PT. INDONESIA DIGITAL IDENTITY

CERTIFICATE POLICY
PENYELENGGARA SISTEM ELEKTRONIK
PT. INDONESIA DIGITAL IDENTITY (VIDA)

Nomor Dokumen	PL-COM-P-001
Tanggal Berlaku	8 June 2020
Versi	2.2
Klasifikasi	**PUBLIK**

Digitally signed by
GAJENDRAN KANDASAMY
Date: 2020.06.17 16:44:35
+07'00'

LEMBAR CATATAN REVISI / REVIEW

Tanggal	Rev	Uraian	Oleh
15 Desember 2018	1.0	Initial Release	Policy authority
13 May 2019	2.0	Penyesuaian berdasarkan Audit Checklist PSrE Kominfo	Policy authority
2 September 2019	2.1	* Penyempurnaan OID pada Bagian 1.2 * Perbaikan redaksional pada Bagian 2.3 * Perbaikan redaksional pada Bagian 4.9.8 * Perbaikan redaksional pada Bagian 6.1.5	Policy authority
8 Juni 2020	2.2	* Penyesuaian berdasarkan ketentuan Webtrust CA 2.2	Policy authority

DAFTAR ISI / TABLE OF CONTENT

1. INTRODUCTION / PENGANTAR

PT. Indonesia Digital Identity ("**IDI**") adalah Penyelenggara Sertifikasi Elektronik ("**PSrE**") yang beroperasi mengacu pada Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik,, berikut dengan segala perubahannya yang mungkin timbul di kemudian hari (untuk selanjutnya disebut "**PSRE IDI**"). Sebagai perusahaan swasta, PSrE IDI merupakan penyelenggara non-instansi menerbitkan sertifikat kepada pihak swasta untuk kepentingan transaksi komersial antara pihak-pihak swasta.

PT. Indonesia Digital Identity ("**IDI**") is a Certification Authority ("**CA**") operating by virtue of Regulation of the Government of the Republic of Indonesia number 71 of 2019 concerning Electronic System and Transaction Operation, along with its revision in the future (hereinfer "**IDI CA**"). As a private company, IDI CA is a non-government CA that issues digital certificates to private parties for the purpose of commercial transaction among these private parties.

Dokumen ini, "Certificate Policy Penyelenggara Sertifikasi IDI" (CP PSrE IDI) adalah kebijakan utama yang mengatur PSrE IDI. CP menetapkan persyaratan bisnis, hukum, dan teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dan menyediakan layanan kepercayaan kepada seluruh pemangku kepentingan.

This document, "IDI CA Certificate Policy" (CP) is the principal statement of policy governing the IDI CA. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing, digital Certificates and providing associated trust services for all participants.

Persyaratan ini melindungi keamanan dan integritas PSrE IDI dan terdiri atas seperangkat aturan yang berlaku secara konsisten di seluruh Indonesia, sehingga memberikan jaminan kepercayaan yang seragam di seluruh IKP Indonesia.

These requirements protect the security and integrity of ID CA and comprise a single set of rules that apply consistently Indonesia PKI-wide, thereby providing assurances of uniform trust throughout the Indonesia PKI.

Dokumen ini ditargetkan pada:

This document is targeted at:

- PSrE IDI yang harus beroperasi sesuai dengan Certificate Practice Statement (CPS) dimana CPS tersebut mengacu kepada persyaratan yang tertuang di dalam CP
- IDI CA who has to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP
- Pihak Pengandal yang perlu memahami seberapa besar kepercayaan untuk dimasukkan ke dalam sertifikat PSrE CA Indonesia, atau tanda tangan digital menggunakan sertifikat itu.
- Relying parties who need to understand how much trust to place in a IDI CA certificate, or a digital signature using that certificate.

1.1. Overview / Ringkasan

CP ini berlaku untuk semua Sertifikat Digital yang diterbitkan oleh PSrE IDI. Tujuan dari CP ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan sertifikat PSrE IDI untuk menunjukkan kepatuhan terhadap akreditasi yang diterima industri formal.

This CP applies to all Digital Certificates that it issues by IDI CA. The purpose of this CP is to present the practices and procedures in managing IDI CA in order to demonstrate compliance with formal industry accepted accreditations.

Selain itu, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan pengakuan atas tanda tangan elektronik yang digunakan untuk tujuan otentikasi atau nirsangkal.

Additionally, the Law Of The Republic Of Indonesia Number 11/2008 Concerning Electronic Information And Transactions (the “Law”) provides for the recognition of electronic signatures that are used for the purposes of authentication or nonrepudiation.

CP ini menetapkan tujuan, peran, tanggung jawab, dan praktek semua entitas yang terlibat dalam siklus hidup Sertifikat yang diterbitkan berdasarkan CP ini. Dalam istilah sederhana, CP menyatakan "apa yang harus dipatuhi", menetapkan kerangka aturan operasional untuk produk dan layanan.

This CP sets out the objectives, roles, responsibilities and practices of all entities involved in the life cycle of Digital Certificates issued under this CP. In simple terms, a CP states “what is to be adhered to”, setting out an operational rule framework for products and services.

CPS melengkapi CP ini dan menyatakan, “bagaimana PSrE IDI mematuhi CP”. CPS menyediakan Pemilik dengan ringkasan proses, prosedur, dan ketentuan umum yang berlaku bahwa PSrE IDI (yaitu entitas yang memberikan Sertifikat Digital kepada Pemilik) akan digunakan dalam membuat dan mengelola Sertifikat Digital tersebut. Demikian juga, PSrE IDI membuat CPS mereka sendiri yang berlaku untuk produk dan layanan yang mereka tawarkan

A CPS complements this CP and states, “how IDI CA adheres to the CP”. A CPS provides an end user with a summary of the processes, procedures and overall prevailing conditions that the IDI CA (i.e. the entity which provides the Subscriber its Certificate) will use in creating and managing such Certificates. Likewise, IDI CAs maintain their own CPS applicable to products and services they offer.

1.2. Document Name and Identification

Dokumen ini adalah dokumen Certificate Policy PSrE IDI (CP). Object Identifier (OID) yang digunakan untuk CP ini adalah 2.16.360.1.1.1.12.4.4.1

The document is the Certificate Policy for IDI CA (CP). Object Identifier (OID) used for this CP is: 2.16.360.1.1.1.12.4.4.1

1.3. PKI Participants/ Partisipan IKP

1.3.1. Certification Authorities / Penyelenggara Sertifikasi Elektronik (PSrE)

PSrE IDI beroperasi sesuai dengan ketentuan perundang-undangan yang berlaku di Indonesia tentang Sertifikasi Elektronik.

IDI CA operates pursuant to the prevailing laws and regulations in Indonesia concerning Digital Certificates.

PSrE IDI bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat Digital PSrE ID, sebagaimana dirinci dalam CP ini, termasuk

- Pengendalian terhadap proses pendaftaran
- Proses identifikasi dan autentikasi
- Proses penerbitan Sertifikat
- Publikasi Sertifikat
- Pencabutan Sertifikat, dan
- Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE yang diterbitkan sesuai dengan CP ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP ini.

IDI CA shall be responsible for all aspects of the issuance and management of those Digital Certificates, as detailed in this CP, including:

- The control over the registration process,
- The identification and authentication process,
- The Certificate manufacturing process,
- The publication of Certificates,
- The revocation of Certificates, and
- Ensuring that all aspects of the services, operations, and infrastructures related to IDI CA Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of this CP.

1.3.2. Registration Authorities / Otoritas Pendaftaran (RA)

PSrE dapat menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan identifikasi dan autentikasi Pemilik, penerimaan permohonan dan pencabutan Sertifikat sesuai dengan yang telah didefinisikan pada CP dan dokumen terkait.

IDI CAs may designate a specific Registration Authority (RA) to perform identification and authentication of Subscribers, as well as accepting applications for certificate requests and revocations as defined in the CP and other related documents.

1.3.2.1. Function of Registration Authorities / Fungsi dari RA

RA berkewajiban untuk melaksanakan fungsi tertentu yang mengacu pada perjanjian RA, meliputi hal-hal sebagai berikut:

a. menyusun prosedur pendaftaran untuk Pemohon sertifikat;
b. melakukan identifikasi dan otentikasi Pemohon sertifikat;

The RA is obliged to perform certain functions pursuant to an RA agreement, including the following:

a. establish enrollment procedures for end-user certificate Applicants;
b. perform identification and authentication of certificate Applicants;

c. memulai atau meneruskan proses permohonan pembatalan sertifikat; dan

d. menyetujui permohonan untuk memperbaharui sertifikat atau pembaharuan kunci atas nama PSrE.

c. initiate or pass along revocation requests for certificates; and

d. approve applications for certificate re-key or renewal on behalf of a CA.

1.3.2.2. RA Specific Requirement for Extended Validation SSL Certificate / Persyaratan khusus RA untuk Sertifikat EV SSL

Tidak ada ketentuan

No stipulation.

1.3.3. Subscribers / Pemilik

Pemilik adalah entitas yang memohon dan berhasil mendapatkan Sertifikat Digital yang ditandatangani oleh PSrE IDI. Entitas Pemilik berarti subjek pemegang Sertifikat Digital sekaligus entitas yang terikat dengan PSrE IDI sebagai penerbit Sertifikat Digital. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat Digital, Pemegang disebut sebagai Pemohon.

Subscribers are entities who request and successfully acquire a Certificate signed by IDI CA. Subscriber refers to both the Subject of the Certificate and the entity that contracted with the CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, an entity is an Applicant.

PSrE IDI boleh menerbitkan Sertifikat kepada semua Pemilik

IDI CA may issue certificates to any Subscriber.

1.3.4. Relying Parties / Pihak Pengandal

Pihak Pengandal adalah entitas yang mempercayai Sertifikat Digital dan Tanda Tangan Digital yang diterbitkan oleh PSrE IDI. Pihak Pengandal harus terlebih dahulu memeriksa respon dari Certificate Revocation Lists (CRL) atau Online Certificate Status Protocol (OCSP) PSrE IDI yang sesuai sebelum memanfaatkan informasi yang ada dalam Sertifikat.

Relying Parties are entities that rely on Certificates and/or Digital Signatures issued by IDI CA. Relying Parties must check the appropriate response from the CA's CRL or OCSP before relying on information featured in a Certificate.

Pihak Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama Pemilik dengan kunci publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pihak Pengandal dapat menggunakan informasi dalam Sertifikat untuk menentukan kecocokan penggunaan Sertifikat. Pihak Pengandal

A Relying Party is an entity that relies on the validity of the Subscriber's Name attached to the Public Key. The Relying Party is responsible for checking the status of the information in the certificate. A Relying Party may use the information in the certificate to determine the conformity of the Certificate to particular use and purposes such as:

menggunakan informasi dalam Sertifikat Digital untuk:

a. Memeriksa tujuan penggunaan Sertifikat
b. Melakukan verifikasi tanda tangan digital
c. Memeriksa apakah Sertifikat Digital termasuk di dalam CRL
d. Penyetujuan batas tanggung jawab dan jaminan

Pihak Pengandal meliputi lembaga keuangan, perusahaan e-Commerce, Instansi Penyelenggara Negara dan entitas lain yang menggunakan tanda tangan elektronik di dalam layanannya.

a. Checking for which purpose a certificate is used;
b. Verifying the Digital Signatures;
c. Checking whether a Certificate is in Revocation List; and
d. Acknowledgement of applicable liability caps and warranties.

Relying parties include Banks, e-Commerce companies, government institutions and other institutions which use digital signatures in their services.

1.3.5. Other Participants / Partisipan Lain

PSrE IDI dapat menentukan Partisipan Lain yang berhubungan dengan operasional sertifikasi elektronik.

IDI CA may designate Other Participants that related to the operational of electronic certification.

1.4. Certificate Usage / Kegunaan Sertifikat

1.4.1. Appropriate Certificate Uses / Penggunaan Sertifikat yang Semestinya

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

- Autentikasi;
- Tanda Tangan Elektronik & Non-Repudiasi; dan
- Enkripsi

Pemilik Sertifikat dapat memilih Tingkat Jaminan yang sesuai sebagai identitas yang akan mereka tunjukkan kepada Pihak Pengandal. Tingkatan Jaminan yang dimaksud dibedakan menjadi Kelas Sertifikat sebagai berikut:

Level 3: Sertifikat dengan Tingkat Jaminan Sedang. Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap Data identitas yang dimiliki oleh pemerintah.

Subscriber's Certificate usage is restricted by the Key Usage and Extended Key Usage of the Certificate Extension. IDI CA's Certificate can be used to issue Certificates for transactions that require:

- Authentication;
- Digital Signature & Non-Repudiation; and
- Encryption

Subscribers may choose an appropriate Level of Assurance in their identity that they wish to present to Relying Parties. Level of Assurance is distinguished in these following Certificate Class:

Level 3: Medium Assurance Certificate, which verifies identities with Government-owned identity data.

Level 4: Sertifikat dengan Tingkat Jaminan Tinggi. Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap data identitas yang dimiliki oleh pemerintah dan data biometrik.

Level 4: High Assurance Certificate High Assurance Certificate, which verifies identities with Government-owned identity data and biometric data.

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

Unauthorised use of Certificates may result in the voiding of warranties offered by IDI CAs to Subscribers and their Relying Parties.

Kelas Sertifikat/ Certificate Class	Tingkat Jaminan / Assurance Level			Penggunaan / Usage		
	Jaminan Rendah / Low Assurance	Jaminan Sedang / Medium Assurance	Jaminan Tinggi / High Assurance	Autentikasi / Authentication	Tanda Tangan Digital / Digital Signature	Enkripsi / Encryption
Sertifikat Individu / Individual Certificates						
Level 3		✓		✓	✓	✓
Level 4			✓	✓	✓	✓
Sertifikat Entitas / Entity Certificates						
Level 3		✓		✓	✓	✓
Level 4			✓	✓	✓	✓

1.4.2. Prohibited Certificate Uses / Penggunaan Sertifikat yang Dilarang

Sertifikat yang diterbitkan di bawah CP ini dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

Certificate issued under this CP are prohibited under any use not specified in Section 1.4.1.

1.5. Policy Administration / Administrasi Kebijakan

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

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

Policy Authority (PA) is an internal entity of a CA. The PA has roles and responsibilities as follows:

- Approves the Certificate Policy (CP);
- Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are well performed in accordance with the requirements, representations, and warranties of the CP; and
- Approves the establishment of trust relationships with external PKIs that approximately have equivalent Level of Assurance.

1.5.1. Organization Administering the Document / Organisasi Pengelola Dokumen

CP dan Dokumen Referensi lainnya dikelola oleh: compliance@vida.id Telp: 021 2598 3275	This CP and the document referenced herein are maintained by: compliance@vida.id Telp: 021 2598 3275

1.5.2. Contact Person / Kontak

Mailing address: Satrio Tower 25th Floor Jl. Prof. Dr. Satrio C4 No. 5 Jakarta 12950
Email: help@vida.id
URL: https://www.vida.id
Telp: 021 2598 3275

1.5.3. Person Determining CPS Suitability for the Policy / Personil yang menentukan Kesesuaian CPS dengan Kebijakan

Policy Authority (PA) PSrE IDI menentukan kesesuaian konten CP dan kesesuaian antara CP dengan CPS.	*Policy Authority* (PA) of IDI CA determines suitability of this CP and the conformance of CPS to this CP.

1.5.4. CP & CPS Approval Procedures / Prosedur Persetujuan CP & CPS

PSrE IDI menyetujui CP/CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CP/CPS atau dengan mempublikasikan adendum. IDI CA menentukan apakah perubahan atas CP ini membutuhkan pemberitahuan atau perubahan OID.	IDI CA approves the CP/CPS and any amendments. Amendments are made by either updating the entire CP/CPS or by publishing an addendum. IDI CA determines whether an amendment to this CP requires notice or an OID change.

1.6. Definitions and Acronyms / Definisi dan Akronim

Lihat Lampiran A untuk tabel akronim dan definisi.	See Appendix A for a table of acronyms and definitions.

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

2.1. Repositories / Repositori

PSrE IDI mengoperasikan repositori di mana dokumen kebijakan, sertifikat dari PSrE, CRL dipublikasikan	IDI CA operates online repositories where policy documents, Certificates, and CRL are published.

2.2. Publication of Certification Information / Publikasi Informasi Sertifikat

PSrE IDI memelihara repositori yang dapat diakses melalui internet yang mempublikasikan Sertifikat, CRL terakhir, dokumen CP/CPS, dan dokumen publik lain yang berkaitan dengan operasionalnya.	IDI CA maintains a repository accessible through the Internet in which it publishes Certificates, the latest CRL, the CP/CPS, and other public documents related to its operations.

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

CP ini dan tiap perubahan selanjutnya harus dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui.	This CP and any subsequent changes shall be made publicly available within 7 (seven) calendar days after its approval.
PSrE IDI akan mempublikasikan sertifikat Pemilik dan data pencabutan sertifikat dalam waktu 30 (tiga puluh) Menit setelah penerbitan.	IDI CA shall publish Subscriber certificates and revocation data within 30 (thirty) minutes after issuance.
CRL diperbaharui sesuai pengaturan pada bagian 4.9.7.	The CRL is updated according to the section 4.9.7.

2.4. Access Controls on Repositories / Kendali Akses pada Repositori

Informasi yang terpublikasi pada repositori adalah informasi publik. PSrE IDI akan memberikan akses baca yang tidak dibatasi pada repositori dan harus menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.	Information published on a repository is public information. IDI CA will provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.
CA IDI akan melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.	CA IDI shall protect information not intended for public dissemination or modification

3. IDENTIFICATION AND AUTHENTICATION / IDENTIFIKASI DAN OTENTIFIKASI

3.1. Naming / Penamaan

3.1.1. Types of Names / Tipe Nama

PSrE IDI akan membuat dan menandatangani Sertifikat dengan subyek Distinguished Name (DN) yang non-null dan mematuhi standar ITU X.500. Tabel di bawah meringkas DN dari Sertifikat yang diterbitkan oleh PSrE di bawah CP ini.

IDI CA will generate and sign certificates with a non-null subject Distinguished Name (DN) that complies with the ITU X.500 standards. The table below summarizes the DNs of the certificates issued by the CAs under this CP.

Certificate Type	Distinguished Name
CA Certificate	CN=<Certification Authority Name>, O=<organization name>, C=ID
Subscriber certificate	CN=<person name>,EMAILADDRESS=<email>,OU=<organizational unit>,O=<organization name>,C=ID
Entity certificate	CN=<person name>,EMAILADDRESS=<email>,OU=<organizational unit>,O=<organization name>,C=ID

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

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

The Certificates issued pursuant to this CP are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Names used in the Certificates shall identify the person or object to which they are assigned in a meaningful way.

Nama subjek dan penerbit yang terkandung dalam sertifikat HARUS bermakna dalam arti bahwa PSrE memiliki bukti keterkaitan yang cukup antara nama dengan entitasnya. Untuk mencapai tujuan ini, penggunaan nama harus diotorisasi oleh pemilik yang sah atau perwakilan resmi dari pemilik yang sah.

The subject and issuer name contained in a certificate MUST be meaningful in the sense that the CA has proper evidence of the existent association between these names and the entities to which they belong. To achieve this goal, the use of a name must be authorized by the rightful owner or a legal representative of the rightful owner.

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

PSrE tidak boleh menerbitkan sertifikat anonim atau pseudonim.	CAs shall not issue anonymous or pseudonymous certificates.

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

Distinguished Name (DN) dalam Sertifikat diinterpretasikan menggunakan standar X.500	Distinguished Name (DN) in Certificates are interpreted using X.500 standards.

3.1.5. Uniqueness of Names / Keunikan Nama

Semua distinguished name (DN) harus unik di dalam ranah IKP Indonesia.	All distinguished names shall be unique within the domain of Indonesia PKI.

3.1.6. Recognition, Authentication, and Role of Trademarks / Pengakuan, Otentikasi, dan Peran Merek Dagang

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE IDI tidak perlu memverifikasi hak Pemohon untuk penggunaan merek dagang. Merupakan tanggung jawab Pemilik untuk memastikan penggunaan nama-nama pilihan yang sah.	Subscriber may not request certificates with any content that infringes the intellectual property rights of other parties. IDI CA is not required to verify an applicant's right to use a trademark. It is the sole responsibility of the subscriber to ensure lawful use of chosen names.
PSrE dapat menolak setiap permohonan atau melakukan pencabutan Sertifikat apapun yang menjadi bagian dari konflik merk dagang.	CAs may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2. Initial Identity Validation / Validasi Identitas Awal

3.2.1. Method to Prove Possession of Private Key / Pembuktian Kepemilikan Private Key

Metode untuk membuktikan kepemilikan private key harus PKCS#10 (CSR), atau permintaan lain yang ekuivalen secara kriptografi (permintaan ditandatangani secara digital dengan private key).	The method to prove possession of a private key shall be PKCS #10 (CSR), or another cryptographically equivalent request (digitally signed request using private key).
Untuk sertifikat pemilik, pasangan kunci dapat dibangkitkan oleh PSrE IDI, dengan syarat bahwa kunci privat diamankan dengan menggunakan modul kriptografis yang memenuhi persyaratan FIPS-140 level 2 dan hanya dapat diakses oleh Pemilik, dengan minimal dua faktor autentikasi.	For subscriber certificate, the key pair may be generated by IDI CAs, with the condition that the subscriber's private key is secured using cryptographic modules that fulfill the requirement of FIPS-140 Level 2, and may only be accessed by the subscriber using a minimum of 2 (two) factors authentication.

3.2.2. Authentication of Organization Identity / Autentikasi dari Identitas Organisasi

Aplikasi bagi organisasi untuk menjadi Pelanggan harus dilakukan oleh orang yang berwenang untuk bertindak atas nama organisasi. Aplikasi ini harus sesuai dengan persyaratan sebagaimana tercantum dalam CPS dan termasuk rincian tentang salinan yang valid dari dokumen organisasi.
IDI CA kemudian melakukan verifikasi identitas dan status pekerjaan Pemohon dan wewenang mereka untuk menerima sertifikat untuk organisasi itu.

An application for an organization to become a Subscriber shall be made by a person authorized to act on behalf of the organization. This application shall conform to the requirements as set forth in the CPS and include details about the valid copy of organization document.
IDI CA then verifies the identity and employment status of the Applicant and their authority to receive the certificate for that organization.

3.2.3. Authentication of Individual Identity / Autentikasi dari Identitas Individu

Sebuah permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut.

An application for an individual to be a Subscriber may be made by the individual, or by another person or organization legally authorized to act on behalf of the prospective Subscriber.

PSrE IDI akan menyimpan dokumen dan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

IDI CA shall keep a record of the type and details of identification used for the authentication of the individual for at least the life of the issued certificate.

3.2.4. Non-Verified Subscriber Information / Informasi Pemilik yang Tidak Terverifikasi

Informasi yang tidak bisa diverifikasi tidak boleh disertakan di dalam sertifikat.

Information that is not verified shall not be included in Certificates.

3.2.5. Validation of Authority / Validasi Otoritas

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

Certificates that contain explicit or implicit organisational affiliation shall be issued only after ascertaining the applicant has the authorisation to act on behalf of the organisation in the asserted capacity.

3.2.6. Criteria for Interoperation / Kriteria Inter-Operasi

Tidak berlaku.

Not applicable.

3.3. Identification and Authentication for Re-Key Requests / Identifikasi dan Autentikasi untuk Permintaan Penggantian Kunci (Re-Key)

3.3.1. Identification and Authentication for Routine Re-Key / Identifikasi dan Autentikasi untuk kegiatan Re-Key

Re-key dilakukan secara adhoc, penggantian sertifikat secara rutin tidak disediakan.

Re-key is performed on an adhoc basis, certificate routine re-key is not provided.

3.3.2. Identification and Authentication for Re-Key after Revocation / Identifikasi dan Autentikasi untuk Re-Key setelah Revokasi

Pengguna yang mengajukan permintaan re-key setelah sertifikat dicabut harus menjalani proses pembuatan sertifikat baru.

A subscriber requesting re-key after a certificate is revoked shall undergo the initial registration process.

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

Permintaan pencabutan harus selalu diautentikasi. Permintaan untuk mencabut Sertifikat dapat diautentikasi menggunakan Kunci Publik yang terhubung dengan Sertifikat, tanpa mempertimbangkan apakah Kunci Privat telah terkompromi.

Revocation requests shall always be authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's associated Public Key, regardless of whether the Private Key has been compromised.

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

4.1. Certificate Application / Permohonan Sertifikat

4.1.1. Who can Submit a Certificate Application / Siapa yang dapat mengajukan sebuah permohonan sertifikat

PSrE IDI akan memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat dimana Sertifikat yang dimaksud menampilkan identitas kepada Pihak Pengandal atau Pemilik. Pemohon harus memberikan informasi yang cukup sehingga memungkinkan PSrE IDI dan RA untuk melakukan verifikasi atas identitas tersebut. PSrE IDI dan RA harus melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses permohonan.

Pemohon harus menyetujui kontrak berlangganan yang ditetapkan oleh PSrE IDI sebelum melakukan pendaftaran

IDI CA will maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties or Subscribers. Applicants should submit sufficient information to allow IDI CA and RAs to successfully perform the required verification. IDI CA and RAs shall protect communications and securely store information presented by the Applicant during the enrollment process.

Applicant shall accept subscription agreement before enrollment process.

4.1.2. Enrollment Process and Responsibilities / Proses Tanggung Jawab

PSrE IDI memelihara sistem dan proses yang secara memadai mengautentikasi identitas Pemohon untuk semua jenis Sertifikat yang menyajikan identitas kepada Pihak Pengandal. Pemohon harus mengirimkan informasi yang cukup untuk memungkinkan PSrE dan RA IDI melakukan verifikasi yang diperlukan. PSrE CA dan RA IDI harus melindungi komunikasi dan menyimpan informasi yang disajikan dengan aman oleh Pemohon selama proses aplikasi sesuai dengan Kebijakan Privasi PSrE IDI.
Secara umum, proses aplikasi mencakup langkah-langkah berikut:

- Mengajukan permintaan untuk jenis Sertifikat dengan persyaratan pendaftaran yang sesuai;
- Membuat Pasangan Kunci;

IDI CA maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow IDI CA and RA to successfully perform the required verification. IDI CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process in compliance with the IDI CA Privacy Policy.

Generally, the application process includes the following steps:

- Submitting a request for a Certificate type and appropriate application information;
- Generating a suitable Key Pair;

- Membuat *Certificate Siging Request* (CSR); dan
- Menyetujui *Subscriber Agreement* atau syarat dan ketentuan lain yang berlaku.

- Generating a Certificate Signing Request (CSR); and
- Agreeing to a Subscriber Agreement or other applicable terms and conditions.

4.2. Certificate Application Processing / Pemrosesan Permohonan Sertifikat

4.2.1. Performing Identification and Authentication Functions / Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi

Identifikasi dan autentikasi Pemilik harus memenuhi persyaratan yang ditentukan seperti yang tertera pada Bagian 3.2 dari CP ini. Untuk keterangan lebih rinci, harap mengacu pada CPS terkait.

The identification and authentication of the Subscriber shall meet the requirements specified in Sections 3.2 of this CP. For further details, please refer to the related CPS.

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

Setelah semua pemeriksaan identitas dan atribut Pemohon, konten aplikasi untuk sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap sertifikat atau permohonannya mengandung kesalahan, PSrE harus menolak permohonan. Apabila tidak ada masalah, permohonan disetujui.

After all identity and attribute checks of the Applicant, the content of the application for the certificate is also checked. In case the applicant is not eligible for a certificate or the application contains faults, CA shall reject the application. Otherwise the application is approved.

4.2.3. Time to Process Certificate Applications / Waktu Pemrosesan Permohonan Sertifikat

Semua pihak yang terlibat dalam pemrosesan permohonan sertifikat harus melakukan usaha untuk memastikan permohonan sertifikat diproses tepat waktu.

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner.

4.3. Certificate Issuance / Penerbitan Sertifikat

4.3.1. CA Actions during Certificate Issuance / Tindakan PSrE Selama Penerbitan Sertifikat

PSrE IDI memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan semua field dan ekstensi telah diisi dengan benar.	IDI CA verifies the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.
PSrE IDI akan mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, baru kemudian membuat Sertifikat milik Pemohon.	IDI CA shall authenticate a Certificate Request, ensure that the Public Key is bound to the correct Subscriber, obtain a proof of possession of the Private Key, then generate a Certificate.
PSrE IDI akan melakukan tindakannya selama proses penerbitan sertifikat secara aman.	IDI CA shall perform its actions during the certificate issuance process in a secure manner.

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

PSrE harus memberitahu Pemilik dalam selang waktu yang wajar tentang berhasilnya penerbitan sertifikat sesuai dengan prosedur yang diatur dalam CPS terkait.	CA shall notify the Subscriber within a reasonable time of successful certificate issuance in accordance with procedures set forth in the applicable CPS.

4.4. Certificate Acceptance / Penerimaan Sertifikat

4.4.1. Conduct Constituting Certificate Acceptance / Sikap Yang Dianggap Sebagai Menerima Sertifikat

PSrE IDI akan memberitahu Pemilik bahwa mereka tidak dapat memakai Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.	IDI CA shall notify to the Subscriber that they cannot use the certificate before checking all the information of certificate.
Ketika tidak ada keluhan dari Pemilik dalam jangka waktu tertentu sesuai yang ditentukan pada CPS, Pemilik dianggap menerima semua informasi Sertifikat.	When there are no complaint from Subscriber within certain period as per detailed in CPS, the Subscriber is deemed to accept all certificate information.
Untuk penerbitan Sertifikat PSrE IDI, PSrE Induk harus menyiapkan prosedur penerimaan yang mengindikasikan dan mendokumentasikan penerimaan atas Sertifikat yang diterbitkan	For the issuance of CA Certificates, IDI CA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

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

PSrE IDI harus mempublikasikan Sertifikat dalam suatu repositori, sesuai dengan praktik publikasi sertifikat milik PSrE IDI sebagaimana didefinisikan dalam CPS, termasuk juga ketika menerbitkan informasi pencabutan terkait Sertifikat tersebut.	IDI CA shall publish certificates in a repository based on the certificate publishing practices of the IDI CA (as defined in the CPS), as well as revocation information concerning such certificates.
Semua sertifikat harus dipublikasikan dalam repositori, sesuai dengan bagian 2, segera setelah diterbitkan.	All certificates shall be published in repository according to section 2 as soon as they are issued.

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

Tidak ada ketentuan.	No stipulation.

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

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

Baik Pemilik dan PSrE IDI harus melindungi Kunci Privat mereka dari penggunaan tanpa izin atau pengungkapan oleh pihak lain, dan harus memakai Kunci Privat mereka hanya untuk tujuan yang sudah ditentukan.	Both Subscriber and IDI CA shall protect their Private Key from unauthorized use or disclosure by other parties and shall use their Private Keys only for their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage / Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat

Pihak Pengandal harus menggunakan perangkat lunak yang patuh kepada X.509. PSrE harus menyatakan pembatasan penggunaan Sertifikat melalui ekstensi sertifikat dan harus menyatakan mekanisme untuk menentukan keabsahan sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan patuh kepada informasi ini sesuai dengan kewajiban mereka sebagai Pihak Pengandal.	Relying Parties shall use software that is compliant with X.509. CAs shall specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP). Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties.
Pihak Pengandal harus berhati-hati ketika mengandalkan sertifikat dan harus mempertimbangkan keseluruhan	A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of

keadaan dan risiko kerugian sebelum mengandalkan sertifikat. Mengandalkan tanda tangan atau sertifikat digital yang belum diproses sesuai dengan standar yang berlaku dapat menyebabkan risiko bagi Pihak Pengandal. Pihak Pengandal hanya bertanggung jawab atas risiko semacam itu. Dari keadaan menunjukkan bahwa diperlukan jaminan tambahan, Pihak Pengandal harus mendapatkan jaminan tersebut sebelum menggunakan sertifikat.

loss prior to relying on a certificate. Relying on a digital signature or certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. Of the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6. Certificate Renewal / Pembaruan Sertifikat

4.6.1. Circumstance for Certificate Renewal / Kondisi untuk Pembaruan Sertifikat

Pembaruan Sertifikat didefinisikan sebagai pembuatan Sertifikat baru yang memiliki detail yang sama dengan Sertifikat yang telah dikeluarkan sebelumnya namun dengan pasangan kunci yang berbeda dan bertanggal 'Not After' yang baru. PSrE IDI akan mengidentifikasi produk dan layanan di mana pembaruan dapat diterima. PSrE dapat memperbarui Sertifikat selama:

- Sertifikat asli yang akan diperbarui belum dicabut;
- Kunci Publik dari Sertifikat asli belum masuk daftar hitam karena alasan apa pun; dan
- Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan.
- PSrE dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya.

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate with different key pair but contains a new 'Not After' date. IDI CA will identify the products and services under which renewals can be accepted. A CA may renew a Certificate so long as:

- The original Certificate to be renewed has not been revoked;
- The Public Key from the original Certificate has not been blacklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.
- CAs may renew Certificates which have either been previously renewed.

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

Pemilik yang belum pernah dicabut sertifikatnya boleh meminta pembaruan Sertifikatnya ke PSrE IDI.

The Subscriber which has never been revoked may request the renewal of its Certificate.

4.6.3. Processing Certificate Renewal Requests / Pemrosesan Permintaan Pembaruan Sertifikat

PSrE IDI akan melakukan identifikasi dan autentifikasi permintaan pembaruan sertifikat.	IDI CA must identify and authenticate the Certificate renewal application.

4.6.4. Notification of New Certificate Issuance to Subscriber / Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik

Prosedur penerbitan sertifikat baru sebagaimana dinyatakan pada bagian 4.3.2.	The same new certificate issuance procedure is followed, as stated in section 4.3.2.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate / Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui

Pemilik dapat menerima sertifikat yang telah diperbarui sesuai dengan prosedur pendaftaran dan penerimaan sertifikat yang dinyatakan dalam bagian 4.4.1.	The Subscriber should receive the renewed certificate following the same procedure of acceptance and receipt of a new certificate, as stated in section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA / Publikasi Sertifikat yang Diperbarui oleh PSrE

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam bagian 4.4.2.	The new certificate is published according to the procedures stated in section 4.4.2.

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

Tidak ditentukan.	No stipulation

4.7. Certificate Re-Key / Re-Key Sertifikat

4.7.1. Circumstance for Certificate Re-Key / Lingkup Re-Key Sertifikat

Re-key sertifikat terdiri atas pembuatan sertifikat baru dengan kunci publik baru dan informasi subjek yang sama. Sertifikat baru tersebut dapat memiliki periode validitas ataupun kunci penandatanganan yang berbeda. Setelah re-key sertifikat selesai dilakukan, PSrE dapat mencabut sertifikat yang lama.	Re-keying a certificate consists of creating a new certificate with a new public key and subject information the same. The new certificate may have a different validity period, and a different signing key. After rekeying a certificate, IDI CA may revoke the old certificate.

4.7.2. Who May Request Certification of a New Public Key / Siapa yang Dapat Meminta Sertifikasi dari sebuah Kunci Publik Baru

Re-key certificate dapat diinisiasi atas permintaan Pemilik sertifikat.	Certificate re-key may be initiated upon a subscriber's request to IDI CA.

4.7.3. Processing Certificate Re-Keying Requests / Pemrosesan Permintaan Penggantian Kunci Sertifikat

Pelanggan mengajukan CSR baru yang akan IDI CA gunakan dan selanjutnya melakukan verifikasi ulang atas informasi yang dikirim.	Subscriber submits a new CSR which IDI CA will use the CSR and perform re-verification of the information submitted.

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

Prosedur notifikasi terhadap penerbitan sertifikat dilakukan adalah sama sebagaimana dinyatakan pada bagian 4.3.2.	The same notification procedure of the new certificate issuance is followed, as stated in section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate / Sikap yang Dianggap Sebagai Menerima Sertifikat yang Kuncinya Digantikan

Sertifikat yang dikeluarkan dianggap diterima setelah IDI CA mengirimkan pemberitahuan kepada Pelanggan.	Issued certificates are considered accepted after IDI CA notifies Subscriber.

4.7.6. Publication of the Re-Keyed Certificate by the CA / Publikasi Sertifikat yang Kuncinya Digantikan oleh PSrE

Tidak ditentukan.	No Stipulation.

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

Tidak ditentukan.	No Stipulation.

4.8. Certificate Modification / Modifikasi Sertifikat

4.8.1. Circumstance for Certificate Modification / Keadaan Bagi Modifikasi Sertifikat

Modifikasi informasi sertifikat tidak diizinkan.	Modification of certificate information is not permitted.

4.8.2. Who May Request Certificate Modification / Siapa yang Berhak Meminta Modifikasi Sertifikat

Tidak ditentukan.	No stipulation.

4.8.3. Processing Certificate Modification Requests / Pemrosesan Permintaan Modifikasi Sertifikat

Tidak ditentukan.	No stipulation.

4.8.4. Notification of New Certificate Issuance to Subscriber / Pemberitahuan tentang Penerbitan Sertifikat Baru ke Pemilik

Tidak ditentukan.	No stipulation.

4.8.5. Conduct Constituting Acceptance of Modified Certificate / Sikap yang Dianggap Sebagai Menerima Sertifikat yang Dimodifikasi

Tidak ditentukan.	No stipulation.

4.8.6. Publication of the Modified Certificate by the CA / Publikasi Sertifikat yang Dimodifikasi oleh PSrE

Tidak ditentukan.	No stipulation.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities / Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain

Tidak ditentukan.	No stipulation.

4.9. Certificate Revocation and Suspension / Pencabutan dan Pembekuan Sertifikat

4.9.1. Circumstances for Revocation / Keadaan untuk Pencabutan

PSrE IDI akan mencabut sertifikat Pemilik dalam keadaan berikut:	IDI CA shall revoke a subscriber's certificate in the following circumstances:
• Komponen informasi identifikasi atau afiliasi dari nama dalam sertifikat menjadi tidak valid.	• Identifying information or affiliation components of any names in the certificate becomes invalid.
• Informasi apapun dalam sertifikat menjadi tidak valid.	• Any information in the certificate becomes invalid.
• Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya.	• The subscriber can be shown to have violated the stipulations of its subscriber agreement.

- Ada alasan untuk meyakini bahwa kunci privat telah dikompromikan/rusak.
- Pemilik atau pihak berwenang lainnya meminta sertifikatnya dicabut.

Sertifikat harus dicabut ketika hubungan antara subyek dan kunci publiknya yang didefinisikan dalam sertifikat sudah tidak valid lagi. Ketika hal ini terjadi sertifikat seharusnya dicabut dan diletakkan pada CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status sertifikat sampai sertifikat kedaluwarsa.

- There is reason to believe the private key has been compromised.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. When this occurs, the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2. Who can Request Revocation / Siapa yang Dapat Meminta Pencabutan

Sertifikat dapat diminta untuk dicabut oleh Pemilik atau entitas lain yang dapat membuktikan terungkapnya kunci privat atau penyalahgunaan sertifikat sesuai dengan Kebijakan Sertifikat.

The certificate can be requested to be revoked by the subscriber or by another entity that can prove the exposure or the misuse of the certificate according to the Certification Policy.

4.9.3. Procedure for Revocation Request / Prosedur Permintaan Pencabutan

PSrE IDI akan memverifikasi identitas dan wewenang (untuk entitas penegak hukum) dari Pemilik yang mengajukan pencabutan sertifikat. Validitas identitas Pemilik dibutuhkan sesuai dengan bagian 3.4.

Permintaan pencabutan Sertifikat oleh entitas lain harus menyerahkan bukti bahwa:

a. kunci privat sertifikat telah terungkap, atau
b.
c. penggunaan sertifikat tidak sesuai dengan Kebijakan Sertifikat, atau
d. pemilik sertifikat tidak memiliki hubungan dengan institusi

Langkah-langkah pada proses permintaan pembatalan sertifikat dijelaskan lebih rinci dalam CPS.

IDI CA shall verify the identity and authority (for juridical entity) of a subscriber making the request for revocation. The validation of the subscriber's identity is required according to section 3.4.

Request for revocation by other entity must have submission of proof that,

a. the private key of the certificate has been exposed, or
b. the use of the certificate does not conform to the Certification Policy or
c. the certificate owner's relationship with the institution does not exist.

The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.9.4. Revocation Request Grace Period / Masa Tenggang Permintaan Pencabutan

Tidak ada masa tenggang untuk pembatalan dalam kebijakan ini.	There is no grace period for revocation under this policy.

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

PSrE IDI akan memulai permintaan investigasi dalam satu (1) hari kerja kecuali dalam hal *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang cukup akan diproses sesegera mungkin.	IDI CA must start the investigation of revocation requests within one (1) business day except from force majeure cases. Revocation requests that provide adequate supporting evidence will be processed immediately.

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

Pihak Pengandal harus memvalidasi sertifikat terhadap CRL terbaru melalui repositori maupun terhadap server OCSP penerbit yang relevan.	Relying parties should validate any presented certificate against the most updated CRL via repository or against the relevant issuer's OCSP server.

4.9.7. CRL Issuance Frequency (if applicable) / Frekuensi Penerbitan CRL (bila berlaku)

CRL harus diperbarui dan dipublikasi: ● untuk sertifikat end-user/perangkat, segera setelah adanya proses yang memicu perubahan CRL atau paling sedikit sekali setiap satu (1) hari. CRL akan berdampak dalam waktu maksimum sepuluh (10) hari. ● untuk sertifikat PSrE, sedikitnya setiap enam (6) bulan. CRL akan berdampak dalam waktu maksimum enam (6) bulan.	The CRL must be updated and published: ● for end-user/device certificates, immediately after a process triggers a CRL update or at least once every single (1) day. The CRL will be in effect for a maximum time of ten (10) days. ● for CA certificates, at least every six (6) months. The CRL will be in effect for a maximum time of six (6) months.
Dalam kasus kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat PSrE IDI, CRL terbaru HARUS dipublikasi dalam waktu 24 jam semenjak stempel waktu (timestamp) pencabutan.	In case of secret key exposure or of any other important security compromise incident, for example a sub CA revocation, an updated Certificate Revocation List MUST be published within 24 hours from the revocation timestamp.
CRL harus disimpan pada lingkungan yang dilindungi untuk menjamin integritas dan keotentikannya.	CRLs shall be stored in a protected environment in order to ensure their integrity and authenticity

4.9.8. Maximum Latency for CRLs (if applicable) / Latensi Maksimum CRL (bila berlaku)

Pembaruan CRL dipublikasikan otomatis ke repositori daring paling lambat 30 menit setelah adanya perubahan atau akan dipublikasikan secara teratur sesuai dengan jadwal.	CRLs are posted automatically to the online repository within 30 minutes after any update otherwise they will be published regularly as per schedule.

4.9.9. On-Line Revocation/Status Checking Availability / Ketersediaan Pemeriksaan Pencabutan/Status Daring

PSrE IDI memberikan layanan validasi daring, Jika validasi daring tersedia, diharapkan melakukan pengecekan menggunakan Server OCSP yang disediakan.	IDI CA provides online validation service. If online validation is available, it is expected to perform revocation checks using the OCSP Server provided.

4.9.10. On-Line Revocation Checking Requirements / Persyaratan Pemeriksaan Pencabutan Daring

Tidak ditentukan.	No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available / Bentuk Lain dari Pengumuman Pencabutan yang Tersedia

Tidak ditentukan.	No stipulation.

4.9.12. Special Requirements Re-Key Compromise / Kompromi Re-Key Persyaratan Khusus

Tidak ditentukan.	No stipulation.

4.9.13. Circumstances for Suspension / Keadaan untuk Pembekuan

Pembekuan sertifikat tidak disediakan.	Certificate suspension is not provided.

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

Pembekuan sertifikat tidak disediakan.	Certificate suspension is not provided.

4.9.15. Procedure for Suspension Request / Prosedur Permintaan Pembekuan

Pembekuan sertifikat tidak disediakan.	Certificate suspension is not provided.

4.9.16. Limits on Suspension Period / Batas Waktu Pembekuan

Pembekuan sertifikat tidak disediakan.	Certificate suspension is not provided.

4.10. Certificate Status Services / Layanan Status Sertifikat

4.10.1. Operational Characteristics / Karakteristik Operasional

Status sertifikat publik tersedia dari CRL di dalam repositori.	The status of public certificates is available from CRL's in the repositories.

4.10.2. Service Availability / Ketersediaan Layanan

PSrE IDI akan melakukan semua tindakan yang diperlukan untuk menjamin ketersediaan layanan validasi status sertifikat.	IDI CA shall take all necessary measures to ensure availability of certificate status validation service.

4.10.3. Optional Features / Fitur Opsional

Tidak ditentukan.	No stipulation.

4.11. End of Subscription / Akhir Berlangganan

Pemilik dapat mengakhiri langganan dengan membiarkan sertifikatnya kedaluwarsa atau mencabut sertifikatnya tanpa meminta sertifikat yang baru.	Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12. Key Escrow and Recovery / Pemulihan dan Penitipan Kunci

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

Tidak ditentukan.	No stipulation.

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

Tidak ditentukan.	No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS / FASILITAS, MANAJEMEN, DAN KENDALI OPERASI

5.1. Physical Controls / Kendali Fisik

5.1.1. Site Location and Construction / Lokasi dan Konstruksi

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

The location and construction of the facility housing IDI CA equipment used to administer the IDI CA, are consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and CCTV, has provided robust protection against unauthorized access to the IDI CA equipment and records.

5.1.2. Physical Access / Akses Fisik

Perangkat PSrE IDI harus selalu diberikan pengamanan dari akses yang tidak diperbolehkan. Mekanisme keamanan fisik untuk PSrE IDI setidaknya harus dilakukan untuk:

- Memastikan tidak ada akses ke perangkat keras tanpa izin
- Menyimpan semua media dan kertas yang berisi informasi teks polos yang sensitif dalam wadah yang aman.
- Memonitor, baik secara manual maupun elektronik, dari intrusi tanpa hak setiap saat.
- Memelihara dan secara berkala memeriksa log akses.

IDI CA equipment shall always be protected from unauthorized access. The physical security mechanisms for CAs at a minimum shall be in place to:

- Ensure no unauthorized access to the hardware is permitted
- Store all removable media and paper containing sensitive plain-text information in secure containers.
- Monitor, either manually or electronically, for unauthorized intrusion at all times.
- Maintain and periodically inspect an access log.

5.1.3. Power and Air Conditioning / Daya dan Penyejuk Udara

PSrE IDI memiliki daya cadangan yang cukup untuk me-lockout secara otomatis,

IDI CA has backup power sufficient to automatically lockout input, finish any

menyelesaikan beberapa hal/tindakan yang tertunda, dan mencatat keadaan peralatan sebelum kekurangan daya atau 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 kelangsungan operasi.

pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories have been provided with Uninterrupted Power and Power Generator sufficient for a minimum of 6 (six) hours operation in the absence of commercial power, to support continuity of operations.

5.1.4. Water Exposures / Pemaparan Air

IDI CA dilindungi terhadap air dengan cara meletakkannya di atas tanah atau menggunakan raised floor. Sistem pencegahan kebakaran seperti sprinkler termasuk ke dalam pengecualian.

IDI CA equipment is protected against water by having it located above ground or using raised flooring. Fire prevention systems such as sprinklers are considered as exceptions.

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

Peralatan PSrE IDI ditempatkan di fasilitas dengan sistem deteksi dan pemadaman kebakaran yang memadai.

IDI CA equipment is placed in facilities with adequate fire detection and suppression systems.

5.1.6. Media Storage / Penyimpanan Media

Media PSrE IDI 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 aman.

IDI CA Indonesia's Media were stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media containing audit, archive, or backup information were duplicated and stored in a secure manner.

5.1.7. Waste Disposal / Pembuangan Limbah

Bahan limbah yang mengandung informasi sensitif harus dihancurkan informasi yang ada di dalamnya sebelum dibuang.

All sensitive information which is contained in waste material must be destroyed before it is disposed of in a designated place.

5.1.8. Off-Site Backup / Backup Off-Site

Backup sistem dari PSrE, dimana backup tersebut cukup untuk memulihkan dari kegagalan sistem, harus dilakukan secara berkala. Backup harus dilakukan dan disimpan di luar lokasi tidak kurang dari sekali setiap

System backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule. Backups shall be performed and stored offsite not less than once every seven (7) days. At least one (1) full backup copy shall be stored at an offsite

tujuh (7) hari. Setidaknya satu (1) salinan backup lengkap harus disimpan di lokasi di luar kantor (di lokasi yang terpisah dari peralatan PSrE). Hanya backup lengkap terbaru yang perlu dipertahankan. Data backup harus dilindungi dengan kendali fisik dan prosedural yang sepadan dengan operasional PSrE.

location (at a location separate from the CA equipment). Only the latest full backup needs to be retained. The backup data shall be protected with physical and procedural controls commensurate to that of the operational CA.

5.2. Procedural Controls / Kendali Prosedur

5.2.1. Trusted Roles / Peran Terpercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

- CA Team Leader

Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan PSrE

- Key Manager

Bertanggung jawab untuk menjaga token CA dan perangkat HSM

- Administrator CA

Melakukan operasional dan maintenance aplikasi manajemen PSrE

- Administrator RA

Identifikasi dan Validasi identitas permohonan permintaan sertifikat

- Administrator VA

Bertanggung jawab dalam proses validasi sertifikat dan ketersediaan layanan tersebut

- Manajer Repositori

Bertanggung jawab terhadap konten yang dipublikasikan pada repositori

- Pengembang Piranti Lunak

Bertanggung jawab dalam mengembangkan aplikasi dan melakukan integrasi terkait dengan sistem PSrE

- Facility Engineer

Bertanggung jawab terhadap kelancaran perangkat CA

- Policy Authority

Bertanggung jawab untuk pembuatan, revisi dan persetujuan CP dan CPS

Trusted role includes, but not limited to:

- CA Team Leader

Overall responsibility for managing all CA security practices

- Key Manager

Accountable for keeping the CA and HSM tokens

- CA Administrator

Conduct operasional and maintenance of CA management application

- RA Administrator

Identification and validation of certificate request application

- VA Administrator

Responsible for certificate validation process and ensure the services are available

- Repository Manager

Responsible for all contents that published in repository

- Software Developer

responsible for developing applications and performing integrations related to the CA organization systems

- Facility Engineer

Responsible for the smooth running of CA equipments

- Policy Authority

Responsible for creation, revision and approval of CP and CPS

- Security Officer

Bertanggung jawab terhadap keamanan fisik maupun logis dari sistem PSrE

- Internal Auditor

Melakukan audit internal terhadap pelaksanaan operasional PSrE

- Security Officer

Accountable for the Physical and Logical security of the CA organization and systems

- Internal Auditor

Conduct internal audit of CA operational

5.2.2. Number of Persons Required per Task / Jumlah Orang yang Dibutuhkan per Tugas

Untuk kegiatan yang memerlukan kendali multi-pihak, semua partisipan harus memegang peran terpercaya. Kendali multi-pihak harus tidak dicapai dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan tiga orang atau lebih

- Pembangkitan kunci PSrE
- Penandatanganan Kunci PSrE IDI
- Pencabutan Sertifikat

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require three or more persons:

- CA key generation
- IDI CA's Key Signing
- Certificate Revocation

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

Semua individu yang ditugaskan dalam peran terpercaya harus diidentifikasi dan diautentikasi menggunakan Surat Penugasan.

All individuals assigned to a trusted role shall be identified and authenticated using Assignment Letter.

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

Role yang ditidak boleh diperankan bersamaan adalah:

- Policy Authority dan administrator operasional
- Internal audit dan semua peran lain
- Pengembang aplikasi dan semua peran lain.

Same person was not assigned to another role for:

- Policy authority and operational administrator
- Internal audit and any other role.
- Application developer and any other role).

5.3. Personnel Controls / Kendali Personil

5.3.1. Qualifications, Experience, and Clearance Requirements / Persyaratan Kualifikasi, Pengalaman, dan Clearance

Semua personil di PSrE IDI dipilih atas dasar keterampilan, pengalaman, kesetiaan, kepercayaan, dan integritas. Personil yang ditunjuk untuk peran terpercaya harus secara resmi diangkat oleh manajemen senior

All persons shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. Personnel appointed to trusted roles shall be formally appointed by senior management).

5.3.2. Background Check Procedures / Prosedur Pemeriksaan Latar Belakang

Semua personil di PSrE harus lulus pemeriksaan latar belakang. Lingkup pemeriksaan latar belakang mencakup area berikut, yang paling sedikit lima (5) tahun:

- Kontak Referensi Pekerjaan
- Pendidikan atau sertifikasi
- Identifikasi Kependudukan (KTP)
- Catatan Kepolisian

All persons shall have completed a background check. The scope of the background check shall include the following areas covering at least the past five (5) years:

- Employment Contact Reference
- Education or certification
- Residential Identification
- Police Certificate of Good Conduct

Prosedur pemeriksaan latar belakang harus dijelaskan pada CPS

Background check procedures shall be described in the CPS.

5.3.3. Training Requirements / Persyaratan Training

Semua personil PSrE harus dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan ini akan membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, dan prosedur terkait.

Pelatihan tersebut harus mencakup operasional minimum dari PSrE (termasuk perangkat keras, perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP ini, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil PSrE harus dilakukan minimal 1 (satu) kali dalam setahun).

All CA personnel shall be appropriately trained to perform their duties. Such training will address relevant topics, such as security requirements, operational responsibilities and associated procedures.

The training shall include minimum operations of the CA (including CA hardware, software and operating system), operational and security procedures, this CP and the applicable CPS. The adequacy of the competence of CA personnel shall be conducted at least 1 (one) time a year.

5.3.4. Retraining Frequency and Requirements / Frekuensi dan Persyaratan Training Ulang

PSrE IDI akan memberikan penyegaran pelatihan dan pembaruan pada personilnya sejauh dan sesering yang dibutuhkan untuk memastikan personil tersebut mempertahankan tingkat kemampuan yang dipersyaratkan untuk melakukan tanggung jawab pekerjaannya secara kompeten dan memuaskan).

IDI CA shall provide refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

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

PSrE IDI akan memastikan bahwa perubahan staf tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

IDI CA should ensure that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6. Sanctions for Unauthorized Actions / Sanksi untuk Tindakan Tidak Terotorisasi

Sanksi disiplin yang sesuai berlaku pada personel yang melanggar ketentuan dan kebijakan dalam CP ini, CPS, atau prosedur operasional PSrE terkait).

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within the CP, CPS or CA related operational procedures).

5.3.7. Independent Contractor Requirements / Persyaratan Kontraktor Independen

Personel sub-kontraktor yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional PSrE harus memenuhi persyaratan yang berlaku yang ditetapkan dalam CP ini (misalnya, semua persyaratan pada bagian 5.3).

Sub-Contractor personnel employed to perform functions pertaining to CA operations shall meet applicable requirements set forth in this CP (e.g., all requirements of section 5.3).

5.3.8. Documentation Supplied to Personnel / Dokumentasi yang Diberikan kepada Personil

PSrE harus menyediakan kepada para personilnya Certificate Policy yang mereka gunakan, CPS, dan setiap undang-undang yang relevan, kebijakan, atau kontrak apapun. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) harus

CAs shall make available to its personnel the Certificate Policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the trusted personnel to perform their duties
.

disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

5.4. Audit Logging Procedures / Prosedur Log Audit

PSrE IDI akan mengakses kerentanan sistem PSrE atau komponennya paling tidak sekali setahun.

IDI CA shall assess the vulnerability of its CA system or its components at least on a yearly basis.

5.4.1. Types of Events Recorded / Jenis Kejadian yang Direkam

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

All security auditing capabilities of the CA and RA operating system and the CA, VA, and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. IDI CA should ensure all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services.

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

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

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event,
- Serial or sequence number of entry
- The date and time the event occurred.
- Source of entry
- Success or failure where appropriate,
- The identity of the entity and/or operator that caused the event

5.4.2. Frequency of Processing Log / Frekuensi Pemrosesan Log

Log audit harus ditinjau sedikitnya sebulan sekali. Tinjauan tersebut termasuk verifikasi bahwa log tersebut tidak dirusak, tidak ada diskontinuitas atau hilangnya data audit, dan kemudian secara singkat memeriksa semua entri log, dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan dalam log.
Tindakan yang diambil sebagai hasil dari peninjauan ini harus didokumentasikan.

Audit logs shall be reviewed at least monthly. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Actions taken as a result of these reviews shall be documented.

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

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

IDI CA audit log shall be retained for 1 (satu) years in order to be available for any lawful control. This period may be modified depending on developments of relevant laws.

5.4.4. Protection of Audit Log / Proteksi Log Audit

PSrE IDI akan mengakses kerentanan sistem PSrE atau komponennya paling tidak sekali setahun.

IDI CA shall assess the vulnerability of its CA system or its components at least on a yearly basis.

5.4.5. Audit Log Backup Procedures / Prosedur Backup Log Audit

Log audit PSrE IDI harus di-backup sedikitnya sebulan sekali. Media backup harus disimpan di tempat lokal pada lokasi yang aman. Salinan kedua dari log audit harus diletakkan pada tempat yang lain setiap bulan.

IDI CA's Audit logs shall be backed up at least monthly. Backup media shall be stored locally in a secure location. A second copy of the audit log shall be sent off-site on a monthly basis.

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

Sistem pengumpulan log audit adalah internal ke sistem PSrE IDI.

The audit log collection system was internal to the IDI CA system.

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

Tidak ditentukan.

No stipulation.

5.4.8. Vulnerability Assessments / Asesmen Kerentanan

PSrE IDI akan mengakses kerentanan sistem PSrE atau komponennya paling tidak sekali setahun.

IDI CA shall assess the vulnerability of its CA system or its components at least on a yearly basis.

5.5. Records Archival / Pengarsipan Record

5.5.1. Types of Records Archived / Tipe Record yang Diarsipkan

Catatan arsip PSrE IDI akan harus cukup rinci untuk menentukan operasional PSrE yang benar dan validitas sertifikat apapun (termasuk yang dicabut atau kedaluwarsa) yang dikeluarkan oleh PSrE. Minimal, data berikut harus dicatat pada arsip:

- Siklus hidup Sertifikat termasuk di dalamnya permohonan sertifikat, permintaan pencabutan sertifikat, dan permintaan re-key.
- Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh PSrE IDI.
- Data konfigurasi sistem IKP Indonesia
- Dokumen CP dan semua CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.

IDI CA archives records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- Certificate life cycle operations including certificate requests, revocation requests, and re-key requests.
- All certificates and CRLs as issued or published by the CAs.
- Indonesia PKI system configuration data
- This CP document and all applicable CPSs including modifications and amendments to these documents.

5.5.2. Retention Period for Archive / Periode Retensi Arsip

Catatan yang diarsipkan harus disimpan setidaknya selama tujuh (7) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.

Archived records shall be retained for at least tujuh (7) years. Applications necessary to read these archives shall be maintained for the retention period.

5.5.3. Protection of Archive / Perlindungan Arsip

Catatan yang diarsipkan harus dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan yang

The archived records shall be protected against unauthorized viewing, modification, deletion, or tampering. The media holding the archived records and the applications

diarsipkan dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan harus dipelihara dan dilindungi sesuai peraturan yang ditentukan dalam CP ini dan CPS yang berlaku.

required to process the archived records shall be maintained and protected as per the rules specified in this CP and applicable CPSs.

5.5.4. Archive Backup Procedures / Prosedur Backup Arsip

Prosedur backup arsip yang memadai dan teratur harus dilakukan agar jika terjadi kehilangan atau kerusakan arsip utama, tersedia satu set lengkap salinan backup di lokasi terpisah. CPS atau dokumen yang diacu harus menguraikan bagaimana rekaman arsip di-backup, dan bagaimana backup arsip dikelola.

Adequate and regular backup procedures shall be in place so that in the event of loss or destruction of the primary archives, a complete set of backup copies held in a separate location will be available. The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5. Requirements for Time-Stamping of Records / Kewajiban Pemberian Label Waktu pada Rekaman Arsip

Rekaman arsip PSrE IDI arus diberi label waktu saat dibuat.

IDI CA archive records shall be time-stamped as they are created.

5.5.6. Archive Collection System (Internal or External) / Sistem Pengumpulan Arsip (Internal atau Eksternal)

Pengumpulan arsip di PSrE IDI dilakukan oleh internal PSrE.

Archive Collection Process is conducted by IDI CA internally.

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

Media penyimpanan arsip informasi di PSrE diperiksa pada saat dibuat. Dalam waktu berkala, sampel informasi yang diarsip akan diperiksa untuk memastikan informasi tetap terintegrasi dan dapat dibaca. Hanya jabatan-jabatan tertentu dan terpercaya, serta karyawan yang terotorisasi yang dapat mengakses arsip. Permintaan untuk mendapatkan dan memverifikasi informasi di arsip dikoordinasi oleh operator dari jabatan terpercaya.

Media storing of CA archive information is checked upon creation. Periodically, samples of archived information are tested to check the continued integrity and readability of the information. Only authorised CA, trusted role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by operators in trusted roles.

5.6. Key Changeover / Pergantian Kunci

Untuk meminimalkan risiko dari kondisi Kunci Privat PSrE terkompromi, Kunci Privat dapat sering diubah. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat yang lama, namun masih berlaku, akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat terkait kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama harus disimpan dan dilindungi.

To minimize risk from compromise of a IDI CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

Apabila PSrE IDI memperbarui kunci privat dan dengan demikian menghasilkan kunci publik baru, PSrE IDI harus memberitahu semua Pemilik dan Pihak Pengandal bahwa telah terjadi perubahan.

When IDI CA updates its private signature key and thus generates a new public key, the IDI CA will notify all Subscribers and Relying Parties that it has been changed.

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

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

PSrE IDI memiliki rencana tanggap darurat dan rencana pemulihan bencana.

IDI CA shall have an incident response plan and a disaster recovery plan.

Jika PSrE IDI dicurigai telah terkompromi, penerbitan Sertifikat oleh PSrE tersebut harus dihentikan seketika. Investigasi independen oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan harus dinilai untuk menentukan prosedur perbaikan yang tepat. Jika Kunci Privat PSrE dicurigai sudah terkompromi, prosedur pada Bagian 5.7.3 harus diikuti.

If compromise of IDI CA is suspected, certificate issuance by that CA shall be stopped immediately. An independent, third-party investigation shall be performed in order to determine the nature and the degree of damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

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

Dalam kasus PSrE mengakhiri operasinya, mereka harus memberitahu ke PSrE Induk, PA, dan para Pemilik sebelum penutupan agar mematuhi Peraturan Pemerintah.

In the event that a CA terminates its operation, it shall provide notice to Root CA Indonesia, PA, and subscribers prior to termination in compliance with Government Regulations.

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

Dalam kasus PSrE Induk kehilangan kunci privat PA ataupun CA Team Leader akan mendapatkan pemberitahuan dan bekerja sama dengan perwakilan dari PSrE Induk untuk melaksanakan tindakan yang dapat menyelesaikan isu tersebut.

If the private key of the Root CA is lost, Root CA shall notify the PA or CA Team leader will be notified and work closely with Root CA representative to take appropriate actions to resolve the issue.

Dalam kasus IDI CA kehilangan kunci priva atau terkompromi, semua Pemilik dan Pihak Penganda yang terkait mendapat pemberitahuan, semua sertifikat Pemilik yang diterbitkan oleh PSrE IDI yang terkompromi tersebut dicabut bersamaan dengan sertifikat milik PSrE, serta kunci-kunci beserta sertifikat-sertifikat baru diterbitkan segera setelah kondisi kondusif.

In case of IDI CA's private key is compromised or lost, all related subscribers and Relying Parties are notified, all related subscriber certificates issued by the compromised CA are revoked along with the certificate of the CA, and new keys and certificates are issued as soon as after the condition is getting conducive.

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

PSrE IDI menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbaharui. Suatu pemulihan layanan secara penuh harus terlaksana dalam 24 jam bila ada bencana.

IDI CA shall prepare a disaster recovery plan which has been tested, verified and continually updated. A full restoration of services shall be done within 24 hours in case of disaster.

5.8. CA or RA Termination / Penutupan CA atau RA

Dalam kasus PSrE IDI mengakhiri operasinya, mereka harus memberitahu ke PSrE Induk, PA, dan para Pemilik sebelum penutupan agar mematuhi Peraturan Pemerintah.

In the event that a CA terminates its operation, it shall provide notice to Root CA Indonesia, PA, and subscribers prior to termination in compliance with Government Regulations.

6. TECHNICAL SECURITY CONTROLS / KENDALI KEAMANAN TEKNIS

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

6.1.1. Key Pair Generation / Pembangkitan Pasangan Kunci

6.1.1.1. CA Key Pair Generation / Pembangkitan Pasangan Kunci CA

Material kunci kriptografi yang digunakan oleh PSrE untuk menandatangani sertifikat, CRL atau informasi status harus dibuat di dalam modul kriptografi yang sesuai standar FIPS 140, atau standar lain yang setara. Kendali multi-pihak dibutuhkan untuk pembangkitan pasangan kunci PSrE, seperti yang ditentukan pada bagian 6.2.2.	Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in cryptographic modules validated to FIPS 140, or some other equivalent standard. Multi-party control is required for CA key pair generation, as specified in section 6.2.2.
Pembangkitan pasangan kunci PSrE harus menghasilkan jejak audit yang dapat diverifikasi yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. Dokumentasi prosedur harus cukup rinci untuk menunjukkan bahwa pemisahan peran yang tepat digunakan. Pihak ketiga yang independen harus memvalidasi pelaksanaan prosedur pembangkitan kunci baik dengan menyaksikan pembangkitan kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci	CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. Appropriate role separation of the key generation process was documented in the internal document of IDI CA. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation

6.1.1.2. Subscriber Key Pair Generation / Pembangkitan Pasangan Kunci Pemilik

Pembangkitan pasangan kunci Pemilik harus dilakukan oleh Pemilik menggunakan aplikasi yang dikembangkan oleh PSrE IDI atau oleh PSrE IDI. Jika PSrE IDI membangkitkan pasangan kunci untuk Pemilik, persyaratan pengiriman pasangan kunci yang dinyatakan dalam bagian 6.1.2 juga harus dipenuhi dan PSrE harus membangkitkan kunci dalam suatu perangkat keras kriptografis yang tervalidasi FIPS 140.	Subscriber key pair generation shall be performed by either the subscriber through an application developed by IDI CA or by IDI CA. If the CA generates key pairs for subscriber, the requirements for key pair delivery specified in section 6.1.2 must also be met and the CA shall generate key within a secure FIPS 140 validated cryptographic hardware.

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

Jika Pemilik membangkitkan sendiri Pasangan Kuncinya, maka tidak ada kebutuhan pengiriman Kunci Privat, dan bagian ini tidak berlaku.

Bila PSrE IDI membangkitkan kunci atas nama Pemilik pada HSM milik PSrE IDI, maka Kunci Privat harus disimpan secara aman di server PSrE IDI. Kunci privat dapat juga dikirim secara elektronik atau dikirimkan pada modul kriptografi hardware.

Dalam semua kasus , Kunci Privat harus dilindungi terhadap aktivasi, *compromise*, atau perubahan selama proses pengiriman.

If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply.

When IDI CA generates keys on behalf of the Subscriber at the HSM of IDI CA, then the Private Key shall be stored securely in the server of IDI CA. Private keys may also be delivered electronically or may be delivered on a hardware cryptographic module.

In all cases, the Private Key shall be protected from activation, compromise, or modification during the delivery process.

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

Apabila pasangan kunci dibangkitkan oleh Pemilik, kunci publik dan identitas Pemilik harus dikirimkan dengan aman (misalnya menggunakan TLS dengan algoritma dan panjang kunci yang disetujui) pada PSrE untuk penerbitan sertifikat. Mekanisme pengiriman harus menyertakan identitas Pemilik yang telah diverifikasi dan ditandatangani menggunakan kunci privat pemilik.

Where key pairs are generated by the Subscriber, the public key and the subscriber's identity must be delivered securely (e.g., using TLS with approved algorithms and key lengths) to the CA for certificate issuance. The delivery mechanism shall include Subscriber's identity that has been verified and signed using Subscriber's private key.

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

Setiap sertifikat digital yang diterbitkan oleh PSrE berisi kunci publik. PSrE IDI harus menyediakan mekanisme pengiriman secara digital (*digital delivery*) yang aman bagi semua sertifikat yang diterbitkan. Sebagai contoh, semua sertifikat dari setiap PSrE dipublikasikan melalui suatu situs web yang aman, yang identitasnya disertifikasi oleh penyedia SSL terpercaya.

Public Key is included in digital certificate issued by the CA. IDI CA shall provide mechanisms for securing digital delivery of all certificates. This may include publication through a trusted SSL secured website.

Pada jangka waktu tertentu sebelum kunci publik PSrE kedaluwarsa, suatu pasangan kunci penandatanganan sertifikat yang baru akan dibangkitkan untuk menjaga operasional PSrE berjalan normal.

For a certain period before the expiry date of a CA's public key, a new key pair for certificate signing will generated so that CAs keep working normally.

Penjelasan tentang publikasi dan repositori sertifikat mengacu pada Bagian 2.1.

Certificate publication and repository responsibilities is referred to Section 2.1 of this CP.

6.1.5. Key Sizes / Ukuran Kunci

PSrE yang membuat sertifikat dan CRL di bawah policy ini harus menggunakan algoritma RSA dengan panjang kunci 4096 bit dan hash SHA-384 ketika membuat tanda tangan digital.

CAs that generate certificates and CRLs under this policy should use RSA algorithm with a key length of 4096 bit, and SHA-384 hash algorithm when generating digital signatures.

Pemilik sertifikat di bawah policy ini harus menggunakan algoritma RSA dengan panjang kunci 2048 bit dan hash SHA-384 ketika membuat tanda tangan digital.

Certificate subscriber under this policy should use RSA algorithm with a key length of 2048 bit, and SHA-384 hash algorithm when generating digital signatures.

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

Tidak ditentukan.

No stipulation.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field) / Tujuan Penggunaan Kunci (pada field key usage - X509 v3)

Kunci publik yang terikat pada suatu sertifikat harus disertifikasi, agar kunci publik tersebut bisa digunakan untuk autentikasi, penandatanganan, atau enkripsi, tapi tidak semua, kecuali yang sudah ditentukan oleh PSrE IDI. Penggunaan sebuah kunci spesifik ditentukan oleh key usage extension dalam sertifikat X.509.

Subscriber's Public keys that are bound into certificates shall be certified for use in authenticating, signing or encryption, but not all, except as specified by IDI CA. The use of a specific key is determined by the key usage extension in the X.509 certificate.

Kunci PSrE IDI digunakan untuk penandatangan sertifikat dan CRL.

IDI CA keys are used for certificate signing and CRL signing.

6.2. Private Key Protection and Cryptographic Module Engineering Controls / Kendali Kunci Private dan Kendali Teknis Modul Kriptografi

6.2.1. Cryptographic Module Standards and Controls / Kendali dan Standar Modul Kriptografi

PSrE menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 untuk operasional PSrE.	CAs use a FIPS 140-2 validated hardware cryptographic module for CA Operation.

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

Semua kunci privat PSrE harus diakses melalui kendali multi-personil seperti yang ditentukan pada Bagian 5.2.2 (Sejumlah orang dibutuhkan dalam setiap tugas) dari CP ini dan CPS yang berlaku.	All CA private keys shall be accessed through multi-person control as specified in Section 5.2.2 (Number of Persons Required Per Task) of this CP and the applicable CPS.

6.2.3. Private Key Escrow / Penitipan Kunci Privat Kunci

Kunci privat PSrE IDI tidak boleh pernah dititipkan (escrow).	IDI CA private keys shall never be escrowed.

6.2.4. Private Key Backup / Backup Kunci Privat

Kunci privat PSrE harus di-backup di bawah kendali multi-pihak yang sama dengan kunci tanda tangan asli. Paling tidak satu salinan dari kunci privat harus disimpan secara aman. Semua salinan kunci privat PSrE harus dilindungi dengan cara yang sama dengan aslinya.	CA's private key shall be backed up under the same multiparty control as the original key. At least one copy of the private key shall be stored securely. All copies of the CA private key shall be accounted for and protected in the same manner as the original.
Pemilik dapat memilih untuk melakukan backup kunci mereka, tapi backup kunci harus berada di bawah kendali Pemilik.	Subscribers may choose to backup their keys, but must be held under the Subscriber's control.

6.2.5. Private Key Archival / Pengarsipan Kunci Privat

Kunci privat PSrE tidak boleh diarsipkan.	CA private keys shall not be archived.

6.2.6. Private Key Transfer into or from a Cryptographic Module / Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi

Kunci privat PSrE boleh diekspor dari modul kriptografis hanya untuk melaksanakan prosedur backup kunci PSrE. Kunci privat PSrE tidak pernah sekalipun boleh berada dalam bentuk *plaintext*di luar modul kriptografis.	CA private keys may be exported from the cryptographic module only to perform CA key backup procedure. At no time shall the CA private key exist in plaintext outside the cryptographic module.

Bila sebuah kunci privat akan dipindahkan dari satu modul kriptografis ke yang lain, kunci privat harus dienkripsi selama pemindahan. Token yang dipakai untuk mengenkripsi kunci privat harus dilindungi dengan tingkat keamanan yang sama dengan kunci privat.

If a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport. Transport keys used to encrypt private keys shall be handled in the same way as the private key.

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

Kunci Privat PSrE harus disimpan pada modul kriptografis FIPS 140-2, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

CA Private Keys shall be stored on FIPS 140-2 cryptographic module, in encrypted form and password-protected.

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

Aktivasi operasi kunci privat PSrE dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak seperti yang dinyatakan dalam bagian 5.2.2.

Activation of CA's private key operations is performed by authorized person and requires multiparty control as specified in Section 5.2.2.

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

Setelah dipakai, modul kriptografis harus dinonaktifkan oleh personil yang berwenang, mis., melalui prosedur logout manual, atau secara otomatis setelah suatu selang waktu ketidakaktifan sebagaimana didefinisikan dalam CPS yang berlaku.

After use, the cryptographic module shall be deactivated by authorized person, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.

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

Ketika kunci privat PSrE tidak diperlukan lagi, para individu dalam peran terpercaya harus menghapus kunci privat dari Modul Kriptografis dan backupnya dengan menimpa kunci privat atau menginisialisasi modul dengan fungsi *factory reset*dari Modul Kriptografi.

When CA private signature keys are no longer needed, individuals in trusted roles shall delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with the factory reset function of Cryptographic Module.

Kejadian penghancuran kunci privat PSrE harus dicatat ke dalam barang bukti sesuai dengan bagian 5.4.

The event of destroying CA's private key must be recorded into evidence under section 5.4.

6.2.11. Cryptographic Module Rating / Pemeringkatan Modul Kriptografis

Seperti diuraikan dalam bagian 6.2.1.	As described in section 6.2.1.

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

6.3.1. Public Key Archival / Pengarsipan Kunci Publik

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.	The Public Key is archived as part of the Certificate archival.

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

Periode operasional pasangan kunci didefinisikan oleh periode operasional dari sertifikat digital yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai sepuluh (10) tahun bagi PSrE IDI, dan maksimal dua (2) tahun untuk sertifikat Pengguna.. Periode operasional harus didefinisikan menurut ukuran kunci dan perkembangan teknologi terkini di bidang kriptografi, sehingga tingkat terbaik untuk keamanan dan efisiensi penggunaan terjamin.	The key pair operational period is defined by the operational period of the corresponding digital certificate. The maximum operational period of the keys is defined as ten (10) years for ID CA, and maximum two (2) years for Subscriber certificates. The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography, so that the best level of security and efficiency of use is guaranteed.

6.4. Activation Data / Data Aktivasi

6.4.1. Activation Data Generation and Installation / Pembuatan dan Instalasi Data Aktivasi

Aktivasi data harus dibuat secara otomatis oleh HSM yang cocok dan dikirimkan ke *shareholder*, dimana *shareholder*tersebut haruslah orang yang memiliki Peran Terpercaya.	Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder, of whom the shareholder must be in a trusted role.

6.4.2. Activation Data Protection / Aktivasi Perlindungan Data

Aktivasi data PSrE harus dilindungi dari pengungkapan kerahasiaan, perlindungan diberikan melalui kombinasi antara kriptografi dan mekanisme kendali akses fisik. Aktivasi data PSrE harus disimpan dalam token fisik.	CA activation data must be protected from disclosure through a combination of cryptographic and physical access control mechanisms. CA activation data must be stored in a physical token.

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

Tidak ditentukan.

No stipulation.

6.5. Computer Security Controls / Kendali Keamanan Komputer

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

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

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

Ketika peralatan PSrE diwadahi dalam suatu platform terevaluasi dalam mendukung persyaratan penjaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak, sistem operasi) harus, kalau mungkin, beroperasi dalam konfigurasi terevaluasi. Paling tidak, platform tersebut harus memakai versi yang sama dari sistem operasi komputer dengan yang menerima peringkat evaluasi.
Sistem komputer PSrE harus dikonfigurasi dengan akun yang diperlukan dan layanan jaringan yang minimum.

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Require use of cryptography for communication session and database security
- Provide self-protection for the operating system

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

The CA-computer system shall be configured with minimum of the required accounts, network services.

6.5.2. Computer Security Rating / Peringkat Keamanan Komputer

Tidak ditentukan.	No stipulation.

6.6. Life Cycle Technical Controls / Kendali Teknis Siklus Hidup

6.6.1. System Development Controls / Kendali Pengembangan Sistem

Tidak ditentukan.	No stipulation.

6.6.2. Security Management Controls / Kendali Manajemen Keamanan

Konfigurasi dari sistem PSrE IDI serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen PSrE IDI. Ada mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi milik PSrE IDI.	The configuration of the IDI CA system as well as any modifications and upgrades are documented and controlled by the IDI CA management. There is a mechanism for detecting unauthorized modification to the IDI CA software or configuration.

6.6.3. Life Cycle Security Controls / Kendali Keamanan Siklus Hidup

PSrE IDI melakukan pengawasan terhadap kebutuhan skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak yang telah dievaluasi dan disertifikasi.	IDI CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

6.7. Network Security Controls / Kendali Keamanan Jaringan

PSrE IDI akan menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa mereka terjaga dari *denial of service* dan serangan intrusi. Langkah-langkah sedemikian harus termasuk penggunaan firewall dan router penyaring. Port jaringan dan layanan yang tidak dipakai harus dimatikan. Setiap perangkat lunak jaringan yang ada harus perlu bagi berfungsinya PSrE.	IDI CA will employ appropriate network security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the CA.

6.8. Time-Stamping / Stempel Waktu

Semua komponen PSrE secara berkala disinkronisasikan dengan sebuah layanan waktu, seperti contohnya layanan *atomic clock* atau Network Time Protocol (NTP).	All CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such

Sebuah otoritas khusus untuk menyediakan waktu yang terpercaya juga bisa digunakan jika perlu, misalnya dengan membentuk sebuah otoritas *timestamp* tersendiri. Waktu yang didapat dari layanan waktu diatas akan digunakan untuk menentukan waktu pada saat:

- Validitas waktu permulaan untuk sebuah sertifikat PSrE
- Pencabutan sertifikat PSrE
- Pembaruan CRL, dan
- Penerbitan sertifikat pemilik dan entitas
- Prosedur elektronik atau manual bisa digunakan untuk tetap mempertahankan akurasi waktu pada sistem. Pencocokan jam merupakan sebuah aktivitas yang bisa untuk diaudit.

as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.
- Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

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

7.1. Certificate Profile / Profil Sertifikat

Profile sertifikat mengikuti standar RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”. PSrE harus melakukan review terhadap profil sertifikat secara berkala minimal setahun sekal2.	A certificate profile according to RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” is used. CA shall review certificate profile periodically at least once a year.

7.1.1. Version Number(s) / Nomor Versi

PSrE seharusnya menerbitkan sertifikat X.509 v3 (mengisi versi field dengan integer “2”).	The CA shall issue X.509 v3 certificates (populate version field with integer “2).

7.1.2. Certificate Extensions / Ekstensi Sertifikat

PSrE harus memakai ekstensi sertifikat standar yang mematuhi RFC 5280.	CAs shall use standard certificate extensions that comply with RFC 5280.

7.1.2.1. Key Usage / Key Usage

Sertifikat X.509 Versi 3 biasanya diisi sesuai dengan RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Field criticality dari ekstensi KeyUsage biasanya diisi TRUE.	X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. The criticality field of the KeyUsage extension is generally set to TRUE.

7.1.2.2. Certificate Policies Extension / Certificate Policies Extension

Ekstensi certificatePolicies dari Sertifikat X.509 Versi 3 diisi dengan identifier objek dari CP ini sesuai dengan bagian 7.1.6 dan dengan kualifier kebijakan yang ditentukan dalam bagian 7.1.8. Field criticality dari ekstensi ini harus diisi FALSE.	CertificatePolicies extension of X.509 Version 3 Certificates are populated with the object identifier of this CP in accordance with Section 7.1.6 and with policy qualifiers set forth in Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3. Basic Constraint / Basic Constraint

Ekstensi BasicConstraints Sertifikat X.509 Versi 3 harus memiliki field CA yang diisi TRUE. Ekstensi BasicConstraints Sertifikat Pengguna Akhir harus memiliki field CA yang diisi FALSE. Field criticality dari ekstensi ini harus diisi TRUE untuk Sertifikat CA, tapi boleh diisi TRUE atau FALSE bagi Sertifikat Pemilik.	X.509 Version 3 CA Certificates BasicConstraints extension shall have the CA field set to TRUE. Subscriber Certificates BasicConstraints extension shall have the CA field set to FALSE. The criticality field of this extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

7.1.2.4. Extended Key Usage / Extended Key Usage

Secara baku, ExtendedKeyUsage diatur sebagai suatu ekstensi non-kritikal.	By default, ExtendedKeyUsage is set as a non-critical extension.
Sertifikat CA dapat memuat ekstensi ExtendedKeyUsage sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang mereka terbitkan.	CA Certificates may include the ExtendedKeyUsage extension as a form of technical constraint on the usage of certificates that they issue.
Semua sertifikat Pemilik harus mengandung sebuah ekstensi *extended key usage*untuk tujuan bahwa sertifikat tersebut telah diterbitkan untuk end-user, dan tidak boleh memuat nilai anyEKU.	All End-user Subscriber certificates shall contain an extended key usage extension for the purpose that the certificate was issued to the end user, and shall not contain the anyEKU value

7.1.2.5. CRL Distribution Points / CRL Distribution Points

Sertifikat X.509 Versi 3 diisi dengan suatu ektensi cRLDistributionPoints yang memuat URL dari lokasi dimana Pihak Pengandal dapat memperoleh suatu CRL untuk memeriksa status Sertifikat. Field criticality dari ekstensi ini harus diisi FALSE.	X.509 Version 3 Certificates are populated with a cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the Certificate's status. The criticality field of this extension shall be set to FALSE.
URL harus patuh dengan persyaratan Mozilla yang tidak menyertakan protokol LDAP, dan mungkin muncul beberapa kali di dalam suatu ektensi cRLDistributionPoints.	URLs shall comply with Mozilla requirements to exclude the LDAP protocol, and may appear multiple times within a cRLDistributionPoints extension.

7.1.2.6. Authority Key Identifier / Authority Key Identifier

Sertifikat X.509 Versi 3 biasanya diisi dengan ekstensi authorityKeyIdentifier. Metode untuk menghasilkan keyIdentifier yang berbasis pada kunci publik dari PSrE Penerbit, harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.	X.509 Version 3 Certificates are generally populated with an authorityKeyIdentifier extension The method for generating the keyIdentifier based on the public key of the CA issuing the Certificate shall be calculated in accordance with one of the

Field criticality dari ekstensi ini harus diisi FALSE.	methods described in RFC 5280. The criticality field of this extension shall be set to FALSE.

7.1.2.7. Subject Key Identifier / Subject Key Identifier

Bila ada dalam Sertifikat X.509 Versi 3, field criticality dari ekstensi ini harus diisi dengan FALSE dan metode untuk menghasilkan keyIdentifier yang berbasis pada kunci publik Subyek Sertifikat harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.	If present in X.509 Version 3 Certificates, the criticality field of this extension shall be set to FALSE and the method for generating the keyIdentifier based on the public key of the Subject of the Certificate shall be calculated in accordance with one of the methods described in RFC 5280

7.1.3. Algorithm Object Identifiers / Identifier Objek Algoritme

OID standar X.509v3 harus digunakan.	X.509v3 standard OIDs shall be used.
Algoritma harus berupa enkripsi RSA untuk subject key dan SHA256 dengan enkripsi RSA atau SHA384 dengan enkripsi RSA untuk tanda tangan sertifikat.	Algorithm shall be RSA encryption for the subject key and SHA256 with RSA encryption or SHA384 with RSA encryption for the certificate signature.

7.1.4. Name Forms / Format Nama

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1.	As per the naming conventions and constraints listed in section 3.1.

7.1.5. Name Constraints / Batasan Nama

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1.	As per the naming conventions and constraints listed in section 3.1.

7.1.6. Certificate Policy Object Identifier / Identifier Objek Kebijakan Sertifikat

Sertifikat yang diterbitkan di bawah CP ini harus menggunakan nomor OID Joint-ISO-ITU yang mengacu pada PSrE yang benar dan sesuai dengan Certificate Policy.	Certificates issued under this CP shall use the Joint-ISO-ITU OID number that points to the correct CA as well as Certificate Policy.

7.1.7. Usage of Policy Constraints Extension / Penggunaan Ekstensi Kendala Kebijakan

Tidak ditentukan	No stipulation

7.1.8. Policy Qualifiers Syntax and Semantics / Sintaks dan Semantik Kualifier Kebijakan

Tidak ditentukan	No stipulation

7.1.9. Processing Semantics for the Critical Certificate Policies Extension / Semantik Pemrosesan bagi Ekstensi Kebijakan Sertifikat Kritis

Tidak ditentukan	No stipulation

7.2. CRL Profile / Profil CRL

7.2.1. Version Number(s) / Nomor Versi

PSrE yang beroperasi di bawah CP ini harus menerbitkan CRL X.509 versi 2.	CAs operating under this CP shall issue X.509 version 2 CRLs.

7.2.2. CRL and CRL Entry Extensions / CRL dan Ekstensi Entri CRL

PSrE yang beroperasi di bawah CP ini harus menggunakan CRL dan CRL entry extension RFC 5280.	CAs operating under this CP shall use RFC 5280 CRL and CRL entry extension.

7.3. OCSP Profile / Profil OCSP

PSrE IDI bisa mengoperasikan sebuah responder Online Certificate Status Protocol (OCSP) yang sesuai dengan RFC 6960 atau RFC 5019.	IDI CAs may operate an Online Certificate Status Protocol (OCSP) responder in compliance with RFC 6960 or RFC 5019.

7.3.1. Version Number(s) / Nomor Versi

PSrE IDI harus menerbitkan respon OCSP versi 1.	IDI CAs shall issue OCSP responses Version 1.

7.3.2. OCSP Extensions / Ekstensi OCSP

Tidak ditentukan.	No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS / AUDIT KEPATUHAN DAN ASESMEN LAIN

PSrE IDI akan menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika no 11/2018.

IDI CA will undergo a compliance audit and submit reports periodically as required by Indonesia Ministry of Communication and Informatics Regulation No 11/2018

Semua kebijakan yang terdapat dalam CP ini mencakup semua bagian yang relevan dari standar IKP yang saat ini diterapkan untuk berbagai macam industri IKP vertikal, dimana industri -industri tersebut membutuhkan PSrE agar bisa beroperasi. PSrE diaudit untuk kepatuhan kepada kebutuhan teknis Adobe Approved Trust List 2.0 atau yang lebih baru.

The policies within this CP encompass all relevant portions of currently applicable PKI standards for the various vertical PKI industries in which CAs are required to operate. CAs are audited for compliance to Adobe Approved Trust List Technical Requirement 2.0 or later.

8.1. Frequency or Circumstances of Assessment / Frekuensi atau Keadaan Asesmen

PSrE IDI menjalani audit kepatuhan berkala terhadap skema yang telah ditetapkan minimal sekali setahun, dan juga setiap setelah terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan.

IDI CA will undergo a compliance audit of the currently established scheme, both on a regular basis as well as each time after undergoing significant changes to the established procedures and techniques.

PSrE IDI harus menjalani audit kepatuhan dan menyampaikan laporan berkala minimal sekali setahun yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika no 11/2018.

IDI CA will undergo a compliance audit and submit periodical reports at least once a year as required by Indonesia Ministry of Communication and Informatics Regulation No 11/2018.

8.2. Identity/Qualifications of Assessor / Identitas/Kualifikasi Asesor

Auditor harus menunjukkan kompetensi pada bidang audit kepatuhan dan harus benar-benar memahami persyaratan CPS ini. Auditor kepatuhan harus melakukan audit kepatuhan sebagai tanggung jawab utama.

Auditors shall possess sufficient skills on compliance audit, and shall thoroughly understand the requirements in this CPS. Compliance auditors shall perform compliance audits as their main responsibility.

Auditor kepatuhan harus memiliki kualifikasi sebagai berikut:

a. Auditor harus memiliki tim asesmen independen yang *qualified*.

b. Auditor harus memiliki pengetahuan yang cukup tentang tanda tangan digital, sertifikat

Compliance auditors must possess these qualifications:

a. Auditors shall have a qualified, independent assessment team

b. Auditors shall have a sufficient knowledge on digital signatures,

digital, X.509 versi 3 PKI Certificate Policy and Certification Practices Framework, UU ITE (UU No 11/2008 and UU No 19/2016), PP PSTE (PP 71/2019), Peraturan Menteri Komunikasi dan Informatika tentang Penyelenggaraan Sertifikasi Elektronik (PM Kominfo No 11/2018).	digital certificate, X.509 PKI Certificate Policy and Certificate Practice Framework, Indonesian Law of Electronic Information and Transactions (UU No 11/2008 and UU No 19/2016), Indonesian Government Regulation on Electronic System and Transaction Operations (PP 71/2019), and Indonesia Ministry of Communication and Informatics Regulation on Certification Authority Operations (PM Kominfo 11/2018)
c. memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;	c. Auditors shall have an adequate skills on information security audit, information security device and technique audit, as well as familiarity with PKI technology
d. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah	d. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme.
e. 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.	e. Auditors shall master a set of certain skills, competency testing, and quality assurance such as peer review, standards regarding accurate staff assigning, and involvement and requirements for higher professional education.

8.3. Assessor's Relationship to Assessed Entity / Hubungan Asesor ke Entitas yang Dinilai

PSrE IDI akan memilih auditor / asesor yang independen dari PSrE.	IDI CA will choose an auditor/assessor who is completely independent from the CA.

8.4. Topics Covered by Assessment / Topik yang Dicakup oleh Asesmen

Audit yang dilaksanakan harus memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema audit akan	The audit must meet the requirements of the audit scheme under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme will be

berlaku pada tahun berikutnya setelah PSrE mengadopsi skema yang terbaru.

applicable to the CA in the year following the adoption of the updated scheme.

8.5. Actions Taken as a Result of Deficiency / Tindakan yang Diambil sebagai Hasil dari Kekurangan

Ketika auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana PSrE dirancang atau dioperasikan atau dipelihara terhadap persyaratan CP ini, atau CPS yang berlaku, tindakan berikut harus dilakukan:

a. Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.

b. Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian harus menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CP dan kontrak masing-masing, kemudian melanjutkan untuk membuat. pemberitahuan tersebut dan melakukan tindakan tersebut tanpa penundaan

When the compliance auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, or the applicable CPS, the following actions shall be performed:

a. The compliance auditor shall notify Kominfo of the discrepancy.

b. The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the respective contracts, and then proceed to make such notifications and take such actions without delay.

.

8.6. Communication of Results / Komunikasi Hasil

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada PA sebagaimana diatur dalam bagian 8.1. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam asesmen. Selain itu, hasilnya harus dikomunikasikan seperti yang ditetapkan pada bagian 8.5 di atas.

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, shall be provided to the PA as set forth in section 8.1. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, the results shall be communicated as set forth in 8.5 above.

8.7. Internal Audit / Audit Internal

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

Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.

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

9.1. Fees / Biaya

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

PSrE IDI dapat mengenakan biaya administrasi dalam menerbitkan atau memperbaharui Sertifikat termasuk dalam hal penerbitan ulang sertifikat. Dalam hal ini, syarat dan ketentuan terkait biaya akan disampaikan secara jelas kepada para Pemohon sertifikat.

IDI CA may charge fees for Certificate issuance or renewal. CAs may also charge for re-issuance or re-key. Fees and any associated terms and conditions should be made clear to Applicants.

9.1.2. Certificate Access Fees / Biaya Pengaksesan Sertifikat

PSrE IDI dapat mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan.

IDI CA may charge for access to repositories which store issued Certificates.

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

PSrE IDI dapat mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau pencabutan sertifikat.

IDI CA may charge additional fees to Subscribers for accessing revocation or information status.

9.1.4. Fees for Other Services / Biaya Layanan Lainnya

PSrE IDI dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya.

IDI CA may charge for other additional services.

9.1.5. Refund Policy / Kebijakan Pengembalian Sertifikat

PSrE IDI dapat menyediakan kebijakan pengembalian sertifikat kepada para Pemilik. Bagi pemilik sertifikat yang mengajukan permohonan kebijakan pengembalian, semua sertifikatnya dicabut.

IDI CA may offer a refund policy to Subscribers. Subscribers who choose to invoke the refund policy should have all issued Certificates revoked.

9.2. Financial Responsibility / Tanggung Jawab Keuangan

9.2.1. Insurance Coverage / Cakupan Asuransi

PSrE IDI akan mematuhi persyaratan PM Kominfo No 11/2018 Pasal 12 huruf h berikut segala perubahannya yang terkait.	IDI CA will comply with Article 12 letter h of Communication and Informatics Minister Regulation No 11/2018 along with all of the relevant revisions.

9.2.2. Other Assets / Aset Lainnya

Tidak ada ketentuan.	No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities / Jaminan Asuransi atau Garansi untuk Entitas Akhir

PSrE IDI akan menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik sertifikat.	IDI CA will offer an insurance or warranty policy to Subscribers.

9.3. Confidentiality of Business Information / Kerahasiaan Informasi Bisnis

9.3.1. Scope of Confidential Information / Cakupan Informasi Rahasia

PSrE IDI akan memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Yang termasuk dalam kategori informasi rahasia antara lain: ● Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4; ● Rekam jejak audit (*audit logs*) dari sistem PSrE dan RA; ● Data aktivasi pada saat pengaktifan Kunci Privat PSrE sebagaimana dijabarkan pada Bagian 6.4; ● Dokumentasi bisnis proses PSrE termasuk dokumen Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); dan ● Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0.	The following items are classified as being confidential information and therefore are subject to reasonable care and attention of IDI CA: ● Personal Information as detailed in Section 9.4; ● Audit logs from CA and RA systems; ● Activation data used to active CA Private Keys as detailed in Section 6.4; ● CAs business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and ● Audit Reports from an independent auditor as detailed in Section 8.0.

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

Informasi yang tidak dikategorikan rahasia dalam dokumen CP dianggap informasi publik.	Any information not defined as confidential within the CP shall be deemed public.
Sertifikat dan informasi mengenai status sertifikat termasuk kategori informasi publik.	Certificate status information and Certificates themselves are deemed public.

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

PSrE akan melindungi informasi rahasia. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:	CA will protect confidential information. CA shall enforce protection of confidential information through the following mechanism but not limited to:
• Pelatihan atau peningkatan *awareness*	• training,
• Perjanjian kontrak pegawai	• contracts with employees,
• NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai outsource, dan rekanan.	• NDA with employees, outsource and contractors.

9.4. Privacy of Personal Information / Perlindungan Data Pribadi

9.4.1. Privacy Plan / Rencana Perlindungan Data Pribadi

PSrE IDI akan melindungi informasi pribadi dalam kaitan dengan “Kebijakan Informasi Pribadi“ yang dipublikasikan sesuai dengan ketentuan repositori pada Bagian 2.1.	IDI CA will protect personal information in accordance with a Privacy Policy published on a suitable Repository along with this CP. Section 2.1.

9.4.2. Information Treated as Private / Informasi yang Dianggap Pribadi

PSrE IDI akan melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan Pemilik baik terhadap PSrE maupun RA. Arsip yang dikelola oleh PSrE tidak boleh dirilis kecuali yang diizinkan pada Bagian 9.4.1.	IDI CA will protect all subscribers personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs shall not be released except as allowed by Section 9.4.1.

9.4.3. Information not Deemed Private / Informasi tidak Dianggap Pribadi

Informasi yang termasuk dalam Bagian 7 (Sertifikat, CRL, Profil OCSP) dari CP ini tidak termasuk dalam Bagian 9.4.2.

Information included in Section 7 (Certificate, CRL and OCSP Profiles) of this CP is not subject to protection outlined in Section 9.4.2 (Information Treated as Private) above.

9.4.4. Responsibility to Protect Private Information / Tanggung Jawab Melindungi Informasi Pribadi

PSrE IDI bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan "Perlindungan Data Pribadi" secara aman. Informasi yang disimpan dapat berbentuk digital maupun kertas. Backup informasi pribadi harus dienkripsi setiap akan dipindahkan ke media backup.

IDI CA is responsible for securely storing private information in accordance with a published privacy policy document and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media.

9.4.5. Notice and Consent to use Private Information / Catatan dan Persetujuan untuk memakai Informasi Pribadi

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. PSrE harus mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam *Subscriber Agreement*. *Subscriber Agreement* juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh PSrE.

Personal information obtained from Applicants during the application and enrolment process is deemed private and permission is required from the Applicant to allow the use of such information. CAs should incorporate the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by the CA.

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

PSrE IDI tidak akan membuka informasi pribadi kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, aturan dan peraturan pemerintah, atau perintah pengadilan.

IDI CA will not disclose private information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7. Other Information Disclosure Circumstances

Tidak ada ketentuan.	No stipulation.

9.5. Intellectual Property Rights / Hak atas Kekayaan Intelektual

Semua hak kekayaan intelektual PSrE IDI termasuk semua merek dagang dan hak cipta dari semua dokumen PSrE tetap menjadi milik tunggal dari PSrE IDI.	IDI CA's Intellectual Property Rights including trademarks, copyright and all CA documents remain as sole property of IDI CA.

9.6. Representations and Warranties / Pernyataan dan Jaminan

9.6.1. CA Representations and Warranties / Pernyataan dan Jaminan PSrE

PSrE IDI menyatakan dan menjamin, sejauh yang ditentukan dalam CP, bahwa:	IDI CA represents and warrants, to the extent specified in this CP, that:
● PSrE mematuhi ketentuan yang diatur dalam CP ini,	● CA complies, in all material aspects, with the CP,
● PSrE menerbitkan dan memperbarui CRL secara berkala,	● CA publishes and updates CRL on a regular basis,
● Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP ini,	● All certificates issued will meet the minimum requirements and verified in accordance with this CP and,
● PSrE akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.	● CA will display information that can be accessed publicly through its repositories.

9.6.2. RA Representations and Warranties / Pernyataan dan Jaminan RA

RA menyatakan dan menjamin, sejauh yang ditentukan dalam CP, bahwa	RAs warrant that:
● Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat,	● There are no fallacy on Certificate that have been known or came from the entity who gives an acknowledgement on Certificate application or Certificate issuance
● Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat,	● 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.

- PSrE mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP dan dituangkan dalam kontrak.

- CA required all RAs to guarantee all registration activity that have been done by RAs comply with CP and stated at the contract.

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

Pemilik Sertifikat menjamin bahwa:

- Setiap sertifikat digital yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah merupakan tanda tangan digital pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kedaluwarsa dan telah dicabut) saat tanda tangan digital dibuat;

- Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;

- Sudah melakukan review terhadap informasi dari sertifikat.

- Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;

- Sertifikat Digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CP ini;

- Segera:

  (a) melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat; dan

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,

- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key,

- Have thoroughly reviewed the certificate information

- All information supplied by the Subscriber and contained in the Certificate is true,

- The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP and the applicable CPS, and

- Promptly:

(a) request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;

(b) mengajukan permohonan untuk melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam sertifikat tersebut

(b) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

(c) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut;

(c) stop using the private key whose public key is listed in a digital certificate after the certificate is revoked;

- Akan menanggapi instruksi PSrE terkait *compromise* atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;

- Will respond to CAs instructions regarding compromise or digital certificates misuses within forty eight (48) hours,

- menyetujui dan menerima bahwa PSrE diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika PSrE menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware;*

- Acknowledges and accepts that CA is entitled to revoke the Certificate immediately if the subscriber violates the terms of the Subscriber Agreement or Terms of Use or if CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, and

- pengguna akhir dan bukan merupakan PSrE, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat Digital untuk tujuan penandatangan sertifikat digital PSrE lain

- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

9.6.4. Relying Party Representations and Warranties / Pernyataan dan Perjanjian Pihak Pengandal

Pihak yang mengandalkan Sertifikat PSrE IDI menjamin bahwa:

IDI CA's Certificate relying party guarantee that:

- Memiliki kemampuan teknis untuk menggunakan sertifikat,

- Have the technical capability to use certificates,

- apabila perwakilan dari Pihak Pengandal menggunakan suatu

- If the representative from the Relying Party uses a certificate issued by IDI

sertifikat yang diterbitkan oleh PSrE IDI, Pihak 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,	CA, the relying party should verify the information contained in the certificate before use and carry all the consequences that happened if the relying party fails to apply it.
● Melaporkan langsung kepada RA yang berwenang, jika Pihak Pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat	● Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised,
● mewajibkan Pihak Pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pihak Pengandal yang ada pada CP ini,	● Required relying party to acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the Certificate, that they are fully responsible for deciding to rely on the information or not, and they will carry the legal consequences from the failure to fulfill the obligation of the Relying Party as mentioned in the CP,
● Harus mematuhi ketentuan yang ditetapkan di CP dan perjanjian lain yang terkait.	● must compliance with the provisions of this CP and related agreements.

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

Tidak ditentukan.	No stipulation.

9.7. Disclaimers of Warranties / Pelepasan Jaminan

Kewajiban ganti rugi PSrE akan ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.	CA's indemnification obligations will be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.

9.8. Limitations of Liability / Pembatasan Tanggung Jawab

9.8.1. CA Limitations of Liability / Pembatasan Tanggung Jawab PSrE

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

- semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CP, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
- semua kerusakan yang disebabkan oleh force majeure,
- semua kerusakan yang disebabkan oleh malware (seperti virus atau Trojans) diluar perangkat PSrE.

IDI CA is not responsible for inappropriate use of the Certificate, including:

- all damage caused by the misuse of certificates or key pairs beside the proper use that have been defined in CP, subscribers agreement, or all provision which have been mentioned in The Certificate,
- all damage caused by the force majeure condition,
- all damage caused by the Malware (i.e virus or Trojan) outside CAs devices.

9.8.2. RA Limitation of Liability/ Pembatasan Tanggung Jawab RA

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan PSrE. Secara khusus, RA bertanggung jawab atas pendaftaran pemilik sertifikat.

The cap on Registration Agent's liability is specified in the frame contract between Registration Agent and CAs. In particular, the Registration Agent is liable for the registration of subscribers.

9.9. Indemnities / Ganti Rugi

9.9.1. Indemnification by an CAs / Ganti Rugi oleh PSrE

Kewajiban ganti rugi PSrE IDI akan ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

IDI CA's indemnification obligations will be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.

9.9.2. Indemnification by Subscriber / Ganti Rugi oleh Pemilik Sertifikat

PSrE IDI akan menyertakan persyaratan ganti rugi untuk Pemilik Sertifikat dalam CPS dan dalam Kontrak Berlangganannya.

IDI CA will include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3. Indemnification by Relying Parties/ Ganti Rugi oleh Pihak Pengandal

PSrE IDI akan menyertakan persyaratan ganti rugi untuk Pihak Pengandal dalam CPS.	IDI CA will include its indemnification requirements for Relying Parties in its CPS.

9.10. Term and Termination / Syarat dan Pengakhiran

9.10.1. Term / Syarat

CP ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh PSrE melalui laman atau repositorinya.	Notified changes of this CP are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.2. Termination / Pengakhiran

Perubahan CP ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 hari setelah dipublikasikan.	Notified changes of this CP are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.3. Effect of Termination and Survival / Efek Pengakhiran dan Keberlangsungan

PSrE IDI akan mengkomunikasikan kondisi akibat dari penghentian CP dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui laman atau repositori.	IDI CA will communicate the conditions and effect of this CP's termination on its website or Repository.

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

PSrE IDI menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara digital, dalam bentuk kertas, atau email bersertifikat. PSrE memberikan tanda terima yang valid sebagai bukti bagi pengirim. PSrE harus memberi tanggapan paling lama dua puluh (20) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke PSrE harus dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CP.	IDI CA provides communication media for related parties through electronics document, electronic mail, telephone both digitally signed, in paper form or certified email. CA provides a valid receipt as proof for the sender. CAs must respond for a maximum of twenty (20) working days through the same communication media. Communications made to CAs must be addressed in accordance with those listed in section 1.5.2 of CP.

9.12. Amendments / Amandemen

9.12.1. Procedure for Amendment / Prosedur untuk Amandemen

PSrE IDI akan menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CP ini termasuk juga keterangan waktu ketika CP efektif berlaku. Amandemen CP dilakukan sesuai dengan prosedur persetujuan CP/CPS.

IDI CA will post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted. CP amendments are carried in accordance with the CP/CPS approval procedure.

9.12.2. Notification Mechanism and Period / Periode dan Mekanisme Pemberitahuan

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

IDI CA will post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted. When there is a change, CP must be published no later than 7 (seven) working days from the date it was signed.

9.12.3. Circumstances Under Which OID Must be Changed / Keadaan Dimana OID Harus Diubah

Jika Policy Authority memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, PSrE IDI akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

In case of the PA has the view that it is necessary to change the involved OID numbers, IDI CA will change the OID and enforce the new policy using the new OID.

9.13. Dispute Resolution Provisions / Provisi Penyelesaian Ketidaksepahaman / Ketentuan Penyelesaian Sengketa

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CP ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara PSrE dengan pemilik sertifikat.

In case of dispute or controversy related performance, execution or the interpretation of the CP, all parties will try to reach a peaceful settlement. The official provisions of the dispute are part of the contract agreed upon between The CAs and the certificate owner.

9.14. Governing Law / Hukum yang Mengatur

CP ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat PSrE ataupun produk/ layanan lainnya.

This CP is governed, construed and interpreted in accordance with the laws of Indonesia. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Certificates or other products and services.

Hukum Indonesia juga tetap berlaku dalam hal sertifikat PSrE IDI dipakai atau dirujuk baik secara eksplisit atau implisit untuk kebutuhan komersil atau kontraktual di negara lain terkait dengan produk atau layanan dari PSrE ini.

The laws of Indonesia also apply to all IDI CA's commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to CAs products and services.

Para pihak, termasuk partners CA, Pemilik, Pihak Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

Each party, including CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Indonesia

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

PSrE IDI mematuhi hukum yang berlaku di Indonesia. Ekspor berbagai jenis perangkat lunak tertentu yang digunakan dalam berberapa produk dan layanan manajemen Sertifikat publik PSrE dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang berwenang. Para Pihak (termasuk PSrE, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi undang-undang dan regulasi ekspor yang berlaku di Indonesia.

IDI CA complies with applicable laws of Indonesia. Export of certain types of software used in certain CAs public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including CA, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Indonesia.

9.16. Miscellaneous Provisions / Ketentuan yang belum diatur

9.16.1. Entire Agreement / Seluruh Perjanjian

Tidak ada ketentuan.

No stipulation.

9.16.2. Assignment / Pengalihan Hak

Entitas yang beroperasi dibawah CP ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari PSrE.

Entities operating under this CP must not assign their rights or obligations without the prior consent of CAs.

9.16.3. Severability / Keterpisahan

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

If any provision of this CP, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP will be interpreted in such manner as to affect the original intention of the parties. Each and every provision of this CP that provides for a limitation of liability, is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) / Penegakan Hukum (Biaya Pengacara dan Pengalihan Hak-hak)

PSrE IDI 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 dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak PSrE untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CP ini. Segala hal terkait pelepasan hak dalam pengadilan harus disampaikan secara tertulis dan ditandatangani oleh PSrE.

IDI CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. CA's failure to enforce a provision of this CP does not waive CA's right to enforce the same provisions later or right to enforce any other provisions of this CP. To be effective any waivers must be in writing and signed by CA.

9.16.5. Force Majeure / Keadaan Memaksa

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

IDI CA shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, power and failure of telecommunications lines, lack of Internet access, sabotage, terrorism, and governmental action or any unforeseeable events or situations.

PSrE IDI akan menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas PSrE.	IDI CA will be obliged to provide BCP and DRP with reasonable control in line with the capabilities of the CA.

9.17. Other Provisions / Provisi Lain

Tidak ada ketentuan	No stipulation.

APPENDIX

Table of Acronyms and Definition / Tabel Akronim dan Kepanjangan

Akronim/Acronym	Definition / Definisi
PSrE CA	Penyelenggara Sertifikasi Elektronik Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
EV	Extended Validation
FIPS	Federal Information Processing Standards (US Government)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
IKP PKI	Infrastruktur Kunci Publik Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comment Request
VA	Validation Authority

Term/ Istilah	Definition / Definisi
Pemohon Applicant	Individu 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	Individu 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 IDI IDI CA Certificate	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PSrE IDI untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh PSrE IDI. The self-signed Certificate issued by IDI CA to identify itself and to facilitate verification of Certificates issued to itself.
Sertifikat Pemilik Subscriber's Certificate	Sertifikat yang dikeluarkan oleh PSrE BerinIDIduk The Certificate issued by IDI CA
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.
Certification Practice Statement 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 IDI 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 digital yang berisi informasi yang ditentukan dalam Pedoman EV dan yang telah divalidasi sesuai dengan Pedoman tersebut. A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines.
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.
Key Compromise	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 Ceremony	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan, kunci privasinya ditransfer ke modul kriptografi, kunci privatnya dicadangkan, dan/atau kunci publiknya disertifikasi.
Key Generation Ceremony	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	A unique alphanumeric or numeric identifier yang terdaftar di bawah standar International Organization for Standardization untuk objek atau kelas objek tertentu.
Object Identifier	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	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	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.
Private Key	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	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.
Public Key	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 Keyand/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.