PERURI CA	Nomor	:	01/003/CA/2018
	Mulai Berlaku	:	23 November 2018
	Versi	:	4.0
	Tanggal Perubahan	:	17 September 2021
	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:* *a. Revise statement in section 1.4* *b. Revise statement in section 9.16.5* *c. Cosmetics change*	*CA Organization*
3	*16 January 2019*	1.2	*Minor Update:* *a. Revise statement in section 1.4.1* *b. Add section 5.6.1* *c. Cosmetics change*	*CA Organization*
4	*13 February 2019*	1.3	*Minor Update:* *a. Root CA Indonesia Alignment* *b. Bilingual Bahasa Indonesia*	*CA Organization*
5	*6 May 2019*	2.0	*Major Update:* *a. Footer* *b. Writing Format* *c. CRL Interval* *d. Limitation of Peruri CA Responsibility* *e. 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:* *a. CRL Interval (Point 4.9.7)*	*CA Organization*
7	*6 March 2020*	2.2	*Minor Update:* *a. Archive retention period* *b. Authentication of Individual Identity*	*CA Organization*
8	*10 October 2020*	2.3	*Minor Update:* *a. Alignment Webtrust For CA*	*CA Organization*
9	*21 January 2021*	3.0	*Major Update:* *a. Change of document number from 002/KRC/KBJ/CPS/XII/2018 to 01/005/CA/2018* *b. Improvements for Ministry of Communications and Informatics (Kominfo) Audit Findings*	*CA Organization*
10	*17 September 2021*	4.0	*Major Update:* *a. Improvements for Ministry of Communications and Informatics (Kominfo) Audit Findings* *b. Change of document number 003/KRC/KBJ/CPS/XII/2018 to 01/003/CA/2018*	*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 elektronik (tidak termasuk *Extended Validation Certificate*) ini adalah:

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

OID	Object / Objek
Peruri CA	2.16.360.1.1.1.3.12.3
CP	2.16.360.1.1.1.3.12.3.1
CPS	2.16.360.1.1.1.3.12.3.2
Verification Level 1	2.16.360.1.1.1.4.1
Verification Level 2	2.16.360.1.1.1.4.2
Verification Level 3	2.16.360.1.1.1.4.3

Verification Level 4	2.16.360.1.1.1.4.4
Compliance : AATL	2.16.360.1.1.1.5.1
SII Type : NIK	2.16.360.1.1.1.6.1
Peruntukan Sertifikat elektronik : Individu	2.16.360.1.1.1.7.1
Peruntukan Sertifikat elektronik : Badan Usaha	2.16.360.1.1.1.7.2

1.3. PARTISIPAN IKP / PKI PARTICIPANTS

1.3.1. Penyelenggara Sertifikat elektronik (PSrE) / Certification Authorities

1.3.1.1. PSrE Induk Indonesia / Root CA Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia yang dioperasikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia.

Indonesia Root CA is the Parent CA from PKI Indonesia which is operated by the Ministry of Communication and Informatics of the Republic of Indonesia.

PSrE Induk Indonesia bertanggung jawab terhadap penerbitan dan pengelolaan sertifikat PSrE Berinduk, sebagaimana dirinci dalam CP PSrE Induk Indonesia.

Root CA Indonesia is responsible for all aspects of the issuance and management of those Subordinate CA certificates, as detailed in Indonesia Root CA's CP

1.3.1.2. PSrE Berinduk / Subordinate CA

Peruri CA merupakan PSrE Berinduk Non-Instansi yang menerbitkan sertifikat elektronik kepada entitas selain pemerintah.

Peruri CA is Subordinate Non-government CA that issues electronic certificates to non-government entities.

Peruri CA tidak menjadi induk dari PSrE lainnya.

Peruri CA will not have further subordinate CA.

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

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

a. Pengendalian terhadap proses pendaftaran;
   a. Control over the registration process;
b. Proses identifikasi dan autentikasi;
   b. Identification and authentication process;
c. Proses penerbitan Sertifikat elektronik;
   c. Certificate manufacturing process;
d. Publikasi Sertifikat elektronik;
   d. Publication of Certificates;
e. Pencabutan Sertifikat elektronik; dan
   e. Revocation of Certificates; and
f. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan sertifikat elektronik Peruri CA yang diterbitkan sesuai dengan CPS ini
   f. Ensuring that all aspects of the services, operations and infrastructure related to Peruri CA Certificates issued under this CPS were performed in accordance

dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

with the requirements, representations, and warranties of this CPS.

1.3.2. Otoritas Pendaftaran (RA) / Registration Authorities

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

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.

1.3.2.1. Fungsi dari RA / Function of Registration Authorities

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

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

a. Menyusun prosedur pendaftaran untuk Pemohon sertifikat elektronik;

a. Establish enrollment procedures for end-user certificate applicants,

b. Melakukan identifikasi dan otentikasi Pemohon sertifikat elektronik;

b. Perform identification and authentication of certificate applicants,

c. Memulai atau meneruskan proses permohonan pembatalan sertifikat elektronik; dan

c. Initiate or pass along revocation requests for certificates, and

d. Menyetujui permohonan untuk memperbarui sertifikat elektronik atau pembaruan kunci atas nama Peruri CA.

d. Approve applications for certificates renewal or re-keying on behalf of Peruri CA.

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

Tidak ada ketentuan.

No stipulation.

1.3.3. Pemilik / Subscribers

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

Subscribers are entities who request and successfully acquire a electronic 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

sebagai Pemohon.

Applicant.

1.3.4. Pihak Pengandal / Relying Parties

Pihak Pengandal adalah entitas yang bertindak mempercayai sertifikat elektronik 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 dalam sertifikat elektronik.

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.

Pihak Pengandal mengandalkan keabsahan keterkaitan antara nama Pemilik dengan Kunci Publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat elektronik.

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 elektronik untuk:

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

Relying party uses the information in the Digital Electronic to:

a. Check the intended use of the certificate;
b. Perform digital signature verification;
c. Checks whether a Electronic Certificate is included in the CRL; and
d. Approval of limits of liability and guarantees.

1.3.5. Partisipan Lain / *Other Participants*

1.3.5.1. Penyedia Layanan Pusat Data / Data Center Vendor

Penyedia Layanan Pusat Data adalah Pihak Ketiga yang menyediakan Layanan Pusat Data untuk Operasional Peruri CA

Data Center Vendor is a third party that provides Data Center Service for Peruri CA Operation.

1.3.5.2. Kementrian Komunikasi dan Informasi / Ministry of Communication and Information

Setiap tahunnya Peruri CA akan membuat laporan kerja ke Kementrian Komunikasi dan Informasi.

Every year Peruri CA will make a work report to the Ministry of Communication and Information.

1.4. KEGUNAAN SERTIFIKAT ELEKTRONIK / *CERTIFICATE USAGE*

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

Penggunaan Sertifikat elektronik Pemilik dibatasi sesuai *Key Usage* dan *Extended*

Subscriber's Certificate usage is restricted by the Key Usage and Extended

Key Usage pada *Certificate Extension*. Sertifikat elektronik Peruri CA dapat digunakan untuk menerbitkan Sertifikat elektronik untuk transaksi yang memerlukan:

a. Autentikasi;
b. Tanda Tangan Elektronik & Non-Repudiasi; dan
c. Enkripsi.

Key Usage of the Certificate Extension. Peruri CA's Certificate can be used to issue Certificates for transactions that require:

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

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

a. Kelas 3 : Sertifikat elektronik dengan Jaminan Menengah. Verifikasi identitas dilakukan dengan membandingkan data kartu identitas terhadap data identitas yang dimiliki oleh pemerintah.
b. Kelas 4 : Sertifikat elektronik dengan Jaminan Tinggi. Verifikasi identitas dilakukan dengan membandingkan data kartu identitas dan data biometrik terhadap data identitas yang dimiliki oleh pemerintah.

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. Class 3 : Medium Assurance Certificate. Identity verification by comparing identity cards data with government-owned identity data

b. Class 4 : High Assurance Certificate. Identity verification by comparing identity cards and biometric data with Government-owned identity data.

Sertifikat elektronik Organisasi hanya dapat diterbitkan dengan tingkat jaminan tinggi (Kelas 4).

Organizational electronic certificates can only be issued with a high assurance certificate (Class 4).

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

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

Kelas Sertifikat elektronik / *Certificate Class*	Tingkat Jaminan */ Assurance Level*		Penggunaan */ Usage*		
	Jaminan Sedang */ Medium Assurance*	Jaminan Tinggi / *High Assurance*	Enkripsi / *Encryption*	*Digital Signature* / Tanda Tangan Digital	*Authentication*/ Autentikasi
Class 3	✓		✓	✓	✓
Class 4		✓	✓	✓	✓

1.4.2. Penggunaan Sertifikat elektronik yang Dilarang / Prohibited Certificate Uses

Sertifikat elektronik 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) adalah entitas yang ada di dalam Peruri CA. PA memiliki peran dan tanggung jawab sebagai berikut:

a. Menetapkan Certificate Policy (CP) / Certification Practice Statement (CPS);

b. Memastikan semua layanan, operasional, dan infrastruktur Peruri CA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan

c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki Level Verifikasi yang kurang lebih setara.

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

a. Approves the Certificate Policy (CP)/Certificate Practice Statements (CPS);

b. Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are well performed in accordance with the requirements, representations, and warranties of the CP; and

c. Approves the establishment of trust relationships with external PKIs that approximately have equivalent verification level.

1.5.1. Organisasi Pengaturan Dokumen / Organization Administering the Document

CP / CPS dan dokumen referensinya dikelola oleh Peruri CA

This CP / CPS and the document referenced herein are maintained by Peruri CA

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

Pemilik Sertifikat Elektronik , Pihak Pengandal, dan pihak ketiga lainnya dapat menghubungi Peruri CA melalui email untuk melaporkan dugaan penyalahgunaan sertifikat elektronik yang diterbitkan Peruri CA.

Subscribers, Relying Parties, and other third parties may contact Peruri CA via email to report suspected misuse of electronic certificates issued by Peruri CA.

Email	:	cs.digitala@peruri.co.id
Phone	:	+622127088222 +622127088333

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

Policy Authority (PA) menentukan kesesuaian konten CPS ini dan kesesuaian antara CPS ini dengan CP. PA menerima masukan dari anggota Peran Terpercaya, regulator, dan auditor eksternal untuk melakukan perubahan terhadap dokumen CP dan/atau CPS, menentukan kesesuaian serta penerapannya.	*Policy Authority (PA) determines suitability of this CPS and the conformance of the CPS to CP. PA receives input from Trusted Role members, regulators, and external auditors to make changes to the CP and/or CPS documents, determining the suitability and application of the document.*

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

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

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

2.1. REPOSITORI / REPOSITORIES

Peruri CA bertanggung jawab memelihara repositori yang dapat diakses publik. Dokumen yang dipublikasikan antara lain, namun tidak terbatas pada:	*Peruri CA is responsible for maintaining publicly accessible repositories. Published documents include, but are not limited to:*
a. Sertifikat Elektronik Peruri CA;	*a. Peruri CA Certificate;*
b. CRL;	*b. CRL;*
c. CP / CPS ;	*c. CP / CPS;*
d. Perjanjian Pelanggan;	*d. Subscriber Agreement;*
e. Kebijakan Privasi; dan	*e. Privacy Policy; and*
f. Perjanjian Pihak Pengandal.	*f. Relying Party Agreement.*
Dokumen dapat dibuat menggunakan dwibahasa. Dalam hal terjadi ketidaksesuaian antara versi bahasa Indonesia dengan versi bahasa Inggris, maka versi bahasa Indonesia didahulukan.	*Documents can be created using bilingual. In the event of a discrepancy between the Indonesian version and the English version, the Indonesian version takes precedence.*
Peruri CA berhak untuk tidak mengunggah dokumen penunjang Operasional lainnya yang tidak bersifat publik.	*Peruri CA reserves the right not to upload other operational supporting documents that are not public.*

2.2. PUBLIKASI INFORMASI SERTIFIKASI / PUBLICATION OF CERTIFICATION INFORMATION

Peruri CA memelihara repositori yang dapat diakses melalui internet, dimana dipublikasikan sertifikat dari Peruri CA, CRL terakhir, dokumen CP/CPS	*Peruri CA maintains a repository accessible through the Internet in which it publishes Peruri CA Certificate , current version of CRL and CP/CPS*
Repositori Legal Peruri CA dapat diakses pada https://ca.peruri.co.id/ca/legal.	*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.	*This CPS and any subsequent changes shall be made publicly available within seven (7) calendar days after its approval.*
Peruri CA mempublikasikan Sertifikat elektronik Pemilik dan data pencabutan sertifikat elektronik dalam waktu 30 (tiga puluh) menit setelah penerbitan.	*Peruri CA publish Subscriber's Certificates data and and revocation data within 30 (thirty) minutes after issuance.*
CRL diperbarui sesuai dengan Frekuensi	*The CRL is updated according to the*

Penerbitan CRL bagian 4.9.7.	*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 dan menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.	*Information published on a repository is public information. Peruri CA provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.*
Peruri CA harus melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.	*Peruri CA shall protect information not intended for public dissemination or modification.*

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 elektronik dengan subyek *Distinguished Name* (DN) yang non-null dan mematuhi standar ITU X.500. Tabel di bawah meringkas DN minimum dari Sertifikat elektronik yang diterbitkan oleh Peruri CA

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 minimum DNs of the certificates issued by the Peruri CA

Tipe Sertifikat elektronik		(DN) Distinguised Name
Sertifikat elektronik Peruri CA		CN=<namaPeruriCA>, O=<Peruri>,C=ID
Sertifikat elektronik Pemilik	Individual	CN=<nama >, Email Address=<email>, OU=Personal, O=Peruri CA, C=IDE
	Individual dengan afiliasi	CN=<nama >, Email Address=<email>,OU=Personal, O=<nama_afiliasi>, C=ID
	Organisasi	CN=<nama_Organisasi>, EmailAddress=<email_organnisasi>, OU=Personal, O=<nama_organisasi>, C=ID

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

Sertifikat elektronik yang diterbitkan sesuai dengan CPS ini bermakna hanya jika nama-nama yang muncul dalam Sertifikat elektronik dapat dipahami dan digunakan oleh Pihak Pengandal. Nama yang digunakan dalam Sertifikat elektronik 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 elektronik 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 elektronik 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 elektronik 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 (DN) dalam sertifikat elektronik harus unik di dalam ranah Peruri CA.	*Distinguished Names in Certificates shall be unique within Peruri CA domain.*
Untuk meningkatkan keunikan DN, Peruri CA dapat menambahkan informasi apabila ditemukan DN yang sama.	*To increase the uniqueness of DN, Peruri CA can add information if the same DN is found.*

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

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat elektronik 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 elektronik 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 penyelidikan hukum apa pun untuk memastikan identitas pemohon baik itu organisasi atau individu. Peruri CA dapat menolak untuk mengeluarkan sertifikat elektronik 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 pada *secure usb token* adalah dengan membandingkan Kunci Publik pada sertifikat dengan Kunci Publik pada PKCS#10	*The method to prove possession of a Private Key in a secure usb token is by comparing the public key on the certificate with the public key in PKCS # 10.*

Untuk Sertifikat pemilik, pasangan kunci dapat dibangkitkan oleh Peruri Digital, dengan syarat Kunci Privat diamankan dengan menggunakan modul kriptografis yang memenuhi persyaratan FIPS 140-2 level 2 dan hanya dapat diakses oleh Pemilik dengan minimal dua faktor autentikasi.

For Subscriber Certificate, key pairs can be generated by Peruri Digital, that the Private Key is secured using a cryptographic module that meets FIPS 140-2 level 2 requirements and can only be accessed by the subscriber with a minimum of two-factor authentication.

3.2.2. Autentikasi Identitas Organisasi / Authentication of Organization Identity

Permohonan Sertifikat atas organisasi hanya dapat dilakukan oleh pihak yang berwenang untuk mewakili organisasi tersebut, dibuktikan dengan surat resmi.

Applications for certificates for organizations *can only be made by the authorized party to represent the organization, as evidenced by an official letter.*

Peruri CA akan memeriksa identitas (KTP) dan jabatan/wewenang dari Pemohon, surat kuasa (jika dibutuhkan), dokumen pendukung pengesahan Badan Hukum/Badan Usaha (termasuk namun tidak terbatas kepada NIB, SIUP, SK Kementerian, NPWP, dan perubahan anggaran dasar terakhir).

Peruri CA will check the identity (KTP) and position/authority of the Applicant, power of attorney (if needed), supporting documents for ratification of Legal Entities/Business Entities (including but not limited to NIB, SIUP, Ministry Decree, NPWP, and the latest amendments to the articles of association).

Peruri CA menyimpan catatan tentang jenis dan rincian dari identifikasi, yang digunakan untuk autentikasi bagi organisasi.

Peruri CA maintains a record of the type and details of the identification, which is used for authentication for the organization.

3.2.3. Autentikasi Identitas Individu / Authentication of Individual Identity

Permohonan untuk menjadi Pemilik Sertifikat elektronik dapat dilakukan oleh individu atau organisasi yang berwenang secara hukum untuk bertindak atas nama calon Pemilik.

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.

Peruri CA melakukan verifikasi identitas individu dengan cara memastikan *liveness detection* dari pemohon serta mendapatkan hasil pencocokan data, termasuk data biometrik, yang dikelola oleh lembaga pemerintah penyelenggara administrasi kependudukan. Peruri CA kemudian menerbitkan sertifikat elektronik level 4.

Peruri CA verifies individual identity by ensuring liveness detection from the applicant and obtaining data matching results, including biometric data, which is managed by the government agency administering population administration. Peruri CA then issues a level 4 electronic certificate.

Dalam hal pencocokan data identitas dilakukan oleh Peruri CA dengan menggunakan data referensi dari lembaga pemerintah penyelenggara administrasi kependudukan, maka diterbitkan sertifikat

In the event that identity data matching is carried out by Peruri CA using reference data from the government agency administering population administration, a level 3 electronic certificate is issued.

elektronik level 3.

Untuk tujuan identifikasi dan otentikasi calon pemilik sertifikat individu wajib memberikan informasi sebagai berikut:

a. Memberikan salinan identitas resmi yang dikeluarkan oleh pemerintah
b. Memberikan salinan identitas resmi yang dikeluarkan oleh perusahaan (untuk calon pemilik sertifikat individu dengan afiliasi)
c. Alamat surat elektronik (*email*)
d. Nomor *handphone*
e. Data Biometrik
f. Peruri CA berhak meminta dokumen pendukung identitas seperti paspor dan SIM

For the purpose of identification and authentication of prospective individual certificate owners, they are required to provide the following information:

a. Give copy of the official identity issued by the government
b. Show the official identity issued by the company (for affiliates)
c. Email address
d. Cell Phone number
e. *Biometric data*
f. Peruri CA has the right to request identity supporting documents such as passports and driving licenses

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

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 elektronik.

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 elektronik 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 elektronik habis, Pemilik tidak dapat meminta penggantian kunci karena Peruri CA tidak melayani penggantian kunci sertifikat elektronik 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 elektronik dicabut selain karena alasan pambaruan, Pemilik harus mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2 untuk mendapatkan sertifikat elektronik 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 elektronik dapat diautentikasi menggunakan Kunci Publik yang terhubung dengan sertifikat elektronik, memvalidasi identitas pemohon sesuai dengan bagian 3.2, dan memastikan keabsahan permintaan, terlepas dari apakah Kunci Privat telah terkompromi.	*Revocation requests shall always be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated Public Key, validating Applicant identity in accordance with Section 3.2 and ensuring the validity of the request, regardless of whether the Private Key has been compromised.*
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 ELEKTRONIK / CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. PERMOHONAN SERTIFIKAT ELEKTRONIK / CERTIFICATE APPLICATION

4.1.1. Siapa yang Dapat Mengajukan Permohonan Sertifikat elektronik / Who Can Submit A Certificate Application

Permohonan sertifikat hanya dapat dilakukan oleh individu atau entitas non-instansi pemerintah. Entitas instansi pemerintah dapat melakukan permohonan sertifikat disertai dengan perjanjian khusus. Identitas yang disertakan pada proses permohonan sertifikat harus dapat diverifikasi. Pemohon wajib menyetujui syarat dan ketentuan Peruri CA. Pemohon wajib memberikan informasi yang cukup sehingga Peruri CA dapat melakukan verifikasi atas dokumen tersebut.	*Certificate applications can only be made by individuals or non-government entities. Government agency entities can apply for a certificate accompanied by a special agreement. The identity included in the certificate application process must be verifiable. The applicant must agree to the terms and conditions of Peruri CA. The applicant must provide sufficient information so that Peruri CA can verify the document.*

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

Pemohon harus bertanggung jawab untuk menyediakan informasi yang akurat serta menyetujui kontrak berlangganan sebelum melakukan permohonan sertifikat elektronik.	*The applicant must be responsible for providing accurate information and agreeing to a subscription contract before applying for an electronic certificate.*
Peruri CA dan RA (jika ada) bertanggung jawab untuk menyediakan dan memproses pendaftaran dengan langkah-langkah berikut: a. memberikan formulir Permohonan Pendaftaran Sertifikat kepada pemohon; b. menerima formulir Permohonan Pendaftaran Sertifikat yang telah diisi oleh pemohon; dan c. memastikan bahwa pemohon telah menyetujui Kontrak Berlangganan yang berlaku.	*Peruri CA and RA (if any) are responsible for providing and processing the registration with the following steps:* *a. provide a Certificate Registration Application form to the applicant;* *b. receive the Certificate Registration Application form which has been filled out by the applicant; and* *c. ensure that the applicant has agreed to the applicable Subscription Contract.*
Pemohon wajib membayar biaya yang berlaku sesuai dengan Kontrak Berlangganan.	The *applicant is required to pay the applicable fees in accordance with the Subscription Contract.*
Peruri CA memelihara sistem dan proses yang mampu mengautentikasi identitas pemohon untuk semua jenis Sertifikat. Sertifikat yang dimaksud menampilkan identitas kepada Pihak Pengandal atau Pemilik.	Peruri *CA maintains systems and processes capable of authenticating applicant identity for all types of Certificates. The certificate in question displays identity to the Relying Party or Owner.*
Peruri CA dan RA (jika ada) melindungi	*Peruri CA and RA (if any) protect*

komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses pendaftaran.

communications and securely store information provided by applicants during the registration process.

4.2. PEMROSESAN PERMOHONAN SERTIFIKAT ELEKTRONIK / 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 elektronik / Approval or Rejection of Certificate Applications

Setelah semua pemeriksaan identitas dan atribut pemohon, konten permohonan untuk sertifikat elektronik juga diperiksa. Dalam hal pemohon tidak memenuhi syarat untuk sertifikat elektronik 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 elektronik / Time to Process Certificate Applications

Semua pihak yang terlibat dalam proses permohonan sertifikat elektronik harus melakukan usaha untuk memastikan permohonan sertifikat elektronik 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 elektronik 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 ELEKTRONIK / CERTIFICATE ISSUANCE

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

Peruri CA memverifikasi sumber permohonan sertifikat elektronik sebelum diterbitkan. Sertifikat elektronik harus diperiksa untuk memastikan bahwa semua *field* dan ekstensi telah diisi

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.

dengan benar.

Peruri CA melakukan otentikasi permohonan sertifikat elektronik, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membangitkan sertifikat elektronik, dan menyediakan sertifikat elektronik kepada Pemohon. Peruri CA mempublikasikan sertifikat elektronik 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.

1. Peruri CA memeriksa dokumen; dan
2. Setelah ditandatangani, sertifikat elektronik akan diserahkan kepada Pemilik.

1. *Peruri CA check documents; and*
2. *After signed, digital certificate will be handed over to Subscriber.*

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

Peruri CA memberitahu Pemilik dalam waktu maksimal tujuh (7) hari kerja tentang penerbitan sertifikat elektronik melalui email.

Peruri CA notify the Subscriber within a maximum seven (7) days of successful certificate issuance via email.

4.4. PENERIMAAN SERTIFIKAT ELEKTRONIK / CERTIFICATE ACCEPTANCE

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

Pemilik harus memeriksa semua informasi tentang Sertifikat elektronik dan menandatangani formulir penerimaan sertifikat elektronik sebelum menggunakan sertifikat elektronik tersebut. Peruri CA harus memberitahu ke Pemilik bahwa mereka tidak dapat menggunakan sertifikat elektronik sebelum dilakukan pemeriksaan semua informasi dari sertifikat elektronik.

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 elektronik.

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 elektronik PSrE, Peruri CA harus membuat prosedur penerimaan dan mendokumentasikan penerimaan Sertifikat elektronik PSrE yang terbitkan pada bagian 4.4.2.	*For the issuance of CA Certificates Peruri CA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate ini section 4.4.1*

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

Peruri CA harus mempublikasikan Sertifikat elektroniknya dalam sebuah repositori sebagaimana tercantum pada bagian 2.2 segera setelah sertifikat elektronik diterbitkan, termasuk ketika menerbitkan informasi pencabutan terkait Sertifikat elektronik tersebut pada repositori. Peruri CA harus mempublikasikan sertifikat elektronik Pengguna Akhir dengan mengirimkannya ke Pemilik sertifikat elektronik.	*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 elektronik oleh Peruri CA ke Entitas Lain / Issuance of Certificate by Peruri CA to Other Entities

Tidak ada ketentuan.	*No stipulation.*

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

4.5.1. Pemilik Kunci Privat dan Penggunaan Sertifikat elektronik / 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 elektronik / 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 elektronik melalui ekstensi sertifikat elektronik dan harus membuat mekanisme untuk menentukan validitas sertifikat elektronik (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 elektronik dan harus mempertimbangkan keseluruhan keadaan dan risiko kerugian sebelum mengandalkan sertifikat elektronik. Mengandalkan tanda tangan atau sertifikat elektronik 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 elektronik.

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. PEMBARUAN SERTIFIKAT ELEKTRONIK / CERTIFICATE RENEWAL

Pembaruan Sertifikat didefinisikan sebagai pembuatan Sertifikat baru yang memiliki rincian yang sama dengan Sertifikat yang telah diterbitkan sebelumnya namun dengan pasangan kunci yang baru dan berisi tanggal yang baru pada *field 'Not After'* dan *'Not Before'*.

Certificate Renewal is defined as the creation of a new Certificate which has the same details as the previously issued Certificate but with a new key pair and contains a new date in the 'Not After' and 'Not Before' fields.

Peruri CA melakukan proses pembaruan sertifikat dengan metode Penggantian Kunci Sertifikat Elektronik sebagaimana tercantum pada bagian 4.7.

Peruri CA performs the certificate renewal process using the Certificate Re-Key method as stated in section 4.7.

4.6.1. Kondisi untuk Pembaruan Sertifikat elektronik / Circumstance for Certificate Renewal

Peruri CA dapat memperbarui Sertifikat Elektronik Pemilik selama:

a. Sertifikat masih aktif, sudah habis masaberlakunya dan atau sudah

Peruri CA may renew a Subscriber Digital Certificate so long as::

a. The original Certificate to be renewed has not been revoked;

dicabut;

b. Kunci Publik dari Sertifikat asli belum masuk daftar hitam karena alasan apa pun;

b. Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan; dan

d. Peruri CA dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya.

b. The Public Key from the original Certificate has not been blacklisted for any reason;

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

d. Peruri CA may renew Certificates which have either been previously renewed.

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

Pemilik yang belum pernah dicabut sertifikat elektroniknya boleh meminta pembaruan sertifikat elektroniknya ke Peruri CA.

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

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat elektronik / Processing Certificate Renewal Requests

Perpanjangan sertifikat elektronik harus memenuhi salah satu dari proses berikut:

a. Proses pendaftaran awal seperti yang dijelaskan pada bagian 3.2; atau

b. 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:

a. Initial registration process as described in Section 3.2; or

b. 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 elektronik Baru ke Pemilik / Notification of New Certificate Issuance to Subscriber

Prosedur pemberitahuan penerbitan sertifikat elektronik 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 elektronik yang Diperbarui / Conduct constituting acceptance of a renewal certificate

Pemilik harus menerima sertifikat elektronik yang diperbarui mengikuti prosedur pendaftaran dan penerimaan sertifikat elektronik yang sama, sebagaimana dinyatakan dalam bagian 4.4.1.

The Subscriber should receive the renewed certificate following the same procedure of registration and receipt of a new certificate, as stated in section 4.4.1.

4.6.6. Publikasi Sertifikat elektronik yang Diperbarui oleh Peruri CA / Publication of the renewal certificate by the CA

Sertifikat elektronik 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 elektronik oleh Peruri CA ke Entitas Lain / Notification of certificate issuance by the CA to other entities

RA (*Registration Authority*) dapat menerima pemberitahuan tentang pembaruan sertifikat elektronik 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 ELEKTRONIK / CERTIFICATE RE-KEY

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

Peruri CA may re-key a Certificate as long as:

a. Sertifikat elektronik asli yang diganti belum pernah dibatalkan/dicabut;

a. The original Certificate to be re-keyed has not been revoked;

b. Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun;

b. The new public key has not been blacklisted for any reason; and

c. Seluruh rincian yang terkait dengan Sertifikat elektronik tersebut tetap akurat dan tidak dibutuhkan validasi baru dan tambahan; dan

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

d. Kunci Privat Peruri CA bocor.

d. 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 elektronik / Processing Certificate Re-Keying Requests

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

Sertifikat elektronik 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 elektronik dari Penggantian Kunci / Conduct Constituting Acceptance of a Re-Keyed Certificate

Pemilik harus menerima sertifikat elektronik 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 elektronik Penggantian Kunci oleh Peruri CA / Publication of the Re-Keyed Certificate by the CA

Sertifikat elektronik 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 elektronik oleh Peruri CA ke Entitas Lain / Notification of Certificate Issuance by the CA to Other Entities

Tidak ada ketentuan.	*No Stipulation.*

4.8. MODIFIKASI SERTIFIKAT ELEKTRONIK / CERTIFICATE MODIFICATION

Modifikasi / mengubah detail dari Sertifikasi tidak diizinkan. Jika terjadi kesalahan selama penerbitan Sertifikat elektronik (contoh: ejaan), sertifikat elektronik dicabut dan dilakukan Proses	*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*

Penerbitan Penggantian Kunci sebagaimana dinyatakan pada bagian 4.3.	*section 4.3.*

4.8.1. Kondisi untuk Modifikasi Sertifikat elektronik / Circumstance for Certificate Modification

Modifikasi / mengubah informasi pada sertifikat elektronik tidak diizinkan.	*Modification of certificate information is not permitted.*

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

Tidak ada ketentuan.	*No stipulation.*

4.8.3. Pemrosesan Permintaan Modifikasi Sertifikat elektronik / Processing Certificate Modification Requests

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

4.9. PENCABUTAN DAN PEMBEKUAN SERTIFIKAT ELEKTRONIK / CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Keadaan untuk Pencabutan / Circumstances for Revocation

Peruri CA harus mencabut sertifikat elektronik pemilik dalam keadaan berikut:	*Peruri CA shall revoke a subscriber's certificate in the following circumstances:*
a. Mengidentifikasi informasi atau komponen afiliasi dari setiap nama di dalam Sertifikat elektronik menjadi tidak valid.	*a. Identifying information or affiliation components of any names in the certificate becomes invalid.*

b. Setiap informasi dalam Sertifikat elektronik menjadi tidak valid.

b. Any information in the certificate becomes invalid.

c. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya.

c. The subscriber can be shown to have violated the stipulations of its subscriber agreement.

d. Ada alasan untuk meyakini bahwa Kunci Privat telah bocor.

d. There is reason to believe the private key has been compromised.

e. Pemilik atau pihak lain yang berwenang (sesuai ketentuan pada CPS) meminta agar sertifikat elektroniknya dicabut.

e. The subscriber or other authorized party (as defined in the CPS) asks for its certificate to be revoked.

f. Peruri CA berhenti beroperasi.

f. Peruri CA termination.

g. Sertifikat elektronik yang dibuat untuk uji coba.

g. The certificate is issued for trial run.

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

Digital certificate must be revoked when the relationship between the subject and its public key defined in the electronic certificate is no longer valid. When this happens, the electronic certificate must be revoked and placed on the CRL and/or added to the OCSP responder. A revoked electronic certificate must be included in all new publications on electronic certificate status information until the electronic certificate expires.

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

Sertifikat elektronik dapat diminta untuk dicabut oleh:

Digital certificates may be requested to be revoked by :

a. Pemilik;

a. Subscriber;

b. Organisasi yang berafiliasi dengan Pemilik yang dapat membuktikan hilangnya hubungan pemilik;

b. Organizations affiliated with the Owner who can prove the loss of the owner relationship;

c. Entitas lain seperti lembaga penegak hukum yang dapat membuktikan terungkapnya Kunci Privat atau penyalahgunaan sertifikat sesuai CP dan CPS; dan

c. Other entities such as law enforcement agencies that can prove the disclosure of Private Keys or misuse of certificates according to CP and CPS; and

d. Peruri CA

d. Peruri CA.

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.

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.

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

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

a. Kunci Privat dari Sertifikat elektronik telah terungkap;

a. The private key of the certificate has been exposed;

b. Penggunaan Sertifikat elektronik tidak sesuai dengan Certification Policy (CP); dan

b. The use of the certificate does not conform to the Certification Policy; and

c. Pemilik Sertifikat elektronik tidak memiliki hubungan dengan institusi.

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 elektronik 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 Peruri CA 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 elektronik 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 elektronik 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 pemilik/perangkat, paling sedikit setiap satu (1) hari. CRL akan berdampak dalam waktu maksimum sepuluh (10) hari.

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 ten (10) working days.

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

In case of private key leakage or other critical security incident, for example revocation of owner's electronic certificate, the latest CRL must be published within 24 hours from the time of revocation according to the timestamp.

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 elektronik, CRL dikeluarkan dan repositori diperbarui. CRL diterbitkan di repositori maksimum dalam tiga puluh (30) menit setelah diterbitkan. Sertifikat elektronik ditandai sebagai "dicabut" dalam repositori.

After the revocation of the electronic certificate, a CRL is issued and the repository is updated. CRLs are published in the repository within a maximum of thirty (30) minutes after they are published. Digital certificates are 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 elektronik tidak disediakan.	*Certificate suspension is not provided.*

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

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

4.9.15. Prosedur untuk Permintaan Pembekuan / Procedure for Suspension Request

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

4.9.16. Batas Masa Pembekuan / Limits on Suspension Period

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

4.10. LAYANAN STATUS SERTIFIKAT ELEKTRONIK / CERTIFICATE STATUS SERVICES

4.10.1. Karakteristik Operasional / Operational Characteristics

Status Sertifikat elektronik 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 elektronik.	*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 sertifikat elektroniknya kadaluarsa atau mencabut sertifikat elektroniknya tanpa meminta sertifikat elektronik yang baru. Terdapat prosedur pencabutan sertifikat elektronik 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 Digital atau disimpan sendiri atas persetujuan Pemilik Kunci.	*Subscriber's private key can be escrowed to Peruri Digital 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:

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

The Peruri CA equipments are always be protected from unauthorized access. The physical security mechanisms Peruri CA has been implemented to:

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

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.

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 Penyimpanan / Media Storage

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 berisi informasi sensitive akan dibuang dengan cara yang aman.	*Waste material containing sensitive information will be disposed of in a safe manner.*

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*	*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.*

data dilakukan dan disimpan diluar lokasi 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.

Backups shall be performed and stored offsite not less than once every seven (7) days. At least one (1) full backup copy shall be stored at an offsite 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.

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).

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:

a. *Head of Peruri CA*

   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan Peruri CA.

b. *Policy Authority*
   Pembuatan atau revisi *Certificate Policy* dan *Certification Practice Statement.*
c. *Internal Auditor*
   Melakukan audit internal operasional Peruri CA.
d. *Network and Security Unit*
   Menjaga seluruh fasilitas termasuk namun tidak terbatas pada barang, orang, fasilitas, perangkat IKP milik Peruri CA.
e. *Administrator of Appliance & HSM*
   Bertanggung jawab terhadap administrasi Perangkat Keras dan HSM dalan seluruh sistem IKP.
f. *Administrator of OS*
   Manajemen halaman WEB, publikasi.
g. *Certification Authority Unit / Key Custodian*
   Pembuatan dan pencabutan pasangan kunci Peruri CA.

Trusted roles including:

a. *Head of Peruri CA*

   Overall responsibility for administering the implementation of the Peruri CA's security practices

b. *Policy Authority*
   Establishment or revision of Certificate Policy and Certification Practice Statement.
c. *Internal Auditor*
   Conduct internal audit of Peruri CA operational.
d. *Network and Security Unit*
   Maintain all facilities including but not limited to goods, people, facilities, PKI equipment belonging to Peruri CA.
e. *Administrator of Appliance & HSM*
   Responsible for hardware and HSM administration in the entire PKI system.
f. *Administrator of OS*
   WEB pages management, publication.
g. *Certification Authority Unit / Key Custodian*
   Generation and revocation of Peruri CA key pairs.

h. *Administrator of CA Unit Application (CA)*
Akses sistem CA, persetujuan siklus penerbitan sertifikat elektronik, pencabutan dan penangguhan sertifikat elektronik.

i. Service Unit

Bertanggung jawab terhadap laporan kegiatan di *service unit* dan penerbitan sertifikat elektronik.

j. Administrator of Service Unit Application (RA)

Akses dan manajemen Sistem RA, Persetujuan untuk identifikasi dilakukan oleh *Validation Specialist.*

k. Validation Specialist
Identifikasi Pengguna dan verifikasi dokumen.

l. Operation & Maintenance Unit
Bertanggung jawab terhadap setiap kegiatan operasional dan pemeliharaan sistem IKP di Peruri CA.

m. 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.

h. Administrator of CA Unit Application (CA)

CA System access, Certificate Lifecycle management approval of the generation, revocation and suspension of certificates.

i. Service Unit
Responsible for activity reports in service units and issuance of electronic certificates.

j. Administrator of Service Unit Application (RA)
RA System accesses and management, LRA management, Approval for identification conducted by Validation Specialist.

k. Validation Specialist
User Identification and documents verification.

l. Operation & Maintenance Unit
Responsible for every operational activity and maintenance of the PKI system at Peruri CA.

m. 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:

a. Pembuatan kunci Peruri CA;

b. Pengaktifan kunci Peruri CA; dan

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:

a. Peruri CA key generation;

b. Peruri CA key activation; and

c.	Pencadangan kunci Peruri CA.	*c. 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 ada personel yang ditugaskan lebih dari satu Peran Terpercaya.	*Individual Peruri CA personnel are specifically designated to roles defined in section 5.2.1 of this CPS and no individual 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:	*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:*
Pembuktian syarat latar belakang, kualifikasi serta pengalaman yang dibutuhkan untuk menjalankan tanggung jawab kerja secara efisien dan cukup. Membuktikan tidak ada catatan criminal.	Proof of the requisite background, qualifications as well as experience necessary to efficiently and sufficiently perform their job responsibilitie. 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:	*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:*
a. Kontak Referensi Pekerjaan;	a. Employment Contact Reference;
b. Pendidikan atau sertifikasi;	b. Education and certification ;
c. Identifikasi Kependudukan (KTP); dan	c. Place of residence; and
d. Catatan Kepolisian	d. Police Certificate of Good Conduct
Peruri CA akan menggunakan teknik investigasi pengganti yang diizinkan oleh	*Peruri CA will utilize a substitute investigative technique permitted by law*

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.

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

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

Sub-Contractor personnel employed to perform functions pertaining to Peruri CA operations shall meet applicable

memenuhi persyaratan yang berlaku yang diatur dalam CPS ini pada poin 5.3.1 dan 5.3.2.

requirements set forth in this CPS in section 5.3.1 and 5.3.2.

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

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, 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):

a. Tipe Kejadian;
b. Nomor rekaman atau urutan rekaman;
c. Tanggal dan waktu kejadian;

a. The type of event;
b. Serial or sequence number of entry;
c. The date and time of the incident;

d.	Asal perekaman;	*d.*	*Source of entry;*
e.	Indikator keberhasilan atau kegagalan jika perlu; dan	*e.*	*A success or failure indicator, where appropriate; and*
f.	Identitas dan entitas dan/atau operator yang menyebabkan kejadian tersebut	*f.*	*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 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.	*Audit logs were reviewed monthly, including verification that the log has not 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. Prosedur Backup Log Audit / Audit Log Backup Procedures

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	*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*

situs lain per bulan.

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 melakukan penilaian 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 elektronik apapun (termasuk yang dicabut atau kedaluwarsa) yang dikeluarkan oleh Peruri CA. Data berikut dicatat pada arsip:

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:

Siklus operasi sertifikat elektronik termasuk permintaan sertifikat elektronik, permintaan pencabutan, permintaan pembangiktan ulang pasangan kunci.

The electronic certificate operation cycle includes electronic certificate requests, revocation requests, key pair re-generation requests.

a. Semua sertifikat elektronik dan CRL yang telah diterbitkan;

a. All certificates and CRLs issued;

b. Log Audit;

b. Audit logs;

c. Data konfigurasi sistem IKP;

c. PKI system configuration data;

d. Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini; dan

d. The CP document and all applicable CPSs including modifications and amendments to these documents; and

e. Data pendaftaran pelanggan Peruri CA.

e. Peruri CA's subscriber document

5.5.2. Periode Retensi Arsip / Retention Period for Archive

Catatan yang diarsipkan harus disimpan

Archived records shall be retained for at

setidaknya selama 5 (lima) tahun. Aplikasi yang dibutuhkan untuk membaca arsip ini harus dipelihara selama masa retensi.	*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 menyimpan catatan arsip dan aplikasi yang dibutuhkan untuk memproses catatan arsip dipelihara dan dilindungi.	*The archived records were protected against unauthorized viewing, modification, deletion, or tampering. The 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 sesuai dengan SOP Management Backup.	*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 in accordance with the Backup Management SOP.*

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)

Dilakukan oleh internal Peruri CA sendiri.	*Performed by internal Peruri CA itself.*

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

Media penyimpanan informasi arsip Peruri CA diperiksa setelah dibuat. Secara berkala, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya Peruri CA, peran terpercaya (trusted roles) dan pihak-pihak lain yang berwenang yang diijinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada peran terpercaya.	Peruri CA archive information storage media are checked after they are created. Periodically, samples of archival information are tested to check the integrity and readability of the information. Only Peruri CA, trusted roles and other authorized parties are allowed to access the archives. Requests to obtain and verify archive information are coordinated by operators in trusted roles.

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;dan
d. Pemohon memastikan integritas informasi.

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

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;and
d. The requester verifies the integrity of information.

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 atau jika ada kebutuhan khusus apabila ada resiko kebocoran kunci. Sejak kunci privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat elektronik. Sertifikat elektronik yang lama masih berlaku, dapat digunakan untuk verifikasi tanda tangan lama sampai semua sertifikat elektronik 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 the risk of Peruri CA's private key leak, the private key can be changed periodically every 10 (ten) years or if there is a special need if there is a risk of key leakage. 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 elektronik yang mengandalkan Sertifikat elektronik 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.

5.7. 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 elektronik 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 mengalami kebocoran, prosedur pada Bagian 5.7.3. diikuti.

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 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:

a. Memberitahu Policy Authority, Network and Security Officer, CA Unit, Service Unit, Operation and Maintenance Unit, dan Head of Peruri CA;

b. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi backup terakhir;

c. Mengoperasikan kembali Peruri CA, memprioritaskan kemampuan membangkitkan informasi status sertifikat elektronik untuk penerbitan CRL sesuai jadwal;dan

d. 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:

a. Notify Policy Authority, Network and Security Officer, CA Unit, Service Unit, Operation and Maintenance Unit, dan Head of Peruri as soon as possible;

b. 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;

c. Re-establish Peruri CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule; and

d. 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 dari Peruri CA, semua Pemilik Sertifikat elektronik dari Peruri CA akan diberitahu, semua sertifikat elektronik Pemilik yang diterbitkan oleh Peruri CA yang terkompromi tersebut dicabut, bersamaan dengan sertifikat elektronik milik Peruri CA.	*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 Policy Authority, Pihak Pengandal, *subscriber,* dan Root CA melalui pengumuman publik. Peruri CA harus menghentikan layanan, memberitahu semua Pemilik dari semua pemilik sertifikat elektronik, melanjutkan dengan pencabutan semua sertifikat elektronik, 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 Peruri CA's private key is lost or leaked, Peruri CA must notify the Policy Authority, Relying Parties, Subscribers, and Root CA through a 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	*The Peruri CA has been operating a backup site, whose purpose is to ensure*

memastikan kelangsungan operasi jika terjadi kegagalan pada situs utama dan untuk mengurangi dampak dari segala jenis bencana alam atau bencana buatan manusia.

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* dan Root CA, Peruri CA memberikan pemberitahuan kepada pemilik kunci dan pihak pengandal melalui email dan/atau pengumuman publik. Rencana tersebut dapat dilihat sebagai berikut:

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:

a. Memberitahu status layanan ke pengguna yang terkena dampak;
b. Mencabut semua sertifikat elektronik;
c. Menyimpan dalam jangka panjang informasi Peruri CA dan pemilik sertifikat elektronik dalam periode yang dinyatakan di sini;
d. Menyediakan dukungan hak dan kewajiban berlaku sesuai dengan perjanjian yang berlaku dan menjawab pertanyaan; dan
e. Menangani dengan tepat pasangan kunci Peruri CA dan perangkat keras yang terkait.

a. Notify the status of the service to affected users;
b. Revoke all certificates;
c. Long-term store information of Peruri CA and its subscribers according to the period herein specified;
d. Provide support for applicable rights and obligations in accordance with applicable agreements and answer questions; and
e. Properly handle Peruri CA key pair and associated hardware.

Dalam kasus Peruri CA mengakhiri operasinya, mereka harus memberitahu ke Root CA Indonesia, PA, dan para Pemilik sebelum penutupan agar sesuai degan Peraturan Perundang-Undangan.	*In the event that Peruri CA terminates its operation, it shall provide notice to Root CA Indonesia, PA, and subscriber prior to termination in compliance with Government regulation.*

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 elektronik, 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 dapat diwakili Peruri Digital.	*Subscriber key pair generation shall be performed by either the subscriber or representative.*
Pemilik harus membangkitkan kunci dalam suatu perangkat dengan standar FIPS 140-2.	*Pemilik shall generate keys within a secure FIPS 140-2.*

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

Peruri CA tidak mengirimkan kunci privat ke pemilik sertifikat elektronik.	*Peruri CA does not deliver private key to subscribers.*
Apabila dibutuhkan Peruri Digital dapat membangkitkan pasangan kunci pemilik dari *Secure USB Token* dan menyerahkan nya secara langsung setelah penerbitan	*If needed Peruri Digital can generate Subscriber key pair using Secure USB Token and submit it directly after certificate issuance.*

sertifikat.

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

Peruri Digital atas nama Pemilik membangkitkan pasangan kunci dan mengirimkan Kunci Publiknya kepada Peruri CA dalam sebuah CSR dalam proses permohonan penerbitan sertifikat.	*Peruri Digital on behalf of the Subscriber generates a key pair and sends its Public Key to Peruri CA in a CSR in the certificate issuance application process.*
Peruri CA hanya menerima permohonan penerbitan sertifikat berdasarkan CSR dari lingkungan Peruri.	*Peruri CA only accepts requests for certificate issuance based on CSR from the Peruri environment.*

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

Peruri CA menyediakan mekanisme publikasi untuk penyampaian semua sertifikat elektronik yang memuat kunci publik Peruri CA melalui repositori sesuai bagian 2.1.	*Peruri CA provides mechanisms for the secure digital delivery of all certificates containing public key, via repository according to section 2.1 .*
Mekanisme tersebut diamankan menggunakan SSL.	*That mechanisms is secured using SSL.*

6.1.5. Ukuran Kunci / Key Sizes

Certificate	Encryption Algorithm	Key Length
Peruri CA	RSA	4096
End User	RSA	2048

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

Peruri CA membangkitkan Pasangan Kunci PSrE dengan menggunakan modul kriptografi sesuai standar FIPS 140-2 level 3 dan menggunakan suatu metode yang wajar untuk memvalidasi kesesuaian Kunci Publik.	*Peruri CA generates Key Pairs using a cryptographic module according to the FIPS 140-2 level 3 standard and uses a reasonable method to validate Public Key compliance.*
Peruri CA akan melakukan pemeriksaan secara berkala untuk menguji ukuran Kunci dan memastikan pemutakhiran berdasarkan standar keamanan industri dan persyaratan regulasi.	*Peruri CA will conduct periodic checks to test the size of the Key and ensure updates to industry security standards and regulatory requirements.*

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 elektronik (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 untuk mengaktifkan sebuah kunci privat Peruri CA yang disimpan di dalam modul.	*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 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. 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	*Peruri's private signature key was backed up under the same multiparty control as*

dengan kunci privat asli. Paling tidak satu salinan dari kunci privat harus disimpan *off-site*. Semua salinan kunci privat Peruri CA dan pemilik harus dilindungi dengan cara yang sama dengan aslinya.

the original signature key. At least one copy of the private signature key was stored off-site. All copies of the Peruri CA and subscriberprivate 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 privat harus ditangani dengan cara yang sama dengan kunci privat.

If a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport. Transport keys used to encrypt private keys will be handled in the same 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.*
Peruri CA tidak melakukan penghancuran kunci Pemilik.	*Translation results Peruri CA does not destroy subscriber key.*

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

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

Periode operasi pasangan kunci ditentukan oleh periode operasional sertifikat elektronik yang sesuai. Jangka waktu operasional maksimum kunci ditentukan selama sepuluh (10) tahun untuk Peruri CA. Sementara untuk kunci Pemilik memiliki periode 1 tahun.	*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. The subscriber key has a period of 1 year.*

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

Tidak ada ketentuan.	*No stipulation.*

6.5. KENDALI KEAMANAN KOMPUTER / COMPUTER SECURITY CONTROLS

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

Peruri CA memastikan bahwa sistem yang menjaga perangkat lunak Peruri CA 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.	*Peruri CA ensures that the systems maintaining Peruri CA software and data 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 menggunakan kunci privat.	*The Peruri CA server associated with the private signing key is operated using the private key.*

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

Semua komponen Peruri CA secara berkala disinkronisasikan dengan sebuah layanan waktu, seperti contohnya layanan *atomic clock* atau *Network Time Protocol* (NTP). Sebuah otoritas khusus untuk menyediakan waktu yang terpercaya juga bisa digunakan jika perlu, misalnya dengan membentuk sebuah otoritas *timestamp* tersendiri. Waktu yang didapat dari layanan waktu diatas akan digunakan untuk menentukan waktu pada saat:	*All Peruri CA components are periodically synchronized with a time service, such as an atomic clock or Network Time Protocol (NTP) service. A special authority to provide reliable times can also be used if necessary, for example by establishing a separate timestamp authority. The time obtained from the above time service will be used to determine the time when:*

a. Validitas waktu permulaan untuk sebuah sertifikat Peruri CA

b. Pencabutan sertifikat Peruri CA

c. Pembaruan CRL, dan

d. Penerbitan sertifikat pemilik dan entitas

a. Start-up validity for a Peruri CA certificate

b. Revocation of Peruri CA certificate

c. CRL update, and

d. Issuance of certificates of owners and entities

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

Electronic or manual procedures can be used to maintain accurate timing of the system. Hours matching is an auditable activity.

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

7.1. PROFIL SERTIFIKAT ELEKTRONIK / CERTIFICATE PROFILE

Profil sertifikat dan *Certificate Revocation List (CRL)* mengikuti RFC 5280 Internet X.509 *Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) profile.*

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

Peruri CA 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.

7.1.1. Nomor Versi/Version Number(s)

Peruri CA menerbitkan sertifikat elektronik X.509 versi 3 (mengisi versi field dengan integer "2").

Peruri CA issue X.509 version 3 certificates (fill the field version with integer "2").

7.1.2. Ekstensi Sertifikat elektronik / Certificate Extensions

Peruri CA memakai ekstensi sertifikat elektronik 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 elektronik 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".

Field	Sertifikat Peruri CA	Sertifikat Pemilik	
		Level 3	Level 4
Critical	True	True	True
digitalSignature	True	True	True
nonRepudation	False	False	True
keyEncipherment	False	False	False
dataEncipherment	False	False	False
keyAgreement	False	False	False
keyCertSign	True	False	False
cRLSign	True	False	False
encipherOnly	False	False	False
decipherOnly	False	False	False

7.1.2.2. Perluasan Kebijakan Sertifikat elektronik / Certificate Policies Extension

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

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

ditentukan dalam bagian 7.1.8.

policy qualifiers set forth in section 7.1.8.

7.1.2.3. Batasan Dasar / Basic Constraint

Ekstensi *Basic Constraints* Sertifikat elektronik X.509 Versi 3 harus memiliki *field* CA yang diisi TRUE. Ekstensi *Basic Constraints* Sertifikat elektronik Pengguna Akhir harus memiliki *field* CA yang diisi FALSE. *Field criticality* dari ekstensi ini harus diisi TRUE untuk Sertifikat elektronik CA, tapi boleh diisi TRUE atau FALSE bagi Sertifikat elektronik Pengguna Akhir.

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 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

Secara baku, *ExtendedKeyUsage* diatur sebagai suatu ekstensi non-kritikal. Sertifikat elektronik yang diterbitkan oleh Peruri CA dapat memuat ekstensi ExtendedKeyUsage sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang diterbitkan. Semua sertifikat elektronik harus mengandung sebuah ekstensi extended key usage untuk tujuan bahwa sertifikat tersebut telah diterbitkan untuk end-user, dan tidak boleh memuat nilai anyEKU.

By default, ExtendedKeyUsage is set as a non-critical extension. Digital Certificate issued by Peruri CA may contain the ExtendedKeyUsage extension as a form of technical restriction on the use of the certificates they issue. All Owner certificates must contain an extended key usage extension for the purpose that the certificate has been issued to end-users, and must not contain anyEKU values.

7.1.2.5. Titik Distribusi CRL / CRL Distribution Points

Sertifikat elektronik 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 elektronik. *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 elektronik X.509 Versi 3 biasanya diisi dengan ekstensi authorityKeyIdentifier. Metode untuk menghasilkan key identifier yang berbasis pada kunci publik dari Peruri CA, harus

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

dihitung sesuai dengan salah satu metode yang diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini harus diisi FALSE.	*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 elektronik 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 elektronik 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 elektronik.	*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 elektronik / Certificate Policy Object Identifier

Sertifikat elektronik yang diterbitkan di bawah CPS ini menggunakan nomor OID 2.16.360.1.1.1.3.12.3 yang mengacu pada PSrE Induk.	*Certificates issued under this CPS use OID number 2.16.360.1.1.1.3.12.3 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 elektronik 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 CRL X.509 versi 2.	*Peruri CA shall issue X.509 CRL version 2.*

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.*
Peruri CA wajib untuk memberikan laporan berkala minimal 1 Tahun sekali kepada Kementerian Komunikasi dan Informatika Republik Indonesia.	*Peruri CA is required to provide periodic reports at least once a year to the Ministry of Communication and Information Technology of the Republic of Indonesia.*

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:	*Compliance auditors must possess these qualifications:*
a. Auditor harus dilaksanakan oleh personel yang sudah melalui proses asesmen dan memenuhi syarat;	*a. The auditor must be carried out by personnel who have gone through the assessment process and qualified;*
b. Auditor harus memiliki pengetahuan yang cukup tentang tanda tangan elektronik, sertifikat digital, X.509 versi 3 PKI Certificate Policy and Certification Practices Framework, UU ITE (UU No 11 2008 dan UU No 19 2016), PP PSTE (PP71 2019), Peraturan Menteri Komunikasi dan Informatika no 11/2018;	*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. Auditor harus emiliki 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; dan

d. Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and

e. Auditor harus 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 Peruri CA 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 Peruri 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

Ketika auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana Peruri CA dirancang atau dioperasikan atau dipelihara terhadap persyaratan CPS ini, tindakan berikut harus dilakukan:

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

a. Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.

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

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

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

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 bisnis. Audit internal dilakukan minimal 1 tahun sekali.

Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes. Internal audit is carried out at least once a year.

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 memperbarui sertifikat termasuk dalam hal penerbitan ulang sertifikat. Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat. Mengenai detil biaya permohonan penerbitan atau pembaruan sertifikat tercantum pada setiap dokumen terkait *Manual Marketing, Sales, and Product*.	*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. The details of the application fee for certificate issuance or renewal are listed in each document related to Manual Marketing, Sales, and Product.*

9.1.2. Biaya Pengaksesan Sertifikat / Certificate Access Fees

Peruri CA akan mengenakan biaya administrasi untuk setiap akses ke repositori yang berisi sertifikat yang telah diterbitkan.	*Peruri CA will 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 akan mengenakan biaya tambahan bagi Pemilik untuk setiap akses ke informasi status atau informasi pencabutan sertifikat.	*Peruri CA will charge additional fees to Subscribers for any access to certificate revocation status or certificate information status.*

9.1.4. Biaya Layanan Lainnya / Fees for Other Services

Peruri CA akan mengenakan biaya untuk mendapatkan layanan tambahan lainnya di luar penerbitan dan pembaruan sertifikat.	*Peruri CA will charge a fee for other additional services beyond certificate issuance and renewal.*

9.1.5. Kebijakan Pengembalian Sertifikat/ Refund Policy

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

9.2. TANGGUNG JAWAB KEUANGAN / FINANCIAL RESPONSIBILITY

9.2.1. Cakupan Asuransi / Insurance Coverage

Peruri CA menjamin kerugian akibat kegagalan layanan Penyelenggaraan Sertifikasi Elektronik, kesengajaan, dan/atau kelalaian kepada orang, badan	*Peruri CA guarantees losses due to failure of Electronic Certification Implementation services, intentional, and/or negligence to people, business entities, or agencies due*

usaha, atau Instansi karena kegagalannya dalam mematuhi kewajiban sebagai PsrE berinduk sesuai dengan ketentuan perundang-undangan yang diatur dalam dokumen Kebijakan Jaminan.

to their failure to comply with obligations as CA in accordance with the provisions of the legislation as stipulated in the Guarantee Policy document.

9.2.2. Aset Lainnya / Other Assets

Peruri CA memiliki sumber modal usaha yang cukup untuk menjalankan kegiatan operasionalnya dan menjalankan fungsinya.

Peruri CA has sufficient sources of venture capital to carry out its operational activities and carry out its functions.

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

Batasan tanggung jawab Peruri CA kepada Pemilik Sertifikat atas setiap perselisihan yang timbul dari atau sehubungan dengan layanan Peruri CA atau penggunaan Situs oleh Pemilik Sertifikat, terlepas dari forum penyelesaian perselisihan atau terlepas dari tuntutan berasal dari perbuatan melawan hukum, wanprestasi atau lain sebagainya, dijelaskan lebih lanjut pada Kebijakan Jaminan.

The limitations of Peruri CA's liability to the Certificate Owner for any disputes arising out of or in connection with Peruri CA's services or the use of the Site by the Certificate Owner, regardless of the dispute resolution forum or regardless of claims stemming from unlawful acts, default or otherwise, are further explained. on the Warranty Policy.

9.3. KERAHASIAAN INFORMASI BISNIS / CONFIDENTIALITY OF BUSINESS INFORMATION

Peruri CA melindungi kerahasiaan informasi bisnis sensitif yang dapat mengarah pada penyalahgunaan atau penipuan. Peruri 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. Peruri 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 termasuk dalam kategori informasi rahasia antara lain:

The following items are classified as being confidential information and therefore are subject to reasonable care and attention Peruri CA:

a. Informasi pribadi data pelanggan sebagaimana dijabarkan pada Bagian 9.4;

a. Personal Information form subscriber as detailed in Section 9.4;

b. Rekam jejak audit (*audit logs*) dari

b. Audit logs from Peruri CA and RA

sistem Peruri CA dan RA;

c. Data aktivasi pada saat pengaktifan Kunci Privat Peruri CA sebagaimana dijabarkan pada Bagian 6.4;

d. Dokumentasi bisnis proses Peruri CA termasuk dokumen *Disaster Recovery Plans (DRP) dan Business Continuity Plans (BCP)*;

e. Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0; dan

f. Dokumen terkait *Business Plan,* hasil VA / *pentest*, topologi *network* dengan *IP Address*, hasil penilaian kerja karyawan, *log system administrator,* dan dokumen lainnya.

systems;

c. Activation data used to active Peruri CA Private Keys as detailed in Section 6.4;

d. Peruri CA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP);

e. Audit reports from independent auditors as described in Section 8.0; and

f. Documents related to the Business Plan, VA / pentest results, network, topology with IP Address, employee performance appraisal results, system administrator logs, and other documents.

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:

a. Pelatihan atau peningkatan *awareness;*

b. Perjanjian kontrak pegawai; dan

c. NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

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

a. Training;

b. Contracts with employees; and

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

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

Peruri CA harus melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan Pemilik baik terhadap Peruri CA maupun RA. Arsip yang dikelola oleh Peruri CA tidak boleh dirilis kecuali yang diizinkan pada Bagian 9.4.1.

Peruri CA shall protect all subscribers personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by Peruri CA shall not be released except as allowed by Section 9.4.1.

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. Informasi yang disimpan debat berbentuk digital maupun kertas. *Backup* informasi pribadi harus dienkripsi setiap akan dipindahkan ke media *backup.*

Peruri CA has implemented security measure to protect private information. The information stored in the debate is in digital or paper form. Backups of personal information must be encrypted each time it is transferred to the backup media.

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

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. Peruri CA harus mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam *Subscriber Agreement*. *Subscriber Agreement* juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang

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

digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh Peruri CA.

service being offered by the Peruri CA.

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

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

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

9.4.7. 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; dan
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 in 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; and
d. Peruri CA maintain a repository of public information on its website.

9.6.2. Pernyataan dan Jaminan RA / RA Representations and Warranties

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

a. Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang

RAs warrant that:

a. There are no fallacy on Certificate that have been known or came from the entity who gives an

menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat;

acknowledgement on Certificate application or Certificate issuance;

b. Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat; dan

b. There are no false information in the Certificate carried by the entity that approves the registration of the Certificate as a result of inaccuracy in the Certificate Registration Management; and

c. Peruri CA mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP dan dituangkan dalam kontrak.

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

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

Pemilik Sertifikat menjamin bahwa:

Subscribers warrant that:

a. 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;

a. 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;

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

b. Their private key is protected and that no unauthorized person has ever had access to the subscriber's private key;

c. Sudah melakukan *review* terhadap informasi dari sertifikat;

c. Have thoroughly reviewed the certificate information;

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

d. All information supplied by the subscriber and contained in the certificate is true,;

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

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

f. Segera:

g. Promptly:

i. Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan

i. Request revocation of the certificate, and cease using it and its associated private key,

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,

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,

ii. 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, dan

ii. Request revocation of the certificate, and cease using it, if any information in the certificate is or becomes incorrect or inaccurate, and

iii. Menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut.

iii. Stop using the private key whose public key is listed in a digital certificate after the certificate is revoked.

g. Akan menanggapi instruksi Peruri CA terkait kebocoran atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;

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

h. 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*;

h. 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

i. Pemilik sertifikat adalah pengguna akhir dan bukan merupakan penyelenggara sertifikat elektronik, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam sertifikat digital untuk tujuan penandatangan sertifikat digital penyelenggara sertifikat elektronik lain.

i. The owner of the certificate is the end user and is not the provider of the electronic certificate, and does not use the private key whose public key is listed in the digital certificate for the purpose of signing the digital certificate of another electronic certificate provider.

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

Pihak yang mengandalkan Sertifikat Peruri CA menjamin bahwa:

a. Memiliki kemampuan teknis untuk menggunakan sertifikat;
b. 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;
c. Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi kebocoran/penyalahgunaan pada kunci privat;
d. 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; dan
e. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

Peruri CA's Certificate relying party guarantee that:

a. Have the technical capability to use certificates;
b. 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;
c. Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised;
d. 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; and
e. 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:

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

a. Kecuali untuk jaminan yang telah tercantum dalam CPS dan kontrak perjanjian dan sepanjang diizinkan oleh hukum, Peruri CA mengabaikan semua jaminan atau kondisi lainnya (tersurat, tersirat, lisan atau tertulis), termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu;
b. Penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Pasangan Kunci dan Penggunaan Sertifikat); dan
c. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing sertifikat.

a. Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, Peruri CA disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use;
b. Misuse of a certificate that is inconsistent with its usage as shown in section 4.5 (Key Pair and Certificate Usage); and
c. 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:

a. 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;
b. Semua kerusakan yang disebabkan oleh *force majeure;*
c. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau *trojan*) diluar perangkat Peruri CA;
d. Semua kesalahan data informasi sertifikat yang berasal dari pemilik sertifikat setelah periode verifikasi data selesai; dan
e. Sertifikat yang tidak diterbitkan atau dikelola sesuai dengan Kebijakan Sertifikat dan / atau Pernyataan praktik Sertifikasi.

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

a. 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;
b. All damage caused by the force majeure condition;
c. All damage caused by the malware (i.e virus or trojan) outside Peruri CA devices;
d. All incorrect certificate information that comes from subscriber after data verification period is complete; and
e. 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

9.9.1. Ganti Rugi oleh Peruri CA / Indemnification by Peruri CA

Kewajiban ganti rugi Peruri CA harus ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.	*Peruri CA's indemnification obligations must be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.*
Peruri CA tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.	*Peruri CA has no liability for the improper use of Certificate.*

9.9.2. Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Relying Parties

Diatur dalam Kontrak Berlangganan dan atau *Subsciber Agreement.*	*Regulated in the Subscription Contract and or Subsciber Agreement.*

9.9.3. Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Relying Parties

Diatur dalam Kontrak Berlangganan dan atau *Relaying Party Agreement.*	*Regulated in the Subscription Contract and or Relaying Party Agreement.*

9.10. JANGKA WAKTU BERLAKU DAN PENGAKHIRAN / VALIDITY PERIOD AND TERMINATION

9.10.1. Jangka Waktu Berlaku / Validity Period

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

sertifikat yang telah terbit melalui laman atau repositori.

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 elektronik, 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

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

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

9.12.2. Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

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

Each time the CPS is changed, the CPS will be announced within seven (7) working days of the change and is known by all interested parties and has been signed (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 Policy Authority 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 Policy Authority 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 CPS 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 CPS, 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 diatur, ditafsirkan, dan dipahami sesuai dengan aturan hukum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat dari Peruri CA ataupun produk/ layanan lainnya. Termasuk apabila sertifikat Peruri CA dipakai untuk kebutuhan komersil atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan Peruri CA, tetap menerapkan aturan hukum di Indonesia. Para pihak, termasuk partner dari Peruri CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.	*This CPS is governed, construed and interpreted in accordance with the laws of Indonesia. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of certificates Peruri CA or other products and services. The laws of Indonesia also apply to all CAs commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to CAs products and services where CAs acts as a provider, supplier, beneficiary receiver or otherwise.* *Each party, including Peruri CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Indonesia.*

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

Peruri CA mematuhi hukum yang berlaku di Indonesia. Ekspor berbagai jenis perangkat lunak tertentu yang digunakan dalam berberapa produk dan layanan manajemen Sertifikat publik Peruri CA dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang	*Peruri CA complies with applicable laws of Indonesia. Export of certain types of software used in certain CAs public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including Peruri CA, Subscribers*

berwenang. Para Pihak (termasuk Peruri CA, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi undang-undang dan regulasi ekspor yang berlaku di Indonesia.

and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in 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 Jika terdapat ketentuan dari dari CPS ini, termasuk pembatasan dari klausul pertanggungan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CPS ini selanjutnya akan ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CPS ini yang menjelaskan batasan tanggung jawab, dimaksudkan dapat dipisahkan dan bersifat independen dari ketentuan lain dan harus diberlakukan dengan sebagaimana harusnya.

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

9.16.4. 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. Kegagalan Peruri CA dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak Peruri CA untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CPS ini. Segala hal terkait pelepasan hak dalam pengadilan harus disampaikan secara tertulis dan ditandatangani oleh Peruri CA.

Peruri CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Peruri CA's failure to enforce a provision of this CP does not waive Peruri CA's right to enforce the same provisions later or right to enforce any other provisions of this CPS. 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 kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada diluar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga. Peruri CA wajib menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Peruri CA.	*CAs shall not be liable for any failure or delay in its performance under this CPS due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, power and failure of telecommunications lines, lack of Internet access, sabotage, terrorism, and governmental action or any unforeseeable events or situations. Peruri CA is required to provide BCP and DRP with reasonable control in accordance with Peruri CA's capabilities.*

9.17. PROVISI LAIN / OTHER PROVISIONS

Tidak ada ketentuan.	*No stipulation.*

"Sertifikat elektronik" 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 elektronik.	***"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 Pengandal untuk memverifikasi Tanda Tangan Digital yang dibuat oleh pemegangnya.	***"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.*
"*Pihak Pengandal*" entitas yang mempercayai pada informasi yang terkandung dalam sertifikat elektronik atau token stempel waktu.	***"Relying Party"*** *means an entity that relies upon either the information contained within a certificate or a time-stamp token.*
"Peruri Digital" adalah unit bisnis Peruri yang memberikan layanan tandatangan digital. Bertindak atas nama pemilik sertifikat untuk membangkitkan pasangan kunci, membuat CSR, dan menggunakan kunci untuk kebutuhan penandatanganan dokumen elektronik. Menerapkan kontrol pengamanan terhadap kunci privat dan 2FA untuk penggunaan penandatanganan .	***"Peruri Digital"*** *is Peruri's business unit that provides digital signature services. Act on behalf of the certificate owner to generate key pairs, generate CSRs, and use keys for electronic document signing needs. Implement security controls over private keys and 2FA for signing usage.*