PERURI CA	Nomor	:	01/005/CA/2018
	Mulai Berlaku	:	23 November 2018
	Versi	:	3.0
	Tanggal Perubahan	:	21 Januari 2020
	OID	:	2.16.360.1.1.1.3.12.3.2
	Klasifikasi	:	Biasa

Peruri CA
Certificate Practice Statement

Disetujui Oleh / Approved By:

Policy Authority

CATATAN REVISI / REVISION NOTE

NO	TANGGAL / DATE	VERSI / VERSION	DESKRIPSI / DESCRIPTION	OLEH / BY
1	*23 November 2018*	1.0	*Initial Release*	*CA Organization*
2	*14 December 2018*	1.1	*Minor Update:* - *Revise statement in section 1.4* - *Revise statement in section 9.16.5* - *Cosmetics change*	*CA Organization*
3	*16 January 2019*	1.2	*Minor Update:* - *Revise statement in section 1.4.1* - *Add section 5.6.1* - *Cosmetics change*	*CA Organization*
4	*13 February 2019*	1.3	*Minor Update:* - *Root CA Indonesia Alignment* - *Bilingual Bahasa Indonesia*	*CA Organization*
5	*6 May 2019*	2.0	*Major Update:* - *Footer* - *Writing Format* - *CRL Interval* - *Limitation of Peruri CA Responsibility* - *Point 4.12.1, 4.9.7, 6.1.2, 6.2.1, 6.2.5, and 9.81*	*CA Organization*
6	*10 July 2019*	2.1	*Minor Update:* - *CRL Interval (Point 4.9.7)*	*CA Organization*
7	*6 March 2020*	2.2	*Minor Update:* - *Archive retention period* - *Authentication of Individual Identity*	*CA Organization*
8	*10 October 2020*	2.3	*Minor Update:* - *Alignment Webtrust For CA*	*CA Organization*
9	*21 January 2021*	3.0	*Major Update:* - *Change of document number from 002/KRC/KBJ/CPS/XII/2018 to 01/005/CA/2018* - *Improvements for Ministry of Communications and Informatics (Kominfo) Audit Findings*	*CA Organization*

DAFTAR ISI / TABLE OF CONTENTS

1. PENDAHULUAN / INTRODUCTION

1.1. RINGKASAN / OVERVIEW

Infrastruktur Kunci Publik (IKP) Peruri adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikat Elektronik (PSrE) Induk Indonesia. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk Indonesia. Peruri CA merupakan PSrE non-Instansi di bawah PSrE Induk Indonesia. CPS ini diatur oleh CP Peruri CA.

Peruri CA's Public Key Infrastructure is a hierarchical PKI with the trust chain starting from the Root CA Indonesia. Ministry of Communication and Information Technology, Republic of Indonesia (MCIT) operates Root CA Indonesia. Peruri is a non-Government CA under Root CA Indonesia. This CPS is governed by the Peruri CA's CP.

CPS ini mendefinisikan persyaratan prosedural dan operasional yang dianut oleh Peruri CA saat menerbitkan dan mengelola objek yang ditandatangani secara digital dalam lingkungan IKP Peruri CA. CPS ini juga sesuai dengan kebijakan versi terbaru dari kebijakan Kominfo.

This CPS defines the procedural and operational requirements that Peruri adheres to when issuing and managing digitally signed objects within Peruri CA's Public Key Infrastructure. This CPS also comply with the current version of Root CA Indonesia policies.

CPS ini sesuai dengan standar *Request for Comments* 3647 (RFC 3647) dari *Internet Engineering Task Force* (IETF) tentang Internet X.509 versi 3 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework*.

This CPS is consistent with Request for Comments 3647 (RFC 3647) of the Internet Engineering Task Force (IET) Internet X.509 version 3 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

1.2. IDENTIFIKASI DAN NAMA DOKUMEN / DOCUMENT NAME AND IDENTIFICATION

Dokumen ini adalah Dokumen *Certification Practice* Statement (CPS) Peruri CA. *Object Identifier* (OID) yang digunakan untuk sertifikat (tidak termasuk *Extended Validation Certificate*) ini adalah: 2.16.360.1.1.1.3.12.3.2

This document is Certification Practice Statement Peruri CA. Object Identifier (OID) value used for certificate (not include EV certificate) for this CPS is: 2.16.360.1.1.1.3.12.3.2

OID	Penggunaan / Usage
2.16.360.1.1.1.3.12.3.1	CP
2.16.360.1.1.1.3.12.3.2	CPS
2.16.360.1.1.1.3.12.3.3.3	Peruri CA Level 3
2.16.360.1.1.1.3.12.3.3.4	Peruri CA Level 4

1.3. PARTISIPAN IKP / PKI PARTICIPANTS

1.3.1. Penyelenggara Sertifikat Elektronik (PSrE) / Certification Authorities

1.3.2. PSrE Induk Indonesia / Root CA Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia. PSrE Induk menerbitkan dan mencabut Sertifikat Digital Peruri CA (PSrE Non-Instansi) berdasarkan status pengakuan yang diberikan oleh Kominfo.

Root CA Indonesia is the root CA of Indonesia PKI. Root CA Indonesia issues and revokes certificates to Peruri CA (Non-Government CA) upon authorization by Policy Authority (PA).

Peruri CA bertanggung jawab terhadap semua aspek penerbitan dan pengelolaan sertifikat, sebagaimana dirinci dalam CPS ini, termasuk:

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

Peruri CA is responsible for all aspects of the issuance and management of those Subscriber Certificates, as detailed in this CPS, including:

- *Control over the registration process,*
- *Identification and authentication process,*
- *Certificate manufacturing process,*
- *Publication of Certificates,*
- *Revocation of Certificates, and*
- *Ensuring that all aspects of the services, operations and infrastructure related to Peruri CA Certificates issued under this CPS were performed in accordance with the requirements, representations, and warranties of this CPS.*

1.3.3. Peruri CA

Peruri CA merupakan PSrE Non-Instansi yang menerbitkan sertifikat digital kepada entitas selain pemerintah. Peruri CA tidak boleh memiliki PSrE Berinduk di bawahnya.

Peruri CA is Non-government CAs that issues digital certificates to non-government entities. Peruri CA will not have further subordinate CA.

1.3.4. Otoritas Pendaftaran (RA) / Registration Authorities

Peruri CA dapat menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan Identifikasi dan autentikasi Pemilik, serta permohonan dan pencabutan sertifikat sesuai dengan yang telah didefinisikan pada CP dan dokumen terkait. Peruri CA memiliki Otoritas Registrasi (RA) sendiri di internal, dan tidak melakukan proses

Peruri CA may designate specific RAs to perform the Subscriber Identification and Authentication, and certificate request and revocation functions defined in the CP and related documents. Peruri CA has its own Registry Authority (RA) from within, and does not carry out the verification process through business partners.

verifikasi melalui mitra bisnis.

1.3.4.1. Fungsi dari RA / Function of Registration Authorities

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

- Menyusun prosedur pendaftaran untuk Pemohon sertifikat;
- Melakukan identifikasi dan otentikasi Pemohon sertifikat;
- Memulai atau meneruskan proses permohonan pembatalan sertifikat; dan
- Menyetujui permohonan untuk memperbaharui sertifikat atau pembaharuan kunci atas nama Peruri CA.

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

- *Establish enrollment procedures for end-user certificate applicants,*
- *Perform identification and authentication of certificate applicants,*
- *Initiate or pass along revocation requests for certificates, and*
- *Approve applications for certificates renewal or re-keying on behalf of Peruri CA.*

1.3.4.2. Persyaratan Khusus RA untuk Sertifikat EV SSL / RA Specific Requirement for Extended Validation SSL Certificate

Tidak ada ketentuan.

No stipulation.

1.3.5. Pemilik / Subscribers

Pemilik adalah entitas yang memohon dan berhasil mendapatkan sertifikat digital yang ditandatangani oleh Peruri CA. Pemilik berarti subjek pemegang sertifikat digital sekaligus entitas yang terikat dengan Peruri CA. Sebelum dilakukan verifikasi identitas dan diterbitkannya sertifikat, entitas disebut sebagai Pemohon.

Subscribers are entities who request and successfully acquire a digital certificate signed by Peruri CA. Subscriber refers to both the subject of the certificate and the entity which has contract agreement with the Peruri CA. Prior to verification of identity and issuance of a certificate, an entity is an Applicant.

1.3.6. Pihak Pengandal / Relying Parties

Pihak Pengandal adalah entitas yang bertindak mempercayai sertifikat dan/atau tanda tangan digital yang diterbitkan oleh Peruri CA. Pihak Pengandal harus terlebih dahulu memeriksa respon *Certificate Revocation Lists* (CRL) atau *Online Certificate Status Protocol* (OCSP) yang sesuai sebelum memanfaatkan informasi yang ada

Relying Parties are entities that act reliance on a certificate and/or digital signature issued by Peruri CA. Relying Parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

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.

A relying party is the entity that relies on the validity of the binding of the subscriber's name to the public key. The relying party is responsible for checking the status of the information in the certificate.

Pihak Pengandal menggunakan informasi dalam Sertifikat Digital untuk:

- Memeriksa tujuan penggunaan sertifikat
- Melakukan verifikasi tanda tangan digital
- Memeriksa apakah Sertifikat Digital termasuk di dalam CRL
- Penyetujuan batas tanggung jawab dan jaminan.

Relying party uses the information in the Digital Certificate to:

- *Check the intended use of the certificate*
- *Perform digital signature verification*
- *Checks whether a Digital Certificate is included in the CRL*
- *Approval of limits of liability and guarantees.*

1.3.7. Partisipan Lain / *Other Participants*

1.3.7.1. Otoritas Kebijakan (PA) / *Policy Authority*

Otoritas Kebijakan (PA) adalah entitas internal dari Peruri CA. PA mempunyai peran dan tanggung jawab sebagai berikut:

- Menetapkan Certificate Policy (CP)
- Memastikan bahwa semua aspek layanan, operasional, dan infrastruktur Peruri CA seperti yang dijelaskan dalam CPS dilakukan sesuai dengan persyaratan, representasi, dan jaminan CP.
- Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki tingkat jaminan yang kurang lebih setara.

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

- *Approves the Certificate Policy (CP)*
- *Ensures that all aspects of the Peruri CA services, operations, and infrastructure as described in the CPS are performed in accordance with the requirements, representations, and warranties of the CP.*
- *Approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance.*

1.4. KEGUNAAN SERTIFIKAT / *CERTIFICATE USAGE*

1.4.1. Penggunaan Sertifikat yang Semestinya / *Appropriate Certificate Uses*

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

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

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

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

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

a. Level 3: Sertifikat dengan Tingkat Jaminan Sedang
   Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap Data identitas yang dimiliki oleh pemerintah.
b. Level 4: Sertifikat dengan Tingkat Jaminan Tinggi
   Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap data identitas yang dimiliki oleh pemerintah dan data biometrik.

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

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

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

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

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

b. Level 4 : High Assurance Certificate

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

Improper use can result in the loss of the guarantee that Peruri CA provides to the Owner and the Dependent.

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

Sertifikat yang diterbitkan di bawah CPS ini dapat digunakan untuk tujuan yang ditentukan dalam *field key usage* dan

Certificate issued under this CPS may be used for the purposes designated in the key usage and extended key usage fields

extended key usage yang ditemukan dalam sertifikat.

found in the certificate.

1.4.2. Penggunaan Sertifikat yang Dilarang / Prohibited Certificate Uses

Sertifikat yang dikeluarkan oleh Peruri CA dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1.

Certificates issued by Peruri CA are prohibited under any use not specified in Section 1.4.1.

1.5. ADMINISTRASI KEBIJAKAN / POLICY ADMINISTRATION

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

1. Menentukan persyaratan bisnis dan kebijakan untuk menggunakan sertifikat digital dan menetapkannya dalam Certificate Policy (CP) dan perjanjian pendukung lainnya.
2. Menentukan dan menyetujui Certificate Policy. Certificate Policy disetujui oleh PA sesuai dengan proses tinjauan tahunan yang ditetapkan, termasuk tanggung jawab untuk memelihara dan melacak perubahan pada Certificate Policy.

The Policy Authority (PA) has roles and responsibilities as follows:

1. *Define the business requirements and policies for using digital certificates and specify them in the Certificate Policy (CP) and other supporting agreements.*
2. *Determine and approve the Certificate Policy. The Certificate Policy is approved by the PA according to an established annual review process, including responsibility for maintaining and tracking changes to the Certificate Policy.*

1.5.1. Organisasi Pengaturan Dokumen / Organization Administering the Document

CPS dan dokumen referensinya dikelola oleh:

This CPS and the document referenced herein are maintained by:

Email	:	policy.ca@peruri.co.id
Phone	:	+62 21 739 5000
Fax	:	+62 21 7221 156
Web	:	https://ca.peruri.co.id/ca/legal

1.5.2. Narahubung / Contact Person

Email	:	info.digital@peruri.co.id
Phone	:	+62 21 739 5000
Fax	:	+62 21 7221 1567
Web	:	https://ca.peruri.co.id/ca/legal

1.5.3. Person Determining CPS Suitability for The Policy / Personil yang Menentukan Kesesuaian CPS dengan Kebijakan

Peruri CA mempekerjakan Otoritas Kebijakan (PA) untuk memastikan kesesuaian CPS dengan CP ini dan bahwa CPS ini sejalan dengan CP Peruri CA.

Peruri CA employs a Policy Authority (PA) to ensure conformance of the CPS to this CP and that this CPS is in line with the Peruri CA's CP.

1.5.4. Prosedur Persetujuan CPS / CPS Approval Procedures

Peruri CA menyetujui CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan adendum. Otoritas Kebijakan Peruri CA menentukan apakah perubahan atas CPS ini membutuhkan pemberitahuan atau perubahan OID.

Peruri CA approves the CPS and any amendments. Amendments are made by either updating the entire CPS or by publishing an addendum. Peruri CA determines whether an amendment to this CPS requires notice or an OID change.

1.6. DEFINISI DAN AKRONIM / DEFINITIONS AND ACRONYMS

"Sertifikat" adalah dokumen yang bersifat elektronik yang memuat tanda tangan elektronik untuk mengikat Kunci Publik dan identitas.

"Certificate" *means an electronic document that uses a digital signature to bind a Public Key and an identity.*

"*OCSP Responder*" adalah aplikasi perangkat lunak online yang dioperasikan di bawah wewenang Peruri CA dan terhubung ke repositori untuk memproses status permintaan sertifikat.

"OCSP Responder" *means an online software application operated under the authority of Peruri CA and connected to its repository for processing certificate status requests.*

"*Hardware Security Module*" adalah perangkat komputasi fisik yang melindungi dan mengelola kunci digital untuk otentikasi yang kuat dan menyediakan operasi kriptografi yang sesuai dengan FIPS 140-2 Security Level 3

"Hardware Security Module" *means a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic operation that conform to FIPS 140-2 Security Level 3*

"Kunci Privat" adalah kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.

"Private Key" *means 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" adalah kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Privat terkait dan yang digunakan oleh Pihak Penghandal untuk memverifikasi Tanda Tangan Digital yang dibuat oleh

"Public Key" *means 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*

pemegangnya.

"*Pihak Pengandal*" entitas yang mempercayai pada informasi yang terkandung dalam sertifikat atau token stempel waktu.	***"Relying Party"*** *means an entity that relies upon either the information contained within a certificate or a time-stamp token.*

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

2.1. REPOSITORI / REPOSITORIES

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

Peruri CA shall operate online repositories where Policy Documents, Peruri CA's Certificates, and CRL are published.

2.2. PUBLIKASI INFORMASI SERTIFIKASI / PUBLICATION OF CERTIFICATION INFORMATION

Peruri CA memelihara repositori yang dapat diakses melalui internet yang mempublikasikan versi terakhir dari:

- Sertifikat Peruri CA,
- CRL terakhir,
- Dokumen CP/CPS,
- Perjanjian Pelanggan,
- Kebijakan Privasi

Repositori Peruri CA dapat diakses pada https://ca.peruri.co.id/ca/legal.

Peruri CA maintains a repository accessible through the Internet in which it publishes a current version of:

- *Its own CA certificates*
- *The current CRL*
- *The Certificate Policy or Certification Practice Statement document*
- *Subscriber Agreement*
- *Privacy Policy*

Peruri CA's legal repository is located at https://ca.peruri.co.id/ca/legal.

2.3. WAKTU ATAU FREKUENSI PUBLIKASI / TIME OF FREQUENCY OF PUBLICATION

Dokumen CPS dan setiap perubahan yang dilakukan harus dapat diakses secara publik dalam waktu tujuh (7) hari kalender setelah disetujui. Peruri CA harus mempublikasikan data Sertifikat Pemilik dan data pencabutan sertifikat dalam waktu 30 (tiga puluh) menit setelah penerbitan. CRL untuk Sertifikat Pemilik setidaknya diterbitkan sekali sehari.

This CPS and any subsequent changes shall be made publicly available within seven (7) calendar days after its approval. Peruri CA shall publish Subscriber's Certificates data and and revocation data within 30 (thirty) minutes after issuance. CRLs for Subscriber's Certificates are issued at least once per day.

CRL diperbaharui sesuai dengan Frekuensi Penerbitan CRL bagian 4.9.7.

The CRL is updated according to the section 4.9.7.

2.4. KENDALI AKSES PADA REPOSITORI / ACCESS CONTROLS ON REPOSITORIES

Informasi yang terpublikasi pada repositori adalah informasi publik. Peruri CA memberikan akses baca yang tidak dibatasi pada repositori. Peruri CA menerapkan kontrol terhadap informasi yang dipublikasikan pada repositori dengan menerapkan kendali logis dan

Information published on a repository is public information. Peruri CA shall provide unrestricted read access to its repositories. Peruri CA implements control over the information published in the repository, logical and physical controls to prevent unauthorized write

fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.

access to such repositories.

Peruri CA harus melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik (menambahkan, menghapus, atau mengubah entri repositori).

Peruri CA shall protect information not intended for public dissemination or modification (adding, deleting, or modifying repository entries).

3. IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION

3.1. PENAMAAN / NAMING

3.1.1. Tipe Nama / Types of Names

Peruri CA 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 Peruri CA di bawah CPS ini.

Peruri CA 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 Peruri CA under this CPS.

Tipe Sertifikat	(DN) Distinguised Name
Sertifikat Peruri CA	CN=<Peruri CA - G1>, O=<Peruri>,C=ID
Sertifikat Pemilik	CN=<nama_orang>, Email Address=<email>, OU=<unit_organisasi>, O=<nama_organisasi>, C=ID

Contoh: CN:SubPeruriCASatuDuaTiga - G1, O=PT. SubPeruriSatuDuaTiga, C=ID

Certificate Type	(DN) Distinguised Name
Peruri CA Certificate	CN=<Peruri CA - G1>,O=<Peruri>,C=ID
Subscriber Certificate	CN=<person_name>, Email Address=<email> OU=<organizational_unit>,O=<organization_name>, C=ID

Example: CN:SubPeruriCASatuDuaTiga - G1, O=PT. SubPeruriSatuDuaTiga, C=ID

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

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

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

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

The subject and issuer name contained in a certificate MUST be meaningful in the sense that the Peruri 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. Anonimitas atau Pseudonimitas Pemilik / Anonymity or Pseudonymity of Subscribers

Peruri CA tidak akan menerbitkan sertifikat pemilik yang anonim atau pseudonim.

Peruri CA does not issue end-entity anonymous or pseudonymous certificates.

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

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

Distinguished Name (DN) in Certificates are interpreted using X.500 standards.

3.1.5. Keunikan Nama / Uniqueness of Names

Distinguished Name dalam sertifikat harus unik di dalam ranah Peruri CA.

Distinguished Names in Certificates shall be unique within Peruri CA domain.

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

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. Peruri CA tidak perlu memverifikasi hak pemohon untuk penggunaan merek dagang. Merupakan tanggung jawab Pemilik untuk memastikan penggunaan nama-nama pilihan yang sah.

Subscriber may not request certificates with any content that infringes the intellectual property rights of another entity. Peruri CA is not required to verify an applicant's right to use a trademark. It is the sole responsibility of the subscriber to ensure lawful use of chosen names.

Peruri CA dapat menolak setiap permohonan atau melakukan pencabutan sertifikat apapun yang menjadi bagian dari sengketa merek dagang.

Peruri CA may reject any application or require revocation of any certificate that is part of a trademark dispute.

3.2. VALIDASI IDENTITAS AWAL / INITIAL IDENTITY VALIDATION

Peruri CA dapat menggunakan sarana komunikasi atau penelidikan hukum apa pun untuk memastikan identitas pemohon baik itu organisasi atau individu. Peruri CA dapat menolak untuk mengeluarkan sertifikat atas kebijakannya sendiri.

Peruri CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual applicant. Peruri CA may refuse to issue a certificate in its sole discretion.

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

Metode untuk membuktikan kepemilikan kunci privat harus menggunakan PKCS#10, atau permintaan lain yang ekuivalen secara kriptografi (permintaan ditandatangani secara digital dengan kunci privat).

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

- Pemilik menyerahkan kunci publik
- *Subscribers submit public key*

- Pemilik menyerahkan CSR secara *offline*

- *Subscribers submit CSR offline*

3.2.2. Autentikasi Identitas Organisasi / Authentication of Organization Identity

Peruri CA memverifikasi keberadaan organisasi dan identitas pemohon menggunakan pihak ketiga dan pemerintah (jika diperlukan) atau melalui sarana komunikasi langsung lainnya dengan entitas yang mengatur penciptaan, keberadaan atau pengakuan hukum keorganisasian. Jika upaya semacam itu tidak cukup, maka organisasi menyerahkan dokumen resmi perusahaan seperti izin usaha, sertifikat pajak, piagam perusahaan, surat resmi atau dokumen terkait lainnya.

Peruri CA verifies the organizational existence and identity of applicants using reliable third party and government databases (if necessary) or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition. If such efforts are insufficient to submit official company documentation, such as a business license, tax certificate, corporate charter, official letter or other relevant documents

Peruri CA menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi selama masa berlaku sertifikat yang diterbitkan.

Peruri CA keeps 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.

Persyaratan identifikasi dan autentikasi untuk suatu organisasi:

a. Izin usaha (SIUP)
b. Sertifikat Pajak (NPWP)
c. Piagam perusahaan (Akta Pendirian)
d. Surat resmi atau
e. Dokumen terkait lainnya

Identification and authentication requirements for an organization:

a. Business Licence
b. Tax certificate
c. Corporate charter
d. Official letter
e. Another relevant document

3.2.3. Autentikasi Identitas Individu / Authentication of Individual Identity

Sebuah permohonan untuk individu menjadi Pemilik hanya dapat dibuat oleh individu tersebut atau organisasi yang secara hukum berwenang untuk bertindak atas nama calon pemohon.

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

Untuk menjadi pemilik dapat dilakukan oleh organisasi yang berwenang secara hukum untuk bertindak atas nama calon pemilik setelah mereka mengisi formulir yang sesuai dan mengikuti proses dan prosedur yang ditetapkan. Untuk tujuan identifikasi dan otentikasi harus:

1. Memberikan salinan identitas resmi yang dikeluarkan oleh pemerintah
2. Memberikan salinan identitas resmi

Becoming an owner may be undertaken by an organization that is legally authorized to act on behalf of the prospective owner after they have filled out the appropriate forms and followed established processes and procedures. For the purpose of identification and authentication of the individual shall:

1. Give copy of the official identity issued by the government
2. Show the official identity issued by

yang dikeluarkan oleh perusahaan
3. Alamat email
4. Nomor handphone
5. Jawaban atas pertanyaan keamanan (security question)
6. Data biometrik

the company
3. Email address
4. Cell Phone number
5. Answer to security questions (security question)
6. Biometric data

Peruri CA menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi selama masa berlaku sertifikat yang diterbitkan.

Peruri CA keeps a record of the type and details of identification used for the authentication of the individual for at least the life of the issued certificate.

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

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. Validasi Otoritas / Validation of Authority

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

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

Sertifikat yang mencantumkan afiliasi organisasi yang eksplisit atau implisit harus diterbitkan hanya setelah memastikan pemohon memiliki otorisasi untuk bertindak atas nama organisasi dalam kapasitas yang dinyatakan dengan tegas.

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

3.2.6. Kriteria Inter-operasi / Criteria for Interoperation

Tidak ada ketentuan.

No stipulation.

3.3. IDENTIFIKASI DAN AUTENTIKASI UNTUK PERMINTAAN PENGGANTIAN KUNCI (RE-KEY) / IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identifikasi dan Autentifikasi untuk Kegiatan Penggantian Kunci / Identification and Authentication for Routine Re-Key

Sebelum masa berlaku sertifikat habis, Pemilik tidak dapat meminta penggantian kunci karena Peruri CA tidak melayani penggantian kunci sertifikat Pemilik.

Prior to the expiry of a certificate, Subscribers does not allowed to request for a re-key because Peruri CA does not provide routine Re-key.

3.3.2. Identifikasi dan Autentifiasi untuk Penggantian Kunci setelah Pencabutan / Identification and Authentication for Re-Key after Revocation

Setelah sertifikat dicabut selain karena alasan pambaruan, Pemilik harus mengulang proses permohonan 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. IDENTIFIKASI DAN OTENTIKASI UNTUK PERMINTAAN PENCABUTAN / IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

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.

Pencabutan sertifikat harus memenuhi salah satu dari proses berikut:

- Pencabutan yang dilakukan secara luring; atau
- Pencabutan yang dilakukan secara daring.

A certificate revoke shall be achieved using one of the following processes:

- *Offline revocation; or*
- *Online Revocation.*

Prosedur bagaimana permintaan pencabutan dapat diajukan dijelaskan di bagian 4.9.3.

The procedure of how the revocation request can be submitted is described in section 4.9.3.

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

4.1. PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION

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

Hanya pemohon dari individu / perwakilan individu / entitas / yang memiliki identitas yang dapat diverifikasi, dan telah menyetujui syarat dan ketentuan Peruri CA yang dapat mengajukan permohonan sertifikat. Pemohon harus memberikan informasi yang cukup sehingga memungkinkan Peruri CA untuk melakukan verifikasi atas identitas tersebut. Pemohon harus menyetujui kontrak berlangganan yang ditetapkan oleh Peruri CA sebelum melakukan pendaftaran

Only applicants from individuals / representatives of individuals / entities / who have a verifiable identity, and have agreed to the CA Peruri terms and conditions can apply for a certificate. The applicant must provide sufficient information to allow the Peruri CA to verify the identity. The applicant must agree to the subscription contract stipulated by Peruri CA before registering.

4.1.2. Proses Pendaftaran dan Tanggung Jawabnya / Enrollment Process and Responsibilities

Pemohon Sertifikat Kunci Publik harus bertanggung jawab untuk menyediakan informasi yang akurat dalam permohonan sertifikat mereka. Peruri CA bertanggung jawab untuk memproses pendaftaran dengan langkah-langkah berikut:

1. Peruri CA akan mengirimkan formulir Permohonan Pendaftaran Sertifikat kepada pemohon,
2. Peruri CA membangkitkan pasangan kunci sesuai dengan menggunakan *platform* yang layak dan aman jika pemohon telah lolos dari proses verifikasi,
3. Peruri CA memberikan Pasangan Kunci kepada pemohon / pemilik,
4. Peruri CA memastikan bahwa pemohon telah menyetujui Kontrak Berlangganan yang berlaku,
5. Pemohon / Pemilik wajib membayar biaya yang berlaku sesuai dengan Kontrak Berlangganan.

Applicants for Public Key Certificates shall be responsible for providing accurate information in their applications for certification. Peruri CA responsible to process the enrollments with these steps:

1. *Peruri CA will send a Certificate Registration Application form to the applicant,*
2. *Peruri CA generates a suitable key pair using a proper and secure platform if the applicant has passed the verification process,*
3. *Peruri CA assigns a Key Pair to the applicant / owner,*
4. *Peruri CA ensures that the applicant has agreed to the applicable Subscription Contract,*
5. *The Applicant / Owner is required to pay the applicable fees in accordance with the Subscription Contract.*

4.2. PEMROSESAN PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION PROCESSING

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

Identifikasi dan otentikasi Pemilik harus memenuhi persyaratan yang ditentukan untuk otentikasi pemilik sebagaimana dalam CPS bagian 3.2.

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 of this CPS.

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

Setelah semua pemeriksaan identitas dan atribut pemohon, konten permohonan untuk sertifikat juga diperiksa. Dalam hal pemohon tidak memenuhi syarat untuk sertifikat atau permohonannya mengandung kesalahan, maka Peruri CA harus menolak permohonan tersebut. Apabila tidak ada masalah, maka 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 error, Peruri CA shall reject the application. Otherwise the application is approved.

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

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

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

Peruri CA akan menyelesaikan proses validasi dan menerbitkan atau menolak permintaan sertifikat tidak lebih dari tiga (3) hari kerja setelah menerima semua rincian dan dokumen yang diperlukan dari Pemohon, meskipun peristiwa di luar kendali Peruri CA dapat menunda proses penerbitan.

Peruri CA will usually complete the validation process and issue or reject a certificate application no more than three working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of Peruri CA can delay the issuance process.

4.3. PENERBITAN SERTIFIKAT / CERTIFICATE ISSUANCE

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

Peruri CA memverifikasi sumber permohonan sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan bahwa semua *field* dan ekstensi telah diisi dengan benar.	*Peruri CA verifies the source of a Certificate Request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.*

Peruri CA melakukan otentikasi permohonan sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membangitkan sertifikat, dan menyediakan sertifikat kepada Pemohon. Peruri CA mempublikasikan sertifikat ke suatu repositori sesuai dengan CP dan CPS terkait. Semua hal ini harus dilaksanakan secara tepat waktu sesuai dengan uraian pada bagian 4.2.	*Peruri CA authenticate a Certificate Request, ensure that the Public Key is bound to the correct Applicant, obtain a proof of possession of the Private Key, then generate a Certificate, and provide the Certificate to the Applicant. Peruri CA publish the Certificate to a repository in accordance with this CP and the applicable CPS. This is done in a timely manner, which is detailed in section 4.2.*
● Peruri CA memeriksa dokumen	● *Peruri CA check documents*
● Setelah ditandatangani, sertifikat digital akan diserahkan kepada Pemilik	● After signed, digital certificate will be handed over to Subscriber

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

Peruri CA memberitahu Pemilik dalam waktu maksimal tujuh (7) hari kerja tentang penerbitan sertifikat melalui email.	*Peruri CA notify the Subscriber within a maximum seven (7) days of successful certificate issuance via email.*

4.4. PENERIMAAN SERTIFIKAT / CERTIFICATE ACCEPTANCE

4.4.1. Sikap yang Dianggap sebagai Menerima Sertifikat / Conduct Constituting Certificate Acceptance

Pemilik harus memeriksa semua informasi tentang Sertifikat dan menandatangani formulir penerimaan sertifikat digital sebelum menggunakan sertifikat tersebut. Peruri CA harus memberitahu ke Pemilik bahwa mereka tidak dapat menggunakan sertifikat sebelum dilakukan pemeriksaan semua informasi dari sertifikat.	*Subscriber should check all information of certificate and sign digital certificate acceptance form before using the certificate. Peruri CA shall notify the Subscriber that they cannot use the certificate before checking all the information of the certificate.*
Bila tidak ada keluhan dari Pemilik dalam waktu tujuh (7) hari kerja, Pemilik dianggap menerima semua informasi sertifikat.	*When there is no complaint from Subscriber within seven (7) working days, the Subscriber is deemed to accept all certificate information.*
Dalam hal penerbitan Sertifikat PSrE, Peruri CA harus membuat prosedur penerimaan dan mendokumentasikan penerimaan Sertifikat PSrE yang terbitkan.	*For the issuance of CA Certificates Peruri CA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.*

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

Peruri CA harus mempublikasikan Sertifikatnya dalam sebuah repositori sebagaimana tercantum pada bagian 2.2 segera setelah sertifikat diterbitkan, termasuk ketika menerbitkan informasi pencabutan terkait Sertifikat tersebut pada repositori. Peruri CA harus mempublikasikan sertifikat Pengguna Akhir dengan mengirimkannya ke Pemilik sertifikat.

Peruri CA shall publish certificates in a repository as stated in section 2.2 as soon as they are issued, as well as revocation information concerning such certificates in a repository. Peruri CA shall publish the end-user certificate by sending it to the certificate owner.

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

Tidak ada ketentuan.

No stipulation.

4.5. PASANGAN KUNCI DAN PENGGUNAAN SERTIFIKAT / KEY PAIR AND CERTIFICATE USAGE

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

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

Pihak Pengandal harus menggunakan perangkat lunak yang sesuai dengan X.509. Peruri CA harus menentukan batasan penggunaan sertifikat melalui ekstensi sertifikat dan harus membuat mekanisme untuk menentukan validitas sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan memahami informasi ini sesuai dengan kewajiban mereka sebagai Pihak Pengandal.

Relying Parties shall use software that is compliant with X.509. Peruri CA shall specify restrictions on the use of a certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP). Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties.

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

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. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the certificate.

4.6. PEMBAHARUAN SERTIFIKAT / CERTIFICATE RENEWAL

4.6.1. Kondisi untuk Pembaharuan Sertifikat / Circumstance for Certificate Renewal

Peruri CA dapat memperbarui Sertifikat Pemilik 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.
- Peruri CA dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya
- Berisi informasi yang sama (identitas, domain, dll.) Seperti sertifikat lama
- Memiliki periode validitas baru yang berakhir setelah periode validitas sertifikat lama
- Berisi kunci publik yang sama dengan sertifikat lama

Selain itu, periode validitas tidak boleh melebihi masa berlaku Kunci Privat, sebagaimana ditentukan dalam bagian 5.6. Persyaratan pemeriksaan identitas yang tercantum dalam bagian 3.3.1 juga harus dipenuhi. Pembaharuan / perpanjangan dikenakan biaya tambahan

Peruri CA may renew a Subscriber 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.*
- *Peruri CA may renew Certificates which have either been previously renewed.*
- *Contains the same information (identity, domain, etc.) as the old certificate.*
- *Has a new validity period which ends after the old certificate validity period.*
- *Contains the same public key as the old certificate.*

In addition, the validity period of the Certificate must not exceed the remaining lifetime of the Private Key, as specified in Section 5.6. The identity proofing requirement listed in Section 3.3.1 shall also be met.

4.6.2. Siapa yang Dapat Meminta Pembaharuan / Who May Request Renewal

Pemilik yang belum pernah dicabut sertifikatnya boleh meminta pembaruan Sertifikatnya ke Peruri CA.

The Subscriber which have never been revoked may request the renewal of its Certificate to Peruri CA

4.6.3. Pemrosesan Permintaan Pembaharuan Sertifikat / Processing Certificate Renewal Requests

Perpanjangan sertifikat harus memenuhi salah satu dari proses berikut:

- Proses pendaftaran awal seperti yang dijelaskan pada bagian 3.2; atau
- Identifikasi dan otentikasi untuk penggantian kunci sebagaimana dijelaskan pada bagian 3.3, kecuali kunci lama juga dapat digunakan sebagai kunci baru.

A certificate renewal shall be achieved using one of the following processes:

- *Initial registration process as described in Section 3.2; or*
- *Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.*

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

Prosedur pemberitahuan penerbitan sertifikat baru sama seperti 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. Sikap yang Dianggap sebagai Menerima Sertifikat yang Diperbaharui / Conduct constituting acceptance of a renewal certificate

Pemilik harus menerima sertifikat yang diperbaharui mengikuti prosedur penerimaan dan penerimaan sertifikat yang sama, sebagaimana 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. Publikasi Sertifikat yang Diperbaharui oleh PSrE / Publication of the renewal certificate by the CA

Sertifikat baru diterbitkan sesuai prosedur yang dinyatakan dalam bagian 4.4.2.

The new certificate is published according the procedures stated in section 4.4.2

4.6.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain / Notification of certificate issuance by the CA to other entities

RA (*Registration Authority*) dapat menerima pemberitahuan tentang pembaharuan sertifikat bila RA terlibat dalam proses penerbitan.

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7. PENGGANTIAN KUNCI SERTIFIKAT / CERTIFICATE RE-KEY

Penggantian kunci sertifikat adalah penerbitan kembali sertifikat menggunakan informasi subjek dan tanggal kedaluwarsa ("validTo" field) yang sama tetapi dengan pasangan kunci yang baru. Namun, Peruri CA tidak melakukan penggantian kunci sertifikat Pemilik.

Certificate re-key is the re-issuance of a certificate using the same subject information and expiration date ("validTo" field) but with a new key pair. However, Peruri CA does not re-key from key subscriber.

4.7.1. Kondisi untuk Penggantian Kunci / Circumstance for Certificate Re-Key

Penggantian kunci (*re-key*) sertifikat adalah penerbitan ulang suatu sertifikat yang memakai informasi subyek dan tanggal kadaluarsa yang sama (*field "validTo"*) namun dengan pasangan kunci yang baru.

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.

Peruri CA dapat melakukan penggantian kunci selama:

- Sertifikat asli yang diganti belum pernah dibatalkan/dicabut;
- Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun;
- Seluruh rincian yang terkait dengan Sertifikat tersebut tetap akurat dan tidak dibutuhkan validasi baru dan tambahan; dan
- Kunci Privat Peruri CA bocor.

Peruri 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.*
- *Peruri CA private key compromise.*

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

Sesuai dengan kondisi yang ditentukan pada bagian 4.7.1, hanya Peruri CA yang dapat meminta dan melakukan penggantian kunci publik yang baru

According to the conditions specified in section 4.7.1, only CA Peruri may request and perform a new public key replacement

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

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

Sertifikat baru diterbitkan sesuai prosedur yang dinyatakan dalam bagian 4.3.2.

The new certificate is published according the procedures stated in section 4.3.2

4.7.5. Melaksanakan Penerimaan Sertifikat dari Penggantian Kunci / Conduct Constituting Acceptance of a Re-Keyed Certificate

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. Publikasi Sertifikat Penggantian Kunci oleh PSrE / Publication of the Re-Keyed Certificate by the CA

Sertifikat dengan Kunci Baru dipublikasikan, sesuai dengan prosedur repositori, sebagaimana yang dinyatakan pada 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. Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain / Notification of Certificate Issuance by the CA to Other Entities

Tidak ada ketentuan.

No Stipulation.

4.8. MODIFIKASI SERTIFIKAT / CERTIFICATE MODIFICATION

Modifikasi / mengubah detail dari Sertifikasi tidak diizinkan. Jika terjadi kesalahan selama penerbitan Sertifikat (contoh: ejaan), sertifikat dicabut dan dilakukan Proses Penerbitan Penggantian Kunci sebagaimana 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-issue issuance process is followed, as stated in section 4.3.

4.8.1. Kondisi untuk Modifikasi Sertifikat / Circumstance for Certificate Modification

Modifikasi / mengubah informasi pada sertifikat tidak diizinkan.

Modification of certificate information is not permitted.

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

Tidak ada ketentuan.

No stipulation.

4.8.3. Pemrosesan Permintaan Modifikasi Sertifikat / Processing Certificate Modification Requests

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

4.8.5. Melakukan Penerimaan Sertifikat yang Dimodifikasi / Conduct Constituting Acceptance of Modified Certificate

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

4.9. PENCABUTAN DAN PEMBEKUAN SERTIFIKAT / CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Keadaan untuk Pencabutan / Circumstances for Revocation

Peruri CA harus mencabut sertifikat pemilik dalam keadaan berikut:

- Mengidentifikasi informasi atau komponen afiliasi dari setiap nama di dalam Sertifikat menjadi tidak valid.
- Setiap informasi dalam Sertifikat menjadi tidak valid.
- Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya.
- Ada alasan untuk meyakini bahwa Kunci Privat telah bocor.

Peruri CA 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.*

- Pemilik atau pihak lain yang berwenang (sesuai ketentuan pada CPS) meminta agar sertifikatnya dicabut.
- Peruri CA berhenti beroperasi.
- Sertifikat yang dibuat untuk uji coba.

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

- *The subscriber or other authorized party (as defined in the CPS) asks for its certificate to be revoked.*
- *Peruri CA termination.*
- *The certificate is issued for trial run.*

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. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

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

Sertifikat dapat diminta untuk dicabut oleh PSrE Penerbit atau entitas lainnya (yang dapat membuktikan adanya penyalahgunaan sertifikat sesuai dengan Certification Policy).

The certificate can be requested to be revoked by the Issuing CA or by another entity (that can prove the misuse of the certificate according to the Certification Policy).

4.9.3. Prosedur Permintaan Pencabutan / Procedure for Revocation Request

Peruri CA memverifikasi identitas dan kewenangan (untuk entitas penegak hukum) yang meminta pencabutan. Validasi identitas pemilik diperlukan sesuai dengan bagian 3.4.

Permohonan untuk pencabutan oleh entitas lain harus ada penyampaian bukti bahwa:

a. Kunci Privat dari Sertifikat telah terungkap,
b. Penggunaan Sertifikat tidak sesuai dengan Certification Policy (CP),
c. Pemilik Sertifikat tidak memiliki hubungan dengan institusi.

Peruri CA verifies the identity and authority (for juridical entity) whom makes 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.

4.9.4. Revocation Request Grace Period / Masa Tenggang Permintaan Pencabutan

Tidak ada tenggang waktu yang diizinkan setelah permintaan pencabutan terverifikasi. Peruri CA akan mencabut sertifikat segera setelah proses verifikasi permintaan pencabutan dilaksanakan.

No grace period is permitted once a revocation request has been verified. Peruri CA will revoke certificates as soon as reasonably practical following verification of a revocation request.

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

Peruri CA harus memulai penyelidikan permintaan pencabutan dalam waktu satu (1) hari kerja kecuali pada kasus *Force Majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang memadai akan segera diproses.

Peruri CA must start the investigation of revocation requests within one (1) working day except from force majeure cases. Revocation requests that provide adequate supporting evidence will be processed immediately.

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

Pihak Pengandal harus memvalidasi setiap sertifikat yang diberikan terhadap CRL yang terbaru yang berada di Peruri CA.

Relying parties should validate any presented certificate against the most updated CRL, which are hosted on Peruri CA.

Pihak Pengandal harus memvalidasi sertifikat terhadap server OCSP yang disediakan oleh Peruri CA sesuai dengan CPS Bagian 4.9.9.

Relying parties should validate any presented certificate against the relevant issuer's OCSP server.

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

CRL harus diperbarui dan dipublikasi:

- Untuk sertifikat *end-user*/perangkat, paling sedikit setiap 24 jam. CRL akan berdampak dalam waktu maksimum satu (1) hari kerja.

The CRL must be updated and published:

- *For end-user/device certificates, at least every 24 hours. The CRL will be in effect for a maximum time of one (1) working days.*

CRL disimpan dan dilindungi untuk menjamin integritas dan keotentikannya.

CRLs shall be stored in a protected environment in order to ensure their integrity and authenticity.

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

Setelah pencabutan sertifikat, CRL dikeluarkan dan repositori diperbaharui. CRL diterbitkan di repositori dalam beberapa menit setelah diterbitkan. Sertifikat ditandai sebagai "dicabut" dalam repositori.

After a certificate revocation, the CRL is issued and the repository is updated. The CRL is published at the Repository within minutes of its issuance. The certificate is marked as revoked in the Repository.

Peruri CA akan mengoperasikan CRL dan OCSP-nya dengan cara yang handal untuk memberikan respon selama sepuluh (10) detik atau kurang dalam kondisi operasional yang normal.

Peruri CA will operate and maintain its CRL and OCSP capability with reliable resources to provide a response time of ten (10) seconds or less under normal operating conditions.

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

Peruri CA memberikan layanan validasi daring. Jika validasi daring tersedia, diharapkan melakukan pengecekan menggunakan Server OCSP yang disediakan.	*Peruri CA provides online validation services. If online validation is available, it is expected to check using the provided OCSP Server.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

4.9.12. Persyaratan Khusus Keterpaparan Penggantian Kunci / Special Requirements Re-Key Compromise

Tidak ada ketentuan.	*No stipulation.*

4.9.13. Kondisi untuk Pembekuan / Circumstances for Suspension

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

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

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

4.9.15. Prosedur untuk Permintaan Pembekuan / Procedure for Suspension Request

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

4.9.16. Batas Masa Pembekuan / Limits on Suspension Period

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

4.10. LAYANAN STATUS SERTIFIKAT / CERTIFICATE STATUS SERVICES

4.10.1. Karakteristik Operasional / Operational Characteristics

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. Ketersediaan Layanan / Service Availability

Peruri CA melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status sertifikat.	*Peruri CA performs all the necessary actions for the uninterruptible - as possible - availability of its certificate status validation service.*

4.10.3. Optional Features / Fitur Opsional

Tidak ada ketentuan.	*No stipulation.*

4.11. AKHIR BERLANGGANAN / END OF SUBSCRIPTION

Pemilik dapat mengakhiri langganan dengan membiarkan sertifikatnya kadaluarsa atau mencabut sertifikatnya tanpa meminta sertifikat yang baru. Terdapat prosedur pencabutan sertifikat pada Peruri CA.	*Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate. There is a certificate revocation procedure at Peruri CA.*

4.12. PEMULIHAN DAN PENITIPAN KUNCI / ESCROW AND RECOVERY

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

Kunci privat Pemilik dapat dititipkan pada Peruri CA atau disimpan sendiri atas persetujuan Pemilik Kunci.	*Subscriber's private key can be escrowed to Peruri CA or Subscriber with permission from the Subscriber.*

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

Tidak ada ketentuan.	*No stipulation.*

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

5.1. KENDALI FISIK / PHYSICAL CONTROLS

5.1.1. Lokasi dan Konstruksi / Site Location and Construction

Lokasi dan konstruksi dari fasilitas penempatan peralatan Peruri CA maupun situs tempat *workstation* yang digunakan untuk mengelola Peruri CA, harus konsisten dengan fasilitas yang digunakan untuk menampung informasi yang bernilai tinggi dan sensitif. Lokasi dan konstruksi situs, 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 Peruri CA.

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

5.1.2. Akses Fisik / Physical Access

Peralatan Peruri CA selalu terlindungi dari akses yang tidak resmi. Mekanisme keamanan fisik untuk Peruri CA telah diimplementasikan untuk:

- Memastikan tidak ada akses tidak resmi yang diizinkan ke perangkat keras.
- Menyimpan semua media dan kertas yang dapat dilepas yang berisi informasi teks biasa yang sensitif dalam tempat yang aman.
- Monitor, baik secara manual maupun elektronik, untuk gangguan yang tidak sah setiap saat.
- Menjaga dan memeriksa log akses secara berkala.

Semua operasional Peruri CA yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan memiliki setidaknya empat lapis keamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif.

The Peruri CA equipments are always be protected from unauthorized access. The physical security mechanisms Peruri CA has been implemented 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. Listrik dan AC / Power and Air Conditioning

Peruri CA memiliki daya cadangan yang cukup untuk mengunci masukan secara otomatis, menyelesaikan setiap tindakan yang tertunda, dan merekam status peralatan sebelum kekurangan daya atau AC yang menyebabkan peralatan mati. Repositori IKP telah dilengkapi dengan Daya Tak Terputus dan Generator Listrik yang cukup untuk pengoperasian paling sedikit 6 (enam) jam saat tidak adanya daya komersial, untuk mendukung keberlangsungan operasional.	*Peruri CA has 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 has been provided with Uninterrupted Power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to support continuity of operations.*

5.1.4. Keterpaparan Air / Water Exposures

Peralatan Peruri CA ditempatkan pada tempat yang tidak terpapar air.	*The Peruri CA equipment installed in a place where there is no danger of exposure to water.*
Paparan air untuk pencegahan kebakaran dan tindakan perlindungan (misalnya sistem *sprinkler*) dikecualikan dari persyaratan ini.	*Water exposures from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.*

5.1.5. Pencegahan dan Perlindungan Kebakaran / Fire Prevention and Protection

Peralatan Peruri CA ditempatkan di fasilitas dengan sistem deteksi dan pemadaman kebakaran yang memadai.	*The Peruri CA equipment were housed in a facility with appropriate fire suppression and protection systems.*

5.1.6. Media Storage / Media Penyimpanan

Media Peruri CA disimpan sehingga bisa melindunginya dari kerusakan akibat kecelakaan (air, api, elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau *backup* diduplikasi dan disimpan di lokasi yang terpisah dari lokasi Peruri CA.	*Peruri CA's media were stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media containing audit, archive, or backup information were duplicated and stored in a location separate from the Peruri CA location.*

5.1.7. Pembuangan Limbah / Waste Disposal

Bahan limbah yang sensitive dibuang dengan cara yang aman.	*Sensitive waste material shall be disposed of in a secure fashion.*

5.1.8. Backup Off-Site / Off-Site Backup

Backup sistem dari Peruri CA cukup untuk memulihkan kegagalan sistem, yang dilakukan secara berkala dan telah dijelaskan pada Peruri CA - CPS. *Backup* data dilakukan dan disimpan diluar lokasi	*System backups of the Peruri CA, sufficient to recover from system failure, shall be made on a periodic schedule, described in the Peruri CA - CPS. Backups shall be performed and stored offsite not*

tidak kurang dari sekali setiap tujuh (7) hari. Setidaknya satu salinan *backup* lengkap disimpan di lokasi luar kantor (di lokasi terpisah dari peralatan Peruri CA). Hanya *backup* lengkap terbaru yang perlu dipertahankan. Data *backup* dilindungi dengan kendali fisik dan kontrol prosedur.

Backup semua sistem dari Peruri CA, yang cukup untuk pulih dari kegagalan sistem, telah dilakukan dengan jadwal berkala dan disimpan di lokasi yang aman dan *offsite* (di lokasi yang terpisah dari peralatan Peruri CA).

less than once every seven (7) days. At least one (1) full backup copy shall be stored at an offsite location (at a location separate from the Peruri CA equipment). Only the latest full backup need be retained. The backup data shall be protected with physical and procedural controls.

System backups of the Peruri CA, sufficient to recover from system failure, shall be made on a periodic schedule and stored at a secure, offsite location (at a location separate from the Peruri CA equipment).

5.2. KENDALI PROSEDUR / PROCEDURAL CONTROLS

5.2.1. Peran yang Dipercaya / Trusted Roles

Peran-peran terpercaya meliputi:

- Koordinator
  Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan Peruri CA.
- *Policy Authority Officer (Compliance Officer)*
  Pembuatan atau revisi *Certificate Policy* dan *Certification Practice Statement.*
- *Network and Security Unit Manager*
  Menjaga seluruh fasilitas termasuk namun tidak terbatas pada barang, orang, fasilitas, perangkat IKP milik Peruri CA.
- *Internal Auditor*
  Melakukan audit internal operasional PSrE.
- *Certification Authority Unit Manager / Key Custodian*
  Pembuatan dan pencabutan pasangan kunci Peruri CA.
- *Administrator of CA Unit Application (CA)*
  Akses sistem CA, persetujuan siklus penerbitan sertifikat, pencabutan dan penangguhan sertifikat.
- *Administrator of Service Unit Application (RA)*
  Akses dan manajemen Sistem RA,

Trusted roles including:

- *Head*
  Overall responsibility for administering the implementation of the Peruri CA's security practices
- *Policy Authority Officer (Compliance Officer)*
  Establishment or revision of Certificate Policy and Certification Practice Statement.
- *Network and Security Unit Manager*
  Maintain all facilities including but not limited to goods, people, facilities, PKI equipment belonging to Peruri CA.
- *Internal Auditor*
  Conduct internal audit of CA Operational.
- *Certification Authority Unit Manager / Key Custodian*
  Generation and revocation of Peruri CA key pairs.
- *Administrator of CA Unit Application (CA)*
  CA System access, Certificate Lifecycle management approval of the generation, revocation and suspension of certificates.
- *Administrator of Service Unit Application (RA)*
  RA System accesses and

Persetujuan untuk identifikasi dilakukan oleh *Validation Specialist*.

- *Validation Specialist*
  Identifikasi Pengguna dan verifikasi dokumen.
- *Repository (WEB)*
  Manajemen halaman WEB, publikasi.
- *System Administrator PKI*
  Pengembangan CA / RA / OCSP dan sistem terkait lainnya.
- *Administrator of Operation and Maintenance Unit Application*
  Operasi sehari-hari sistem Peruri CA dan pencadangan serta pemulihan sistem.

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

management, LRA management, Approval for identification conducted by Validation Specialist.

- *Validation Specialist*
  User Identification and documents verification.
- *Repository (WEB)*
  WEB pages management, publication.
- *System Administrator PKI*
  Development CA/RA/OCSP and other relevant systems.
- *Administrator of Operation and Maintenance Unit Application*
  Day-to-day operation of Peruri CA systems and system backup and recovery.

Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation

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

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

- Pembuatan kunci
- Pengaktifan kunci
- Pencadangan kunci

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 an Internal Auditor role with the exception of audit functions. The following tasks requires three or more persons:

- *Peruri CA key generation*
- *Peruri CA key activation*
- *Peruri CA key backup*

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

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

Setiap personel Peruri CA disusun secara khusus untuk peran yang telah ditentukan pada Bagian 5.2.1 dan tidak

Individual Peruri CA personnel are specifically designated to roles defined in section 5.2.1 of this CPS and no individual

ada personel yang ditugaskan lebih dari satu Peran Terpercaya.

has been assigned more than one Trusted Role.

5.3. KENDALI PERSONEL / PERSONNEL CONTROLS

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

Semua personil Peruri CA telah terpilih berdasarkan kemampuan dasar, pengalaman, kesetiaan, kepercayaan, dan integritas berdasarkan persyaratan tersebut:

- Pembuktian syarat latar belakang, kualifikasi serta pengalaman yang dibutuhkan untuk menjalankan tanggung jawab kerja secara efisien dan cukup; dan
- Membuktikan tidak ada catatan criminal.

All persons filling trusted roles are citizen of Indonesia and has been selected on the basis of skills, experience, loyalty, trustworthiness, and integrity in accordance of following requirements:

- *Proof of the requisite background, qualifications as well as experience necessary to efficiently and sufficiently perform their job responsibilities; and*
- *Proof of criminal record clearances.*

5.3.2. Prosedur Pemeriksaan Latar Belakang / Background Check Procedures

Semua personil di Peruri CA telah menyelesaikan pemeriksaan latar belakang. Ruang lingkup pemeriksaan latar belakang mencakup area berikut yang mencakup paling tidak dalam lima (5) tahun terakhir:

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

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

All persons filling Peruri CA trusted roles have completed a background investigation. The scope of the background check includes the following areas covering at least the past five (5) year:

- *Employment Contact Reference*
- *Education and certification*
- *Place of residence*
- *Police Certificate of Good Conduct*

Peruri CA will utilize a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

5.3.3. Persyaratan Pelatihan / Training Requirements

Semua personil Peruri CA harus dilatih untuk menjalankan tugasnya. Pelatihan semacam itu membahas topik yang

All Peruri CA personnel were trained to perform their duties. Such training addressed relevant topics, such as

relevan, seperti persyaratan keamanan, tanggung jawab operasional, prosedur terkait, undang-undang/hukum dan peraturan.

security requirements, operational responsibilities, associated procedures, law and regulation.

Pelatihan juga mencakup operasi IKP (termasuk perangkat keras, perangkat lunak dan sistem operasi Peruri CA), prosedur operasional dan keamanan, CPS, dan CP yang berlaku.

The trainings also include operations of the PKI (including Peruri CA hardware, software, and Operating System), operational and security procedures, this CPS, and the applicable CP.

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

Peruri CA harus melakukan evaluasi terhadap kecukupan kompetensi personil Peruri CA minimal 1 (satu) kali dalam setahun.

Peruri CA shall evaluate the adequacy of personnel's competency at least once a year.

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

Peruri CA memastikan bahwa perubahan staf tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

Peruri CA 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. Sanksi untuk Tindakan yang Tidak Terotorisasi / Sanctions for Unauthorized Actions

Sanksi disipliner yang sesuai diberikan pada personil yang melanggar ketentuan dan kebijakan didalam CP, CPS atau Prosedur operasional Peruri CA.

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

5.3.7. Persyaratan Kontraktor Independen / Independent Contractor Requirements

Personil sub kontraktor yang dipekerjakan untuk melaksanakan fungsi-fungsi yang terkait dengan operasi Peruri CA harus memenuhi persyaratan yang berlaku yang diatur dalam CPS ini. (misalnya, semua persyaratan pada bagian 5.3).

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

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

Peruri CA harus menyediakan kepada para personilnya *Certificate Policy* yang mereka gunakan, CPS, dan setiap undang-undang yang relevan, kebijakan, atau kontrak apapun. Dokumen teknis, operasional, dan administratif lainnya

Peruri CA have made available to its personnel the Certificate Policies they support, the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual,

(misalnya, Panduan Administrator, Panduan Pengguna, dll) harus disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

User Manual, etc.) has been provided in order for the trusted personnel to perform their duties.

5.4. PROSEDUR LOG AUDIT / AUDIT LOGGING PROCEDURES

Berkas log audit harus dibuat untuk semua kejadian yang terkait dengan keamanan Peruri CA, VA, dan RA. Bila memungkinkan, log audit keamanan harus dikumpulkan secara otomatis. Bila ini tidak mungkin, suatu buku log, kertas formulir, atau mekanisme fisik lain harus dipakai. Semua log audit keamanan, elektronik dan non elektronik, harus dipertahankan 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. Jenis Kejadian yang Direkam / Types of Events Recorded

Sebuah pesan dari sumber manapun yang diterima Peruri CA yang meminta suatu tindakan terhadap kondisi operasional Peruri CA adalah kejadian yang dapat diaudit. Setiap rekaman audit termasuk hal-hal berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian yang dapat diaudit):

A message from any source received by the Peruri CA requesting an action related to the operational state of the Peruri CA is an auditable event. Each audit record includes the following (either recorded automatically or manually for each auditable event):

- Tipe Kejadian;
- Nomor rekaman atau urutan rekaman;
- Tanggal dan waktu kejadian;
- Asal perekaman;
- Indikator keberhasilan atau kegagalan jika perlu; dan
- Identitas dan entitas dan/atau operator yang menyebabkan kejadian tersebut

- *The type of event;*
- *Serial or sequence number of entry;*
- *The date and time of the event;*
- *Source of entry;*
- *A success or failure indicator, where appropriate; and*
- *The identity of the entity and/or operator that caused the event.*

5.4.2. Frekuensi Pemrosesan Log / Frequency of Processing Log

Log audit harus ditinjau sedikitnya sebulan sekali, termasuk verifikasi

Audit logs were reviewed monthly, including verification that the log has not

bahwa log tersebut tidak dirusak, tidak ada diskontinuitas atau hilangnya data audit, dan kemudian secara singkat memeriksa semua entri log, dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan dalam log.

been tampered with, there is no discontinuity or other loss of audit data, and brief inspection all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Tindakan yang diambil sebagai hasil dari peninjauan ini harus didokumentasikan.

Actions taken as a result of these reviews were documented.

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

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

Peruri CA audit log were 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. Proteksi Log Audit / Protection of Audit Log

Log Audit dilindungi untuk mencegah perubahan dan mendeteksi gangguan serta untuk memastikan bahwa hanya individu dengan akses tepercaya 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.

Pengarsipan log audit harus memiliki kontrol yang memadai untuk mencegah konflik kepentingan atau menciptakan peluang untuk mengedit, menambahkan, menghapus, memodifikasi entri log.

Archiving of audit logs must have sufficient controls to prevent conflict of interest or create opportunity for editing, adding, deletion, modification of the log enteries.

5.4.5. Audit Log Backup Procedures / Prosedur Backup Log Audit

Log audit dan ringkasan audit di-*backup* per bulan. Media *backup* disimpan secara lokal dalam suatu lokasi yang aman. Salinan kedua dari log audit dikirim ke situs lain per bulan.

Audit logs and audit summaries were backed up monthly. Backup media were stored locally in a secure location. A second copy of the audit log were sent off-site on a monthly basis.

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

Sistem pengumpulan log audit adalah internal ke sistem Peruri CA.

The audit log collection systems were internal to the Peruri CA system

.

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

Tidak ada ketentuan.

No stipulation.

5.4.8. Asesmen Kerentanan / Vulnerability Assessments

Peruri CA mengases kerentanan sistem CA atau komponennya paling tidak satu tahun sekali.

Peruri CA were assessing the vulnerability of its CA system and its components annually.

5.5. PENGARSIPAN CATATAN / RECORDS ARCHIVAL

5.5.1. Tipe Catatan yang Diarsipkan / Types of Records Archived

Catatan arsip Peruri CA harus cukup rinci untuk menentukan operasional CA yang benar dan validitas sertifikat apapun (termasuk yang dicabut atau kedaluwarsa) yang dikeluarkan oleh Peruri CA. Data berikut dicatat pada arsip:

- Siklus operasi sertifikat termasuk permintaan sertifikat, permintaan pencabutan, permintaan pembangiktan ulang pasangan kunci.
- Semua sertifikat dan CRL yang telah diterbitkan
- Log Audit.
- Data konfigurasi sistem IKP
- Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini.
- Data pendaftaran pelanggan Peruri CA.

Peruri CA archive records were sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issued by the Peruri CA. The following data were recorded for archive:

- *Certificate life cycle operations including certificate requests, revocation requests, re-key requests, etc.*
- *All certificates and CRLs issued.*
- *Audit logs*
- *PKI system configuration data*
- *The CP document and all applicable CPSs including modifications and amendments to these documents*
- *Peruri CA's subscriber document*

5.5.2. Periode Retensi Arsip / Retention Period for Archive

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. Perlindungan Arsip / Protection of Archive

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

The archived records were protected against unauthorized viewing, modification, deletion, or tampering. The

menyimpan catatan arsip dan aplikasi yang dibutuhkan untuk memproses catatan arsip dipelihara dan dilindungi.

media holding the archive records and the applications required to process the archive records will be maintained and protected.

5.5.4. Prosedur Backup Arsip / Archive Backup Procedures

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

Adequate and regular backup procedures are 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 is available.

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

Catatan arsip Peruri CA diberikan label waktu secara otomatis.

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

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

Tidak ada ketentuan.

No stipulation.

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

Prosedur untuk menjaga dan memastikan informasi arsip adalah sebagai berikut:

a. Pemohon informasi mengirimkan permintaan akses arsip informasi ke Peruri CA dengan alasan spesifik dan keharusan mendapatkan informasi tersebut serta identifikasi kebutuhan jenis informasi.
b. Peruri CA menentukan kepatutan dan keharusan pemohon dan memberitahu hasil keputusan kepada pemohon.
c. Peruri CA mendapatkan arsip informasi, menentukan akses yang tepat, dan meneruskan ke pemohon.
d. Pemohon memastikan integritas informasi.

Procedures to obtain and verify archive information are as follows:

a. Information requester submits access request to archive information to Peruri CA specifying reasons and necessity of obtaining such information as well as identifying the type of information needed.
b. Peruri CA justifies the appropriateness and necessity of the request and notifies the decision result to the requester.
c. Peruri CA obtains the archive information, defines access rights, and forwards to the requester.
d. The requester verifies the integrity of information.

Konten dari arsip seharusnya tidak diterbitkan kecuali ditentukan oleh Peruri CA atau kebutuhan hukum.

The contents of the archive shall not be released except as determined by Peruri CA or required by law.

5.6. PERGANTIAN KUNCI / CHANGEOVER

Untuk meminimalkan risiko dari kebocoran kunci privat Peruri CA, kunci privat dapat diubah secara berkala setiap 10 (sepuluh) tahun. Sejak kunci privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat yang lama masih berlaku, dapat digunakan untuk verifikasi tanda tangan lama sampai semua sertifikat yang ditandatangani menggunakan kunci privat tersebut kadaluwarsa. Apabila kunci privat yang lama digunakan untuk menandatangani CRL, maka kunci yang lama disimpan dan dilindungi.

To minimize risk from compromise of Peruri CA's private signing key, that key may be changed periodically every 10 (ten) years. From that time on, only the new key shall be used for Certificate signing purposes. The older, but still valid, Certificate will be available to verify old signatures until all of the Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

Apabila Peruri CA memperbarui kunci privat dan menghasilkan kunci publik baru, Peruri CA memberitahu semua pemilik sertifikat yang mengandalkan Sertifikat Peruri CA bahwa telah terjadi perubahan melalui email atau website.

When Peruri CA updates its private signature key and thus generates a new public key, Peruri CA shall notify all subscribers that rely on the CA certificate that it has been changed by email or website.

5.6.1. Interlock Scheme / Skema Interlock

Peruri CA tidak memiliki skema *interlock*. Peruri CA tidak menerbitkan kembali sertifikat yang sama dengan kunci yang berbeda ketika terjadi penggantian kunci.

The Peruri CA does not have interlock scheme. The Peruri CA will not reissuing the same certificate with a different key while doing changeover procedure.

5.7. PEMULIHAN BENCANA DAN KEBOCORAN / COMPROMISE AND DISASTER RECOVERY

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

Peruri CA memiliki rencana tanggap darurat dan rencana pemulihan bencana.

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

Apabila dicurigai telah terjadi kebocoran kunci Peruri CA, penerbitan sertifikat oleh Peruri CA dihentikan seketika. Investigasi independen oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup dari kerusakan dinilai untuk menentukan prosedur perbaikan yang tepat. Apabila kunci privat Peruri CA dicurigai

If compromise of Peruri CA is suspected, certificate issuance by Peruri 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

mengalami kebocoran, prosedur pada Bagian 5.7.3. diikuti.

Peruri CA's private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed.

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

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

- Memberitahu Policy Authority, Security Officer, Key Manager, Head of Peruri CA dan Kominfo selaku Root CA.
- Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi backup terakhir.
- Mengoperasikan kembali Peruri CA, memprioritaskan kemampuan membangkitkan informasi status sertifikat untuk penerbitan CRL sesuai jadwal.

Apabila kunci penandatanganan Peruri CA rusak, mengembalikan operasional Peruri CA secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci Peruri CA yang baru.

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

- *Notify PA, Security Officer, Key Manager, PSrE Head and ROOT CA Indonesia 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.*
- *Re-establish Peruri CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.*

If Peruri CA's signing keys are destroyed, reestablish Peruri CA operations as quickly as possible, giving priority to the generation of a new Peruri CA signing key pair.

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

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

Dalam kasus kehilangan kunci privat dari Peruri CA, semua Pemilik Sertifikat dari Peruri CA akan diberitahu, semua sertifikat Pemilik yang diterbitkan oleh Peruri CA yang terkompromi tersebut dicabut, bersamaan dengan sertifikat milik Peruri CA.

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 Peruri CA and new keys and certificates are issued without interruption of the service.

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

Bila kunci privat Peruri CA hilang atau bocor, Peruri CA harus memberitahu PA dan Pihak Pengandal melalui pengumuman publik. Peruri CA harus menghentikan layanan, memberitahu semua Pemilik dari semua pemilik sertifikat, melanjutkan dengan pencabutan semua sertifikat, menerbitkan suatu CRL akhir, dan memberitahu kontak-kontak keamanan yang relevan. Lalu Infrastruktur Kunci Publik akan disiapkan lagi dengan membangkitkan pasangan kunci Peruri CA yang baru.

If the private key of the Root CA Indonesia is lost, Root CA Indonesia is expected to notify Peruri CA's PA officially and relying parties via public announcement. Peruri CA MUST stop service, notify all subscribers of Peruri 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. Kapabilitas Keberlangsungan Bisnis setelah terjadi Bencana / Business Continuity Capabilities after a Disaster

Untuk memelihara integritas layanan Peruri CA, akan diimplementasikan *backup* data dan prosedur pemulihan. Peruri CA telah mengembangkan Rencana Pemulihan Bencana *(Disaster Recovery Plan*). Sistem Peruri CA dikonfigurasikan secara redundan di sistem utama dan di sistem cadangan dilokasi yang terpisah. DRP dan prosedur pendukung ditinjau dan diuji secara berkala (setidaknya setahun sekali) dan direvisi dan diperbarui sesuai dengan kebutuhan.

To maintain the integrity of the Peruri CA services, it implements data backup and recovery procedures. The Peruri CA has developed a Disaster Recovery Plan (DRP). The Peruri CA system is redundantly configured at its primary site (main site) and is mirrored with a tertiary system located at a separate. The DRP and supporting procedures are reviewed and tested periodically (at least once a year) and are revised and updated as needed.

Pada sistem utama, Peruri CA memelihara sistem secara daring dan luring. Sistem cadangan Peruri CA tersedia apabila fasilitas utama berhenti beroperasi.

At its primary facility (main site), the Peruri CA maintains a fully redundant Peruri CA Online system and its services. The secondary node Peruri CA at the primary facility is readily available in the event that the primary node should cease operation.

Peruri CA telah mengoperasikan pencadangan data, yang bertujuan untuk memastikan kelangsungan operasi jika terjadi kegagalan pada situs utama dan untuk mengurangi dampak dari segala jenis bencana alam atau bencana buatan manusia.

The Peruri CA has been operating a backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary facility or site and mitigate the effects of any kind of natural or man-made disaster.

Operasi Peruri CA dirancang untuk memulihkan layanan penuh dalam waktu 24 jam dari kegagalan sistem utama.

The Peruri CA operations were designed to restore full service within twenty-four (24) hours of main site system failure.

5.8. PENUTUPAN CA ATAU RA / CA OR RA TERMINATION

Bila ada keadaan yang menyebabkan diakhirinya layanan Peruri CA dengan persetujuan *Policy Authority*, Peruri CA memberikan pemberitahuan kepada pemilik kunci dan pihak pengandal melalui email dan/atau pengumuman publik. Rencana tersebut dapat dilihat sebagai berikut:

- Memberitahu status layanan ke pengguna yang terkena dampak.
- Mencabut semua sertifikat.
- Menyimpan dalam jangka panjang informasi Peruri CA dan pemilik sertifikat dalam periode yang dinyatakan di sini.
- Menyediakan dukungan berkelanjutan dan menjawab pertanyaan.
- Menangani dengan tepat pasangan kunci Peruri CA dan perangkat keras yang terkait.

If there is any circumstance to terminate the services of Peruri CA with the approval of Policy Authority, Peruri CA will notify the subscribers, and all relying parties via email and/or public announcement. The action plan is as follow:

- *Notify the status of the service to affected users.*
- *Revoke all certificates.*
- *Long-term store information of Peruri CA and its subscribers according to the period herein specified.*
- *Provide ongoing support and answer questions.*
- *Properly handle Peruri CA key pair and associated hardware.*

6. KENDALI KEAMANAN TEKNIS / TECHNICAL SECURITY CONTROLS

6.1. PEMBANGKITAN DAN INSTALASI PASANGAN KUNCI / KEY PAIR GENERATION AND INSTALLATION

6.1.1. Pembangkitan Pasangan Kunci / Key Pair Generation

6.1.1.1. Pembangkitan Pasangan Kunci Peruri CA / Peruri CA Key Pair Generation

Material kunci kriptografi yang digunakan oleh Peruri CA untuk menandatangani sertifikat, CRL, atau informasi status dibuat di dalam modul kriptografis yang sesuai standar FIPS 140-2 Security Level 3, atau standar lain yang setara. Kontrol multi-pihak dibutuhkan untuk pembangkitan pasangan kunci Peruri CA, seperti yang ditentukan pada bagian 6.2.2.	*Peruri CA CPS Cryptographic keying material used by Peruri CA to sign certificates, CRLs, or status information were generated in cryptographic modules validated to [FIPS 140-2 Security Level 3], or some other equivalent standard. Multi-party control is required for Peruri CA key pair generation, as specified in section 6.2.2.*
Pembangkitan pasangan kunci Peruri CA harus menghasilkan jejak audit yang dapat diverifikasi, yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur diikuti. Pemisahan peran yang tepat atas proses pembuatan kunci didokumentasikan di dalam dokumen internal Peruri CA. 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.	*Peruri CA key pair generation created 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 Peruri CA. An independent third party was validating 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. Pembangkitan Pasangan Kunci Pemilik / Subscriber Key Pair Generation

Pembangkitan pasangan kunci Pemilik harus dilakukan oleh Pemilik atau Peruri CA.	*Subscriber key pair generation shall be performed by either the subscriber or Peruri CA.*
Jika Peruri CA membangkitkan pasangan kunci untuk Pemilik, persyaratan pengiriman pasangan kunci yang dinyatakan dalam bagian 6.1.2 juga harus dipenuhi dan Peruri CA harus membangkitkan kunci dalam suatu perangkat dengan standar FIPS 140-2 Security Level 3.	*If Peruri CA generates key pairs for subscribers, the requirements for key pair delivery specified in section 6.1.2 must also be met and Peruri CA shall generate keys within a secure FIPS 140-2 Security Level 3 standard.*

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

Peruri CA tidak mengirimkan kunci privat ke pemilik sertifikat.

Peruri CA does not deliver private key to subscribers.

Bila Peruri CA 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 dengan spesifikasi FIPS 140-2 Security Level 3. Dalam semua kasus persyaratan berikut harus dipenuhi:

When Peruri 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 FIPS 140-2 Security Level 3 hardware cryptographic module. In all cases, the following requirements shall be met:

- Siapa pun yang membuat kunci penandatanganan pribadi untuk Pelanggan tidak akan menyimpan salinan kunci apa pun setelah pengiriman Kunci Pribadi ke Pelanggan.
- Kunci Pribadi akan dilindungi dari aktivasi, penyusupan, atau modifikasi selama proses pengiriman.
- Pelanggan harus mengakui telah menerima Kunci Pribadi.
- Peruri CA akan menyimpan catatan pengakuan Pelanggan atas penerimaan kunci privat tersebut.

- *Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber.*
- *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. Pengiriman Kunci Publik ke Penerbit Sertifikat / Public Key Delivery to Certificate Issuer

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

Peruri CA menyediakan mekanisme untuk penyampaian digital yang aman dari semua sertifikat yang memuat kunci publik, melalui repositori sesuai bagian

Peruri CA provides mechanisms for the secure digital delivery of all certificates containing public key, via repository according to section 2.1 using SSL.

2.1 yang diamankan menggunakan SSL.

6.1.5. Key Sizes / Ukuran Kunci

Peruri CA membuat sertifikat dan CRL di bawah aturan ini harus menggunakan algoritma RSA dengan panjang kunci minimal 2048-bit dan minimum hash SHA-256 ketika membuat tanda tangan digital.

Peruri CA that generate certificates and CRLs under this policy should use RSA algorithm with a key length minimum 2048 bit and minimum SHA-256 hash algorithm when generating digital signatures.

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

Secara Default, Nilai Parameter Kunci Publik adalah 05 00. Byte 05 00 secara sederhana berarti NULL (tanpa Nilai)

By Default, the Public Key Parameter Value is 05 00. Bytes 05 00 simply mean NULL in DER (and CER and BER)

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

Kunci-kunci Peruri CA dipakai untuk penandatanganan sertifikat (keyCertSign) dan penandatanganan CRL (cRLSign).

Peruri CA keys are used for certificate signing (keyCertSign) and CRL signing (cRLSign).

6.2. KONTROL KUNCI PRIVATE DAN KONTROL TEKNIS MODUL KRIPTOGRAFI / PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

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

Peruri CA menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 Security Level 3 untuk pembangkitan kunci, proses penandatanganan, dan enkripsi.

Peruri CA uses a FIPS 140-2 Security Level 3 cryptographic module for key generation, signing operations and encryption.

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

Peruri CA telah mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif. Suatu jumlah minimum dari *Secret Shares* (n) dari sejumlah total *Secret Shares* yang dibuat dan didistribusikan untuk dipakai di modul kriptografis tertentu (m) diperlukan

Peruri has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive cryptographic operations. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a Peruri CA private key stored in

untuk mengaktifkan sebuah kunci privat Peruri CA yang disimpan di dalam modul.

the module.

Angka ambang yang diperlukan untuk pembuatan kunci adalah 2 dari 4 (dimana n=2 dan m=4), aktivasi kunci penandatanganan adalah 2 dari 4, dan *backup* serta pemulihan kunci privat adalah 2 dari 4.

The threshold number of shares needed for key generation is 2 of 4 (where n=2 and m=4) signing key activation is 2 of 4 and private key backup and restore is 2 of 4.

6.2.3. Escrow Kunci Privat / Private Key Escrow

Kunci Privat Peruri CA tidak akan pernah dititipkan (escrowed). Kunci Privat Pemilik dapat dititipkan di Peruri CA.

Peruri CA private keys will never be escrowed. Subscriber private keys may be escrowed at Peruri CA.

6.2.4. Backup Kunci Privat / Private Key Backup

Kunci privat Peruri CA harus di-*backup* di bawah kendali multi-pihak yang sama dengan kunci privat asli. Paling tidak satu salinan dari kunci privat harus disimpan *off-site*. Semua salinan kunci privat Peruri CA harus dilindungi dengan cara yang sama dengan aslinya.

Peruri's private signature key was backed up under the same multiparty control as the original signature key. At least one copy of the private signature key was stored off-site. All copies of the Peruri private signature key were accounted for and protected in the same manner as the original.

6.2.5. Pengarsipan Kunci Privat / Private Key Archival

Sebelum kunci privat Peruri CA dimusnahkan, kunci harus diarsipkan sesuai dengan ketentuan pengarsipan Peruri CA. Sementara itu, Kunci Privat Pemilik tidak boleh diarsipkan.

Before Peruri CA private signature keys is destroyed, the key shall be archived in accordance to Peruri CA policy. Meanwhile, subscriber private signature keys shall not be archived.

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

Kunci privat Peruri CA boleh diekspor dari modul kriptografis hanya untuk melaksanakan prosedur backup kunci Peruri CA. Kunci privat Peruri CA tidak pernah sekalipun boleh berada dalam bentuk plaintext di luar modul kriptografi.

Peruri CA private keys may be exported from the cryptographic module only to perform Peruri CA key backup procedure. Peruri CA private key has never exist in plaintext outside the cryptographic module.

Bila sebuah kunci privat akan dipindahkan dari satu modul kriptografis ke yang lain, kunci privat harus dienkripsi selama pemindahan. Kunci pemindahan yang dipakai untuk mengenkripsi kunci

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 will be handled in the same

privat harus ditangani dengan cara yang sama dengan kunci privat.

way as the private key

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

Kunci Privat Peruri CA disimpan pada modul kriptografis FIPS 140-2 Security Level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

Peruri CA Private Keys were stored on FIPS 140-2 Security Level 3 cryptographic module, in encrypted form and password-protected.

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

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

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

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

Setelah dipakai, modul kriptografis harus dinonaktifkan oleh personil yang berwenang secara otomatis setelah *secret shares* dicabut dari modul kriptografi.

After use, the cryptographic modules were deactivated by authorized person, e.g., via a manual logout procedure, or automatically after a period of inactivity.

6.2.10. Metode Penghancuran Kunci Privat Method of Destroying Private Key

Ketika kunci tanda tangan privat Peruri CA tidak diperlukan lagi, para individu dalam peran terpercaya harus menghapus kunci privat dari Modul Kriptografi dan *backup*-nya dengan menimpa kunci privat atau menginisialisasi modul dengan fungsi *factory reset* dari Modul Kriptografi.

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

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

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

6.2.11. Pemeringkatan Modul Kriptografis / Cryptographic Module Rating

Seperti diuraikan dalam bagian 6.2.1.

As described in section 6.2.1.

6.3. ASPEK LAIN DARI MANAJEMEN PASANGAN KUNCI / OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Pengarsipan Kunci Publik / Public Key Archival

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.

The Public Key is archived as part of the Certificate archival.

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

Periode operasi pasangan kunci ditentukan oleh periode operasional sertifikat digital yang sesuai. Jangka waktu operasional maksimum kunci ditentukan selama sepuluh (10) tahun untuk Peruri CA.

The key pair operational period is defined by the operational period of the corresponding digital certificate. The maximum operational period of the keys is defined ten (10) years for a Peruri CA.

6.4. AKTIVASI DATA / DATA ACTIVATION

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

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. Perlindungan Data Aktivasi / Activation Data Protection

Data aktivasi untuk perangkat HSM dilindungi seperti yang dijelaskan dalam Bagian 6.2.2 (Kunci Pribadi (n dari m) Kontrol Multi-Orang). Peruri CA menyimpan administrasi kunci privat dalam bentuk token yang terenkripsi dengan perlindungan kata sandi yang kuat.

Activation data for HSM devices are protected as described in Section 6.2.2 (Private Key (n out of m) Multi-Person Control). Peruri CA stores their administrator private keys in encrypted form using hardware token with strong password protection.

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

Tidak ada ketentuan.

No stipulation.

6.5. COMPUTER SECURITY CONTROLS / KONTROL KEAMANAN KOMPUTER

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

Peruri CA memastikan bahwa sistem yang menjaga perangkat lunak Peruri CA

Peruri CA ensures that the systems maintaining Peruri CA software and data

dan file data aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem Peruri CA telah dikonfigurasi dan dikeraskan/dikuatkan menggunakan praktik terbaik industri. Semua sistem operasi membutuhkan identifikasi dan otentikasi untuk *login* yang diautentikasi. Ini memberikan kontrol akses *discretionary,* pembatasan kontrol akses ke layanan berdasarkan identitas yang diotentikasi, kemampuan audit keamanan, dan catatan audit yang dilindungi untuk berbagi sumber daya, perlindungan diri, dan isolasi proses.

files are secure from unauthorized access. All computers that are part of Peruri CA system has been configured and hardened using industry best practices. All operating systems requires identification and authentication for authenticated logins. It provides discretionary access control, access control restrictions to services based on authenticated identity, security audit capability, and a protected audit record for shared resources, self-protection, and process isolation.

Server Peruri CA yang terkait dengan kunci penandatanganan pribadi dioperasikan secara luring.

Peruri CA servers related to private signing key is being operated offline.

6.5.2. Peringkat Keamanan Komputer / Computer Security Rating

Tidak ada ketentuan.

No stipulation.

6.6. KONTROL TEKNIS SIKLUS HIDUP / LIFE CYCLE OF TECHNICAL CONTROLS

6.6.1. Kontol Pengembangan Aplikasi / System Development Controls

Tidak ada ketentuan.

No stipulation.

6.6.2. Kontrol Manajemen Keamanan / Security Management Controls

Peruri CA menggunakan perangkat lunak untuk mendeteksi perubahan konfigurasi sistem manajemen CA. Untuk menjamin integritas perangkat keras, Peruri CA menggunakan *anti-tempered bag*.

Peruri CA uses software to detect configuration changes in the CA management system. To ensure the integrity of the Peruri CA hardware, Peruri CA use an anti-tempered bag

6.6.3. Kontrol Keamanan Siklus Hidup / Life Cycle Security Controls

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

Peruri 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. KONTROL KEAMANAN JARINGAN / NETWORK SECURITY CONTROL

Peruri CA menggunakan tindakan keamanan jaringan yang sesuai untuk memastikannya dijaga dari DoS dan

Peruri CA employs appropriate network security measures to ensure it is guarded against denial of service and intrusion

serangan intrusi. Langkah-langkah tersebut termasuk penggunaan *firewall* dan menyaring *router*. *Port* dan layanan jaringan yang tidak digunakan telah dimatikan. Perangkat lunak jaringan apa pun diperlukan untuk memfungsikan Peruri CA.

attacks. Such measures include the use of firewalls and filtering routers. Unused network ports and services has been turned off. Any network software present were necessary to the functioning of Peruri CA.

6.8. STEMPEL WAKTU / TIME-STAMPING

Jam server daring Peruri CA disinkronkan menggunakan *Network Time Protocol.* Waktu server luring disinkronkan secara manual.

Peruri CA online servers' internal clock were synchronized using Network Time Protocol. Offline servers' time were synchronized manually.

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

7.1. PROFIL SERTIFIKAT / CERTIFICATE PROFILE

Profil sertifikat menurut RFC 5280 "Internet X.509 Infrastruktur Kunci Publik: Profil Daftar Pencabutan Sertifikat (CRL)" digunakan.

A certificate profile according to RFC 5280 "internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) profile" is used.

CA Peruri mereview Profil Sertifikat secara berkala minimal setahun sekali yang dilakukan oleh CA Admin dengan menyesuaikan profil sertifikat dengan Regulasi dan / atau Persyaratan Bisnis

Peruri CA review Certificate Profile periodically at least once a year done by CA Admin by adjusting the certificate profile with Regulations and/or Business Requirements

Profil sertifikat mengikuti standar RFC 5280 "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile".

Profil sertifikat mengikuti standar RFC 5280 "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile"

7.1.1.1. Nomor Versi / Version Number(s)

Peruri CA menerbitkan sertifikat X.509 versi 3.

Peruri CA issue X.509 version 3 certificates.

7.1.2. Ekstensi Sertifikat / Certificate Extensions

Peruri CA memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

Peruri CA use standard certificate extensions that comply with RFC 5280.

7.1.2.1. Penggunaan Kunci / Key Usage

Sertifikat X.509 Versi 3 diisi sesuai dengan RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile (CRL) Profile"

7.1.2.2. Perluasan Kebijakan Sertifikat / Certificate Policies Extension

Ekstensi *Certificate Policies* dari Sertifikat X.509 Versi 3 diisi dengan OID dari CPS ini sesuai dengan bagian 7.1.6 dan dengan qualifier kebijakan yang ditentukan dalam bagian 7.1.8.

Certificate Policies extension of X.509 Version 3. Certificate are populated with the object identifier of this CPS in accordance with Section 7.1.6 and with policy qualifiers set forth in section 7.1.8.

7.1.2.3. Batasan Dasar / Basic Constraint

Ekstensi *Basic Constraints* Sertifikat X.509 Versi 3 harus memiliki *field* CA yang diisi TRUE. Ekstensi *Basic Constraints* Sertifikat Pengguna Akhir harus memiliki *field* CA yang diisi FALSE.

X.509 Version 3 CA Certificates Basic Constraints extension shall have the CA field set to TRUE. End-user Subscriber Certificates Basic Constraints extension shall have the CA field set to FALSE. The

Field criticality dari ekstensi ini harus diisi TRUE untuk Sertifikat CA, tapi boleh diisi TRUE atau FALSE bagi Sertifikat Pengguna Akhir.

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. Penggunaan Kunci Tambahan / Extended Key Usage

Tidak ada ketentuan.

No stipulation.

7.1.2.5. Titik Distribusi CRL / CRL Distribution Points

Sertifikat X.509 Versi 3 diisi dengan suatu ektensi *CRL Distribution Points* yang memuat URL dari lokasi dimana Pihak Pengandal dapat memperoleh suatu CRL untuk memeriksa status sertifikat. *Field criticality* dari ekstensi ini harus diisi FALSE.

X.509 Version 3 Certificates are populated with a CRL Distribution Points extension containing the URL of the location where a Relying Party can obtain a CRL to check the certificate's status. The criticality field of this extension shall be set to FALSE.

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

URLs shall comply with Mozilla requirements to exclude the LDAP protocol, and may appear multiple times within a CRL Distribution Points extension.

7.1.2.6. Pengidentifikasi Kunci Otoritas / Authority Key Identifier

Sertifikat X.509 Versi 3 biasanya diisi dengan ekstensi authorityKeyIdentifier. Metode untuk menghasilkan key identifier yang berbasis pada kunci publik dari Peruri CA, harus dihitung sesuai dengan salah satu metode yang diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini harus diisi FALSE.

X.509 Version 3 Certificates are generally populated with an Authority Key Identifier extension. The method for generating the key identifier based on the public key of the Peruri 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. Pengidentifikasi Kunci Subyek / Subject Key Identifier

Bila ada dalam Sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini harus diisi dengan FALSE dan metode untuk menghasilkan *key identifier* yang berbasis pada kunci publik subyek sertifikat harus dihitung sesuai dengan salah satu 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 key identifier 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. Pengidentifikasi Objek Algoritma / Algorithm Object Identifiers

Menggunakan standar OID X.509 v3. Algoritma berupa enkripsi RSA untuk *subject key* dan SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.	*X.509 Version 3 standard OIDs shall be used. Algorithm RSA encryption for the subject key and SHA256 with RSA encryption for the certificate signature.*

7.1.4. Format Nama / Name Forms

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. Batasan Nama / Name Constraints

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. Pengidentifikasi Objek Kebijakan Sertifikat / Certificate Policy Object Identifier

Sertifikat yang diterbitkan di bawah CPS ini menggunakan nomor OID 2.16.360.1.1.1.12.3 yang mengacu pada PSrE Induk.	*Certificates issued under this CPS use OID number 2.16.360.1.1.1.12.3 that points to the correct Root CA.*

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

Tidak ada ketentuan.	No stipulation.

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

Tidak ada ketentuan.	*No stipulation.*

7.1.9. Memproses Semantik untuk Ekstensi Kebijakan Sertifikat Penting / Processing Semantics for the Critical Certificate Policies Extension

Tidak ada ketentuan.	*No stipulation.*

7.2. PROFIL CRL / CRL PROFILE

7.2.1. Nomor Versi / Verion Number(s)

Peruri CA menerbitkan X.509 dan ekstensi entri CRL.	*Peruri CA shall issue X.509 and CRL entry extension.*

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

Peruri CA menggunakan CRL dan CRL entri extension RFC 5280.	*Peruri CA shall use RFC 5280 CRL and CRL entry extension.*

7.3. PROFIL OCSP / OCSP PROFILE

Peruri CA bisa mengoperasikan sebuah responder *Online Certificate Status Protocol (OCSP)* yang sesuai dengan RFC 6960 atau RFC 5019.

Peruri CA may operate an Online Certificate Status Protocol (OCSP) responder in compliance with RFC 6960 or RFC 5019.

7.3.1. Nomor Versi / Version Number(s)

Peruri CA menerbitkan respon OCSP versi 1.

Peruri CA issue OCSP responses Version 1.

7.3.2. Ekstensi OCSP / OCSP Extensions

Tidak ada ketentuan.

No stipulation.

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

8.1. FREKUENSI ATAU KEADAAN ASESMEN / FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Peruri CA menjalani audit kepatuhan berkala terhadap skema yang telah ditetapkan yang tidak kurang dari sekali setahun dan setiap terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan.

Peruri CA were subjected to annual compliance audits not less than once a year and after any significant changes to the procedures and techniques used due to any change related business system, technology and regulation.

8.2. IDENTITAS / KUALIFIKASI ASESOR / IDENTITY/QUALIFICATIONS OF ASSESSOR

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

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

Auditor kepatuhan harus memiliki kualifikasi sebagai berikut:

a. Auditor harus dilaksanakan oleh tim asesmen independen yang *qualified* .
b. Auditor harus memiliki pengetahuan yang cukup tentang tanda tangan digital, sertifikat digital, X.509 versi 3 PKI, *Certificate Policy and Certification Practices Framework*, UU ITE, PP PSTE, Peraturan Menteri Komunikasi dan Informatika no 11/2018.

Compliance auditors must possess these qualifications:

a. Auditors shall have a qualified, independent assessment team
b. Auditors shall have a sufficient knowledge on digital signatures, digital 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 82 2012),

	and Indonesia Ministry of Communication and Informatics Regulation on Certification Authority Operations (PM Kominfo 11 2018)
c. Memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;	*c. Auditors shall have an adequate skills on information security audit, information security device and technique audit, as well as familiarity with PKI technology*
d. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah	*d. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme*
e. Menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.	*e. Auditors shall master a set of certain skills, competency testing, and quality assurance such as peer review, standards regarding accurate staff assigning, and involvement and requirements for higher professional education*

8.3. HUBUNGAN ASESOR DENGAN BADAN YANG DINILAI / ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Untuk memberikan evaluasi yang tidak bias dan independen, auditor dan pihak yang diaudit tidak boleh memiliki hubungan keuangan, hukum, atau lainnya saat ini atau yang direncanakan yang dapat mengakibatkan konflik kepentingan.	*To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.*

8.4. TOPIK YANG DICAKUP OLEH ASESMEN / TOPICS COVERED BY ASSESSMENT

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. TINDAKAN YANG DIAMBIL SEBAGAI HASIL DARI KEKURANGAN / ACTIONS TAKEN AS A RESULT OF DEFICIENCY

Peruri CA akan menyusun rencana tindakan perbaikan yang akan dilaksanakan untuk memperbaiki kekurangan yang tercatat berdasarkan masukan dari auditor.

Peruri CA will formulate a corrective action plan that will be implemented to rectify any noted deficiency based from the inputs of the auditor.

8.6. KOMUNIKASI HASIL / COMMUNICATION OF RESULTS

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada *Policy Authority* sebagaimana diatur dalam bagian 8.1. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam asesmen.

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

8.7 AUDIT INTERNAL / INTERNAL AUDIT

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. MASALAH BISNIS DAN HUKUM LAINNYA / OTHER BUSINESS AND LEGAL MATTERS

9.1. BIAYA / FEES

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

Peruri CA mengenakan biaya administrasi dalam menerbitkan atau memperbaharui Sertifikat termasuk dalam hal penerbitan ulang sertifikat. Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat.

Peruri CA charge administrative fees for certificate issuance or renewal including in the case of certificate reissue. There are terms and conditions related to fees for certificate applicants.

9.1.2. Biaya Pengaksesan Sertifikat / Certificate Access Fees

Peruri CA dapat mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan.

Peruri CA may charge an administrative fee for each access to the repository that contains a certificate that has been issued.

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

Peruri CA dapat mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau informasi

Peruri CA may charge additional fees to Subscribers for any access to certificate revocation status or certificate

pencabutan sertifikat	*information status.*

9.1.4. Biaya Layanan Lainnya / Fees for Other Services

Peruri CA dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya.	*Peruri CA may charge fees for other additional services.*

9.1.5. Kebijakan Pengembalian Biaya / Refund Policy

Tidak ada Kebijakan Pengembalian Biaya.	*No Refund Policy.*

9.2. TANGGUNG JAWAB KEUANGAN / FINANCIAL RESPONSIBILITY

9.2.1. Cakupan Asuransi / Insurance Coverage

Peruri CA mematuhi persyaratan PM Kominfo Nomor 11 Tahun 2018 Pasal 12 huruf h.	*Peruri CA comply with Article 12 letter h of Communication and Informatics Minister Regulation No.11/2018.*

9.2.2. Aset Lainnya / Other Assets

Tidak ada ketentuan.	*No stipulation.*

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

Peruri CA menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik sertifikat.	*Peruri CA offers an insurance or warranty policy to Subscribers.*

9.3. KERAHASIAAN INFORMASI BISNIS / CONFIDENTIALITY OF BUSINESS INFORMATION

Peruri CA melindungi kerahasiaan informasi bisnis sensitif yang dapat mengarah pada penyalahgunaan atau penipuan. Misalnya, CA melindungi data pelanggan yang dapat memungkinkan penyerang berkedok sebagai pelanggan. Akses publik ke Peruri CA ditentukan oleh informasi organisasi Peruri CA.	*Peruri CA protects the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. Public access to Peruri CA organizational information determined by Peruri CA.*

9.3.1. Cakupan Informasi Rahasia / Scope of Confidential Information

Peruri CA memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Yang	*The following items are classified as being confidential information and therefore are subject to reasonable care*

termasuk dalam kategori informasi rahasia antara lain:

and attention Peruri CA:

- 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) dan Business Continuity Plans (BCP)*; dan
- Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0.

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

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

Any information not defined as confidential within the CPS shall be deemed public. Certificate status information and Certificates themselves are deemed public.

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

Peruri CA melindungi informasi rahasia. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:

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

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

- *Training,*
- *Contracts with employees,*
- *NDA with employees, outsource and contractors.*

9.4. PRIVASI INFORMASI PRIBADI / PRIVACY OF PERSONAL INFORMATION

9.4.1. Rencana Privasi / Privacy Plan

Peruri CA memiliki Rencana Privasi yang akan selalu melindungi informasi identitas pribadi dari pengungkapan

Peruri CA has Privacy Plan that will always protect personally identifying information from unauthorized disclose.

yang tidak sah. Perlindungan informasi pribadi sesuai dengan Kebijakan Privasi yang dipublikasikan di situs web Peruri CA, https://ca.peruri.co.id/ca/legal

Protection of personal information in accordance with a Privacy Policy published on Peruri CA's web site at https://ca.peruri.co.id/ca/legal

9.4.2. Informasi yang Dianggap Pribadi / Information Treated as Private

Semua informasi tentang Pemegang Sertifikat tidak ditujukan untuk publik melalui konten pada sertifikat yang dikeluarkan, direktori sertifikat atau repositori daring. Informasi tersebut diperlakukan sebagai informasi pribadi.

All information about Certificate Holders that is not publicly available through the content of issued certificate, certificate directory or online repositories. They are treated as private information.

9.4.3. Informasi tidak Dianggap Pribadi / Information not Deemed Private

Informasi yang ada pada sertifikat dan CRL tidak dianggap pribadi.

Information in the certificate and CRL is not deemed private.

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

Peruri CA telah menerapkan tindakan keamanan untuk melindungi informasi pribadi.

Peruri CA has implemented security measure to protect private information.

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

Peruri CA akan menggunakan informasi pribadi hanya jika pemilik informasi menyadari dan menyetujui untuk menggunakan informasi pribadi sesuai dengan kebijakan privasi.

Peruri CA will use private information only if the information owner is noticed and consent to use private information in compliance with privacy policy.

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

Peruri CA dapat mengungkapkan informasi pribadi, tanpa pemberitahuan terlebih dahulu, jika pengungkapannya diharuskan oleh hukum atau peraturan pemerintah.

Peruri CA may disclose private information, without any notice, if the disclosure is required by law or government regulation.

9.4.7. Keadaan Pengungkapan Informasi Lain / Other Information Disclosure Circumstances

Tidak ada ketentuan.

No stipulation.

9.5. HAK ATAS KEKAYAAN INTELEKTUAL / INTELLECTUAL PROPERTY RIGHTS

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

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

9.6. PERTANYAAN DAN JAMINAN / REPRESENTATIONS AND WARRANTIES

9.6.1. Pernyataan Dan Jaminan CA / CA Representations and Warranties

Peruri CA menyatakan dan menjamin, sejauh yang ditentukan dalam CPS, bahwa:

a. Peruri CA mematuhi ketentuan yang diatur dalam CPS ini,
b. Peruri CA menerbitkan dan memperbarui CRL secara berkala,
c. Seluruh sertifikat yang diterbitkan berdasarkan CPS ini akan diverifikasi sesuai dengan CPS ini dan memenuhi persyaratan minimum,
d. Peruri CA mengelola repositori informasi publik pada websitenya.

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

a. Peruri CA complies, in all material aspects, with the CP and this CPS,
b. Peruri CA publishes and updates CRL on a regular basis,
c. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements.
d. Peruri CA maintain a repository of public information on its website.

9.6.2. Pernyataan dan Jaminan RA / RA Representations and Warranties

Tidak ada ketentuan.

No stipulation.

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

Pemilik Sertifikat menjamin bahwa:

1. Setiap sertifikat digital yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada sertifikat adalah merupakan tanda tangan digital pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan digital dibuat;
2. Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;
3. Sudah melakukan review terhadap informasi dari sertifikat;
4. Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang

Subscribers warrant that:

1. Each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
2. Their private key is protected and that no unauthorized person has ever had access to the subscriber's private key,
3. Have thoroughly reviewed the certificate information
4. All information supplied by the subscriber and contained in the

berada di dalam sertifikat adalah benar;

5. Sertifikat digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
6. 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;

7. Akan menanggapi instruksi Peruri CA terkait kebocoran atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;
8. Menyetujui dan menerima bahwa Peruri CA diberikan kewenangan untuk segera melakukan pencabutan sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam kontrak perjanjian atau jika Peruri CA menemukan bahwa sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian *malware*;
9. Pengguna dan bukan merupakan Peruri CA, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam sertifikat digital untuk tujuan penandatangan sertifikat digital PSrE lain.

certificate is true,

5. The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CPS, and

6. 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;

7. Will respond to Peruri CA's instructions regarding compromise or digital certificates misuses within fourty eight (48) hours,

8. Acknowledges and accepts that Peruri CA is entitled to revoke the certificate immediately if the subscriber violates the terms of the subscriber agreement or terms of use or if Peruri CA discovers that the certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, and

9. The subscriber is an end-user subscriber and not a Peruri 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. Pernyataan dan Jaminan Pihak Pengandal / Relying Party Representations and Warranties

Pihak yang mengandalkan Sertifikat Peruri CA menjamin bahwa:

1. Memiliki kemampuan teknis untuk menggunakan sertifikat,
2. Apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh Peruri CA, 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,
3. Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi kebocoran/penyalahgunaan pada kunci privat,
4. 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 CPS ini,
5. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

Peruri CA's Certificate relying party guarantee that:

1. *Have the technical capability to use certificates,*
2. *If the representative from the relying party use a certificate issued by Peruri CA, relying party should verify the information contained in the certificate before use and carry all the consequences that happened if the relying party fail to applied it.*
3. *Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised,*
4. *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 CPS,*
5. *Must compliance with the provisions of this CPS and related agreements*

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

Tidak ada ketentuan.

No stipulation.

9.7. PELEPASAN JAMINAN / DISCLAIMERS OF WARRANTIES

Peruri CA menyatakan dalam CPS bahwasanya tidak menjamin:

1. Kecuali untuk jaminan yang telah tercantum dalam CPS dan kontrak perjanjian dan sepanjang diizinkan oleh hukum, Peruri CA mengabaikan

Peruri CA state in their CPS that they do not warrant:

1. *Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, Peruri CA disclaims*

semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu,

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.

2. Penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Pasangan Kunci dan Penggunaan Sertifikat),

2. Misuse of a certificate that is inconsistent with its usage as shown in section 4.5 (Key Pair and Certificate Usage),

3. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing sertifikat.

3. The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.8. PEMBATASAN TANGGUNG JAWAB / LIMITATIONS OF LIABILITY

9.8.1. Pembatasan Tanggung Jawab Peruri CA / Peruri CA Limitations of Liability

Peruri CA tidak bertanggung jawab atas penggunaan sertifikat yang tidak tepat, termasuk:

1. Semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
2. Semua kerusakan yang disebabkan oleh *force majeure*,
3. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau *trojans*) diluar perangkat Peruri CA.
4. Semua kesalahan data informasi sertifikat yang berasal dari pemilik sertifikat setelah periode verifikasi data selesai.
5. Sertifikat yang tidak diterbitkan atau dikelola sesuai dengan Persyaratan ini atau Kebijakan Sertifikat dan / atau Pernyataan praktik Sertifikasi

Peruri CA is not responsible for inappropriate use of the certificate, including:

1. All damage caused by the misuse of certificates or key pairs beside the proper use that have been defined in CPS, subscriber's agreement, or all provision which have been mentioned in the certificate,
2. All damage caused by the force majeure condition,
3. All damage caused by the malware (i.e virus or trojan) outside Peruri CA devices.
4. All incorrect certificate information that comes from subscriber after data verification period is complete.
5. Certificates not issued or administered in accordance with Peruri CA Certificate Policy and/or Certificate Practice Statement.

9.8.2. Pembatasan Tanggung Jawab RA / RA Limitation of Liability

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

The cap on Registration Authority liability is specified in the frame contract between Registration Authority and Peruri CA. In particular, the Registration Authority is liable for the registration of subscribers.

9.9. GANTI RUGI / INDEMNITIES

Peruri CA tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.

Peruri CA has no liability for the improper use of Certificate.

9.10. SYARAT DAN PENGAKHIRAN / TERM AND TERMINATION

9.10.1. Syarat / Term

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh Peruri CA melalui laman atau repositorinya.

This CPS remains in force until such time as communicated otherwise by Peruri CA on its website or Repository.

9.10.2. Pengakhiran / Termination

Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 hari setelah dipublikasikan.

Notified changes of this CPS are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

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

Peruri CA harus mengkomunikasikan kondisi, akibat dari penghentian CPS, dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui laman atau repositori.

Peruri CA should communicate the conditions and effect of this CPS's termination on its website or Repository.

9.11. PEMBERITAHUAN INDIVIDU DAN KOMUNIKASI DENGAN PARTISIPAN / INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Peruri CA menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, telepon, baik yang ditandatangani secara digital, dalam bentuk kertas, atau email bersertifikat. Peruri CA memberikan tanda terima yang valid sebagai bukti bagi pengirim. Peruri CA harus memberi tanggapan paling lama dua puluh (20) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke Peruri CA harus dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS

Peruri CA provides communication media for related parties through electronics document, electronic mail, telephone both digitally signed, in paper form or certified email. Peruri CA provides a valid receipt as proof for the sender. Peruri CA must respond for a maximum of twenty (20) working days through the same communication media. Communications made to Peruri CA's must be addressed in accordance with those listed in section 1.5.2 of CPS.

9.12. AMANDEMEN / AMENDMENTS

9.12.1. Prosedur untuk Amandemen / Procedure for Amendment

Perubahan CPS patuh terhadap Peruri CA dan harus disetujui oleh PA sebelum pengumuman. Namun, semua perubahan dilakukan sesuai dengan hukum, peraturan atau pengumuman layanan terkait lainnya dari Peruri CA.

Amendment of CPS is subject to Peruri CA and it needs to be approved by PA before announcement. However, all amendments are performed pursuant to laws, regulation or other related service announcements of Peruri CA

9.12.2. Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

Setiap kali CPS diubah, CPS akan diumumkan dalam waktu tujuh (7) hari sejak adanya perubahan dan diketahui oleh semua pihak yang berkepentingan (Penerbit CA, pihak pengandal, pelanggan, dll.). Salinan CPS terbaru dapat ditemukan di: https://ca.peruri.co.id/ca/legal .

Whenever the CPS is amended, it shall be published within seven (7) days of the date the amendment took place and all known concerned parties (Issuing CA, relying parties, subscribers, etc.) shall be notified. The most up to date copy of this CPS can be found at: https://ca.peruri.co.id/ca/legal .

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

Jika PA memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, Peruri CA 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, Peruri CA will change the OID and enforce the new policy using the new OID.

9.13. PROVISI PENYELESAIAN KETIDAKSEPAHAMAN / DISPUTE RESOLUTION PROVISIONS

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 Peruri CA 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 Peruri CA and the certificate owner.

9.14. HUKUM YANG MENGATUR / GOVERNING LAW

CPS ini menerapkan aturan hukum di Republik Indonesia.

This CPS is governed by the laws of the Republic of Indonesia.

9.15. KEPATUHAN ATAS HUKUM YANG BERLAKU / COMPLIANCE WITH APPLICABLE LAW

Peruri CA diharuskan untuk mematuhi hukum Republik Indonesia

Peruri CA are required to comply with the laws of the Republic of Indonesia.

9.16. KETENTUAN YANG BELUM DIATUR / MISCELLANEOUS PROVISIONS

9.16.1. Seluruh Perjanjian / Entire Agreement

Tidak ada ketentuan.

No stipulation.

9.16.2. Pengalihan / Assignment

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

Relying Parties and Subscribers may not assign their rights or obligations under this CPS, by operation of law or otherwise, without Peruri CA prior written approval. Any such attempted assignment shall be void.

9.16.3. Keterpisahan / Severability

Jika terdapat ketentuan bahwa salah satu bagian CPS ini salah atau tidak sah, bagian lain dari CPS ini akan tetap berlaku hingga CPS diperbarui.

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated.

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

Peruri CA dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Segala hal terkait pelepasan hak dalam pengadilan harus disampaikan secara tertulis dan ditandatangani oleh Peruri CA.

Peruri CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. To be effective any waivers must be in writing and signed by Peruri CA.

9.16.5. Keadaan Memaksa / Force Majeure

Peruri CA tidak bertanggung jawab atas pelanggaran garansi, keterlambatan atau kegagalan kinerja yang dihasilkan dari peristiwa di luar kendali seperti, tindakan perang, tindakan terorisme, epidemi, kebakaran, dan bencana alam lainnya.

Peruri CA accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, fire, and other natural disasters.

9.17. PROVISI LAIN / OTHER PROVISIONS

Tidak ada ketentuan.

No stipulation.