunjuk oleh Kemenkominfo. Laporan akan diserahkan secara berkala ke Kemenkominfo.

DTA telah memenuhi audit untuk memastikan semua persyaratan pada CPS ini telah diimplementasikan dan diaudit berdasarkan standar ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi.

8.1. Frekuensi atau Lingkup Penilaian

DTA menjalani audit kepatuhan berkala dalam jangka waktu minimal 1 tahun sekali.

8.2. Identitas/Kualifikasi Penilai

Penilai kelaikan DTA dilaksanakan oleh auditor kepatuhan yang kompeten. Penilai memiliki kompetensi pada bidang Penilaian Kelaikan dan benan-benar memahami persyaratan CPS ini. Penilai melakukan Penilaian Kelaikan sebagai tanggung jawab utama.

Auditor kepatuhan memiliki kualifikasi sebagai berikut:

1. Tidak memiliki konflik kepentingan terhadap DTA;
2. 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, 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;
3. Memiliki kecakapan dalam memeriksa teknologi IKP, peralatan dan teknik keamanan informasi, audit keamanan informasi, dan penilaian pihak ketiga (third-party attestation function);
4. Memiliki sertifikasi sebagai auditor sistem informasi (CISA) atau IT Security specialist, IKP spesialis, yang dapat memberikan masukan terkait acceptable risks, strategi mitigasi, dan best practice industri;
5. Menguasai beberapa keahlian tertentu, pengujian kompetensi, dan jaminan kualitas seperti penelaahan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional; dan
6. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

8.3. Hubungan Penilai dengan Entitas yang Dinilai

Penilaian Kelaikan independen dari DTA sehingga memberikan evaluasi independen yang tidak memihak. Untuk memastikan indepedendsi dan objektivitas, DTA tidak meminta Penilai membantu dalam mengembangkan atau memelihara fasilitas dan/atau CPS. DTA memastikan Penilai memenuhi persyaratan ini.

Selain larangan konflik kepentingan di atas, dalam melaksanakan audit, Penilai memiliki hubungan kontrak yang jelas dengan DTA untuk menjaga independensi / ketidakberpihakan para Penilai. Penilai melaksanakan audit dengan mempertahankan standar etika yang tinggi yang dirancang

untuk memastikan ketidakberpihakan dan pelaksanaan penilaian profesional yang independen dengan tunduk pada ketentuan peraturan perundang-undangan.

8.4. Topik Penilaian

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa DTA beroperasi sesuai dengan CP PSrE Induk. Penilaian Kelaikan mencakup penilaian CPS DTA yang berlaku terhadap CP PSrE Induk,untuk menentukan bahwa CPS DTA telah diimplementasikan dan ditegakkan. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen DTA.

Audit dilaksanakan untuk memenuhi persyaratan dari skema audit yang digunakan dalam penilaian.

8.5. Tindakan yang Diambil Akibat Ketidaksesuaian

Ketika Auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana DTA dirancang atau dioperasikan atau dipelihara terhadap persyaratan CP PSrE Induk dan CPS PSrE DTA yang berlaku, tindakan berikut dilakukan:

a. Mencatat ketidaksesuaian yang ditemukan;
b. Auditor kepatuhan memberitahu PA PSrE DTA dan PSrE Induk tentang ketidaksesuaian;
c. Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CPS dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan tersebut tanpa penundaan.

8.6. Laporan Hasil Penilaian

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

8.7. Audit Internal

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

Audit internal dilaksanakan minimal setahun sekali.

Audit internal juga memeriksa kesesuaian dengan ketentuan peraturan perundang-undangan.

9. BISNIS LAIN DAN MASALAH HUKUM

9.1. Biaya

9.1.1. Biaya Penerbitan atau Pembaruan Sertifikat

DTA mengenakan biaya administrasi dalam menerbitkan atau memperbarui Sertifikat termasuk dalam hal penerbitan ulang Sertifikat.

9.1.2. Biaya Pengaksesan Sertifikat

DTA tidak mengenakan biaya administrasi kepada Pemilik untuk mengakses halaman repositori dan halaman *verify* DTA.

9.1.3. Biaya Pengaksesan Informasi Status atau Pencabutan

DTA tidak mengenakan biaya kepada Pemilik untuk mengakses daftar pencabutan atau verifikasi status.

9.1.4. Biaya Layanan Lainnya

DTA dapat mengenakan biaya tambahan untuk layanan selain Tanda Tangan Digital, sebagai contoh layanan penyimpanan arsip dan e-materai.

9.1.5. Kebijakan Pengembalian Biaya

Bagi Pemilik Sertifikat yang mengajukan permohonan kebijakan pengembalian, maka DTA mencabut Sertifikatnya. DTA tidak menyediakan pengembalian biaya Sertifikat Elektronik bagi Pemohon Sertifikat Elektronik yang permohonannya ditolak.

9.2. Tanggung Jawab Keuangan

9.2.1. Cakupan Asuransi

DTA menjamin kerugian akibat kegagalan layanan Penyelenggaraan Sertifikasi Elektronik, kesengajaan, dan/atau kelalaian kepada perorangan, karena kegagalannya dalam mematuhi kewajiban sebagai PSrE sesuai dengan ketentuan peraturan perundang-undangan yang diatur dalam dokumen Kebijakan Jaminan.

9.2.2. Aset Lainnya

DTA menjamin bahwa DTA memiliki sumber modal usaha yang cukup untuk menjalankan kegiatan operasionalnya dan menjalankan fungsinya.

9.2.3. Cakupan Asuransi atau Garansi untuk Pemilik

Batasan tanggung jawab DTA kepada Pemilik Sertifikat atas setiap perselisihan yang timbul dari atau sehubungan dengan layanan DTA atau penggunaan Situs oleh Pemilik Sertifikat, terlepas dari forum penyelesaian perselisihan atau terlepas dari tuntutan berasal dari perbuatan melawan hukum, wanprestasi atau lain sebagainya yang tidak sehubungan dengan layanan DTA, tidak akan melebihi Rp. 1.000.000 (satu juta Rupiah) selama Sertifikat Elektronik Pemilik aktif.

9.3. Kerahasiaan Informasi Bisnis

9.3.1. Cakupan Informasi Rahasia

DTA memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Yang termasuk dalam kategori informasi rahasia antara lain:

a. Informasi pribadi sebagaimana diatur pada Bagian 9.4;
b. Kunci Privat Pemilik Sertifikat yang disimpan oleh DTA, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
c. Catatan Permohonan Sertifikat;
d. Hasil penilaian kerentanan;
e. Rekam jejak audit (*audit logs*) dari sistem DTA dan RA;
f. Data aktivasi pada saat pengaktifan Kunci Privat DTA sebagaimana diatur pada bagian 6.4;
g. Dokumentasi bisnis proses DTA termasuk dokumen Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP);
h. Laporan audit dari auditor independen dan auditor internal sebagaimana diatur pada Bagian 8.0; dan
i. Kunci Privat DTA.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, sebelum pengungkapan informasi di atas memerlukan persetujuan tertulis dari Pemilik Sertifikat.

9.3.2. Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia

Informasi yang tidak termasuk pada Bagian 9.3.1 dianggap informasi publik.

Informasi yang tidak dikategorikan rahasia dalam dokumen CPS dianggap informasi publik. Sertifikat dan informasi mengenai status Sertifikat termasuk kategori informasi publik.

Sertifikat, respon OCSP, CRL dan informasi pribadi atau perusahaan yang terdapat di dalamnya dan di direktori publik tidak dianggap sebagai informasi rahasia.

9.3.3. Tanggung Jawab untuk Melindungi Informasi Rahasia

DTA melindungi informasi rahasia. DTA menjaga kerahasiaan informasi bisnis rahasia yang secara jelas ditandai atau diberi label sebagai rahasia atau menurut sifatnya harus dipahami secara wajar sebagai rahasia, dan memperlakukan informasi tersebut dengan tingkat perhatian dan keamanan yang sama seperti DTA memperlakukan informasi rahasia miliknya sediri.

Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:
a. Pelatihan atau peningkatan *awareness*;
b. Perjanjian Kontrak Pegawai;
c. NDA (*Non-disclosure Agreement*) dengan pegawai, pegawai outsource, dan pihak ketiga; dan
d. Semua Informasi yang diberi label rahasia.

9.4. Privasi Informasi Pribadi

9.4.1. Rencana Privasi

DTA melindungi Informasi Privat dalam kaitan dengan Kebijakan Privasi yang dipublikasikan dalam repositori DTA sesuai Bagian 2.1.

Kebijakan Privasi DTA mendokumentasikan informasi pribadi yang dikumpulkan, bagaimana informasi tersebut disimpan dan diproses, dan kondisi yang membolehkan informasi tersebut untuk diungkap. DTA patuh terhadap peraturan perundang-undangan terkait perlindungan data pribadi yang terdapat dalam UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

DTA memberikan akses kepada Pemilik Sertifikat untuk mengoreksi atau mengubah informasi pribadi atau organisasi melalui permintaan yang sah kepada DTA. DTA melakukan langkah-langkah untuk mengautentikasi identitas dari pihak yang meminta perubahan informasi pribadi atau organisasi.

DTA mengumpulkan data hanya untuk pendaftaran Sertifikat dan data yang dikumpulkan tidak dikomersialkan.

9.4.2. Informasi yang Diperlakukan sebagai Privat

DTA melindungi semua informasi pribadi Pemohon dari pengungkapan yang tidak sah, baik terhadap Pemohon yang Sertifikatnya berhasil diterbitkan (Pemilik) maupun yang ditolak. DTA menghapus informasi pribadi Pemohon yang ditolak paling lama 30 (tiga puluh) hari kalender. DTA menyimpan Nomor Identitas Kependudukan (NIK) Pemohon disertai alasan penolakan.

Informasi pribadi dapat diungkap atas persetujuan Pemilik Sertifikat terhadap Pengandal. Arsip yang dikelola oleh DTA tidak diungkap kecuali diizinkan pada Bagian 9.4.1.

9.4.3. Informasi yang tidak Dianggap Privat

Informasi yang disertakan dalam Sertifikat tidak dianggap Privat dan tidak tunduk sebagaimana yang diuraikan dalam Bagian 9.4.2.

Pelanggaran atas penggunaan informasi pribadi mengacu pada ketentuan peraturan perundang-undangan.

9.4.4. Tanggung Jawab Melindungi Informasi Privat

DTA bertanggung jawab untuk menyimpan informasi privat, baik dalam bentuk fisik ataupun elektronik sesuai dengan dokumen Kebijakan Privasi DTA yang dipublikasikan dalam halaman repositori DTA. Backup informasi privat dilakukan dalam kondisi terenkripsi.

9.4.5. Pemberitahuan dan Persetujuan untuk menggunakan Informasi Privat

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran diperlakukan sebagai informasi privat sehingga perlu persetujuan dari Pemohon. DTA mengakomodir semua ketentuan terkait penggunaan informasi privat ke dalam Kebijakan Privasi dan Perjanjian Pemilik Sertifikat. Penggunaan informasi privat harus didasarkan pada pelaksanaan Perjanjian Pemilik Sertifikat atau Perjanjian Pengandal, atau dasar hukum lainnya, yang mengacu pada Kebijakan Privasi dan Ketentuan peraturan perundang-undangan.

9.4.6. Pengungkapan Berdasarkan Proses Peradilan atau Administratif

DTA tidak mengungkap informasi privat kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, ketentuan peraturan perundang-undangan, atau perintah pengadilan.

9.4.7. Keadaan Pengungkapan Informasi Lain

Tidak ada ketentuan.

9.5. Hak atas Kekayaan Intelektual

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

DTA tidak akan melanggar hak kekayaan intelektual pihak lain.

9.6. Pernyataan dan Jaminan

9.6.1. Pernyataan dan Jaminan PSrE

DTA menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

1. DTA mematuhi ketentuan yang diatur dalam CPS ini;
2. DTA menerbitkan dan memperbarui CRL sesuai ketentuan dalam CPS ini;
3. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini;
4. DTA akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya;
5. Kunci Privat DTA terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;
6. Semua pernyataan yang dibuat oleh DTA dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh DTA; dan
7. Setiap Pemilik Sertifikat telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik Sertifikat yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

9.6.2. Pernyataan dan Jaminan RA

DTA tidak menggunakan external RA. DTA sebagai RA menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

a. Tidak ada kekeliruan dalam Sertifikat yang diketahui atau berasal dari entitas yang menyetujui permohonan 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. DTA menjamin bahwa kegiatan registrasi dilakukan sesuai dengan CPS; dan
d. Pemilik Sertifikat dikenakan kewajiban sebagaimana disebutkan dalam Bagian 9.6.3. Pemilik Sertifikat mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

9.6.3. Pernyataan dan Jaminan Pemilik Sertifikat

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

1. 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 Pemilik Sertifikat dan Sertifikat telah diterima dan valid (tidak kedaluwarsa atau dicabut) pada saat Tanda Tangan Digital dibuat;
2. Kunci Privat Pemilik Sertifikat disimpan dan diamankan oleh DTA dan hanya Pemilik Sertifikat yang memiliki akses terhadap Kunci Privat tersebut;
3. Sudah melakukan reviu terhadap informasi dari Sertifikat;
4. Semua informasi yang diberikan oleh Pemilik Sertifikat dan informasi yang terkandung di dalam Sertifikat sudah sesuai;
5. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
6. Pemilik Sertifikat dan/atau Pemohon Segera memberitahukan DTA dalam hal:
    a. Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat dan Kunci Privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari Kunci Privat Pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat;
    b. Mengajukan permohonan untuk melakukan pencabutan Sertifikat dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam Sertifikat tersebut; atau
    c. Menghentikan penggunaan Kunci Privat yang Kunci Publiknya tercantum dalam CRL.
7. Akan menanggapi instruksi DTA terkait keadaan terkompromi atau penyalahgunaan Sertifikat dalam kurun waktu 48 (empat puluh delapan) jam;
8. Menyetujui dan menerima bahwa DTA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Pemilik Sertifikat atau jika DTA menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti phishing, penipuan atau pendistribusian malware;
9. Pemilik Sertifikat adalah 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

Pihak yang mengandalkan Sertifikat DTA menjamin bahwa:

1. Memiliki kemampuan teknis untuk memverifikasi Sertifikat;
2. Apabila perwakilan dari Pengandal menggunakan suatu Sertifikat yang diterbitkan oleh DTA, Pengandal secara benar memverifikasi informasi yang tercantum di dalam Sertifikat sebelum digunakan dan menanggung akibat apa pun yang terjadi jika lalai dalam melakukan hal tersebut;
3. Melaporkan langsung kepada DTA, jika Pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat;
4. Memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat, bahwa Pengandal sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi ketentuan yang ada dalam CPS ini; dan
5. Mematuhi ketentuan yang ditetapkan dalam CPS ini.

9.6.5. Pernyataan dan Jaminan Partisipan Lain

Tidak ada ketentuan.

9.7. Pelepasan Jaminan

DTA tidak menjamin:

a. Penyalahgunaan Sertifikat yang tidak sesuai dengan peruntukannya sebagaimana diatur pada Bagian 4.5 (*Certificate Usage*);
b. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat; dan
c. Selain jaminan yang telah tercantum dalam Kebijakan Jaminan dan sepanjang diizinkan oleh hukum, DTA mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu.

9.8. Pembatasan Tanggung Jawab

9.8.1. Pembatasan Tanggung Jawab PSrE

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

a. Semua kerusakan yang diakibatkan dari penggunaan Sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Pemilik 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 DTA.

9.8.2. Pembatasan Tanggung Jawab RA

DTA sebagai RA tidak bertanggung jawab atas setiap akibat atau kerugian, baik secara langsung maupun tidak langsung, yang dapat timbul, termasuk namun tidak terbatas pada hal-hal yang disebabkan karena kesalahan Pemilik yaitu:

a. Kehilangan data,
b. Kehilangan pendapatan, keuntungan, atau pemasukan lainnya; dan/atau
c. Kehilangan, kerusakan atau kerugian yang timbul dari penggunaan informasi atau data pribadi yang tidak sesuai, akurat dan/atau valid, yang diberikan oleh Pemilik kepada DTA dalam penggunaan layanan DTA berdasarkan CPS ini.

9.8.3. Pembatasan Tanggung Jawab Pemilik

Tanggung jawab Pemilik Sertifikat dan/atau batasannya diatur dalam Perjanjian Pemilik Sertifkat, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak.

Pemilik Sertifikat secara khusus bertanggung jawab atas kerugian yang disebabkan oleh kelalaian, pelanggaran kelaikan seperti memindahtangankan atau membuat dapat diaksesnya metode atau faktor autentikasi kepada orang lain ataupun tidak mencabut Sertifikat yang telah atau diduga terkompromi.

9.9. Ganti Rugi

9.9.1. Ganti Rugi oleh DTA

Kewajiban ganti rugi oleh DTA ditetapkan dalam CPS, Perjanjian Pemilik Sertifikat, Kebijakan Jaminan dan Perjanjian Pengandal termasuk setiap kewajiban apa pun kepada pihak ketiga penerima manfaat, dengan mengacu pada ketentuan peraturan perundang-undangan.

9.9.2. Ganti Rugi oleh Pemilik

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

1. Pelanggaran yang dilakukan oleh Pemilik Sertifikat terhadap Perjanjian Pemilik Sertifikat, CSP ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
2. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik Sertifikat;
3. Penggunaan Sertifikat oleh Pemilik Sertifikat untuk melakukan perbuatan melawan hukum;
4. Kegagalan Pemilik Sertifikat untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu pihak manapun;
5. Kegagalan Pemilik 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; atau
6. Penggunaan nama oleh Pemilik 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 DTA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerusakan, biaya dan segala tuntutan yang diakibatkan oleh:

1. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pengandal, CPS ini, atau hukum yang berlaku;
2. 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 dinyatakan berlaku sampai ada pemberitahuan perubahan lebih lanjut oleh DTA melalui *website* dan repositori DTA.

9.10.2. Pengakhiran

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

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

OID dalam CPS DTA tetap berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan perubahan baru pada CP PSrE Induk, dokumen Hierarki OID dan/atau kebijakan lainnya yang berdampak pada OID DTA.

9.10.3. Dampak Pengakhiran dan Ketentuan yang tetap Berlaku

DTA mengomunikasikan kondisi, dampak dari penghentian CPS, dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit melalui website DTA di alamat https://www.xignature.co.id atau repositori di alamat https://repository.xignature.co.id/.

Dalam hal CPS DTA tidak berlaku lagi, DTA tetap mematuhi aturan terkait perlindungan data dan arsip informasi.

9.11. Pemberitahuan Individu dan Komunikasi dengan Partisipan

DTA menyediakan media komunikasi bagi para pihak terkait melalui alamat dan media komunikasi yang dicantumkan pada situs DTA. Pemberitahuan dianggap telah diterima apabila pengirim menerima pernyataan penerimaan dari DTA.

DTA akan memberikan tanggapan atas permintaan yang diberikan paling lambat 20 (dua puluh) hari kerja dari diterimanya permintaan tersebut.

9.12. Amendemen

Pemilik Sertifikat dan Pengandal akan diberitahu apabila diperlukan.

9.12.1. Prosedur untuk Perubahan atau Amandemen

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

9.12.2. Periode dan Mekanisme Pemberitahuan

DTA menerbitkan pemberitahuan terkait perubahan dari CPS ini termasuk keterangan ketika CPS efektif berlaku melalui halaman situs web https://www.xignature.co.id. Perubahan CPS dipublikasikan paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.

9.12.3. Keadaan Dimana OID Harus Diubah

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

9.13. Ketentuan Penyelesaian Perselisihan/Sengketa

Jika terdapat perselisihan/sengketa antara DTA dengan Pemilik Sertifikat atau dengan Pengandal, maka para pihak akan berusaha untuk mencapai penyelesaian damai disertai dengan pemberitahuan dari DTA ke pihak lainnya. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak atau perjanjian yang disepakati antara DTA dengan Pemilik Sertifikat atau dengan Pengandal.

9.14. Hukum yang Mengatur

CPS ini ditafsirkan dan dipahami sesuai dengan ketentuan peraturan perundang-undangan di Indonesia. Pemilihan aturan hukum ini untuk memastikan interpretasi yang sama dalam CPS ini, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat DTA atau pun produk dan layanan lainnya. Termasuk apabila Sertifikat DTA digunakan untuk kebutuhan komersial atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan DTA, tetap menerapkan hukum di indonesia.

Para pihak, termasuk pertners CA, Pemilik Sertifikat, Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan di atas.

9.15. Kepatuhan atas Hukum yang Berlaku

DTA 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. Seluruh Perjanjian

DTA secara kontraktual mewajibkan RA yang terlibat dalam penerbitan Sertifikat untuk mematuhi CPS ini dan semua panduan terkait.

9.16.2. Pengalihan Hak

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

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 diberlakukan dengan sebagaimana harusnya.

9.16.4. Penegakan Hukum (Biaya Pengacara dan Pelepasan Hak)

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

9.16.5. Keadaan Memaksa

DTA tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam melaksanakan CPS, 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. DTA telah menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas DTA.

9.17. Ketentuan Lain

9.17.1. Versi CPS yang Memiliki Kekuatan Hukum

CPS ini mengikat secara hukum.

LAMPIRAN 1 – PROFIL SERTIFIKAT

1. Sertifikat DTA CA

Basic Certificate Fields	*Value*
Version	3
Signature Algorithm	sha256WithRSAEncryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	DTA CA
Subject: OrganizationName	PT Digital Tandatangan Asli
Subject: CountryName	ID
Subject Alternative Name	N/A
Serial Number	Automatically assigned by application
Validity Starts	YYYY/MM/DD HH:MM:SS [ten years of validity period]
Validity Ends	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Sign CRL, Sign Certificate (CA)
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URI = 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

2. Sertifikat Pemilik

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

Basic Certificate Fields	*Value*
Version	3
Signature Algorithm	sha256WithRSAEncryption
Issuer: CN	DTA CA
Issuer: O	PT Digital Tandatangan Asli
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar)
Subject: OrganizationName	Personal
Subject: CountryName	ID
Subject: UserID	XignatureID (username)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS [one year of validity period]
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 URI = http://crl.xignature.co.id/ca.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URI=http://ocsp.xignature.co.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.6.0.2.1 URL: https://repository.xignature.co.id OID : 2.16.360.1.1.1.3.12.6 Notice=” PT Digital Tandatangan Asli (DTA)” OID : 2.16.360.1.1.1.5.1.2.2 Notice=”Individu Non-Instatansi Online Level 2”
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

2.2. Sertifikat Non-Instansi Verifikasi Level 2 (Offline)

Basic Certificate Fields	*Value*
Version	3
Signature Algorithm	sha256WithRSAEncryption
Issuer: CN	DTA CA
Issuer: O	PT Digital Tandatangan Asli
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar)
Subject: OrganizationName	Personal
Subject: CountryName	ID
Subject: UserID	XignatureID (username)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS [one year of validity period]
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 URI = http://crl.xignature.co.id/ca.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URI=http://ocsp.xignature.co.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.6.0.2.1 URL: https://repository.xignature.co.id OID : 2.16.360.1.1.1.3.12.6 Notice=” PT Digital Tandatangan Asli (DTA)” OID : 2.16.360.1.1.1.5.1.1.2 Notice=”Individu Non-Instatansi Offline Level 2”
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

3. Sertifikat Badan Usaha

Basic Certificate Fields	*Value*
Version	3
Signature Algorithm	sha256WithRSAEncryption
Issuer: CN	DTA CA
Issuer: O	PT Digital Tandatangan Asli
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar)
Subject: OrganizationName	Personal
Subject: CountryName	ID
Subject: UserID	XignatureID (username)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS [one year of validity period]
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 URI = http://crl.xignature.co.id/ca.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URI=http://ocsp.xignature.co.id
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.6.0.2.1 URL: https://repository.xignature.co.id OID : 2.16.360.1.1.1.3.12.6 Notice=” PT Digital Tandatangan Asli (DTA)” OID : 2.16.360.1.1.1.8.1 Notice=” Badan Usaha (Segel El)”
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

LAMPIRAN 2 - TABEL AKRONIM DAN DEFINISI

Tabel Akronim

Istilah	Definisi
PSrE	Penyelenggara Sertifikat Elektronik
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DTA	PT Digital Tandatangan Asli
FIPS	Federal Information Processing Standards (US Government)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
IKP	Infrastruktur Kunci Publik
RA	Registration Authority
RFC	Request for Comment
VA	Validation Authority

Definisi

Istilah	Definisi
IKP Indonesia	Seperangkat perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan, dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan Sertifikat dan kunci yang dapat dipercaya berdasarkan pada kriptografi Infrastruktur Kunci Publik sesuai peraturan Indonesia.
PSrE	Entitas yang berwenang untuk mengeluarkan, mengelola, mencabut, dan memperbarui Sertifikat dalam lingkup IKP Indonesia.
PSrE Induk	Entitas legal yang memiliki otoritas Sertifikasi tingkat teratas yang menandatangani Sertifikat DTA dalam rantai IKP Indonesia.
PSrE Indonesia (PSrE Berinduk) atau DTA	Entitas legal yang Sertifikatnya ditandatangani oleh PSrE Induk dan bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Pemilik.
PSrE Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi.
PSrE non-Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat non-Instansi.
Pemohon	Individu atau Badan Hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik.
Pemilik	Individu yang merupakan subjek dari Sertifikat, telah diterbitkan Sertifikatnya.
Sertifikat	Sertifikat adalah Sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik.
Sertifikat PSrE Induk	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PSrE Induk untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh DTA.
Sertifikat DTA	Sertifikat yang dikeluarkan oleh PSrE Induk Indonesia.
Sertifikat Pemilik	Sertifikat yang dikeluarkan oleh DTA.
Kebijakan Sertifikat (Certificate Policy)	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum.
Pernyataan Kebijakan Sertifikasi (Certification Practice Statement)	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat.
Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh DTA yang menerbitkan Sertifikat.
Certificate Signing Request	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat.

Kompromi	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif.
Extended Validation Certificate	Sertifikat yang berisi informasi yang ditentukan dalam Pedoman EV dan yang telah divalidasi sesuai dengan Pedoman tersebut.
Kebocoran Kunci	Kunci Privat dikatakan dikompromikan jika nilainya telah diungkapkan kepada orang yang tidak berkepentingan, orang yang tidak sah memiliki akses ke sana, atau ada praktek teknis yang memungkinkan orang yang tidak berwenang mendapatkan nilainya.
Upacara Pembangkitan Kunci	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan, kunci privasinya ditransfer ke modul kriptografi, Kunci Privatnya dicadangkan, dan/atau Kunci Publiknya disertifikasi.
Object Identifier	Sebuah tanda pengenal alfanumerik atau numerik yang terdaftar di bawah standar yang berlaku terhadap objek atau kelas objek tertentu yang diterbitkan oleh Organisasi Standardisasi Internasional (International Organization for Standardization).
Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi Pengandal yang berisi informasi mengenai status Sertifikat.
Kunci Privat	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.
Kunci Publik	Kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Pribadi terkait dan yang digunakan oleh Pihak yang Mengandalkan untuk memverifikasi Tanda Tangan Digital yang dibuat dengan Kunci Pribadi dan / atau untuk mengenkripsi pesan Pemiliknya sehingga dapat didekripsi hanya dengan Kunci Publik yang sesuai.