PERURI CA	Number : 002/KRC/KBJ/CP/XII/2018 Start From : 23 November 2018 Version : 2 Revision : 2 Revision Date : 6 Maret 2020 Page : 67 Pages OID : 2.16.360.1.1.1.12.3

Peruri CA
Certificate Practice Statement

REVISION NOTE / CATATAN REVISI

NO.	DATE	VERSION	REVISION	DESCRIPTION
1	23 November 2018	1	0	*Initial Release*
2	14 December 2018	1	1	*Updated Document* - *1.6 Definitions and Acronyms*
3	16 January 2019	1	2	*Statement Change* 6.1.2
4	13 February 2019	1	3	*Major Update* - Root CA Indonesia Alignment - *Bilingual* Bahasa Indonesia
5	6 May 2019	2	0	*Major Update* - *OID Number* - *Footer* - *CRL Interval* - *Limitation of Peruri CA Responsibility* - *Point 4.12.1, 4.9.7, 6.1.2, 6.2.1, 6.2.4, 6.2.5, and 9.8.1*
6	10 July 2019	2	1	*Minor Update* - *Typo Correction* - *Writing Format* - CRL Interval (Point 4.9.7) - Interlock Scheme (Point 5.6.1) - Table of Content Revision
7	6 Maret 2020	2	2	Minor update - Archive retention period - Types of Records Archived - Authentication of Individual Identity

Dwina Septiani W.

PRESIDENT DIRECTOR OF PERURI / Direktur Utama Peruri

TABLE OF CONTENTS / DAFTAR ISI

1. INTRODUCTION / PENDAHULUAN

1.1 OVERVIEW / RINGKASAN

Peruri CA's Public Key Infrastructure is a hierarchical PKI with the trust chain starting from the Root CA Indonesia. Ministry of Communication and Information Technology, Republic of Indonesia (MCIT) operates Root CA Indonesia.

Peruri is a non-Government CA under Root CA Indonesia. This CPS is governed by the Peruri CA's CP.

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

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.

Infrastruktur Kunci Publik (IKP) Peruri adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikat Elektronik (PSrE) Induk Indonesia. Kementerian Komunikasi dan Informatika Republik Indonesia (Kemenkominfo) mengoperasikan PSrE Induk Indonesia.

Peruri CA merupakan PSrE non-Instansi di bawah PSrE Induk Indonesia. CPS ini diatur oleh CP Peruri CA.

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

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*.

1.2 DOCUMENT NAME AND IDENTIFICATION/ IDENTIFIKASI DAN NAMA DOKUMEN

This document is Certification Practice Statement Peruri CA.

Object Identifier (OID) value used for certificate (not include EV certificate) for this CPS is: 2.16.360.1.1.1.12

Dokumen ini adalah Dokumen *Certification Practice Statement* (CPS) Peruri CA.

Object Identifier (OID) yang digunakan untuk sertifikat (tidak termasuk *Extended Validation Certificate*) ini adalah: 2.16.360.1.1.1.12.3

1.3 PKI PARTICIPANTS / PARTISIPAN IKP

1.3.1 Certification Authorities / Penyelenggara Sertifikat Elektronik (PSrE)

1.3.1.1 Root CA Indonesia / PSrE Induk Indonesia

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

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

- *Control over the registration process,*
- *Identification and authentication process,*
- *Certificate manufacturing process,*

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

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

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

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

1.3.1.2 Peruri CA

Peruri CA is a subordinate CA under the Root CA Indonesia

Peruri CA merupakan PSrE Berinduk di bawah PSrE Induk Indonesia.

1.3.2 Registration Authorities / Otoritas Pendaftaran (RA)

Peruri CA may designate specific RAs to perform the Subscriber Identification and Authentication and certificate request and revocation functions defined in the CP, CPS and related documents.

Peruri CA dapat menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan Identifikasi dan Autentikasi Pemilik, serta permohonan dan pencabutan sertifikat sesuai dengan yang telah didefinisikan pada CP, CPS dan dokumen terkait.

1.3.2.1 Function of Registration Authorities / Fungsi dari RA

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

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

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

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

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

No stipulation

Tidak ada ketentuan.

1.3.3 Subscribers / Pemilik

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

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

1.3.4 Relying Parties / Pihak Pengandal

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

A relying party is the entity that relies on the validity of the binding of the subscriber's name to the public key. The relying party is responsible for checking the status of the information in the certificate. A relying party may use the information in the certificate to determine the suitability of the certificate to a particular use. Such information includes the following:

- *Purpose for which a certificate is used;*
- *Digital signature verification responsibilities;*
- *Revocation checking responsibilities; and*
- *Acknowledgement of applicable liability caps and warranties.*

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

Pihak Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama pemilik dengan kunci publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat. Pihak Pengandal dapat menggunakan informasi dalam sertifikat untuk menentukan kesesuaian penggunaan sertifikat. Informasi yang dimaksud adalah sebagai berikut:

- Tujuan penggunaan sertifikat
- Tanggung jawab verifikasi tanda tangan digital
- Tanggung jawab pemeriksaan pencabutan sertifikat
- Pengakuan atas batasan kewajiban dan jaminan yang berlaku

1.3.5 Other Participants / Partisipan Lain

1.3.5.1 Policy Authority / Otoritas Kebijakan (PA)

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

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

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

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

1.4 CERTIFICATE USAGE / KEGUNAAN SERTIFIKAT

1.4.1 Appropriate Certificate Uses / Penggunaan Sertifikat yang Semestinya

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

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

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

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

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

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

Certificate Class / Kelas Sertifikat	*Assurance Level* / Tingkat Jaminan			*Usage* / Penggunaan		
	Low Assurance /Jaminan Rendah	*Medium Assurance* /Jaminan Sedang	*High Assurance* /Jaminan Tinggi	*Encryption* /Enkripsi	*Digital Signature* /Tanda Tangan Digital	*Email Protection*/ Perlindungan Email
Individual Certificates / Sertifikat Individu						

Level 3		✓		✓	✓	
Level 4			✓	✓	✓	
Organizational Certificate / Sertifikat Organisasi						
Organizational Certificate/ Sertifikat Organisasi			✓		✓	

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

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

1.4.2 Prohibited Certificate Uses / Penggunaan Sertifikat yang Dilarang

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

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

1.5 POLICY ADMINISTRATION / ADMINISTRASI KEBIJAKAN

1.5.1 Organization Administering the Document / Organisasi Pengaturan Dokumen

This CPS and the document referenced herein are maintained by:

CP dan dokumen referensinya dikelola oleh:

Email :policy.ca@peruri.co.id

Phone : +62 21 739 5000

Fax : +62 21 7221 156

Web : https://www.peruri.co.id/ca/legal_repository

1.5.2 Contact Person / Narahubung

Email : admin.ca@peruri.co.id

Telepon: +62 21 739 5000

Fax : +62 21 7221 156

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

Peruri CA employs a Compliance Officer (CO) and internal auditor (IA) to ensure conformance of the CPS to this CP and that this CPS is inline with the Root CA Indonesia CPS.

Peruri CA mempekerjakan Petugas Kepatuhan (CO) dan auditor internal (IA) untuk memastikan kesesuaian CPS dengan CP dan bahwa CPS ini sejalan dengan CPS Root CA Indonesia.

1.5.4 CPS Approval Procedures / Prosedur Persetujuan CPS

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

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

1.6 DEFINITIONS AND ACRONYMS

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

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

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

"Private Key" *means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.*

"Public Key" *means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's*

"Relying Party" *means an entity that relies upon either the information contained within a certificate or a time-stamp token.*

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

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

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

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

"Kunci Publik" adalah kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Privat terkait dan yang digunakan oleh Pihak Penghandal untuk memverifikasi Tanda Tangan Digital yang dibuat oleh pemegangnya.

*"***Pihak Pengandal***"* entitas yang mempercayai pada informasi yang terkandung dalam sertifikat atau token stempel waktu.

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

2.1 REPOSITORIES / REPOSITORI

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

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION / PUBLIKASI INFORMASI SERTIFIKASI

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

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

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

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

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

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

2.3 TIME OF FREQUENCY OF PUBLICATION / WAKTU ATAU FREKUENSI PUBLIKASI

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

The CRL is updated according to the section 4.9.7

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

CRL diperbaharui sesuai dengan Frekuensi Penerbitan CRL bagian 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES / KENDALI AKSES PADA REPOSITORI

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

Informasi yang terpublikasi pada repositori adalah informasi publik. Peruri CA memberikan akses baca yang tidak dibatasi pada repositori dan harus menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.

3. IDENTIFICATION AND AUTHENTICATION / IDENTIFIKASI DAN AUTENTIKASI

3.1 NAMING / PENAMAAN

3.1.1 Types of Names / Tipe Nama

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

Certificate Type	*(DN) Distinguised Name*
Peruri CA Certificate	*CN=<Nama PSrE>,O=<nama organisasi>,C=ID*
Subscriber Certificate	*CN=<person name>, OU=<organizational_unit>,O=<organization_name>, C=ID*

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

Tipe Sertifikat	(DN) Distinguised Name
Sertifikat Peruri CA	CN=<Nama PSrE>,O=<nama organisasi>,C=ID
Sertifikat Pemilik	CN=<nama_orang>, OU=<unit_organisasi>, O=<nama_organisasi>, C=ID

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

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

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

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

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

3.1.3 Anonymity or Pseudonymity of Subscribers / Anonimitas atau Pseudonimitas Pemilik

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

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

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

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

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

3.1.5 Uniqueness of Names / Keunikan Nama

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

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

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

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

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

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

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

3.2 INITIAL IDENTITY VALIDATION / VALIDASI IDENTITAS AWAL

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.

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

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

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

- *Subscribers submit public key*
- *Subscribers submit CSR offline*

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

- Pemilik menyerahkan kunci publik
- Pemilik menyerahkan CSR secara *offline*

3.2.2 Authentication of Organization Identity / Autentikasi Identitas Organisasi

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

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

Identification and authentication requirements for an organization:

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

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

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

Persyaratan identifikasi dan autentikasi untuk suatu organisasi:

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

3.2.3 Authentication of Individual Identity / Autentikasi Identitas Individu

An application to be a Subscriber may be made by an organization legally authorized to act on behalf of the prospective Subscriber after they complete the appropriate forms and follow the established processes and procedures. For the purpose of identification and authentication of the individual shall:

1. *Shows the official identity issued by the government*
2. *Show the official identity issued by the company*
3. *Email address*
4. *Cellphone number*

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

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

1. Menunjukan identitas resmi yang dikeluarkan oleh pemerintah
2. Menunjukan identitas resmi yang dikeluarkan oleh perusahaan
3. Alamat email
4. Nomor handphone

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

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

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

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

3.2.5 Validation of Authority / Validasi Otoritas

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

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

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

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

3.2.6 Criteria for Interoperation / Kriteria Inter-operasi

No stipulation.

Tidak ada ketentuan.

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

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

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

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

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

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

Setelah sertifikat dicabut selain karena alasan pambaruan, Pemilik harus mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2 untuk mendapatkan sertifikat baru dengan kunci yang baru.

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

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

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

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

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

Pencabutan sertifikat harus memenuhi salah satu dari proses berikut:

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

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

4.1 CERTIFICATE APPLICATION / PERMOHONAN SERTIFIKAT

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

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to Peruri CA.

Peruri CA does not issue Certificates to entities on a government denied list maintained by the Republic of Indonesia or that is located in a country with which the laws of the Republic of Indonesia prohibit doing business.

Baik pemohon atau individu yang berwenang untuk meminta Sertifikat atas nama Pemohon dapat mengajukan permintaan Sertifikat. Pemohon bertanggung jawab atas data apapun yang Pemohon atau agen dari Pemohon sediakan untuk Peruri CA.

Peruri CA tidak menerbitkan Sertifikat kepada entitas pendaftar yang ditolak pemerintah yang dikelola oleh badan hukum Republik Indonesia

4.1.2 Enrollment Process and Responsibilities / Proses Pendaftaran dan Tanggung Jawabnya

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

In no particular order, the enrollment process includes:

1. *Submitting a certificate application,*
2. *Generating a Key Pair,*
3. *Delivering Key Pair to Subscriber,*
4. *Agreeing to the applicable Subscriber Agreement, and*
5. *Paying any applicable fees.*

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

1. Mengirimkan Permohonan Sertifikat,
2. Membangkitkan Pasangan Kunci,
3. Memberikan Pasangan Kunci kepada Pemilik,
4. Menyetujui Perjanjian Pemilik yang berlaku,
5. Membayar biaya yang berlaku.

4.2 CERTIFICATE APPLICATION PROCESSING / PEMROSESAN PERMOHONAN SERTIFIKAT

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

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

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

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

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

Setelah semua pemeriksaan identitas dan atribut pemohon, konten permohonan untuk sertifikat juga diperiksa. Dalam hal pemohon tidak memenuhi syarat untuk sertifikat atau permohonannya mengandung kesalahan, maka Peruri CA harus menolak permohonan tersebut. Apabila tidak ada masalah, maka permohonan disetujui.

4.2.3 Time to Process Certificate Applications / Waktu Pemrosesan Permohonan Sertifikat

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

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

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

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

4.3 CERTIFICATE ISSUANCE / PENERBITAN SERTIFIKAT

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

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 authenticate a Certificate Request, ensure that the Public Key is bound to the correct Applicant, obtain a proof of possession of the Private Key, then generate a Certificate, and provide the Certificate to the Applicant. Peruri CA publish the Certificate to a repository in accordance with this CP and the applicable CPS. This is done in a timely manner, which is detailed in section 4.2.

- *Peruri CA check documents*
- *After signed, digital certificate will be handed over to Subscriber*

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

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

- Peruri CA memeriksa dokumen
- Setelah ditandatangani, sertifikat digital akan diserahkan kepada Pemilik

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

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

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

4.4 CERTIFICATE ACCEPTANCE / PENERIMAAN SERTIFIKAT

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

Subscriber should check all information of certificate and sign digital certificate acceptance form before using the certificate. Peruri CA shall notify to the Subscriber that they cannot use the certificate before checking all the information of certificate.

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

For the issuance of CA Certificates Peruri CA shall set up an acceptance procedure indicating and documenting the acceptance of the issued CA Certificate.

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

Bila tidak ada keluhan dari Pemilik dalam waktu tujuh (7) hari kerja, Pemilik dianggap menerima semua informasi sertifikat.

Dalam hal penerbitan Sertifikat PSrE, Peruri CA harus membuat prosedur penerimaan dan mendokumentasikan penerimaan Sertifikat PSrE yang terbitkan.

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

Peruri CA publish certificates in a repository as stated in section 2.2 as soon as they are issued. Peruri CA publish end-user certificate by sending it to the certificate owner.

Peruri CA mempublikasikan sertifikatnya dalam sebuah repositori sebagaimana tercantum pada bagian 2.2 segera setelah sertifikat diterbitkan. Peruri CA mempublikasikan sertifikat Pengguna Akhir dengan mengirimkannya ke Pemilik sertifikat.

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

No stipulation.

Tidak ada ketentuan.

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

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

All Subscriber and Peruri CA shall protect their Private Key from unauthorized use or disclosure by other parties and shall use their Private Keys only for their intended purpose.

Semua Pemilik dan Peruri CA harus melindungi Kunci Privat mereka dari penggunaan tanpa izin atau pengungkapan oleh pihak lain, dan harus menggunakan Kunci Privat mereka hanya untuk tujuan yang ditentukan.

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

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

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

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

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

4.6 CERTIFICATE RENEWAL / PEMBAHARUAN SERTIFIKAT

4.6.1 Circumstance for Certificate Renewal / Kondisi untuk Pembaharuan Sertifikat

A Certificate may be renewed if:

1. *the Public Key has not reached the end of its validity period*
2. *the associated Private Key has not been revoked or compromised*
3. *the Issuing CA name and attributes are unchanged.*

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

Sertifikat dapat diperpanjang/diperbaharui bila:

1. Kunci Publik belum mencapai akhir masa berlakunya,

2. Kunci Privat terkait tidak dicabut atau bocor,
3. Nama dan atribut PSrE Penerbit tidak berubah

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

4.6.2 Who May Request Renewal / Siapa yang Dapat Meminta Pembaharuan

The Subscriber may request the renewal of its Certificate.

Pemilik dapat meminta pembaharuan sertifikatnya.

4.6.3 Processing Certificate Renewal Requests / Pemrosesan Permintaan Pembaharuan Sertifikat

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

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

Perpanjangan sertifikat harus memenuhi salah satu dari proses berikut:

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

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

The same new certificate issuance procedure is followed, as stated in section 4.3.2.

Prosedur pemberitahuan penerbitan sertifikat baru sama seperti yang dinyatakan pada bagian 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate / Sikap yang Dianggap sebagai Menerima Sertifikat yang Diperbaharui

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

PSrE Penerbit harus menerima sertifikat yang diperbaharui mengikuti prosedur penerimaan dan penerimaan sertifikat yang sama, sebagaimana dinyatakan dalam bagaian 4.4.1.

4.6.6 Publication of the renewal certificate by the CA / Publikasi Sertifikat yang Diperbaharui oleh PSrE

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

Sertifikat baru diterbitkan sesuai prosedur yang dinyatakan dalam bagian 4.4.2.

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

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

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

4.7 CERTIFICATE RE-KEY / PENGGANTIAN KUNCI SERTIFIKAT

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

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

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

Prior to the expiration of an existing certificate of Peruri CA, Peruri CA may renew its keys if it deemed necessary regarding to one of the following reasons:

- *Migration of hardware;*
- *The keys have low cryptographic strength;*
- *The Private and Public Key will reach the end of its validity period soon;*
- *The keys have high exposure; or*
- *Enforced by standards or applications.*
- *Peruri CA private key compromise.*

Sebelum sertifikat Peruri CA yang ada berakhir, Peruri CA dapat memperbarui kuncinya jika dianggap perlu terkait dengan salah satu alasan berikut:

- Migrasi perangkat keras;
- Kunci memiliki kekuatan kriptografi yang rendah;
- Kunci Privat dan Publik akan mencapai akhir masa berlakunya;
- Kunci memiliki frekuensi pemakaian yang tinggi; atau
- Diperkuat oleh standar atau aplikasi.
- Kunci Privat bocor.

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

In accordance with the conditions specified in section 4.7.1, only Peruri CA may request re-key of its CA certificate.

Subscriber is not allowed for request re-key.

Sesuai dengan ketentuan yang terdapat pada bagian 4.7.1, hanya Peruri CA yang dapat meminta Penggantian Kunci Sertifikat.

Pemilik sertifikat tidak diijinkan untuk meminta Penggantian Kunci Sertifikat.

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

Peruri CA re-keying procedure is processed in accordance with internal document of Peruri CA.

Prosedur Penggantian Kunci untuk Peruri CA dilaksanakan sesuai dengan dokumen internal Peruri CA.

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

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

Sertifikat baru diterbitkan sesuai prosedur yang dinyatakan dalam bagian 4.4.2.

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

No Stipulation.

Tidak ada ketentuan.

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

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

Sertifikat dengan Kunci Baru dipublikasikan, sesuai dengan prosedur repositori, sebagaimana yang dinyatakan pada bagian 4.4.2.

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

No Stipulation.

Tidak ada ketentuan.

4.8 CERTIFICATE MODIFICATION / MODIFIKASI SERTIFIKAT

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

Modifikasi / mengubah detail dari Sertifikasi tidak diizinkan. Jika terjadi kesalahan selama penerbitan Sertifikat (contoh: ejaan), sertifikat dicabut dan dilakukan Proses Penerbitan Penggantian Kunci sebagaimana dinyatakan pada bagian 4.3.

4.8.1 Circumstance for Certificate Modification / Kondisi untuk Modifikasi Sertifikat

Modification of certificate information is not permitted.

Modifikasi / mengubah informasi pada sertifikat tidak diizinkan.

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

No stipulation.

Tidak ada ketentuan.

4.8.3 Processing Certificate Modification Requests / Pemrosesan Permintaan Modifikasi Sertifikat

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

4.9 CERTIFICATE REVOCATION AND SUSPENSION /PENCABUTAN DAN PEMBEKUAN SERTIFIKAT

4.9.1 Circumstances for Revocation / Keadaan untuk Pencabutan

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

- *Identifying information or affiliation components of any names in the certificate becomes invalid.*
- *Any information in the certificate becomes invalid.*
- *The subscriber can be shown to have violated the stipulations of its subscriber agreement.*
- *There is reason to believe the private key has been compromised.*
- *The subscriber or other authorized party (as defined in the CPS) asks for its certificate to be revoked.*
- *Peruri CA termination.*
- *The certificate is issued for trial run.*

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid.

When this occurs, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

Peruri CA harus mencabut sertifikat pemilik dalam keadaan berikut:

- Mengidentifikasi informasi atau komponen afiliasi dari setiap nama di dalam Sertifikat menjadi tidak valid.
- Setiap informasi dalam Sertifikat menjadi tidak valid.
- Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya.
- Ada alasan untuk meyakini bahwa Kunci Privat telah bocor.
- Pemilik atau pihak lain yang berwenang (sesuai ketentuan pada CPS) meminta agar sertifikatnya dicabut.
- Peruri CA berhenti beroperasi.
- Sertifikat yang dibuat untuk uji coba.

Sertifikat harus dicabut ketika hubungan antara Subjek dan Kunci Publik milik Subjek yang didefinisikan dalam sertifikat sudah tidak valid lagi.

Bila hal ini terjadi, sertifikat yang terkait harus dicabut dan ditempatkan pada CRL. Sertifikat yang dicabut harus disertakan pada semua publikasi baru pada informasi status sertifikat hingga sertifikat kadaluarsa.

4.9.2 Who can Request Revocation / Siapa yang Dapat Meminta Pencabutan

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

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

4.9.3 Procedure for Revocation Request / Prosedur Permintaan Pencabutan

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

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

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

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

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

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

4.9.4 Revocation Request Grace Period / Masa Tenggang Permintaan Pencabutan

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

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

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

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

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

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

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

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

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

Pihak Pengandal harus memvalidasi setiap sertifikat yang diberikan terhadap server penerbit OCSP yang berkaitan.

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

The CRL must be updated and published:

- *For end-user/device certificates, at least every 24 hours. The CRL will be in effect for a maximum time of thirty (30) working days.*

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

CRL harus diperbarui dan dipublikasi:

- Untuk sertifikat *end-user*/perangkat, paling sedikit setiap satu (1) hari. CRL akan berdampak dalam waktu maksimum tiga puluh (30) hari kerja.

CRL disimpan dan dilindungi untuk menjamin integritas dan keotentikannya.

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

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

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

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

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

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

Peruri CA will provide online validation service. If online validation is available, it is expected to perform revocation checks using the OCSP Server provided.

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP.

In addition to publishing CRLs, Peruri CA provides Certificate status information through query functions in the Root CA Repository.

Peruri CA akan menyediakan layanan validasi secara daring. Tersedianya layanan validasi daring diharapkan Peruri CA dapat melakukan pemeriksaan pencabutan menggunakan server OCSP yang ada.

Pencabutan dan informasi status sertifikat secara daring tersedia melalui repositori berbasis web dan melalui OCSP yang tersedia.

Selain menerbitkan CRL, Peruri CA memberikan informasi status Sertifikat melalui fungsi *query* di repositori PSrE Induk.

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

No stipulation.

Tidak ada ketentuan.

4.9.11 Other Forms of Revocation Advertisements Available / Pentuk Lain Pengumuman Pencabutan

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

4.9.13 Circumstances for Suspension / Kondisi untuk Pembekuan

Certificate suspension is not provided.

Pembekuan Sertifikat tidak disediakan.

4.9.14 Who can Request Suspension / Siapa yang Dapat Meminta Pembekuan

No stipulation.

Tidak ada ketentuan.

4.9.15 Procedure for Suspension Request / Prosedur untuk Permintaan Pembekuan

No stipulation.

Tidak ada ketentuan.

4.9.16 Limits on Suspension Period / Batas Masa Pembekuan

No stipulation.

Tidak ada ketentuan.

4.10 CERTIFICATE STATUS SERVICES / LAYANAN STATUS SERTIFIKAT

4.10.1 Operational Characteristics / Karakteristik Operasional

The status of public certificates is available from CRL's in the repositories.

Status Sertifikat Publik tersedia dari CRL di dalam repositori.

4.10.2 Service Availability / Ketersediaan Layanan

Peruri CA performs all the necessary actions for the uninterruptible - as possible - availability of its certificate status validation service.

Peruri CA melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status sertifikat.

4.10.3 Optional Features / Fitur Opsional

No stipulation.

Tidak ada ketentuan.

4.11 END OF SUBSCRIPTION / AKHIR BERLANGGANAN

No stipulation.

Tidak ada ketentuan.

4.12 ESCROW AND RECOVERY / PEMULIHAN DAN PENITIPAN KUNCI

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

Subscriber's private key can be escrowed to Peruri CA or Subscriber with permission from the Subscriber.

Kunci privat Pemilik dapat dititipkan pada Peruri CA atau disimpan sendiri atas persetujuan Pemilik Kunci.

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

No stipulation.

Tidak ada ketentuan.

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

5.1 PHYSICAL CONTROLS / KENDALI FISIK

5.1.1 Site Location and Construction / Lokasi dan Konstruksi

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

Lokasi dan konstruksi dari fasilitas penempatan peralatan Peruri CA maupun situs tempat *workstation* yang digunakan untuk mengelola Peruri CA, harus konsisten dengan fasilitas yang digunakan untuk menampung informasi yang bernilai tinggi dan sensitif. Lokasi dan konstruksi situs, ketika dikombinasikan dengan mekanisme perlindungan keamanan fisik lainnya seperti penjagaan dan sensor intrusi, harus memberikan perlindungan yang kuat terhadap akses yang tidak sah ke peralatan dan catatan Peruri CA.

5.1.2 Physical Access / Akses Fisik

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

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

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

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

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

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

5.1.3 Power and Air Conditioning / Listrik dan AC

Peruri CA has backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. PKI Repositories has been provided with Uninterrupted Power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to support continuity of operations.

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.

5.1.4 Water Exposures / Keterpaparan Air

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

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

Peralatan Peruri CA harus ditempatkan pada tempat yang tidak terpapar air.

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

5.1.5 Fire Prevention and Protection / Pencegahan dan Perlindungan Kebakaran

The Peruri CA equipment were housed in a facility with appropriate fire suppression and protection systems.

Peralatan Peruri CA ditempatkan di fasilitas dengan sistem deteksi dan pemadaman kebakaran yang memadai.

5.1.6 Media Storage / Media Penyimpanan

Peruri CA's media were stored so as to protect it from accidental damage (water, fire, electromagnetic), theft, and unauthorized access. Media containing audit, archive, or backup information were duplicated and stored in a location separate from the Peruri CA location.

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.

5.1.7 Waste Disposal / Pembuangan Limbah

Sensitive waste material shall be disposed of in a secure fashion.

Limbah material yang sensitif dibuang dengan cara yang aman.

5.1.8 Off-Site Backup / Backup Off-Site

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

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).

5.2 PROCEDURAL CONTROLS / KENDALI PROSEDUR

5.2.1 Trusted Roles / Peran yang Dipercaya

Trusted roles including:

- *Head*
  Overall responsibility for administering the implementation of the Peruri CA's security practices
- *Policy Administrator (Compliance Officer)*
  Establishment or revision of Certificate Policy and Certification Practice Statement
- *Security Officer / Internal Auditor*
  Viewing and maintenance of Peruri CA system archives and audit logs
- *Key Manager*
  Generation and revocation of Peruri CA key pairs
- *CA Administrator (CA)*
  CA System access, Certificate Lifecycle management approval of the generation, revocation and suspension of certificates
- *RA Administrator (RA)*
  RA System accesses and management, LRA management, Approval for identification conducted by Validation Specialist
- *Validation Specialist*
  User Identification and documents verification and WHOIS verification for SSL certificates.
- *Repository (WEB)*
  WEB pages management, publication
- *Developer*
  Development CA/RA/OCSP and other relevant systems
- *Operator*
  Day-to-day operation of Peruri CA systems and system backup and recovery

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

Peran-peran terpercaya meliputi:

- Koordinator
  Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan Peruri CA.
- *Policy Administrator (Compliance Officer)*
  Pembuatan atau revisi *Certificate Poicy* dan *Certification Practice Statement*

- *Security Officer / Internal Auditor.*
  Melihat dan memelihara arsip sistem CA dan log audit Peruri
- *Key Manager*
  Pembuatan dan pencabutan pasangan kunci Peruri CA
- *CA Administrator (CA)*
  Akses sistem CA, persetujuann siklus penerbitan sertifikat, pencabutan dan penangguhan sertifikat
- *RA Administrator (RA)*
  Akses dan manajemen Sistem RA, Persetujuan untuk identifikasi dilakukan oleh *Validation Specialist*
- *Validation Specialist*
  Identifikasi Pengguna dan verifikasi dokumen
- *Repository (WEB)*
  Manajemen halaman WEB, publikasi
- *Developer*
  Pengembangan CA / RA / OCSP dan sistem terkait lainnya
- *Operator*
  Operasi sehari-hari sistem Peruri CA dan pencadangan serta pemulihan sistem

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

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

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 two or more persons:

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

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

- Pembuatan kunci
- Pengaktifan kunci
- Pencadangan kunci

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

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

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

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

Individual Peruri CA personnel are specifically designated to roles defined in section 5.2.1 of this CPS and no individual has been assigned more than one Trusted Role.

Setiap personel Peruri CA disusun secara khusus untuk peran yang telah ditentukan pada Bagian 5.2.1 dan tidak ada personel yang ditugaskan lebih dari satu Peran Terpercaya.

5.3 PERSONNEL CONTROLS / KENDALI PERSONEL

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

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

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

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

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

5.3.2 Background Check Procedures / Prosedur Pemeriksaan Latar Belakang

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

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

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

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

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

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

5.3.3 Training Requirements / Persyaratan Pelatihan

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.

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

Semua personil Peruri CA harus dilatih untuk menjalankan tugasnya. Pelatihan semacam itu membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, prosedur terkait, undang-undang/hukum dan peraturan.

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

5.3.4 Retraining Frequency and Requirements / Frekuensi dan Persyaratan Pelatihan Ulang

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

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

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

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

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

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

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

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

5.3.7 Independent Contractor Requirements / Persyaratan Kontraktor Independen

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

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

5.3.8 Documentation Supplied to Personnel / Dokumentasi yang Diberikan kepada Personil

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

Peruri CA harus menyediakan kepada para personilnya *Certificate Policy* yang mereka gunakan, CPS, dan setiap undang-undang yang relevan, kebijakan, atau kontrak apapun. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) harus disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

5.4 AUDIT LOGGING PROCEDURES / PROSEDUR LOG AUDIT

Audit log files shall be generated for all events relating to the security of the CAs, VAs, and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.5.2.

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

5.4.1 Types of Events Recorded / Jenis Kejadian yang Direkam

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

a. The type of event;
b. The date and time of the event;
c. A success or failure indicator, where appropriate; and
d. The identity of the entity and/or operator that caused the event.

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. Tipe Kejadian;
b. Tanggal dan waktu kejadian;
c. Indikator keberhasilan atau kegagalan jika perlu;
d. Identitas dan entitas dan/atau operator yang menyebabkan kejadian tersebut

5.4.2 Frequency of Processing Log / Frekuensi Pemrosesan Log

Audit logs were reviewed monthly, including verification that the log has not been tampered with, there is no discontinuity or other loss of audit data, and brief inspection all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Actions taken as a result of these reviews were documented.

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

Tindakan yang diambil sebagai hasil dari peninjauan ini harus didokumentasikan.

5.4.3 Retention Period for Audit Log / Periode Retensi Log Audit

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.

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

5.4.4 Protection of Audit Log / Proteksi Log Audit

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.

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

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

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

5.4.5 Audit Log Backup Procedures / Prosedur Backup Log Audit

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.

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

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

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

Sistem pengumpulan log audit adalah internal ke sistem Peruri CA.

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

No stipulation.

Tidak ada ketentuan.

5.4.8 Vulnerability Assessments / Asesmen Kerentanan

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

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

5.5 RECORDS ARCHIVAL / PENGARSIPAN CATATAN

5.5.1 Types of Records Archived / Tipe Catatan yang Diarsipkan

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

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

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

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

- Semua sertifikat dan CRL yang telah diterbitkan
- Log Audit.
- Data konfigurasi sistem IKP.
- Dokumen CP dan semua CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen-dokumen ini.
- Data pendaftaran pelanggan Peruri CA.

5.5.2 Retention Period for Archive / Periode Retensi Arsip

Archived records shall be retained for at least 5 (five) years. Applications necessary to read these archives shall be maintained for the retention period.

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

5.5.3 Protection of Archive / Perlindungan Arsip

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.

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.

5.5.4 Archive Backup Procedures / Prosedur Backup Arsip

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.

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

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

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

Catatan arsip Peruri CA diberikan label waktu secara otomatis.

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

Archive Collection System is internal to Peruri CA only.

Sistem pengumpulan arsip hanya dilakukan oleh internal Peruri CA.

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

Procedures to obtain and verify archive information are as follows:

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

d. The requester verifies the integrity of information.

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

Prosedur untuk menjaga dan memastikan informasi arsip adalah sebagai berikut:

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

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

5.6 KEY CHANGEOVER / PERGANTIAN KUNCI

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

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

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

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

5.7 COMPROMISE AND DISASTER RECOVERY / PEMULIHAN BENCANA DAN KEBOCORAN

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

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

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

Peruri CA memiliki rencana tanggap darurat dan rencana pemulihan bencana.

Apabila dicurigai telah terjadi kebocoran kunci Peruri CA, penerbitan sertifikat oleh Peruri CA dihentikan seketika. Investigasi independen oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup dari kerusakan dinilai untuk menentukan prosedur perbaikan yang tepat. Apabila kunci privat Peruri CA dicurigai mengalami kebocoran, prosedur pada Bagian 5.7.3. diikuti.

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

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

- *Notify PA, Security Officer, Key Manager, PSrE Head and ROOT CA Indonesia as soon as possible.*
- *Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.*
- *Re-establish Peruri CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.*
- *If Peruri CA's signing keys are destroyed, reestablish Peruri CA operations as quickly as possible, giving priority to the generation of a new Peruri CA signing key pair.*

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

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

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

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

If the private key of the Peruri CA is lost, Peruri CA shall notify the PA and relying parties via public announcement. Peruri CA must stop the service, notify all subscribers proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security contacts. Then the Public Key Infrastructure will be set up again with generate new key-pairs.

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

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

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

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

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

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

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

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

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.

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

5.8 CA OR RA TERMINATION / PENUTUPAN CA ATAU RA

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

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

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

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

6. TECHNICAL SECURITY CONTROLS / KENDALI KEAMANAN TEKNIS

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

6.1.1 Key Pair Generation / Pembangkitan Pasangan Kunci

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

Peruri CA CPS Cryptographic keying material used by Peruri CA to sign certificates, CRLs, or status information were generated in cryptographic modules validated to [FIPS 140-2 Security Level 3], or some other equivalent standard. Multi-party control is required for Peruri CA key pair generation, as specified in section 6.2.2.

Peruri CA key pair generation created a verifiable audit trail demonstrating that the security requirements for procedures were followed. Appropriate role separation of the key generation process were documented in the internal document of Peruri CA. An independent third party was validating the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

Material kunci kriptografi yang digunakan oleh Peruri CA untuk menandatangani sertifikat, CRL, atau informasi status dibuat di dalam modul kriptografis yang sesuai standar FIPS 140-2 Security Level 3, atau standar lain yang setara. Kontrol multi-pihak dibutuhkan untuk pembangkitan pasangan kunci Peruri CA, seperti yang ditentukan pada bagian 6.2.2.

Pembangkitan pasangan kunci Peruri CA harus menghasilkan jejak audit yang dapat diverifikasi, yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur diikuti. Pemisahan peran yang tepat atas proses pembuatan kunci didokumentasikan di dalam dokumen internal Peruri CA. Pihak ketiga yang independen harus memvalidasi pelaksanaan prosedur pembangkitan kunci baik dengan menyaksikan pembangkitan kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci.

6.1.1.2 Subscriber Key Pair Generation / Pembangkitan Pasangan Kunci Pemilik

Subscriber key pair generation shall be performed by either the subscriber or Peruri CA.

If Peruri CA generates key pairs for subscriber, the requirements for key pair delivery specified in section 6.1.2 must also be met and Peruri CA shall generate key within a secure FIPS 140-2 Security Level 3 standard.

Pembangkitan pasangan kunci Pemilik harus dilakukan oleh Pemilik atau Peruri CA.

Jika Peruri CA membangkitkan pasangan kunci untuk Pemilik, persyaratan pengiriman pasangan kunci yang dinyatakan dalam bagian 6.1.2 juga harus dipenuhi dan Peruri CA harus membangkitkan kunci dalam suatu perangkat dengan standar FIPS 140-2 Security Level 3.

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

Peruri CA does not deliver private key to subscribers.

When Peruri CA generate keys on behalf of the Subscriber, then the Private Key shall be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a FIPS 140-2 Security Level 3 hardware cryptographic module. In all cases, the following requirements shall be met:

- *Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber.*
- *The Private Key shall be protected from activation, compromise, or modification*

during the delivery process.

- *The Subscriber shall acknowledge receipt of the Private Key(s).*
- *The CA shall maintain a record of the Subscriber acknowledgement of receipt of the private key.*

Peruri CA tidak mengirimkan kunci privat ke pemilik sertifikat.

Bila Peruri CA membangkitkan kunci atas nama Pemilik, maka Kunci Privat harus dikirimkan secara aman kepada Pemilik. Kunci privat dapat dikirim secara elektronik atau dikirimkan pada modul kriptografi dengan spesifikasi FIPS 140-2 Security Level 3. Dalam semua kasus persyaratan berikut harus dipenuhi:

- Siapa pun yang membuat kunci privat penandatanganan untuk Pemilik tidak boleh menyimpan salinan kunci apa pun setelah pengiriman Kunci Privat ke Pemilik.
- Kunci Privat harus dilindungi terhadap aktivasi, kebocoran, atau perubahan selama proses pengiriman.
- Pemilik harus memberikan pernyataan penerimaan Kunci Privat.
- Peruri CA harus menyimpan pernyataan penerimaan Pemilik atas Kunci Privat.

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

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

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

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

Peruri CA provides mechanisms for the secure digital delivery of all certificates containing public key using SSL.

Peruri CA menyediakan mekanisme untuk penyampaian digital yang aman dari semua sertifikat yang memuat kunci publik, melalui repositori sesuai bagian 2.1 yang diamankan menggunakan SSL.

6.1.5 Key Sizes / Ukuran Kunci

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.2.3 Private Key Escrow / Escrow Kunci Privat

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

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

6.2.4 Private Key Backup / Backup Kunci Privat

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

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

6.2.5 Private Key Archival / Pengarsipan Kunci Privat

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

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

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

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

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.

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

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

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

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

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

6.2.8 Method of Activating Private Key / Metode Pengaktifan Kunci Privat

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

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

6.2.9 Method of Deactivating Private Key / Metode Penonaktifan Kunci Privat

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

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

6.2.10 Method of Destroying Private Key / Metode Penghancuran Kunci Privat

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

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

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

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

6.2.11 Cryptographic Module Rating / Pemeringkatan Modul Kriptografis

As described in section 6.2.1.

Seperti diuraikan dalam bagian 6.2.1.

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

6.3.1 Public Key Archival / Pengarsipan Kunci Publik

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

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat.

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

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

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

6.4 DATA ACTIVATION/ AKTIVASI DATA

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

Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder, of whom the shareholder must be in a trusted role.

Aktivasi data harus dibuat secara otomatis oleh HSM yang cocok dan dikirimkan ke *shareholder*, dimana *shareholder* tersebut haruslah orang yang memiliki Peran Terpercaya.

6.4.2 Activation Data Protection / Perlindungan Data Aktivasi

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.

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

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

No stipulation.

Tidak ada ketentuan.

6.5 COMPUTER SECURITY CONTROLS / KONTROL KEAMANAN KOMPUTER

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

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

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

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

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

6.5.2 Computer Security Rating / Peringkat Keamanan Komputer

No stipulation.

Tidak ada ketentuan.

6.6 LIFE CYCLE OF TECHNICAL CONTROLS / KONTROL TEKNIS SIKLUS HIDUP

6.6.1 System Development Controls / Kontol Pengembangan Aplikasi

No stipulation.

Tidak ada ketentuan.

6.6.2 Security Management Controls / Kontrol Manajemen Keamanan

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

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

6.6.3 Life Cycle Security Controls / Kontrol Keamanan Siklus Hidup

Peruri CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

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

6.7 NETWORK SECURITY CONTROL / KONTROL KEAMANAN JARINGAN

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.

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.

6.8 TIME-STAMPING / STEMPEL WAKTU

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

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

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

7.1 CERTIFICATE PROFILE / PROFIL SERTIFIKAT

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

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

7.1.1 Version Number(s) / Nomor Versi

Peruri CA issue X.509 versi 3 certificates.

Peruri CA menerbitkan sertifikat X.509 versi 3.

7.1.2 Certificate Extensions / Ekstensi Sertifikat

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

Peruri CA memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

7.1.2.1 Key Usage / Penggunaan Kunci

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

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

7.1.2.2 Certificate Policies Extension / Perluasan Kebijakan Sertifikat

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

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

7.1.2.3 Basic Constraint / Batasan Dasar

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

The criticality field of this extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

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

7.1.2.4 Extended Key Usage / Penggunaan Kunci Tambahan

By default, extended key usage is set as a non-critical extension.

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

All end-user subscriber certificates shall contain an extended key usage extension for the purpose that the certificate was issued to the end user, and shall not contain the any extended key usage value.

Secara baku, *extended key usage* diatur sebagai suatu ekstensi non-kritikal.

Sertifikat CA dapat memuat ekstensi *extended key usage* sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang mereka terbitkan.

Semua sertifikat Pemilik harus mengandung sebuah ekstensi *extended key usage* untuk tujuan bahwa sertifikat tersebut telah diterbitkan untuk *end-user*, dan tidak boleh memuat nilai *extended key usage* apa pun.

7.1.2.5 CRL Distribution Points / Titik Distribusi CRL

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

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

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

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

7.1.2.6 Authority Key Identifier / Pengidentifikasi Kunci Otoritas

X.509 Version 3 Certificates are generally populated with an Authority Key Identifier extension. The method for generating the key identifier based on the public key of the Peruri CA, issuing the certificate shall be calculated in accordance with one of the methods described in RFC 5280. The criticality field of this extension shall be set to FALSE.

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

7.1.2.7 Subject Key Identifier / Pengidentifikasi Kunci Subyek

If present in X.509 Version 3 Certificates, the criticality field of this extension shall be set to FALSE and the method for generating the key identifier based on the public key of the subject of the certificate shall be calculated in accordance with one of the methods described in RFC 5280.

Bila ada dalam Sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini harus diisi dengan FALSE dan metode untuk menghasilkan *key identifier* yang berbasis pada kunci publik subyek sertifikat harus dihitung sesuai dengan salah satu metode yang diuraikan dalam RFC 5280.

7.1.3 Algorithm Object Identifiers / Pengidentifikasi Objek Algoritma

X.509 Version 3 standard OIDs shall be used. Algorithm RSA encryption for the subject key and SHA256 with RSA encryption for the certificate signature.

Menggunakan standar OID X.509 v3. Algoritma berupa enkripsi RSA untuk *subject key* dan SHA256 dengan enkripsi RSA untuk tanda tangan sertifikat.

7.1.4 Name Forms / Format Nama

As per the naming conventions and constraints listed in section 3.1.

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1.

7.1.5 Name Constraints / Batasan Nama

As per the naming conventions and constraints listed in section 3.1

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1.

7.1.6 Certificate Policy Object Identifier / Pengidentifikasi Objek Kebijakan Sertifikat

Certificates issued under this CPS use OID number 2.16.360.1.1.1.12.3 *that points to the correct Root CA.*

Sertifikat yang diterbitkan di bawah CPS ini menggunakan nomor OID 2.16.360.1.1.1.12.3 yang mengacu pada PSrE Induk.

7.1.7 Usage of Policy Constraints Extension / Penggunaan Ekstensi Batasan Kebijakan

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

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

No stipulation.

Tidak ada ketentuan.

7.2 CRL PROFILE / PROFIL CRL

7.2.1 Verion Number(s) / Nomor Versi

Peruri CA shall issue X.509 and CRL entry extension.

Peruri CA menerbitkan X.509 dan ekstensi entri CRL.

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

Peruri CA shall use RFC 5280 CRL and CRL entry extension.

Peruri CA menggunakan CRL dan CRL entri extension RFC 5280.

7.3 OCSP Profile / Profil OCSP OCSP PROFILE / PROFIL OCSP

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

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

7.3.1 Version Number(s) / Nomor Versi

Peruri CA issue OCSP responses Version 1.

Peruri CA menerbitkan respon OCSP versi 1.

7.3.2 OCSP Extensions / Ekstensi OCSP

No stipulation.

Tidak ada ketentuan.

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

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT / FREKUENSI ATAU KEADAAN ASESMEN

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

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR / IDENTITAS / KUALIFIKASI ASESOR

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

Compliance auditors must possess these qualifications:

a. *Auditors shall have a qualified, independent assessment team*
b. *Auditors shall have a sufficient knowledge on digital signatures, digital certificate, X.509 PKI, Certificate Policy and Certificate Practice Framework, Indonesian Law of Electronic Information and Transactions (UU No 11 2008 and UU No 19 2016), Indonesian Government Regulation on Electronic System and Transaction Operations (PP 82 2012), and Indonesia Ministry of Communication and Informatics Regulation on Certification Authority Operations (PM Kominfo 11 2018)*
c. *Auditors shall have an adequate skills on information security audit, information security device and technique audit, as well as familiarity with PKI technology*
d. *Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme*

e. *Auditors shall master a set of certain skills, competency testing, and quality assurance such as peer review, standards regarding accurate staff assigning, and involvement and requirements for higher professional education*

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

Auditor kepatuhan harus memiliki kualifikasi sebagai berikut:

a. Auditor harus dilaksanakan oleh tim asesmen independen yang *qualified* .
b. Auditor harus memiliki pengetahuan yang cukup tentang tanda tangan digital, sertifikat digital, X.509 versi 3 PKI, *Certificate Policy and Certification Practices Framework*, UU ITE, PP PSTE, Peraturan Menteri Komunikasi dan Informatika no 11/2018.
c. Memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
d. Auditor harus memiliki bukti bahwa dirinya memenuhi kualifikasi auditor untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah
e. Menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.

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

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.

Untuk memberikan evaluasi yang tidak memihak dan independen, auditor dan pihak yang diaudit tidak boleh memiliki hubungan keuangan, hukum, atau hubungan lainnya saat ini atau yang direncanakan yang dapat mengakibatkan konflik kepentingan.

8.4 TOPICS COVERED BY ASSESSMENT / TOPIK YANG DICAKUP OLEH ASESMEN

The scope of the assessment includes:

- *Key management operations*
- *Environmental controls*
- *Certificate lifecycle management*
- *Business practices disclosure*
- *Infrastructure / administrative controls.*

Ruang lingkup asesmen terdiri dari:

- Operasional manajemen kunci
- Pengendalian lingkungan
- Manajemen siklus hidup sertifikat
- Pemaparan praktek bisnis
- Pengendalian infrastruktur / administrasi

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

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

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

8.6 COMMUNICATION OF RESULTS / KOMUNIKASI HASIL

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

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES / BIAYA

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

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

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

9.1.2 Certificate Access Fees / Biaya Pengaksesan Sertifikat

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

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

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

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

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

9.1.4 Fees for Other Services / Biaya Layanan Lainnya

Peruri CA may charge fees for other additional services.

Peruri CA dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya.

9.1.5 Refund Policy / Kebijakan Pengembalian Biaya

No Refund Policy.

Tidak ada Kebijakan Pengembalian Biaya.

9.2 FINANCIAL RESPONSIBILITY / TANGGUNG JAWAB KEUANGAN

9.2.1 Insurance Coverage / Cakupan Asuransi

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

Peruri CA mematuhi persyaratan PM Kominfo Nomor 11 Tahun 2018 Pasal 12 huruf h.

9.2.2 Other Assets / Aset Lainnya

No stipulation.

Tidak ada ketentuan.

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

Peruri CA offer an insurance or warranty policy to Subscribers.

Peruri CA menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik sertifikat.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION / KERAHASIAAN INFORMASI BISNIS

Peruri CA protect the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. Public access to Peruri CA organizational information determined by Peruri CA.

Peruri CA melindungi kerahasiaan informasi bisnis sensitif yang dapat mengarah pada penyalahgunaan atau penipuan. Misalnya, CA melindungi data pelanggan yang dapat memungkinkan penyerang berkedok sebagai pelanggan. Akses publik ke Peruri CA ditentukan oleh informasi organisasi Peruri CA.

9.3.1 Scope of Confidential Information / Cakupan Informasi Rahasia

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

- *Personal Information as detailed in Section 9.4;*
- *Audit logs from CA and RA systems;*
- *Activation data used to active CA Private Keys as detailed in Section 6.4;*
- *CAs business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and*
- *Audit Reports from an independent auditor as detailed in Section 8.0.*

Peruri CA memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Yang termasuk dalam kategori informasi rahasia antara lain:

- Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
- Rekam jejak audit (*audit logs*) dari sistem PSrE dan RA;
- Data aktivasi pada saat pengaktifan Kunci Privat PSrE sebagaimana dijabarkan pada Bagian 6.4;
- Dokumentasi bisnis proses PSrE termasuk dokumen *Disaster Recovery Plans (DRP) dan Business Continuity Plans (BCP)*; dan
- Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0.

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

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

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

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

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

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

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

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

9.4 PRIVACY OF PERSONAL INFORMATION / PRIVASI INFORMASI PRIBADI

9.4.1 Privacy Plan / Rencana Privasi

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

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

9.4.2 Information Treated as Private / Informasi yang Dianggap Pribadi

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

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

9.4.3 Information not Deemed Private / Informasi tidak Dianggap Pribadi

Information in the certificate and CRL is not deemed private.

Informasi yang ada pada sertifikat dan CRL tidak dianggap pribadi.

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

Peruri CA has implemented security measure to protect private information.

Peruri CA telah menerapkan tindakan keamanan untuk melindungi informasi pribadi.

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

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

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

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

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

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

9.4.7 Other Information Disclosure Circumstances / Keadaan Pengungkapan Informasi Lain

No stipulation.

Tidak ada ketentuan.

9.5 INTELLECTUAL PROPERTY RIGHTS / HAK ATAS KEKAYAAN INTELEKTUAL

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

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.

9.6 REPRESENTATIONS AND WARRANTIES / PERTANYAAN DAN JAMINAN

9.6.1 CA Representations and Warranties / Pernyataan Dan Jaminan CA

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

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

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

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

9.6.2 RA Representations and Warranties / Pernyataan dan Jaminan RA

No stipulation.

Tidak ditentukan.

9.6.3 Subscriber Representations and Warranties / Pernyataan dan Jaminan Pemilik Sertifikat

Subscribers warrant that:

1. *Each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,*
2. *Their private key is protected and that no unauthorized person has ever had access to the subscriber's private key,*
3. *Have thoroughly reviewed the certificate information*
4. *All information supplied by the subscriber and contained in the certificate is true,*
5. *The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CPS, and*
6. *Promptly:*
    a. *Request revocation of the certificate, and cease using it and its associated private key, if there is any actual or suspected misuse or compromise of the subscriber's private key associated with the public key included in the Certificate;*
    b. *Request revocation of the certificate, and cease using it, if any information in the certificate is or becomes incorrect or inaccurate;*
    c. *Stop using the private key whose public key is listed in a digital certificate after the certificate is revoked;*
7. *Acknowledges and accepts that Peruri CA is entitled to revoke the certificate immediately if the subscriber violates the terms of the subscriber agreement or terms of use or if Peruri CA discovers that the certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, and*
8. *The subscriber is an end-user subscriber and not a Peruri CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise.*

Pemilik Sertifikat menjamin bahwa:

1. Setiap sertifikat digital yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada sertifikat adalah merupakan tanda tangan digital pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan digital dibuat;
2. Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;
3. Sudah melakukan review terhadap informasi dari sertifikat;
4. Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;
5. Sertifikat digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
6. Segera:
    a. Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam sertifikat; dan
    b. Mengajukan permohonan untuk melakukan pencabutan sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam sertifikat tersebut
    c. Menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut;
7. Menyetujui dan menerima bahwa Peruri CA diberikan kewenangan untuk segera melakukan pencabutan sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang

tercantum dalam kontrak perjanjian atau jika Peruri CA menemukan bahwa sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian *malware*;

8. Pengguna dan bukan merupakan Peruri CA, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam sertifikat digital untuk tujuan penandatangan sertifikat digital PSrE lain.

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

Peruri CA's Certificate relying party guarantee that:

1. *Have the technical capability to use certificates,*
2. *If the representative from the relying party use a certificate issued by Peruri CA, relying party should verify the information contained in the certificate before use and carry all the consequences that happened if the relying party fail to applied it.*
3. *Notify the appropriate RA immediately, if the relying party becomes aware of or suspects that a private key has been compromised,*
4. *Required relying party to acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the certificate, that they are fully responsible for deciding to rely on the information or not, and they will carry the legal consequences from the failure to fulfill the obligation of the relying party as mentioned in the CPS,*
5. *Must compliance with the provisions of this CPS and related agreements*

Pihak yang mengandalkan Sertifikat Peruri CA menjamin bahwa:

1. Memiliki kemampuan teknis untuk menggunakan sertifikat,
2. Apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh Peruri CA, pihak pengandal harus secara benar memverifikasi informasi yang tercantum di dalam sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut,
3. Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi kebocoran/penyalahgunaan pada kunci privat,
4. Mewajibkan pihak pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban pihak pengandal yang ada pada CPS ini,
5. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

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

No stipulation.

Tidak ada ketentuan.

9.7 DISCLAIMERS OF WARRANTIES / PELEPASAN JAMINAN

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

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

conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.

2. *Misuse of a certificate that is inconsistent with its usage as shown in section 4.5 (Key Pair and Certificate Usage),*
3. *The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.*

Peruri CA menyatakan dalam CPS bahwasanya tidak menjamin:

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

9.8 LIMITATIONS OF LIABILITY / PEMBATASAN TANGGUNG JAWAB

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

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

1. *All damage caused by the misuse of certificates or key pairs beside the proper use that have been defined in CPS, subscriber's agreement, or all provision which have been mentioned in the certificate,*
2. *All damage caused by the force majeure condition,*
3. *All damage caused by the malware (i.e virus or trojan) outside Peruri CA devices.*
4. *All incorrect certificate information that comes from subscriber after data verification period is complete.*

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

1. Semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
2. Semua kerusakan yang disebabkan oleh *force majeure*,
3. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau *trojans*) diluar perangkat Peruri CA.
4. Semua kesalahan data informasi sertifikat yang berasal dari pemilik sertifikat setelah periode verifikasi data selesai.

9.8.2 RA Limitation of Liability / Pembatasan Tanggung Jawab RA

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

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

9.9 INDEMNITIES / GANTI RUGI

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

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

9.10 TERM AND TERMINATION / SYARAT DAN PENGAKHIRAN

9.10.1 Term / Syarat

This CPS becomes effective upon publication in the repository.

CPS ini berlaku efektif setelah dipublikasikan di repositori.

9.10.2 Termination / Pengakhiran

This CPS shall remain in force until it is amended or replaced by a new version.

CPS ini akan tetap berlaku sampai dilakukan perubahan atau pergantian dengan versi yang baru.

9.10.3 Effect of Termination and Survival / Efek Pengakhiran dan Keberlangsungan

Upon termination of this CPS, Issuing CA are bound by its terms for all certificates issued for the remainder of the validity periods of such certificates. The following sections of this CPS shall survive any termination or expiration of this CPS: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

Setelah pengakhiran CPS ini, Peruri CA terikat oleh ketentuan-ketentuannya untuk semua sertifikat yang dikeluarkan selama sisa masa berlaku sertifikat tersebut. Bagian berikut dari CPS ini akan bertahan dari pengakhiran atau pemberhentian CPS ini: 2.1, 2.2, 5.4, 5.5, 6.2-6.4, 6.8, 9.2-9.4, 9.7-9.10, 9.13-9.16.

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

Peruri CA will communicate to those participants using reliable channel as soon as possible in accordance with the importance of information.

Peruri CA akan berkomunikasi dengan para partisipan menggunakan saluran yang handal secepat mungkin sesuai dengan pentingnya informasi.

9.12 AMANDEMENTS / AMANDEMEN

9.12.1 Procedure for Amendment / Prosedur untuk Amandemen

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

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

9.12.2 Notification Mechanism and Period / Periode dan Mekanisme Pemberitahuan

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

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

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

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

Jika PA memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, Peruri CA akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

9.13 DISPUTE RESOLUTION PROVISIONS / PROVISI PENYELESAIAN KETIDAKSEPAHAMAN

The decisions of Peruri CA pertaining to matters within the scope of this CPS are final. Any claims should be submitted to Peruri CA. In the event of undefined, Policy Authority has jurisdiction over the dispute.

Keputusan Peruri CA yang berkaitan dengan hal-hal dalam lingkup CPS ini bersifat final. Setiap klaim harus diajukan ke Peruri CA. Dalam hal yang tidak terdefinisi, Otoritas Kebijakan memiliki kekuasaan hukum atas perselisihan tersebut.

9.14 GOVERNING LAW / HUKUM YANG MENGATUR

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

CPS ini menerapkan aturan hukum di Republik Indonesia.

9.15 COMPLIANCE WITH APPLICABLE LAW / KEPATUHAN ATAS HUKUM YANG BERLAKU

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

Peruri CA diharuskan untuk mematuhi hukum Republik Indonesia.

9.16 MISCELLANEOUS PROVISIONS / KETENTUAN YANG BELUM DIATUR

9.16.1 Entire Agreement / Seluruh Perjanjian

No stipulation.

Tidak ada ketentuan.

9.16.2 Assignment / Pengalihan

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

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

9.16.3 Severability / Keterpisahan

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

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

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

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

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

9.16.5 Force Majeure / Keadaan Memaksa

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

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

9.17 OTHER PROVISIONS / PROVISI LAIN

No stipulation.

Tidak ada ketentuan.