PERURI CA	Nomor	:	01/003/CA/2018
	Mulai Berlaku	:	23 November 2018
	Versi	:	4.1
	Tanggal Perubahan	:	30 Juni 2022
	OID	:	2.16.360.1.1.1.3.12.3.2
	Klasifikasi	:	Biasa

Peruri CA
Certificate Practice Statement

Disetujui Oleh / Approved By:

Farah Fitria R.

Policy Authority

CATATAN REVISI / REVISION NOTE

NO/ NO	TANGGAL / DATE	VERSI / VERSION	DESKRIPSI / DESCRIPTION	OLEH / BY
1	*23 November 2018*	1.0	*Initial Release*	*Peruri CA*
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*	*Peruri CA*
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*	*Peruri CA*
4	*13 February 2019*	1.3	*Minor Update:* *a. Indonesia Root CA Alignment* *b. Bilingual Bahasa Indonesia*	*Peruri CA*
5	*6 May 2019*	2.0	*Major Update:* *a. Footer* *b. Writing format* *c. CRL interval* *d. Limitation of Peruri CA responsibility* *e. Sections 4.12.1, 4.9.7, 6.1.2, 6.2.1, 6.2.5, and 9.81*	*Peruri CA*
6	*10 July 2019*	2.1	*Minor Update:* *a. CRL Interval (Section 4.9.7)*	*Peruri CA*
7	*6 March 2020*	2.2	*Minor Update:* *a. Archive retention period* *b. Authentication of individual identity*	*Peruri CA*
8	*10 October 2020*	2.3	*Minor Update:* *a. Alignment Webtrust for CA*	*Peruri CA*
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 (MCIT) Audit Findings*	*Peruri CA*
10	*17 September 2021*	4.0	*Major Update:* *a. Improvements for Ministry of Communications and Informatics (MCIT) Audit Findings* *b. Change of document number 003/KRC/KBJ/CPS/XII/2018 to 01/003/CA/2018*	*Peruri CA*
11	*30 June 2022*	4.1	*Minor Update:* *a. Improvements for Ministry of Communications and Informatics (MCIT) Audit Findings* *b. Additional rquirements for foreign citizens*	*Peruri CA*

DAFTAR ISI / TABLE OF CONTENTS

1. PENDAHULUAN / INTRODUCTION

1.1. RINGKASAN / OVERVIEW

Infrastruktur Kunci Publik (IKP) Peruri CA adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikasi 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 mengacu kepada CP Peruri CA, selanjutnya CP Peruri CA mengacu kepada CP PSrE Induk Indonesia.

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

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

This CPS defines the procedural and operational requirements that Peruri CA adheres to when issuing and managing electronically signed objects within Peruri CA's PKI. This CPS also comply with the current version of Indonesia Root CA 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 (CPS) Peruri CA. Object Identifier (OID) value used for Electronic Certificate (not including EV certificate) for this CPS is:

OID	Objek / Object
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

OID	Objek / Object
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 (*Individual)*	2.16.360.1.1.1.7.1
Peruntukan Sertifikat Elektronik : Badan Usaha (*Business Entity)*	2.16.360.1.1.1.7.2

1.3. PARTISIPAN IKP / PKI PARTICIPANTS

1.3.1. Penyelenggara Sertifikasi Elektronik (PSrE) / Certification Authorities (CA)

1.3.1.1 PSrE Induk Indonesia / Indonesia Root CA

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia yang dioperasikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo).	*Indonesia Root CA is the root CA of Indonesia PKI which is operated by the Ministry of Communications and Informatics Technology of the Republic of Indonesia (MCIT).*
PSrE Induk Indonesia bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat Elektronik PSrE Berinduk, sebagaimana dirinci dalam CP PSrE Induk Indonesia.	*Indonesia Root CA is responsible for all aspects of the issuance and management of those Subordinate CA Electronic 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, Tanda Tangan Elektronik, dan Segel Elektronik kepada orang, badan usaha atau badan hukum selain pemerintah.	*Peruri CA is Subordinate Non-government CA that issues Electronic Certificate, Digital Signature, and Electronic Seal to person, business entity or legal entity other than non-government entity.*
Peruri CA tidak menjadi induk dari PSrE lainnya dan tidak berinduk kepada PSrE lain.	*Peruri CA will not have further subordinate CA and not become others 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 Electronic 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. Process of Electronic Certificate issuance;

d. Publikasi Sertifikat Elektronik;

d. Publication of Electronic Certificates;

e. Pencabutan Sertifikat Elektronik; dan

e. Revocation of Electronic Certificates; and

f. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan Sertifikat Elektronik Peruri CA yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

f. Ensuring that all aspects of the services, operations and infrastructure related to Peruri CA Electronic Certificates issued under this CPS were performed in accordance with the requirements, representations, and warranties of this CPS.

1.3.2. Otoritas Pendaftaran (RA) / Registration Authorities (RA)

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 RA sendiri di internal, dan tidak melakukan proses verifikasi melalui mitra bisnis.

Peruri CA may designate specific Registration Authority (RA) to perform the Subscriber identification and authentication, and Electronic Certificate request and revocation functions defined in the CP and related documents. Peruri CA has its own internal RA, and does not carry out the verification process through business partners.

1.3.2.1. Fungsi dari Otoritas Pendaftaran (RA) / Function of Registration Authorities (RA)

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 dan melaksanakan prosedur pendaftaran untuk Pemohon Sertifikat Elektronik;

a. Establish and execute enrollment procedures for end-user Electronic Certificate Applicants;

b. Melakukan identifikasi dan autentikasi Pemohon Sertifikat Elektronik;

b. Perform identification and authentication of Electronic Certificate Applicants;

c. Memulai atau meneruskan proses permohonan pencabutan Sertifikat Elektronik; dan

c. Initiate or pass along revocation requests for Electronic Certificates; and

d. Menyetujui permohonan untuk memperbarui Sertifikat Elektronik atau pembaruan kunci atas nama Peruri CA.

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

1.3.2.2. Persyaratan Khusus Otoritas Pendaftaran (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 orang, badan usaha, atau badan hukum 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, Pemilik disebut sebagai Pemohon.

Pemohon terdiri atas 2 (dua) yaitu:

a. Pemohon individu terdiri atas Warga Negara Indonesia (WNI) atau Warga Negara Asing (WNA).
b. Pemohon badan usaha terdiri atas organisasi atau entitas non pemerintah.

Subscriber is a person, business entity, or legal entity who requests and successfully acquire an Electronic Certificate signed by Peruri CA. Subscriber refers to both the subject of Electronic Certificate and the entity which has contract agreement with Peruri CA. Prior to verification of identity and issuance of an Electronic Certificate, a Subscriber is an Applicant.

There are 2 (two) Applicants namely:

a. Individual Applicants consist of Indonesian Citizens (WNI) or Foreign Citizens (WNA).
b. Business entity Applicants consist of organization or non-governmental entity.

1.3.4. Pihak Pengandal / Relying Parties

Pihak Pengandal adalah pihak yang bertindak mempercayai Sertifikat Elektronik dan/atau Tanda Tangan Elektronik yang diterbitkan oleh Peruri CA. Pihak Pengandal terlebih dahulu memeriksa respon *Certificate Revocation Lists* (CRL) dan/atau *Online Certificate Status Protocol* (OCSP) yang sesuai sebelum memanfaatkan informasi yang ada dalam Sertifikat Elektronik.

Relying Parties are parties that act reliance on an Electronic Certificate and/or digital signature issued by Peruri CA. Relying Parties must check the appropriate Certificate Revocation Lists (CRL) and/or Online Certificate Status Protocol (OCSP) response prior to relying on information featured in an Electronic 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.

The Relying Party 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 Electronic Certificate.

Pihak Pengandal menggunakan informasi dalam Sertifikat Elektronik untuk:

a. Memeriksa tujuan penggunaan Sertifikat Elektronik;
b. Melakukan verifikasi Tanda Tangan Elektronik;

The Relying Party uses the information in the Electronic Certificate to:

a. Check the usage purpose of the Electronic Certificate;
b. Perform digital signature *verification;*

c. Memeriksa apakah Sertifikat Elektronik termasuk di dalam CRL; dan

d. Penyetujuan batas tanggung jawab dan jaminan.

Pihak Pengandal dapat meliputi bank, perusahaan *e-commerce*, instansi penyelenggara negara, dan entitas lain.

c. Checks whether an Electronic *Certificate is included in the CRL; and*

d. Approval of limits of liability and guarantees.

Relying Parties include banks, e-commerce companies, government institutions, and other institutions.

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 Informatika Republik Indonesia / Ministry of Communications and Informatics Technology of The Republic of Indonesia

Setiap tahunnya Peruri CA membuat laporan kerja ke Kementrian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo).

Peruri CA make a work report to the Ministry of Communications and Informatics Technology of The Republic of Indonesia (MCIT) annually.

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 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 & nir-sangkal; dan

c. Enkripsi.

Subscriber's Electronic Certificate usage is restricted by the key usage and extended key usage of the certificate extension. Peruri CA's Electronic Certificate can be used to issue Electronic Certificates for transactions that require:

a. Authentication;

b. Digital Signature & non-repudiation; and

c. Encryption.

Pemilik 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 dengan cara memastikan *liveness detection*

Subscribers may choose an appropriate level of assurance in their identitities that they wish to present to Relying Parties. Level of assurance is distinguished in these following Electronic Certificate class:

b. Class 3 : Electronic Certificate with medium warranty. Identity verification is carried out by ensuring the liveness detection of the Applicant and comparing the identity

dari Pemohon serta 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.

card data against the identity data held by the government.

b. Class 4 : high assurance Electronic Certificate. Identity verification by comparing identity cards and biometric data with government-owned identity data.

Sertifikat Elektronik organisasi hanya dapat diterbitkan Sertifikat Elektronik dengan tingkat jaminan tinggi (Kelas 4).

Organizational Electronic Certificates can only be issued with a high assurance Electronic Certificate (Class 4).

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

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

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

1.4.2. Penggunaan Sertifikat Elektronik yang Dilarang / Prohibited Electronic Certificate Uses

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

Electronic 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:

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

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

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

b. Memastikan semua layanan, operasional, dan infrastruktur

b. Ensures that all aspects of the CA services, operations, and

Peruri CA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP; dan

infrastructure as described in the CPS are well performed in accordance with the requirements, representations, and warranties of the CP; and

c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang kurang lebih setara.

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 ini dikelola oleh Peruri CA.

This CP / CPS are maintained by Peruri CA.

1.5.2. Narahubung / Contact Person

Pemilik, Pihak Pengandal, dan pihak ketiga lainnya dapat menghubungi Peruri CA melalui surat elektronik (surel) dan/atau melalui dokumen fisik bertandatangan basah untuk melaporkan dugaan penyalahgunaan Sertifikat Elektronik yang diterbitkan Peruri CA.

Subscribers, Relying Parties, and other third parties may contact Peruri CA via email and/or through wet-signed physical documents to report suspected misuse of Electronic Certificates issued by Peruri CA.

Surel / *Email*	:	cs.digital@peruri.co.id / policy.ca@peruri.co.id
Telepon / *Phone*	:	+62 21 739 5000
Fax / *Fax*	:	+62 21 7221 156
Situs *Web* / *Website*	:	https://ca.peruri.co.id
Alamat / *Address*	:	Perum Percetakan Uang RI (Peruri) Jalan Palatehan No.4 Blok K-V, Kebayoran Baru, Jakarta 12160 Indonesia

1.5.3. Personel 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, kemudian menentukan kesesuaian dan 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, then determining the suitability and application of the document.

1.5.4. Prosedur Persetujuan CPS / CPS Approval Procedures

Policy Authority (PA) menyetujui CPS dan segala perubahannya. Perubahan dibuat

Policy Authority (PA) approves the CPS and any amendments. Amendments are

dengan mengubah seluruh CPS atau dengan mempublikasikan addendum. PA menentukan apakah perubahan atas CPS ini membutuhkan pemberitahuan atau perubahan OID.	*made by either updating the entire CPS or by publishing an addendum. PA 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:

a. Sertifikat Elektronik Peruri CA;
b. CRL;
c. CP / CPS ;
d. Perjanjian Pelanggan;
e. Kebijakan Privasi;
f. Perjanjian Pihak Pengandal; dan
g. Kebijakan Jaminan.

Peruri CA is responsible for maintaining publicly accessible repositories. Published documents include, but are not limited to:

a. Peruri CA Electronic Certificate;
b. CRL;
c. CP / CPS;
d. Subscriber Agreement;
e. Privacy Policy;
f. Relying Party Agreement; and
g. Warranty Policy.

Dokumen dibuat menggunakan dwibahasa. Dalam hal terjadi ketidaksesuaian, yaitu Bahasa Indonesia dan Bahasa Inggris, maka Bahasa Indonesia didahulukan.

Documents are bilingual. In the event of a discrepancy, namely Indonesian and English, Indonesian shall take 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, yang mempublikasikan Sertifikat Elektronik dari Peruri CA, CRL terakhir, dokumen CP/CPS, dan dokumen lainnya yang berkaitan dengan operasional Peruri CA.

Peruri CA maintains an internet-accessible repository, which publishes Electronic Certificates from Peruri CA, latest CRLs, CP/CPS documents, and other documents related to Peruri CA operationals.

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 dapat diakses secara publik dalam waktu selambat-lambatnya 7 (tujuh) hari kalender setelah disetujui.

This CPS document and any changes made can be accessed publicly at the latest 7 (seven) calendar days after being approved.

Peruri CA mempublikasikan Sertifikat Elektronik Pemilik dan data pencabutan

Peruri CA publishes Subscriber's Electronic Certificates data and and

Sertifikat Elektronik dalam waktu 30 (tiga puluh) menit setelah penerbitan.	*revocation data within 30 (thirty) minutes after issuance.*
CRL diperbarui sesuai dengan frekuensi penerbitan CRL bagian 4.9.7.	*The CRL is updated according to the section 4.9.7.*

2.4. KENDALI AKSES PADA REPOSITORI / ACCESS CONTROLS ON REPOSITORIES

Informasi yang terpublikasi pada repositori adalah informasi publik (biasa). 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 (general). Peruri CA provide unrestricted read access to its repositories and shall implement logical and physical controls to preventunauthorized write access to such repositories.*
Peruri CA melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.	*Peruri CA protects 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 men-*generate* (membangkitkan) dan menandatangani Sertifikat Elektronik dengan subjek *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 generates and sign Electronic 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 Electronic Certificates issued by Peruri CA

Tipe Sertifikat Elektronik / *Electronic Certificate Type*		Distinguised Name (DN) / *Distinguished Name (DN)*
Sertifikat Elektronik Peruri CA / *Peruri CA Electronic Certificate*		CN=<Nama Peruri CA>, O=<Peruri>, C=ID
Sertifikat Elektronik Pemilik / *Subscriber Electronic Certificate*	Individual / *Individual*	CN=<Nama >, *Email Address*=<*Email*>, OU=Personal, O=Peruri CA, C=IDE
	Individual dengan afiliasi / *Affiliated individual*	CN=<Nama>, *Email Address*=<*Email*>, OU=Personal, O=<Nama Afiliasi>, C=ID
	Organisasi / *Organization*	CN=<nama_Organisasi>, *Email Address*=<*Email* Organisasi>, 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 mengidentifikasi orang atau objek tersebut.

The Electronic Certificates issued pursuant to this CPS are meaningful only if the names that appear in the Electronic Certificates can be understood and used by Relying Parties. Names used in the Electronic 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 memiliki arti bahwa Peruri CA memiliki bukti keterkaitan yang cukup antara nama dengan Pemilik. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh Pemilik yang sah atau perwakilan resmi dari Pemilik yang sah.

The subject and issuer name contained in an Electronic Certificate means that Peruri CA has proper evidence of the existent association between these names and the Subscribers to which they belong. To achieve this goal, the use of a name must be authorized by the rightful Subscriber or a legal representative of the rightful Subscriber.

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

Peruri CA tidak akan menerbitkan Sertifikat Elektronik bagi Pemilik yang anonim atau pseudonim.

Peruri CA shall not issue end-entity anonymous or pseudonymous Electronic 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 Electronic Certificates are interpreted using X.500 standards.

3.1.5. Keunikan Nama / Uniqueness of Names

Distinguished Name (DN) dalam Sertifikat Elektronik unik di dalam ranah Peruri CA.

Distinguished Names in Electronic Certificates is unique within Peruri CA domain.

3.1.6. Pengakuan, Autentikasi 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 akan memverifikasi hak Pemohon untuk penggunaan merek dagang. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih.

Subscriber may not request Electronic Certificates with any content that infringes the intellectual property rights of another entity. Peruri CA will not verify Subscriber right to trademark use. Subscriber is responsible for ensuring the legal user of the chosen name.

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 Electronic 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 menerbitkan 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 dengan membandingkan Kunci Publik pada Sertifikat Elektronik dengan Kunci Publik pada PKCS#10.

The method to prove possession of a Private Key is by comparing the Public Key on the Electronic Certificate with the Public Key in PKCS#10.

Untuk Sertifikat Elektronik Pemilik, Pasangan Kunci dibangkitkan oleh Peruri CA, dengan syarat Kunci Privat dibangkitkan dengan menggunakan modul kriptografis yang memenuhi persyaratan FIPS 140-2 Level 3 dan hanya dapat diakses oleh Pemilik dengan minimal menggunakan 2 (dua) faktor

For Subscriber Electronic Certificate, Key Pairs generated by Peruri CA, that the Private Key is secured using a cryptographic module that meets FIPS 140-2 Level 3 requirements and can only be accessed by Subscriber using a minimum of 2 (two) factor authentication.

autentikasi.

3.2.2. Autentikasi Identitas Organisasi / Authentication of Organization Identity

Permohonan Sertifikat Elektronik untuk organisasi hanya dapat dilakukan oleh Badan Usaha yang telah melakukan Perjanjian Kerja Sama (PKS) dengan Perum Peruri dan diajukan oleh pihak yang berwenang untuk mewakili organisasi tersebut dibuktikan dengan dokumen Badan Usaha apabila diwakilkan oleh Pimpinan tertinggi organisasi atau Direktur Utama atau yang mewakili yang dibuktikan dengan surat kuasa.	*Applications for Electronic Certificates for organizations can only be made by a Business Entity that has entered into a Cooperation Agreement (PKS) with Perum Peruri and is submitted by an authorized party to represent the organization as evidenced by a Business Entity document if it is represented by the organization's highest leadership or the President Director or who represents the organization. evidenced by a power of attorney.*
Peruri CA akan memeriksa identitas (KTP) dan jabatan dari Pemohon disesuaikan dengan dokumen Badan Usaha termasuk namun tidak terbatas kepada Akta Pendirian Perusahaan dan perubahannya, NIB, SIUP, NPWP, dan khusus organisasi yang dimaksud adalah Badan Usaha Milik Negara (BUMN) maka melampirkan SK Penunjukan Pejabat yang memohonkan dari Otoritas Pengatur dan Pengawas Sektor. Bagi Pemohon yang diwakilkan wajib melampirkan surat kuasa yang ditandatangani oleh Direktur Perusahaan dan Kartu Identitas Pegawai.	*Peruri CA will check the resdential identification (KTP) and position of the Applicant in accordance with the legalized Business Entity documents including but not limited to the Company Establishment Deed, NIB, SIUP, NPWP, and in terms of the Organization such as State Owned Enterprise, The Apllicant can attach a Letter of CEO Appointment from Regulatory Authority and Sector. Applicants who are represented are required to attach a power of attorney signed by the Director of the Company and an Employee Identity Card.*
Peruri CA menyimpan dokumen terkait identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya selama masa berlaku dari Sertifikat Elektronik yang diterbitkan.	*Peruri CA maintains a record of the type and details of the identification, which is used for authentication for the organization at least during the validity period of the issued Electronic Certificate.*

3.2.3. Autentikasi Identitas Individu / Authentication of Individual Identity

Permohonan untuk menjadi Pemilik Sertifikat Elektronik dilakukan oleh individu atau organisasi yang berwenang secara hukum untuk bertindak atas nama calon Pemilik.	*An application to be an Electronic Certificate Subscriber is made by the individual or an organization legally authorized to act on behalf of the prospective Subscriber.*
Peruri CA melakukan verifikasi identitas individu WNI yang berafiliasi dengan perusahaan sebagai pegawai internal atau merupakan bagian dari perusahaan (kemudian disebut dengan C*orporate Users*) dan WNI yang memanfaatkan Pihak Pengandal dari Peruri CA untuk menerbitkan Sertifikat Elektronik sebagai pengguna layanan (kemudian disebut dengan *Corporate Clients*) dengan cara	*Peruri CA verifies the identity of Indonesian citizens who are affiliated with related companies as internal employees or are part of the company (later referred to as Corporate Users) and Indonesian citizens who use Peruri CA's Relying Party to issue Electronic Certificates as service users (later referred to as Corporate Clients) by ensuring the liveness detection of the Applicant and obtaining the results*

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.

of matching data, including biometric data, which is managed by the government agency administering the 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 Elektronik level 3.

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.

Untuk tujuan identifikasi dan autentikasi calon Pemilik Sertifikat Elektronik WNI *Corporate Users* wajib memberikan informasi sebagai berikut:

For the purpose of identification and authentication of prospective Electronic Certificate Subscribers, Indonesian Citizen Corporate Users are required to provide the following information:

a. Memberikan salinan identitas resmi Kartu Tanda Penduduk (KTP) yang dikeluarkan oleh lembaga pemerintah yang mengeluarkan administrasi kependudukan;
b. Memberikan salinan identitas resmi yang dikeluarkan oleh perusahaan;
c. Informasi data diri berupa NIK, nama lengkap, tempat dan tanggal lahir, alamat surel perusahaan (*email*), serta nomor telepon seluler; dan
d. Melakukan proses verifikasi data biometrik melalui *liveness detection.*

a. Give copy of residential identification (KTP) issued by the the government agency administering population administration;
b. Give copy of official identity issued by the company;
c. Personal data information in the form of NIK, full name, place and date of birth, company electronic mail address (email), and cellular phone number; and
d. Verify biometric data through liveness detection.

Untuk WNI *Corporate Clients* wajib memberikan informasi sebagai berikut:

Meanwhile, Indonesian Citizens Corporate Clients are required to provide the following information:

a. Memberikan salinan identitas resmi (Kartu Tanda Penduduk) yang dikeluarkan oleh lembaga pemerintah yang mengeluarkan administrasi kependudukan;
b. Informasi data diri berupa NIK, nama lengkap, tempat dan tanggal lahir, surel pribadi (*email*), serta nomor telepon seluler; dan

a. Give copy of the official identity (residential identity) issued by the the government agency administering population administration;
b. Personal data information in the form of NIK, Full Name, Place and Date of Birth, Personal electronic mail address (email), and cellular phone number; and

c. Melakukan proses verifikasi data biometrik melalui *liveness detection*;

c. Verify biometric data through liveness detection;

Sementara bagi WNA (Warga Negara Asing) wajib memberikan ;

a. Paspor;
b. KITAS/KITAP/National ID;
c. Mengisi Formulir Pendaftaran Sertifikat Elektronik;dan
d. Surat jaminan dari perusahaan yang ditandatangani oleh penanggung jawab perusahaan dimana Pemohon bekerja.

Meanwhile, foreigners (foreign citizens) are required to provide;

a. Passport;
b. KITAS/KITAP/National ID;
c. Fill out the Electronic Certificate Registration Form; and
d. Guarantee letter from the company signed by the person in charge of the company where the Applicant works.

Peruri CA kemudian menerbitkan Sertifikat Elektronik level 3. Bagi WNA yang memiliki KTP, wajib melampirkan KTP tersebut untuk diterbitkan Sertifikat Elektronik level 4 oleh Peruri CA dengan membandingkan data biometrik terhadap data identitas yang dimiliki oleh pemerintah.

Peruri CA then issues a level 3 Electronic Certificate. Foreigners who have a residential identification (KTP) are required to provide attachments for the issuance of a level 4 Electronic Certificate by Peruri CA by comparing biometric data against identity data held by the government.

Peruri CA melakukan pemeriksan dan proses validasi terdahap informasi tambahan lainnya sesuai dengan poin 4.2.2 yang telah diterima dari Pemohon untuk mendeteksi kebenaran dan keasilannya serta mencari jika ada perubahan atau pemalsuan terhadap informasi lainnya tersebut.

Peruri CA examines and validates other additional information in accordance with point 4.2.2 that has been received from the Applicant to detect the truth and accuracy and look for changes or falsification of the other information.

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 Electronic 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 Electronic Certificates.

3.2.5. Validasi Otoritas / Validation of Authority

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

Sertifikat Elektronik yang mencantumkan afiliasi organisasi yang eksplisit atau

Electronic Certificates that contain explicit or implicit organizational affiliation shall be

implisit diterbitkan hanya setelah memastikan Pemohon memiliki otorisasi untuk bertindak atas nama organisasi dalam kapasitas yang dinyatakan dengan tegas.	*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 dapat meminta penggantian kunci kepada Peruri CA dan Peruri CA akan menerbitkan Sertifikat Elektronik baru dengan masa berlaku yang baru (*re-key*). Pemilik mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2.2 dan 3.2.3 untuk mendapatkan Sertifikat Elektronik baru dengan kunci yang baru.	*Prior to the expiry of an Electronic Certificate, Subscriber may request for a re-key and Peruri CA will issue a new Electronic Certificate with a new validity perior (re-key). Subscriber repeats the application process as described in sections 3.2.2 and 3.2.3 to obtain a new Electronic Certificate with a new key.*

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

Setelah Sertifikat Elektronik dicabut selain karena alasan pembaruan pada bagian 3.3.1 untuk mendapatkan Sertifikat Elektronik baru dengan kunci yang baru, Pemilik mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2.2 dan 3.2.3.	*After an Electronic Certificate has been revoked during a renewal action in section 3.3.1, the Subscriber is required to go through the initial registration process described in section 3.2.2 and 3.2.3 to obtain a new Electronic Certificate with new keys.*

3.4. IDENTIFIKASI DAN AUTENTIKASI UNTUK PERMINTAAN PENCABUTAN / IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Permintaan pencabutan selalu diautentikasi. Permintaan untuk mencabut Sertifikat Elektronik dapat diautentikasi menggunakan Kunci Publik yang terhubung dengan Sertifikat Elektronik atau 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 an Electronic Certificate may be authenticated using that Electronic Certificate's associated Public Key or 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 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 / ELECTRONIC CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. PERMOHONAN SERTIFIKAT ELEKTRONIK / ELECTRONIC CERTIFICATE APPLICATION

4.1.1. Siapa yang Dapat Mengajukan Permohonan Sertifikat Elektronik / Who Can Submit an Electronic Certificate Application

Permohonan Sertifikat Elektronik hanya dapat dilakukan oleh individu atau entitas non-instansi pemerintah. Entitas instansi pemerintah dapat melakukan permohonan Sertifikat Elektronik disertai dengan perjanjian khusus. Proses pendaftaran disertai dengan identitas Pemohon yang 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.

Applications for Electronic Certificates can only be made by individuals or non-government entities. Government agency entities can apply for Electronic Certificates accompanied by special agreements. The registration process is accompanied by a verifiable identity of the Applicant. 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.

Verifikasi dan Validasi Dokumen / Verification and Document Validation	Pemohon / Applicant			
	Individu / Individual			Badan Usaha / Business Entity
	Warga Negara Indonesia (WNI) / Indonesia Citizen		Warga Negara Asing (WNA) / Foreign Citizen	
	Corporate User	Corporate Client		
KTP / *Residential Identification*	✓	✓	✓ (jika memiliki / *if any*)	✓
Paspor / *Passport*			✓	
KITAS /KITAP / ID Nasional (*National ID)*			✓	
Informasi: NIK, Nama Lengkap & TTL / *Information: Resident Number, Full Name & Date of Birth*	✓	✓		✓
Nomor Telepon Seluler / *Handphone Number*	✓	✓	✓	✓
Kartu Pegawai / *Company ID Card*	✓		✓ (jika memiliki / *if any*)	✓
Kartu Identitas Lain / *Other ID Card*			✓ (opsional / *optional*)	
Surel Perusahaan / *Corporate Email*	✓		✓ (jika memiliki / *if any*)	✓
Surel Pribadi / *Private Email*		✓	✓ (jika memiliki / *if any*)	
Formulir Pendaftaran Sertifikat / *Certificate Registration Form*			✓	

Verifikasi dan Validasi Dokumen / Verification and Document Validation	Pemohon / Applicant			
	Individu / Individual			Badan Usaha / Business Entity
	Warga Negara Indonesia (WNI) / Indonesia Citizen		Warga Negara Asing (WNA) / Foreign Citizen	
	Corporate User	Corporate Client		
Verifikasi Data Biometrik/Deteksi Kehidupan / *Biometric Data Verification/Liveness Detection*	✓	✓	✓	✓
Akta Pendirian Perusahaan / *Deed of Incorporation*				✓
NIB, SIUP, NPWP				✓
SK Penunjukan Pejabat / *Statement of Appointment*				✓
Surat Kuasa (apabila diwakilkan) / *Power of Attorney (if represented)*				✓

*WNI : Warga Negara Indonesia (*Indonesia Citizen*)
**WNA : Warga Negara Asing (*Foreign Citizen*)
***KITAS : Kartu Izin Tinggal Terbatas (*Limited Stay Permit Card*)
****KITAP : Kartu Izin Tinggal Tetap (*Permanent Stay Permit Card*)
*****NIB : Nomor Induk Berusaha (*Business Number*)
******SIUP : Surat Izin Usaha Perusahaan (*Single Business Number*)
*******NPWP : Nomor Pokok Wajib Pajak (*Tax Identification Number*)
*******Untuk WNA dapat mencantumkan surel pribadi jika tidak memiliki surel perusahaan.

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

Pemohon 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 bertanggung jawab untuk menyediakan dan memproses pendaftaran dengan langkah-langkah berikut:

Peruri CA is responsible for providing and processing the registration with the following steps:

a. memberikan formulir Permohonan Pendaftaran Sertifikat kepada Pemohon;
b. menerima formulir permohonan pendaftaran Sertifikat Elektronik yang telah diisi oleh Pemohon; dan
c. memastikan bahwa Pemohon telah menyetujui Perjanjian Pelanggan yang berlaku; dan
d. memastikan bahwa Pemohon telah menyetujui Perjanjian dengan Pihak Pengandal (*Relying Party Agreement*).

a. provide an Electronic Certificate Registration Application form to the Applicant;
b. receive the Electronic Certificate registration application form which has been filled out by the Applicant; and
c. ensure that the Applicant has agreed to the Subscriber Agreement; and
d. ensure that the Applicant has agreed to the Relying Party Agreement.

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 Elektronik. Sertifikat Elektronik yang dimaksud menampilkan identitas kepada Pihak Pengandal atau Pemilik.	*Peruri CA maintains systems and processes capable of authenticating Applicant identity for all types of Electronic Certificates. The Electronic Certificate in question displays identity to the Relying Party or Subscriber.*
Peruri CA melindungi komunikasi dan menyimpan informasi yang diberikan oleh Pemohon selama proses pendaftaran dengan aman.	*Peruri CA protects communications and securely stores 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 Autentikasi / Performing Identification and Authentication Functions

Identifikasi dan autentikasi Pemohon memenuhi persyaratan yang ditentukan untuk autentikasi Pemilik sebagaimana dalam CPS bagian 3.2.	*Identification and authentication The Applicant meets the requirements specified for Subscriber authentication as set out in CPS section 3.2.*

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

Setelah semua pemeriksaan identitas dan atribut Pemohon yang mengacu pada poin 4.1.1 dipenuhi maka Sertifikat Elektronik dapat diterbitkan.	*After all checking of the identity and attributes of the Applicant referring to point 4.1.1 is fulfilled the Electronic Certificate can be issued.*
Apabila Pemohon tidak memenuhi syarat untuk penerbitan Sertifikat Elektronik atau permohonannya mengandung kesalahan, Peruri CA langsung menolak proses permohonan tersebut. Peruri CA dapat meminta tambahan informasi lainnya seperti SIM, paspor, dan dokumen lainnya yang menjelaskan identitas serta memuat foto Pemohon untuk dilakukan proses verifikasi lebih lanjut dan selanjutnya permohonan disetujui apabila proses verifikasi dan validasi telah sesuai.	*If the Applicant does not meet the requirements for the issuance of Electronic Certificate or the application contains errors, Peruri CA rejects the application process directly. Peruri CA may request additional information such as driver's license, passport, and other documents that explain identity and contain photo of the Applicant for further verification process and then the application is approved if the verification and validation process is appropriate.*

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

Semua pihak yang terlibat dalam proses permohonan Sertifikat Elektronik melakukan usaha untuk memastikan permohonan Sertifikat Elektronik diproses tepat waktu.	*All parties involved in the Electronic Certificate application process make efforts to ensure that the Electronic Certificate application is processed in a timely manner.*

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

Peruri CA will complete the validation process and issue or reject the Electronic Certificate request no later than 3 (three) working days after receiving all required details and documents from the Applicant, as long as there is no events beyond Peruri CA's control that may delay the issuance process.

4.3. PENERBITAN SERTIFIKAT ELEKTRONIK / ELECTRONIC CERTIFICATE ISSUANCE

4.3.1. Tindakan Peruri CA Selama Penerbitan Sertifikat Elektronik / Peruri CA Actions During Electronic Certificate Issuance

Peruri CA melakukan verifikasi sumber permohonan Sertifikat Elektronik sebelum diterbitkan. Sertifikat Elektronik diperiksa untuk memastikan bahwa semua *field* dan ekstensi telah diisi dengan benar.

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

Peruri CA melakukan autentikasi permohonan sertifikat elektronik, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membangkitkan Sertifikat Elektronik, dan menyerahkan Sertifikat Elektronik kepada Pemohon. Peruri CA mempublikasikan Sertifikat Elektronik ke suatu repositori sesuai dengan CP dan CPS terkait. Semua hal ini dilaksanakan secara tepat waktu sesuai dengan uraian pada bagian 4.2.

Peruri CA authenticate an Electronic Certificate Request, ensure that the Public Key is bound to the correct Applicant, obtain a proof of possession of the Private Key, then generate an Electronic Certificate, and provide Electronic Certificate to the Applicant. Peruri CA publish the Electronic 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, Electronic 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 Electronic Certificate

Peruri CA memberitahu Pemilik dalam waktu maksimal 7 (tujuh) hari kerja tentang penerbitan Sertifikat Elektronik melalui surel.

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

4.4. PENERIMAAN SERTIFIKAT ELEKTRONIK / CERTIFICATE ACCEPTANCE

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

Pemilik memeriksa semua informasi tentang Sertifikat Elektronik dan melakukan penerimaan Sertifikat Elektronik sebelum menggunakan Sertifikat Elektronik tersebut.	*The Subscriber checks all information about the Electronic Certificate and receives the Electronic Certificate before using the Electronic Certificate.*
Bila tidak ada keluhan dari Pemilik dalam waktu 7 (tujuh) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat Elektronik.	*When there is no complaint from Subscriber within 7 (seven) working days, the Subscriber is deemed to accept all certificate information.*
Dalam hal penerbitan Sertifikat Elektronik, Peruri CA membuat prosedur penerimaan dan mendokumentasikan penerimaan Sertifikat Elektronik yang terbitkan pada bagian 4.4.2.	*In the case of Electronic Certificate issuance, Peruri CA makes acceptance procedures and documents receipt of Electronic Certificates issued in section 4.4.2.*

4.4.2. Publikasi Sertifikat Elektronik oleh Peruri CA / Publication of The Electronic Certificate by Peruri CA

Peruri CA mempublikasikan Sertifikat Elektroniknya dalam sebuah Repositori sebagaimana tercantum pada bagian 2.2 paling lambat 1 (satu) hari setelah Sertifikat Elektronik diterbitkan, termasuk ketika menerbitkan informasi pencabutan terkait Sertifikat Elektronik tersebut pada Repositori. Peruri CA mempublikasikan Sertifikat Elektronik Pemilik dengan mengirimkannya ke Pemilik tersebut.	*Peruri CA publishes its Electronic Certificate in a Repository as stated in section 2.2 no later than 1 (one) day after the Electronic Certificate is issued, including when issuing revocation information regarding the Electronic Certificate in the Repository. Peruri CA publishes the Subscriber's Electronic Certificate by sending it to the Subscriber.*

4.4.3. Penerbitan Sertifikat Elektronik oleh Peruri CA ke Entitas Lain / Issuance of Electronic Certificate by Peruri CA to Other Entities

Tidak ada ketentuan.	No stipulation.

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

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

Peruri CA melindungi Kunci Privat Pemilik dari penggunaan tanpa izin atau pengungkapan oleh pihak lain dengan menggunakan *Hardware Security Module* (HSM) milik Peruri CA.	Peruri *CA protects the Subscriber's Private Key from unauthorized use or disclosure by others by using Peruri CA's Hardware Security Module (HSM).*
Peruri CA menerapkan kombinasi minimal 2 (dua) faktor autentikasi bagi Pemilik yang akan menggunakan Kunci Privatnya. Pemilik melindungi parameter autentikasi	*Peruri CA applies a combination of at least 2 (two) factor authentication for Subscriber who will use their Private Keys. The Subscriber protects the*

yang digunakan untuk mengaktifkan Kunci Privatnya.

authentication parameters used to activate his Private Key.

Pemilik memakai Kunci Privatnya hanya untuk tujuan yang sudah ditentukan.

The Subscriber uses Private Key only for the specified purpose.

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

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

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

Pihak Pengandal berhati-hati dalam mengandalkan Sertifikat Elektronik dan mempertimbangkan keseluruhan keadaan serta risiko kerugian sebelum mengandalkan Sertifikat Elektronik. Mengandalkan Tanda Tangan Elektronik atau Sertifikat Elektronik yang belum diproses sesuai dengan standar yang berlaku dapat menyebabkan risiko bagi Pihak Pengandal. Pihak Pengandal bertanggung jawab atas risiko tersebut. Apabila diperlukan jaminan tambahan, Pihak Pengandal mendapatkan jaminan tersebut sebelum menggunakan Sertifikat Elektronik.

Relying Parties are careful to rely on Electronic Certificates and consider the overall circumstances and risks of loss before relying on Electronic Certificates. Relying on Digital Signatures or Electronic Certificates that have not been processed in accordance with applicable standards may pose a risk to the Relying Party. The Relying Party is responsible for such risks. If additional guarantees are required, the Relying Party obtains such guarantees before using the Electronic Certificate.

4.6. PEMBARUAN SERTIFIKAT ELEKTRONIK / CERTIFICATE RENEWAL

Pembaruan Sertifikat Elektronik adalah penerbitan Sertifikat Elektronik baru kepada Pemilik dengan tanpa mengganti Kunci Publik maupun informasi utama lain pada Sertifikat Elektronik. Proses ini akan memperbarui periode validitas dari Sertifikat Elektronik.

Electronic Certificate Renewal is the issuance of a new Electronic Certificate to Subscriber without changing the Public Key or other key information on the Electronic Certificate. This process will renew the validity period of the Electronic Certificate.

Peruri CA melakukan proses pembaruan Sertifikat Elektronik Pemilik.

Peruri CA carries out the process of renewing the Subscriber's Electronic Certificate.

4.6.1. Kondisi untuk Pembaruan Sertifikat Elektronik / Circumstance for Electronic Certificate Renewal

Kondisi untuk melakukan pembaruan Sertifikat Elektronik memiliki ketentuan:	*The conditions for renewing the Electronic Certificate have the following conditions:*
a. Sertifikat Elektronik asli belum pernah dibatalkan/dicabut;	*a. The original Electronic Certificate has never been canceled/revoked;*
b. Kunci Publik yang digunakan tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun;	*b. The 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 Electronic Certificate remain accurate and no new or additional validation is required.*
d. Mendapatkan pemberitahuan Sertifikat Elektronik akan kedaluwarsa mulai H-30.	*d. Get notification that Electronic Certificate will expire from H-30.*
e. Pemilik memberikan persetujuan untuk melakukan pembaruan Sertifikat Elektronik.	*e. Subscriber gives consent to renew Electronic Certificate.*
f. Sertifikat Elektronik belum kedaluwarsa.	*f. Electronic Certificate has not expired.*

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

Peruri CA dan Pemilik Sertifikat Elektronik dengan ketentuan kondisi sesuai dengan poin 4.6.1.	*Peruri CA and Subscriber of Electronic Certificate with the conditions in accordance with point 4.6.1.*

4.6.3. Pemrosesan Permintaan Pembaruan Sertifikat Elektronik / Processing Electronic Certificate Renewal Requests

Berlaku prosedur penerbitan Sertifikat Elektronik seperti yang dinyatakan pada bagian 4.3.	*The procedure for issuing Electronic Certificate is followed, as stated in section 4.3.*

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

Peruri CA memberitahu Pemilik dalam waktu maksimal 7 (tujuh) hari kerja tentang penerbitan pembaruan Sertifikat Elektronik melalui surel.	*Peruri CA notifies the Subscriber within a maximum of 7 (seven) working days of the issuance of the renewal of the Electronic Certificate by email.*

4.6.5. Sikap yang Dianggap sebagai Menerima Sertifikat Elektronik yang Diperbarui / Conduct Constituting Acceptance of ARenewal Electronic Certificate

Pemilik sesuai dengan yang dinyatakan pada poin 4.4.1.	*Subscriber as stated in point 4.4.1.*

4.6.6. Publikasi Sertifikat Elektronik yang Diperbarui oleh Peruri CA / Publication of The Renewal Electronic Certificate by The CA

Sertifikat Elektronik yang telah diperbarui akan dipublikasikan sesuai dengan	*The updated Electronic Certificate will be published in accordance with the*

prosedur Repositori, sebagaimana yang dinyatakan pada bagian 4.4.2.

Repository procedures, as stated in section 4.4.2.

4.6.7. Pemberitahuan Penerbitan Sertifikat Elektronik oleh Peruri CA ke Entitas Lain / Notification of Electronic Certificate Issuance by The CA to Other Entities

Tidak ada ketentuan.

No stipulation.

4.7. PENGGANTIAN KUNCI SERTIFIKAT ELEKTRONIK / ELECTRONIC CERTIFICATE RE-KEY

Penggantian kunci Sertifikat Elektronik adalah penerbitan Sertifikat Elektronik baru kepada Pemilik dengan menerbitkan Pasangan Kunci baru serta informasi lain pada Sertifikat Elektronik.

Electronic Certificate re-key is the issuance of a new Electronic Certificate to the Subscriber by issuing a new Key Pair and other information on the Electronic Certificate.

Pada saat Peruri CA melakukan penggantian kunci Sertifikat Elektronik, *field 'Not After'* dan *'Not Before'* diisi dengan tanggal yang baru.

When Peruri CA performs Electronic Certificate re-key, the 'Not After' and 'Not Before' fields are filled with new dates.

Setelah proses penggantian kunci Sertifikat Elektronik berhasil dilakukan, hanya Sertifikat Elektronik terbaru yang dapat digunakan.

After the Electronic Certificate re-key process is successful, only the most recent Electronic Certificate can be used.

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

Peruri CA dapat melakukan penggantian kunci Sertifikat Elektronik selama:

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

Peruri CA may re-key an Electronic Certificate as long as:

a. The original Electronic Certificate to be re-keyed has not been revoked;
b. The new Public Key has not been blacklisted for any reason; and
c. All details within the Electronic Certificate remain accurate and no new or additional validation is required.
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, Pemilik dapat meminta penggantian kunci dan Peruri CA dapat melakukan proses penggantian kunci.

In accordance with the conditions specified in section 4.7.1, the Subscriber can request a key replacement and Peruri CA can carry out the key replacement process.

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

Berlaku prosedur penerbitan Sertifikat Elektronik seperti yang dinyatakan pada bagian 4.3.	*The procedure for issuing Electronic Certificate 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 Electronic 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 menerima Sertifikat Elektronik dengan kunci baru mengikuti prosedur penerimaan yang sama sebagaimana diuraikan dalam bagian 4.4.1.	*The Subscriber receives the Electronic Certificate with a 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 Electronic 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 / ELECTRONIC CERTIFICATE MODIFICATION

Peruri CA tidak melakukan modifikasi Sertifikat Elektronik.	*Peruri CA does not modify the Electronic Certificate.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

4.8.3. Pemrosesan Permintaan Modifikasi Sertifikat Elektronik / Processing Electronic Certificate Modification Requests

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

4.9.1. Keadaan untuk Pencabutan / Circumstances for Revocation

Peruri CA mencabut Sertifikat Elektronik Pemilik dalam keadaan berikut:	*Peruri CA revokes the Subscriber's Electronic 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 Electronic Certificate becomes invalid.*
b. Setiap informasi dalam Sertifikat Elektronik menjadi tidak valid.	*b. Any information in the Electronic Certificate becomes invalid.*
c. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Pelanggannya.	*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 Electronic Certificate is issued for trial run.*

Sertifikat Elektronik dicabut ketika hubungan antara subjek dan Kunci Publiknya yang didefinisikan dalam Sertifikat Elektronik sudah tidak valid lagi. Ketika hal ini terjadi, Sertifikat Elektronik dicabut dan diletakkan pada CRL dan/atau ditambahkan pada responder OCSP. Sertifikat Elektronik yang dicabut disertakan dalam semua publikasi baru tentang informasi status Sertifikat Elektronik sampai kedaluwarsa.

The Electronic Certificate is 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 is revoked and placed on the CRL and/or added to the OCSP responder. A revoked Electronic Certificate is included in all new publications of Electronic Certificate status information until expiration.

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

Sertifikat Elektronik dapat diminta untuk dicabut oleh:

a. Pemilik;
b. Organisasi yang berafiliasi dengan Pemilik yang dapat membuktikan hilangnya hubungan Pemilik;
c. Entitas lain seperti lembaga penegak hukum yang dapat membuktikan terungkapnya Kunci Privat atau penyalahgunaan Sertifikat Elektronik sesuai CP dan CPS; dan
d. Peruri CA

Electronic Certificates may be requested to be revoked by :

a. Subscriber;
b. Organizations affiliated with the Subscriberwho can prove the loss of the Subscriber relationship;
c. Other entities such as law enforcement agencies that can prove the disclosure of Private Keys or misuse of Electronic Certificates according to CP and CPS; and
d. Peruri CA.

4.9.3. Prosedur Permintaan Pencabutan / Procedure for Revocation Request

Peruri CA melakukan verifikasi identitas dan kewenangan (untuk entitas penegak hukum) yang meminta pencabutan Sertifikat Elektronik. Validasi identitas Pemilik diperlukan sesuai dengan bagian 3.4.

Peruri CA verifies the identity and authority (for juridical entity) whom makes request for Electronic Certificate revocation. The validation of the subscriber's identity is required according to section 3.4.

Permintaan pencabutan Sertifikat Elektronik oleh Pemilik harus menyerahkan bukti bahwa:

a. Kunci Privat dari Sertifikat Elektronik telah terungkap;
b. Penggunaan Sertifikat Elektronik tidak sesuai dengan CP/CPS; dan/atau
c. Terdapat alasan relevan lain yang diberikan oleh Pemilik.

Electronic Certificate revocation request by Subscriber shall attach evidences that:

a. The Private Key of the Electronic Certificate has been exposed;
b. The use of the Electronic Certificate does not conform to the CP/CPS; and/or
c. Any other relevant reasons for revocation by the Subscriber.

Permintaan pencabutan Sertifikat oleh pihak yang berwenang lainnya harus menyerahkan 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 Electronic Certificate has been exposed;

b. Penggunaan Sertifikat Elektronik tidak sesuai dengan CP/CPS, Perjanjian Pemilik, dan perjanjian lainnya; dan/atau

b. The use of the Electronic Certificate does not conform to the CP/CPS, Subscriber Agreement, and other agreements; and/or

c. Pemilik tidak memiliki hubungan dengan institusi.

c. Subscriber's relationship with the institution does not exist.

4.9.4. Masa Tenggang Permintaan Pencabutan / Revocation Request Grace Period

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 Electronic Certificates as soon as reasonably practical following verification of a revocation request.

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

Peruri CA memulai penyelidikan permintaan pencabutan dalam waktu 1 (satu) hari kerja kecuali pada kasus *force majeure*. Permintaan pencabutan yang disertai dengan bukti pendukung yang memadai akan segera diproses.

Peruri CA begins an investigation of the revocation request within 1 (one) working day except in the case of force majeure. Revocation requests accompanied by sufficient supporting evidence will be processed immediately.

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

Pihak Pengandal melakukan validasi setiap Sertifikat Elektronik yang diberikan terhadap CRL yang terbaru yang disediakan oleh Peruri CA.

The Relying Party must validate each Electronic Certificate issued against the most recent CRL provided by Peruri CA.

Pihak Pengandal melakukan validasi Sertifikat Elektronik terhadap server OCSP yang disediakan oleh Peruri CA sesuai dengan CPS bagian 4.9.9.

The Relying Party validates the Electronic Certificate against the OCSP server provided by Peruri CA in accordance with CPS section 4.9.9.

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

CRL diperbarui dan dipublikasi untuk Sertifikat Elektronik Pemilik/perangkat, paling sedikit setiap 1 (satu) hari. CRL akan berdampak dalam waktu maksimum 10 (sepuluh) hari.

CRLs are updated and published for Subscriber/device Electronic Certificates, at least every 1 (one) day. The CRL will take effect within a maximum of 10 (ten) days.

Dalam hal kebocoran Kunci Privat atau insiden keamanan penting lainnya, contohnya pencabutan Sertifikat Elektronik Pemilik, CRL terbaru dipublikasikan dalam waktu 24 jam semenjak waktu pencabutan sesuai

In case of Private Key leakage or other important security incident, for example revocation of Subscriber's Electronic Certificate, the latest CRL is published within 24 hours from the time of revocation according to the timestamp.

dengan stempel waktu (*timestamp*).

CRL disimpan dan dilindungi untuk menjamin integritas dan keautentikannya.	*CRLs are stored and protected to ensure their integrity and authentication.*

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 30 (tiga puluh) 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 30 (thirty) minutes after they are published. Electronic Certificates are marked as "revoked" in the repository.*
Peruri CA akan mengoperasikan CRL dan OCSP-nya dengan cara yang handal untuk memberikan respon selama 10 (sepuluh) detik atau kurang dalam kondisi operasional yang normal.	*Peruri CA will operate its CRL and OCSP in a reliable manner to provide a response of 10 (ten) 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

Tidak ada ketentuan.	*No stipulation.*

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

Tidak ada ketentuan.	*No stipulation.*

4.9.15. Prosedur untuk Permintaan Pembekuan / Procedure for Suspension Request

Tidak ada ketentuan.	*No stipulation.*

4.9.16. Batas Masa Pembekuan / Limits on Suspension Period

Tidak ada ketentuan.	*No stipulation.*

4.10. LAYANAN STATUS SERTIFIKAT ELEKTRONIK / ELECTRONIC CERTIFICATE STATUS SERVICES

4.10.1. Karakteristik Operasional / Operational Characteristics

Status Sertifikat Elektronik publik tersedia dari CRL di dalam repositori.	*The status of public Electronic Certificates are 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. Fitur Opsional/ Optional Features

Tidak ada ketentuan.	*No stipulation.*

4.11. AKHIR BERLANGGANAN / END OF SUBSCRIPTION

Pemilik dapat mengakhiri langganan dengan membiarkan Sertifikat Elektroniknya kedaluwarsa 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 Electronic Certificate to expire or revoking its Electronic Certificate without requesting a new Electronic Certificate. There is an Electronic 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 Peruri CA dan Kunci Privat Pemilik yang terasosiasi dengan Sertifikat Elektronik yang berisi *key usage digitalSignature* tidak boleh dieskro.	*Peruri CA's Private Key and Subscriber's Private Key associated with an Electronic Certificate that asserts a digitalSignature key usage shall not be escrowed.*
Kunci Privat Pemilik yang digunakan hanya untuk dekripsi dapat dieskrokan.	*The Subscriber's Private Key used for decryption only can be escrowed.*

4.12.2. Kebijakan dan Praktik Pemulihan dan Enkapsulasi KunciSesi / 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	*The location and construction of the facility housing Peruri CA equipment as well as sites housing remote workstations*

untuk mengelola Peruri CA, telah 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, sudah memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan catatan Peruri CA.

used to administer 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 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:

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

a. Memastikan tidak ada akses tidak resmi yang diizinkan ke perangkat keras;

a. Ensure no unauthorized access to the hardware is permitted;

b. Menyimpan semua media dan kertas yang dapat dilepas yang berisi informasi teks biasa yang sensitif dalam tempat yang aman.

b. Store all removable media and paper containing sensitive plain-text information in secure containers;

c. Monitor, baik secara manual maupun elektronik, untuk gangguan yang tidak sah setiap saat; dan

c. Monitor, either manually or electronically, for unauthorized intrusion at all times; and

d. Menjaga dan memeriksa log akses secara berkala.

d. Maintain and periodically inspect an access log.

Semua operasional Peruri CA yang sangat penting dan memiliki risiko tinggi 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 Supply and power generator sufficient for a minimum of 6 (six) hours operation in the absence of commercial power, to support continuity of operations.

5.1.4. Keterpaparan Air / Water Exposures

Peralatan Peruri CA ditempatkan pada tempat yang tidak terpapar air.	*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.	*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 Peruri CA location.*

5.1.7. Pembuangan Limbah / Waste Disposal

Bahan limbah yang berisi informasi sensitif akan dihancurkan dan dibuang dengan cara yang aman.	*Waste material containing sensitive information will be destroyed and 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 CPS ini. *Backup* data dilakukan dan disimpan di luar lokasi tidak kurang dari sekali setiap 7 (tujuh) hari. Setidaknya 1 (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.	*System backups of Peruri CA, sufficient to recover from system failure, shall be made on a periodic schedule, described in this CPS. Backups shall be performed and stored offsite not less than once every 7 (seven) days. At least 1 (one) full backup copy shall be stored at an offsite location (at a location separate from 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 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 Peruri CA equipment).*

5.2. KENDALI PROSEDUR / PROCEDURAL CONTROLS

5.2.1. Peran Terpercaya / Trusted Roles

Peran Terpercaya meliputi:

a. Head of Peruri CA
   Bertanggung jawab secara keseluruhan dalam operasional Peruri CA.
b. *Policy Authority*
   Bertanggung jawab dalam memastikan Peruri CA berjalan sesuai regulasi yang berlaku serta sesuai dengan CP / CPS Peruri CA yang sudah selaras dengan milik PSrE Induk.
c. *Policy Authority Officer*
   Bertanggung jawab membantu *Policy Authority* dalam menjalankan tugasnya.
d. *Internal Auditor*
   Bertanggung jawab menentukan ruang lingkup audit internal dan rencana audit tahunan.
e. *Certification Authority Unit Manager*
   Bertanggung jawab atas operasional terkait kunci milik Peruri CA dan berperan untuk memimpin proses *Key Ceremony*.
f. *Administrator of CA Unit Application (CA)*
   Bertanggung jawab melakukan kegiatan operasional yang berkaitan dengan sistem IKP CA.
g. *Service Unit Manager*
   Bertanggung jawab segala operasional terkait dengan penerbitan kunci dan Sertifikat Elektronik serta meninjau log IKP terkait VA, RA, dan TMSRA.
h. *Administrator of Service Unit Application (RA)*
   Bertanggung jawab terhadap operasional terkait administrasi VA, RA, dan TMSRA.
i. *Validation Specialist*
   Bertanggung jawab dalam proses verifikasi dan validasi data calon Pemilik Sertifikat Elektronik.
j. *Operation & Maintenance Unit Manager*
   Bertanggung jawab terhadap setiap kegiatan operasional dan pemeliharaan sistem IKP di Peruri

Trusted Roles including:

a. *Head of Peruri CA*
   Responsible for overall operations of Peruri CA.
b. *Policy Authority*
   Responsible for ensuring that Peruri CA runs in accordance with applicable regulations and in accordance with Peruri CA's CP / CPS which are already in line with Root CA's CP/CPS.
c. *Policy Authority Officer*
   Responsible for assisting Policy Authority in carrying out its duties.
d. *Internal Auditor*
   Responsible for determing the scope of the internal audit and the annual audit plan.
e. *Certification Authority Unit Manager*
   Responsible for operations related to Peruri CA's key and leading the Key Ceremony process.
f. *Administrator of CA Unit Application (CA)*
   Responsible for carrying out operational activities related to the CA IKP system.
g. *Service Unit Manager*
   Responsible for all operations related to key issuance and Electronic Certificates as well as reviewing IKP logs related to VA, RA, and TMSRA.
h. *Administrator of Service Unit Application (RA)*
   Responsible for operations related to the administration of VA, RA, and TMSRA.
i. *Validation Specialist*
   Responsible for verification process and data validation of prospective Electronic Certificate Subscribers.
j. *Operation & Maintenance Unit Manager*
   Responsible for every operational activity and maintenance of the PKI system at Peruri CA.

CA.

k. *Administrator of Operation and Maintenance Unit Application* Bertanggung jawab terhadap operasional dan perawatan sistem repositori.	k. *Administrator of Operation and Maintenance Unit Application Responsible for operation and maintenance of the repository system.*
l. *Network and Security Unit* Bertanggung jawab terhadap keamanan fisik, logikal, dan jaringan pada operasional Peruri CA.	l. *Network and Security Unit Responsible for physical, logical, and network security in Peruri CA operations.*
m. *Administrator of Appliance & HSM* Bertanggung jawab terhadap administrasi Perangkat Keras dan HSM dalam seluruh sistem IKP.	m. *Administrator of Appliance & HSM Responsible for hardware and HSM administration in the entire PKI system.*
n. *Administrator of Operating System* Bertanggung jawab terhadap administrasi sistem operasi dalam seluruh sistem IKP.	n. *Administrator of Operating System Responsible for Operating System administration in the entire IKP system.*
Peran terpercaya lainnya bisa didefinisikan dalam dokumen lain, yang menjelaskan mengenai persyaratan peran-peran tersebut pada operasional Peruri CA.	*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 memegang peran terpercaya. Kendali multi-pihak tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan tiga orang atau lebih:	*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. Pembuatan kunci Peruri CA;	*a. Peruri CA key generation;*
b. Pengaktifan kunci Peruri CA; dan	*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 diidentifikasi dan diautentikasi menggunakan Surat Penugasan atau Surat Keputusan.	*All individual assigned to trusted role are identified and authenticated using Assignment Letter or Decree.*

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

yang ditugaskan lebih dari satu peran terpercaya.

has been assigned more than one trusted role.

5.3. KENDALI PERSONEL / PERSONNEL CONTROLS

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

Semua personil Peruri CA telah terpilih berdasarkan kemampuan dasar, pengalaman, kesetiaan, kepercayaan, dan integritas berdasarkan pembuktian syarat latar belakang, kualifikasi serta pengalaman yang dibutuhkan untuk menjalankan tanggung jawab kerja secara efisien dan cukup dan dengan dokumen yang membuktikan tidak ada catatan kriminal.

All Peruri CA personnel have been selected based on basic abilities, experience, loyalty, trustworthiness, and integrity based on proving the background requirements, qualifications and experience needed to carry out work responsibilities efficiently and adequately and with documents proving no criminal record.

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 5 (lima) tahun terakhir:

a. *Curriculum Vitae;*
b. Pendidikan atau sertifikasi;
c. Identifikasi Kependudukan (KTP); dan
d. Catatan Kepolisian

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 5 (five) year:

a. *Curriculum Vitae;*
b. *Education and certification;*
c. *Residential Identification; and*
d. *Police Certificate of Good Conduct*

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

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

5.3.3. Persyaratan Pelatihan / Training Requirements

Semua personil Peruri CA 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

The trainings also include operations of the PKI (including Peruri CA hardware,

lunak dan sistem operasi Peruri CA), prosedur operasional dan keamanan, CPS, dan CP yang berlaku.

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 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 this CP, 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 telah memenuhi persyaratan yang berlaku yang diatur dalam CPS ini pada poin 5.3.1 dan 5.3.2.

Sub-Contractor personnel employed to perform functions pertaining to Peruri CA operations have complied with the applicable 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 menginformasikan kepada para personilnya perihal CP, CPS, dan setiap undang-undang yang relevan, kebijakan, atau kontrak apapun. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

Peruri CA informs its personnel about CP, CPS and any relevant laws, policies or contracts. Other technical, operational and administrative documents (e.g., Administrator's Manual, User's Guide, etc.) must be provided to enable trusted personnel to carry out their duties.

5.4. PROSEDUR LOG AUDIT / AUDIT LOGGING PROCEDURES

Berkas log audit dibuat untuk semua kejadian yang terkait dengan keamanan Peruri CA, VA, dan RA. Bila memungkinkan, log audit keamanan dikumpulkan secara otomatis. Bila ini tidak mungkin, suatu buku log, kertas

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

formulir, atau mekanisme fisik lain dipakai. Semua log audit keamanan, elektronik dan non elektronik, dipertahankan dan tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai dengan bagian 5.5.2.

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

a. Tipe Kejadian;	*a. The type of event;*
b. Nomor rekaman atau urutan rekaman;	*b. Serial or sequence number of entry;*
c. Tanggal dan waktu kejadian;	*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 ditinjau sedikitnya 3 (tiga) bulan 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 every 3 (three) months 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 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 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 terpercaya yang berwenang yang mampu melakukan operasi apa pun tanpa memodifikasi integritasnya.	*The records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized trusted access are able to perform any operations without modifying integrity.*
Pengarsipan log audit memiliki kontrol yang memadai untuk mencegah konflik kepentingan atau menciptakan peluang untuk mengedit, menambahkan, menghapus, memodifikasi entri log.	*Archiving of audit logs 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 tempat lain per bulan.	*Audit logs and audit summaries were backed up monthly. Backup media were stored locally in a secure location. A second copy of the audit log were sent off-site on a monthly basis.*

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

Sistem pengumpulan log audit adalah internal ke sistem Peruri CA.Pengumpulan log audit eksternal tidak berlaku.	*The audit log collection systems were internal to Peruri CA system.The external audit log collection systems were not applicable.*

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 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's archival records are detailed enough to determine the correct operation of the CA and the validity of any Electronic Certificate (including revoked or expired) issued by Peruri CA. The following data is recorded on the archive:*
a. Siklus operasi Sertifikat Elektronik termasuk permintaan Sertifikat Elektronik, permintaan pencabutan, permintaan pembangiktan ulang	*a. The Electronic Certificate operation cycle includes Electronic Certificate requests, revocation requests, Key Pair re-generation requests.*

Pasangan Kunci.

b. Semua Sertifikat Elektronik dan CRL yang telah diterbitkan;

c. Log audit;

d. Data konfigurasi sistem IKP;

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

f. Data pendaftaran Pemilik.

b. All Electronic Certificates and CRLs issued;

c. Audit logs;

d. PKI system configuration data;

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

f. Subscriber's registration document.

5.5.2. Periode Retensi Arsip / Retention Period for Archive

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

Archived records are kept for at least 5 (five) years. Applications required to read these files must be maintained throughout 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 dilakukan agar jika terjadi kehilangan atau rusaknya arsip utama, satu set lengkap salinan cadangan yang ada di lokasi terpisah akan tersedia sesuai dengan SOP Manajemen Pencadangan.

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. Peruri CA tidak mengumpulkan arsip eksternal.

Performed by internal Peruri CA itself. Peruri CA does not collect external archives.

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 dan pihak-pihak lain yang berwenang yang diizinkan 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:

Procedures to obtain and verify archive information are as follows:

a. Pemohon informasi mengirimkan permintaan akses arsip informasi ke Peruri CA dengan alasan spesifik dan keharusan mendapatkan informasi tersebut serta identifikasi kebutuhan jenis informasi;

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 menentukan kepatutan dan keharusan Pemohon dan memberitahu hasil keputusan kepada Pemohon;

b. Peruri CA justifies the appropriateness and necessity of the request and notifies the decision result to the requester;

c. Peruri CA mendapatkan arsip informasi, menentukan akses yang tepat, dan meneruskan ke Pemohon;dan

c. Peruri CA obtains the archive information, defines access rights, and forwards to the requester;and

d. Pemohon memastikan integritas informasi.

d. The requester verifies the integrity of information.

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

The contents of the archive is not published 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 sepuluh (10) tahun atau jika ada kebutuhan khusus apabila ada risiko kebocoran kunci. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat Elektronik. Sertifikat Elektronik yang lama masih berlaku, dapat

To minimize the risk of Peruri CA's private key leak, the Private Key can be changed periodically every ten (10) years or if there is a special need if there is a risk of key leakage. From that time on, only the new Key Private shall be used for Electronic Certificate signing purposes. The older, but still valid, Electronic Certificate will be available to verify old signatures until all of the Electronic Certificates signed using

digunakan untuk verifikasi tanda tangan lama sampai semua Sertifikat Elektronik yang ditandatangani menggunakan Kunci Privat tersebut kedaluwarsa. Apabila Kunci Privat yang lama digunakan untuk menandatangani CRL, maka kunci yang lama disimpan dan dilindungi.

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 surel atau situs web.

When Peruri CA updates its Private 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 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 investigation by a third party was carried out to determine the nature and extent of the 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:

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

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

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

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

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

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

d. Apabila kunci penandatanganan Peruri CA rusak, Peruri CA mengembalikan operasional Peruri CA dalam kurun waktu ± 4 (empat) jam dari kejadian sesuai dengan dokumen *Business Continuity Plan* (BCP), dengan memberikan prioritas ke pembangkitan Pasangan Kunci Peruri CA yang baru.

d. If Peruri CA signing key is damaged, Peruri CA restores Peruri CA operation within + 4 (four) hours of the event according to the Business Continuity Plan (BCP) document, giving priority to the generation of a new Peruri CA Key Pair.

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

Dalam kasus terjadi kehilangan atau kebocoran/kompromi 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 or compromised of Peruri CA, all subscribers of Peruri CA are notified, all subscriber certificates issued by the compromised Issuer CA are revoked, along with Peruri CA's Electronic Certificate.

Bila Kunci Privat Peruri CA hilang atau terjadi kebocoran/kompromi, Peruri CA memberitahu *Policy Authority*, Pihak Pengandal, Pemilik, dan PSrE Induk melalui pengumuman publik. Peruri CA 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 Peruri CA's Private Key is loss or compromised, Peruri CA must notify the Policy Authority, Relying Parties, Subscribers, and Root CA through a public announcement. Peruri CA shall 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 by generating a new Key Pair for Peruri CA.

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

To maintain the integrity of Peruri CA services, it implements data backup and recovery procedures. Peruri CA has developed a Disaster Recovery Plan (DRP). Peruri CA system is redundantly configured at its primary site (main site)

dikonfigurasikan secara redundan di sistem utama dan di sistem cadangan di lokasi yang terpisah. DRP dan prosedur pendukung ditinjau dan diuji secara berkala (setidaknya setahun sekali) dan di revisi dan diperbarui sesuai dengan kebutuhan.

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), Peruri CA maintains the system online and offline. The secondary node Peruri CA at the primary facility is readily available in the event that the primary node should cease operation.

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

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

Operasi Peruri CA dirancang untuk memulihkan layanan penuh dalam waktu 24 (dua puluh empat) jam dari kegagalan sistem utama.

Peruri CA operations were designed to restore full service 24 (twenty four) 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 PSrE Induk, Peruri CA memberikan pemberitahuan kepada Pemilik dan Pihak Pengandal melalui surel 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 and Root CA, 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;

a. Notify the status of the service to affected users;

b. Mencabut semua Sertifikat Elektronik;

b. Revoke all Electronic Certificates;

c. Menyimpan dalam jangka panjang informasi Peruri CA dan Pemilik Sertifikat Elektronik dalam periode yang dinyatakan dalam poin 5.5.2;

c. Keep in the long term Peruri CA and Electronic Certificate Subscribers information for the period stated in point 5.5.2;

d. Menyediakan dukungan hak dan kewajiban berlaku sesuai dengan perjanjian yang berlaku dan menjawab pertanyaan; dan

d. Provide support for applicable rights and obligations in accordance with applicable agreements and answer questions; and

e. Menangani dengan tepat Pasangan Kunci Peruri CA dan perangkat keras yang terkait.

Apabila Peruri CA mengakhiri operasinya, Peruri CA memberitahu PSrE Induk, *Policy Authority*, dan para Pemilik sebelum penutupan agar sesuai dengan Peraturan Perundang-Undangan.

e. Properly handle Peruri CA Key Pair and associated hardware.

In the event that Peruri CA terminates its operation, it shall provide notice to Root CA, Policy Authority, and Subscribers 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 Level 3. 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 Electronic Certificates, CRLs, or status information were generated in cryptographic modules validated to FIPS 140-2 Level 3,. Multi-party control is required for Peruri CA Key Pair generation, as specified in section 6.2.2.*
Pembangkitan Pasangan Kunci Peruri CA 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 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 was 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 dilakukan oleh Peruri CA atas persetujuan Pemilik dan Kunci Privat Pemilik dititipkan kepada Peruri CA.	*Subscriber Key Pairs are generated by Peruri CA with Subscriber concent and the Subscriber's Private Key is entrusted to Peruri CA.*

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

Peruri CA tidak melakukan pengiriman Kunci Privat kepada Pemilik.	*Peruri CA does not deliver Private Keys to Subscribers.*

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

Peruri CA hanya menerima Kunci Publik dalam format PKCS#10 (CSR) yang berasal dari lingkungan Peruri.	*Peruri CA only accepts Public Key in PKCS#10 (CSR) format from Peruri environment.*

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

Peruri CA menyediakan repositori untuk mengakses Kunci Publik Peruri CA.	*Peruri CA provides a repository for accessing Peruri CA's Public Keys*
Mekanisme tersebut diamankan menggunakan TLS.	*That mechanism is secured using TLS.*

6.1.5. Ukuran Kunci/ Key Sizes

Sertifikat Elektronik / ElectronicCertificate	Algoritma Enkripsi / Encryption Algorithm	Panjang Kunci / Key Length
Peruri CA	SHA 512 RSA	4096
End User	SHA 512 RSA	2048

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

Tidak ditentukan.	*No stipulation.*

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 Electronic Certificate signing (keyCertSign) and CRL signing (cRLSign).*

6.2. KONTROL KUNCI PRIVAT 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 Level 3 untuk pembangkitan kunci, proses penandatanganan, dan enkripsi.	*Peruri CA uses a FIPS 140-2 Level 3 cryptographic module for key generation, signing operations and encryption.*
Pemilik menerapkan kombinasi 2 (dua) faktor autentikasi untuk mengakses Kunci Privat.	*Subscriber using 2 (two) factor authentication for accessing Private Key.*

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	*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 (n) out of the total number of Secret Shares created and distributed for a particular hardware*

didistribusikan untuk dipakai di modul kriptografis tertentu (m) diperlukan untuk mengaktifkan sebuah Kunci Privat Peruri CA yang disimpan di dalam modul.

cryptographic module (m) is required to activate a Peruri CA private key stored in the module.

Angka ambang yang diperlukan untuk pembuatan kunci adalah 2 dari 3 (dimana n=2 dan m=3), aktivasi kunci penandatanganan adalah 2 dari 3, dan backup serta pemulihan Kunci Privat adalah 2 dari 3.

The threshold number of shares needed for key generation is 2 of 3 (where n=2 and m=3) signing key activation is 2 of 3 and Private Key backup and restore is 2 of 3.

6.2.3. Eskro Kunci Privat / Private Key Escrow

Lihat pada bagian 4.12.1.

See section 4.12.1.

Kunci Privat entitas akhir yang hanya digunakan untuk dekripsi dapat dieskro sebelum pembangkitan kunci Sertifikat Elektronik yang terkait dengan Kunci Privat tersebut. Pengamanan kunci yang dieskro minimal harus setara seperti ketika kunci dibangkitkan.

The end entity Private Keys used solely for decryption may be escrowed prior to the generation of the corresponding Electronic Certificates. The escrowed keys must be secured with at least the same level of security used when generating the key.

6.2.4. Backup Kunci Privat / Private Key Backup

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

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

Kunci Privat pemilik yang dititipkan kepada Peruri CA di-*backup*.

The Subscriber's Private Key entrusted to Peruri CA can be backed up.

Semua *backup* Kunci Publik Pemilik dicatat dan dilindungi dengan cara yang sama dengan Kunci Publik asal.

All backups of the Subscriber's Public Key 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 diarsipkan sesuai dengan ketentuan pengarsipan Peruri CA. Sementara itu, Kunci Privat Pemilik tidak boleh diarsipkan.

Before Peruri CA Private Keys is destroyed, the keys are archived in accordance to Peruri CA policy. Meanwhile, Subscribers Private Keys shall not be archived.

6.2.6. Perpindahan Kunci Privat kedalam 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

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

pernah sekalipun boleh berada dalam bentuk *plaintext* di luar modul kriptografi.

plaintext outside the cryptographic module.

Bila sebuah Kunci Privat akan dipindahkan dari satu modul kriptografis ke yang lain, Kunci Privat dienkripsi selama pemindahan. Kunci pemindahan yang dipakai untuk mengenkripsi Kunci Privat 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 Level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi. Kunci Privat Pemilik disimpan minimal dalam perangkat FIPS 140-2 Level 2. Kunci Privat tidak dapat diakses tanpa mekanisme autentikasi.

Peruri CA Private Keys were stored on FIPS 140-2 Level 3 cryptographic module, in encrypted form and password-protected. The Subscriber's Private Key is stored at a minimum in a FIPS 140-2 Level 2 device. The Private Key cannot be accessed without an authentication mechanism.

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.

Pengaktifan Kunci Privat Pemilik dilakukan dengan cara mengautentikasi Pemilik ke modul kriptografi sebelum melakukan aktivasi Kunci Privat terkait. Entri data aktivasi harus dilindungi dari pengungkapan (data tidak boleh ditampilkan saat dimasukkan).

Activation of the Subscriber's Private Key is done by authenticating the Subscriber to the cryptographic module before activating the associated Private Key. Activation data entry must be protected from disclosure (data must not be displayed while it is entered).

Pemilik bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemilik atau kontrak berlangganan.

Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or subscription contract.

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

Setelah dipakai, modul kriptografis 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 Privat Peruri CA tidak diperlukan lagi, para individu dalam peran terpercaya menghapus Kunci Privat dari

When Peruri CA Private Keys are no longer needed, individuals in trusted roles willl delete the Private Keys from

modul kriptografi dan *backup*-nya dengan menimpa Kunci Privat atau menginisialisasi modul dengan fungsi *factory reset* dari Modul Kriptografi.	*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 dicatat ke dalam barang bukti sesuai dengan bagian 5.4.	*The event of destroying Peruri CA's Private Key must be recorded into evidence under section 5.4.*

6.2.11. Pemeringkatan Modul Kriptografis / Cryptographic Module Rating

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

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

6.3.1. Pengarsipan Kunci Publik / Public Key Archival

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat Elektronik.	*The Public Key is archived as part of the Electronic 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 10 (sepuluh) tahun untuk Peruri CA. Sementara untuk kunci Pemilik memiliki periode 1 (satu) 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 10 (ten) years for a Peruri CA. The subscriber key has a period of 1 (one) year.*

6.4. AKTIVASI DATA / DATA ACTIVATION

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

Aktivasi data dibuat secara otomatis oleh HSM yang cocok dan dikirimkan ke *shareholder*, dimana *shareholder* tersebut merupakan orang yang memiliki Peran Terpercaya.	*Activation data is created automatically by the appropriate HSM and sent to the shareholder, where the shareholder is a person who has 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 Privat (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 autentikasi untuk *login* yang diautentikasi. Ini memberikan kontrol akses *discretionary,* pembatasan kontrol akses ke layanan berdasarkan identitas yang diautentikasi, kemampuan audit keamanan, dan catatan audit yang dilindungi untuk berbagi sumber daya, perlindungan diri, dan isolasi proses.	*Peruri CA ensures that the systems maintain 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.	*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 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 Network Time Protocol (NTP).

All Peruri CA components are periodically synchronized with a time service Network Time Protocol (NTP)

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

7.1. PROFIL SERTIFIKAT ELEKTRONIK / CERTIFICATE PROFILE

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

An Electronic 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 meninjau profil Sertifikat Elektronik secara berkala minimal setahun sekali yang dilakukan oleh CA Admin dengan menyesuaikan profil Sertifikat Elektronik dengan regulasi dan / atau persyaratan bisnis.

Peruri CA review Electronic Certificate profile periodically at least once a year done by CA Admin by adjusting the Electronic 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 Electronic 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 Electronic Certificate extensions that comply with RFC 5280.

7.1.2.1. Penggunaan Kunci / Key Usage

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

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

Field / Field	Sertifikat Elektronik Peruri CA / Peruri CA Electronic Certificate	Sertifikat Elektronik Pemilik / Subscriber Electronic Certificate	
		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 ditentukan dalam bagian 7.1.8 dan *field*

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

criticality dari ekstensi ini diisi dengan FALSE.

7.1.8 and the criticality field of this extension is set to FALSE.

7.1.2.3. Batasan Dasar / Basic Constraint

Ekstensi *Basic Constraints* Sertifikat Elektronik X.509 Versi 3 memiliki *field* CA yang diisi TRUE. Ekstensi *Basic Constraints* Sertifikat Elektronik Pemilik memiliki *field* CA yang diisi FALSE. *Field criticality* dari ekstensi ini diisi TRUE untuk Sertifikat Elektronik Peruri CA, tapi bisa diisi TRUE atau FALSE bagi Sertifikat Elektronik Pemilik.

The X.509 Version 3 Electronic Certificate Basic Constraints extension has a CA field filled with TRUE. The Subscriber's Electronic Certificate Basic Constraints extension has a CA field filled with FALSE. The criticality field of this extension is set to TRUE for Peruri CA Electronic Certificates, but can be filled in TRUE or FALSE for Electronic Certificates Subscriber.

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 Elektronik yang diterbitkan. Semua Sertifikat Elektronik dapat mengandung sebuah ekstensi *ExtendedKeyUsage* untuk tujuan bahwa Sertifikat Elektronik tersebut telah diterbitkan untuk *end-user*, dan tidak boleh memuat nilai anyEKU.

By default, ExtendedKeyUsage is set as a non-critical extension. Electronic Certificate issued by Peruri CA may contain the ExtendedKeyUsage extension as a form of technical restriction on the use of the Electronic Certificates they issue. All Electronic Certificate Subscriber can contain an ExtendedKeyUsage extension for the purpose that the Electronic 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 diisi FALSE.

X.509 Version 3 Electronic 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 Electronic Certificate's status. The criticality field of this extension shall be set to FALSE.

URL 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, dihitung sesuai dengan salah satu metode yang

X.509 Version 3 Electronic Certificates are generally populated with an Authority Key Identifier extension. The method for generating the key identifier based on the Public Key of Peruri CA, issuing the Electronic Certificate shall be calculated in accordance with one of the methods

diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini diisi FALSE.	*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 diisi dengan FALSE dan metode untuk menghasilkan *key identifier* yang berbasis pada Kunci Publik subjek Sertifikat Elektronik dihitung sesuai dengan salah satu metode yang diuraikan dalam RFC 5280.	*If present in X.509 Version 3 Electronic 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 Electronic 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 Electronic 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 yang mengacu pada bagian 1.2.	*Electronic Certificates issued under this CPS use OID number that points to section 1.2.*

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 ekstensi entri CRL 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 yang dilakukan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) 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 undergoes annual compliance audits counducted by Ministry of Communication and Information Technology of the Republic of Indonesia (MCIT) 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 memberikan laporan berkala minimal 1 (satu) tahun sekali kepada Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo).	*Peruri CA provide periodic reports at least once a year to the Ministry of Communication and Information Technology of the Republic of Indonesia (MCIT).*

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

Auditor menunjukkan kompetensi pada bidang audit kepatuhan dan benar-benar memahami persyaratan CPS ini. Auditor kepatuhan melakukan audit kepatuhan sebagai tanggung jawab utama.	*Auditor demonstrates competence in the field of compliance audit and shall thoroughly understand the requirements in this CPS. Compliance auditors shall perform compliance audit as their main responsibility.*
Auditor kepatuhan memiliki kualifikasi sebagai berikut:	*Compliance auditors must possess these qualifications:*
a. Tidak memiliki konflik kepentingan terhadap Peruri CA;	*a. Have no conflict of interst with Peruri CA;*
b. Memiliki kemampuan untuk melakukan audit berdasarkan standar audit dalam ketentuan peraturan perundang-undangan termasuk pengetahuan terkait pemanfaatan layanan yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik, X.509 versi 3 IKP *Certificate Policy and Certification Practices Framework*, Undang undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Kemenkominfo terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik;	*b. Auditors shall possess abilities to perform audit based on audit standards stipulated on laws and regulations, including have a sufficient knowledge related the use of services using Electronic Certificate such as Digital Signature, Electronic Seal, X.509 PKI version 3 Certificate Policy and Certificate Practice Framework, Indonesian Law of Electronic Information and Transactions, Indonesian Government Regulation on Electronic System and Transaction Operations, and Indonesia Ministry of Communication and Informatics Regulation on Certification Authority Governance;*

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

c. Auditors shall have adequate skills on IKP technology, information security device and techniques, information security audit, and third party attestation function;

d. Memiliki sertifikasi sebagai auditor sistem informasi (CISA) atau IT Security specialist, spesialis IKP, yang dapat memberikan masukan terkait risiko yang diterima, strategi mitigasi, dan *best practice* industri;

d. Have certification as an information systems auditor (CISA) or IT Security specialist, IPKI specialist, who can provide input related to acceptable risks, mitigation strategies, and industry best practices;

e. Menguasai beberapa keahlian tertentu, pengujian kompetensi, dan jaminan kualitas seperti penelaahan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional; dan

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; and

f. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

f. Bound by law, government regulation, or professional code of ethics.

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 telah 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 carried out has met the needs of the audit scheme used in the assessment. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to 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 dilakukan:

a. Auditor mencatat ketidaksesuaian tersebut;
b. Auditor kepatuhan memberitahu Kementerian Komunikasi dan Informatika Republik Indonesia tentang ketidaksesuaian yang ada;
c. Peruri CA bertanggung jawab untuk memperbaiki ketidaksesuaian dan harus menentukan tindak lanjut yang diperlukan agar sesuai dengan persyaratan CP/CPS dan/atau kontrak masing-masing, kemudian melaksanakan perbaikan tanpa penundaan.

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

a. The auditor shall note the discrepancy;
b. The compliance auditor notifies the Ministry of Communication and Informatics Technology of The Republic of Indonesia of any non-conformities;
c. Peruri CA is responsible for correcting the discrepancy shall and determine what further notifications or actions are necessary pursuant to the requirements of this CP/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 auditor kepatuhan, diberikan kepada *Policy Authority* sebagaimana diatur dalam bagian 8.1. Laporan tersebut mengidentifikasi versi CP dan CPS yang digunakan dalam penilaian.

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, provide 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 satu (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 Elektronik/ Electronic Certificate Issuance or Renewal Fees

Peruri CA mengenakan biaya administrasi dalam menerbitkan atau memperbarui Sertifikat Elektronik termasuk dalam hal penerbitan ulang Sertifikat Elektronik. Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat. Mengenai detail biaya permohonan penerbitan atau pembaruan Sertifikat Elektronik tercantum pada setiap dokumen terkait *Manual Marketing, Sales, and Product*.	*Peruri CA charge administrative fees for Electronic Certificate issuance or renewal including in the case of Electronic 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 Elektronik / Electronic Certificate Access Fees

Peruri CA mengenakan biaya administrasi pengaksesan Sertifikat Elektronik yang telah diterbitkan untuk Tanda Tangan Elektronik dan Segel Elektronik.	*Peruri CA charges administrative fees for accessing Electronic Certificates that have been issued for Digital Signatures and Electronic Seals.*

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

Peruri CA tidak mengenakan biaya terhadap pencabutan Sertifikat Elektronik atau pengecekan status keabsahan Sertifikat Elektronik melalui CRL.	*Peruri CA does not charge fees for revocation of Electronic Certificates or checking the validity status of Electronic Certificates through CRL.*

9.1.4. Biaya Layanan Lainnya / Fees for Other Services

Peruri CA dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya di luar penerbitan dan pembaruan Sertifikat Elektronik.	*Peruri CA may charge a fee for other additional services beyond Electronic Certificate issuance and renewal.*

9.1.5 Kebijakan Pengembalian Sertifikat Elektronik / Electronic Certificate Refund Policy

Tidak ada Kebijakan Pengembalian Sertifikat Elektronik.	*No Electronic Certificate refund policy.*

9.2. TANGGUNG JAWAB KEUANGAN / FINANCIAL RESPONSIBILITY

9.2.1. CakupanAsuransi / Insurance Coverage

Peruri CA menjamin kerugian akibat kegagalan layanan Penyelenggaraan Sertifikasi Elektronik yang dapat dibuktikan akibat kelalaian Peruri CA dalam mematuhi kewajiban sebagai PSrE sesuai dengan Ketentuan Perundang-	*Peruri CA guarantees losses due to failure of Certification Authority services which can be proven due to their failure to comply with obligations as CA in accordance with the provisions of the*

undangan yang diatur dalam dokumen Kebijakan Jaminan.

legislation as stipulated in the Warranty 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 atas setiap perselisihan yang timbul dari atau sehubungan dengan layanan Peruri CA atau penggunaan Situs oleh Pemilik Sertifikat Elektronik, 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 Subscriber for any disputes arising out of or in connection with Peruri CA's services or the use of the Site by the Electronic Certificate Subscriber, 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 Pemilik sebagaimana dijabarkan pada bagian 9.4;

a. Personal Information from Subscriber as detailed in section 9.4;

b. Rekam jejak audit (*audit logs*) dari sistem Peruri CA dan RA;

b. Audit logs from Peruri CA and RA systems;

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

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

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

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

Plans (BCP);

Continuity Plans (BCP);

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

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

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

f. Documents related to the Business Plan, VA / pentest results, network topology with IP Address, employee work assessment results, system administrator logs, and other documents mentioned in the SOP for Document and Records Control.

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 (biasa). Informasi mengenai status Sertifikat Elektronik dan Sertifikat Elektronik itu sendiri termasuk kategori informasi publik.

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

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

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

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

a. Pelatihan atau peningkatan *awareness;*

a. Training or increase awareness;

b. Perjanjian kontrak pegawai; dan

b. Contracts with employees; and

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

c. Non-Disclosure Agreement (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 melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat dirilis atas permintaan

Peruri CA protects all Subscribers personally identifiable information from unauthorized disclosure. Personal information may be released at the

Pemilik terhadap Peruri CA. Arsip yang dikelola oleh Peruri CA tidak boleh dirilis kecuali yang diizinkan pada bagian 9.4.1.

request of the Subscriber against Peruri CA. 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 Elektronik, profil OCSP dan CRL tidak dianggap pribadi.

Information contained in Electronic Certificates, OCSP profiles and CRLs is not considered 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 berbentuk digital maupun kertas. *Backup* informasi pribadi 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. Backup personal information is encrypted every time it is moved 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 mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Perjanjian Pelanggan mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh Peruri CA.

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 accommodates all provisions related to the use of personal information into the Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by Peruri CA.

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

Peruri CA tidak membuka informasi pribadi kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, ketentuan peraturan perundang-undangan, atau perintah pengadilan.

Peruri CA not disclose personal information to any third party except as authorized by this policy, required by law, statutory provisions, or court orders.

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 PERNYATAAN 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 Elektronik yang diterbitkan berdasarkan CPS ini diverifikasi sesuai dengan CPS ini dan memenuhi persyaratan minimum; dan
d. Peruri CA mengelola Repositori informasi publik pada situs web-nya.

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 Electronic Certificates issued under this CPS is 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

Tidak ada ketentuan.

Not applicable.

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat / Subscriber Representations and Warranties

Pemilik menjamin bahwa:

a. Setiap Sertifikat Elektronik yang dibuat menggunakan Kunci Privat serta berkorespondensi dengan Kunci Publik yang tercantum pada Sertifikat Elektronik adalah merupakan Tanda Tangan Elektronik Pemilik dan Sertifikat Elektronik yang sudah disetujui serta secara operasional (tidak kedaluwarsa dan telah dicabut) saat Tanda Tangan Elektronik dibuat;
b. Setiap Kunci Privat diamankan dan hanya Pemilik yang memiliki akses terhadap Kunci Privat tersebut;
c. Sudah melakukan peninjauan terhadap informasi dari Sertifikat Elektronik;
d. Semua informasi yang diberikan oleh Pemilik dan informasi yang berada di dalam Sertifikat Elektronik adalah benar;

Subscribers warrant that:

a. Each Electronic Certificate created using the Private Key corresponding to the Public Key listed in the Electronic Certificate is the Digital Signature of the Subscriber and the Electronic Certificate has been accepted and is operational (not expired or revoked) at the time the Digital Signature is created;
b. Each Private Key must be secured and only the Sucscriber has access to the Private Key;
c. Have thoroughly reviewed the Electronic Certificate information;
d. All information supplied by the Subscriber and contained in the Electronic Certificate is true;

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

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

f. Segera:
   i. Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat Elektronik 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 Elektronik,
   ii. Mengajukan permohonan untuk melakukan pencabutan Sertifikat Elektronik, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam Sertifikat Elektronik tersebut, dan
   iii. Menghentikan penggunaan Kunci Privat yang Kunci Publik-nya tercantum dalam Sertifikat Elektronik setelah dicabut.

f. Promptly:
   i. Request revocation of the Electronic Certificate and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Electronic Certificate,
   ii. Request revocation of the Electronic Certificate, and cease using it, if any information in the Electronic Certificate is or becomes incorrect or inaccurate, and
   iii. Stop using the Private Key whose Public Key is listed in an Electronic Certificate after revoked.

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

g. Will respond to Peruri CA's instructions regarding compromise or Electronic Certificates misuses within 48 (forty eight) hours,

h. Menyetujui dan menerima bahwa Peruri CA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat Elektronik jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Pelanggan atau jika Peruri CA menemukan bahwa Sertifikat Elektronik tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware*;

h. Acknowledges and accepts that Peruri CA is entitled to revoke the Electronic Certificate immediately if the Subscriber violates the terms of the Subscriber Agreement or terms of use or if Peruri CA discovers that the Electronic Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, and

i. Pemilik adalah pengguna akhir dan bukan merupakan Penyelenggara Sertifikasi Elektronik, dan tidak menggunakan Kunci Privat yang Kunci Publiknya tercantum dalam Sertifikat Elektronik untuk tujuan

i. Subscriber of the Electronic 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 Electronic

penandatangan Sertifikat Elektronik Penyelenggara Sertifikasi Elektronik lain.

Certificate of another Certification Authority.

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

Pihak yang mengandalkan Sertifikat Elektronik Peruri CA menjamin bahwa:

a. Memiliki kemampuan teknis untuk menggunakan Sertifikat Elektronik;
b. Apabila perwakilan dari Pihak Pengandal menggunakan suatu Sertifikat Elektronik yang diterbitkan oleh Peruri CA, Pihak Pengandal secara benar memverifikasi informasi yang tercantum di dalam Sertifikat Elektronik 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 Elektronik, 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. Mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

Peruri CA's Electronic Certificate relying party guarantee that:

a. Have the technical capability to use Electronic Certificates;
b. If the representative from the relying party use an Electronic Certificate issued by Peruri CA, Relying Party should verify the information contained in the Electronic 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 Electronic 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 dalam CPS ini tidak menjamin bahwa:

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 Elektronik yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Pasangan Kunci dan Penggunaan Sertifikat Elektronik); dan
c. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau *testing* Sertifikat Elektronik.

Peruri CA in this CPS that they do not warrant that:

a. Except for the warranties stated in the CPS and contractual agreements and to the extent permitted by law, Peruri CA disclaims all warranties or other conditions (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use;

b. Misuse of an Electronic Certificate that is inconsistent with its usage as shown in section 4.5 (Key Pair and Electronic Certificate Usage); and

c. The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo Electronic 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 Elektronik yang tidak tepat, termasuk:

a. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat Elektronik atau Pasangan Kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Pelanggan, atau yang diatur dalam Sertifikat Elektronik 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 Elektronik yang berasal dari Pemilik setelah periode verifikasi data selesai; dan
e. Sertifikat Elektronik yang tidak diterbitkan atau dikelola sesuai dengan CP dan CPS Peruri CA.

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

a. All damage caused by the misuse of Electronic Certificatesor Key Pairs beside the proper use that have been defined in CPS, subscriber's agreement, or all provision which have been mentioned in the Electronic Certificates;
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 Electronic Certificate information that comes from Subscriber after data verification period is complete; and
e. Electronic Certificate not issued or administered in accordance with Peruri CA CP and CPS.

9.8.2 Pembatasan Tanggung Jawab RA / RA Limitation of Liability

Tidak ada ketentuan.	*No stipulation.*

9.9 GANTI RUGI / INDEMNITIES

9.9.1 Ganti Rugi oleh Peruri CA / Indemnification by Peruri CA

Kewajiban ganti rugi Peruri CA ditetapkan dalam CPS, Perjanjian Kerja Sama dengan klien, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat yang diatur dalam Kebijakan Jaminan.	*Peruri CA's indemnification obligations must be set forth in its CPS, Subscription Contract with clients, or Relying Party Agreement including any obligation to third party beneficiaries as set in Warranty Policy.*
Peruri CA tidak bertanggung jawab atas penggunaan Sertifikat Elektronik yang tidak tepat.	*Peruri CA has no liability for the improper use of Electronic Certificate.*

9.9.2 Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Subscibers

Diatur dalam Perjanjian Kerja Sama (PKS) dan atau Kebijakan Jaminan.	*Regulated in the Subscription Contract and Warranty Policy.*

9.9.3 Ganti Rugi oleh Pihak Pengandal / Indemnification by Relying Parties

Diatur dalam Perjanjian Kerja Sama (PKS) dan atau Kebijakan Jaminan.	*Regulated in the Subscription Contract and Warranty Policy.*

9.10 JANGKA WAKTU DAN PENGAKHIRAN / TERM AND TERMINATION

9.10.1 Jangka Waktu / Term

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh Peruri CA melalui situs web atau laman 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 (tiga puluh) hari setelah dipublikasikan.	*Notified changes of this CPS are appropriately marked by an indicated version. Following publications, changes become applicable 30 (thirty) days thereafter.*

9.10.3 Efek Pengakhiran dan Keberlangsungan / Effect of Termination and Survival

Peruri CA mengkomunikasikan kondisi, akibat dari penghentian CPS, dan juga kondisi keberlangsungan dari sertifikat yang telah terbit melalui situs web atau laman repositorinya.	*Peruri CA communicates the conditions, consequences of terminating the CPS, as well as the state of sustainability of the certificates that have been issued via the website or repository.*

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

Peruri CA menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, baik yang ditandatangani secara elektronik, telepon atau surel. Peruri CA memberikan tanda terima yang valid sebagai bukti bagi pengirim. Peruri CA memberi tanggapan paling lama 7 (tujuh) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke Peruri CA dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS.

Peruri CA provides communication media for related parties through electronic documents, electronic mail, whether electronically signed, telephone or email. Peruri CA provides a valid receipt as proof for the sender. Peruri CA will respond within 7 (seven) working days through the same communication media. Communications made to Peruri CA must be addressed as stated in section 1.5.2 of the CPS.

9.12 AMENDEMEN / AMENDMENTS

9.12.1 Prosedur untuk Amendemen / Procedure for Amendment

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

Peruri CA should post appropriate notice on the website 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 7 (tujuh) hari kerja sejak ditandatangani dan semua pihak yang berkepentingan dianggap mengetahui perubahan yang telah diumumkan. Salinan CPS terbaru dapat dilihat pada situs web https://ca.peruri.co.id/ca/legal.

Each time the CPS is changed, the CPS will be announced within 7 (seven) working days from the date it was signed and all interested parties are deemed to be aware of the changes that have been announced. The latest CPS can be found on the website https://ca.peruri.co.id/ca/legal.

9.12.3 Keadaan Dimana OID Diubah / Circumstances Under Which OID Changed

Peruri CA mengikuti kebijakan perubahan OID yang dilakukan oleh PSrE Induk.

Peruri CA follows the OID change policy made by Root CA.

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

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 Electronic Certificate Subscriber.

antara Peruri CA dengan Pemilik Sertifikat Elektronik.

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 Elektronik Peruri CA dipakai untuk kebutuhan komersial atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan Peruri CA, tetap menerapkan aturan hukum di Indonesia.

This CPS is governed, construed and understood in accordance with the laws of Indonesia. The choice of this rule of law is to obtain the same understanding, regardless of the location of domicile or the location of the use of Peruri CA Certificates or other products/services. Including if Peruri CA Electronic Certificate is used for commercial or contractual needs in other countries, whether implied or expressly using Peruri CA services, still applying the rule of law in Indonesia.

Para pihak, termasuk *partner* dari Peruri CA, Pemilik dan Pihak Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

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 beberapa produk dan layanan manajemen Sertifikat Elektronik Peruri CA dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang berwenang. Para Pihak (termasuk Peruri CA, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi Ketentuan Perundang-undangan terkait regulasi ekspor yang berlaku di Indonesia.

Peruri CA complies with applicable laws of Indonesia. Export of certain types of software used in certain CAs Electronic Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including Peruri CA, Subscribers 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

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.

dari Peruri CA. Setiap adanya upaya percobaan maka akan dibatalkan.

Any such attempted assignment shall be void.

9.16.3 Keterpisahan / Severability

Jika terdapat ketentuan dari CPS ini, termasuk pembatasan dari klausul pertanggungan, ditetapkan 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 diberlakukan dengan sebagaimana mestinya.

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, intended to be separable and independent from other provisions and enforced accordingly.

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 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 telah menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Peruri CA.

Peruri 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 has provided BCP and DRP with reasonable control in accordance with Peruri CA's capabilities.

9.17 PROVISI LAIN / OTHER PROVISIONS

Tidak ada ketentuan. *No stipulation.*

"Pemohon" adalah orang, badan usaha, atau badan hukum yang mengajukan permohonan penerbitan Sertifikat Elektronik kepada Peruri CA.	***"Applicant"*** *is a person, business entity, or legal entity that submits an application for the issuance of Electronic Certificates to Peruri CA.*
"Pemilik" adalah orang, badan usaha, atau badan hukum yang sudah diterbitkan dan memiliki Sertifikat Elektronik.	***"Subscriber"*** *is a person or business entity that has been issued and has an Electronic Certificate.*
"Pelanggan" adalah orang atau badan usaha yang menggunakan layanan Peruri CA tetapi tidak memiliki atau diterbitkan Sertifikat Elektronik.	***"Customer"*** *is a person or business entity that uses PERuri CA services but does not have or issue Electronic Certificates.*
"Peran Terpercaya" adalah peran-peran yang melakukan fungsi yang sangat penting, dimana jika fungsi tersebut tidak dilakukan dengan benar dan sesuai, dapat menimbulkan dampak yang sangat buruk bagi tingkat kepercayaan PSrE.	***"Trusted Roles"*** *are roles that perform critical actions, which, when those actions are not performed correctly and appropriately, can result in a detrimental effect for CA's trustworthiness.*
"Sertifikat Elektronik" adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Peruri CA sebagai Penyelenggara Sertifikasi Elektronik (PSrE).	***"Electronic Certificate"*** *is an electronic certificate containing a Digital Signature and identity indicating the status of the legal subjects of the parties in the Electronic Transaction issued by Peruri CA as Certificate Authority (CA).*
"Tanda Tangan Elektronik" adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.	***"Digital Signature"*** *is a signature consisting of electronic information that is attached, associated, or related to other electronic information used as a means of verification and authentication.*
"Segel Elektronik" adalah data elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik dan/atau dokumen elektronik untuk menjamin asal, integritas dan keutuhan dari informasi elektronik dan/atau dokumen elektronik yang digunakan oleh Badan Usaha atau Instansi.	***"Electronic Seal"*** *is electronic data attached, associated, or related to electronic information and/or electronic documents to guarantee the origin, integrity and integrity of electronic information and/or electronic documents used by Business Entities or Institutions.*
"*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"*** *is an online software application operated under the authority of Peruri CA and connected to its repository for processing Electronic Certificate status requests.*

"*Hardware Security Module*" adalah perangkat komputasi fisik yang melindungi dan mengelola kunci digital untuk autentikasi yang kuat dan menyediakan operasi kriptografi yang sesuai dengan FIPS 140-2 Level 3.	*"Hardware Security Module" is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic operation that conform to FIPS 140-2 Level 3.*
"Pasangan Kunci" adalah Kunci Privat dan Kunci Publik yang mengacu ke entitas yang sama, yang memiliki karakterisitik khusus, sehingga suatu pesan yang dienkripsi memakai Kunci Privat hanya dapat didekripsi dengan Kunci Publik pasangannya, dan sebaliknya.	***"Key Pair"** is Private Key and Public Key referring to the same entity, which possess certain characteristics, so that a message encrypted by a Private Key can only be decrypted by the corresponding Public Key, and vice versa.*
"Kunci Privat" adalah kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Elektronik dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.	***"Private Key"** is 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 Elektronik yang dibuat oleh pemegangnya.	***"Public Key"** is 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.*
"Pihak Pengandal" adalah orang, badan usaha, atau badan hukum yang mempercayai pada informasi yang terkandung dalam Sertifikat Elektronik atau token stempel waktu.	***"Relying Party"** is person, business entity, or legal entity that relies upon either the information contained within an Electronic Certificate or a time-stamp token.*
"Peruri CA" adalah unit bisnis Peruri yang memberikan layanan Tanda Tangan Elektronik, Sertifikat Elektronik, dan Stempel Elektronik. Bertindak dengan persetujuan Pemilik Sertifikat Elektronik untuk membangkitkan Pasangan Kunci, membuat CSR, dan menggunakan kunci untuk kebutuhan penandatanganan dokumen elektronik. Menerapkan control pengamanan terhadap Kunci Privat dan 2FA untuk penggunaan penandatanganan	**"Peruri CA"***is Peruri's business unit that provides Digital Signature, Electronic Certificate, and Electronic Seal services. Act on behalf of the Electronic Certificate Subscriber 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.*
"Kebijakan Jaminan" adalah dokumen yang berisikan ketentuan pemberian ganti rugi yang dialami Pemilik Sertifikat akibat kegagalan penyelenggaraan layanan.	***"Warranty Policy"** is a document which contains the provision of compensation experienced by the Subscriber as a result of the failure to provide services.*

"Perjanjian Pelanggan" adalah perjanjian yang melibatkan Pemilik sebagai pihak yang telah diterbitkan Tanda Tangan Elektronik, Sertifikat Elektronik, dan Stempel Elektronik oleh Peruri CA.	***"Subscriber Agreement"*** *is an agreement involving the Subscriber as a party that has been issued a Digital Signature, Electronic Certificate, and Electronic Seal by Peruri CA.*