Tata Cara Pengelolaan Sertifikat /
Certification Practice Statement (CPS)

Penyelenggara Sertifikasi Elektronik (PSrE) /
Certificate Authority (CA)

PSrE Digisign /
Digisign CA

15 Januari 2026
15 January 2026

Versi 3.5
Version 3.5

Catatan :

- UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang diterbitkan **iOTENTIK/BSrE**

Halaman Persetujuan / *Approval Page*

Dokumen ini disetujui secara elektronik sesuai dengan waktu penandatanganannya.
This document is approved electronically according to the time of signing.

Menyetujui,
Approved by,

PSrE Induk / *Root CA*	PSrE Digisign / *Digisign CA*
	Ditandatangani elektronik: Fajar Aji Suryawan 14-01-2026 15:36:13 WIB
Teguh Arifiyadi	**Fajar Aji Suryawan**
Direktur Pengawasan Sertifikasi dan Transaksi Elektronik Kementerian Komunikasi dan Digital (selaku *Policy Authority* PSrE Induk)	Policy Authority PT Solusi Net Internusa (Digisign CA)

Riwayat Perubahan / *Change Notes*

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
1 May 2019	1.0	Dokumen Awal *Initial Release*	Manager Kebijakan *Policy Manager*
6 Aug 2019	1.1	Perubahan Judul CPS, menjadi PSrE Terdaftar *CPS title change, to Registered PSrE*	Policy Authority
6 Aug 2019	1.2	Penghapusan Point 1.4.1 (OID) *Point 1.4.1 deletion (OID)*	Policy Authority
6 Aug 2019	1.3	Penghapusan tabel 1.4.1 *Table 1.4.1 deletion*	Policy Authority
6 Aug 2019	1.4	Penghapusan point 5.5.1 *Point 5.5.1 deletion*	Policy Authority
16 Jun 2020	2.0	Perubahan Judul CPS dan seluruh kalimat PSrE Terdaftar, menjadi PSrE Tersertifikasi *Change of CPS Title and editorial of Registered PSrE, into Certified PSrE* Penambahan Nomor Level pada point 6.2.1 *Addition of Level Number at point 6.2.1*	Policy Authority
17 May 2021	3.0	1.1 Uraian PSrE Digisign sebagai PSrE Non Instansi *1.1 Description of Digisign CA as a Non-Agency PSrE* 1.2 Update OID *1.2 OID Update* 1.3.2 Menghilangkan proses CSR *1.3.2 CSR process elimination* 1.4.1 Menghilangkan Level 2 pada layanan *1.4.1 Elimination Level 2 on the service* 1.5.4 Memperjelas status dan PIC peran PA *1.5.4 PIC status and PA role clarification* 2.1 Melengkapi dokumen-dokumen di repositori *2.1 Repository documents completion* 2.3 Waktu dirubah dari 1 jam menjadi 30 menit *2.3 Time changes from 1 hour to 30*	Policy Authority

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		minutes 3.2.1 Detail pengamanan *3.2.1 Security details* 3.2.2 Detail persyaratan *3.2.2 Details of requirements* 3.2.3 Detail persyaratan *3.2.3 Details of requirements* 3.2.4 NPWP dan Alamat dihilangkan *3.2.4 Removal of NPWP and Address* 4.1.1 Detail persyaratan Sertifikat *4.1.1 Details of Certificate requirements* 4.1.2 Penambahan tanggung jawab PSrE Digisign *4.1.2 Addition on Digisign CA responsibilities* 4.2.2 Penambahan detail alasan penolakan *4.2.2 Details of reasons for rejection added* 4.2.3 Perubahan waktu permohonan Sertifikat *4.2.3 Change of time for Certificate application* 4.5.1 Penambahan detail perlindungan kunci privat *4.5.1 Added private key protection details* 4.5.2 Penambahan informasi dokumen Relying Parties Agreement *4.5.2 Addition of Relying Parties Agreement document information* 4.6 Penambahan Not before pada pembaharuan *4.6 Added Not before to the update* 4.6.1 Informasi H-30 Sertifikat akan kedaluwarsa *4.6.1 Information H-30 Certificate expiration* 4.9.1 Penambahan responder OCSP *4.9.1 Addition of OCSP responders*	

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		4.9.8 Di Update OCSP menjadi 30 menit *4.9.8 Update OCSP to 30 minutes* 4.12.1 Detail spesifikasi tingkat keamanan *4.12.1 Detailed security level specifications* 5.2.1 Penyempurnaan trusted role *5.2.1 Enhanced trusted roles* 5.3.8 Penambahan detail dokumen yang disediakan *5.3.8 Adding detailed documents provided* 5.4.1 Penambahan detail kejadian yang direkam *5.4.1 Added details of recorded events* 5.4.2 Update menjadi 1 bulan sekali *5.4.2 Update to once a month* 5.6 Perubahan kunci PSrE Digisign di tahun ke 8 (Interlock) *5.6 Digisign CA key signing change in year 8 (Interlock)* 6.2.8 Update quorum *6.2.8 Quorum update* 6.4.2 Detail perlindungan data aktivasi *6.4.2 Activation data protection details* 6.8 Update pencocokan waktu *6.8 Time match update* 7.1.2.1 Penambahan table Sertifikat Pemilik *7.1.2.1 Addition Subscriber Certificate table* 8 Update detail audit kepatuhan dan penilaian *8 Update details of compliance audit and assessment.* 9.1.2 update biaya *9.1.2 Fee update* 9.1.3 update biaya *9.1.3 Fee update* 9.4.3 Penambahan OCSP *9.4.3 Addition of OCSP*	

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		9.4.4 Update perlindungan informasi pribadi *9.4.4 Update protection of personal information* 9.9.1 Penambahan kebijakan jaminan *9.9.1 Addition warranty policy* 9.15 Penambahan Root CA Indonesia *9.15 Addition Root CA Indonesia*	
8 Sep 2021	3.1	*1.2* Penyesuaian identifikasi dan nama dokumen *1.2 Customization of document identification and name* 4.9.7 Penyesuaian frekuensi penerbitan CRL *4.9.7 Adjustment of CRL issuance frequency* 5.2.1 Penyempurnaan poin trusted role *5.2.1 Improvement on trusted role points* 5.4.5 Penyempurnaan backup Log audit, secara *realtime* *5.4.5 Improved audit log backup, in realtime* 5.4.6 Penyesuaian Prosedur Backup Lainya, update Redaksional *5.4.6 Adjustment of other Backup Procedures, editorial update*	Staff Policy Authority
10 Jan 2022	3.2	Perubahan Judul dokumen, dari Certificate Practice Statement menjadi *Certification Practice Statement.* *Change of document title, from Certificate Practice Statement to Certification Practice Statement.* 1.1 Memperbaiki kalimat pada bagian Ringkasan *1.1 Summary section sentences correction* 1.2 Memperbaiki kalimat pada bagian Identifikasi *1.2 Identification section sentences editorial* 1.3.1 Revisi Definisi PSrE Induk dan Berinduk. *1.3.1 Revision of definition of Root PSRE and Subordinate PSRE*	Staff Policy Authority

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		1.3.2 Revisi Bagian Otoritas Pendaftaran (RA), termasuk fungsi RA. *1.3.2 Revision of the Registration Authority (RA) Section, including RA functions.* 1.4.1 Menghapus poin a. Otentikasi pada penerbitan Sertifikat untuk transaksi. Termasuk memperbaiki kalimat penjelasan tentang Level Sertifikat. *1.4.1 Point a deletion. Authentication on issuance of Certificates for transactions. Including fixing the explanatory sentence about Certificate Level.* 1.5.1 Menambahkan no kontak PA menjadi +62 21 3111 6109/10. *1.5.1 Added PA contact number to +62 21 3111 6109/10.* 1.5.3 Melengkapi personil membantu PA dalam kesesuaian CPS dengan CP. *1.5.3 Equip personnel assist PA in conformance of CPS with CP.* 3.2.3 Autentikasi identitas orang perseorangan Level 3 bagi WNA. *3.2.3 Level 3 individual identity authentication for individual Foreigner.* 4.9.3.1 Menambahkan Prosedur Permintaan Pencabutan oleh Perorangan *4.9.3.1 Individual Revocation Request Procedure added* 5.5.3 Memperbaiki kalimat bagian Perlindungan arsip. *5.5.3 Archive protection section sentence editorial.* 8.1 Memperbaiki kalimat pada bagian Frekuensi atau keadaan asesmen. *8.1 Frequency section or the state of the assessment sentence fixing.* Memperbaiki Redaksional pada beberapa kalimat, dan menyiapkan bilingual. *Editorial in sentences, and bilingual preparation.* 9.16.6 Penambahan Poin Bahasa –	

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		9.16.6 Additional Point for Language Perubahan CPS menjadi Dua Bahasa – *Changes on CPS to bilingual*	
8 Feb 2022	3.3	Perubahan tipe nama: *Distinguished Name* untuk O: perseorangan, menjadi O, Personal. Poin 3.1.1 *Changes on Distinguished Name for O:perseorangan to O:Personal. Point 3.1.1*	Staff Policy Authority
8 Mar 2022	3.3.1	Perubahan tanggal pada Lembar Catatan Review / Revisi dari 8 January 2022 menjadi 8 February 2022 *Changes date on Review / Revision Sheet previous 8 January 2022 become 8 February 2022*	Staff Policy Authority
17 Mar 2022	3.4	Penambahan poin 9.2.1 Batasan maksimum cakupan Jaminan PSrE Digisign, dan ketentuan setiap pengguna diatur dalam Kebijakan Jaminan *Added at points 9.2.1 for Maximum limit of Digisign CA Warranty coverage, and the terms of each user are set out in the Warranty Policy*	Staff Policy Authority
11 May 2022	3.4.1	Penambahan poin 4.9.1 menjadi b. Informasi apapun dalam Sertifikat menjadi tidak valid, *Added at points 4.9.1 become* *b. Any information in the certificate becomes invalid.* Penghapusan PSrE Induk pada poin 4.9.1e. *Deleted Root PSrE on poin 4.9.1 e.*	Staff Policy Authority
30 Aug 2023	3.4.2	Perubahan OID pada butir 1.2 merujuk pada Hierarki OID untuk IKP Indonesia 1.2 *Addition OID in point 1.2 refers to the OID Hierarchy for Indonesia PKI version 1.2* Penyesuaian definisi “Pemilik” pada butir 1.3.3. *Adjustment of Subscriber definition at section 1.3.3.* Penyesuaian OID pada butir 1.4.1 merujuk pada Hierarki OID untuk IKP Indonesia 1.2 *The OID adjustment in item 1.4.1 refers to*	Policy Authority

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		the OID Hierarchy for Indonesia PKI version 1.2 Penyesuaian tabel 1 pada butir 1.4.1 merujuk pada Standar Verifikasi Identitas versi 1.1 *Adjustment of the Table 4 in point 4.1.1 refers to the Verification Identity Standard version 1.3* Penyesuaian butir 1.5.1, 1.5.4 merujuk pada CP PSrE Induk versi 3.3. *Adjustment of point 1.5.1, 1.5.4 refers to Root's CP version 1.5.1* Penyesuaian tabel 2 pada butir 3.1.1 merujuk pada Standar Interoperabilitas versi 1.3 dan dipindahkan ke lampiran C *Adjustment of the Table 2 in point 1.3 refers to the Interoperability Standard version 1.3 and move to appendix C* Penyesuaian butir 3.1.5, 3.2.1, 3.2.3, 3.3.2 & 3.4 merujuk pada CP PSrE Induk versi 3.3. dan Standar Verifikasi Identitas versi 1.1 *Adjustment of points 3.1.5, 3.2.1, 3.2.3, 3.3.2 & 3.4 refers to Root's CP version 3.3. and Verification Identity Standard version 1.1* Penyesuaian butir 4.1.1, 4.1.2, 4.2.2, 4.2.3 merujuk pada CP PSrE Induk versi 3.3. dan Standar Verifikasi Identitas versi 1.1 *Adjustment of point 4.1.1, 4.1.2, 4.2.2, 4.2.3 refers to Root's CP version 3.3. and Verification Identity Standard version 1.1* Penyesuaian proses rekey beserta periode pasangan kunci dan periode sertifikat terkait. *Adjustment of rekey process including key pair period and corresponding certificate's period.* Penyesuaian butir 4 dan turunannya dengan CP PSrE Induk versi 3.3., Standar Verifikasi Identitas versi 1.1 dan Hierarki OID untuk IKP Indonesia 1.2. *Adjustment of point 4 and all section with*	

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		Root's CP version 3.3., Verification Identity Standard version 1.1 and OID Hierarchy for Indonesia PKI version 1.2. Penyesuaian butir 5.1.1, 5.1.2, 5.1.6, 5.1.7, 5.1.8, 5.2.2, 5.3.1, 5.3.3, 5.4.1, 5.5.1, 5.5.3, 5.6, 5.7.1, 5.7.2, 5.7.3 dan 5.7.4 dengan CP PSrE Induk versi 3.3. *Adjustment of points 5.1.1, 5.1.2, 5.1.6, 5.1.7, 5.1.8, 5.2.2, 5.3.1, 5.3.3, 5.4.1, 5.5.1, 5.5.3, 5.6, 5.7.1, 5.7.2, 5.7.3 and 5.7.4 with Root's CP version 3.3.* Penyesuaian judul dan kalimat pada bab 6 dan turunannya dengan CP PSrE Induk versi 3.3. *Adjustment of the title and sentence in chapter 6 and all of its sections with Root's CP version 3.3.* Penyesuaian isi bab 7 dan memindahkan detail pada lampiran C & D. *Adjustment of chapter 7 and move details into appendix C & D.* Penyesuaian judul-judul Bab dan Sub-babnya beserta kalimatnya dengan CP PSrE Induk v.3.3. *Adjustment of titles of chapter 8 & 9 and its sections including wordings with Root's CP v.3.3.* Penyesuaian lampiran A & B untuk tambahan akronim dan istilah *Adjustment of appendix A & B for additional acronym and definition* Penambahan lampiran C & D untuk Profil Sertifikat, CRL & OCSP *Additional appendix C & D for Certificate, CRL and OCSP Profiles*	
21 Sep 2023	3.4.2	Penyesuaian lampiran C & D untuk Profile Sertifikat dengan Hirarki untuk IKP Indonesia. *Adjustment appendix C & D for Certificate with Hierarchy of OID for IKP indonesia*	Policy Authority
27 Sep 2023	3.4.2	Penjelasan periode sertifikat "peninggalan", perbaikan paragraf pada *liveness detection*, contoh pihak berwenang	Policy Authority

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		Description of Legacy certificate period, example of authority by law, revision on liveness detection paragraph	
5 Feb 2024	3.4.2	Penyesuaian DigisignID.CA.Level4 G3 menjadi DigisignID.CA.Level2 G3 *Adjusting Digisign ID.CA.Level4 G3 to Digisign.CA.Level2 G3*	Staff Policy Authority
6 May 2024	3.4.3	Penyesuaian profil sertifikat pada Lampiran C *Adjustment of certificate profile in Appendix C*	Staff Policy Authority
29 Jul 2024	3.4.4	Penambahan klausul untuk Otoritas Pendaftaran Eksternal *Additional clause for external Registration Authority*	Staff Policy Authority
15 Jan 2026	3.5	Penambahan Bahasa Indonesia pada halaman judul dokumen *Addition of Indonesian language on the document title page* Penyesuaian “Menteri Komunikasi dan Informatika” menjadi “Menteri Komunikasi dan Digital” di seluruh Dokumen *Adjustment of “Minister of Communication and Informatics” to “Minister of Communication and Digital” throughout the document* 1.3.2 Penyesuaian pada deskripsi Otoritas Pendaftaran *1.3.2 Adjustments to the description of the Registration Authority* 1.3.3 Penyesuaian pada deskripsi Pemilik *1.3.3 Adjustments to description of the Owner* 3.2.1 Penyesuaian pada Metode Pembuktian Kepemilikan Kunci Privat *3.2.1 Adjustments to the Method for Proving Ownership of the Private Key* 3.2.2 Penyesuaian pada Otentikasi Identitas Organisasi *3.2.2 Adjustments to Organization Identity Authentication* 3.2.3 Penyesuaian pada Otentikasi	Policy Authority

Tanggal *Date*	Versi *Version*	Deskripsi *Description*	Oleh *By*
		Identitas Individu *3.2.3 Adjustments to Individual Identity Authentication* 4.4.1 Penyesuaian pada Sikap Yang Dianggap Sebagai Menyetujui Sertifikat *4.4.1 Adjustments to Conduct Deemed as Acceptance of a Certificate* 4.4.2 Penyesuaian pada Publikasi Sertifikat oleh PSrE Digisign *4.4.2 Adjustments to Certificate Publication by PSrE Digisign* 4.5.1 Penyesuaian pada Penggunaan Kunci Privat dan Sertifikat oleh Pemilik *4.5.1 Adjustments to the Use of Private Keys and Certificates by the Subscriber* 4.6.3 Penyesuaian pada Pemrosesan Permintaan Pembaruan Sertifikat *4.6.3 Adjustments to the Processing of Certificate Renewal Requests* Penyesuaian Peran Terpercaya *Adjustment of Trusted Role* Penyesuaian persyaratan verifikasi badan usaha *Adjustment of entity verification requirement* Penghapusan layanan sertifikat Level 3 untuk individu *Removal of Level 3 certificate services for individual*	

Daftar Isi / *Table of Contents*

1. PENGANTAR / *INTRODUCTION*

1.1 Ringkasan / *Overview*

Infrastruktur Kunci Publik (IKP) Indonesia adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikat Elektronik (PSrE) Induk. Kementerian Komunikasi dan Digital Republik Indonesia (Komdigi) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah nomor 71 Tahun 2019 tentang Penyelenggara Sistem dan Transaksi Elektronik. PSrE dibawah PSrE Induk terdiri atas 2 (dua) jenis PSrE yaitu PSrE Instansi Penyelenggara Negara (PSrE Instansi) dan PSrE non-Instansi Penyelenggara Negara (PSrE non-Instansi). PSrE Digisign adalah PSrE Indonesia (PSrE Berinduk) non-Instansi yang menerbitkan Sertifikat di bawah PSrE Induk. Sebagai PSrE non-instansi, PSrE Digisign menerbitkan Sertifikat kepada orang perseorangan warga negara Indonesia (WNI) dan warga negara asing (WNA) baik untuk kepentingan pribadi maupun untuk kepentingan entitas terafiliasi pada suatu badan usaha dalam transaksi elektronik. PSrE Digisign juga menerbitkan sertifikat untuk badan usaha yang dapat digunakan sebagai segel elektronik.

Indonesia's Public Key Infrastructure (PKI) is a hierarchy of PKIs with a chain of trust starting from the Main Certification Authority (CA/PSrE). The Ministry of Communication and Digital of the Republic of Indonesia (Komdigi) operates the Root PSRE in accordance with Government Regulation number 71 of 2019 concerning Electronic System and Transaction Operators. PSrE under the Subordinate PSrE consists of 2 (two) types of PSrE, namely PSrE for State Organizing Agencies (Instansi PSrE) and PSrE for non-State Organizing Agencies (PSrE for non-Agencies). Digisign CA is a non-Agency Indonesian CA (Subordinate CA) that issues Certificates under the Root CA. As a non-agency CA, Digisign CA issues Certificates to both individual Indonesian citizens (WNI) and registered foreigners (WNA), whether for personal use or for the purpose of being an affiliated entity of a business entity in electronic transactions. Digisign CA also issues certificates for businesses, which can serve as electronic seals.

Dokumen Certification Practice Statement PSrE Digisign (CPS PSrE Digisign)

This Certification Practice Statement Digisign CA Certification Authority (CPS

mengacu pada persyaratan yang diatur di dalam CP PSrE Induk. CPS ini mendefinisikan persyaratan prosedural dan operasional yang dianut oleh PSrE Digisign saat menerbitkan dan mengelola objek yang ditandatangani secara elektronik dalam lingkungan IKP Indonesia. CPS ini sesuai dengan Standard 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.

Digisign CA) refers to the requirement outlined in the root CP. This CPS defines the procedural and operational requirements adopted by Digisign CA when issuing and managing electronically signed objects within the Indonesian PKI environment..This CPS complies with the Standard Request for Comments 3647 (RFC 3647) from the Internet Engineering Task Force (IETF) regarding the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework.

1.2 Identifikasi dan Nama Dokumen / *Document Name and Identification*

Digisign, sesuai kewenangannya, ditetapkan untuk memiliki *Object Identifier* (OID) dengan nomor identifikasi joint-iso-ccitt (2) country (16) id (360) gov (1) kominfo (1) psre-induk (1) psre-indonesia (3) psre-non-instansi (12) PSrE Digisign (2).

Digisign CA, under its jurisdiction, is determined to have an Object Identifier (OID) with identification number OID Digisign CA is joint-iso-ccitt (2) country (16) id (360) gov (1) kominfo (1) psre-induk (1) psre-indonesia (3) psre-non-instansi (12) Digisign (2).

OID yang tercatat dalam sertifikat bergantung pada persyaratan dan pedoman dari CP PSrE Induk. Atribut-atribut OID pada sertifikat yang diterbitkan sebelum mulai berlakunya CPS ini ditunjukkan pada table di bawah ini sebagai “Peninggalan” karena diterbitkan sebelum CPS ini berlaku.

The OID mentioned in the certificate depends on the requirements and guidelines of the Root’s CP. The OID attributes on certificates issued before this CPS enforced are shown in the table below as “Legacy” due to they were issued prior this CPS enforced.

Berikut merupakan OID (tidak termasuk *Extended Validation Certificate*) yang digunakan oleh PSrE Digisign.

The following is the OID (excluding Extended Validation Certificate) used by Digisign CA.

Deskripsi / *Description*	Atribut / *Attribute*
OID PSrE Digisign / *Digisign CA's OID*	**Nomor OID (Notasi) / *OID Number (Notation)***
CPS PSrE Digisign	Dibutuhkan / *Required:* 2.16.360.1.1.1.3.12.2.1.2 (Cps-digisign)
Individu non-Instansi Offline Level 2	Dibutuhkan / *Required:* 2.16.360.1.1.1.5.1.1.2 (individu-wni offline level2) Peninggalan / *Legacy:* 2.16.360.1.1.1.3.12 (Sertifikat Non instansi) dan / *and* 2.16.360.1.1.1.7.1 (Sertifikat Individu) dan / *and* 2.16.360.1.1.1.4.4 (Verification Level 4)
Individu non-Instansi Online Level 2	Dibutuhkan / *Required:* 2.16.360.1.1.1.5.1.2.2 (individu-wni online level2) Peninggalan / *Legacy:* 2.16.360.1.1.1.3.12 (Sertifikat Non instansi) dan / *and* 2.16.360.1.1.1.7.1 (Sertifikat Individu) dan / *and* 2.16.360.1.1.1.4.4 (Verification Level 4)
Individu WNA Offline level 2	Dibutuhkan / *Required:* 2.16.360.1.1.1.5.2.1.2 (individu-wna offline level2) Peninggalan / *Legacy:* 2.16.360.1.1.1.3.12 (Sertifikat Non instansi) dan / *and* 2.16.360.1.1.1.7.1 (Sertifikat Individu) dan / *and* 2.16.360.1.1.1.4.4 (Verification Level 4)
Individu WNA Online level 2	Dibutuhkan / *Required:* 2.16.360.1.1.1.5.2.2.2 (individu-wna online level2) Peninggalan / *Legacy:* 2.16.360.1.1.1.3.12 (Sertifikat Non instansi) dan / *and* 2.16.360.1.1.1.7.1 (Sertifikat Individu) dan / *and* 2.16.360.1.1.1.4.4 (Verification Level 4)
Badan Usaha	Dibutuhkan / *Required:* 2.16.360.1.1.1.8.1 (badan-usaha) Peninggalan / *Legacy:* 2.16.360.1.1.1.3.12 (Sertifikat Non instansi) dan / *and* 2.16.360.1.1.1.7.2 (Sertifikat Badan Usaha) dan / *and* 2.16.360.1.1.1.4.3 (Verification Level 3)

Sertifikat Pemilik dengan OID "Peninggalan" tidak akan diterbitkan lagi oleh PSrE Digisign saat CPS ini berlaku. Sertifikat "Peninggalan" ini akan tetap dapat digunakan sampai dengan masa berlakunya habis (menurut tanggal *NotAfter* pada sertifikat pemilik).

Subscriber Certificates with "Legacy" OID will not be issued after this CPS is enforced. This "Legacy" certificate is valid until it expires (according to NotAfter date at subscriber's certificate).

PSrE Digisign akan menerbitkan sertifikat level 2 untuk yang sebelumnya memiliki sertifikat “Peninggalan” level 4.	*Digisign CA will issue level 2 certificate for previous “Legacy certificate level 4.*

1.3 Partisipan IKP / *PKI Participant*

1.3.1 Penyelenggara Sertifikasi Elektronik (PsrE) / *Certification Authority (CA)*

1.3.1.1 PSrE Induk Indonesia / *Root CA Indonesia*

PSrE Induk adalah induk dari IKP Indonesia. PSrE Induk menerbitkan dan/atau mencabut Sertifikat PSrE Indonesia (PSrE Instansi maupun PSrE non-Instansi) berdasarkan status pengakuan yang diberikan oleh Komdigi. PSrE Induk tidak menerbitkan Sertifikat kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Indonesia, sebagaimana dirinci dalam CPS ini, termasuk namun tidak terbatas pada:	*Root CA is the root CA of Indonesian PKI. Root CA issues and revokes Certificates of the Indonesian CAs (Government CAs and Non-Government CAs) upon recognition by Komdigi and it does not issue Certificates to Subscribers. Root CA is responsible for all aspects of the issuance and management of those Indonesian CA’s Certificates, as detailed in this CPS, including:*
1. Pengendalian terhadap proses pendaftaran calon PSrE Indonesia,	*1. The control over the registration process of Indonesia CA Candidate,*
2. Proses identifikasi dan autentikasi,	*2. The identification and authentication process,*
3. Proses penerbitan self-sign Sertifikat PSrE Induk,	*3. Generate self signed Root Certificate,*
4. Proses penerbitan Sertifikat PsrE Indonesia,	*4. Issuance of Indonesian CA’s Certificate,*
5. Proses penerbitan Daftar Pencabutan Sertifikat (Certificate Revocation List/CRLs),	*5. The Certificate Revocation List (CRLs) issuance process,*
6. Publikasi Sertifikat dan CRLs,	*6. The publication of Certificates and CRLs,*
7. Validasi Sertifikat,	*7. The validation of Certificates,*

8. Pencabutan Sertifikat,
9. Membangun dan memelihara sistem PSrE Induk, dan
10. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE Induk yang diterbitkan sesuai dengan CP ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk.

8. The revocation of Certificates,
9. Establishing and maintaining Root CA system, and
10. Ensuring that all aspects of the services, operations, and infrastructures related to Root CA detailed in this CPS are performed in accordance with the requirements, representations, and warranties stated in Root CA's CP.

PA PSrE Induk menjadi wakil PSrE Digisign dalam menjalin hubungan kepercayaan dengan IKP dari negara lain.

Root CA's PA represents Digisign CA in establishing mutual recognition with foreign PKI.

1.3.1.2 PSrE Indonesia / *Indonesian CAs*

PSrE Indonesia adalah PSrE yang mendapatkan pengakuan dari Menteri Komunikasi dan Digital (Menteri) dengan berinduk kepada PSrE Induk yang diselenggarakan oleh Menteri yang Sertifikatnya telah ditandatangani oleh PsrE Induk.

Indonesia Root CA is a CA which is recognized by the Indonesian Minister of Communication and Digital by subordinating to the Root CA which is operated by the Minister, Indonesian CA Certificates' has been signed by the Root CA. Digisign CA as an Indonesian CA issues Certificates to Subscriber.

Sebagai PSrE non-instansi, PSrE Digisign menerbitkan Sertifikat kepada WNI dan WNA baik untuk kepentingan pribadi maupun untuk kepentingan entitas terafiliasi pada suatu badan usaha dalam transaksi elektronik. PSrE Digisign juga menerbitkan sertifikat untuk badan usaha yang dapat digunakan sebagai segel elektronik.

As a non-agency CA, Digisign CA issues Certificates to both WNI and WNA, whether for personal use or for the purpose of being an affiliated entity of a business entity in electronic transactions. Digisign CA also issues certificates for businesses, which can serve as electronic seals.

PSrE Digisign bukan induk bagi PSrE lain dan tidak berinduk kepada PsrE Indonesia lain.	*Digisign CA is not root to other CAs nor become root to other Indonesian CAs.*
PSrE Digisign membuat dan memelihara CPS serta memastikan bahwa semua aspek layanan PSrE, operasi, dan infrastruktur dilakukan sesuai dengan CP PSrE Induk.	*Digisign CA creates and maintains CPS as well as assuring that all aspects of CA services, operational and infrastructures is performed according to the Root CA's CP.*

1.3.2 Otoritas Pendaftaran / *Registration Authority (RA)*

Otoritas Pendaftaran (*Registration Authority*/RA) bertanggung jawab untuk menerima permintaan penerbitan sertifikat dan melakukan otentikasi identitas Pemohon dan melaksanakan fungsi berikut: 1. Menyusun dan melaksanakan prosedur penerimaan pendaftaran Pemohon Sertifikat; 2. Melakukan identifikasi dan otentikasi Pemohon; 3. Memulai atau meneruskan proses permohonan pencabutan Sertifikat; dan 4. Menyetujui atau menolak permohonan untuk pembaruan Sertifikat dan/atau penggantian kunci (re-key) atas nama PSrE Digisign.	*Registration Authority (RA) is responsible for receiving requests for certificates issuance and authenticating the identity of the Applicants and perform functions as follows:* 1. *Establish and execute enrollment procedures for end-user certificate Applicants;* 2. *Perform identification and authentication of certificate Applicants;* 3. *Initiate or pass along revocation requests for Certificates; and* 4. *Approve or reject applications for Certificate renewal and/or re-key on behalf of a Digisign CA.*
PSrE Digisign melakukan audit terhadap RA untuk memastikan keamanan dan kesesuaian dengan ketentuan yang berlaku, termasuk CP PSrE Induk dan CPS.	*Digisign CA conducts an audit of the RA to ensure security and compliance with applicable regulations, including the Root CA's CP and CPS.*
Dalam hal PSrE Digisign menunjuk pihak ketiga sebagai RA, fungsi di atas tercantum	*When Digisign CA appoints a third party as its RA, the above functions are stated in the*

dalam perjanjian kerja sama antara PSrE Digisign dengan RA pihak ketiga.

agreement between the Digisign CA and the third party RA.

1.3.3 Pemilik / *Subscribers*

Pemilik adalah pihak atau entitas yang identitasnya tertera dalam Sertifikat yang diterbitkan oleh PSrE Digisign dan sudah melalui proses verifikasi. Sebelum dilakukan verifikasi identitas dan Sertifikat diterbitkan, entitas disebut sebagai Pemohon.

The Subscriber is the party or entity whose identity is stated in the Certificate issued by Digisign CA and has undergone the verification process. Before identity verification is carried out and the Certificate is issued, the entity is referred to as the Applicant.

PSrE Digisign menerbitkan sertifikat untuk Warga Negara Indonesia (WNI), Warga Negara Asing (WNA), dan Badan Usaha / Badan Hukum. PSrE Digisign tidak menerbitkan sertifikat untuk Instansi dan pegawai Instansi.

Digisign CA issues certificates for Indonesian Citizens (WNI), Foreign Citizens (WNA), and Business Entities / Legal Entities. Digisign CA does not issue certificates for Government Agencies and their employees.

1.3.4 Pengandal / *Relying Parties*

Pengandal adalah pihak yang memercayai informasi yang ada dalam Sertifikat dan/atau Tanda Tangan Elektronik yang diterbitkan oleh PSrE Digisign. Pengandal harus terlebih dahulu memeriksa respon dari *Certificate Revocation List* (CRL) atau *Online Certificate Status Protocol* (OCSP) PSrE Digisign sebelum memanfaatkan informasi yang ada dalam Sertifikat.

Relying Parties are parties that trust Certificates information stated on Certificate and/or Electronic Signatures issued by Digisign CA. Relying Parties must first check the response from the appropriate Digisign CA Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) before making use of the information contained in the Certificate.

Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pengandal dapat

The Relying Party is responsible for checking the status of the information in the Certificate. Relying Parties may use the

menggunakan informasi dalam Sertifikat untuk menentukan kecocokan penggunaan Sertifikat. Pengandal menggunakan informasi dalam Sertifikat untuk:

1. Memeriksa tujuan penggunaan Sertifikat,
2. Melakukan verifikasi Tanda Tangan Elektronik,
3. Memeriksa apakah Sertifikat termasuk di dalam CRL dan/atau OCSP, dan
4. Penyetujuan batas tanggung jawab dan jaminan.

information in the Certificate to determine suitability for use of the Certificate. The Relying Party uses the information in the Certificate to:

1. *The Certificate usage purpose,*
2. *Electronic Signature Verification,*
3. *Inspects if the Certificate is included in the CRL, and*
4. *Liability and warranty limits Agreement.*

Pengandal meliputi Bank, Perusahaan E-Commerce, Non-Instansi dan entitas lain yang menggunakan tanda tangan elektronik di dalam layanannya.

Relying Parties include Banks, E-Commerce Companies, Non-State Organizing Agencies, and other entities that use electronic signatures in their services

1.3.5 Partisipan Lain / *Other Participants*

Dalam hal PSrE Digisign bekerja sama dengan partisipan lain untuk menyelenggarakan layanannya, PSrE Digisign mendapat persetujuan dari Komdigi.

In accordance with Digisign CA collaborates with other participants to provide its services, Digisign CA obtains approval from Komdigi.

1.3.5.1 Penyedia Layanan Pusat Data / *Data Center Service Provider*

Penyedia Layanan Pusat Data adalah Pihak Ketiga yang menyediakan layanan Pusat Data untuk operasional PSrE Digisign.

Data Center Service Provider is a Third Party that provides Data Center services for Digisign CA operations.

1.4 Kegunaan Sertifikat / *Certificate Usage*

1.4.1 Penggunaan Sertifikat yang Semestinya / *Appropriate Certificate Uses*

Penggunaan Sertifikat Pemilik dibatasi sesuai *Key Usage* dan *Extended Key Usage* pada *Certificate Extension.* Sertifikat PSrE Digisign dapat digunakan untuk:

1. Tanda tangan Elektronik
2. Nirsangkal

The usage of Subscriber's Certificate is restricted based on Key Usage and Extended Key Usage in the Certificate Extension. Digisign CA certificates can be used for the following purposes:

1. *Electronic Signature*
2. *Non-Repudiation.*

Segel elektronik adalah tanda tangan elektronik yang dilakukan oleh entitas badan usaha.

An electronic seal is an electronic signature performed by a business entity.

Pemilik Sertifikat dapat memilih tingkat verifikasi yang sesuai sebagai identitas yang akan mereka tunjukkan kepada Pengandal. Tingkatan verifikasi yang dimaksud dibedakan menjadi kelas Sertifikat yang diatur di dalam Standar Verifikasi Identitas PSrE Induk.

Certificate Subscriber may choose an appropriate level of verification for their identity when presenting it to the Relying Party. These levels of verification are categorized into certificate classes as defined in the Identity Verification Standards of the root CA.

Penggunaan yang tidak sesuai dapat berakibat pada hilangnya jaminan yang diberikan oleh PSrE Digisign kepada Pemilik Sertifikat dan Pengandal.

Improper use may result in the loss of the warranty provided by Digisign CA to the Subscriber Certificate and Relying Parties.

PSrE Digisign membuat pemisahan kelas Sertifikat yang dipakai untuk membedakan tingkat kepercayaan (level verifikasi), tingkat jaminan (garansi), penggunaan Sertifikat (tanda tangan digital, enkripsi, dll), dan tipe pengguna (orang perseorangan atau organisasi) sebagaimana diterangkan pada

Digisign CA makes a classification of Certificate classes that are used to differentiate the verification level, warranty, Certificate use, and user type as described on the following table:

tabel berikut:

Pengguna / *User*	Metode Verifikasi / *Verification Method*	Level Sertifikat / *Certificate Level*	Tingkat Jaminan / *Assurance Level*	Penggunaan / *Usage*
Individu WNI / *Individual WNI*	Online	2	Menengah / *Medium*	Tanda Tangan Elektronik / *Electronic Signature*
Individu WNI / *Individual WNI*	Offline	2	Menengah / *Medium*	Tanda Tangan Elektronik / *Electronic Signature*
Individu WNA / *Individual WNA*	Online	2	Menengah / *Medium*	Tanda Tangan Elektronik / *Electronic Signature*
Individu WNA / *Individual WNA*	Offline	2	Menengah / *Medium*	Tanda Tangan Elektronik / *Electronic Signature*
Badan Hukum atau Badan Usaha / *Legal Entity or Business Entity*	Online	-	Tinggi / *High*	Segel Elektronik / *Electronic Seal*

1.4.2 Penggunaan Sertifikat yang Dilarang / *Prohibited Certificate Uses*

Sertifikat yang diterbitkan oleh PSrE Digisign dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

Certificates issued by Digisign CA are prohibited from being used for uses not stated in Section 1.4.1.

1.5 Administrasi Kebijakan / *Policy Administration*

Policy Authority (PA) PSrE Digisign memiliki peran dan tanggung jawab sebagai berikut:

1. Menetapkan *Certificate Practice Statement* (CPS),
2. Memastikan semua layanan, operasional dan infrastruktur Digisign CA yang didefinisikan dalam CPS telah dilakukan sesuai dengan

Digisign CA Policy Authority (PA) roles and responsibilities are as follows:

1. *Establishing Certificate Practice Statement (CPS)*,
2. *Ensuring that all Digisign CA services, operations, and infrastructure defined in the CPS have been performed in accordance with Root's CA CP*

persyaratan, representasi, dan jaminan dari CP PSrE Induk, dan

3. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki tingkat verifikasi yang setara.

requirements, representations, and warranties, and

3. *Approval of the establishment of a relationship of trust with an external PKI that has equal level of verification.*

1.5.1 Organisasi Pengelola Dokumen / *Organization Administering the Document*

CPS dan dokumen referensi lainnya dikelola oleh Policy Authority (PA) PSrE Digisign.

CPS and other reference documents are maintained by the Digisign CA Policy Authority (PA).

1.5.2 Narahubung / *Contact Person*

Alamat	: PT Solusi Net Internusa (Digisign), Pasaraya Blok M Gedung B Lt. 4 Jalan Iskandarsyah II No. 2 RT.3/RW.1 Melawai, Kby. Baru, Kota Jakarta Selatan Jakarta 12160	*Address*	: *PT. Solusi Net Internusa (Digisign), Pasaraya Blok M Gedung B Lt. 4 Jalan Iskandarsyah II No. 2 RT.3/RW.1 Melawai, Kby. Baru, Kota Jakarta Selatan Jakarta 12160.*
Email	: corpsec@digi-id.id	*Email*	: *corpsec@digi-id.id*
URL	: https://digisign.id	*URL*	: *https://digisign.id*
Tel.	: +62 21 29101053	*Tel.*	: *+62 21 29101053*

1.5.3 Personil yang Menentukan Kesesuaian CPS dengan Kebijakan / *Person Determining CPS Suitability for the Policy*

Policy Authority (PA) dari PSrE Digisign menentukan kesesuaian dan penerapan CPS ini berdasarkan CP PSrE Induk. PA dibantu oleh tim legal dan kepatuhan serta menerima masukan dari peran terpercaya lainnya.

Policy Authority (PA) of Digisign CA determines suitability and implementation of this CPS based on Root CP. PA is assisted by legal and compliance as well as receiving inputs from other trusted roles.

1.5.4 Prosedur Persetujuan CPS / *CPS Approval Procedures*

PA PSrE Digisign dalam hal ini adalah personil yang menyetujui CPS. Amandemen / perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum.	*PA Digisign CA is the personnel who approves the CPS. Amendments / changes are made by changing the entire CPS or by publishing an addendum.*
PA PSrE Digisign menyetujui CPS PSrE Digisign dan segala perubahannya setelah mendapat persetujuan dari PA PSrE Induk. PA PSrE Digisign menentukan apakah amandemen / perubahan ke CPS ini memerlukan pemberitahuan atau perubahan OID.	*Digisign CA's PA approves the CPS of the Digisign CA and any amendments after the CPS is approved by Root CA's PA.* *PA Digisign CA determines whether amendments/changes to this CPS require notification or changes to the OID.*

1.6 Definisi dan dan Akronim / *Definitions and Acronyms*

Lihat tabel pada Lampiran A untuk akronim dan Lampiran B untuk definisi.	*Refer to table on Attachment A for acronyms and Attachment B for definitions.*

2. TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI / *PUBLICATION AND REPOSITORY RESPONSIBILITIES*

2.1 Repositori / *Repositories*

PSrE Digisign memelihara repositori daring yang bisa diakses publik termasuk namun tidak terbatas pada:

1. CPS PSrE Digisign,
2. Kebijakan Privasi PSrE Digisign,
3. Perjanjian Pemilik
4. Kebijakan Jaminan PSrE Digisign,
5. Perjanjian Pengandal,
6. Sertifikat PSrE Digisign, dan
7. CRL PSrE Digisign.
8. OCSP PSrE Digisign.

Digisign maintains a publicly accessible online repository including but not limited to:

1. *Digisign CA CPS,*
2. *Digisign CA Privacy Policy,*
3. *Subscriber Agreement,*
4. *Digisign CA WarrantyPolicy,*
5. *Relying Parties Agreement,*
6. *Digisign CA Certificate, and*
7. *Digisign CA CRL.*
8. *OCSP Digisign CA*

2.2 Publikasi Informasi Sertifikat / *Publication of Certification Information*

PSrE Digisign memelihara repositori yang dapat diakses melalui internet, tempat publikasi Sertifikat PSrE Digisign, CRL terakhir, dokumen CPS dan dokumen kebijakan lainnya. Repositori PSrE Digisign terletak di https://repository.digisign.id.

Digisign CA maintains a repository accessible via the internet, where Digisign CA Certificates are published, latest CRLs, CPS documents and other policy documents. The Digisign CA repository is located at https://repository.digisign.id.

2.3 Waktu atau Frekuensi Publikasi / *Time or Frequency of Publication*

CPS ini dan tiap perubahan selanjutnya dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui. PSrE Digisign mempublikasikan informasi CRL secara reguler dan terjadwal sebagaimana diatur dalam bagian 4.9.7.

This CPS and any subsequent amendments are publicly accessible within 7 (seven) calendar days after approval. Digisign CA publish the CRL information on a regular schedule as regulated in Section 4.9.7.

2.4 Kendali Akses pada Repositori / *Access Control on Repositories*

Informasi yang dipublikasikan pada repositori adalah informasi publik. PSrE Digisign memberikan akses baca yang tidak dibatasi pada repositorinya dan menerapkan kontrol logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut. PSrE Digisign melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

Information published on the repository is public information. Digisign CA grants unrestricted read access to its repositories and implements logical and physical controls to prevent unauthorized write access to those repositories. Digisign CA protects information that is not intended for public dissemination or modification by the public.

3. IDENTIFIKASI DAN AUTENTIKASI / *IDENTIFICATION AND AUTHENTICATION*

3.1 Penamaan / *Naming*

3.1.1 Tipe Nama / *Type of Names*

PSrE Digisign membuat dan menandatangani Sertifikat dengan subyek *Distinguished Name* (DN) yang non-null dan mematuhi standar ITU X.500.	*Digisign CA creates and signs a Certificate with a non-null subject Distinguished Name (DN) that complies with the ITU X.500 standard.*
Pengaturan parameter Sertifikat mengacu pada Standar Interoperabilitas PSrE Indonesia sebagaimana disampaikan pada Lampiran C.	*Further stipulations on Certificate parameters comply with Indonesian CA Interoperability Standard.*

3.1.2 Kebutuhan Nama yang Bermakna / *Need for Names to be Meaningful*

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 harus mengidentifikasi orang atau objek tersebut.	*Certificates issued in accordance with this CPS are meaningful only if the names appearing on the Certificate can be understood and used by the Relying Party. The name used in the Certificate must identify the person or object.*
Nama subyek dan penerbit yang terkandung dalam Sertifikat HARUS bermakna dalam arti bahwa PSrE Digisign memiliki bukti cukup yang menunjukkan keterkaitan antara nama dengan entitasnya. Untuk mencapai tujuan ini, penggunaan nama harus diotorisasi oleh Pemilik yang sah atau perwakilan legal dari Pemilik yang sah.	*The name of the subject and issuer contained in the Certificate MUST be meaningful in the sense that Digisign CA has sufficient evidence showing the relationship between the name and the entity. To achieve this purpose, use of the name must be authorized by the rightful Subscriber or the legal representative of the rightful Subscriber.*

3.1.3 Anonimitas atau Pseudonimitas Pemilik / *Anonymity or Pseudonymity of Subscribers*

PSrE Digisign tidak menerbitkan Sertifikat Pemilik yang anonim atau pseudonym.	*Digisign CA does not issue anonymous or pseudonymous Certificates*

3.1.4 Aturan Interpretasi Berbagai Bentuk Nama / *Rules for Interpreting Various Name Forms*

Distinguished Name (DN) dalam Sertifikat diinterpretasikan dengan menggunakan standar X.500.	*Distinguished Name (DN) in a Certificate is interpreted using X.500 Standard.*

3.1.5 Keunikan Nama / *Uniqueness of Names*

Distinguished Name (DN) dalam Sertifikat harus unik di dalam ranah PSrE Digisign, yang berarti keunikan nama tersebut harus sesuai dengan data yang dimasukkan oleh Pemilik. Pemilik bertanggung jawab penuh atas data yang didaftarkan dan harus akurat serta sesuai dengan data yang ada pada dokumen identitas.	*The Distinguished Name (DN) in the Certificate must be unique within the Digisign CA, which means the uniqueness of the name must match the data entered by the Subscriber. The Subscriber is fully responsible for the data registered and must be accurate and in accordance with the data in the identity document.*

3.1.6 Pengakuan, Autentikasi, dan Peran Merek Dagang / *Recognition, Authentication and Role of Trademarks*

Pemohon tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE Digisign tidak perlu memverifikasi hak pemohon untuk penggunaan merek dagang. Merupakan tanggung jawab Pemohon untuk memastikan penggunaan	*Applicants are not allowed to apply for a Certificate with content that violates the intellectual property rights of others. Digisign CA does not need to verify the applicant's rights to trademark use. It is the responsibility of the Applicant to ensure the use of validly chosen names.*

nama-nama pilihan yang sah.

PSrE Digisign dapat menolak setiap permohonan atau melakukan pencabutan Sertifikat apapun yang menjadi bagian dari sengketa merek dagang.	*Digisign CA may refuse any application or revoke any Certificate that is part of a trademark dispute.*

3.2 Validasi Identitas Awal / *Initial Identity Validation*

3.2.1 Metode Pembuktian Kepemilikan Kunci Privat */ Method to Prove Possession of Private Key*

Pasangan Kunci untuk Sertifikat Pemilik yang diterbitkan oleh PSrE Digisign dibuat dan diamankan menggunakan modul kriptografi yang memenuhi standar minimum Federal Information Protection Standards (FIPS) 140-2 Level 2.	*The Key Pair for Subscriber Certificate issued by Digisign CA is generated and secured using a cryptographic module that meets a minimum Federal Information Protection Standards (FIPS) 140-2 Level 2.*
PSrE Digisign membuktikan kepemilikan kunci privat Pemilik dengan terlebih dahulu memvalidasi status Sertifikat untuk memastikan Sertifikat masih aktif (belum kedaluwarsa atau tidak dicabut). Informasi pada Sertifikat dimanfaatkan untuk menelusuri Permintaan Penandatangan Sertifikat (*Certificate Signing Request*/CSR). PSrE Digisign melakukan verifikasi tanda tangan digital CSR dengan kunci publik CSR untuk membuktikan bahwa CSR dibuat dengan kunci privat yang berpasangan. Selanjutnya, kunci publik pada Sertifikat dan informasi antara Sertifikat dan CSR dibandingkan untuk membuktikan kesamaan pasangan kunci. PSrE Digisign	*Digisign CA proves the Owner's possession of the private key by first validating the Certificate status to ensure that the Certificate is still active (not expired or revoked). The information contained in the Certificate is used to trace the Certificate Signing Request (CSR). Digisign CA verifies the CSR's digital signature using the CSR public key to prove that the CSR was generated with the corresponding private key. Subsequently, the public key in the Certificate and the information between the Certificate and the CSR are compared to prove that they belong to the same key pair. Digisign CA verifies the chronological consistency of registration records, key pair*

memverifikasi konsistensi kronologis catatan pendaftaran, pembangkitan pasangan kunci, pembuatan CSR, dan penerbitan Sertifikat untuk memastikan integritas rantai pencatatan.

generation, CSR creation, and Certificate issuance to ensure the integrity of the recording chain.

3.2.2 Autentikasi Identitas Organisasi / *Authentication of Organization Identity*

Permohonan atas nama suatu organisasi harus dilakukan oleh seseorang yang berwenang mewakili organisasi tersebut, yaitu pemimpin tertinggi organisasi atau pihak lain yang kewenangannya dapat dibuktikan dengan surat kuasa.

Applications for an organization must be made by a person authorized to represent the organization, namely the highest leader of the organization or another person whose authority can be proven by a power of attorney.

Permohonan atas nama organisasi harus dilengkapi dengan dokumen atau informasi berikut:

1. Formulir pendaftaran Sertifikat;
2. Surat penugasan untuk perwakilan organisasi;
3. Identitas perwakilan sesuai dengan butir 3.2.3;
4. Akta Pendirian, Akta terakhir, dan bukti relevan yang menunjukkan bahwa akta tersebut telah didaftarkan di Kementerian Hukum dan Hak Asasi Manusia;
5. Dokumen Nomor Pokok Wajib Pajak (NPWP);
6. Email resmi organisasi.

Application for an organization must be accompanied with the following documents or information:

1. *Certificate registration form;*
2. *Assignment letter for the organization representative;*
3. *Identity of the representative in accordance with point 3.2.3;*
4. *Deed of Establishment, the latest Deed and the relevant evidence that is has been registered to the Ministry of Law and Human Rights;*
5. *Tax Identification Number Document;*
6. *Organization official email.*

Otoritas Pendaftaran melakukan verifikasi identitas organisasi dengan:

1. Memeriksa kelengkapan dan kebenaran

Registration Authority verifies the organization identity by

1. *Checking the completeness and*

semua dokumen dan/atau informasi yang diberikan;
2. Melakukan otentikasi identitas perwakilan sesuai dengan butir 3.2.3;
3. Memverifikasi keberadaan organisasi dengan membandingkan data pada basis data resmi pemerintah.

correctness of all the provided documents and/or information;
2. *Running authentication of representatives identity in accordance with 3.2.3;*
3. *Verifying organization existence by comparing with the database officially published by the government.*

PSrE Digisign tidak menerbitkan sertifikat kepada organisasi yang gagal dalam salah satu proses verifikasi di atas.

Digisign CA does not issue certificates to organizations that fail in any of the above verification.

3.2.3 Autentikasi Identitas Individu / *Authentication of Individual Identity*

Pemohon individu, baik Warga Negara Indonesia (WNI) maupun Warga Negara Asing (WNA) dapat mengajukan permohonan penerbitan Sertifikat kepada PSrE Digisign dengan menyampaikan persyaratan sebagai berikut:

Individual Applicants, both Indonesian Citizens (WNI) and Foreign Citizens (WNA), may apply for the issuance of a Certificate to Digisign CA by submitting the following requirements:

Warga Negara Indonesia (WNI)

PSrE Digisign menerbitkan Sertifikat elektronik untuk WNI, baik untuk kepentingan individu (personal) maupun berafiliasi dengan Badan Usaha atau Badan Hukum di Indonesia.

Indonesian Citizens (WNI)

Digisign CA issues electronic certificates for Indonesian citizens (WNI), either for individual (personal) purposes, or as affiliate with business entities or legal entities in Indonesia.

Pemohon WNI melengkapi permohonan penerbitan sertifikat dengan informasi sebagai berikut:

1. Persetujuan penerbitan sertifikat elektronik,
2. Salinan Kartu Tanda Penduduk (KTP),

WNI applicants must complete the certificate issuance application with the following information:

1. *Consent to the issuance of the electronic certificate,*
2. *A copy of the Identity Card (KTP),*

3. Foto wajah,
4. Nomor ponsel dan/atau alamat email.

3. *A facial photo,*
4. *Mobile phone number and/or email address.*

Pembuktian identitas Pemohon WNI dilakukan dengan memanfaatkan basis data yang disediakan oleh Kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional sesuai dengan Standar Verifikasi Identitas yang ditentukan oleh Kementerian Komdigi. Pembuktian identitas secara online disertai dengan deteksi *liveness*.

The identity verification of WNI applicants is carried out by utilizing the database provided by the Ministry responsible for national civil registration administration, in accordance with the Identity Verification Standards established by the Ministry of Komdigi. Online identity verification is accompanied by liveness detection.

Warga Negara Asing (WNA):

PSrE Digisign hanya menerbitkan Sertifikat elektronik untuk WNA yang terdaftar sebagai karyawan atau mendapatkan penugasan dari Badan Hukum atau Badan Usaha di Indonesia.

Foreign Citizens (WNA)

Digisign CA only issues electronic Certificates for foreign nationals who are registered as employees or assigned by a Legal Entity or Business Entity in Indonesia.

Pemohon WNA melengkapi permohonan penerbitan sertifikat dengan informasi sebagai berikut:

1. Persetujuan penerbitan sertifikat elektronik,
2. Salinan dokumen identitas berupa KTP/KITAS (Kartu Tanda Penduduk/Kartu Izin Tinggal Sementara) dan/atau Paspor. KITAS/KTP wajib untuk WNA yang berdomisili di Indonesia,
3. Surat permohonan dari institusi tempat Pemohon WNA bekerja atau mendapatkan penugasan

WNA applicants must complete the certificate issuance application with the following information:

1. *Consent to the issuance of the electronic certificate,*
2. *A copy of an identity document in the form of KTP/KITAS (Identity Card/Temporary Stay Permit) and/or Passport. KITAS/KTP is mandatory for WNA residing in Indonesia,*
3. *A request letter from the institution where the WNA applicant is employed or get assignment from,*

4. Foto wajah,
5. Nomor ponsel dan/atau alamat email.

4. *A facial photo,*
5. *Mobile phone number and/or email address.*

Pembuktian identitas Pemohon WNA dilakukan dengan cara sebagai berikut:

1. Pemeriksaan kelengkapan seluruh persyaratan, keabsahan seluruh informasi (antara lain masa berlaku dokumen identitas) dan tanda tangan Pemohon,
2. Otentikasi Badan Hukum atau Badan Usaha dibuktikan sesuai dengan butir 3.2.2.

Identity verification for WNA applicants is conducted as follows:

1. *Review of all required documents for completeness, validity of all information (including identity document expiration), and applicant's signature,*
2. *Legal Entity or Business Entity authentication is verified in accordance with clause 3.2.2.*

Apabila dimungkinkan (antara lain untuk WNA yang memiliki KTP), pembuktian identitas WNA dilakukan dengan memanfaatkan basis data yang disediakan oleh Kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional sesuai dengan Standar Verifikasi Identitas yang ditentukan oleh Kementerian Komdigi. Pembuktian identitas secara online disertai dengan deteksi *liveness*.

Where possible (e.g., for WNA holding an Indonesian Identity Card), identity verification of WNA is carried out by utilizing the database provided by the Ministry responsible for national civil registration administration, in accordance with the Identity Verification Standards established by the Ministry of Komdigi. Online identity verification is accompanied by liveness detection.

Otentikasi dan verifikasi identitas dilakukan dengan seizin Pemohon. PSrE Digisign menyimpan catatan tentang rincian proses otentikasi dan verifikasi setidaknya selama masa berlaku dari Sertifikat yang diterbitkan.

Authentication and identity verification are conducted with the applicant's consent. Digisign CA keeps a record of the details of the authentication and verification process for at least the validity period of the issued Certificate.

PSrE Digisign mempersyaratkan

Digisign CA requires biometric verification

pemeriksaan biometrik yang dilengkapi dengan deteksi *liveness*. Apabila proses ini mengalami kegagalan, Pemohon dapat mengajukan tatap muka secara *online* dengan RA dan tetap dianggap sebagai permohonan secara *online*.

with liveness detection. If this process fails, the applicant may request an online face-to-face session with the Registration Authority (RA), which will still be considered as an online application.

PSrE Digisign tidak menerbitkan sertifikat kepada Pemohon yang tidak dapat / gagal diverifikasi.

Digisign CA does not issue certificates to applicants who cannot be or fail to be verified.

3.2.4 Informasi Pemilik yang Tidak Terverifikasi / *Non-verified Subscriber Information*

PSrE Digisign tidak menerbitkan Sertifikat untuk Pemohon Sertifikat terhadap informasi yang tidak dapat diverifikasi.

Digisign CA does not issue Certificates to Certificate Applicants against information that cannot be verified.

3.2.5 Validasi Otoritas / *Validation of Authority*

Validasi Otoritas melibatkan penentuan apakah seseorang memiliki hak khusus, hak, atau izin khusus, termasuk izin untuk bertindak atas nama organisasi untuk mendapatkan Sertifikat.

Validation Authority involves determining whether a person has special rights, rights, or permissions, including permission to act on behalf of the organization to obtain a Certificate.

Sertifikat yang mengandung afiliasi keorganisasian secara eksplisit atau implisit hanya dapat diterbitkan setelah memastikan bahwa Pemohon adalah benar memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan organisasinya.

Certificates containing explicit or implicit organizational affiliations may only be issued after confirming that the Applicant is properly authorized to act in the capacity conferred by his organization.

PSrE Digisign bertanggung jawab untuk memverifikasi dan mengautentikasi perwakilan resmi yang sah secara hukum

Digisign CA is responsible for verifying and authenticating a legally authorized representative by examining the following

dengan memeriksa dokumen berikut:

1. Surat dari pihak yang memiliki wewenang, dan
2. Dalam hal pemilik wewenang tidak dapat mewakili, maka orang yang ditunjuk oleh organisasi untuk mewakili organisasi harus menyampaikan Surat Penunjukan Perwakilan Resmi.

documents:

1. *Letter from the authorized party, and*
2. *If the authorized party is unable to represent, the person appointed by the organization to represent the organization must submit a Letter of Appointment of Authorized Representative.*

3.2.6 Kriteria Inter-operasi / *Criteria for Interoperation*

Tidak ada ketentuan.

Not stipulated.

3.3 Identifikasi dan Otentikasi untuk Permintaan Penggantian Kunci (*Rekey*) / *Identification and Authentication for Rekey Requests*

3.3.1 Identifikasi dan Autentikasi untuk Rekey Rutin / *Identification and Authentication for Routine Rekey*

Sebelum masa berlaku Sertifikat berakhir, Pemilik dapat meminta penggantian kunci yang selanjutnya disebut *rekey* dan Pemilik harus diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau menggunakan proses pemeriksaan identitas awal sebagaimana diatur pada Bagian 3.2.

Prior to the expiry of a Certificate, Subscribers may request for a rekey and Subscribers shall be authenticated through signing using their current Certificates or by using the initial identity-proofing process as described in Section 3.2.

3.3.2 Identifikasi dan Autentikasi untuk Rekey setelah Pencabutan / *Identification and Authentication for Rekey After Revocation*

Setelah pencabutan Sertifikat, Pemilik harus

After a Certificate has been revoked other

mengulang proses pendaftaran sebagaimana diatur pada bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

than during a renewal action, the Subscriber is required to go through the initial registration process described in section 3.2 to obtain a new Certificate with new keys.

3.4 Identifikasi dan Autentikasi untuk Permintaan Pencabutan / *Identification and Authentication for Revocation Request*

Permintaan pencabutan Sertifikat selalu diautentikasi. Permintaan untuk mencabut Sertifikat di autentikasi dengan menggunakan atribut pengidentifikasian yang terhubung dengan Sertifikat serta formulir permohonan pencabutan yang ditandatangani dengan tanda tangan elektronik oleh Pemilik.

Subscriber Certificate revocation requests always be authenticated. A request to revoke a Certificate is authenticated by using identification attribute(s) linked to the Certificate and the revocation request form which is signed by an electronic signature of the Subscriber.

4. PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT / *CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS*

4.1 Permohonan Sertifikat / *Certificate Application*

4.1.1 Siapa yang Dapat Mengajukan Sebuah Permohonan Sertifikat / *Who can Submit a Certificate Application*

Permohonan dari WNI dan WNA (individu) hanya dapat dilakukan oleh individu tersebut atau oleh orang lain atau organisasi yang secara resmi berwenang untuk mewakilinya. Permohonan dari Badan Hukum/ Badan Usaha diajukan oleh orang yang berwenang mewakili Badan Usaha tersebut.	*Applications from individual WNI or WNA may only be made by himself, or by another person or organization that legally has the authority to represent him. Application from Legal Organization/ Business Entities must be submitted by a person authorized to represent the Business Entity.*
Pemohon merupakan individu yang bertindak untuk kepentingan dirinya sendiri atau orang yang ditunjuk oleh suatu organisasi non-instansi / badan usaha (Admin Badan Usaha).	*The Applicant is an individual acting for personal purposes, or authorized person by legal non-Government organization/ business entity (Admin Corporate).*

4.1.2 Proses Pendaftaran dan Tanggung Jawab / *Enrollment Process and Responsibilities*

Pemohon Sertifikat bertanggung jawab untuk memberikan informasi yang akurat dalam mengisi informasi pada halaman permohonan Sertifikat.	*The Certificate Applicant is responsible for providing accurate information in filling out all fields on the Certificate application page.*
Secara umum, proses pendaftaran terdiri dari langkah-langkah berikut: 1. Mengisi dan melengkapi data pribadi. 2. Menyetujui Kebijakan Privasi,	*Generally, the registration process consists of the following steps:* *1. Fill out and complete personal data.* *2. Agreement to the Privacy Policy,*

Perjanjian Kepemilikan Sertifikat dan Kebijakan Jaminan,

3. PSrE Digisign dapat menolak permohonan Sertifikat dari pemohon yang sebelumnya melanggar kebijakan PSrE Digisign, dan
4. PSrE Digisign tidak wajib untuk memberikan alasan kepada Pemohon terkait permohonan Sertifikat yang ditolak.

Subscriber Agreement and Warranty Policy,

3. *Digisign CA may refuse Certificate applications from applicants who previously violated Digisign CA policies, and*
4. *Digisign CA is not under any obligation to provide reasons to the Applicant regarding the rejected Certificate application.*

PSrE Digisign bertanggung jawab atas pemeliharaan sistem dan proses autentikasi identitas Pemohon untuk setiap jenis Sertifikat, dan dapat menampilkan identitas Pemilik Sertifikat kepada Pengandal. PSrE Digisign juga bertanggung jawab atas penyimpanan informasi Data Pribadi Pemohon ketika melakukan proses pendaftaran Sertifikat.

Digisign CA is responsible for maintaining systems and processes that authenticate the identity of the Applicant for each type of Certificate and can display the identity of the Subscriber Certificate to the Relying Party. Digisign CA is also responsible for storing Applicant's Personal Data information when carrying out the Certificate registration process.

4.2 Pemrosesan Permohonan Sertifikat / *Certificate Application Processing*

4.2.1 Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi / *Performing identification and Authentication Functions*

Pemohon wajib memenuhi persyaratan identifikasi dan autentikasi untuk memastikan bahwa Pemohon adalah orang yang tepat dan sesuai dengan data yang didaftarkan sebagaimana tercantum pada bagian 3.2 CPS ini.

The Applicant shall meet the identification and authentication requirements to ensure that the Applicant is the correct person and matches the registered data as set out in section 3.2 of this CPS.

PSrE Digisign memastikan bahwa Pemohon memenuhi persyaratan identifikasi dan

Digisign CA ensures that the Applicant meets the identification and authentication

autentikasi sehingga Pemohon adalah orang yang tepat dan sesuai dengan data yang didaftarkan sebagaimana tercantum pada bagian 3.2 CPS ini.

requirements to ensure that the Applicant is the correct person and matches the registered data as set out in section 3.2 of this CPS.

4.2.2 Persetujuan atau Penolakan Permohonan Sertifikat / *Approval or Rejection of Certificate Applications*

Persetujuan atas permohonan Sertifikat dapat dilakukan setelah seluruh rangkaian pendaftaran berhasil dilakukan sebagaimana diatur pada Bagian 4.1. dan data yang didaftarkan sesuai dengan hasil verifikasi dan autentikasi dengan sumber data dari instansi yang berwenang.

Approval of the certificate application can be made after the entire series of registrations is successful with requirements stipulated in Section 4.1 and the data registered is in accordance with the results of verification and authentication with data sources from the authorized agency.

Setelah semua pemeriksaan identitas dan atribut Pemohon, Permohonan dapat tidak disetujui atau ditolak jika:

1. data mengandung kesalahan, tidak sesuai atau tidak akurat, dan
2. data tidak dapat diverifikasi di sumber data.

After all identity verification and applicant attribute checks, the application may be either approved or rejected due to:

1. *The data contains errors, is inappropriate or inaccurate, and*
2. *The data cannot be verified in the data source.*

Apabila terdapat ketidaksesuaian data maka dilakukan proses ulang. Bila data tersebut dapat disesuaikan dan setelah pemeriksaan kembali dinyatakan sesuai, maka permohonan Sertifikat dapat disetujui.

If there is a data discrepancy, the data is re-processed. If the data can be adjusted and after re-examination it is declared appropriate, then the certificate application can be approved.

Apabila masih terdapat ketidaksesuaian pada data setelah penyesuaian dilakukan, maka permohonan sertifikat tidak dapat disetujui.

If there are still discrepancies in the data after the adjustments are made, the certificate application cannot be approved.

4.2.3 Waktu untuk Memproses Permohonan Sertifikat / Time to Process Certificate Applications

PSrE Digisign memastikan permohonan Sertifikat diproses tepat waktu. Sertifikat diterbitkan setelah proses verifikasi dan autentikasi berhasil serta Pemohon telah menyetujui Kebijakan Privasi, Perjanjian Kepemilikan Sertifikat dan Kebijakan Jaminan. Proses ini memerlukan waktu tidak lebih dari 24 (dua puluh empat) jam.

Digisign CA ensures that Certificate applications are processed on time. Certificates are issued after the verification and authentication process is successful and the Applicant has agreed to the Privacy Policy, Subscriber Agreement and Warranty Policy. This process takes no more than 24 (twenty four) hours.

4.3 Penerbitan Sertifikat / *Certificate Issuance*

4.3.1 Tindakan PSrE Digisign Selama Penerbitan Sertifikat / Digisign CA Actions During Certificate Issuance

PSrE Digisign melakukan tindakan-tindakan sebagai berikut:

1. Memastikan identitas Pemohon sebagaimana diatur pada Bagian 3.2.2 dan 3.2.3,
2. Memverifikasi otoritas Pemohon 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 Pemilik setelah Pemilik secara formal menyetujui kewajibannya

Digisign CA perform the following actions:

1. *Ensure the Applicant's identity as regulated in Section 3.2.2 and 3.2.3,*
2. *Verify the Applicant's authority as regulated in Section 3.2.5,*
3. *Prepare and signs Certificates after all requirements have been fulfilled,*
4. *Ensure Indonesian CA received the Certificate as regulated in Section 4.4,*
5. *Make the Certificate available to the Subscriber after the Subscriber formally agrees to their obligations as*

sebagaimana diatur pada Bagian 9.6.3.	*regulated in Section 9.6.3.*

4.3.2 Pemberitahuan ke Pemilik oleh PSrE Digisign tentang Diterbitkannya Sertifikat / *Notification to Subscriber by Digisign CA of Issuance of Certificate*

Tergantung pada jenis Sertifikat, PSrE Digisign dan/atau RA akan memberitahukan Pemilik Sertifikat mengenai penerbitan Sertifikat melalui email, nomor telepon, atau cara pemberitahuan lainnya dalam waktu paling lambat 1x24 jam.	*Depending on the Certificate type, Digisign CA and/or RA shall notify the Subscriber on the issuance of a Certificate via email or phone number or other means within 1x24 hours.*

4.4 Pernyataan Persetujuan Sertifikat / *Certificate Acceptance*

4.4.1 Sikap Yang Dianggap Sebagai Menyetujui Sertifikat / *Conduct Constituting Certificate Acceptance*

Pemilik harus memeriksa semua informasi Sertifikat sebelum menggunakan Sertifikat tersebut. Pemilik dianggap telah menyetujui semua informasi sertifikat apabila telah ada bukti bahwa pemilik telah menggunakan sertifikatnya atau tidak menyampaikan keluhan dalam jangka waktu 7 (tujuh) hari kerja.	*The Subscriber must check all Certificate information before using the Certificate. Subscriber is deemed to have agreed on all Certificate information if there is evidence that Subscriber has used the certificate or if no complaint is received from the Subscriber within 7 (seven) working days.*
Apabila Pemegang Sertifikat memiliki keluhan terhadap informasi yang tertera pada Sertifikat, maka Pemegang Sertifikat mengajukan permohonan pencabutan Sertifikat sesuai ketentuan yang diatur pada bagian 4.9. melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Digisign di situs web PSrE Digisign.	*If the Subscriber has a complaint about the information contained in the Certificate, the Subscriber submits a Certificate revocation request in accordance with the provisions set out in section 4.9. through the communication media provided by Digisign CA on Digisign CA website.*

4.4.2 Publikasi Sertifikat oleh PSrE Digisign / *Publication of the Certificate by Digisign CA*

Sertifikat PSrE Digisign dapat diunduh pada repositori PSrE Digisign sebagaimana dimaksud Bagian 2.2.	*Digisign CA Certificates can be downloaded at Digisign CA's repository as stated on Section 2.2.*
PSrE Digisign tidak mempublikasikan Sertifikat Pemilik.	*Digisign CA does not publish Subscriber Certificates.*

4.4.3 Pemberitahuan Penerbitan Sertifikat oleh PSrE Digisign ke Entitas Lain / *Notification of Certificate Issuance by Digisign CA to Other Entities*

Tidak ada ketentuan.	*No Condition*.

4.5 Penggunaan Pasangan Kunci dan Sertifikat / *Key Pair and Certificate Usage*

4.5.1 Penggunaan Kunci Privat dan Sertifikat oleh Pemilik / *Subscriber Private Key and Certificate Usage*

Pemilik mengendalikan dan mempercayakan Kunci Privat mereka kepada PSrE Digisign. PSrE Digisign menjaga dan mengambil langkah-langkah keamanan yang wajar untuk melindungi Kunci Privat tersebut dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS 140-2.	*The Subscribers control and entrust their Private Key to Digisign CA. DIgisign CA safeguards and take reasonable security measures to protect the Private Keys using cryptographic modules that meet the requirements of FIPS 140-2.*
PSrE Digisign menerapkan minimal dua faktor autentikasi bagi Pemilik untuk dapat menggunakan Kunci Privat yang disimpan di PSrE Digisign. Pemilik wajib melindungi parameter autentikasi dan hanya boleh	*Digisign CA enforces a minimum of two-factors of authentication for Subscribers to use the Private Key stored in Digisign CA. The Subscribers must protect the authentication parameters and shall only*

menggunakan Kunci Privat mereka sesuai dengan tujuan yang telah ditetapkan. Tujuan penggunaan tersebut didefinisikan melalui ekstensi Sertifikat, yang ditentukan dalam KeyUsage dan/atau ExtendedKeyUsage.

use their Private Key for the designated purpose. The intended usage is defined through Certificate extensions, specified within KeyUsage and/or ExtendedKeyUsage.

4.5.2 Penggunaan Kunci Publik dan Sertifikat oleh Pengandal / *Relying Party Public Key and Certificate Usage*

Pengandal menggunakan perangkat lunak yang sesuai dengan X.509. PSrE Digisign menentukan pembatasan dan cakupan dari penggunaan Sertifikat melalui Sertifikat ekstensi dan menentukan mekanisme untuk menentukan validitas Sertifikat (CRL dan OCSP). Pengandal memproses dan mengikuti / mematuhi informasi ini sesuai dengan kewajibannya sebagai Pengandal.

Relying Parties use X.509 compliant software. Digisign CA determines the limitations and scope of use of Certificates via Certificate extensions and defines a mechanism for determining Certificate validity (CRL and OCSP). The Relying Party processes and follows / complies with this information in accordance with its obligations as a Relying Party.

Pengandal harus berhati-hati ketika mengandalkan Sertifikat dengan mempertimbangkan keseluruhan keadaan dan risiko kerugian sebelum mengandalkan Sertifikat atau tanda tangan elektronik. Pengandal bertanggung jawab atas risiko mengandalkan sertifikat elektronik atau tanda tangan elektronik yang belum diperiksa sesuai standar. Jika keadaan menunjukkan bahwa diperlukan jaminan tambahan, Pengandal mendapatkan jaminan tersebut sebelum menggunakan Sertifikat dan dapat dilihat pada dokumen Perjanjian Pengandal yang ada pada dokumen repositori PSrE Digisign.

Relying Parties shall exercise caution when relying on Certificates and consider the overall circumstances and risks of loss before relying on Certificates or electronic signatures. The Relying Party is responsible for risks in relying on electronic certificates or electronic signatures that have not been checked in accordance with the standards. If circumstances indicate that additional guarantees are required, the Relying Party obtains such guarantees before using the Certificate and can be found in the Relying Parties Agreement document contained in the Digisign CA repository document.

4.6 Pembaruan Sertifikat / *Certificate Renewal*

4.6.1 Kondisi Untuk Pembaruan Sertifikat / *Circumstance for Certificate Renewal*

Pembaruan Sertifikat (renewal) adalah penerbitan Sertifikat baru dengan menggunakan nama, kunci, dan informasi yang sama dengan Sertifikat lama yang belum kedaluwarsa, namun masa berlaku dan serial number Sertifikat yang diperbarui.

Certificate renewal is an issuance of a new Certificate with similar name, keys, and information with the older unexpired Certificate, but with updated validity and serial number.

Pembaruan Sertifikat Pemilik ini dapat dilakukan oleh PSrE Digisign selama:

1. Sertifikat Pemilik lama yang akan diperbarui belum dicabut atau belum terkompromi,
2. Semua rincian dalam Sertifikat Pemilik tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi, dan
3. PSrE Digisign dapat memperbarui Sertifikat Pemilik yang sudah pernah diperbarui sebelumnya.

Digisign CA may renew a Certificate as long as:

1. *The original Subscriber Certificate to be renewed has not been revoked,*
2. *All details within the Subscriber Certificate remain accurate and no new or additional validation is required, and*
3. *Digisign CA may renew Subscriber Certificates which have either been previously renewed.*

Pembaruan Sertifikat Pemilik dengan key usage *digitalSignature* (tanda tangan digital) dan *nonRepudiation* (nirsangkal) hanya diperbolehkan ketika umur kunci belum melampaui ketentuan sebagaimana diatur pada Bagian 6.3.2.

Certificate renewal for Subscribers' Certificate with key usage of digitalSignature (digital signature) and nonRepudiation (non repudiation) is permitted only when the Keys' lifetime does not exceed the stipulation in Section 6.3.2.

4.6.2 Siapa Yang Dapat Meminta Pembaruan / *Who May Request Renewal*

Pemilik yang belum pernah dicabut

Subscribers who previously never had their

Sertifikatnya boleh meminta pembaruan Sertifikatnya ke PSrE Digisign melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Digisign di situs web PSrE Digisign.	*Certificate revoked may request a renewal of their Certificate from Digisign CA through the communication media provided by Digisign CA on Digisign CA website.*

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat / *Processing Certificate Renewal Request*

PSrE Digisign mengikuti prosedur sebagaimana diatur pada Bagian 4.3.	*Digisign CA follows the procedures as stipulated in Section 4.3.*

4.6.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik / *Notification of New Certificate Issuance to Subscriber*

Sama seperti prosedur penerbitan Sertifikat baru seperti pada bagian 4.3.2.	*Certificate renewal must be achieved using the initial registration process as in section 4.3.2.*

4.6.5 Sikap yang Dianggap Sebagai Menyetujui Pembaruan Sertifikat / *Conduct Constituting Acceptance of a Renewal Certificate*

Pemilik menyetujui Sertifikat baru sesuai prosedur penerimaan Sertifikat pada bagian 4.4.1.	*Subscriber agrees to the renewed Certificate according to the procedures stated in section 4.4.1.*

4.6.6 Publikasi Pembaruan Sertifikat oleh PSrE Digisign / *Publication of Renewal Certificate by Digisign CA*

Sertifikat baru dipublikasikan sesuai ketentuan sebagaimana diatur pada Bagian 4.4.2.	*The new Certificate is published according to the procedures stated in Section 4.4.2.*

4.6.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE Digisign ke Entitas Lain / *Notification of Certificate Issuance by Digisign CA to Other Entities*

Tidak ada ketentuan.	*No stipulation.*

4.7 *Rekey* Sertifikat / *Certificate Rekey*

4.7.1 Kondisi *Rekey* Sertifikat / *Circumstance for Certificate Rekey*

Penerbitan ulang Sertifikat dengan penggantian kunci (*rekey*) adalah pembuatan/penerbitan Sertifikat baru dengan Kunci Publik, *serial number*, *dan key identifier* yang baru, sementara informasi pribadi Pemilik yang terverifikasi dalam Sertifikat baru masih sama dengan Sertifikat lama. Sertifikat baru diisi masa berlaku yang baru, dan/atau diisi dengan tempat publikasi CRL yang baru, dan/atau ditandatangani dengan kunci yang baru.	*Re-issuing Certificates with rekey consists of creating new Certificates with a new Public Key, serial number and key identifier while retaining the remaining other information in the old certificate that describe the Subject/Subscriber. The new Certificate is assigned a new validity period, and/or specifies a new CRL distribution point, and/or be signed with a different key.*
Pemilik dapat melakukan *rekey* selama Sertifikat yang akan diterbitkan memiliki karakteristik (misalnya *key usage*) dan level verifikasi yang sama dengan Sertifikat yang lama.	*Subscribers may rekey Certificate if the new Certificate has the same characteristics (including key usage) and the same verification level as the older one.*
PSrE Digisign melakukan *rekey* bagi Pemilik selama: 1. Sertifikat lama yang akan diganti belum dicabut, terkompromi, atau kedaluwarsa, 2. PSrE Digisign menerbitkan Sertifikat baru kepada Pemilik setelah Pemilik memberi persetujuan untuk	*Digisign CA rekey Subscribers' Certificate as long as:* 1. *The old Certificate to be rekeyed has not been revoked, compromised, or expired,* 2. *Digisign CA issues new Certificate to the Subscribers after the Subscriber has given approval to a generation of a*

pembangkitan Pasangan Kunci baru dan terasosiasi dengan Sertifikat tersebut, dan

new Key Pair and is associated to the Certificate, and

3. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi.

3. All details within the Certificate remain accurate and no new or additional validation is required.

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

If the Subscriber's Private Key is compromised or expired or revoked, Subscribers may submit a new Certificate application as described in Section 4.1.

4.7.2 Pihak yang Dapat Meminta *Rekey* Sertifikat / *Who May Request Certification of a New Public Key*

Permintaan Rekey hanya dapat dilakukan oleh Pemilik melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Digisign di situs web PSrE Digisign.

Rekey Requests can only be made by the Subscriber through the communication media provided by Digisign CA on Digisign CA website.

4.7.3 Pemrosesan Permintaan *Rekey* Sertifikat / *Processing Certificate Rekeying Requests*

PSrE Digisign mengikuti prosedur sebagaimana diatur pada Bagian 3.3 dan 4.3.

Digisign CA follows procedures stated in Sections 3.3 and 4.3.

PSrE Digisign menggunakan masa berlaku Sertifikat baru yang sama seperti masa berlaku Sertifikat sebelumnya.

Digisign CA uses a similar validity period for the new Certificate to the older Certificate.

4.7.4 Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik / *Notification of New Certificate Issuance to Subscriber*

PSrE Digisign melakukan pemberitahuan penerbitan Sertifikat baru kepada Pemilik sebagaimana diatur pada Bagian 4.3.2.	*Digisign CA notifies issuance of a new Certificate to the Subscriber as regulated in Section 4.3.2.*

4.7.5 Sikap yang Dianggap Sebagai Menyetujui Sertifikat yang di Rekey / *Conduct Constituting Acceptance of a Rekeyed Certificate*

Pemilik menyetujui Sertifikat yang telah diperbarui sesuai dengan prosedur sebagaimana diatur pada Bagian 4.4.1.	*The subscriber agrees to the rekeyed Certificate in accordance with the procedure described in Section 4.4.1.*

4.7.6 Publikasi Sertifikat yang di *Rekey* oleh PSrE Digisign / *Publication of the Rekeyed Certificate by Digisign CA*

Sertifikat *rekey* dipublikasikan sesuai ketentuan yang diatur pada Bagian 4.4.2.	*The rekeyed Certificate is published according to the stipulation in section 4.4.2.*

4.7.7 Pemberitahuan Penerbitan Sertifikat oleh PSrE Digisign ke Entitas Lain / *Notification of Certificate Issuance by Digisign CA to Other Entities*

Tidak ada ketentuan	*No stipulation.*

4.8 Modifikasi Sertifikat / *Certificate Modification*

Modifikasi rincian Sertifikat tidak diizinkan. Dalam hal terjadi kesalahan selama penerbitan Sertifikat (contohnya ejaan), Sertifikat yang sudah terbit dicabut dan diikuti dengan proses penerbitan Sertifikat sebagaimana diatur pada Bagian 4.3.	*Modification of Certificate details is not permitted. In case there is a mistake during Certificate issuance (e.g., spelling), the Certificate is revoked and the rekey issuance process is followed, as stated in Section 4.3.*

4.9 Pencabutan dan Pembekuan Sertifikat / *Certificate Revocation and Suspension*

4.9.1 Kondisi untuk Pencabutan / *Circumstances for Revocation*

PSrE Digisign mencabut Sertifikat Pemilik dalam keadaan berikut:

1. Komponen informasi yang berafiliasi dengan nama dalam Sertifikat menjadi tidak valid,
2. Informasi apa pun dalam sertifikat menjadi tidak valid,
3. Pemilik dapat dibuktikan telah melanggar ketentuan peraturan perundang-undangan,
4. Ada alasan untuk percaya bahwa kunci privat telah *compromise* / rusak / hilang,
5. Pemilik atau pihak berwenang (sesuai ketentuan Peraturan Perundang-undangan semisal kepolisian, kejaksaan, perintah pengadilan) meminta agar Sertifikatnya dicabut sebagaimana diatur Bagian 4.9.2,
6. Penghentian operasional PSrE Digisign,
7. Pemilik sudah tidak bisa lagi menggunakan Sertifikat (misal: meninggal - salinan sertifikat kematian harus ditunjukkan ke PSrE).

Digisign CA revokes Subscriber's Certificate in the following circumstances:

1. *Identifying information or affiliation components of any names in the certificate becomes invalid,*
2. *Any information in the certificate becomes invalid,*
3. *Subscriber proved to have violated the provisions of the legislation,*
4. *Grounds for reason that the private key has been compromised / damaged / lost,*
5. *Subscriber or authorities (according to the provisions of the Laws and Regulations such as police, attorney, court order) request that the Certificate be revoked as governed on Section 4.9.2,*
6. *Decommissioning of Digisign CA,*
7. *Subscriber is not able to use Certificate (Death - copy of Death certificate made available to the issuing CA).*

Sertifikat yang dicabut ditempatkan di CRL dan ditambahkan pada responder OCSP. Sertifikat yang dicabut disertakan pada

The Certificate revocation information is placed in the CRL and added to an OCSP responder. The revoked certificate is

semua publikasi baru pada informasi status Sertifikat sampai Sertifikat kedaluwarsa.

included in all new publications of the Certificate status information until the Certificate expires.

Kondisi untuk pencabutan Sertifikat Pemilik diatur dalam Prosedur Pencabutan Sertifikat.

Circumstances for revocation of Subscribers Certificate are regulated in Certificate Revocation Procedure.

4.9.2 Pihak yang Dapat Meminta Pencabutan / *Who can Request Revocation*

Permintaan pencabutan Sertifikat dapat dilakukan oleh:

1. Pemilik, atau
2. Pihak berwenang sebagaimana dimaksud pada Bagian 3.2.5. atau
3. Pihak lainnya yang diberikan kewenangan oleh hukum, ketentuan peraturan perundang-undangan, atau perintah pengadilan

Certificate revocation may be requested by:

1. *Subscriber, or*
2. *Authorized parties as stipulated in section 3.2.5., or*
3. *Parties authorized by laws and regulations or judicial order*

Permintaan pencabutan Sertifikat disampaikan secara resmi kepada PSrE Digisign melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Digisign di situs web PSrE Digisign.

The request for certificate revocation is formally submitted to Digisign CA through the communication channels provided and designated by Digisign on its CA website.

4.9.3 Prosedur Permintaan Pencabutan / *Procedure for Revocation Request*

PSrE Digisign memverifikasi identitas dan wewenang pihak yang meminta pencabutan Sertifikat. Validasi identitas dan wewenang pihak yang meminta pencabutan dibutuhkan sebagaimana diatur Bagian 3.2.5 dan 3.4.

Digisign CA verifies the identity and authority (for juridical entity) of a Subscriber making the request for revocation. The validation of the subscriber's identity and authority is required according to Section 3.2.5 and 3.4.

Permintaan pencabutan Sertifikat oleh Pemilik harus menyerahkan bukti bahwa:

1. Kunci Privat Sertifikat telah terungkap,
2. Penggunaan Sertifikat tidak sesuai dengan CPS PSrE Digisign, atau
3. Terdapat alasan relevan lain yang diberikan oleh Pemilik.

Certificate revocation request by Subscriber shall attach evidences that:

1. *The Certificate's Private Key has been Exposed,*
2. *The usage of the Certificate is not conform with CPS Digisign CA, or*
3. *Any other relevant reasons for revocation by the Subscriber.*

Permintaan pencabutan Sertifikat oleh pihak yang lainnya harus menyerahkan bukti bahwa:

1. Kunci Privat Sertifikat telah terungkap,
2. Penggunaan Sertifikat tidak sesuai dengan CP Induk dan CPS PSrE Digisign, Perjanjian Pemilik/Kontrak Berlangganan, dan perjanjian lainnya, atau
3. Pemilik sudah tidak terasosiasi dengan institusi yang bersangkutan

Request for revocation by entity must have submission of proof that:

1. *The Private Key of the Certificate has been exposed,*
2. *The use of the Certificate does not conform to the CPS, Subscriber Agreement, and other agreements, or*
3. *The Certificate Subscriber's relationship with the institution does not exist.*

Permintaan pencabutan juga bisa dilakukan oleh pihak berwenang dengan mengisi formulir permintaan pencabutan untuk seseorang dan menyertakan surat perintah resmi.

Requests for revocation can also be made by the authority by filling out a request for revocation for someone and attaching an official warrant.

4.9.4 Masa Tenggang Permintaan Pencabutan / *Revocation Request Grace Period*

Tidak ada masa tenggang untuk pencabutan dalam kebijakan ini. Pihak yang disebutkan di Bagian 4.9.2 meminta pencabutan segera setelah mengidentifikasi

There is no grace period for revocation under this policy. The parties identified in Section 4.9.2 who request for revocation promptly after identifying the need for

perlunya pencabutan sertifikat	*revocation.*

4.9.5 Tenggat Waktu Dimana PSrE Harus Memproses Permintaan Pencabutan / *Time Within which CA Must Process the Revocation Request*

PSrE Digisign melakukan upaya terbaik untuk memproses permintaan pencabutan Sertifikat dalam waktu 2 (dua) hari kerja setelah permohonan pencabutan yang valid diterima.	*Digisign CA makes the best efforts to process revocation requests within 2 (two) business days after a valid revocation request is received.*
PSrE Digisign memproses pencabutan sertifikat sehingga dapat dipublikasikan pada CRL, kecuali jika permintaan tersebut diterima dan disetujui dalam waktu kurang dari 2 (dua) jam sebelum penerbitan CRL berikutnya.	*Digisign CA processes revocation requests so that the revocation can be published on the next CRL, unless the revocation request is accepted and approved within 2 (two) hours before the next CRL release.*

4.9.6 Persyaratan Pemeriksaan Pencabutan bagi Pengandal / *Revocation Checking Requirement for Relying Parties*

Penggunaan Sertifikat yang sudah dicabut dapat menimbulkan kerugian bagi Pengandal. Oleh karena itu, Pengandal harus memvalidasi Sertifikat terhadap CRL dan/atau OCSP milik PSrE Digisign yaitu: 1. pemeriksaan CRL dilakukan minimal 1x24 jam setelah proses pencabutan dilakukan, dan/atau 2. pemeriksaan OCSP dilakukan 1 jam setelah proses pencabutan dilakukan.	*The use of revoked Certificate may cause detriment to Relying Parties. Therefore, Relying Parties must validate Certificates with the Digisign CA's CRL and/or OCSP:* *1. CRL verification is performed within 24 hours after revocation, and/or* *2. OCSP verification is performed within 1 hour after revocation,*
Frekuensi validasi Sertifikat terhadap CRL dan/atau OCSP milik PSrE ditentukan oleh Pengandal.	*The frequency for Certificate validation is determined by the Relying Parties*

4.9.7 Frekuensi Penerbitan CRL / *CRL Issuance Frequency*

CRL akan diperbarui secara berkala dalam jangka waktu 1 x 24 jam dan dapat diakses melalui Repositori https://repository.digisign.id/	*CRL will be updated regularly within 1x 24 hours and can be accessed through the Repository* https://repository.digisign.id.
Untuk pencabutan Sertifikat Pemilik, waktu *nextUpdate* pada CRL PSrE Digisign paling lambat 72 (tujuh puluh dua) jam setelah waktu penerbitan (*thisUpdate time*). Repositori untuk mengakses CRL terlindungi untuk memastikan integritas dan keasliannya.	*For Subscriber Certificate's revocation, the value for nextUpdate field in Digisign CA's CRL is no later than 72 (seventy two) hours after the issuance time (thisUpdate time).* *Repositories for accessing CRLs are protected to ensure their integrity and authenticity.*

4.9.8 Latensi Maksimum CRL / *Maximum Latency for CRLs*

PSrE Digisign mempublikasikan data pencabutan Sertifikat selambat lambatnya dalam waktu 30 (tiga puluh) menit setelah CRL diperbarui.	*Digisign CA publishes Certificate revocation data no later than 30 (thirty) minutes after the CRL has been updated.*

4.9.9 Ketersediaan Pemeriksaan Pencabutan/Status secara Daring / *Online Revocation/Status Checking Availability*

PSrE Digisign memberikan layanan pengecekan informasi status Sertifikat secara daring sesuai daftar repositori sebagaimana tertera pada bagian 2.2. diluar waktu pemeliharaan sistem PSrE Digisign.	*Digisign CA provides an online validation service as listed on repository as described in section 2.2. outside the maintenance window of Digisign CA system.*

4.9.10 Persyaratan Pemeriksaan Pencabutan secara Daring / *Online Revocation Checking Requirements*

Semua layanan pengecekan informasi status sertifikat sesuai dengan standar *Internet Engineering Task Force* (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas. Daftar semua responder OCSP yang dioperasikan PSrE DigiSign dipublikasikan dalam repositori yang tertera di bagian 2.2	*All Online Certificate Status Service comply with the Internet Engineering Task Force (IETF) RFC 6960 to meet security and interoperability requirements. A list of all OCSP responders operated by DigiSign CA is published in the repository described in section 2.2.*

4.9.11 Bentuk Lain dari Pengumuman Pencabutan yang Tersedia / *Other Forms of Revocation Advertisement Available*

Tidak ada ketentuan.	*No Condition.*

4.9.12 Persyaratan Khusus terkait Kebocoran Kunci / *Special Requirement Related to Key Compromise*

Tidak ada ketentuan.	*No Condition.*

4.9.13 Kondisi untuk Pembekuan / *Circumstances for Suspension*

Pembekuan Sertifikat tidak disediakan.	*Certificate suspension is not provided.*

4.9.14 Siapa yang Dapat Meminta Pembekuan / *Who can Request Suspension*

Pembekuan Sertifikat tidak disediakan.	*Certificate suspension is not provided.*

4.9.15 Prosedur Permintaan Pembekuan / *Procedure for Suspension Request*

Pembekuan Sertifikat tidak disediakan.	*Certificate suspension is not provided.*

4.9.16 Batas Waktu Pembekuan / *Limits on Suspension Period*

Pembekuan Sertifikat tidak disediakan.	*Certificate suspension is not provided*

4.10 Layanan Status Sertifikat / *Certificate Status Services*

4.10.1 Karakteristik Operasional / *Operational Characteristics*

Layanan Status Sertifikat tersedia melalui OCSP dan CRL pada repositori.	*Certificate Status Service available through OCSP and CRL at repository.*

4.10.2 Ketersediaan Layanan / *Service Availability*

PSrE Digisign menjamin ketersediaan layanan validasi status Sertifikat di luar waktu pemeliharaan.	*Digisign CA ensures the availability of Certificate status validation services outside the maintenance window.*

4.10.3 Fitur Opsional / *Optional Features*

Tidak ada ketentuan.	*No Condition*

4.11 Akhir Berlangganan / *End of Subscription*

Pemilik dapat mengakhiri layanan penggunaan sertifikat yang diterbitkan oleh PSrE Digisign dengan membiarkan Sertifikatnya kedaluwarsa atau mencabut Sertifikatnya tanpa meminta Sertifikat yang baru.	*Subscriber can terminate the usage of a certificate issued by Digisign CA by letting his Certificate expire or revoke his Certificate without requesting a new Certificate.*

4.12 Pemulihan dan Eskro Kunci / Key Escrow and Recovery

4.12.1 Kebijakan dan Praktik Pemulihan dan Eskro Kunci / Key Escrow and Recovery Policy and Practices

Kunci Privat PSrE Digisign dan Kunci Privat Pemilik yang terasosiasi dengan Sertifikat yang berisi *key usage digitalSignature* tidak dieskro.	*Digisign CA's Private and Subscriber's Private Key associated with a Certificate that asserts a digitalSignature key usage is not escrowed.*

4.12.2 Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi / *Session Key Encapsulation and Recovery Policy and Practices*

Tidak ada ketentuan.	*No Condition.*

5. KENDALI FASILITAS, MANAJEMEN, DAN OPERASIONAL / *FACILITY, MANAGEMENT, AND OPERATION CONTROLS*

5.1 Kendali Fisik / *Physical Controls*

5.1.1 Lokasi dan Konstruksi / *Site Location and Construction*

Lokasi dan konstruksi dari fasilitas penempatan peralatan PSrE Digisign serta juga tempat-tempat yang menampung *workstation* jarak jauh yang digunakan untuk mengelola PSrE Digisign sesuai dengan fasilitas yang digunakan untuk menyimpan informasi yang sensitif. Lokasi dan konstruksi tempat kerja, dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjaga dan CCTV, telah memberikan perlindungan terhadap akses yang tidak sah ke peralatan PSrE Digisign.	*The location and construction of Digisign CA equipment placement facilities as well as the places that house remote workstations used to manage Digisign CA according to the facilities used to store sensitive information. The location and construction of the workplace, combined with other physical security protection mechanisms such as guards and CCTV, has provided protection against unauthorized access to Digisign CA equipment.*
Sistem cadangan PSrE Digisign disiapkan di *Data Center* (DC) cadangan (yaitu DC yang difungsikan sebagai DRC/*Disaster Recovery Center*), dan mampu memulihkan layanan sistem ketika terjadi kegagalan di DC utama.	*Digisign CA's backup system is set up in a backup DC (a DC that functions as a DRC/Disaster Recovery Center). The backup system must be able to recover the system services when the main DC malfunctioned.*
DRC berada di lokasi yang Ketika terjadi bencana alam pada DC utama, DRC tidak ikut terkena dampaknya. Lokasi fisik DC dan DRC berada di Indonesia.	*DRC is a location where, in a circumstance where a natural disaster happened in the main DC, the DRC remains unaffected.* *DC and DRC are physically located in Indonesia.*
PSrE Digisign mengukur risiko untuk	*PSrE Digisign measures risk to determine*

menentukan jarak antara DC dan DRC yang mempertimbangkan ketersediaan layanan PSrE Digisign.

the distance between DC and DRC considering the availability of PSrE Digisign services

5.1.2 Akses Fisik / *Physical Access*

Peralatan PSrE Digisign terlindungi dari akses yang tidak berhak. Mekanisme keamanan fisik untuk PSrE Digisign telah diimplementasikan untuk:

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

Digisign CA equipment is protected against unauthorized access. Physical security mechanisms for Digisign CA have been implemented to:

1. *Ensure that no unauthorized access is allowed to the hardware,*
2. *Store all removable media and paper containing sensitive plain text information in a secure container,*
3. *Monitor, either manually or electronically, for unauthorized interference at all times, and*
4. *Maintain and periodically check access logs.*

Semua kegiatan operasional PSrE Digisign yang memiliki resiko tinggi dilakukan di dalam fasilitas yang aman dan kegiatan tersebut tercatat. Fasilitas tersebut memiliki setidaknya empat lapis keamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif. Fasilitas tersebut secara fisik terpisah dari fasilitas organisasi yang lain, sehingga hanya peran terpercaya PSrE Digisign yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

All high-risk Digisign CA operations are conducted in a secure facility and logged. These facilities have at least four layers of security to allow access to sensitive hardware and software. These facilities are physically separated from other organizational facilities, so that only Digisign CA's trusted roles with the authority can access these facilities.

Modul kriptografis yang *removable* harus dinonaktifkan sebelum disimpan. Ketika tidak digunakan, modul kriptografis yang *removable*, informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografis harus ditempatkan pada tempat penyimpanan yang aman.	*Removable cryptographic modules must be disabled before saving. When not in use, the removable cryptographic module, the activation information used to access or activate the cryptographic module must be placed in a secure storage location.*

5.1.3 Daya dan Penyejuk Udara / *Power and Air Conditioning*

PSrE Digisign memiliki daya cadangan yang cukup ketika listrik utama mati, untuk dapat menyelesaikan beberapa hal/tindakan yang tertunda, dan mencatat keadaan peralatan sebelum kekurangan daya atau pengatur suhu udara (AC) yang menyebabkan peralatan mati. Repositori IKP telah dilengkapi dengan *Uninterrupted Power* dan Generator Listrik yang cukup untuk pengoperasian minimal 6 (enam) jam tanpa adanya listrik/daya dari PLN, untuk mendukung keberlangsungan operasional.	*Digisign CA has enough backup power when the main power goes out, to be able to finish some pending things/actions and record the state of the equipment before a lack of power or air conditioning causes the equipment to shut down. The IKP Repository has been equipped with Uninterrupted Power and sufficient Electricity Generator to operate for a minimum of 6 (six) hours without electricity/power from PLN, to support operational continuity.*

5.1.4 Keterpaparan Air / *Water Exposures*

Peralatan PSrE Digisign dilindungi terhadap air dan diletakkan di atas tanah dengan *raised floor.*	*Digisign CA equipment is protected against water and placed on the ground with a raised floor.*

5.1.5 Pencegahan dan Perlindungan dari Kebakaran / *Fire Prevention and Protection*

Peralatan PSrE Digisign ditempatkan di	*Digisign CA equipment is housed in facilities*

fasilitas dengan sistem deteksi dan pemadaman kebakaran yang memadai.	*with adequate fire detection and suppression systems.*

5.1.6 Penyimpanan Media / *Media Storage*

PSrE Digisign memastikan media penyimpanan yang digunakan ditangani secara aman, terlindungi dari kerusakan, pencurian, dan akses yang tidak berhak.	*Digisign CA ensures all storage media are handled securely, protected from damage, theft, and unauthorized access.*
Media *backup* PSrE Digisign disimpan sehingga bisa melindunginya dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau *backup* diduplikasi dan disimpan di lokasi yang terpisah dari lokasi Data Center PSrE Digisign.	*Digisign CA backup media are stored so they can protect against accidental damage (water, fire, electromagnetic), theft and unauthorized access. Media containing audit, archive, or backup information is duplicated and stored in a separate location from the Digisign CA's Data Centre location.*

5.1.7 Pembuangan Limbah / *Waste Disposal*

Dokumen yang mengandung informasi sensitif dihancurkan sampai tidak dapat direkonstruksi kembali.	*Documents which contain sensitive information are destroyed until those documents are unable to be recovered.*
Semua informasi sensitif yang terdapat pada barang yang sudah tidak digunakan dihancurkan sebelum dibuang.	*All sensitive information which is contained in waste material is destroyed before being disposed of.*
Seluruh perangkat kriptografis yang sudah tidak digunakan dihancurkan fisiknya sampai tidak dapat digunakan Kembali sebelum dibuang.	*All unused cryptographic devices are physically destroyed until those devices are irreparable before being disposed of.*

5.1.8 Backup Off-Site / *Off-Site Backup*

Pencadangan semua sistem dari PSrE PSrE Digisign yang cukup untuk pulih dari kegagalan sistem, dilakukan secara berkala 6 (enam) bulan sekali dan minimal 1 salinan *back up* terkini disimpan di lokasi yang aman dan *offsite* (di lokasi yang terpisah dari DC dan DRC PSrE Digisign). Data *backup* semua sistem PSrE Digisign dilindungi dengan pengamanan fisik dan prosedur yang setara, sesuai pengamanan pada operasional PSrE Digisign.	*Digisign CA system data backups are performed at least once every 6 (six) months or whenever there is a change in data. The data backup results are saved in the DRC location. Physical precautions and methods similar to those used in Digisign CA operations protect the backup data. The off-site backup is stored in a location that is not affected by a natural disaster that occurs on the DC.*
Backup offsite berada di lokasi yang berdasarkan pertimbangan ketika terjadi bencana alam baik pada DC dan DRC, *Backup offsite* tidak ikut terkena dampaknya.	*Off-site backup is located in a location where, in a circumstance where a natural disaster happens in either DC or DRC, the off-site backup remains unaffected.*

5.2 Kendali Prosedur / *Procedural Controls*

5.2.1 Peran Terpercaya / *Trusted Roles*

Peran terpercaya meliputi tapi tidak terbatas pada:	*Trusted role shall include but not limited to*:
1. Policy Authority (PA)	*1. Policy Authority (PA)*
2. Manager PSrE	*2. CA Manager*
3. Manager RA	*3. RA Manager*
4. Admin Sekuriti	*4. Security Officer*
5. Admin Aplikasi	*5. Application Administrator*
6. Admin Infrastruktur	*6. Infrastructure Administrator*
7. Admin Sistem	*7. System Administrator*
8. Pengelola Kunci	*8. Key Manager*
9. Internal Auditor	*9. Internal Auditor*
10. Pemegang material kriptografi	*10. Crypto material custodian*
11. Pemegang akses kunci fisik	*11. Physical Key Access Holder*

Peran dan tanggung jawab dari masing-masing peran dijelaskan dalam dokumen sesuai dengan kebijakan internal.	*Roles and responsibilities from each trusted role are described in the document according to internal policy.*

5.2.2 Jumlah Orang yang Dibutuhkan untuk setiap Tugas / *Number of Persons Required per Task*

PSrE Digisign memastikan bahwa setiap kegiatan terkait manajemen kunci, manajemen sertifikat dan aktivitas terkait lain, dilaksanakan oleh personil yang tercatat dalam peran terpercaya.	*Digisign CA ensures that all activities related to key management, certificate management, and other related activities are carried out by personnel registered in trusted roles.*
Tugas dan kegiatan berikut memerlukan 2 (dua) atau lebih personil yang semuanya tercatat dalam peran terpercaya: 1. Pembangkitan pasangan kunci PSrE Digisign, 2. Pencadangan dan pemulihan kunci privat PSrE Digisign, 3. Akses fisik dan logis ke fasilitas kritis dan aset kritis untuk operasional PSrE Digisign.	*The following tasks and activities require two (2) or more personnel, all of whom must be registered in trusted roles:* *1. Generation of Digisign CAs key pairs,* *2. Digisign CAs private key backup and recovery,* *3. Physical and logical access to critical facilities and critical assets for Digisign CA operations.*

5.2.3 Identifikasi dan Autentikasi untuk Setiap Peran / *Identification and Authentication for Each Role*

Semua individu yang ditugaskan dalam Peran Terpercaya merupakan karyawan dari PSrE Digisign atau afiliasi yang sudah melalui proses pemeriksaan latar belakang sesuai Bagian 5.3.2. Sebelum menjalankan tugas, Peran Terpercaya harus diberikan mandat melalui Surat Penugasan.	*All individuals assigned to a Trusted Role are employees of the Digisign CA or affiliates who already passed background checks as defined in Section 5.3.2. Prior to assignment, the Trusted Roles are mandated by using an Assignment Letter.*

Semua Peran Terpercaya diharuskan untuk mengautentikasi diri ke sistem PSrE dan/atau RA sebelum mereka dapat menjalankan tugas peran mereka yang melibatkan sistem tersebut.	*All Trusted Roles are required to authenticate themselves to CA and/or RA systems before they may perform the duties of their role involving those systems.*
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.	*The authentication of Trusted Roles is performed by physical access control and system level access control. The authentication shall be based on an identification of the person accessing the room or system and the access rights configured in accordance with the person's role.*

5.2.4 Peran yang Membutuhkan Pemisahan Tugas / *Roles Requiring Separation of Duties*

Peran yang tidak dapat diperankan bersamaan adalah: 1. Policy Authority dan Manajer PSrE, 2. Auditor Internal dan semua peran lain, dan 3. Pengelola Kunci dan peran pemegang kunci kriptografis.	*The roles that are not played concurrently are:* *1. Policy Authority and CA Manager,* *2. Internal Audit and all other roles, and* *3. Key Manager and Crypto material custodian.*

5.3 Kendali Personil / *Personnel Controls*

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan Penugasan/ *Qualification, Experience and Clearance Requirements*

Semua personil Peran Terpercaya telah dipilih atas dasar keterampilan, pengalaman, *track record* personil,	*All Trusted Role personnel have been selected on the basis of skills, experience, personnel track record, trustworthiness, and*

kepercayaan, dan integritas sesuai dengan persyaratan sebagai berikut:

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

integrity in accordance with the following requirements:

1. *Proof of the necessary background, qualifications, and experience necessary to carry out their job responsibilities efficiently and adequately, and*
2. *Proof of a clean criminal record.*

Personel yang ditunjuk untuk Peran Terpercaya secara resmi diangkat oleh pimpinan organisasi.

Personnel appointed to Trusted Roles are formally appointed by management.

5.3.2 Prosedur Pemeriksaan Latar Belakang / *Background Check Procedures*

Semua personil di PSrE Digisign telah menyelesaikan pemeriksaan latar belakang. Ruang lingkup pemeriksaan latar belakang mencakup area berikut yang cakupannya:

1. Surat pengalaman Pekerjaan
2. Pendidikan atau sertifikasi
3. Identifikasi Kependudukan (KTP)
4. Surat Keterangan Catatan Kepolisian
5. Informasi finansial dari sistem pemeriksaan finansial yang dikeluarkan oleh otoritas yang berwenang

All personnel at Digisign CA have completed background checks. The scope of the background check covers the following areas which it covers:

1. *Work experience letter*
2. *Education or certification*
3. *Population Identification (KTP)*
4. *Police Certificate of Good Conduct.*
5. *Financial data from the relevant authorities related to financial area*

5.3.3 Persyaratan Pelatihan / *Training Requirements*

Personil Peran Terpercaya Digisign mendapatkan pelatihan yang sesuai dengan perannya.

Digisign Trusted Role personnel receive training appropriate to their role.

Lingkup pelatihan meliputi, namun tidak terbatas pada: 1. Keamanan informasi 2. Operasional PSrE Digisign, termasuk perangkat keras dan perangkat lunak 3. Pemulihan bencana dan kelangsungan bisnis 4. Kebijakan yang berlaku, seperti CPS dan CP Root	*The scope of training includes, but is not limited to:* *1. Information security* *2. Digisign PSrE operations, including hardware and software* *3. Disaster recovery and business continuity* *4. Applicable policies, such as CPS and Root CP*
Evaluasi terhadap kecukupan kompetensi personil PSrE Digisign minimal 1 (satu) kali dalam setahun.	*Evaluation of the competency adequacy of Digisign CA personnel at least 1 (one) time a year.*

5.3.4 Frekuensi dan Persyaratan Pelatihan Ulang / *Retraining Frequency and Requirements*

PSrE Digisign memberikan pelatihan ulang kepada personil Peran Terpercaya minimal 1 kali dalam 1 tahun.	*Digisign CA provides retraining to Trusted Role personnel at least once a year.*
Pelatihan ini bertujuan agar personel Peran Terpercaya meningkatkan keterampilan yang dibutuhkan dalam melaksanakan tugasnya secara efektif dan sesuai dengan standar yang berlaku.	*The training aims to improve the skills needed for Trusted Role personnel to carry out their duties effectively and in accordance with applicable standards.*

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan / *Job Rotation Frequency and Sequence*

PSrE Digisign memastikan bahwa perubahan staf tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.	*Digisign CA ensures that staff changes will not affect the operational effectiveness of the service or system security.*

6.3.6 Sanksi untuk Tindakan yang Tidak Terotorisasi / *Sanctions for Unauthorized Actions*

Sanksi disipliner yang sesuai diberikan pada personil yang melanggar ketentuan dan kebijakan didalam CP / CPS atau prosedur operasional PSrE Digisign.	*Appropriate disciplinary sanctions are imposed on personnel who violate the provisions and policies in the CP / CPS or Digisign CA operational procedures*

5.3.7 Persyaratan Kontraktor Independen / *Independent Contractor Requirements*

Personil sub kontraktor yang dipekerjakan untuk melaksanakan fungsi-fungsi yang terkait dengan operasi PSrE Digisign harus memenuhi persyaratan yang berlaku yang diatur dalam CPS ini, sesuai pada bagian 5.3.1, 5.3.2 dan 5.3.3.	*Sub-contractor personnel employed to perform functions related to Digisign CA's operations must comply with the applicable requirements set out in this CPS, in accordance with sections 5.3.1, 5.3.2 and 5.3.3.*

5.3.8 Dokumentasi yang Diberikan kepada Personel / *Documentation Supplied to Personnel*

PSrE Digisign telah membuat dokumen-dokumen yang tersedia bagi personilnya, antara lain *Certificate Policy* (Kebijakan Sertifikat) yang diacu, CPS, undang-undang terkait, kebijakan, dan kontrak yang relevan. Dokumen teknis, operasi, dan administratif lain (sebagai contoh Panduan Administrasi, Manual Penggunaan, dsb) juga tersedia agar peran terpercaya dapat melaksanakan kewajiban mereka.	*Digisign CA has made available the documents to its personnel, These include the referenced Certificate Policy, the CPS, and related regulations, policies, and contracts. Other technical, operational, and administrative documents (e.g., Administration Guides, Usage Manuals, etc.) are also available to enable trusted roles to carry out their duties.*

5.4 Prosedur Log Audit / *Audit Logging Procedures*

Berkas log audit disimpan untuk semua kejadian yang terkait dengan keamanan PSrE Digisign. Pengumpulan log audit keamanan dilakukan secara otomatis. Namun bila tidak memungkinkan, terdapat cara lain seperti penggunaan buku log, kertas formulir, atau mekanisme fisik lainnya. Semua log audit keamanan, dalam bentuk elektronik dan non elektronik, disimpan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai dengan bagian 5.5.2

Audit log files are kept for all events related to Digisign CA security. Security audit logs should be collected automatically. If this is not possible, there are other means such as the use of logbooks, paper forms, or other physical mechanisms. All security audit logs, electronic and non-electronic, are stored and made available during the compliance audit. Security audit logs for each auditable event defined in this section are maintained in accordance with section 5.5.2

5.4.1 Jenis Kejadian yang Direkam / *Types of Events Recorded*

PSrE Digisign mengaktifkan semua kapabilitas audit keamanan dari sistem operasi PSrE Digisign, termasuk memastikan aplikasi *Certification Authority* PSrE Digisign agar seluruh kegiatan yang berkaitan dengan siklus Sertifikat disimpan secara otomatis untuk menjamin keterlacakan setiap tindakan *Trusted Role* dalam operasional PSrE Digisign. Informasi yang akan disimpan dalam bentuk log, termasuk namun tidak terbatas pada:

1. tipe kejadian dan tanggal serta waktu kejadian,
2. nomor urut rekaman,
3. sumber perekaman,

Digisign CA enables all security audit capabilities of the Digisign CA operating system, including to ensure Digisign CA Certification Authority application automatically stores all activities related to the Certificate cycle to ensure traceability of every Trusted Role's action in Digisign CA operations. Information to be stored in log form, including but not limited to:

1. *the type of event and the date and time of the incident,*
2. *recording serial number,*
3. *recording source,*

4. indikator sukses atau gagal yang sesuai,
5. identitas dari operator yang menyebabkan kejadian tersebut.

4. *appropriate success or failure indicators,*
5. *the identity of the operator that caused the event.*

Waktu sistem di PSrE Digisign disinkronkan dengan otoritas sumber waktu dengan ketelitian 1 (satu) menit.

Time at Digisign CA's system is synchronized with an authoritative time source to within one minute.

5.4.2 Frekuensi Pemrosesan Log / *Frequency of Processing Log*

Log audit ditinjau secara berkala, dan diverifikasi bahwa log tidak rusak atau hilang, tidak diacak, dan tidak adanya jenis kehilangan lain terhadap data audit, kemudian dilakukan pemeriksaan semua entri log, serta penyelidikan yang lebih menyeluruh jika terdapat peringatan atau penyimpangan yang muncul dalam log.

Audit logs are reviewed periodically, and verified that logs are not corrupted or missing, not randomized, and that there are no other types of loss to audit data, then all log entries are checked, and a more thorough investigation of any warnings or irregularities that arise in the logs.

Segala tindakan yang diambil sebagai hasil dari peninjauan ini dibuat dokumentasinya.

All actions taken as a result of this review are documented.

5.4.3 Periode Retensi Log Audit / *Retention Period for Audit Log*

Log audit PSrE Digisign dipertahankan selama 1 (satu) tahun agar tersedia untuk pengendalian yang sah. Periode ini dapat diubah tergantung pada perkembangan regulasi yang terkait.

Digisign CA audit logs are maintained for 1 (one) year to be available for legal control. This period may be changed depending on the relevant regulation developments.

5.4.4 Proteksi Log Audit / *Protection of Audit Log*

Log Audit yang tercatat dilindungi untuk mencegah dan mendeteksi perubahan dari file log, serta memastikan bahwa hanya individu dengan akses peran terpercaya dan berwenang yang dapat mengakses log tanpa memodifikasi integritasnya.	*The recorded Audit logs are protected to prevent and detect changes to log files and ensure that only individuals with trusted and authorized role access can access the logs without modifying their integrity.*

5.4.5 Prosedur *Backup* Log Audit / *Audit Log Backup Procedures*

Log audit dikelola dengan metode *hot backup*. dan ringkasan audit dicadangkan setiap hari. Media backup disimpan secara lokal dalam suatu lokasi yang aman.	*Audit logs are managed by the hot backup mechanism. Backup media is stored locally in a secure location.*

5.4.6 Sistem Pengumpulan Audit (Internal vs External) / *Audit Collection System (Internal vs External)*

Sistem pengumpulan log audit adalah internal ke sistem PSrE Digisign. Log audit meliputi sistem, infrastruktur dan jaringan.	*The audit log collection system is internal to the Digisign CA system. Audit logs are covering system, infrastructure and network.*

5.4.7 Pemberitahuan ke Subyek Penyebab Kejadian / *Notification to Event-Causing Subject*

Tidak ada pemberitahuan kepada Pemilik, organisasi, Pihak Pengandal dan badan usaha yang menyebabkan kejadian tersebut.	*There was no notification to the Subscriber, organization, Relying Party and business entity that caused the incident.*

5.4.8 Asesmen Kerentanan / *Vulnerability Assessments*

PSrE Digisign melaksanakan asesmen	*Digisign CA performs regular vulnerability*

kerentanan sistemnya secara berkala. Dalam hal terdapat temuan pada saat asesmen kerentanan, PSrE Digisign memperbaiki temuan tersebut. Uji penetrasi ke sistem PSrE Digisign dilakukan minimal 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem PSrE Digisign.

assessment. When vulnerabilities are found during the assessment, Digisign CA promptly repairs the vulnerabilities. Penetration tests shall be performed on Digisign CA's system at least annually or when there are significant changes in the Digisign CA's system.

5.5 Pengarsipan Record / *Record Archival*

5.5.1 Tipe Record yang Diarsipkan / *Types of Records Archived*

Catatan arsip PSrE Digisign menentukan kesesuaian operasional dan validitas Sertifikat yang dikeluarkan oleh PSrE Digisign (termasuk yang dicabut atau kadaluwarsa). Data yang dicatat pada arsip memuat paling sedikit namun tidak terbatas pada:

1. Siklus hidup operasi Sertifikat termasuk permohonan Sertifikat, permintaan pencabutan dan permintaan *rekey*,
2. Semua Sertifikat dan CRL yang diterbitkan dan dipublikasikan oleh PSrE Digisign,
3. Data konfigurasi sistem IKP,
4. Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini,
5. Data pendaftaran Pemohon atau Data Pribadi Pemilik Sertifikat PSrE Digisign.
6. Data audit
7. Data pendukung SMPI:

Digisign CA's archival records determine the operational suitability and validity of Certificates issued by Digisign CA (including revoked or expired). Data that is recorded in the archives include at least but not limited to:

1. *The Certificate operation lifecycle includes Certificate requests, revocation requests and rekey request,*
2. *All Certificates and CRLs issued and published by Digisign CA,*
3. *PKI system configuration data,*
4. *CP documents and all applicable CPS including modifications and amendments to these documents,*
5. *Applicant registration data or Digisign CA Subscriber Certificate Personal Data.*
6. *Audit data*
7. *ISMS supporting data:*

a. Penunjukkan dan pencabutan peran dan kewenangan,
b. Akses ke fasilitas PSrE Digisign,
c. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak,
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.

a. Assignment and revocation of roles and privileges,
b. Access to Digisign CAs facilities,
c. Changes and maintenance of hardware and software
d. Detection and processing of security incidents,
e. Emergency drill,
f. Risk Assessment and treatment,
g. Changes of assets, procedures, and responsibilities, and
h. Changes of documentations.

5.5.2 Periode Retensi Arsip / *Retention Period for Archive*

Catatan yang diarsipkan disimpan setidaknya selama 5 (lima) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini juga dipelihara selama masa retensi.

Archived records are kept for at least 5 (five) years. Applications required to read these files also be maintained throughout the retention period.

5.5.3 Perlindungan Arsip / *Protection of Archive*

PSrE Digisign melindungi catatan arsip dan hanya orang yang berwenang yang dapat mengakses. Catatan yang diarsipkan dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah dengan menggunakan sistem yang handal. Media yang menyimpan catatan arsip dan aplikasi yang dibutuhkan untuk memproses catatan arsip dipelihara dan dilindungi.

Digisign CA protects archival records and only authorized persons have access. Archived records are protected from unauthorized access, modification, deletion, or tampering by using a reliable system. The media that stores archival records and the applications required to process archival records are maintained and protected.

Muatan arsip tidak boleh diungkap kecuali berdasarkan ketentuan pada Bagian 9.3

The contents of the archive shall not be released except in accordance with

dan 9.4. Catatan dari transaksi individu dapat diungkap berdasarkan permintaan dari pemilik yang terlibat dalam transaksi atau berdasarkan permintaan dari agen pemilik yang dikenali oleh hukum.

Sections 9.3 and 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

5.5.4 Prosedur *Backup* Arsip / *Archive Backup Procedures*

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 telah tersedia.

Adequate and regular backup procedures are in place so that in the event of loss or damage to master archives, a complete set of backup copies held in separate locations is available.

5.5.5 Persyaratan Pemberian Penanda Waktu pada Rekaman Arsip / *Requirement for Time-Stamping of Records*

Rekaman arsip PSrE Digisign diberi stempel waktu ketika dibuat.

Digisign CA archive records are timestamped when they are created.

5.5.6 Sistem Pengumpulan Arsip / *Archive Collection System*

Pengumpulan arsip di PSrE Digisign dilakukan oleh internal PSrE Digisign.

The collection of archives at Digisign CA is carried out by Digisign CA internally.

5.5.7 Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip / *Procedures to Obtain and Verify Archive Information*

Penyimpanan media untuk informasi arsip PSrE Digisign diperiksa saat pembuatan. Dalam waktu 1 bulan sekali, sampel informasi yang diarsipkan diuji untuk memeriksa integritas dan keterbacaan informasinya. Hanya peran terpercaya, dan orang-orang resmi lainnya yang diizinkan untuk mengakses arsip. Permintaan untuk

Media storage for Digisign CA archive information is checked at creation. Once a month, a sample of archived information is tested to check the integrity and legibility of the information. Only trusted roles, and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by

mendapatkan dan memverifikasi informasi arsip dikoordinasikan oleh Admin Sistem.

System Administrator.

5.6 Pergantian Kunci / *Key Changeover*

Untuk meminimalkan risiko dari kondisi Kunci Privat PSrE Digisign terkompromi, Kunci Privat dapat diubah. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat.

To minimize the risk of the Digisign CA Private Key being compromised, the Private Key can be changed. Since the Private Key was changed, only the new key can be used for Certificate signing.

Sertifikat lama yang masih berlaku, tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat lama habis masa berlakunya. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama disimpan dan dilindungi sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat lama habis masa berlakunya.

The old, but still valid, certificate will be available to verify the old signature until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign the CRL, then the old key is stored and protected.

Apabila PSrE Digisign memperbarui Kunci Privat dan dengan demikian menghasilkan Kunci Publik baru, PSrE Digisign memberitahu melalui email atau sistem elektronik lain kepada semua Pemilik dan Pengandal Sertifikat PSrE Digisign bahwa telah terjadi perubahan.

If Digisign CA updates the Private Key and thereby generates a new Public Key, Digisign CA notifies via email or other electronic system to all Digisign Subscriber Certificate and Relying Parties that a change has occurred.

PSrE Digisign tidak membangkitkan (*generate*) Sertifikat Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat PSrE Digisign. Dengan demikian, Kunci

Digisign CA does not generate a Certificate for a Subscriber whose validity period would be longer than the Digisign CA's Certificate validity period. Hence, Digisign CA Private Key is changed periodically every 10 (ten)

Privat PSrE Digisign diubah secara berkala setiap 10 (sepuluh) tahun, paling lambat pada saat kedaluwarsa dikurangi masa berlaku Sertifikat Pemilik.

Kunci PSrE Digisign yang berlaku beserta masa berlakunya dijelaskan pada bagian 6.3.2.

years, at the latest, at the time of expiration minus the validity period of the Subscriber's Certificate.

The valid Digisign CA keys and their validity periods are explained in section 6.3.2.

5.7 Pemulihan Bencana dan Keadaan Terkompromi / *Compromise and Disaster Recovery*

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi / *Incident and Compromise Handling Procedures*

PSrE Digisign menangani bencana dan insiden *compromise* sesuai dengan prosedur penanganan bencana untuk meminimalkan dampak dari peristiwa seperti itu.
PSrE Digisign memiliki rencana tanggap darurat (*Business Continuity Plan*) dan rencana pemulihan bencana (*Disaster Recovery Plan*).

Digisign CA handles disasters and compromise incidents in accordance with disaster management procedures to minimize the impact of such events.
Digisign CA has an emergency response plan (Business Continuity Plan) and a disaster recovery plan (Disaster Recovery Plan).

Jika Kunci PSrE Digisign dicurigai telah terkompromi, penerbitan Sertifikat dihentikan, PSrE Digisign melakukan Investigasi untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan dinilai untuk menentukan prosedur perbaikan yang tepat, apabila dicurigai terpapar atau bocor maka harus mengikuti prosedur seperti pada pasal 5.7.3

If the Digisign CA Key is suspected of having been compromised, the issuance of the Certificate is stopped, Digisign CA carries out an Investigation to determine the nature and extent of the damage. The scope of potential damage is assessed to determine the appropriate repair procedure, if it is suspected of being exposed or leaking it must follow the procedures as in Article 5.7.3

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

1. Terdeteksinya atau adanya indikasi sistem PSrE Digisign terkompromi,
2. Adanya upaya untuk menembus sistem PSrE Digisign, baik secara fisik maupun elektronik,
3. Serangan Denial of Service pada sistem PSrE Digisign, dan / atau
4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam field "*nextupdate*" pada CRL nya yang valid saat ini.

In case that there is an event that affects the security of Digisign CA system, Digisign CA notifies the root CA if any of the following occur:

1. *Suspected or detected compromise of any Root CA system or subsystem,*
2. *Physical or electronic penetration of any Root CA system or subsystem,*
3. *Successful denial of service attacks on any Root CA system or subsystem, and/or*
4. *Any incident preventing Root CA from issuing and publishing a CRL within 180 (one hundred eighty) days from the time indicated in the "nextUpdate" field in the currently published CRL.*

Prosedur ditinjau dan diperbarui setiap 3 (tiga) bulan sekali atau sesuai kebutuhan.

The procedures are reviewed and updated quarterly or as needed.

Semua sistem pencadangan/pemulihan diuji minimal setahun sekali.

All Backup/Recovery Systems are tested at least once a year.

Jika PSrE Digisign mendapatkan pemberitahuan dari PSrE Induk bahwa PSrE Induk terkompromi maka PSrE Digisign menghentikan layanan, memberitahu semua Pemilik dan Pengandal agar mengeluarkan Sertifikat PSrE Digisign yang berinduk kepada sertifikat PSrE Induk yang terkompromi dari rantai kepercayaannya, dilanjutkan dengan

If Digisign CA receives notification from the Root CA that the Root CA is compromised, then Digisign CA stops the service, notifies all Subscribers and Relying parties to exclude the Digisign CA Certificate which having the compromised Root CAs certificate from their Trust Anchor, followed by revoking all Subscriber Certificates, issuing the final CRL, and notify relevant

pencabutan semua Sertifikat, menerbitkan CRL terakhir, dan memberitahu kontak-kontak yang relevan.

contacts.

5.7.2 Sumber Daya Komputasi, Perangkat Lunak, dan/atau Data Rusak / Computing Resources, Software and/or Data are Corrupted

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

1. Memberitahu PSrE Induk sesegera mungkin sesuai prosedur penangan insiden,
2. Memastikan integritas sistem telah direstorasi sebelum mengembalikan pada operasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir *backup*,
3. Mengoperasikan kembali PSrE Digisign, memberikan prioritas pada kemampuan untuk membangkitkan informasi status Sertifikat dalam jadwal penerbitan CRL, dan
4. Jika kemampuan untuk membangkitkan informasi status Sertifikat tidak beroperasi atau rusak, PSrE Digisign akan memulihkan kemampuan untuk membangkitkan informasi status Sertifikat sesegera mungkin sesuai dengan prosedur yang ditetapkan dalam CPS. Jika kemampuan PSrE Digisign untuk membangkitkan informasi status Sertifikat tidak bisa dipulihkan dalam jangka waktu yang wajar, PSrE

When computer resources, software and/or data are damaged, Digisign CA does the following:

1. *Notify the Root PSrE as soon as possible according to incident handling procedure,*
2. *Ensure system integrity has been restored prior to restore in operation and determine how much data has been lost since the last backup position,*
3. *Re-operating Digisign CA, giving priority to the ability to generate Certificate status information in the CRL issuance schedule, and*
4. *If the ability to generate Certificate status information is inoperative or damaged, Digisign CA re-establish its ability to generate Certificate status information as quickly as possible. If in a reasonable time-frame Digisign CA is not capable of doing so, Digisign CA determines whether to request revocation of its Certificate(s) to the Root CA.*

Digisign akan menentukan apakah perlu untuk meminta pencabutan Sertifikat miliknya kepada PSrE Induk.

5. Bila kunci penandatanganan PSrE Digisign rusak, operasional PSrE Digisign dilakukan kembali secepat mungkin, memberikan prioritas ke pembangkitan pasangan kunci baru PSrE Digisign sesuai dengan prosedur yang ditetapkan dalam CPS.

5. *When a Digisign CA signing key is damaged, Digisign CA operations are resumed as quickly as possible, giving priority to the generation of a new Digisign CA key pair in accordance with the procedures stipulated in the CPS.*

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

If both primary and disaster recovery sites cannot be used for revocation capability in a reasonable time-frame, the Digisign CA systems will be treated as compromised.

5.7.3 Prosedur Kunci Privat Entitas Terkompromi / *Entity Private Key Compromise Procedures*

Dalam kasus kehilangan Kunci Privat atau terjadi kebocoran/kompromi terhadap parameter yang digunakan untuk membangkitkan Kunci Privat dan Sertifikat, PSrE Digisign akan mencabut semua Sertifikat yang terkait, kemudian semua kunci serta Sertifikat baru diterbitkan tanpa menghentikan layanan.

In case of loss of Private Keys or compromise of the algorithms and parameters used to generate the Private Key and Certificate, Digisign CA will revoke all related Certificates, then all new keys and Certificates are issued without interrupting its services.

Bila Kunci Privat PSrE Digisign hilang atau terkompromi, maka PSrE Digisign:

1. Memberitahu PSrE Induk dan Pihak Pengandal melalui pengumuman publik.
2. Memberitahu semua Pemilik kemudian dilanjutkan dengan pencabutan semua

If a Digisign CA Private Key is lost or compromised, then Digisign CA shall:

1. *Notify the Root PSrE and the Relying Party through public announcements.*
2. *Notify all Subscriber then proceed with revocation of all Certificates.*

Sertifikat.

3. Membangkitkan Pasangan Kunci PSrE Digisign baru sesuai dengan prosedur yang ditetapkan dalam CPS.
4. PSrE Digisign meminta penerbitan Sertifikat PSrE baru ke Menteri sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CPS.

3. Generate a new Digisign CA Key Pair in accordance with procedures specified in CPS.
4. Digisign CA requests the issuance of a new Certificate from the Minister, following the initial registration process as outlined in the CPS.

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

Reissuance of the Subscriber's Private Key due to compromise can be initiated by Subscriber through submitting a Certificate request as outlined in Section 4.1.

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

Digisign CA investigates the cause of compromise or loss and determines the necessary actions to prevent such compromise from recurring.

5.7.4 Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana / *Business Continuity Capabilities after a Disaster*

Untuk menjamin integritas layanan, PSrE Digisign melakukan backup data dan menyiapkan prosedur pemulihan.
PSrE Digisign menyiapkan suatu rencana pemulihan bencana yang telah diuji, ditinjau ulang, dan diperbaiki secara berkala.

Digisign CA implements data backup and recovery procedures to maintain the integrity of the services.
Digisign CA has a disaster recovery plan which has been tested, verified, and continually updated.

Layanan berikut diupayakan kembali pulih dalam kurun waktu paling lama 24 (dua puluh empat) jam bila ada bencana:

1. Penerbitan Sertifikat,
2. Pencabutan Sertifikat,
2. Penerbitan CRL, dan

These services are expected within 24 (twenty four) hours in case of disaster:

1. Certificate issuance,
2. Certificate revocation,
2. CRL issuance, dan

3. Publikasi CRL dan Sertifikat.

3. *Certificate and CRL publication.*

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan PSrE Digisign rusak secara fisik dan semua salinan Kunci Privat milik PSrE Digisign hancur, PSrE Digisign melakukan proses pencabutan Sertifikat sebagaimana diatur pada Bagian 5.7.3.

In the case of a disaster whereby all Digisign CA installations are physically damaged and all copies of the Digisign CA Signing Key are destroyed as a result, Digisign CA requests that its Certificates be revoked as governed in Section 5.7.3.

PSrE Digisign memelihara suatu sistem online dan offline pada Pusat Data PSrE Digisign. Fasilitas Pusat Pemulihan Bencana PSrE Digisign tersedia bila Pusat Data berhenti beroperasi.

Digisign CA maintains an online system and offline system. Digisign CA's Disaster Recovery Center is available if the primary facility (main site) should cease operation.

5.8 Penutupan PSrE Digisign / *Digisign CA Termination*

Bila ada keadaan yang menyebabkan diakhirinya layanan PSrE Digisign dengan persetujuan dari *Policy Authority*, PSrE Digisign akan memberitahu Menteri, Pengawas Penyelenggaraan Sertifikasi Elektronik (P2SE), PSrE Induk, LS PSrE, Pemilik, dan Pengandal serta pihak berwenang lainnya. Rencana aksi PSrE Digisign adalah sebagai berikut, namun tidak terbatas pada:

1. Memberitahu status layanan ke pengguna yang terkena dampak,
2. Mencabut semua Sertifikat,
3. Menyimpan dalam jangka panjang informasi PSrE Digisign dan memastikan bahwa para Pemilik bisa mengakses informasi Sertifikat sesuai

If there are circumstances that cause the termination of Digisign CA's services with the approval of the Policy Authority, Digisign CA will notify the Minister, Root CA, CA Certification Bodies, Subscriber, Relying Parties and other relevant authorities. Digisign CA's action plans are as follows, but are not limited to:

1. *Notify affected users of service status,*
2. *Revoke all Certificates,*
3. *Store Digisign CA information in the long term and ensure that Subscriber can access Certificate information according to the validity period of the*

dengan masa berlaku Sertifikatnya,
4. Menyediakan dukungan berkelanjutan dan menjawab pertanyaan, dan
5. Menangani dengan tepat pasangan kunci PSrE Digisign dan perangkat keras yang terkait yaitu dengan menghancurkan sistem IKP dan Kunci Privat PSrE Digisign.

Certificate,
4. *Provide ongoing support and answer questions, and*
5. *Properly handle Digisign CA key pairs and associated hardware by destroying the Digisign CA PKI and Private Key systems.*

6. KENDALI KEAMANAN TEKNIS / *TECHNICAL SECURITY CONTROLS*

6.1 Pembangkitan dan Instalasi Pasangan Kunci / *Key Pair Generation and Installation*

6.1.1 Pembangkitan Pasangan Kunci / *Key Pair Generation*

Tabel berikut berisi persyaratan minimal pembangkitan Pasangan Kunci pada sistem PSrE Digisign.

The table below describes the minimum requirements for key pair generation at Digisign CA.

Entitas / *Entity*	**FIPS 140-2 Level**	**Perangkat Keras atau Perangkat Lunak (Modul Kriptografi) / *Hardware or Software (Cryptographic Module)***	**Dibangkitkan di dalam Modul Kriptografis / *Generated in Cryptographic Module***
Digisign CA	3	Perangkat Keras / *Hardware*	Ya / *Yes*
Digisign TSA	3	Perangkat Keras / *Hardware*	Ya / *Yes*
OCSP Responder	3	Perangkat Keras / *Hardware*	Ya / *Yes*
Pemilik untuk TTE / Subscriber for Signature	2	Perangkat Keras / *Hardware*	Ya / *Yes*
	1	Perangkat Lunak atau Perangkat Keras (apabila kunci dibangkitkan di perangkat Pemilik) *Software or Hardware (If Key is generated in Subscriber's mobile device)*	Ya / *Yes*

Kontrol multipihak dibutuhkan untuk pembangkitan pasangan kunci PSrE Digisign sebagaimana diatur pada Bagian 6.2.2. Pemisahan peran yang tepat atas proses pembuatan kunci didokumentasikan di dalam dokumen internal PSrE Digisign. Pihak ketiga yang independen memvalidasi pelaksanaan prosedur pembangkitan kunci baik dengan menyaksikan pembangkitan

Multi-party control is required for the generation of Digisign CA key pairs. The proper segregation of roles for the key generation process is documented in internal Digisign CA documents. An independent third party validates the execution of key generation procedures either by witnessing key generation or by checking signed and documented records of

kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci.	*key generation.*
Jika pembangkitan Pasangan Kunci Pemilik dilakukan oleh PSrE Digisign, maka menghasilkan jejak audit yang dapat diverifikasi, yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur diikuti.	*If Subscriber's Key pair generation is done by Digisign CA, it results in a verifiable audit trail, which demonstrates that the security requirements for procedures were followed.*

6.1.2 Pengiriman Kunci Privat ke Pemilik / *Private Key Delivery to Subscriber*

Kunci Privat Pemilik yang dibangkitkan oleh PSrE Digisign tidak dikirimkan ke Pemilik, Kunci Privat Pemilik dititipkan di PSrE Digisign, dan Pemilik secara sadar menyetujui dokumen Perjanjian Kepemilikan Sertifikat.	*The Subscriber's Private Key that is generated by Digisign CA is not sent to the Subscriber, the Subscriber's Private Key is deposited with Digisign CA, and the Subscriber approves the Subscriber Agreement document.*

6.1.3 Pengiriman Kunci Publik ke Penerbit Sertifikat / *Public Key Delivery to Certificate Issuer*

Pasangan Kunci Pemilik dibangkitkan oleh PSrE Digisign. Kunci Publik dilekatkan pada Sertifikat Pemilik oleh PSrE Digisign	*The Subscribers Key Pair is generated by Digisign CA. Public Key is attached to the Subscribers Certificate by the Digisign CA.*

6.1.4 Pengiriman Kunci Publik PSrE Digisign kepada Pengandal / CA Public Key Delivery to Relying Parties

Setiap Sertifikat yang diterbitkan oleh PSrE Digisign berisi Kunci Publik. PSrE Digisign tidak mengirimkan Kunci Publik kepada Pengandal, Pengandal dapat memvalidasi	*Public Key is included in electronic Certificates issued by Digisign CA. Digisign CA does not send Public Keys to Relyers. Relyers can validate Subscriber's Public*

Kunci Publik Pemilik Sertifikat dengan memeriksa validitas sertifikat menggunakan OCSP atau CRL yang diterbitkan oleh PSrE Digisign.	*Keys through checking validity of the Certificate by using Digisign CA's OCSP or CRL published by Digisign CA.*
Penjelasan tanggung jawab tentang publikasi dan repositori Sertifikat mengacu pada Bagian 2.1.	*Certificate publication and repository responsibilities are referred to Section 2.1.*

6.1.5 Ukuran Kunci / *Key Sizes*

PSrE Digisign membuat dan memakai Kunci RSA 4096-bit dengan *Secure Hash Algorithm* versi 2 (SHA-256) untuk menandatangani Sertifikat dan CRL yang diterbitkannya dan RSA 2048 bit untuk kunci Pemilik.	*Digisign CA generates and uses a 4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256) to sign the Certificate and CRL it issues and a 2048 bit RSA for the Subscriber key.*

6.1.6 Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik / *Public Key Parameters Generation and Quality Checking*

Pembangkitan pasangan kunci menghasilkan pasangan kunci yang sesuai dengan FIPS 186-4.	*Key pair generation generates FIPS 186-4 compliant key pairs.*

6.1.7 Tujuan Penggunaan Kunci (pada field key usage – X.509 V3) / *Key Usage Purposes (as per X.509 v3 key usage field)*

Penggunaan kunci dibatasi oleh ekstensi Key Usage pada Sertifikat X.509. Semua Sertifikat menyertakan ekstensi *KeyUsage* dan ditandai sebagai Critical.	*The use of a specific key is constrained by the key usage extension in the X.509 Certificate. All Certificates include a keyUsage extension and be marked as critical.*

Kunci yang terikat dengan Sertifikat Pemilik digunakan hanya untuk menandatangani. Kunci-kunci PSrE Digisign dipakai untuk melakukan penandatanganan Sertifikat (*keyCertSign*) dan penandatanganan CRL (*cRLSign*).	*Keys that are bound into Subscriber Certificates are used only for signing.* *Digisign CA keys are used for Certificate signing (keyCertSign) and CRL signing (cRLSign).*

6.2 Kendali Kunci Privat Dan Kendali Teknis Modul Kriptografis / *Private Key Protection and Cryptographic Module Engineering Controls*

6.2.1 Kendali dan Standar Modul Kriptografis / *Cryptographic Module Standards and Controls*

PSrE Digisign menggunakan modul kriptografi sesuai standard FIPS untuk pembangkitan Kunci PSrE Digisign dan Kunci Pemilik dengan level sesuai tabel pada bagian 6.1.1. dengan aktivasi yang diotentikasi sesuai Bagian 6.2.2.	*Digisign CA uses a cryptographic module that complies with the FIPS 140-2 Level 3 standard to generate Digisign CA's Keys and Subscribers Keys as stipulated at Section 6.2.2.*
Kunci privat Pemilik hanya dapat diakses oleh Pemilik melalui 2 (dua) faktor otentikasi yang berupa kombinasi dari faktor "what you know", "what you have" atau "what you are".	*The Subscriber's private key can only be accessed by the Subscriber via 2 (two) factor authentication that consists of "what you know", "what you have" or "what you are" combination.*

6.2.2 Kendali Multi Personil (n dari m) Kunci Privat / *Private Key (n out of m) Multi-Person Control*

PSrE Digisign mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif diakses melalui kendali multipersonel sebagaimana	*Digisign CA implements technical and procedural mechanisms that require the participation of several trusted roles to carry out sensitive cryptographic operations accessed through multi-person control as set out in Section 5.2.2 (a certain number of*

diatur pada Bagian 5.2.2 (sejumlah orang dibutuhkan dalam setiap tugas).

people are required for each task).

Modul kriptografis yang memuat seluruh kunci penandatanganan PSrE tidak boleh diaktivasi atau diakses hanya oleh 1 (satu) orang. Kunci penandatanganan PSrE harus dicadangkan hanya melalui kendali multi personel. Akses ke kunci penandatanganan PSrE yang dicadangkan untuk pemulihan bencana harus melalui kendali multi personel. Nama-nama pihak yang terlibat dalam kendali multi personel harus dicatat dalam sebuah daftar yang tersedia untuk pemeriksaan selama Audit.

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA signing key. CA signing keys shall be backed up only under multi-party control. Access to CA signing keys backed up for disaster recovery shall be under multi-party control. The names of the parties used for multi-party control shall be maintained on a list that shall be made available for inspection during Compliance Audits.

6.2.3 Escrow Kunci Privat / *Private Key Escrow*

Kunci Privat PSrE Digisign tidak dieskro. PSrE Digisign tidak melakukan eskro terhadap Kunci Privat Pemilik.

Digisign CA Private Key is not escrowed. Digisign CA does not escrow Subscribers Private Keys.

Kunci Privat Pemilik yang terasosiasi dengan Sertifikat yang berisi *key usage digitalSignature* tidak dieskro.

Subscriber's Private Key associated with a Certificate that asserts a digitalSignature key usage is not escrowed.

6.2.4 Cadangan (*Backup*) Kunci Privat / *Private Key Backup*

Kunci Privat PSrE Digisign dicadangkan di bawah kendali multipihak yang sama dengan kunci tanda tangan asli. Paling tidak satu salinan dari Kunci Privat disimpan off-site. Semua salinan Kunci Privat PSrE Digisign dilindungi dengan cara yang sama dengan aslinya.

Digisign CA Private Keys are backed up under the same multiparty control as the original signature keys. At least one copy of the Private Key is kept off-site. All copies of the Digisign CA Private Key are protected in the same way as the original.

Kunci Privat Pemilik yang dititipkan pada PSrE Digisign dicadangkan dan dienkripsi dengan pembungkus kunci dari modul kriptografis pembangkit terkait.	*Subscriber's Private Key stored in Digisign CA is backed up with key wrapper encryption from its cryptographic module origin.*
Semua backup Kunci Publik Pemilik dicatat dan dilindungi dengan cara yang sama dengan Kunci Publik asal.	*All backups of the Subscriber's Public Key shall be accounted for and protected in the same manner as the original.*

6.2.5 Pengarsipan Kunci Privat / *Private Key Archival*

Kunci Privat PSrE Digisign dan Kunci Privat Signing Pemilik tidak diarsipkan.	*Digisign CA's Private Keys and Subscriber Private Keys for Signing are not archived.*

6.2.6 Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografis / *Private Key Transfer Into or From the Cryptographic Module*

Kunci Privat PSrE Digisign diekspor dari modul kriptografis hanya untuk melaksanakan prosedur pencadangan kunci PSrE Digisign. Kunci Privat PSrE Digisign tidak pernah sekalipun berada dalam bentuk *plaintext* di luar modul kriptografi.	*Digisign CA Private Keys is exported from the cryptographic module only to carry out the Digisign CA key backup procedure. Digisign CA Private Keys are never once in plaintext outside the cryptography module.*
Pemindahan Kunci Privat dalam kondisi terenkripsi dari satu modul kriptografis ke yang lain. Kunci pemindahan yang dipakai untuk mengenkripsi Kunci Privat ditangani dengan cara yang sama dengan Kunci Privat.	*Private Key transfer is encrypted from one cryptographic module to another. The transfer key used to encrypt the Private Key is handled in the same way as the Private Key.*
Ketika PSrE Digisign mengetahui bahwa Kunci Privat Pemilik telah disampaikan kepada orang atau entitas yang tidak	*If Digisign CA becomes aware that a Subscriber's Private Key has been communicated to an unauthorized person or*

berwenang dan berafiliasi dengan Subscriber tersebut, maka PSrE Digisign mencabut semua Sertifikat yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.	*an organization not affiliated with the Subscriber, Digisign CA revokes all Certificates that include the Public Key corresponding to the communicated Private Key.*

6.2.7 Penyimpanan Kunci Privat pada Modul Kriptografis / *Private Key Storage on Cryptographic Module*

PSrE Digisign menyimpan Kunci Privatnya dalam perangkat FIPS 140-2 Level 3. Kunci Privat Pemilik yang dibangkitkan oleh PSrE Digisign disimpan dalam perangkat minimal FIPS 140-2 Level 2. Kunci Privat tidak dapat diakses tanpa mekanisme autentikasi.	*Digisign CA stores its Private Keys on FIPS 140-2 level 3 devices. Subscriber Private Keys that are generated by Digisign CA are stored on minimum FIPS 140-2 level 2 devices. The Private Keys are not accessible without an authentication mechanism.*

6.2.8 Metode Pengaktifan Kunci Privat / *Method of Activating Private Key*

Aktivasi operasi Kunci Privat PSrE Digisign dilakukan oleh personil yang berwenang dan memerlukan kendali multipihak.	*Activation of a Digisign CA Private Key operation is carried out by authorized personnel and requires multi-party control.*
Kunci Privat Pemilik yang pasangan kuncinya dibangkitkan oleh PSrE Digisign diaktifkan bersamaan dengan penandatangan permohonan sertifikat (*certificate signing request*/CSR) dengan Kunci Privat tersebut. Otentikasi Pemilik mengacu butir 4.2.3	*The Subscriber's Private Key, whose key pair is generated by Digisign CA, is activated simultaneously with the signing of the Certificate Signing Request (CSR) using that Private Key. The Subscriber's authentication refers to section 4.2.3.*

6.2.9 Metode Penonaktifan Kunci Privat / *Method of Deactivating Private Key*

Modul kriptografis yang sudah diaktivasi	*The cryptographic modules that have been*

tidak ditinggal tanpa pengawasan atau dapat diakses secara tidak sah. Dalam hal modul kriptografis akan dinonaktifkan, modul kriptografis dinonaktifkan oleh personel yang berwenang sebagaimana didefinisikan dalam CPS. Ketika PSrE Digisign tidak lagi beroperasi, Kunci Privat PSrE Digisign dihapus dari modul kriptografis. Penonaktifan kunci Pemilik karena penghentian operasional PSrE Digisign mengikuti prosedur Penutupan PSrE Digisign.	*activated are not left unattended or otherwise available to unauthorized access. When the cryptographic module is about to be deactivated, the cryptographic module is deactivated by an authorized person as defined in the applicable CPS. When Digisign CA is no longer operational, its Private Keys are removed from the cryptographic module. Deactivation of the Subscriber key due to the cessation of CA Digisign operations follows the CA Digisign Closing procedure*

6.2.10 Metode Penghancuran Kunci Privat / *Method of Destroying Private Key*

Sertifikat yang terkait dengan Kunci Privat tersebut telah dicabut atau kadaluwarsa. Penghancuran Kunci Privat dan salinannya dapat dilakukan dengan menimpa (overwrite) Kunci Privat atau menginisialisasi modul dengan fungsi *factory reset* dari modul kriptografis sehingga tidak ada lagi informasi yang dapat 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 dihancurkan secara fisik. Proses penghancuran dilakukan pada lingkungan fisik yang aman.	*Digisign CA's Private Keys are destroyed by the trusted roles when they are no longer needed or when the Certificate to which they correspond has expired or are revoked. All the private keys and their backups are destroyed by either overwriting the data, or by initiating factory reset function in the cryptographic module, in a manner that any information cannot be used to recover any part of the private key. If the functions of cryptographic modules are not accessible in order to destroy the key contained inside, then the cryptographic modules are physically destroyed. The destruction operation is realized in a physically secure environment.*
PSrE Digisign mengatur prosedur penghancuran Kunci Privat Pemilik.	*Digisign CA set the procedure for Subscriber's Private Key destruction.*

6.2.11 Peringkat Modul Kriptografis / *Cryptographic Module Rating*

Seperti diuraikan dalam bagian 6.2.1.	*As described in point 6.2.1*

6.3 Aspek Lain dari Manajemen Pasangan Kunci / *Other Aspects of Key Pair Management*

6.3.1 Pengarsipan Kunci Publik / *Public Key Archival*

Semua Kunci Publik yang digunakan untuk tujuan verifikasi diarsipkan setidaknya selama 5 (lima) tahun sebagai satu kesatuan dari Sertifikat yang diterbitkan. Rincian tentang pengarsipan diatur pada Bagian 5.5.	*All Public Keys used for verification purposes are archived as integral parts of the Certificates issued for at least 5 (five) years. Detail on archival is described in Section 5.5.*

6.3.2 Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci / *Certificate Operational Periods and Key Pair Usage Periods*

Periode operasi pasangan kunci sama dengan periode operasi sertifikat terkait. Operasi pasangan kunci dan periode operasional Sertifikat terkait adalah sebagai berikut:	*The operating period of the key pair equals the corresponding Certificate operation period. The operating period of the key pair and the operating period of the corresponding Certificate as follow:*

Kunci/Key	Algoritma/Algorithm			
	2048 bit Keys (RSA)		4096 bit Keys (RSA)	
	Kunci Private / Private Key	Sertifikat / Certificate	Kunci Private / Private Key	Sertifikat / Certificate
Digisign CA	n/a	n/a	10 tahun / 10 years	10 tahun / 10 years

TSA Digisign	3 tahun / 3 years	3 tahun / 3 years	n/a	n/a
Pemilik untuk TTE / Subscriber for Digital Signature	maksimal 2 tahun / maximum 2 years	maksimal 2 tahun / maximum 2 years	n/a	n/a
Segel Elektronik Badan Usaha / Business Entity Seal	maksimal 2 tahun / maximum 2 years	maksimal 2 tahun / maximum 2 years	n/a	n/a

6.4 Data *Aktivasi* / *Activation Data*

6.4.1 Pembangkitan dan Instalasi Data Aktivasi / *Activation Data Generation and Installation*

Pembangkitan dan penggunaan data aktivasi PSrE Digisign untuk mengaktifkan Kunci Privat PSrE Digisign dibuat pada saat *key ceremony* (merujuk pada Bagian 6.1.1). Data aktivasi dibangkitkan secara otomatis dengan modul kriptografis yang sesuai.

Generation and use of activation data to activate Digisign CA's Private Keys is made during a key ceremony (Refer to Section 6.1.1). Activation data is generated automatically by the appropriate cryptographic modules.

Data aktivasi untuk mengaktifkan Kunci Privat PSrE Digisign dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan.

The activation data used to activate Private Keys is protected based on an appropriate security level in accordance with the cryptographic module used.

Jika data aktivasi ditransmisikan maka data aktivasi ditransmisikan melalui saluran yang dilindungi dengan perlindungan yang sesuai dan dapat diketahui tempat dan waktu transmisi dari modul kriptografis yang terasosiasi dengan data aktivasi tersebut.

If the activation data is transmitted, it is via an appropriately protected channel, and distinct in time and place from the associated cryptographic modules.

Penggunaan data aktivasi Kunci Privat

The usage of the Subscriber's Private Key's

Pemilik dimasukkan oleh Pemilik saat aktivasi.	*activation data shall be entered by the Subscriber upon activation.*

6.4.2 Perlindungan Data Aktivasi / *Activation Data Protection*

Data aktivasi Kunci Privat PSrE Digisign dilindungi dari pengungkapan kerahasiaan melalui kombinasi antara kriptografis dan mekanisme kendali akses fisik. Data aktivasi Kunci Privat PSrE Digisign disimpan dalam token fisik.	*Digisign CA Private Key's activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. Digisign CA's activation data is stored in a physical token.*
Token fisik diakses dengan *passphrase* yang dihafal. Tulisan dari *passphrase* tersebut diamankan pada tingkat yang setara dengan pengamanan modul kriptografis dan tidak disimpan bersamaan dengan modul kriptografis.	*Physical tokens are accessed by passphrase memorization. Written passphrase is secured at the equal level with the cryptographic module's security and stored separately with the cryptographic module.*
Kesalahan memasukkan *passphrase* pada modul kriptografis setelah 3 (tiga) kali kesalahan akan menyebabkan aktifnya pewaktu penalti yang akan bertambah terus menerus seiring jumlah kegagalan sesuai konfigurasi modul kriptografis yang digunakan.	*A failed attempt in entering a passphrase on the cryptographic module after 3 (three) failure will cause an active penalty timer which will increase continuously along with the number of failures according to the configuration of the cryptographic module used.*
Setelah mengalami kegagalan login sebanyak 3 (tiga) kali, akun pemilik dikunci sementara waktu selama 10 (sepuluh) menit.	*After 3 (three) times of failed login attempts, the subscriber account is temporarily locked for 10 (ten) minutes.*
Pemilik diwajibkan untuk selalu menjaga kerahasiaan data aktivasi.	*Subscribers are obliged to always keep the activation data secret.*

6.4.3 Aspek Lain dari Data Aktivasi / *Other Aspects of Activation Data*

Tidak ada ketentuan.	*No Condition.*

6.5 Kendali *Keamanan* Komputer / *Computer Security Controls*

6.5.1 Persyaratan Teknis Keamanan Komputer Spesifik / *Specific Computer Security Technical Requirements*

PSrE Digisign memastikan bahwa sistem yang menjaga perangkat lunak PSrE Digisign dan file data aman dari akses yang tidak berhak. Semua komputer yang merupakan bagian dari sistem PSrE Digisign telah dikonfigurasi dan diperkuat (*hardening*) menggunakan praktik terbaik industri. Semua sistem operasi membutuhkan identifikasi dan otorisasi untuk login yang di autentikasi.	*Digisign CA ensures that the systems that maintain Digisign CA software and data files are secure from unauthorized access. All computers that are part of a Digisign CA system are configured and hardened using industry best practices. All operating systems require identification and authentication for authenticated logins.*
Fungsi keamanan komputer berikut disediakan oleh sistem operasi, atau melalui kombinasi sistem operasi, perangkat lunak, dan perlindungan fisik. Fungsi keamanan PSrE Digisign mencakup namun tidak terbatas untuk: 1. Membutuhkan login terautentikasi, 2. Menyediakan *Role Base Access Control,* 3. Menyediakan kapabilitas audit keamanan, 4. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data, dan 5. Menyediakan perlindungan mandiri	*The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical protection. Digisign CA security functions include but are not limited to:* *1. Requires authenticated login,* *2. Provide Role Base Access Control,* *3. Provide security audit capabilities,* *4. Requires use of cryptography for communication sessions and database security, and* *5. Provides self-protection for the operating system*

untuk sistem operasi.

Ketika peralatan PSrE Digisign di-host pada *platform* yang dievaluasi untuk mendukung persyaratan jaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak dan sistem operasi) beroperasi dalam konfigurasi yang dievaluasi. Minimal *platform* tersebut menggunakan versi yang sama dari sistem operasi komputer seperti yang menerima penilaian evaluasi.	*When Digisign CA equipment is hosted on a platform that is evaluated to support computer security assurance requirements then the system (hardware, software and operating system) operates in the configuration that is evaluated. At a minimum the platform uses the same version of the computer operating system as the one receiving the evaluation assessment.*
Sistem komputer PSrE Digisign dikonfigurasi dengan akun yang diperlukan dan layanan jaringan yang diperlukan.	*Digisign CA computer systems are configured with the required accounts and required network services.*

6.5.2 Peringkat Keamanan Komputer / *Computer Security Rating*

Tidak ada ketentuan.	*No Stipulation.*

6.6 Kendali Teknis Siklus Hidup / *Life Cycle Technical Controls*

6.6.1 Kendali Pengembangan Sistem / *System Development Controls*

Kendali pengembangan sistem PSrE Digisign 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	*The System Development Controls for the Digisign CA are as follows:* *1. Use software that has been designed and developed under a formal, documented development methodology,* *2. Hardware and software procured is purchased in a fashion to reduce the likelihood that any particular component was tampered with,*

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 serta jaringan komputer didedikasikan untuk melaksanakan aktivitas IKP,
5. Perawatan dilakukan untuk mencegah perangkat lunak yang berbahaya dimuat ke perangkat. Perangkat keras dan perangkat lunak selalu dipindai untuk kode-kode berbahaya pada penggunaan pertama dan secara periodik,
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.

3. *Hardware and software is developed in a controlled environment, and the development process is defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software,*
4. *The hardware and software is dedicated to performing the PKI activities.*
5. *Proper care is taken to prevent malicious software from being loaded onto the equipment. Digisign CA scans hardware and software for malicious code on first use and periodically thereafter,*
6. *Hardware and software updates are purchased or developed in the same manner as original equipment and installed by trusted and trained personnel in a defined manner.*

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

For both ready-made software and in-house developed software by Digisign CA that are used in certificate management, are checked to ensure the software is genuine and fully tested in non-production environment before deployment in production environment. Any changes to

reviu Kontrol Manajemen Perubahan dan persetujuan.

systems or components go through the Change Management Control review and approval process.

6.6.2 Kendali Manajemen Keamanan / *Security Management Controls*

Konfigurasi dari sistem PSrE Digisign serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen PSrE Digisign. Mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi milik PSrE Digisign menggunakan *File Integrity Monitoring* (FIM).

The configuration of the Digisign CA system and all modifications and upgrades are documented and controlled by Digisign CA Management. A mechanism for detecting unauthorized modifications to Digisign CA's software or configuration using File Integrity Monitoring (FIM).

PSrE Digisign memiliki prosedur dan jadwal untuk pemeliharaan sistem serta pemeliharaan dari prosedur dan jadwal tersebut. Personel PSrE Digisign bertanggung jawab melakukan monitoring dan pemeriksaan sistem secara rutin. Sebagai tambahan, PSrE Digisign memiliki proses otomatis yang menginformasikan Peran Terpercaya ketika ada aktivitas yang tidak wajar pada sistem.

Digisign CA has procedures and schedules for system maintenance and maintenance of these procedures and schedules. Digisign CA personnel are responsible for monitoring and checking the system regularly. In addition, Digisign CA has an automated process that informs Trusted Roles when there is unusual activity on the system.

6.6.3 Kendali Keamanan Siklus Hidup / *Life Cycle Security Controls*

PSrE Digisign melakukan pengawasan terhadap kebutuhan skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak yang telah dievaluasi dan disertifikasi oleh sistem keamanan informasi.

Digisign CA supervises the need for a maintenance scheme to maintain the level of trustworthiness of hardware and software that have been evaluated and certified by the information security system.

6.7 Kendali Keamanan Jaringan / *Network Security Controls*

PSrE Digisign menggunakan tindakan keamanan jaringan yang sesuai untuk memastikan agar terjaga dari DoS dan serangan intrusi. Langkah-langkah tersebut termasuk penggunaan *firewall* dan menyaring *router*. *Port* dan layanan jaringan yang tidak digunakan dimatikan. Hanya perangkat lunak jaringan yang diperlukan untuk mengoperasikan layanan PSrE Digisign yang diizinkan terpasang.

Digisign CA uses appropriate network security measures to ensure that it is protected against DoS and intrusion attacks. Such measures include the use of firewalls and filtering routers. Unused network ports and services are turned off. Only required network software for Digisign CA services operation is permitted to be installed.

6.8 Tanda Waktu / *Time-Stamping*

Jam server online PSrE Digisign disinkronkan menggunakan *Network Time Protocol*. Waktu *server offline* disinkronkan secara manual. Sebuah otoritas khusus untuk menyediakan waktu yang terpercaya juga bisa digunakan jika perlu, misalnya dengan membentuk sebuah otoritas *timestamp* tersendiri. Waktu yang didapatkan dari layanan waktu di atas akan digunakan untuk menentukan waktu pada saat:

1. Validitas waktu permulaan untuk sebuah Sertifikat PSrE Digisign,
2. Pencabutan Sertifikat PSrE Digisign,
3. Pembaruan CRL, dan
4. Penerbitan Sertifikat Pemilik dan entitas.
5. Respon OCSP.

Digisign CA's online server clocks are synchronized using the Network Time Protocol. The offline server time is manually synced. A special authority to provide reliable times can also be used, if necessary, for example by establishing a separate timestamp authority. The time obtained from the above time service will be used to determine the time when:

1. *Start-up validity for a Digisign CA Certificate,*
2. *Digisign CA Certificate Revocation,*
3. *CRL updates, and*
4. *Issuance of Subscriber and entity Certificates.*
5. *OCSP Response.*

Prosedur elektronik atau manual digunakan untuk tetap mempertahankan akurasi waktu pada sistem. Pencocokan jam merupakan sebuah aktivitas yang dapat diaudit sebagaimana diatur pada Bagian 5.4.1.

Electronic or manual procedures are used to maintain time accuracy in the system. Hour's matching is an auditable activity as stipulated in Section 5.4.1.

Dalam menyelenggarakan layanan Penanda Waktu Elektronik tersertifikasi, PSrE Digisign mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

When providing a certified electronic timestamp service, Digisign CA refers to the national timestamp provided by a government agency whose authority concerns meteorology, climatology, and geophysics.

7. PROFIL OCSP, CRL, DAN SERTIFIKAT / *CERTIFICATE, CRL, AND OCSP PROFILES*

7.1 Profil Sertifikat / *Certificate Profile*

Profil Sertifikat mengikuti RFC 5280 "*Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*". PSrE Digisign melakukan tinjauan terhadap profil Sertifikat yang tersusun di Lampiran C, secara berkala paling sedikit setahun sekali mengacu ke Standar Interoperabilitas PSrE Indonesia.	*Certificate Profiles following RFC 5280 "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile". Digisign CA reviews the Certificate profile as composed at appendix C, regularly at least once a year refer to the Indonesian CA Interoperability Standard.*

7.2 Profil CRL / *CRL Profile*

Profil CRL PSrE Digisign yang tersusun di Lampiran C sesuai dengan Standar Interoperabilitas PSrE Indonesia dan menggunakan CRL dan CRL *entry extension* RFC 5280.	*Digisign CA's CRL Profile as composed at appendix C complies with Indonesian CA Interoperability Standard and uses the RFC 5280 CRL and CRL entry extension.*

7.3 Profil OCSP / *OCSP Profile*

PSrE Digisign mengoperasikan *Online Certificate Status Protocol responder* (responder OCSP) yang tersusun di Lampiran C dengan mengacu kepada Standar Interoperabilitas PSrE Indonesia.	*Digisign CA operates an Online Certificate Status Protocol (OCSP) as composed at appendix C referring to Indonesian CA Interoperability Standard.*

8. AUDIT KEPATUHAN DAN PENILAIAN KELAIKAN LAINNYA / *COMPLIANCE AUDIT AND OTHER ASSESSMENTS*

Praktik dalam CPS ini dirancang untuk memenuhi persyaratan standar industri yang diterima secara umum yaitu ISO/IEC 27001:2022 termasuk standar PSrE Indonesia dari PSrE Induk yaitu Kementerian Komdigi.

The practices in this CPS are designed to meet the requirements of generally accepted industry standards of ISO/IEC 27001:2022 including standard of Indonesia CA from root CA of Komdigi Ministry.

8.1 Frekuensi atau Lingkup Penilaian / *Frequency or Circumstances of Assessment*

PSrE Digisign menjalani audit kepatuhan setiap terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan secara berkala terhadap skema yang telah ditetapkan paling sedikit 1 (satu) tahun sekali. frekuensi atau lingkup Penilaian Kelaikan dan frekuensi penilaian lainnya yang relevan pada CPS.

Digisign CA undergoes a compliance audit every time there is a significant change to the procedures and techniques that are applied periodically to the established scheme at least once a year. The frequency or Circumstances of Assessments and the frequency of other relevant assessments on the CPS.

8.2 Identitas / Kualifikasi Penilai / *Identity / Qualification of Auditor*

Auditor kepatuhan memiliki kualifikasi sebagai berikut:

1. Auditor dilaksanakan oleh tim asesmen independen yang *qualified* dan tidak memiliki konflik kepentingan dengan PSrE Digisign,
2. Memiliki kemampuan untuk melaksanakan audit sesuai dengan standar audit yang diatur dalam peraturan perundang-undangan, termasuk pengetahuan tentang pemanfaatan layanan yang

Compliance auditors have the following qualifications:

1. *The auditor is carried out by a qualified independent assessment team and do not have conflict of interest with Digisign CA,*
2. *Having the capability to conduct audits based on audit standards within the provisions of legal regulations, including knowledge related to the utilization of services involving Electronic Certificates, such as*

menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik, X.509 versi ke-3 PKI *Certificate Policy and Certification Practices Framework*, Undang-Undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah mengenai Penyelenggaraan Sistem dan Transaksi Elektronik, serta Peraturan Menteri yang terkait dengan Tata Kelola Penyelenggaraan Sertifikasi Elektronik,

Electronic Signatures, Electronic Seals, X.509 version 3 PKI Certificate Policy and Certification Practices Framework, the Law on Electronic Information and Transactions, Government Regulations on the Implementation of Electronic Systems and Transactions, and Ministerial Regulations regarding the Governance of Electronic Certification,

3. Memiliki kecakapan dalam memeriksa teknologi IKP, peralatan dan Teknik keamanan informasi, audit keamanan informasi, dan penilaian pihak ketiga (third-party attestation function),

3. Auditors shall have adequate skills on information security audit, information/security device and technique audit, third party attestation function, as well as familiarity with PKI technology,

4. auditor harus memiliki dokumentasi yang menunjukkan bahwa dirinya memenuhi persyaratan kualifikasi auditor untuk suatu skema audit. Dokumentasi tersebut dapat berupa sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah. Selain itu, seorang auditor harus memiliki sertifikasi sebagai auditor sistem informasi (CISA) atau sebagai spesialis keamanan teknologi informasi (IT Security), spesialis IKP. Hal ini diperlukan agar auditor dapat memberikan masukan terkait risiko yang dapat diterima (acceptable risks), strategi mitigasi, dan praktik

4. An auditor must possess documentation evidencing their compliance with the auditor qualification requirements for a given audit scheme. Such documentation may include certifications, accreditations, licenses, or other valid assessments. Furthermore, an auditor is required to hold a certification as an Information Systems Auditor (CISA) or as an Information Technology (IT) Security specialist, PKI specialist. This certification is necessary for the auditor to provide insights concerning acceptable risks, mitigation strategies, and industry best practices,

terbaik dalam industri,

5. Menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.
6. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik professional.

5. *Mastering certain skill sets, competency testing, quality assurance measures such as peer review, standards regarding proper staff assignment, to engagement and requirements for continuing professional education.*
6. *Bound by law, government regulation, or professional code of ethics.*

8.3 Hubungan Penilai dengan Entitas yang Dinilai / *Auditor's Relationship to Assessed Entity*

PSrE Digisign memilih auditor/asesor yang bersifat independen untuk memberikan evaluasi yang tidak memihak. Dalam rangka memastikan independensi dan objektivitas, Penilai tidak terlibat dalam kegiatan pengembangan atau pemeliharaan fasilitas dan/atau CPS milik PSrE Digisign.

Digisign CA selects an independent auditor/assessor to provide impartial evaluations. To ensure independence and objectivity, the Assessor refrains from involvement in the development or maintenance of Digisign CA's facilities and/or its CPS.

Selain larangan konflik kepentingan di atas, dalam menjalankan audit, Penilai menjalin hubungan kontrak yang jelas dengan PSrE Digisign untuk menjaga independensi/ketidakberpihakan Penilai. Penilai diharuskan menjaga standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan pelaksanaan penilaian yang independen secara profesional, selalu mematuhi peraturan perundang-undangan yang

In addition to the above conflict of interest prohibition, during the course of conducting the audit, the Assessor maintains a clear contractual relationship with Digisign CA to preserve the independence and impartiality of the Assessor. The Assessor is required to uphold high ethical standards designed to ensure impartiality and the professional execution of assessments with independence, always in compliance with applicable legal regulations.

berlaku.

8.4 Topik Penilaian / Topics *Covered by Assessment*

Penilaian Kelaikan memiliki tujuan untuk memverifikasi bahwa PSrE Digisign beroperasi sesuai dengan CP PSrE Induk yang berlaku serta sesuai dengan ketentuan peraturan perundang-undangan yang berlaku. Penilaian Kelaikan ini harus mencakup evaluasi terhadap CPS yang berlaku terhadap CP PSrE Induk, dengan tujuan untuk menentukan bahwa CPS telah diimplementasikan dan ditegakkan. Evaluasi ini minimal mencakup aspek organisasi, operasional, pelatihan personel, dan manajemen PSrE Digisign.	*The Fitness Assessment aims to verify that Digisign CA operates in accordance with the applicable Root CP and adheres to the provisions of the prevailing legal regulations. This Fitness Assessment must encompass an evaluation of the applicable CPS in relation to the CP, with the purpose of ascertaining the implementation and enforcement of CPS. This evaluation should, at a minimum, encompass organizational, operational, personnel training, and management aspects of Digisign CA.*
Audit yang dijalankan memenuhi persyaratan dari skema audit yang digunakan dalam penilaian. Persyaratan tersebut dapat berubah sesuai dengan pembaruan skema audit yang berlaku. Skema audit yang baru diberlakukan paling lama dalam waktu 1 (satu) tahun setelah diumumkan secara publik.	*The conducted audit must meet the requirements of the audit scheme employed in the assessment. These requirements may evolve in line with updates to the applicable audit scheme. A new audit scheme shall take effect no later than 1 (one) year after its public announcement.*

8.5 Tindakan yang Diambil Akibat Ketidaksesuaian / *Actions Taken as a Result of Deficiency*

Ketika Penilai menemukan adanya ketidaksesuaian antara bagaimana PSrE Digisign direncanakan, dioperasikan, atau dipelihara dengan persyaratan CP atau CPS yang berlaku, Penilai diharuskan untuk	*When the Assessor identifies discrepancies between how Digisign CA is designed, operated, or maintained and the requirements of the applicable CP or CPS, the Assessor is required to take the*

mengambil langkah-langkah berikut:

1. Mencatat ketidaksesuaian tersebut,
2. Memberitahukan PSrE Digisign, dan
3. Melaporkan hal tersebut kepada PSrE Induk.

following steps:

1. *Record the identified discrepancies,*
2. *Notify Digisign CA, and*
3. *Report the situation to the Parent PSrE.*

PSrE Digisign memiliki tanggung jawab untuk menetapkan tindakan perbaikan yang diperlukan untuk memastikan kepatuhan dengan persyaratan CP/CPS dan/atau kontrak yang relevan, serta melaksanakan tindakan perbaikan tersebut tanpa penundaan.

Digisign CA is responsible for determining the necessary follow-up actions to ensure compliance with the requirements of the CP/CPS and/or relevant contracts and promptly implementing the required corrective measures.

8.6 Laporan Hasil Penilaian / *Communication of Results*

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, diberikan kepada *Policy Authority* sebagaimana diatur pada bagian 8.1. Laporan tersebut mengidentifikasi versi CPS yang digunakan dalam asesmen. Selain itu, hasilnya dikomunikasikan sebagaimana dimaksud pada bagian 8.5.

The Audit Compliance Report, including identification of corrective actions taken or taken by the component, is provided to the Policy Authority as stipulated in section 8.1. The report identifies the CPS versions used in the assessment. In addition, the results are communicated as referred to in section 8.5.

8.7 Audit Internal / *Internal Audit*

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

Audits on operational systems are planned and agreed to minimize the risk of disruption to business processes.

PSrE Digisign terus memonitor tingkat kepatuhannya terhadap CP PSrE Induk, CPS PSrE Digisign, serta ketentuan

Digisign CA continuously monitors its compliance level with the Root CP, Digisign CA's CPS, and the prevailing legal

peraturan perundang-undangan yang berlaku, dan melakukan pengendalian mutu layanan secara ketat. Tindakan ini melibatkan pelaksanaan audit internal setidaknya satu kali dalam setahun terhadap sampel yang dipilih secara acak dari minimal 1 persen total Sertifikat yang diterbitkan dalam tahun yang bersangkutan.

regulations, while rigorously maintaining the quality of its services. This involves conducting internal audits at least once annually on randomly selected samples, constituting at least 1 percent of the total Certificates issued within the given year.

9. BISNIS LAIN DAN MASALAH HUKUM / *OTHER BUSINESS AND LEGAL MATTERS*

9.1 Biaya / Fees

9.1.1 Biaya Penerbitan atau Pembaruan Sertifikat / *Certificate Issuance or Renewal Fees*

PSrE Digisign mengenakan biaya atas layanan yang terkait dengan penerbitan atau pembaruan Sertifikat Pemilik, termasuk dalam situasi penerbitan ulang Sertifikat. Biaya layanan yang dikenakan oleh PSrE Digisign adalah berdasarkan kategori retail dan korporat.

PSrE Digisign charges fees for services related to the issuance or renewal of a Owner's Certificate. The service fees charged by PSrE Digisign are based on retail and corporate categories.

Biaya layanan untuk kategori retail mengikuti harga yang ditetapkan PSrE Digisign secara umum sedangkan biaya layanan untuk kategori korporat diatur melalui suatu perjanjian kontrak yang disetujui bersama.

Service fees for the retail category follow the prices set by PSrE Digisign in general, while service fees for the corporate category are regulated through a mutually agreed contractual agreement.

Baik kategori retail dan korporat, Pemilik Sertifikat tetap diwajibkan mematuhi CPS PSrE Digisign dan kebijakan layanan PSrE Digisign.

In both retail and corporate categories, Certificate Subscriber are still required to comply with the Digisign CA CPS and Digisign CA service policies.

9.1.2 Biaya Pengaksesan Sertifikat / *Certificate Access Fees*

PSrE Digisign tidak mengenakan biaya kepada Pemilik dan Pengandal untuk mengakses Sertifikat.

Digisign CA does not charge fees to Subscriber and Relying Parties to access Certificate.

9.1.3 Biaya Pengaksesan Informasi Status atau Pencabutan / *Revocation or Status Information Access Fees*

PSrE Digisign tidak mengenakan biaya kepada Pemilik dan Pengandal untuk mengakses daftar pencabutan atau status informasi Sertifikat.	*Digisign CA does not charge Subscriber and Relying Parties for access to revocation lists or certificate status information.*

9.1.4 Biaya Layanan Lainnya / *Fees for Other Services*

PSrE Digisign dapat mengenakan biaya untuk layanan tambahan lainnya seperti biaya e-meterai dan biaya integrasi layanan yang diatur melalui suatu perjanjian kontrak yang disetujui bersama.	*PSrE Digisign may charge fees for other additional services such as e-stamp fees and service integration fees which regulated through a mutually agreed contractual agreement.*

9.1.5 Kebijakan Pengembalian Biaya / *Refund Policy*

Pemilik harus mengajukan permohonan pengembalian biaya dalam jangka waktu 30 hari kalender sejak Sertifikat diterbitkan. PSrE Digisign mencabut setiap sertifikat Pemilik yang mengajukan pengembalian biaya. PSrE Digisign mengatur lebih lanjut hal ini pada dokumen Kebijakan Jaminan.	*Subscribers should submit a refund request within 30 (thirty) calendar days after certificate issuance. Digisign CA revokes every Subscriber certificate which requested to be refunded. Digisign CA regulates Refund Policy in Warranty Policy document.*

9.2 Tanggung Jawab Keuangan / *Financial Responsibility*

9.2.1 Cakupan Asuransi / *Insurance Coverage*

PSrE Digisign menjamin atas kerugian yang diakibatkan kelalaiannya dalam memenuhi kewajibannya sesuai peraturan perundang-undangan yang berlaku di Negara Republik Indonesia.	*Digisign CA guarantees for losses caused by its negligence in fulfilling its obligations in accordance with applicable Regulation in the Republic of Indonesia.*
Ketentuan Jaminan dan Batasan Jaminan	*Warranty Terms and Warranty Limitations*

atas layanan PSrE Digisign terdapat dalam dokumen Kebijakan Jaminan. Dokumen dapat dilihat di halaman repositori PSrE Digisign: https://repository.digisign.id/

for Digisign CA services are contained in the Guarantee Policy document. Documents can be viewed on the Digisign CA repository page: https://repository.digisign.id/

9.2.2 Aset lainnya / *Other Assets*

PSrE Digisign menjaga kapasitas finansial yang memadai untuk mendukung operasionalnya agar dapat memenuhi kewajibannya terhadap Partisipan IKP, sesuai dengan ketentuan yang diuraikan pada Bagian 1.3.

Digisign CA maintains a reasonable financial capacity to support its operations in fulfilling its obligations to PKI Participants, as outlined in Section 1.3.

9.2.3 Cakupan Asuransi atau Garansi untuk Pemilik / *Insurance or Warranty Coverage for End-Entities*

PSrE Digisign menyediakan jaminan atau garansi untuk para Pemilik Sertifikat jika PSrE Digisign sengaja atau lalai sebagaimana diatur lebih lanjut pada Kebijakan Jaminan yang dapat diakses pada halaman repositori PSrE Digisign: https://repository.digisign.id

Digisign CA provides insurance or warranty policy to Certificate Subscriber in cases where Digisign CA intentionally or negligently fails to meet its responsibilities, as further outlined in the Warranty Policy accessible through the Digisign CA repository page: https://repository.digisign.id

9.3 Kerahasiaan Informasi Bisnis / *Confidentiality of Business Information*

9.3.1 Cakupan Informasi Rahasia / *Scope of Confidential Information*

PSrE Digisign memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia, yang termasuk dalam kategori informasi rahasia antara lain namun tidak terbatas pada:

Digisign CA takes into consideration and provides special handling for categories of confidential information, which include but not limited to:

1. Informasi pribadi sebagaimana diatur pada bagian 9.4;
2. Rekam jejak audit (*audit logs*) dari sistem PSrE Digisign;
3. Data aktivasi pada saat pengaktifan Kunci Privat PSrE Digisign sebagaimana diatur pada bagian 6.4,
4. Dokumentasi bisnis proses PSrE Digisign termasuk dokumen *Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP)*;
5. Laporan audit dari auditor independen sebagaimana diatur pada Bagian 8., dan
6. Hasil penilaian kerentanan.

1. *Personal information as stipulated in Section 9.4,*
2. *Audit logs from the Digisign CA system,*
3. *Activation data when the Digisign CA Private Key is activated, as described in Section 6.4,*
4. *Documentation of Digisign CA's business processes, including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP),*
5. *Audit reports from independent auditors as outlined in Section 8., and*
6. *Vulnerability assessment results.*

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

Unless required by law or court order, prior written consent from the Subscriber is necessary before disclosing the aforementioned information.

9.3.2 Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia / *Information Not Within the Scope of Confidential Information*

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

Information that is not classified as confidential in a CPS document is considered public information. Certificates and information on the status of Certificates belong to the category of public information.

Oleh karena itu, Sertifikat, respon OCSP, CRL beserta informasi pribadi atau perusahaan yang muncul di dalamnya dan di direktori publik tidak dianggap sebagai

In that respect, Certificates, OCSP responses, CRLs and personal or corporate information appearing in them and in public directories are not considered as private or

informasi rahasia.

confidential.

9.3.3 Tanggung Jawab untuk Melindungi Informasi yang Rahasia / *Responsibility to Protect Confidential Information*

PSrE Digisign melindungi informasi rahasia. PSrE Digisign secara jelas menandai informasi yang bersifat rahasia atau menurut sifatnya harus dipahami secara wajar sebagai rahasia dengan label sebagai rahasia dan memperlakukan informasi tersebut dengan tingkat perhatian dan keamanan yang sama dengan informasi rahasia milik sendiri.

Digisign CA protects confidential information. Digisign CA clearly labelled as confidential or by its nature should reasonably be understood as confidential and treat such information with the same degree of care and security as its own confidential information.

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

1. Pelatihan atau peningkatan kesadaran,
2. Perjanjian kontrak pegawai, dan
3. NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

The form of implementation of responsibilities in terms of protection of confidential information includes but is not limited to:

1. *Training or awareness improvement,*
2. *Employee contract agreement, and*
3. *NDA (Non-Disclosure Agreement) with employees, outsourced employees, and partners.*

9.4 Privasi Informasi Pribadi / Privacy *of Personal Information*

9.4.1 Rencana Privasi / *Privacy Plan*

PSrE Digisign menjaga keamanan informasi pribadi sesuai dengan persyaratan yang diatur dalam Kebijakan Privasi yang telah dipublikasikan dalam repositori https://repository.digisign.id dan sesuai dengan ketentuan di Bagian 2.1.

Digisign CA safeguards personal information in accordance with the requirements stipulated in the Privacy Policy, which is publicly available in the repository https://repository.digisign.id and as detailed in Section 2.1.

Kebijakan Privasi ini disesuaikan dengan hukum dan peraturan yang berlaku di Indonesia terkait perlindungan data pribadi serta informasi dan transaksi elektronik. Di dalamnya termuat informasi mengenai pengumpulan data pribadi, bagaimana data tersebut disimpan dan diproses, serta situasi di mana data tersebut dapat diungkapkan.

This Privacy Policy aligns with the applicable laws and regulations in Indonesia concerning the protection of personal data and electronic information and transactions. It contains information about the collection of personal data, how the data is stored and processed, and the circumstances under which the data may be disclosed.

Para Pemilik dan Pengandal memiliki hak untuk mengakses dan memperbaiki atau mengubah informasi pribadi atau informasi organisasi mereka melalui permohonan yang sah kepada PSrE Digisign. Akses terhadap informasi tersebut akan diberikan setelah PSrE Digisign mengambil langkah-langkah untuk memastikan keaslian identitas pihak yang mengajukan permohonan.

Subscribers and Relying Parties are granted access and the ability to correct or modify their personal or organizational information through valid requests made to Digisign CA. Access to such information will be provided after Digisign CA takes steps to authenticate the identity of the requesting party.

PSrE Digisign hanya mengumpulkan data yang diperlukan untuk keperluan pendaftaran dan sertifikasi, dan data tersebut hanya digunakan untuk tujuan tersebut. PSrE Digisign tidak menggunakan data ini untuk tujuan komersial apa pun.

Digisign CA only collects data necessary for registration and certification purposes, and this data is exclusively used for those purposes. Specifically, Digisign CA does not employ this data for any commercial purposes.

9.4.2 Informasi yang diperlakukan sebagai Privat / *Information Treated as Private*

PSrE Digisign melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah, baik terhadap Pemohon yang Sertifikatnya berhasil diterbitkan

Digisign CA protects all the Subscriber's personally identifiable information from unauthorized disclosure, regardless of the acceptance of their applications approval.

(Pemilik) maupun yang ditolak. PSrE Digisign menghapus informasi pribadi Pemohon yang ditolak paling lama 30 (tiga puluh) hari kalender. PSrE Digisign hanya menyimpan nomor identitas kependudukan (NIK) Pemohon disertai alasan penolakan.	*Digisign CA deletes personal information of the rejected Applicants in no later than 30 (thirty) days thereafter. Digisign CA keeps Applicant's national Identity number (NIK number) accompanied by the reason for application's rejection.*
Informasi pribadi dapat diungkapkan atas persetujuan Pemilik terhadap Pengandal. Informasi Pemilik dapat dirilis atas permintaan Pemilik atau sebagaimana diatur oleh hukum yang berlaku. Arsip yang dikelola oleh PSrE Digisign tidak boleh dirilis kecuali yang diizinkan pada bagian 9.4.1.	*Personal information may be disclosed with the Subscriber's consent to the Reliance. Subscriber Information may be released at Subscriber's request or as required by applicable law. Archives maintained by Digisign CA may not be released except as permitted in 9.4.1.*

9.4.3 Informasi yang tidak Dianggap Privat / *Information not Deemed Private*

Informasi yang termasuk dalam Bagian 7 (Sertifikat, CRL dan OCSP) dari CPS ini tidak dianggap privat dan tidak termasuk dalam perlakuan yang diuraikan di bagian 9.4.2.	*Information included in Section 7 (Certificates, CRL and OCSP) of this CPS is not deemed private and is not included to the protection as stipulated in section 9.4.2*
Pelanggaran atas penggunaan informasi pribadi diatur dalam ketentuan peraturan perundang-undangan.	*Violations against personal information are stipulated in laws and regulations.*

9.4.4 Tanggung Jawab Melindungi Informasi Privat / *Responsibility to Protect Private Information*

PSrE Digisign bertanggung jawab untuk menyimpan informasi privat sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan berbentuk digital. Cadangan informasi privat dienkripsi setiap akan	*Digisign CA shall be responsible for securely storing personal information in accordance with the Privacy Policy. The information stored is in digital form. Backup personal information is encrypted every time*

dipindahkan ke media *backup*.

it is moved to the backup media.

9.4.5 Pemberitahuan dan Persetujuan untuk menggunakan Informasi Privat / *Notice and Consent to use Private Information*

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk data pribadi sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. PSrE Digisign mengakomodir semua ketentuan terkait penggunaan informasi privat ke dalam Perjanjian Kepemilikan Sertifikat / *Subscriber Agreement.*

Personal information obtained from the Applicant during the registration process is classified as private data, so it requires approval from the Applicant in order to use the information. Digisign CA accommodates all provisions related to the use of personal information into the Certificate Subscriber Agreement / Subscriber Agreement.

Penggunaan data pribadi harus didasarkan pada pelaksanaan Perjanjian Pemilik atau Perjanjian Pihak Pengandal, atau dasar hukum lainnya, yang mengacu pada Kebijakan Privasi dan ketentuan peraturan perundang-undangan.

The use of private data must be based on the implementation of the Subscriber Agreement or Relying Party Agreement, or other legal basis, which refers to the Privacy Policy and provisions of laws and regulations.

9.4.6 Pengungkapan Berdasarkan Proses Peradilan atau Administratif / *Disclosure Pursuant to Judicial or Administrative Process*

PSrE Digisign tidak membuka informasi privat kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh CPS, diwajibkan oleh hukum, aturan, atau perintah pengadilan.

Digisign CA does not disclose personal information to any third party except as authorized by CPS, required by law, regulation or court order.

9.4.7 Keadaan Pengungkapan Informasi Lainnya / *Other Information Disclosure Circumstances*

Tidak ada ketentuan.	*No Condition.*

9.5 Hak atas Kekayaan Intelektual / *Intellectual Property Rights*

Semua hak kekayaan intelektual PSrE Digisign termasuk semua merek dagang dan hak cipta dari semua dokumen PSrE Digisign termasuk layanan PSrE Digisign (termasuk namun tidak terbatas pada aplikasi perangkat lunak beserta fiturnya, informasi, teks, huruf, angka, susunan warna, gambar, logo, nama, foto, audio, video, audio dan video, struktur basis data, desain, sertifikat yang diterbitkan beserta pasangan kunci yang dibangkitkan) tetap menjadi milik tunggal dari PSrE Digisign.	*All Digisign CA intellectual property rights including all trademarks and copyright of all Digisign CA documents including Digisign CA services (including but not limited to software application and its features, information, text, letter, number, color composition, picture, logo, name, photo, audio, video, audio and video, database structure, design, issued certificate and its generated key pair) remain the sole property of Digisign CA.*
PSrE Digisign tidak melanggar hak kekayaan intelektual pihak lain.	*Digisign CA does not violate the intellectual property rights of others.*

9.6 Pernyataan dan Jaminan / Representations and Warranties

9.6.1 Pernyataan dan Jaminan PSrE Digisign / *Digisign CA Representations and Warranties*

PSrE Digisign menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa: 1. PSrE Digisign mematuhi ketentuan yang diatur dalam CPS ini, 2. PSrE Digisign menerbitkan dan memperbarui CRL sesuai ketentuan dalam CPS ini, 3. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini dan hanya	*Digisign CA state and warrant, as what is set in CPS that:* *1. Digisign CA complies, in all material aspects, with the CPS,* *2. Digisign CA publishes and updates CRL according to stipulations in this CPS,* *3. All Certificates issued meet the minimum requirements and verified in accordance with this CPS and only*

Informasi yang telah diverifikasi yang ditampilkan di Sertifikat,

4. PSrE Digisign menampilkan informasi yang dapat diakses secara publik melalui repositorinya,
5. Kunci Privat PSrE Digisign terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang,
6. Semua pernyataan yang dibuat oleh PSrE Digisign dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh PSrE Digisign, dan
7. Setiap Pemilik telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

verified information appears in the Certificate,

4. *Digisign CA display information that can be accessed publicly through its repositories,*
5. *Digisign CA private key is protected and that no unauthorized person has ever had access to that private key,*
6. *All representations made by Digisign CA in any applicable agreements are true and accurate, to the best knowledge of Digisign CA, and*
7. *Each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, and/or contained in the Certificate is true.*

9.6.2 Pernyataan dan Jaminan RA / *RA* Representations *and Warranties*

RA yang menjalankan fungsi pendaftaran seperti yang dijelaskan dalam klausul ini mematuhi ketentuan peraturan perundang-undangan, kebijakan ini, dan mematuhi CPS PSrE Digisign yang disetujui oleh *Policy Authority*. RA yang diketahui bertindak dengan cara yang tidak sesuai dengan kewajiban ini dapat dicabut tanggung jawabnya sebagai RA.

An RA that performs registration functions as described in this policy comply with the stipulations of this policy, government rule or regulation, and comply with Digisign CA's CPS approved by the Policy Authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RAs responsibilities.

RA menyatakan dan menjamin, bahwa:

1. Tidak ada kekeliruan dalam Sertifikat yang diketahui atau berasal dari entitas yang menyetujui permohonan

An RA represents and warrants:

1. *There are no fallacies on Certificate that have been known or came from the entity who gives an*

pendaftaran Sertifikat,

2. Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat. RA memelihara bukti bahwa pemeriksaan (due diligence) telah dilakukan dalam memvalidasi informasi yang terdapat dalam Sertifikat,
3. PSrE Digisign mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CPS dan dituangkan dalam kontrak, dan
4. Pemilik dikenakan kewajiban sebagaimana disebutkan dalam Bagian 9.6.3. Pemilik mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

acknowledgement on Certificate application,

2. *There is no false information in the Certificate carried by the entity that approves the registration of the Certificate as a result of inaccuracy in the Certificate Registration Management. RA maintains evidence that due diligence was exercised in validating the information contained in the Certificate,*
3. *Digisign CA required all RAs to guarantee all registration activities that have been done by RAs comply with CPS and stated at the contract, and*
4. *Obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.*

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat / *Subscriber Representations and Warranties*

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

1. Setiap Sertifikat yang dibuat

The Applicant agrees to the following documents, which contain the requirements that must be met regarding the protection of the Private Key and the use of the Certificate, before the Certificate is issued. The Subscriber and/or Applicant agrees to the following:

1. *Every Certificate created using a*

menggunakan Kunci Privat serta berkorespondensi dengan Kunci Publik yang tercantum pada Sertifikat merupakan tanda tangan elektronik Pemilik dan Sertifikat yang sudah disetujui serta secara operasional (tidak kedaluwarsa dan telah dicabut) saat tanda tangan elektronik dibuat,

2. Setiap Kunci Privat diamankan dan hanya Pemilik Sertifikat yang memiliki akses terhadap Kunci Privat tersebut,
3. Sudah melakukan reviu dan verifikasi terhadap akurasi informasi dari Sertifikat yang diterimanya,
4. Semua informasi yang diberikan oleh Pemilik Sertifikat dan informasi yang berada di dalam Sertifikat adalah benar,
5. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini,
6. Segera:
   (i). 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,
   (ii). mengajukan permohonan untuk

Private Key and corresponding to the Public Key listed on the Certificate is the electronic signature of the Subscriber and the Certificate that has been approved and operationally (not expired and has been revoked) when the electronic signature is made,

2. *Each Private Key is secured and only the Certificate Subscriber has access to the Private Key,*
3. *Has reviewed and verified the accuracy of the information from the Certificate received,*
4. *All information provided by the Certificate Subscriber and the information contained in the Certificate is correct,*
5. *Certificates are used only for legal purposes and are permitted in accordance with the requirements contained in this CPS,*
6. *Immediately:*
   (i). request to revoke and terminate the use of the Certificate and its associated Private Key, if there is any suspicious activity and misuse or leakage of the Subscriber's Private Key associated with the Public Key included in the Certificate,
   (ii). apply for revocation of the

melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam Sertifikat tersebut, dan

Certificate, and stop using it, if any information is inconsistent or becomes inappropriate in the Certificate, and

(iii). menghentikan penggunaan Kunci Privat yang kunci publiknya tercantum dalam Sertifikat setelah Sertifikat dicabut.

(iii). discontinue use of the Private Key whose public key is listed in the Certificate after the Certificate has been revoked.

7. Akan menanggapi permintaan dari PSrE Digisign mengenai kompromi atau penyalahgunaan Sertifikat. Dalam kurun waktu 48 (empat puluh delapan) jam.

7. respond to requests from Digisign CA regarding compromise or misuse of Certificates. Within 48 (Forty Eight) hours,

8. Menyetujui dan menerima bahwa PSrE Digisign diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Kepemilikan Sertifikat atau jika PSrE Digisign menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware,* dan

8. Agree and accept that Digisign CA is authorized to immediately revoke the Certificate if subscriber violates the provisions contained in the Certificate Subscriber Agreement or if Digisign CA finds that the Certificate is used to facilitate criminal acts such as phishing, fraud, or distribution of malware, and

9. Pemilik adalah Pengguna akhir dan bukan merupakan PSrE Digisign, dan tidak menggunakan Kunci Privat yang Kunci Publiknya tercantum dalam Sertifikat untuk tujuan penandatangan Sertifikat PSrE lain.

9. *The Subscriber is an End user subscriber and not Digisign CA and may not use the Private Key whose Public Key is listed in the Certificate for the purpose of signing other PSrE Certificates.*

9.6.4 Pernyataan dan Jaminan Pengandal / *Relying Party Representations and Warranties*

Pengandal Sertifikat PSrE Digisign menjamin bahwa:

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

The Digisign CA Certificate Relying Party warrants that:

1. *Have the technical ability to use the Certificate,*
2. *If a representative of a Relying Party uses a Certificate issued by Digisign CA, the Relying Party must properly verify the information contained in the Certificate before use and bear any consequences if it fails to do so,*
3. *Notify Digisign CA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised,*
4. *Relying Party has sufficient information to make an informed decision as to the extent to which the Relying Party chooses to rely on the information in the Certificate, that the Relying Party is solely responsible for deciding whether or not to rely on such information, and the Relying Party will bear the consequences the law of failure to fulfill the Relying Party's obligations under this CPS, and*
5. *Comply with the conditions set out in*

di CPS dan perjanjian lain yang terkait.

the CPS and other relevant agreements.

9.6.5 Pernyataan dan Jaminan Partisipan Lain / *Representations and Warranties of other Participants*

Tidak ada ketentuan.

No Condition

9.7 Pelepasan Jaminan / Disclaimers *of Warranties*

PSrE Digisign membuat pernyataan dalam CPS bahwa PSrE Digisign tidak menjamin:

1. Kecuali untuk jaminan yang telah tercantum dalam CPS, kontrak perjanjian, Kebijakan Jaminan, Kebijakan Privasi, Perjanjian Kepemilikan Sertifikat / *Subscriber Agreement* dan Perjanjian Pengandal / *relying party agreement* dan sepanjang diizinkan oleh hukum, PSrE Digisign mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu,
2. Penyalahgunaan Sertifikat yang tidak sesuai dengan peruntukannya yang diatur pada bagian 4.5 (Penggunaan Sertifikat / *Certificate Usage*), dan
3. Keakuratan, keaslian, kelengkapan, atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat.

As stated in the CPS that Digisign CA does not warrant:

1. *Except for the warranties set forth in the CPS, contractual agreements, Warranty Policy, Privacy Policy, Certificate Subscriber Agreement / subscriber agreement and relying party agreement and to the extent permitted by law, Digisign CA disclaims all warranties or other conditions (expressed, implied, verbal or written), including any warranties of merchantability or fitness for a particular purpose,*
2. *Misuse of Certificates that are not in accordance with their designation as regulated in section 4.5 (Certificate Usage), and*
3. *The accuracy, authenticity, completeness or suitability of any information contained in the demonstration or testing of the Certificate.*

9.8 Pembatasan Tanggung Jawab / *Limitations of Liability*

9.8.1 Pembatasan Tanggung Jawab PSrE Digisign / *Digisign CA Limitation of Liability*

PSrE Digisign tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat, termasuk:

1. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Kepemilikan Sertifikat, atau yang diatur dalam Sertifikat itu sendiri,
2. Semua kerusakan yang disebabkan oleh *force majeure*, dan
3. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau Trojans) di luar perangkat PSrE Digisign

Digisign CA shall not be held responsible for improper use of Certificates, including:

1. *Any damages resulting from the use of the Certificate or key pair in a manner other than as defined in the CPS, the Certificate Subscriber Agreement, or as provided for in the Certificate itself,*
2. *All damages caused by force majeure, and*
3. *Any damage caused by malware (such as viruses or Trojans) outside the Digisign CA device.*

9.8.2 Pembatasan Tanggung Jawab RA / *RA Limitation of Liability*

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan PSrE Digisign, dan mengacu kepada ketentuan peraturan perundang-undangan. Secara khusus, RA bertanggung jawab atas pendaftaran Pemilik.

The cap on RA's liability is specified in the contract between the RA and the Digisign CA, and in accordance with laws and regulations. In particular, the RA is liable for the registration of Subscribers.

PSrE Digisign sebagai RA tidak bertanggung jawab atas akibat dan kerugian yang timbul baik secara langsung atau tidak langsung, pada:

1. Kehilangan atau kerusakan,
2. Kerugian, dan

Digisign CA as RA shall not be held responsible for the consequences and losses that arise either directly or indirectly of:

1. *Loss or damage,*

3. Kehilangan data. Dari ketidaksesuaian data yang diberikan dalam proses Sertifikat dan tidak sesuai dengan CPS ini.	*2. Loss, and* *3. Data loss.* *From the discrepancy of the data provided in the Certificate process and not in accordance with this CPS*

9.8.3 Pembatasan Tanggung Jawab Pemilik / *Subscriber Limitation of Liability*

Tanggung jawab Pemegang Sertifikat dan/atau batasannya diuraikan dalam kontrak berlangganan atau Perjanjian Pemilik, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak.	*The responsibilities of the Certificate Holder and/or their limitations are described in a Subscriber contract or Subscriber Agreement, with reference to the provisions of laws and regulations governing the relationship between the two parties.*
Pemilik secara khusus bertanggung jawab atas kerugian yang disebabkan oleh kelalaian, pelanggaran kelaikan (*due diligence*) atau penggunaan sertifikat selain yang ditentukan pada CPS ini.	*The Subscriber is specifically liable for losses caused by negligence, breach of due diligence or use of a certificate other than those specified in this CPS.*

9.9 Ganti Rugi / *Indemnities*

9.9.1 Ganti Rugi oleh PSrE Digisign / *Indemnification by Digisign CA*

Kewajiban ganti rugi PSrE Digisign ditetapkan dalam CPS, Perjanjian Kepemilikan Sertifikat, Kebijakan Jaminan atau Perjanjian Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat. Kewajiban ganti rugi harus sesuai dengan ketentuan peraturan perundang-undangan.	*Digisign CA's indemnity obligations are set out in the CPS, Certificate Subscriber Agreement, Warranties Policy, or Relying Party Agreement including any liability to third beneficiary parties. The indemnities obligations shall conform to the applicable laws and regulations.*

9.9.2 Ganti Rugi oleh Pemilik Sertifikat / *Indemnity by Subscribers*

Kewajiban ganti rugi PSrE Digisign tidak meliputi atas kerugian yang disebabkan oleh kelalaian, pelanggaran dalam menjaga kerahasiaan kredensial, seperti memindahtangankan atau membuat dapat diaksesnya metode atau faktor autentikasi kepada orang lain dan/ataupun tidak mencabut Sertifikatnya yang telah atau diduga terkompromi.

Digisign CA's liability for compensation does not cover losses caused by negligence, violations in maintaining the confidentiality of credentials, such as transferring or making accessible authentication methods or factors to other people and/or not revoking their certificates which have been or are suspected to be compromised.

Tanggung jawab pemegang sertifikat diuraikan dalam PKS atau perjanjian pemegang sertifikat dan mengacu pada ketentuan peraturan perundang-undangan yang mengatur kesepakatan para pihak.

The responsibilities of the certificate holder are described in the PKS or certificate holder agreement and refer to the provisions of laws and regulations governing the agreement of the parties.

Batasan tanggung jawab PSrE Digisign diatur dalam CPS, Perjanjian Kepemilikan Sertifikat, Kebijakan Jaminan atau Perjanjian Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

The limitations of Digisign CA's liability are regulated in the CPS, Subscriber Agreement, Warranty Policy or Relying Party Agreement including any liability whatsoever to beneficiary third parties.

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

1. Pelanggaran yang dilakukan oleh Pemilik terhadap perjanjian pemilik

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold Digisign CA no liabilities from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Digisign CA may incur as a result of:

1. *Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's*

atau kontrak berlangganan, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja,

Certificate Application,

2. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik,
3. Penggunaan Sertifikat oleh Pemilik untuk melakukan perbuatan melawan hukum,
4. Kegagalan Pemilik untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu pihak manapun,
5. Kegagalan Pemilik untuk melindungi Kunci Privat, menggunakan system 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 (termasuk namun tidak terbatas pada common name, nama domain, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

2. *Fraudulent or negligent use of Certificates by the Subscriber,*
3. *Unauthorised use of the Certificates by Subscribers including use of Certificates beyond the prescribed use defined by this CPS,*
4. *Failure by the Subscriber to disclose a material fact on the Certificate Application with intent to deceive any party,*
5. *The Subscriber's failure to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key, or*
6. *The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.*

9.9.3 Ganti Rugi oleh Pengandal / *Indemnification by Relying Parties*

Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold

membebaskan PSrE Indonesia dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, 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 kedaluwarsa atau sudah dicabut.

Airbus harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Airbus may incur as a result of:

1. *The Relying Party's failure to perform the obligations of a Relying Party,*
2. *2. The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.*

9.10 Jangka Waktu dan Pengakhiran / *Term and Termination*

9.10.1 Jangka Waktu / *Term*

CPS ini dinyatakan berlaku sampai ada pemberitahuan perubahan lebih lanjut oleh PSrE Digisign melalui halaman repositorinya.

This CPS shall be declared valid until further change notice by Digisign CA via its repository page.

9.10.2 Pengakhiran / *Termination*

Perubahan CPS ditandai dengan perubahan nomor versi yang jelas setelah disetujui oleh *Policy Authority* PSrE Induk. Setiap perubahan efektif berlaku 30 (tiga puluh) hari kalender setelah dipublikasikan.

CPS changes are indicated by a clear version number change after approval by Root CA's Policy Authority. Each change is effective 30 (thirty) calendar days after publication.

Dalam hal terdapat perubahan CP PSrE Induk, dokumen Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan lainnya yang berdampak pada OID PSrE

When there are changes in Root's CP, OID Hierarchy document for Digisign CA, and/or other regulations which implicate the Indonesian CAs' OID, then OID in Digisign

Digisign, maka OID dalam CPS PSrE Digisign dapat tetap berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan dengan ketentuan CP PSrE Induk, Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan terkini lainnya.	*CA's CPS may remain valid for maximum 12 (twelve) months or sooner, after adjusting to the new stipulation in Root's CP, OID Hierarchy document for Indonesian PKI, and/or other latest regulations.*

9.10.3 Dampak Pengakhiran dan Ketentuan yang tetap Berlaku / *Effect of Termination and Survival*

PSrE Digisign mengkomunikasikan kondisi, akibat dari penghentian CPS, dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit dan masih berlaku melalui halaman repositori.	*Digisign CA communicates the conditions resulting from the termination of CPS, as well as the sustainability conditions of the issued and valid Certificates via the repository page.*
Meski CPS sudah tidak berlaku lagi, aturan terkait perlindungan data dan arsip informasi tetap dipatuhi.	*Even once CPS may no longer be valid, the regulations pertaining to the laws on data protection and on archival of information are still observed.*

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan / *Individual Notices and Communications with Participants*

PSrE Digisign menyediakan media komunikasi bagi para pihak terkait melalui aplikasi, telepon, dokumen atau surat elektronik (email) yang ditandatangani secara digital. PSrE Digisign memberikan tanda terima yang valid sebagai bukti bagi pengirim. PSrE Digisign memberi tanggapan paling lama dua puluh 20 (dua puluh) hari kerja melalui media komunikasi yang sama.	*Digisign CA provides communication media for related parties via application, telephone, digitally signed document or electronic mail (email). Digisign CA provides a valid receipt as proof for the sender. Digisign CA responds no later than twenty 20 (twenty) working days through the same communication media.*

Komunikasi yang dibuat ke PSrE Digisign harus dialamatkan sebagaimana diatur pada Bagian 1.5.2.	*Communications made to Digisign CA shall be addressed in accordance with those listed in Section 1.5.2.*

9.12 Perubahan atau Amandemen / *Amandements*

9.12.1 Prosedur untuk Perubahan atau Amandemen / *Procedure for Amendment*

PSrE Digisign menerbitkan pemberitahuan di website dan aplikasi terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Amendemen CPS dilakukan sesuai dengan prosedur persetujuan CPS.	*Digisign CA publishes notices on the website and application regarding major or significant changes to this CPS including a description of the time when the CPS becomes effective. CPS amendments are carried out in accordance with the CPS approval procedure.*

9.12.2 Periode dan Mekanisme Pemberitahuan / *Notification Mechanism and Period*

PSrE Digisign menerbitkan pemberitahuan di website dan aplikasi terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika terjadi perubahan CPS harus dipublikasikan paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.	*Digisign CA publishes notices on the website and application regarding major or significant changes to this CPS including a description of the time when the CPS becomes effective. When a CPS change occurs, it must be published no later than 7 (seven) working days from the date it was signed.*

9.12.3 Keadaan Dimana OID Harus Diubah / *Circumstances under Which OID Must Be Changed*

Jika *Policy Authority* memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, PSrE Digisign akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan	*If the Policy Authority sees the need to change the OID numbers involved, Digisign CA will change the OID and implement the new policy using the new OID.*

menggunakan OID yang baru.

Jika PA PSrE Digisign menambah atau mengubah OID di bawah kebijakan OID PSrE Digisign, PSrE Digisign menginformasikan kepada PA PSrE Induk sebelum OID tersebut diimplementasikan.	*If Digisign CA's PA adds or changes the OID of which is within the boundary of Digisign CA's OID regulation, Digisign CA informs the Root CA's PA prior to its implementation.*

9.13 Ketentuan Penyelesaian Perselisihan/Sengketa / *Dispute Resolution Provisions*

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai.	*If there is a dispute or controversy regarding the performance, execution or interpretation of this CPS, the parties will endeavor to reach an amicable resolution.*
Ketentuan penyelesaian perselisihan/ sengketa antara PSrE Digisign dengan Pemilik maupun antara PSrE Digisign dengan entitas lain yang terikat secara kontrak diselesaikan melalui pengadilan yang disepakati.	*Provisions for resolving disputes/disputes between PSrE Digisign and the Subscriber or between PSrE Digisign and other contractually bound entities are resolved through an agreed court.*
Penjelasan lebih lanjut mengenai ketentuan penyelesaian perselisihan / sengketa disebutkan di dalam dokumen Perjanjian Pemilik.	*Further explanation regarding the provisions for dispute resolution is stated in the Subscribers Agreement document..*

9.14 Hukum yang Mengatur / *Governing Law*

CPS ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat PSrE Digisign ataupun produk/ layanan lainnya. Termasuk	*This CPS applies the rule of law in Indonesia to get the same understanding, regardless of the location of domicile or the location of the use of Digisign CA Certificates or other products/services. Even*

apabila Sertifikat PSrE Digisign dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia.

if the Digisign CA Certificate is used for commercial needs in other countries, it still applies the rule of law in Indonesia.

Para pihak, termasuk mitra PSrE Digisign, Pemilik, dan Pengandal tidak dapat membatalkan acuan hukum yang telah ditentukan di atas.

The parties, including Digisign CA partners, Subscribers, and Relying Parties shall not omit the reference of the law specified above.

9.15 Kepatuhan atas Hukum yang Berlaku / *Compliance with Applicable Law*

Partisipan IKP 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.

PKI Participants comply with all applicable requirements, laws, and regulations pertaining in Indonesia for the provision of products and services described in this CP. Compliance includes, but is not limited to, hardware, software, systems, business information, data processes and all related undertakings during the daily operations of business practices.

9.16 Ketentuan yang belum diatur / *Miscellaneous Provisions*

9.16.1 Seluruh Perjanjian / *Entire Agreement*

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

Digisign CA contractually obligates every RA involved with Certificate issuance to comply with this CPS and all related guidelines.

9.16.2 Pengalihan Hak / *Assignment*

Pengandal dan Pemilik tidak dapat mengalihkan hak atau kewajiban mereka berdasarkan CPS ini, berdasarkan hukum atau sebaliknya, tanpa persetujuan tertulis dari PSrE Digisign. Setiap adanya upaya percobaan maka akan dibatalkan.

Relying party and Subscriber may not transfer their rights or obligations under this CPS, by law or otherwise, without the written consent of Digisign CA. Any attempt to do so will be cancelled.

9.16.3 Keterpisahan / *Severability*

Jika ada pengaturan dalam CPS ini yang dinyatakan tidak sah oleh pengadilan, maka ketentuan lain tetap berlaku hingga CPS diperbarui. Proses pembaruan CPS dijelaskan pada Bagian 9.12.

If any provision of this CPS is held to be invalid by a court, then the remaining provisions will remain in full force and effect until the CPS is updated. The CPS update process is stipulated in Section 9.12.

9.16.4 Penegakan Hukum (Biaya Pengacara dan Pelepasan Hak) / *Enforcement (Attorneys' Fees and Waiver of Rights)*

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

Digisign CA may ask for compensation and reimbursement of attorney's fees to parties who are proven to have caused damage, loss, and other losses caused by that party. Digisign CA's failure to apply this clause in one case does not eliminate Digisign CA's right to continue to use this clause in the future or the right to use other clauses in this CPS. All matters relating to the waiver in court must be submitted in writing and signed by Digisign CA.

9.16.5 Keadaan Memaksa / *Force Majeure*

PSrE Digisign tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada di luar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga. PSrE Digisign menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas PSrE Digisign.

Digisign CA shall not be held responsible for any failure or delay in its performance in this CPS, caused by things beyond its reasonable control, including but not limited to: acts of civil or military authorities, natural disasters, fires, epidemics, floods, earthquakes earth, riot, war, equipment failure, electricity and telecommunications line failure, lack of internet access, sabotage, terrorism, and government action or any unforeseen event or situation. Digisign CA provides BCP and DRP with reasonable control in accordance with Digisign CA's capabilities

9.17 Ketentuan Lain / *Other Provisions*

9.17.1 Versi CPS yang memiliki kekuatan hukum / *Legally Binding Version of CPS*

Dokumen CPS ini dibuat dalam 2 bahasa, yaitu bahasa Indonesia dan bahasa inggris. Apabila terjadi perbedaan penafsiran antara teks bahasa Indonesia dengan teks bahasa inggris, maka yang berlaku adalah teks dalam bahasa Indonesia.

This CPS document is made in 2 languages, namely Indonesian and English. If there is a difference in interpretation between the Indonesian text and the English text, the Indonesian text will prevail.

LAMPIRAN / *APPENDIX*

A. Tabel Akronim / *Table of Acronyms*

Akronim / *Acronym*	**Penjelasan / *Explanation***
FIPS	*(US Government) Federal Information Processing Standards*
CAB	*Conformity Assessment Body*
CRL	Daftar Pencabutan Sertifikat / *Certificate Revocation List*
EV	*Extended Validation*
HSM	*Hardware Security Module*
IKP / *PKI*	Infrastruktur Kunci Publik / *Public Key Infrastructure*
CP	Kebijakan Sertifikat Elektronik / *Certificate Policy*
LS PSrE	Lembaga Sertifikasi PSrE
OID	*Object Identifier*
OCSP	*Online Certificate Status Protocol*
RA	Otoritas Pendaftaran / *Registration Authority*
P2SE	Pengawas Penyelenggaraan Sertifikasi Elektronik / *CA Certification Bodies*
PSrE / CA	Penyelenggara Sertifikasi Elektronik / *Certification Authority*
CSR	Permohonan Penandatangan Sertifikat / *Certificate Signing Request*
CPS	Pernyataan Penyelenggaraan Sertifikasi Elektronik / *Certification Practice Statement*
PA	*Policy Authority*
DC	Pusat Data / *Data Center*
DRC	Pusat Pemulihan Bencana / *Disaster Recovery Center*
BCP	Rencana Keberlangsungan Bisnis / *Business Continuity Planning*
DRP	Rencana Pemulihan Bencana / *Disaster Recovery Planning*
RFC	*Request For Comment*
VA	*Validation Authority*
SMKI / ISMS	Standar Sistem Manajemen Keamanan Informasi / *Information Security Management System*

B. Tabel Definisi / *Table of Definition*

Istilah / *Term*	**Definisi / *Definition***
Badan Usaha *Business Entity*	Perusahaan perseorangan atau perusahaan persekutuan (atau organisasi), baik yang berbadan hukum maupun yang tidak berbadan hukum. *A sole proprietorship or partnership company (or organization) whether in legal entity or non-legal entity form.*
IKP Indonesia *Indonesia PKI*	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 Kunci Publik sesuai peraturan Indonesia. *A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography according to Indonesian regulations.*
PSrE *CA*	Badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat. PSrE berwenang untuk: 1. Memeriksa Pemohon 2. menerbitkan, memperpanjang masa berlaku, melakukan pemblokiran dan/atau pencabutan, melakukan validasi,,dan membuat daftar yang aktif dan yang dicabut dari Sertifikat, dan 3. membuat, melakukan verifikasi dan validasi terhadap Tanda Tangan Elektronik dan/ atau layanan lain yang menggunakan Sertifikat. PSrE dibagi menjadi PSrE Induk dan PSrE Indonesia. *A legal entity that acts as a trustworthy party, which provides and audits Certificates. A CA is authorized to:* *1. Examine the Applicant* *2. Issue, extend the validity period, block and/or revocation, perform validation, and make a list of active and revoked Certificates, and* *3. Create, verify, and validate Electronic Signatures and/or other services using Certificates.* *CA is classified into Root CA and Indonesian CA.*
PSrE Induk *Root CA*	Entitas legal yang memiliki otoritas Sertifikasi tingkat teratas yang menandatangani Sertifikat PSrE Berinduk dalam rantai IKP Indonesia. *The top-level Certification Authority that issues Subordinate CA Certificates in the Indonesian PKI chain.*
PSrE Berinduk *Subordinate CA*	Entitas legal yang Sertifikatnya ditandatangani oleh PSrE Induk dan bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Pemilik. *Legal entity whose Certificate is signed by the Root CA and is responsible for the creation, issuance, revocation, and management of Subscriber's Certificates.*

Istilah / *Term*	Definisi / *Definition*
Instansi *Agency/ Government*	Instansi Penyelenggara Negara yang selanjutnya disebut Instansi adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah, dan instansi lain yang dibentuk dengan peraturan perundang-undangan. *A legislative, executive, and judicial institution at the central and regional levels and such other agencies established under laws and regulations.*
PSrE Instansi *Government CA*	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi. *Subordinate CA who is responsible for the creation, issuance, revocation, and management of Government Certificates.*
PSrE non-Instansi *Non-Government CA*	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat non-Instansi. *Subordinate CA who is responsible for the creation, issuance, revocation, and management of Non-Government Certificates.*
Pemohon *Applicant*	Orang perseorangan atau badan hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik. *The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.*
Pemilik *Subscriber*	Orang perseorangan yang merupakan subjek dari Sertifikat, telah diterbitkan Sertifikatnya. *A person who is the Subject of, and has been issued, a Certificate.*
Sertifikat *Certificate*	Sertifikat adalah Sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik. *Certificate is an electronic certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions*
Sertifikat PSrE Induk *Root CA Indonesia Certificate*	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PsrE Induk untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh PsrE Berinduk. *The self-signed Certificate issued by Root CA Indonesia to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.*
Sertifikat PSrE Berinduk *Subordinate's Certificate*	Sertifikat yang dikeluarkan oleh PSrE Induk. *The Certificate issued by Root CA Indonesia.*
Sertifikat Pemilik *Subscriber's Certificate*	Sertifikat yang dikeluarkan oleh PSrE Berinduk. *The Certificate issued by Subordinate CA.*

Istilah / *Term*	Definisi / *Definition*
Pihak Pengandal *Relying Parties*	Berarti suatu persekutuan, firma, perusahaan, badan hukum, non kementerian, lembaga atau organisasi yang mengandalkan layanan PSrE Digisign. *Means a partnership, firm, company, legal entity, non-ministry, institution, or organization that relies on Digisign CA services.*
Certificate Policies *Certificate Policies*	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum. *A set of rules that indicates the applicability of a named Certificate to a PKI implementation with common security requirements.*
Pernyataan Penyelenggaraan Sertifikasi Elektronik *Certification Practice Statement*	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat. *One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.*
Certificate Revocation List *Certificate Revocation List*	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh PSrE Berinduk yang menerbitkan Sertifikat. *A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.*
Certificate Signing Request *Certificate Signing Request*	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat. *A message conveying a request to have a Certificate issued.*
Kompromi *Compromise*	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif. *A violation of a security policy that results in loss of control over sensitive information.*
Extended Validation Certificate *Extended Validation Certificate*	Sertifikat Elektronik yang berisi informasi yang ditentukan dalam Pedoman Extended Validation dan yang telah divalidasi sesuai dengan Pedoman tersebut *A digital certificate that contains information specified in the Extended Validation Guidelines and that has been validated in accordance with the Guidelines..*
Key Compromise *Key Compromise*	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. *A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.*
Key Generation	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan,

Istilah / *Term*	Definisi / *Definition*
Ceremony *Key Generation Ceremony*	kunci privasinya ditransfer ke modul kriptografi, kunci privatnya dicadangkan, dan/atau kunci publiknya disertifikasi. *A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.*
Object Identifier *Object Identifier*	A unique alphanumeric or numeric identifier yang terdaftar di bawah standar International Organization for Standardization untuk objek atau kelas objek tertentu. *A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.*
Online Certificate Status Protocol *Online Certificate Status Protocol*	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat. *An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information.*
Kunci Privat *Private Key*	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. *The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and / or to decrypt electronic records or files that were encrypted with the corresponding Public Key.*
Kunci Publik *Public Key*	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 Private Key yang sesuai. *The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.*
Pasangan Kunci *Key Pair*	Kunci Privat dan Kunci Publik yang mengacu ke entitas yang sama, yang memiliki karakteristik khusus, sehingga suatu pesan yang dienkripsi memakai Kunci Privat hanya dapat didekripsi dengan Kunci Publik pasangannya, dan sebaliknya. *Private Key and Public Key referring to the same entity, which possess certain characteristics, so that a message encrypted by a Private Key can only be decrypted by the corresponding Public Key, and vice versa.*
Otoritas Pendaftaran *Registration*	Pihak yang bekerja sama dengan PSrE Indonesia untuk meneruskan permohonan kepada PSrE Indonesia dalam hal pemeriksaan kebenaran identitas, perpanjangan masa berlaku, dan pemblokiran dan/atau pencabutan Sertifikat Elektronik memenuhi persyaratan.

Istilah / *Term*	**Definisi / *Definition***
Authority	*An entity which cooperates with an Indonesian CA to forward Certificate applications to the Indonesian CA on the condition that the identity verification, extension of validity period, and suspension and/or revocation of the Certificates fulfill the requirements.*
Penyelenggaraan Sertifikasi Elektronik *CA Operation*	Kegiatan menyediakan, mengelola, dan mengoperasikan infrastruktur dan layanan Penyelenggara Sertifikasi Elektronik, dan memberikan dan pengaudit Sertifikat Elektronik. *Activities consist of provision, management, and operation of CA infrastructures and services, as well as issuance and audit of Electronic Certificates.*
Trust Anchor *Trust Anchor*	Sebuah entitas autoritatif dalam suatu struktur IKP hierarkis yang kepercayaan terhadapnya diterima, bukan diturunkan. *An authoritative entity in a PKI hierarchy for which trust is assumed and not derived.*
Peran Terpercaya *Trusted Roles*	Peran-peran yang melakukan fungsi yang sangat penting, dimana jika fungsi tersebut tidak dilakukan dengan benar dan sesuai, dapat menimbulkan dampak yang sangat buruk bagi tingkat kepercayaan PSrE. *Roles that perform critical functions which, if performed unsatisfactorily, can have an adverse impact upon the degree of trust provided by the CA.*
Penilaian Kelaikan *Compliance Audit*	Penilaian Kelaikan atau audit kepatuhan adalah suatu proses yang dilaksanakan oleh LS PSrE atau P2SE terhadap PSrE Indonesia, dengan mengacu kepada beberapa standar tentang PSrE yang telah diterbitkan oleh Komdigi. *A Compliance Audit is a process conducted by CA CAB or Root CA upon Indonesian CA, by referring to CA standards issued by Komdigi.*

C. Profil Sertifikat PSrE Digisign / *Digisign CA Certificate Profile*

1.1 Profil Sertifikat PSrE Digisign G3 / *Digisign CA Certificate Profile G3*

1.1 *DigisignID.CA.Level2-G3*

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CN	DigisignID.CA.Level2 G3
Subject: O	PT Solusi Net Internusa
Subject: C	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Certificate Policies	Critical=TRUE policy oid: 2.16.360.1.1.1.2.2 cps: https://www.rootca.id/
Basic Constraints	Critical=TRUE Subject Type=CA Path Length Constraint=None
Public Key	RSA 4096 bits

1.2 DigisignID.CA.Seal G3

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CN	DigisignID.CA.Seal G3
Subject: O	PT Solusi Net Internusa
Subject: C	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Certificate Policies	Critical=TRUE policy oid: 2.16.360.1.1.1.2.2 cps: https://www.rootca.id/
Basic Constraints	Critical=TRUE Subject Type=CA Path Length Constraint=None
Public Key	RSA 4096 bits

2. Profil Sertifikat Pemilik / *Subscriber Certificate Profile*

2.1 Profil Sertifikat Pemilik Level 2 / *Subscriber Certificate Profile Level 2*

2.1.1 Sertifikat Individu Non-Instansi Verifikasi Level 2 (Online) / *Non-institutional Individual Certificate Level 2 (Online)*

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Level2 G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Lengkap (Sesuai KTP tanpa gelar)
Subject: O	Opsional (Organisasi yang terafiliasi dengan entitas)
Subject: OU	Opsional (Personal apabila diajukan perorangan)
Subject: C	ID
Subject: UID	Unique Identifier
Subject Alternative Name	Opsional (RFC822Name = EmailAddress)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	160 bit hash (SHA-1)
CRL Distribution Points	CRL HTTP URL = http://repository.digisign.id/crl/lv2-crlv2-G3
Authority Key Identifier	160 bit hash (SHA-1)
Authority Info Access	caissuer=http://repository.digisign.id/cert/digisign_level2_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	Critical=FALSE policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.5.1.2.2 Notice Text=Individu non-Instansi Online Level 2
Public Key	RSA 2048 bits

2.1.2 Sertifikat Individu Warga Negara Asing Verifikasi Level 2 (Online)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Level2 G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Lengkap (Sesuai Tanda Pengenal)
Subject: O	Opsional (Organisasi yang terafiliasi dengan entitas)
Subject: OU	Opsional (Personal apabila diajukan perorangan)
Subject: C	Kode Kewarganegaraan
Subject: UID	Unique Identifier
Subject Alternative Name	Opsional (RFC822Name = EmailAddress)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	160 bit hash (SHA-1)
CRL Distribution Points	CRL HTTP URL = http://repository.digisign.id/crl/lv2-crlv2-G3
Authority Key Identifier	160 bit hash (SHA-1)
Authority Info Access	caissuer=http://repository.digisign.id/cert/digisign_level2_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.5.2.2.2 Notice Text=Individu WNA Online level 2
Public Key	RSA 2048 bits

2.1.3 Sertifikat Individu Non-Instansi Verifikasi Level 2 (Offline)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Level2 G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Lengkap (Sesuai KTP tanpa gelar)
Subject: O	Opsional (Organisasi yang terafiliasi dengan entitas)
Subject: OU	Opsional (Personal apabila diajukan perorangan)
Subject: C	ID
Subject: UID	Unique Identifier berdasarkan NIK
Subject Alternative Name	Opsional (RFC822Name = EmailAddress)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	160 bit hash (SHA-1)
CRL Distribution Points	CRL HTTP URL = http://repository.digisign.id/crl/lv4-crlv2-G3
Authority Key Identifier	160 bit hash (SHA-1)
Authority Info Access	caissuer=http://repository.digisign.id/cert/digisign_level2_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.5.1.1.2 Notice Text=Individu non-Instansi Offline Level 2
Public Key	RSA 2048 bits

2.1.4 Sertifikat Individu Warga Negara Asing Verifikasi Level 2 (Offline)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Level2 G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Lengkap (Sesuai Tanda Pengenal)
Subject: O	Opsional (Organisasi yang terafiliasi dengan entitas)
Subject: OU	Opsional (Personal apabila diajukan perorangan)
Subject: C	Kode Kewarganegaraan
Subject: UID	Unique Identifier -
Subject Alternative Name	Opsional (RFC822Name = EmailAddress)
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	160 bit hash (SHA-1)
CRL Distribution Points	CRL HTTP URL = http://repository.digisign.id/crl/lv2-crlv2-G3
Authority Key Identifier	160 bit hash (SHA-1)
Authority Info Access	caissuer=http://repository.digisign.id/cert/digisign_level2_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.5.2.1.2 Notice Text=Individu WNA Offline level 2
Public Key	RSA 2048 bits

2.2 Sertifikat Profile Badan Usaha

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Seal G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Badan Usaha / Badan Hukum
Subject: O	Opsional (Organisasi Name)
Subject: C	Kode Negara
Subject: UID	Unique Identifier
Subject Alternative Name	-
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Key Usage	Critical=TRUE, Digital Signature, Non-Repudiation
Subject Key Identifier	160 bit hash (SHA-1)
CRL Distribution Points	CRL HTTP URL = http://repository.digisign.id/crl/seal-crlv2-G3
Authority Key Identifier	160 bit hash (SHA-1)
Authority Info Access	caissuer=http://repository.digisign.id/cert/digisign_seal_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.8.1 Notice Text= Badan Usaha
Public Key	RSA 2048 bits

2.3 Sertifikat Profil Pemilik Peninggalan / *Certificate Profile Subscriber Legacy*

2.3.1 Sertifikat Individu Non-Instansi (Legacy)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Level4 G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Lengkap (Sesuai KTP tanpa gelar)
Subject: O	Opsional (Organisasi yang terafiliasi dengan entitas)
Subject: C	ID
Subject: E	Email address
Subject Alternative Name	NONE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://repository.digisign.id/crl/lv4-crlv2-G3
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Authority Info Access	Critical=FALSE caissuer=https://repository.digisign.id/cert/digisign_level2_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	Critical=FALSE policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.3.12 Notice Text=Sertifikat Non instansi policy oid: 2.16.360.1.1.1.7.1 Notice Text=Sertifikat Individu policy oid: 2.16.360.1.1.1.4.4 Notice Text= Verification Level 4
Basic Constraints	Critical=TRUE Subject Type=End Entity Path Length Constraint=None
Public Key	RSA 2048 bits

2.3.3 Sertifikat Badan Usaha (Legacy)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	DigisignID.CA.Seal G3
Issuer: O	PT Solusi Net Internusa
Issuer: C	ID
Subject: CN	Nama Badan Usaha / Badan Hukum
Subject: O	Opsional (Organisasi Name)
Subject: C	ID
Subject Alternative Name	NONE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS
Valid To	YYYY/MM/DD HH:MM:SS (durasi 1 (satu) tahun)
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://repository.digisign.id/crl/seal-crlv2-G3
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Authority Info Access	Critical=FALSE caissuer=https://repository.digisign.id/cert/digisign_seal_v2_G3.crt ocsp=http://ocspv2G3.digisign.id
Certificate Policies	Critical=FALSE policy oid: 2.16.360.1.1.1.3.12.2.1.2 cps: https://repository.digisign.id policy oid: 2.16.360.1.1.1.3.12 Notice Text=Sertifikat Non instansi policy oid: 2.16.360.1.1.1.7.2 Notice Text= Sertifikat Badan Usaha policy oid: 2.16.360.1.1.1.4.3 Notice Text= Verification Level 3
Basic Constraints	Critical=TRUE Subject Type=End Entity Path Length Constraint=None
Public Key	RSA 2048 bits

3. Profil CRL / *CRL Profile*

3.1 Profil CRL / *CRL Profile*

Field	Note	M
Version	V2	M
Issuer	CN = DigisignID.CA.Level2 G3 O = PT Solusi Net Internusa C = ID CN = DigisignID.CA.Seal G3 O = PT Solusi Net Internusa C = ID CN = DigisignID.CA.Level4 G3 O = PT Solusi Net Internusa C = ID	M
thisUpdate	Day, Month Date, Year Time Example: Thursday, August 3, 2023 1:45:14 PM	M
nextUpdate	Day, Month Date, Year Time Example: Friday, August 4, 2023 2:45:13 PM	M
revokedCertificate		
userCertificate	Serial Number	M
revocationDate	Day, Month Date, Year Time Example: Thursday, August 3, 2023 1:45:14 PM	M
crlEntryExtention	Serial Number Revocation Date Revocation Reason	O
crlExtention		M

3.2 CRL Extension Field

Field	Note	C	M
authorityKeyIdentifier	DigisignID.CA.Level2 G3 BF:5B:59:D0:AC:FF:83:B2:8B:90:0E:A5:EF:9E:9E:91:8E:FF:5E:AF DigisignID.CA.Seal G3 9E:2D:17:F7:90:0F:8B:C0:01:33:F0:48:17:3B:81:E8:1C:86:5B:85 DigisignID.CA.Level4 G3 BF:5B:59:D0:AC:FF:83:B2:8B:90:0E:A5:EF:9E:9E:91:8E:FF:5E:AF	N	M
issuerAltName	Use Example: RFC822NAME = {email_address}	N	O
cRLNumber	Use, Critical Example: CRL Number = {hexadecimal}	C	M
issuingDistributionPoint	None	C	O

4. Profil OCSP / *OCSP Profile*

4.1 Permintaan OCSP / *OCSP Request*

Field			OCSP Request
tbsRequest			Version Serial Number Signature Algorithm Issuer Subject Subject Public Key Info X509v3 extensions
Version			Version: 3 (0x2)
requestList			Certificate ID: Hash Algorithm: sha1 Issuer Name Hash: {OCTET STRING} Issuer Key Hash: {OCTET STRING} Serial Number: {OCTET STRING}
	reqCert		
		hashAlgorithm	sha1
		issuerNameHash	Issuer Name Hash: {sha1}
		issuerKeyHash	Issuer Key Hash: {sha1}
		serialNumber	Serial Number: {OCTET STRING}
		singleRequestExtensions	NULL
signatureAlgorithm			1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
signature			Signature Value: {SHA256}
certs			Format certificate X.509 PEM

4.2 Respon OCSP / *OCSP Response*

Field			OCSP Response
responseStatus			successful (0), -- Response has valid confirmations malformedRequest (1), -- Illegal confirmation request internalError (2), -- Internal error in issuer tryLater (3), -- Try again later sigRequired (5), -- Must sign the request unauthorized (6) – Request unauthorized
	responseType		Response Type: Basic OCSP Response
	response		he value for response SHALL be the DER encoding of BasicOCSPResponse
	version		Version: 1 (0x0)
	responderID		KeyHash ::= OCTET STRING -- SHA-1 hash of responder's public key
	producedAt		Example: Aug 15 19:40:12 2023 GMT
	responses		
		certID	Certificate ID: Hash Algorithm: sha1 Issuer Name Hash: {OCTET STRING} Issuer Key Hash: {OCTET STRING} Serial Number: {OCTET STRING}
		certStatus	CHOICE := good : Good revoked : RevokedInfo unknown : Unknown
		thisUpdate	Example: Aug 15 19:40:12 2023 GMT
signature			Signature Value: {SHA256}
certs			Format certificate X.509 PEM

4.3 Profil Sertifikat Responder OCSP / *OCSP Responder Certificate Profile*

4.3.1 Basic Field

Field	OCSP Certificate
signatureAlgorithm, memiliki subfield:	
algorithm	1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
parameters	NULL
signatureValue	DigisignID.CA.Level2 G3 Signature Value: 2e:c8:14:d5:ac:11:5d:d9:5c:d7:41:e1:ea:54:c4:36:01:66:……. . DigisignID.CA.Seal G3 Signature Value: 3e:14:c1:ff:18:92:4c:f7:ed:db:e9:73:a8:1c:8e:29:18:9b:..... DigisignID.CA.Level4 G3 Signature Value: 37:ca:a7:be:31:23:5e:74:54:c4:20:3a:b8:1c:dd:bf:1f:e4.....
version	Version: 3 (0x2)
serialNumber	DigisignID.CA.Level2 G3 Serial Number: 7F:25:D3:FB:84:82:3E:E2:76:BC:24:1B:2C:BE:C3:EF:04:DD:D8:16 DigisignID.CA.Seal G3 Serial Number: 76:4A:C2:6C:CA:EF:0B:BC:5C:31:28:2B:DE:A1:02:AC:FB:94:4C:ED DigisignID.CA.Level4 G3 Serial Number: 20:E2:8A:5F:E9:35:FF:55:9E:3D:93:AE:73:CE:3F:64:7A:1D:8B:98
signature, memiliki subfield:	
algorithm	sha256WithRSAEncryption
parameters	NULL
issuer	DigisignID.CA.Level2 G3 Issuer: C=ID, O=PT Solusi Net Internusa, CN=DigisignID.CA.Level2 G3 DigisignID.CA.Seal G3 Issuer: C=ID, O=PT Solusi Net Internusa, CN=DigisignID.CA.Seal G3

Field	OCSP Certificate
	DigisignID.CA.Level4 G3 (legacy) Issuer: C=ID, O=PT Solusi Net Internusa, CN=DigisignID.CA.Level4 G3
validity, memiliki subfield:	5 Tahun
notBefore	Example: Not Before: Aug 1 07:31:27 2023 GMT
notAfter	Example: Not After : Jul 31 07:31:26 2024 GMT
subject	● Sertifikat Individu Level 2 CN = OCSP DigisignID Level2 G3, O = PT Solusi Net Internusa, OU = OCSP Responder, C = ID ● Sertifikat Individu Level 4 (legacy) CN = OCSP DigisignID Level4 G3, O = PT Solusi Net Internusa, OU = OCSP Responder, C = ID ● Segel Elektronik CN=OCSP DigisignID Seal G3, O=PT Solusi Net Internusa, OU=OCSP Responder, C=ID
subjectPublicKeyInfo, memiliki subfield:	
algorithm	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
parameters	NULL
subjectPublicKey	Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit)
extensions, memiliki subfield:	
extnID	X509v3 Certificate Policies: Policy: 2.16.360.1.1.1.3.12.2.1.2 CPS: https://repository.digisign.id Policy: 2.16.360.1.1.1.5.1.1.2 User Notice Text: Individu non-Instansi Offline Level 2 Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi Policy: 2.16.360.1.1.1.7.1 User Notice Text: Sertifikat Individu Policy: 2.16.360.1.1.1.5.1.2.2 User Notice Text: Individu non-Instansi Online Level 2 Policy: 2.16.360.1.1.1.5.2.1.2 User Notice Text: Individu WNA Offline level 2 Policy: 2.16.360.1.1.1.5.2.2.2

Field			OCSP Certificate
			User Notice Text: Individu WNA Online level 2 Policy:2.16.360.1.1.1.5.3.1 User Notice Text: Badan Usaha Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi) Policy: 2.16.360.1.1.1.7.1 User Notice Text: Sertifikat Individu Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi Policy: 2.16.360.1.1.1.7.2 User Notice Text: Sertifikat Badan Usaha Policy: 2.16.360.1.1.1.4.4 User Notice Text: Verification Level 4
		critical	
		extnValue	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

4.3.1 Standard Extension Field

Field	OID	OCSP Certificate	
		C	**(critical)**
AuthorityKeyIdentifier (seq)	**2.5.29.35**	C	
keyIdentifier			SHA-1 160 bit
authorityCertIssuer			Issuer for CA: Issuer: CN = Root CA Indonesia DS G1, O = Kementerian Komunikasi dan Informatika, C = ID Issuer for Subscriber: Issuer: C = ID, O = PT Solusi Net Internusa, CN = DigisignID.CA.Level2 G3 Issuer: C = ID, O = PT Solusi Net Internusa, CN = DigisignID.CA.Seal G3
authorityCertSerialNumber			DigisignID.CA.Level2-G3 = SN:5182C6CAAE983229 DigisignID.CA.Seal-G3 = SN:703CBE7B8C113902
SubjectKeyIdentifier	**2.5.29.14**	C	SHA-1 160 bit
subjectKeyIdentifier			DigisignID.CA.Level2 G3 BF:5B:59:D0:AC:FF:83:B2:8B:90:0E:A5:EF:9E:9E:91:8E:FF:5E:AF DigisignID.CA.Seal G3 76:82:90:71:67:67:3A:5A:65:24:E0:65:6D:B3:A0:BF:E7:EC:8E:92
KeyUsage	**2.5.29.15**	C	
KeyUsage			CA: Digital Signature, Certificate Sign, CRL Sign Subscriber: Digital Signature, Non Repudiation
policyIdentifier			X509v3 Certificate Policies: Policy: 2.16.360.1.1.1.3.12.2.1.2 CPS: https://repository.digisign.id Policy: 2.16.360.1.1.1.5.1.1.2 User Notice Text: Individu non-Instansi Offline Level 2 Policy: 2.16.360.1.1.1.5.1.2.2 User Notice Text: Individu non-Instansi Online Level 2 Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi Policy: 2.16.360.1.1.1.7.1 User Notice Text: Sertifikat Individu Policy: 2.16.360.1.1.1.5.2.1.2 User Notice Text: Individu WNA Offline level 2 Policy: 2.16.360.1.1.1.5.2.2.2
policyQualifiers			

Field	OID	OCSP Certificate	
		C	**(critical)**
			User Notice Text: Individu WNA Online level 2 Policy:2.16.360.1.1.1.5.3.1 User Notice Text: Badan Usaha Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi) Policy: 2.16.360.1.1.1.7.1 User Notice Text: Sertifikat Individu Policy: 2.16.360.1.1.1.3.12 User Notice Text: Sertifikat Non instansi Policy: 2.16.360.1.1.1.7.2 User Notice Text: Sertifikat Badan Usaha Policy: 2.16.360.1.1.1.4.4 User Notice Text: Verification Level 4
BasicConstraint (seq)	**2.5.29.19**	C	
CA			True
ExtendedKeyUsage (seq size (1...MAX))	**2.5.29.37**	N	
keyPurposeId			1.3.6.1.5.5.7.3.9 (OCSP Signing)