KOMINFO	Nomor	:	CP/20191230/v2.0
	Versi	:	2.0
	Tanggal	:	30 Desember 2019
	Hal	:	87 Halaman
	OID	:	2.16.360.1.1.1.2.1

Certificate Policy (CP)
Penyelenggara Sertifikasi Elektronik (PSrE)
Induk Indonesia

Certificate Policy (CP)
Root CA Indonesia

30 Desember 2019

Policy Authority

Mariam F. Barata

Lembar Catatan Review/Revisi

Tanggal	Rev	Uraian	Oleh
2 Agustus 2018	1.0	Initial Release	CA Employee
4 Desember 2019	2.0	Perubahan tentang: - Contact PA - Terjemahan bahasa inggris dan bahasa indonesia - Format pengisian atribut CN pada Sertifikat Elektronik - Latensi Maksimum untuk CRL - Penyesuaian level verifikasi dan penggunaan untuk masing-masing kelas sertifikat	CA Employee

TABLE OF CONTENTS

DAFTAR ISI

1. INTRODUCTION / PENGANTAR

Infrastruktur Kunci Publik (IKP) Indonesia adalah hirarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikasi Elektronik (PSrE) Induk. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk sesuai dengan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. PSrE dibawah PSrE Induk terdiri atas 2 (dua) jenis PSrE yaitu PSrE Instansi Penyelenggara Negara (PSrE Instansi) dan PSrE non-Instansi Penyelenggara Negara (PSrE non-Instansi). PSrE Instansi menerbitkan Sertifikat Elektronik (selanjutnya disebut Sertifikat) untuk pegawai Instansi (Government to Government dan Government to Government Employee) yang digunakan dalam rangka pelaksanaan jabatan dan/atau kewenangannya. PSrE non-Instansi menerbitkan Sertifikat selain yang diterbitkan oleh PSrE Instansi.

Dokumen Certificate Policy Penyelenggara Sertifikasi Induk Indonesia (CP PSrE Induk Indonesia) adalah kebijakan utama yang mengatur PSrE Induk. CP menetapkan persyaratan bisnis, hukum, dan teknis untuk menyetujui, menerbitkan, mengelola, menggunakan, mencabut, dan memperbarui Sertifikat dalam IKP Indonesia dan menyediakan layanan kepercayaan terkait untuk semua partisipan IKP Indonesia. Persyaratan ini melindungi keamanan dan integritas IKP Indonesia dan terdiri atas seperangkat aturan yang berlaku secara konsisten di seluruh Indonesia, sehingga memberikan jaminan kepercayaan yang seragam di seluruh IKP Indonesia. CP bukan merupakan perjanjian hukum antara PSrE Induk Indonesia dan rantai kepercayaannya (PSrE Berinduk); melainkan kewajiban kontraktual antara PSrE Induk dengan PSrE Berinduk yang ditetapkan melalui perjanjian.

Dokumen ini ditargetkan pada:

- PSrE Induk yang harus beroperasi sesuai dengan Certificate Practice Statement (CPS) dimana CPS tersebut mengacu kepada persyaratan yang tertuang di dalam CP;
- PSrE Berinduk yang perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai pelanggan PSrE Induk dan bagaimana mereka dilindungi oleh PSrE Induk; dan
- Pihak Pengandal yang perlu memahami seberapa besar kepercayaan untuk dimasukkan ke dalam Sertifikat PSrE Induk Indonesia, atau tanda tangan elektronik tersertifikasi (tanda tangan digital) menggunakan Sertifikat itu.

Indonesia Public Key Infrastructure (Indonesia PKI) is a hierarchical PKI with the trust chain starting from the Root Certification Authority Indonesia (Indonesia Root CA). Ministry of Communication and Information Technology of The Republic of Indonesia (MCIT) operates Root CA Indonesia according to Regulation of the Government of the Republic of Indonesia number 71 of 2019 concerning Electronic System and Transaction Operation. Root CA Indonesia has two kinds of Subordinate CAs: Government CAs and Non-Government CAs. Government CAs issue certificates for state civil apparatus which can only be used for carrying out his responsibilities and / or authorities. Non-Government CAs issue certificates other than those issued by Government CAs.

This document, “Indonesia Root CA Certificate Policy” (CP) is the principal statement of policy governing the Root CA Indonesia. The CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing digital certificates within Indonesia PKI and providing associated trust services for all participants within the Indonesia PKI. These requirements protect the security and integrity of the Indonesia PKI and comprise a single set of rules that apply consistently Indonesia PKI-wide, thereby providing uniform trust assurances throughout the Indonesia PKI. The CP is not a legal agreement between

Root CA Indonesia and its trust chain (Subordinate CAs); but rather a contractual obligations between Root CA Indonesia and its trust chain which established by means of agreement.
This document is targeted at:

- Root CA Indonesia who have to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP
- Subordinate CAs who need to understand how they are authenticated and what their obligations are as Root CA Indonesia subscribers and how they are protected under the Root CA Indonesia; and
- Relying parties who need to understand how much trust to place in a Root CA Indonesia certificate, or a digital signature using that certificate

1.1 Overview / Ringkasan

CP ini berlaku untuk hirarki IKP Indonesia dari PSrE Induk (diperlihatkan dalam Diagram 1) dan semua Sertifikat yang diterbitkan baik secara langsung melalui sistem PSrE Induk sendiri maupun secara tidak langsung melalui PSrE Berinduk. Tujuan dari CP ini adalah untuk menyajikan penerapan dan prosedur dalam pengaturan sertifikat PSrE Induk dan PSrE Berinduk untuk menunjukkan kepatuhan terhadap akreditasi yang diterima industri formal seperti WebTrust. Selain itu, Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (UU ITE) memberikan pengakuan atas tanda tangan elektronik yang digunakan untuk tujuan autentikasi, verifikasi, dan nirsangkal. PSrE Induk beroperasi dalam lingkup bagian UU ITE saat memberikan layanannya.

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", yaitu menetapkan kerangka aturan operasional untuk produk dan layanan.

CPS merupakan penjelasan lebih lanjut dari CP, yang menyatakan cara PSrE Induk mematuhi CP. CPS menyediakan ringkasan proses, prosedur, dan ketentuan umum kepada PSrE Berinduk. Ringkasan proses, prosedur, dan ketentuan umum tersebut digunakan oleh PSrE Induk dalam menerbitkan dan memelihara sertifikat mereka. Demikian juga, PSrE Berinduk membuat CPS mereka sendiri yang berlaku untuk produk dan layanan yang mereka tawarkan.

This CP applies to the complete Indonesia PKI hierarchy of Root CA Indonesia (shown in Diagram 1 below) and all Digital Certificates that it issues either directly through its own systems or indirectly through its Subordinate CAs. The purpose of this CP is to present Root CA Indonesia’s practices and procedures in managing Root Certificates and Subordinate CAs in order to demonstrate compliance with formal industry accepted accreditations such as WebTrust. Additionally, the Law Of The Republic Of Indonesia Number 11 Of 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. In this regard, Root CA Indonesia operates within the scope of the applicable sections of the Law when delivering its services.

This CP sets out the objectives, roles, responsibilities and practices of all entities involved in the life cycle of Electronic 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.

A CPS complements this CP, which state how the Root CA Indonesia adheres to the CP. A CPS provides Subordinate CAs with a summary of the processes, procedures and overall prevailing conditions that the Root CA (i.e. the entity which provides the Subordinate CAs their Certificates) will use in creating and managing such Certificates. Likewise, Subordinate CAs maintain their own CPS applicable to products and services they offer.

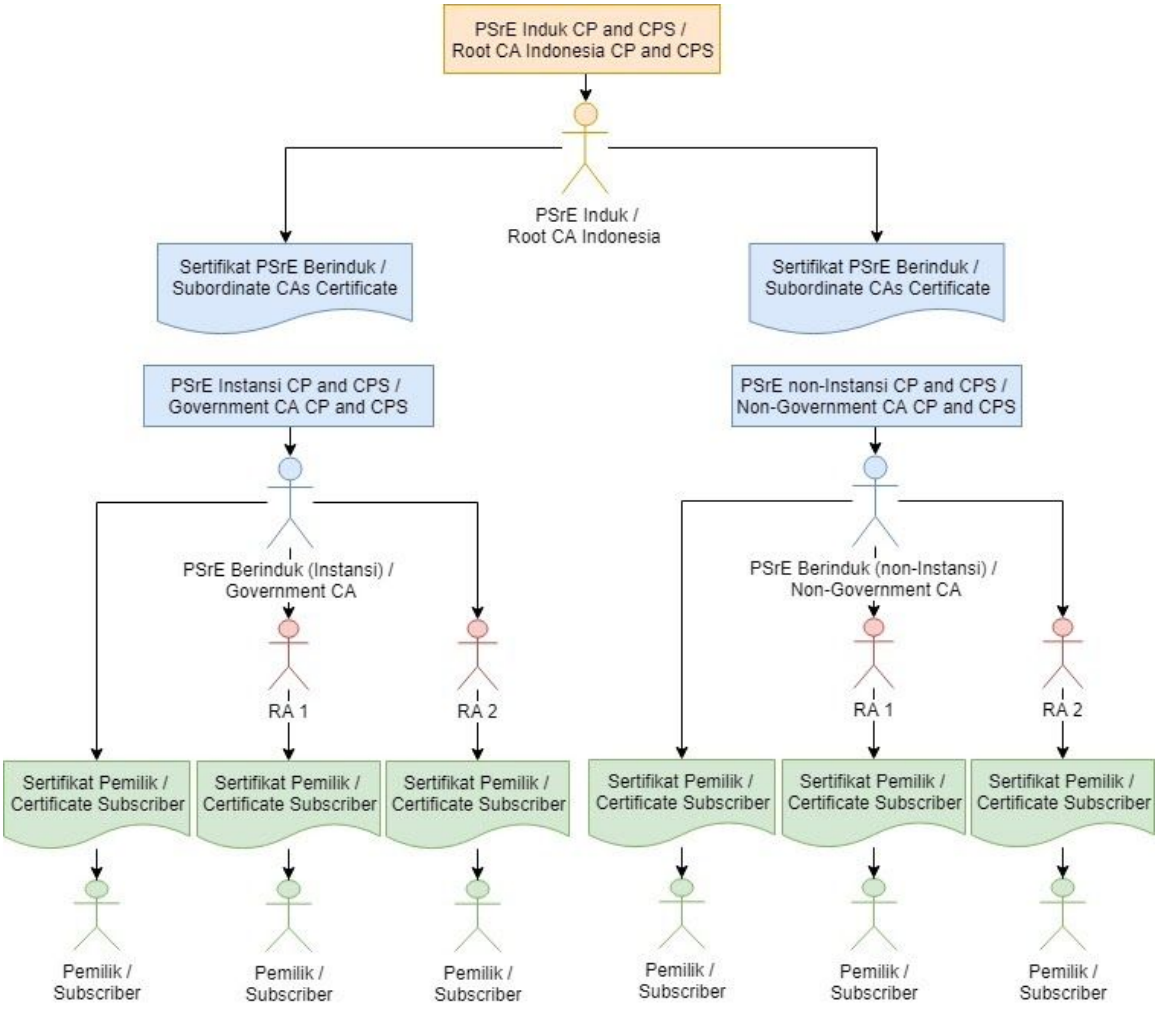

Diagram 1. Structure of the Indonesia PKI hierarchy of Root CA Indonesia

1.2 Document Name and Identification / Identifikasi dan Nama Dokumen

Dokumen ini adalah dokumen CP (Certificate Policy) PSrE Indonesia.

Object Identifier (OID) yang digunakan untuk CP (tidak termasuk Extended Validation Certificate) ini adalah:

1. 2.16.360.1.1.1.11 (PSrE Berinduk Instansi)
2. 2.16.360.1.1.1.12 (PSrE Berinduk Non-Instansi)

The document is the Certificate Policy for CAs Indonesia.

Object Identifiers (OID) used for this CP (not including Extended Validation Certificate) are:

1. 2.16.360.1.1.1.11 (Subordinate Government CA)
2. 2.16.360.1.1.1.12 (Subordinate Non-Government CA)

1.3 PKI Participants / Partisipan IKP

1.3.1 Certification Authorities / Penyelenggara Sertifikasi Elektronik (PSrE)

1.3.1.1. Root CA Indonesia / PSrE Induk Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia. PSrE Induk menerbitkan dan mencabut Sertifikat PSrE Berinduk (PSrE Instansi maupun PSrE non-Instansi) berdasarkan status pengakuan yang diberikan oleh Kemenkominfo. PSrE Induk tidak menerbitkan Sertifikat kepada Pemilik. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Berinduk, sebagaimana dirinci dalam CP ini, termasuk:

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

Root CA Indonesia is the root CA of Indonesia PKI. Root CA Indonesia issues and revokes Electronic Certificates to Subordinate CAs (Government CAs and Non-Government CAs) upon authorization by MCIT and it does not issue Digital Certificates to Subscribers .
Root CA Indonesia is responsible for all aspects of the issuance and management of those Subordinate CA Digital Certificates, as detailed in this CP, including:

- The control over the registration process;
- The identification and authentication process;
- The Certificate issuance process;
- The publication of Certificates;
- The validation of Certificates;
- The revocation of Certificates; and
- Ensuring that all aspects of the services, operations, and infrastructures related to Root CA detailed in this CP are performed in accordance with the requirements, representations, and warranties stated in this CP.

1.3.1.2. Subordinate CAs / PSrE Berinduk

PSrE Berinduk adalah PSrE dengan status pengakuan tersertifikasi yang Sertifikatnya telah ditandatangani oleh PSrE Induk. PSrE Berinduk menerbitkan Sertifikatnya kepada Pemilik sebagaimana digambarkan pada Diagram 1 diatas.

PSrE Berinduk tidak boleh berinduk kepada PSrE lain dan tidak boleh menjadi induk bagi PSrE lainnya.

Subordinate CAs are CAs which have acknowledgement status of Certified and whose certificates are signed by Root CA. Subordinate CAs issue certificates to subscibers as described in Diagram 1.
Neither Subordinate CAs are allowed to rooted themselves on other CAs nor they are allowed to become root to other CAs

1.3.2 Registration Authorities / Otoritas Pendaftaran (RA)

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

CAs may designate 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 antara PSrE dan RA, sebagai berikut:

a. menyusun prosedur pendaftaran untuk Pemohon Sertifikat;
b. melakukan identifikasi dan autentikasi Pemohon Sertifikat;
c. memulai atau meneruskan proses permohonan pencabutan Sertifikat; dan
d. menyetujui permohonan untuk memperbaharui Sertifikat atau pembaharuan kunci, atas nama PSrE.

The RA is obliged to perform certain functions according to the agreement between the CA and RA, as follows:

a. establish enrollment procedures for end-user certificate Applicants;
b. perform identification and authentication of certificate Applicants;
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 yang ditandatangani oleh PSrE Berinduk. Entitas Pemilik berarti subjek pemegang Sertifikat sekaligus entitas yang terikat dengan PSrE Berinduk penerbit Sertifikat. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat, entitas disebut sebagai Pemohon.

Subscribers are entities who request and successfully acquire a Certificate signed by Subordinate 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.

1.3.4 Relying Parties / Pihak Pengandal

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

yang sesuai sebelum memanfaatkan informasi yang ada dalam Sertifikat.

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 kesesuaian penggunaan dan tujuan Sertifikat. Pihak Pengandal menggunakan informasi dalam Sertifikat untuk:

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

Pihak Pengandal dapat meliputi Bank, perusahaan e-Commerce, Instansi Penyelenggara Negara dan entitas lain yang menggunakan tanda tangan digital di dalam layanannya.

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

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 usage and purpose of the Certificate. Relying parties use information on the certificate to:

a. Checking the usage purpose of the Certificate;
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 wajib menentukan Partisipan Lain yang berhubungan dengan penyelenggaraan sertifikasi elektronik.

CAs shall 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 Berinduk dapat digunakan untuk menerbitkan Sertifikat untuk transaksi yang memerlukan:

a. Autentikasi;
b. Tanda Tangan Digital & Nirsangkal; dan
c. Enkripsi.

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

a. Level 3: Sertifikat dengan Level Verifikasi Sedang
   Verifikasi identitas dilakukan dengan tatap muka dengan membandingkan kartu identitas terhadap Data identitas yang dimiliki oleh pemerintah.
b. Level 4: Sertifikat dengan Level Verifikasi Tinggi
   Verifikasi identitas dilakukan menggunakan kartu identitas dan data biometrik yang dibandingkan dengan data identitas yang dimiliki oleh pemerintah.

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

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

a. Authentication;
b. Digital Signature & Non-Repudiation; and
c. Encryption

Subscribers may choose an appropriate verification level in their identity that they wish to present to Relying Parties. Verification level is distinguished in these following Certificate Class:

a. Level 3: Medium Verification Certificate
   The identity is verified with Government-owned identity data.
b. Level 4 High Assurance Certificate
   The identity is verified with Government-owned identity data and Government-owned biometric data.

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

Kelas Sertifikat / Certificate Class	**Level Verifikasi / Verification Level**			**Penggunaan / Usage**		
	Verifikasi Rendah / Low Assurance	**Verifikasi Sedang / Medium Assurance**	**Verifikasi Tinggi / High Assurance**	**Autentikasi / Authentication**	**Tanda Tangan Digital & Nirsangkal / Digital Signature & Non-Repudation**	**Enkripsi / Encryption**
Sertifikat Individu / Individual Certificates						
Level 3		✓		✓	✓	✓
Level 4			✓	✓	✓	✓
Sertifikat Organisasi / Organizational Certificates						
Sertifikat Organisasi / Organizational Certificate			✓		✓	✓

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:

a. Menetapkan *Certificate Policy* (CP)/Certification Practice Statement (CPS);
b. Memastikan semua layanan, operasional, dan infrastruktur PSrE yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki Level Verifikasi yang kurang lebih setara.

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

a. Approves the Certificate Policy (CP)/Certificate Practice Statements (CPS);
b. 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
c. Approves the establishment of trust relationships with external PKIs that approximately have equivalent verification level.

1.5.1 Organization Administering the Document / Organisasi Pengelola Dokumen

CP dan dokumen referensinya dikelola oleh:

policy@rootca.or.id
layanan.aptika@mail.go.id

Telepon : +62 21 34830963
+62 21 386 8159

WA : +62 81519456822

Fax : +62 21 386 8159

This CP and the document referenced herein are maintained by:

policy@rootca.or.id
layanan.aptika@mail.go.id

Telepon : +62 21 34830963
+62 21 386 8159

WA : +62 81519456822

Fax : +62 21 386 8159

1.5.2 Contact Person / Kontak

- Mailing Address / Alamat surat:
  Kepada Direktur Tata Kelola Aptika - Ditjen Aptika Kementerian Kominfo
  Jalan Medan Merdeka Barat No 9 Jakarta 10110
- Email : policy@rootca.or.id
  layanan.aptika@mail.go.id
- URL : rootca.or.id
- Telepon/phone : +62 21 34830963
  +62 21 386 8159
- WA : +62 81519456822
- Fax. : +62 21 386 8159

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

Policy Authority (PA) PSrE menentukan kesesuaian konten CP dan kesesuaian antara CP dengan CPS.

Policy Authority (PA) of a 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 menyetujui CP/CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CP/CPS atau dengan mempublikasikan adendum. PSrE menentukan apakah perubahan atas CP ini membutuhkan pemberitahuan atau perubahan OID.

CAs approves the CP/CPS and any amendments. Amendments are made by either updating the entire CP/CPS or by publishing an addendum. CAs determine whether an amendment to this CP requires a notification or alteration of OID.

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 bertanggung jawab memelihara repositori daring yang dapat diakses publik, berisi dokumen kebijakan, Sertifikat, dan CRL.

CAs shall operate online repositories where policy documents, Certificates, and CRL are published.

2.2 Publication of Certification Information / Publikasi Informasi Sertifikat

PSrE memelihara repositori yang dapat diakses melalui internet yang mempublikasikan Sertifikat, CRL terakhir, dokumen CP/CPS, dan dokumen lain yang berkaitan dengan operasionalnya.

CAs maintain a repository accessible through the Internet in which it publishes Certificates, the latest CRL, the CP/CPS, and other 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.

PSrE Induk harus mempublikasikan sertifikat PSrE Berinduk dan data pencabutan sertifikat dalam waktu 1 (satu) jam setelah penerbitan.

PSrE berinduk harus mempublikasikan sertifikat Pemilik dan data pencabutan sertifikat dalam waktu 30 (tiga puluh) menit setelah penerbitan.

CRL diperbaharui sesuai pengaturan pada bagian 4.9.7.

This CP and any subsequent changes shall be made publicly available within 7 (seven) calendar days after its approval.

Root CA shall publish Subordinate CA certificates and revocation data within 1 (one) hour after issuance.

Subordinate CA shall publish Subscriber certificates and revocation data within 30 (thirty) minutes after issuance.

The CRL is updated according to stipulation in section 4.9.7.

2.4 Access Controls on Repositories / Kendali Akses pada Repositori

Informasi yang terpublikasi pada repositori adalah informasi publik. PSrE harus 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.

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

Information published on a repository is public information. CAs shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

CAs shall protect information not intended for public dissemination or modification.

3. IDENTIFICATION AND AUTHENTICATION / IDENTIFIKASI DAN AUTENTIKASI

3.1 Naming / Penamaan

3.1.1 Types of Names / Tipe Nama

PSrE harus 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.

Tipe Sertifikat	Distinguished Name
Sertifikat PSrE	CN=<Certification Authority Name><Certificate Type><Version>, O=<organization name>, C=ID
Sertifikat Pemilik	CN=<nama orang>,EMAILADDRESS=<email>,OU=<unit organisasi>,O=<nama organisasi>,C=ID

Contoh: CN=SubCASatuDuaTiga SSL G1, O=PT SubCASatuDuaTiga, C=ID

CAs shall 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><Certificate Type><Version>, O=<organization name>, C=ID
Subscriber certificate	CN=<person name>,EMAILADDRESS=<email>,OU=<organizational unit>,O=<organization name>,C=ID

e.g: CN=SubCASatuDuaTiga SSL G1, O=PT SubCASatuDuaTiga, 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.

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

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.

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, Autentikasi, dan Peran Merek Dagang

Pemilik tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE tidak perlu memverifikasi hak Pemohon untuk penggunaan merek dagang. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih.

PSrE dapat menolak permohonan atau melakukan pencabutan Sertifikat yang menjadi bagian dari konflik merek dagang.

Subscriber may not request certificates with any content that infringes the intellectual property rights of other parties. CAs are 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.

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).

Untuk Sertifikat pemilik, pasangan kunci dapat dibangkitkan oleh PSrE Berinduk, 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.

The method to prove possession of a private key shall be PKCS #10 (CSR), or another cryptographically equivalent request (request that digitally signed using private key).

For subscriber certificate, the key pair may be generated by Subordinate 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

Permohonan dari organisasi untuk menjadi Pemilik harus dibuat oleh orang yang berwenang mewakili organisasi tersebut. Permohonan ini harus mengikuti persyaratan seperti yang tercantum dalam CPS milik PSrE penerbit dan menyertakan rincian tentang organisasi dan salinan surat-surat pendirian perusahaan yang dilegalisir.

PSrE harus memverifikasi identitas dan status kepegawaian dari individu yang membuat permohonan dan otoritasnya untuk menerima Sertifikat untuk organisasi tersebut.

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

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 issuer CA's CPS and include details about the organization and a certified copy of their company papers.

CAs shall verify the identity and employment status of the individual making the application and their authority to receive the certificate for that organization.

CAs shall keep a record of the type and details of the identification used for the authentication of the organization for at least the life of the issued certificate.

3.2.3 Authentication of Individual Identity / Autentikasi dari Identitas Individu

Sebuah permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut, atau oleh orang lain atau organisasi yang secara resmi memiliki wewenang untuk mewakili pemohon tersebut.

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

Autentikasi identitas individu pemohon Sertifikat harus sesuai dengan Peraturan Menteri

Komunikasi dan Informatika Nomor 11 Tahun 2018.

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.

CAs 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.

Authentication of applicant's individual identity shall comply with Ministry Regulation of Communication and Informatics no. 11/2018.

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 hanya 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

Inter-Operasi IKP Indonesia tidak diizinkan.

Indonesia PKI Interoperation is not allowed.

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

Sebelum masa berlaku Sertifikat berakhir, Pemilik dapat meminta penggantian kunci yang selanjutnya disebut re-key dan Pemilik harus diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau menggunakan proses pemeriksaan identitas awal seperti yang dijelaskan pada bagian 3.2. PSrE Berinduk tidak dapat meminta re-key kepada PSrE Induk.

Prior to the expiry of a certificate, Subscribers may request for a re-key and Subscribers shall be authenticated through signing using their current Certificates or by using the initial

identity-proofing process as described in section 3.2. Subordinate CAs may not request for a re-key from Root CA Indonesia.

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

Setelah Sertifikat dicabut selain karena alasan pembaruan, Pemilik harus mengulang proses pendaftaran seperti yang dijelaskan pada bagian 3.2 untuk mendapatkan Sertifikat baru dengan kunci yang baru.

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

3.4 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 terkompromikan (*compromised*).

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

Hanya PSrE Tersertifikasi yang dapat mengajukan permohonan Sertifikat PSrE yang ditandatangani oleh PSrE Induk, perwakilan resmi dari PSrE harus mengajukan permohonan kepada PSrE Induk.

PSrE Berinduk Instansi harus menerbitkan sertifikat untuk entitas Pemerintah.

PSrE Berinduk non-Instansi harus menerbitkan sertifikat untuk entitas Non-Pemerintah.

Only certified CAs can submit CA-Certificate application to be signed by Indonesia Root CA, an authorised representative of the Subject CA shall submit the application to the Indonesia Root CA.

Government Subordinate CAs shall issues digital certificates to government entities.

Non-Government Subordinate CAs shall issues digital certificates to non-government entities.

4.1.2 Enrollment Process and Responsibilities / Proses Pendaftaran dan Tanggung Jawab

PSrE Berinduk harus 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 Berinduk dan RA untuk melakukan verifikasi atas identitas tersebut. PSrE Berinduk dan RA harus melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses pendaftaran.

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

Subordinate CAs shall 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 Subordinate CAs and RAs to successfully perform the required verification. Subordinate CAs 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.

4.2 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 permohonan Sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap Sertifikat atau permohonannya mengandung kesalahan, PSrE harus menolak permohonan. Jika 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 berusaha 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 memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan semua *field* dan ekstensi telah diisi dengan benar.

PSrE harus mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membuat Sertifikat Pemohon.

PSrE harus melakukan langkah-langkah proses penerbitan sertifikat secara aman.

CA verifies the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.

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.

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 harus memberitahu Pemilik bahwa mereka tidak dapat menggunakan Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

Ketika tidak ada keluhan dari Pemilik dalam jangka waktu tujuh (7) hari kerja, Pemilik dianggap

menerima semua informasi Sertifikat.

Untuk penerbitan Sertifikat PSrE Berinduk, PSrE Induk harus menyiapkan prosedur penerimaan yang mengindikasikan dan mendokumentasikan penerimaan atas Sertifikat yang diterbitkan.

CAs shall notify to the Subscriber that they cannot use the certificate before checking all the information of certificate.

When there are no complaints from Subscriber within seven (7) working days, the Subscriber is deemed to accept all certificate information.

For the issuance of Subordinate CAs Certificates, Root 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 harus mempublikasikan Sertifikat dalam suatu repositori, sesuai dengan praktik publikasi Sertifikat milik PSrE (sebagaimana didefinisikan dalam CPS), termasuk juga ketika menerbitkan informasi pencabutan Sertifikat.

Semua sertifikat harus dipublikasikan dalam repositori, sesuai dengan bagian 2, segera setelah diterbitkan.

CAs shall publish certificates in a repository based on the certificate publishing practices of the issuer CA (as defined in the CPS), as well as revocation information concerning such certificates.

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

Pemilik harus melindungi Kunci Privatnya dari penggunaan tanpa izin atau pengungkapan oleh pihak lain, menggunakan modul kriptografi yang dikendalikan oleh Pemilik. Pemilik yang menitipkan private keynya kepada pihak ketiga, maka pihak ketiga tersebut harus melindungi private key Pemilik dengan menggunakan Hardware Security Module. Pemilik harus memakai Kunci Privatnya hanya untuk tujuan yang sudah ditentukan.

Subscribers shall protect their Private Key from unauthorized use or disclosure by other parties using cryptographic module that is controlled by the Subscribers. In case of Subscriber escrowed their private key to a third party, that third party is obliged to protect the subscriber’s private key using Hardware Security Module. Subscribers shall use their private key only for the designated

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 batasan 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.

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

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.

A Relying Party should use discretion when relying on a certificate and should consider the totality of the circumstances and risk of 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 rincian yang sama dengan Sertifikat yang telah diterbitkan sebelumnya namun dengan pasangan kunci yang berbeda dan berisi tanggal yang baru pada *field* ‘Not After’. PSrE yang mendukung pembaruan harus 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. CAs that support renewal must 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 dapat meminta pembaruan Sertifikatnya ke PSrE Berinduk.
PSrE Berinduk yang belum pernah dicabut Sertifikatnya dapat meminta pembaruan Sertifikatnya ke PSrE Induk.

The Subscriber which have never been revoked may request the renewal of its Certificate to Subordinate CAs.

The Subordinate CA which have never been revoked may request the renewal of its Certificate to Root CA Indonesia.

4.6.3 Processing Certificate Renewal Requests / Pemrosesan Permintaan Pembaruan Sertifikat

PSrE harus melakukan identifikasi dan autentifikasi permintaan pembaruan Sertifikat.

CAs 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 adalah sebagaimana yang 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 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

Lihat bagian 9.16.

See section 9.16.

4.7 Certificate Re-Key / Re-Key Sertifikat

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

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

PSrE Berinduk dapat melakukan re-key selama :

- Sertifikat asli yang akan diganti belum pernah dicabut;
- Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun; dan
- Seluruh rincian yang terkait dengan Sertifikat tersebut masih akurat dan tidak membutuhkan validasi baru atau tambahan.

Certificate re-keying is the re-issuance of a certificate using the same subject information and expiration date (“validTo” field) but with a new key-pair.

A Subordinate CA may re-key a Certificate as long as:

- The original Certificate to be re-keyed has not been revoked;
- The new public key has not been blacklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

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

Sesuai dengan kondisi yang ditentukan pada bagian 4.7.1, perwakilan resmi PSrE Berinduk dapat meminta re-key dari Sertifikat PSrEnya.

Pemilik menghubungi PSrE Berinduk untuk melakukan re-key Sertifikatnya.

In accordance with the conditions specified in section 4.7.1, an authorized representative of the Subordinate CA may request re-key of its CA certificate.

The Subscribers contact the Subordinate CA in order to re-key their own Certificate.

4.7.3 Processing Certificate Re-Keying Requests / Pemrosesan Permintaan Re-Key Sertifikat

Berlaku prosedur penerbitan re-key Sertifikat seperti yang dinyatakan pada bagian 4.3.

The same re-key issuance procedure is followed, as stated in section 4.3

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

Berlaku prosedur pemberitahuan re-key Sertifikat yang sama dengan yang dinyatakan pada bagian 4.3.2.

The same re-key issuance notification procedure 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 di Re-key

Pemilik harus menerima Sertifikat dengan kunci baru, mengikuti prosedur penerimaan yang sama, sebagaimana diuraikan dalam bagian 4.4.1.

The subscriber must receive the certificate with the new key, following the same acceptance procedure, as described in section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA / Publikasi Sertifikat yang di Re-Key oleh PSrE

Sertifikat dengan kunci baru dipublikasikan, sesuai dengan prosedur repositori, yang dinyatakan dalam bagian 4.4.2.

The certificate with the new key is published, according to the repository procedures, as stated in section 4.4.2.

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

Tidak ada aksi yang dilakukan untuk pemberitahuan atas entitas lain selain apa yang telah dinyatakan dalam bagian 9.16.

No action is taken for the notification of other entities other than what is stated in section 9.16.

4.8 Certificate Modification / Modifikasi Sertifikat

Modifikasi rincian sertifikat tidak diizinkan. Dalam hal terjadi kesalahan selama penerbitan Sertifikat (contohnya ejaan), Sertifikat dicabut dan diikuti dengan proses penerbitan re-key, seperti yang dinyatakan pada bagian 4.3.

Modification of certificate details is not permitted. In case there is a mistake during certificate issuance (e.g. spelling), the certificate is revoked and the re-key issuance process is followed, as stated in section 4.3

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 Berinduk harus mencabut Sertifikat Pemilik dalam keadaan berikut:

- Komponen informasi yang berafiliasi dengan nama dalam Sertifikat menjadi tidak valid.
- Informasi apapun dalam Sertifikat menjadi tidak valid.
- Pemilik terbukti melanggar ketentuan dalam kontrak berlangganannya.
- Ada alasan untuk meyakini bahwa kunci privat telah *compromised*/rusak.
- Pemilik atau pihak berwenang lainnya (sebagaimana didefinisikan dalam CPS) meminta Sertifikatnya dicabut.
- PSrE Berinduk berhenti beroperasi.

Sertifikat harus dicabut ketika hubungan antara subyek dan kunci publiknya yang didefinisikan dalam Sertifikat sudah tidak valid lagi. Ketika hal tersebut terjadi Sertifikat harus dicabut dan dimasukkan dalam CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status Sertifikat sampai masa berlaku Sertifikat berakhir.

CAs shall revoke a subscriber's certificate in the following circumstances:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Any information in the certificate becomes invalid.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- 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.
- Subordinate CA termination.

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 sepanjang mereka dapat membuktikan terjadi penyalahgunaan Sertifikat sebagaimana dijelaskan pada 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 harus memverifikasi identitas dan wewenang (untuk 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. penggunaan sertifikat tidak sesuai dengan CP, atau
c. pemilik sertifikat tidak berasal dari institusi yang bersangkutan.

Proses permintaan pencabutan Sertifikat dijelaskan lebih rinci dalam CPS.

CAs 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 pencabutan 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 harus memulai permintaan investigasi paling lama ditindaklanjuti dalam dua (2) hari kerja kecuali dalam hal *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang cukup akan diproses sesegera mungkin.

CAs must start the investigation of revocation requests within two (2) 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 server PSrE.

Pihak Pengandal harus memvalidasi sertifikat terhadap server OCSP milik PSrE.

Relying parties should validate any presented certificate against the most updated CRL via CA's server.

Relying parties should validate any presented certificate 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 pemilik/perangkat, paling sedikit 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.

Dalam hal kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat PSrE Berinduk, CRL terbaru HARUS dipublikasikan dalam waktu 24 jam semenjak waktu pencabutan sesuai dengan stempel waktu (timestamp).

CRL harus diamankan untuk menjamin integritas dan keautentikannya.

The CRL must be updated and published:

- for end-user/device certificates, at least 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.

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.

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)

PSrE Induk harus mempublikasikan CRL paling lama 24 (dua puluh empat) Jam setelah penerbitan.

PSrE Berinduk harus mempublikasikan CRL paling lama 30 (tiga puluh) Menit setelah penerbitan.

Root CA must publish Certificate Revocation List within 24 (twenty four) hours after Certificate issuance.

CAs must publish Certificate Revocation List within 30 (thirty) Minutes after Certificate issuance.

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

PSrE Induk tidak memberikan layanan validasi daring.

PSrE Berinduk harus memberikan layanan validasi daring. PSrE Berinduk diharapkan melakukan pengecekan menggunakan Server OCSP yang disediakan.

Root CA Indonesia does not provide online validation service.

Subordinate CAs must provide online validation service. If online validation is available, Subordinate CAs are 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

Seperti yang didefinisikan pada bagian 4.9.3.2.

As defined in section 4.9.3.2.

4.9.13 Circumstances for Suspension / Keadaan untuk Pembekuan

Keadaan untuk pembekuan sertifikat Pemilik dinyatakan dalam CPS PSrE Berinduk.

Circumstances for Suspension shall be stated in Subordinate CA's CPS

4.9.14 Who can Request Suspension / Siapa yang Dapat Meminta Pembekuan

Entitas yang dapat meminta pembekuan dinyatakan dalam CPS PSrE Berinduk.

Entities who can request Suspension shall be stated in Subordinate CA's CPS

4.9.15 Procedure for Suspension Request / Prosedur Permintaan Pembekuan

Prosedur permintaan pembekuan sertifikat Pemilik dinyatakan dalam CPS PSrE Berinduk.

Procedure for certificate suspension request shall be stated in Subordinate CA's CPS

4.9.16 Limits on Suspension Period / Batas Waktu Pembekuan

Batas waktu pembekuan sertifikat Pemilik dinyatakan dalam CPS PSrE Berinduk.

Limits on Suspension period shall be stated in Subordinate CA's CPS

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 harus melakukan semua tindakan yang diperlukan untuk menjamin ketersediaan layanan validasi status sertifikat.

CAs 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

Prosedur penghentian berlangganan untuk Pemilik dinyatakan dalam CPS PSrE Berinduk.

Subscription termination procedure for Subscriber shall be stated in Subordinate CA's CPS

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 maupun lokasi tempat kerja yang digunakan untuk mengelola PSrE, harus sama dengan lokasi fasilitas yang digunakan untuk menampung informasi yang bernilai tinggi dan sensitif. Lokasi dan konstruksi tempat kerja, ketika dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjagaan dan sensor intrusi, harus memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan catatan PSrE.

The location and construction of the facility housing CA equipment as well as sites housing remote workstations used to administer the CAs, shall be 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 intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access / Akses Fisik

Peralatan PSrE harus selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik untuk PSrE setidaknya harus dilakukan untuk:

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

Operasional PSrE yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan setidaknya memiliki empat lapis keamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif. Fasilitas tersebut harus terpisah secara fisik dari fasilitas organisasi yang lain, sehingga hanya pegawai PSrE yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

The 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.

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

5.1.3 Power and Air Conditioning / Daya dan Penyejuk Udara

PSrE harus memiliki daya listrik cadangan yang cukup ketika listrik utama mati, dan menyelesaikan setiap aksi yang tertunda, dan merekam status perangkat sebelum kekurangan daya atau AC yang menyebabkan shutdown. Repositori IKP harus dilengkapi Daya Tak Terputus dan Generator Listrik yang cukup untuk beroperasi paling sedikit 6 (enam) jam saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories shall be 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

Peralatan PSrE harus ditempatkan pada tempat yang tidak terpapar air.

Paparan air untuk pencegahan kebakaran dan tindakan perlindungan (misalnya sistem sprinkler) dikecualikan dari persyaratan ini.

The CA equipment shall be installed in a place where there is no danger of exposure to water.

Water exposures from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection / Pencegahan dan Perlindungan dari Kebakaran

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

Root CA Indonesia and its Subordinate CAs' equipments are placed in facilities with adequate fire detection and suppression systems.

5.1.6 Media Storage / Penyimpanan Media

Media Backup dari PSrE harus ditempatkan di lokasi terpisah dan harus disimpan agar terlindungi dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau cadangan harus diduplikasi dan disimpan di lokasi yang terpisah dari PSrE.

CA backup media shall be stored in an offsite location and protected it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media containing audit, archive, or backup information shall be duplicated and stored in a location separate from the CA location.

5.1.7 Waste Disposal / Pembuangan Limbah

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

All sensitive information which are contained in waste material must be destroyed before it is disposed.

5.1.8 Off-Site Backup / Backup Off-Site

Sistem backup PSrE harus dilakukan secara berkala dan harus mampu memulihkan sistem ketika terjadi kegagalan. Sistem backup tersebut harus dijelaskan pada CPS PSrE. Backup harus dilakukan dan hasil backup tersebut disimpan di lokasi terpisah minimal sekali dalam tujuh (7) hari untuk PSrE Berinduk dan sekali dalam enam (6) bulan untuk PSrE Induk. Setidaknya satu (1) salinan backup lengkap harus disimpan di lokasi terpisah (di lokasi yang terpisah dari perangkat PSrE). Hanya backup lengkap terkini yang perlu disimpan. Data backup harus dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional PSrE. Jarak minimal off-site backup adalah 50km.

System backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule, described in the respective CPS. Backups shall be performed and stored offsite not less than once every seven (7) days for Subordinate CA and six (6) months for Root CA Indonesia. At least one (1) full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained. The backup data shall be protected with physical and procedural controls commensurate to that of the operational CA. Minimum range offsite-backup is 50km.

5.2 Procedural Controls / Kendali Prosedur

5.2.1 Trusted Roles / Peran Terpercaya

Peran terpercaya meliputi tapi tidak terbatas pada:

- Koordinator
  Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan PSrE Induk
- Policy Authority (PA)
  Pembuatan, revisi dan persetujuan CP dan CPS
- Staff PA
  Membantu PA dalam menyiapkan dokumen CP dan CPS
- Administrator Aplikasi
  Melakukan operasional dan *maintenance* aplikasi manajemen PSrE Induk
- Administrator OS
  Melakukan operasional dan *maintenance* Sistem Operasi PSrE Induk
- Administrator HSM

Melakukan Operasional dan *maintenance* HSM PSrE Induk.

- Registrasi
  Identifikasi dan Validasi identitas permohonan permintaan sertifikat
- Key Custodian
  Mengelola penyimpanan dan pengamanan kunci
- Internal Audit
  Melakukan audit internal operasional PSrE Induk

Peran Terpercaya lainnya bisa didefinisikan dalam dokumen lain, yang menjelaskan mengenai persyaratan peran-peran tersebut pada operasional PSrE Induk

Trusted role includes, but not limited to:

- Coordinator
  Overall responsibility for managing all CA security practices
- Policy Authority (PA)
  Creation, revision and approval of CP and CPS
- Policy Authority Staff
  Prepare Root CA documents and policies for PA
- Application Administrator
  Conduct operasional and maintenance of CA management application
- OS Administrator
  Conduct operational and maintenance of CA Operating System
- HSM Administrator
  Conduct operational and maintenance of CA HSM
- Registration
  Identification and validation of certificate request application
- Key Custodian
  Manage CA Key’s Security and storage
- Internal Audit
  Conduct internal audit of CA operational

Other trusted role can be defined in other documents, which describe the requirements of the roles in Root 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 tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan tiga orang atau lebih:

- Pembangkitan kunci PSrE
- Penandatanganan Kunci PSrE Berinduk
- Pencabutan Sertifikat
- CRL Generation

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
- Subordinate CA's Key Signing
- Certificate Revocation
- CRL Generation

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 individual assigned to trusted role shall be identified and authenticated using Assignment Letter.

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

Satu orang tidak boleh merangkap peran pada peran-peran berikut:

- 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 PSrE harus warga negara Indonesia dan dipilih atas dasar kemampuan, pengalaman, tingkat kepercayaan, dan integritas. Personil yang ditunjuk untuk peran terpercaya harus secara resmi diangkat oleh manajemen.

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

5.3.2 Background Check Procedures / Prosedur Pemeriksaan Latar Belakang

Semua personil di PSrE harus lulus pemeriksaan latar belakang. Lingkup pemeriksaan latar belakang setidaknya dilakukan untuk lima (5) tahun terakhir mencakup area berikut:

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

Prosedur pemeriksaan latar belakang harus dijelaskan pada CPS.

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

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 tersebut mencakup topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, dan prosedur terkait.

Pelatihan tersebut harus mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras, perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP, 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 Indonesia PKI (including CA hardware, software and operating system), operational and security procedures, this CP and the applicable CPSes. 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 harus memberikan pelatihan ulang yang sifatnya memberi penyegaran dan memutakhirkan kemampuan para personilnya sesuai tingkatan dan frekuensi pelatihan yang dibutuhkan. Hal ini dilakukan untuk memastikan bahwa personil tersebut mempertahankan kompetensi yang dipersyaratkan untuk melakukan tugas dan tanggung jawab pekerjaan secara memuaskan.

The CAs 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 harus memastikan bahwa perubahan pegawai tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

CAs 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, CPS, atau prosedur operasional PSrE terkait.

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

5.3.7 Independent Contractor Requirements / Persyaratan Kontraktor Independen

Pegawai kontrak 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 sejumlah dokumen kepada para personilnya. Dokumen tersebut antara lain CP, CPS, peraturan, kebijakan, dan kontrak yang relevan. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) juga harus disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

CAs shall make available to its personnel the CP 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.

5.4 Audit Logging Procedures / Prosedur Log Audit

Berkas log audit harus dibuat untuk semua kejadian yang terkait dengan keamanan PSrE, VA, dan RA. Bila memungkinkan, log audit keamanan harus dikumpulkan secara otomatis. Bila tidak mungkin, dapat menggunakan buku log, kertas formulir, atau mekanisme fisik lain. Semua log audit keamanan, baik elektronik dan non elektronik, harus disimpan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini harus dipelihara sesuai dengan bagian 5.5.2.

Audit log files shall be generated for all events relating to the security of the CAs, VAs, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained

in accordance with section 5.5.2.

5.4.1 Types of Events Recorded / Jenis Kejadian yang Direkam

PSrE harus mengaktifkan semua fitur audit keamanan dari sistem operasi PSrE dan RA, serta aplikasi PSrE, VA, dan RA yang dipersyaratkan oleh CP ini. Oleh karena itu, sebagian besar dari kejadian yang teridentifikasi harus direkam secara otomatis. PSrE harus memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan Trusted Role dalam operasional PSrE dapat dilacak.

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

- Jenis kejadian,
- Nomor seri atau urutan rekaman,
- Tanggal dan waktu kejadian,
- Sumber perekaman,
- Indikator sukses atau gagal yang sesuai,
- Identitas dari entitas dan/atau operator yang menyebabkan kejadian

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. CAs 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.
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 minimal sebulan sekali. Peninjauan tersebut termasuk melakukan verifikasi bahwa log tersebut tidak dirusak, tidak diacak, dan tidak adanya jenis kehilangan lain terhadap data audit, dan kemudian secara singkat memeriksa semua entri log, dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan yang muncul 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 harus disimpan selama 1 (satu) tahun agar tersedia untuk pengendalian yang sah. Jangka waktu ini dapat berubah sewaktu-waktu sesuai dengan hukum yang berlaku.

CAs audit log shall be retained for 1 (one) year 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

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

The records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized trusted access are able to perform any operations without modifying integrity.

5.4.5 Audit Log Backup Procedures / Prosedur Backup Log Audit

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

Subordinate 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)

Tidak ditentukan.

No stipulation.

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 harus melakukan penilaian akan kerentanan sistem PSrE atau komponennya paling tidak sekali setahun.

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 harus cukup rinci untuk menentukan kesesuaian operasional PSrE dan validitas sertifikat yang dikeluarkan oleh PSrE (termasuk yang dicabut atau kedaluwarsa). 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.
- Data konfigurasi sistem IKP
- Dokumen CP dan semua CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen tersebut.

CA archive 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 5 (lima) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.

Archived records shall be retained for at least 5 (five) 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 diarsipkan dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan tersebut harus dipelihara dan dilindungi sesuai peraturan yang ditentukan dalam CP ini dan dalam CPS yang berlaku.

The archived records shall be protected against unauthorized viewing, modification, deletion, or

tampering. The media holding the archived records and the applications 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 harus diberi label waktu (timestamp) saat dibuat.

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)

Tidak diatur.

No stipulation.

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

Media penyimpanan informasi arsip PSrE diperiksa setelah dibuat. Secara berkala, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya PSrE berwenang, peran terpercaya (trusted roles) dan pihak-pihak lain yang berwenang yang diijinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada peran 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 kebocoran Kunci Privat PSrE, Kunci Privat boleh untuk diubah secara berkala. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat lama yang masih berlaku akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat pada sertifikat lama tersebut kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama harus disimpan dan dilindungi.
Apabila PSrE memperbarui kunci privat dan dengan demikian menghasilkan kunci publik baru, PSrE harus memberitahu semua Pemilik yang mengandalkan Sertifikat PSrE tersebut bahwa telah terjadi perubahan.

To minimize risk from compromise of a 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.

When a CA updates its private signature key and thus generates a new public key, the CA shall notify all subscribers that rely on the CA's certificate 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 harus memiliki rencana tanggap darurat dan rencana pemulihan bencana.

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

CAs shall have an incident response plan and a disaster recovery plan.

If compromise of a 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

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

- Memberitahu PA atau PSrE Induk sesegera mungkin.
- Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.

- Mengoperasikan kembali PSrE, dengan memprioritaskan kemampuan untuk membangkitkan informasi status sertifikat sesuai jadwal penerbitan CRL.
- Bila kunci penandatanganan PSrE rusak, operasional PSrE harus dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci PSrE baru.

When computing resources, software, and/or data are corrupted, CAs shall respond as follows:

- Notify PA or the superior CA as soon as possible.
- Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- Reestablish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signing keys are destroyed, reestablish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.

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

Dalam kasus kehilangan kunci privat atau bocornya algoritma dan parameter yang digunakan untuk membangkitkan kunci privat dan sertifikat, semua sertifikat Pemilik/peranti yang terkait dicabut oleh PSrE berinduk dan kunci-kunci serta sertifikat-sertifikat baru diterbitkan tanpa menghentikan layanan.

Dalam kasus kehilangan kunci privat dari PSrE Berinduk, semua Pemilik dari PSrE Berinduk ini diberitahu, semua sertifikat Pemilik yang diterbitkan oleh PSrE Berinduk yang terkompromi tersebut dicabut, begitu pula dengan sertifikat milik PSrE.

Bila kunci privat dari PSrE Induk hilang, PSrE Induk harus memberitahu PA dan Pihak Pengandal melalui pengumuman publik. PSrE Berinduk HARUS menghentikan layanan, memberitahu semua Pemilik dari semua PSrE Berinduk, dilanjutkan dengan pencabutan semua sertifikat, menerbitkan suatu CRL akhir, dan memberitahu kontak-kontak keamanan yang relevan. Lalu Infrastruktur Kunci Publik akan disiapkan lagi dengan PSrE baru dimulai dengan suatu PSrE Induk baru.

In case of loss of private keys or compromise of the algorithms and parameters used to generate the private key and certificate, all related subscriber/device certificates are revoked by the Subordinate CA and new keys and certificates are issued without interruption of the service.

In case of private key loss of a Subordinate CA, all subscribers of this Subordinate CA are notified, all subscriber certificates issued by the compromised Subordinate CA are revoked, along with the certificate of the CA.

If the private key of the Root CA is lost, Root CA shall notify the PA and relying parties via public announcement. Subordinate CA MUST stop the service, notify all subscribers of all subordinate CA, proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security contacts. Then the Public Key Infrastructure will be set up again with new Certification Authorities starting with a new Root Certification Authority.

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

PSrE harus menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbaharui. Layanan harus kembali pulih dalam kurun waktu 24 jam bila ada

bencana.

CAs shall prepare a disaster recovery plan which have 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 Berinduk mengakhiri operasinya, mereka harus memberitahu ke PSrE Induk, PA, dan para Pemilik sebelum penutupan sesuai dengan Peraturan Pemerintah.

In the event that a Subordinate 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.

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.

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.

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 were documented in the internal document of Root CA Indonesia. 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 atau PSrE Berinduk. Jika PSrE Berinduk 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 or CA. If the CA generates key pairs for subscribers, 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

PSrE harus membangkitkan sendiri pasangan kunci milik PSrE sehingga tidak memerlukan pengiriman kunci privat.

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

Bila PSrE Berinduk membangkitkan kunci atas nama Pemilik, maka Kunci Privat harus dikirimkan secara aman kepada Pemilik. Kunci privat dapat dikirim secara elektronik atau dikirimkan pada modul kriptografi hardware. Dalam semua kasus persyaratan berikut harus dipenuhi:

- Kunci Privat harus dilindungi terhadap aktivasi, *compromise*, atau perubahan selama proses pengiriman.
- Subscriber harus memberikan pernyataan penerimaan Kunci Privat.
- PSrE harus menyimpan pernyataan penerimaan Pemilik atas Kunci Privat.

CAs shall generate their own Key Pair and therefore do not need Private Key delivery.

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

When Subordinate CA generates keys on behalf of the Subscriber, then the Private Key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements shall be met:

- The Private Key shall be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the Private Key(s).
- The CA shall maintain a record of the Subscriber acknowledgement of receipt of the private key.

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 elektronik yang diterbitkan oleh PSrE berisi kunci publik. PSrE 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.

Pada jangka waktu tertentu sebelum kunci publik PSrE kedaluwarsa, suatu pasangan kunci penandatanganan sertifikat yang baru akan dibangkitkan supaya PSrE tetap bisa beroperasi secara normal.

Penjelasan tanggung jawab tentang publikasi dan repositori sertifikat mengacu pada Bagian 2.1.

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

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.

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 2048 bit antara 4096 bit dan hash SHA-256 atau SHA-384 ketika membuat tanda tangan digital.

CAs that generate certificates and CRLs under this policy should use RSA algorithm with a key length between 2048 bit and 4096 bit, and SHA-256 or 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 Berinduk. Penggunaan sebuah kunci spesifik ditentukan oleh key

usage extension dalam sertifikat X.509.

Kunci PSrE Induk dan PSrE Berinduk digunakan untuk penandatangan sertifikat dan CRL.

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 the Subordinate CA. The use of a specific key is determined by the key usage extension in the X.509 certificate.

Root CA Indonesia and Subordinate CAs 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.

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.

6.2.3 Private Key Escrow / Penitipan Kunci Privat

Kunci privat PSrE tidak boleh pernah dititipkan (escrow).

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 off-site. Semua salinan kunci privat PSrE harus dilindungi dengan cara yang sama dengan aslinya.

Pemilik dapat memilih untuk melakukan backup kunci mereka, tapi backup kunci harus berada di bawah kendali Pemilik.

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 off-site. All copies of the CA private key shall be

accounted for and protected in the same manner as the original.

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.

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.

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.

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.

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

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

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 elektronik yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai dua puluh (20) tahun bagi PSrE Induk, sepuluh (10) tahun bagi PSrE Berinduk, dan satu (1) 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 electronic certificate. The maximum operational period of the keys is defined as twenty (20) years for the Root CA, ten (10) years for a Subordinate CA, and one (1) year for Subscriber certificates. The operational period must be defined according to the size of the keys and the current technological developments in 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 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, jika memungkinkan, 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 meminimalisir jumlah akun dan layanan jaringan yang diperlukan.

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 serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen PSrE. Ada mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi milik PSrE.

The configuration of the CA system as well as any modifications and upgrades are documented and controlled by the CA management. There is a mechanism for detecting unauthorized modification to the CA software or configuration.

6.6.3 Life Cycle Security Controls / Kendali Keamanan Siklus Hidup

PSrE melakukan pengawasan terhadap kebutuhan skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak yang telah dievaluasi dan disertifikasi

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 harus 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.

CAs shall 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). 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 dapat diaudit.

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 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 sekali.

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 PSrE, 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.

Sertifikat CA dapat memuat ekstensi ExtendedKeyUsage sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang mereka terbitkan.

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.

By default, ExtendedKeyUsage is set as a non-critical extension.

CA Certificates may include the ExtendedKeyUsage extension as a form of technical constraint on the usage of certificates that they issue.

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.

URL harus patuh dengan persyaratan Mozilla yang tidak menyertakan protokol LDAP, dan mungkin muncul beberapa kali di dalam suatu ektensi cRLDistributionPoints.

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.

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. Field criticality dari ekstensi ini harus diisi FALSE.

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 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. Algoritma harus berupa enkripsi RSA untuk subject key dan SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.

X.509v3 standard OIDs shall be used. Algorithm shall be RSA encryption for the subject key and SHA256 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 Berinduk bisa mengoperasikan sebuah responder Online Certificate Status Protocol (OCSP) yang sesuai dengan RFC 6960 atau RFC 5019.

Subordinate 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 Berinduk harus menerbitkan respon OCSP versi 1.

Subordinate 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 Berinduk harus menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika 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.

Subordinate CA shall undergo a compliance audit and submit reports periodically as required by Indonesia Ministry of Communication and Informatics Regulation No 11 Year 2018

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 harus 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.

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

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

Subscriber CA shall 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 Year 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.

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 elektronik, sertifikat elektronik, X.509 versi 3 PKI Certificate Policy and Certification Practices Framework, UU ITE (UU No 11 2008 dan UU No 19 2016), PP PSTE (PP 71 2019), Peraturan Menteri Komunikasi dan Informatika no 11/2018.
c. memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
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
e. menguasai beberapa keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

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

Compliance auditors must possess these qualifications:

a. Auditors shall have a qualified, independent assessment team
b. Auditors shall have a sufficient knowledge on electronic signatures, electronic 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. Auditors shall have an adequate skills on information security audit, information security device and technique audit, as well as familiarity with PKI technology
d. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme
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 harus memilih auditor / asesor yang independen dari PSrE.

CAs must 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 berlaku pada tahun berikutnya setelah PSrE mengadopsi skema yang terbaru

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 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:

- Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.
- 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:

- The compliance auditor shall notify Kominfo of the discrepancy.
- 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 resiko 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 non-Instansi Penyelenggara Negara dapat mengenakan biaya administrasi dalam menerbitkan atau memperbaharui Sertifikat termasuk dalam hal penerbitan ulang sertifikat. Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat.

PSrE Instansi Penyelenggara Negara menerbitkan atau memperbaharui sertifikat tanpa dikenakan biaya

Non-Government CAs 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.

Government CAs shall not charge fees for issueance or renewal of Certificates.

9.1.2 Certificate Access Fees / Biaya Pengaksesan Sertifikat

PSrE non-Instansi Penyelenggara Negara dapat mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan.

PSrE Instansi Penyelenggara Negara tidak boleh mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan

Non-Government CAs may charge for access to repository which stores issued Certificates.

Government CAs shall not charge for access to repository which stores issued Certificates.

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

PSrE non-Instansi Penyelenggara Negara dapat mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau pencabutan sertifikat.

PSrE Instansi Penyelenggara Negara tidak boleh mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau pencabutan sertifikat.

Non-Government CAs may charge additional fees to Subscribers for accessing revocation or information status.

Government CAs shall not charge additional fees to Subscribers for accessing revocation or information status.

9.1.4 Fees for Other Services / Biaya Layanan Lainnya

PSrE non-Instansi Penyelenggara Negara dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya

PSrE Instansi Penyelenggara Negara tidak boleh mengenakan biaya untuk mendapatkan layanan tambahan lainnya

Non-Government CAs may charge for other additional services.

Government CAs shall not charge for other additional services.

9.1.5 Refund Policy / Kebijakan Pengembalian Sertifikat

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

CAs 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 Berinduk harus mematuhi persyaratan PM Kominfo Nomor 11 Tahun 2018 Pasal 12 huruf h.

CAs shall comply with Article 12 letter h of Communication and Informatics Minister Regulation No. 11/2018.

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 Berinduk harus menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik sertifikat.

Subordinate CAs shall 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 harus 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 CAs:

- 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. Sertifikat dan informasi mengenai status sertifikat termasuk kategori informasi publik.

Any information not defined as confidential within the CP shall be deemed public. 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 harus melindungi informasi rahasia. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:

- Pelatihan atau peningkatan *awareness*
- Perjanjian kontrak pegawai
- NDA (*Non Disclosure Agreement*) dengan pegawai, pegawai outsource, dan rekanan

CAs shall protect confidential information. CAs shall enforce protection of confidential information through the following mechanism but not limited to :

- training,
- contracts with employees,
- NDA with employees, outsource and contractors.

9.4 Privacy of Personal Information / Privasi Informasi Pribadi

9.4.1 Privacy Plan / Rencana Privasi

PSrE harus melindungi informasi pribadi dalam kaitan dengan “Kebijakan Informasi Pribadi“ yang dipublikasikan sesuai dengan ketentuan repositori pada Bagian 2.1.

CAs shall 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 harus 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.

CA shall 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 dikenakan perlindungan sebagaimana dijelaskan pada 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 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.

CAs are 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 CAs.

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

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

The CA shall 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 termasuk semua merek dagang dan hak cipta dari semua dokumen PSrE tetap menjadi milik tunggal dari PSrE.

CA's Intellectual Property Rights including trademarks, copyright and all CA documents remains as sole property of CA.

9.6 Representations and Warranties / Pernyataan dan Jaminan

9.6.1 CA Representations and Warranties / Pernyataan dan Jaminan PSrE

PSrE menyatakan dan menjamin, sejauh yang ditentukan dalam CP, bahwa:

- PSrE mematuhi ketentuan yang diatur dalam CP ini,
- PSrE menerbitkan dan memperbarui CRL secara berkala,
- Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP ini,
- PSrE akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

CA represents and warrants, to the extent specified in this CP, that:

- CA complies, in all material aspects, with the CP,
- CA publishes and updates CRL on a regular basis,
- All certificates issued will meet the minimum requirements and verified in accordance with this CP and,
- 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

- Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat,
- Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat,
- PSrE mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP dan dituangkan dalam kontrak.

RAs warrant that:

- 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
- There are 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.
- CAs 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 elektronik 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 kadaluarsa dan telah dicabut) saat tanda tangan elektronik 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 elektronik 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
    - (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
    - (c) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut;
- Akan menanggapi instruksi PSrE terkait *compromise* atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;
- 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;*
- Untuk PSrE Berinduk, Pemilik sertifikat adalah pengguna akhir dan bukan merupakan PSrE, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat elektronik untuk tujuan penandatangan sertifikat elektronik PSrE lain.

Subscribers warrant that:

- Each electronic signature created using the private key corresponding to the public key listed in the Certificate is the electronic 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) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
    - (c) stop using the private key whose public key is listed in a digital certificate after the certificate is revoked;
- will respond to CAs instructions regarding compromise or electronic certificates misuses within forty eight (48) hours,
- 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
- For subordinate CA, 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 menjamin bahwa:

- Memliki kemampuan teknis untuk menggunakan sertifikat,
- apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh PSrE, 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,
- Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat
- 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,
- Harus mematuhi ketentuan yang ditetapkan di CP dan perjanjian lain yang terkait.

CA’s Certificate relying party guarantee that :

- Have the technical capability to use certificates,
- If the representative from the Relying Party use a certificate issued by CAs, relying party should verified the information contained in the certificate before use and carry all the consequences that happened if the relying party fail to applied it.
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised,
- 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,
- 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

PSrE harus membuat pernyataan dalam CPS bahwa mereka tidak menjamin:

- Kecuali untuk jaminan yang telah tercantum dalam CPS dan kontrak perjanjian dan sepanjang diizinkan oleh hukum, PSrE mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu,
- penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Certificate Usage)
- Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat.

CAs should make statements in their CPS that they do not warrant:

- Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, CAs disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.
- Misuse of a certificate that is inconsistent with its usage as shown in section 4.5 (Certificate Usage),
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo Certificates.

9.8 Limitations of Liability / Pembatasan Tanggung Jawab

9.8.1 CA Limitations of Liability / Pembatasan Tanggung Jawab PSrE

PSrE 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.

CAs 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 harus ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

CA's indemnification obligations must 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 harus menyertakan persyaratan ganti rugi untuk Pemilik Sertifikat dalam CPS dan dalam Kontrak Berlangganannya.

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

9.9.3 Indemnification by Relying Parties/ GantiRugi oleh Pihak Pengandal

PSrE harus menyertakan persyaratan ganti rugi untuk Pihak Pengandal dalam CPS.

CAs shall 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.

This CP remains in force until such time as communicated otherwise by CAs on its website or Repository.

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 harus mengkomunikasikan kondisi akibat dari penghentian CP dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui laman atau repositori.

CAs should 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 menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara elektronik, 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.

CAs provides communication media for related parties through electronics document, electronic mail, telephone both electronically 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 harus 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.

CAs should post appropriate notice on their web sites of any major or significant changes to this CPS 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 harus 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.

CAs should 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 Induk Indonesia 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, Root CA Indonesia 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 diatur, ditafsirkan, dan dipahami sesuai dengan aturan hukum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat PSrE ataupun produk/ layanan lainnya. Termasuk apabila sertifikat PSrE dipakai untuk kebutuhan komersil atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan PSrE, tetap menerapkan aturan hukum di Indonesia.

Para pihak, termasuk partners CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

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. The laws of Indonesia also apply to all CAs commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to CAs products and services where CAs acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including CAs 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 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

CAs 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 CAs, 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 effect 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 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.

CAs 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 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. PSrE wajib menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas PSrE.

CAs 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.

9.17 Other Provisions / Ketentuan Lain

Tidak ada ketentuan

No stipulation.

APPENDIX A. TABLE OF ACRONYMS AND DEFINITIONS

Tabel Akronim / Table of Acronyms

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

VA	Validation Authority

Definisi / Definitions

Istilah / Term	Definisi / Definition
IKP Indonesia	Seperangkat perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan, dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan Sertifikat dan kunci yang dapat dipercaya berdasarkan pada kriptografi Kunci Publik sesuai peraturan Indonesia
Indonesia PKI	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography according to Indonesian regulations
PSrE	Entitas yang berwenang untuk mengeluarkan, mengelola, mencabut, dan memperbarui Sertifikat dalam lingkup IKP Indonesia
CA	An entity authorized to issue, manage, revoke, and renew Certificates within the Indonesia PKI
PSrE Induk	Entitas legal yang memiliki otoritas Sertifikasi tingkat teratas yang menandatangani Sertifikat PSrE Berinduk dalam rantai IKP Indonesia
Root CA Indonesia	The top level Certification Authority that issues Subordinate CA Certificates in the Indonesian PKI chain
PSrE Berinduk	Entitas legal yang Sertifikatnya ditandatangani oleh PSrE Induk dan bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Pemilik
Subordinate CA	Legal entity whose Certificate is signed by the Root CA and is responsible for the creation, issuance, revocation, and management of Subscriber's Certificates
PSrE Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat Instansi
Government CA	Subordinate CA whose responsible for the creation, issuance, revocation, and management of Government Certificates.
PSrE non-Instansi	PSrE Berinduk yang bertanggung jawab atas pembuatan, penerbitan, pencabutan, dan pengelolaan Sertifikat non-Instansi
Non-Government CA	Subordinate CA whose responsible for the creation, issuance, revocation, and management of Non-Government Certificates.

Pemohon Applicant	Individu atau Badan Hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik atau PSrE Berinduk 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 or Subordinate CA.
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 Induk Root CA Indonesia Certificate	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh PSrE Induk untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh PSrE Berinduk The self-signed Certificate issued by Root CA Indonesia to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs
Sertifikat PSrE Berinduk Subordinate's Certificate	Sertifikat yang dikeluarkan oleh PSrE Induk The Certificate issued by Root CA Indonesia
Sertifikat Pemilik Subscriber's Certificate	Sertifikat yang dikeluarkan oleh PSrE Berinduk The Certificate issued by Subordinate CA
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	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat

Certification Practice Statement	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used
Certificate Revocation List Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh PSrE Berinduk yang menerbitkan Sertifikat A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates
Certificate Signing Request Certificate Signing Request	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat A message conveying a request to have a Certificate issued
Kompromi Compromise	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif A violation of a security policy that results in loss of control over sensitive information
Extended Validation Certificate Extended Validation Certificate	Sertifikat 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 Key Compromise	Kunci Privat dikatakan dikompromikan jika nilainya telah diungkapkan kepada orang yang tidak berkepentingan, orang yang tidak sah memiliki akses ke sana, atau ada praktek teknis yang memungkinkan orang yang tidak berwenang mendapatkan nilainya A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value
Key Generation Ceremony 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 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 Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Kunci Privat Private Key	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key
Kunci Publik Public Key	Kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Pribadi terkait dan yang digunakan oleh Pihak yang Mengandalkan untuk memverifikasi Tanda Tangan Digital yang dibuat dengan Kunci Pribadi dan / atau untuk mengenkripsi pesan pemiliknya sehingga dapat didekripsi hanya dengan Private Key yang sesuai The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key