Peruri CA

Certification Practice Statement

Nomor/*Number*	01/003/CA/2018
Mulai Berlaku/*Start From*	23 November 2018
Versi/*Version*	5.1
Tanggal Perubahan/*Revision Date*	4 September 2025
OID/*OID*	2.16.360.1.1.1.3.12.3.2
Klasifikasi/*Classification*	Biasa

Menyetujui/ *Approve*

Edwin Purwandesi
Policy Authority Peruri CA

Policy Authority PSrE Induk

Catatan Revisi/*Revision Note*

No./ *No.*	Tanggal/ *Date*	Versi/ *Version*	Deskripsi/ *Description*	Oleh/ *By*
1	23 November 2018	1.0	Initial Release	Peruri CA
2	14 December 2018	1.1	**Minor Update:** • Revise statement in section 1.4 • Revise statement in section 9.16.5 • Cosmetics change	Peruri CA
3	16 January 2019	1.2	**Minor Update:** • Revise statement in section1.4.1 • Add section 5.6.1 • Cosmetics change	Peruri CA
4	13 February 2019	1.3	**Minor Update** • Indonesia Root CA Alignment • Bilingual Bahasa Indonesia	Peruri CA
5	6 May 2019	2.0	**Major Update** • Footer • Writing format • CRL interval • Limitation of Peruri CA responsibility • Sections 4.12.1, 4.9.7, 6.1.2, 6.2.1, 6.2.5, and 9.8.1	Peruri CA
6	10 July 2019	2.0	**Minor Update** • CRL Interval (Section 4.9.7)	Peruri CA
7	6 March 2020	2.2	**Minor Update** • Archive retention period • Authentication of individual identity	Peruri CA
8	10 October 2020	2.3	**Minor Update** • Alignment Webtrust for CA	Peruri CA
9	21 January 2021	3.0	**Major Update** • Change of document number from 002/KRC/KBJ/CPS/XII/2018 to 01/005/CA/2018 • Improvements for Ministry of Communications and Informatics (MCIT) Audit Findings	Peruri CA

No./ *No.*	Tanggal/ *Date*	Versi/ *Version*	Deskripsi/ *Description*	Oleh/ *By*
10	17 September 2021	4.0	**Major Update** • Improvements for Ministry of Communications and Informatics (MCIT) Audit Findings • Change of document number 003/KRC/KBJ/CPS/XII/2018 to 01/003/CA/2018	Peruri CA
11	30 June 2022	4.1	**Minor Update** • Improvements for Ministry of Communications and Informatics (MCIT) Audit Findings • Additional requirements for foreign citizens	Peruri CA
12	24 January 2024	5.0	**Major Update** • Changes Aligmnment with Root CA's CP v3.3 • Changes to Authentication of Individual Identity • Changes to Who Can Submit an Electronic Certificate Application • Changes to Subscriber Private Key and Electronic Certificate Usage • Changes to Revocation Checking Requirement for Relying Parties • Changes to Trusted Roles.	Peruri CA
13	4 September 2025	5.1	**Minor Update** • Improvements for Ministry of Communications and Digital Audit Findings	Peruri CA

Daftar Isi/*Table of Contents*

SECTION 1

Pendahuluan/*Introduction*

Perum Percetakan Uang Republik Indonesia ("Peruri") adalah Badan Usaha Milik Negara (BUMN) yang didirikan melalui Peraturan Pemerintah (PP) Nomor 60 Tahun 1971. Di dalam perjalanannya, pemerintah telah beberapa kali mengubah PP yang mengatur tentang Peruri hingga perubahan yang terakhir yaitu PP Nomor 6 Tahun 2019. Di dalam PP Nomor 6 Tahun 2019 disebutkan bahwa kegiatan usaha Peruri mencakup: mencetak mata Uang Rupiah guna memenuhi kebutuhan sesuai permintaan Bank Indonesia, pembuatan dokumen sekuriti untuk negara dan dokumen sekuriti lainnya, menyediakan jasa yang mempunyai fitur sekuriti, serta jasa digital sekuriti.

Perum Percetakan Uang Republik Indonesia ("Peruri") is a State-Owned Enterprise (BUMN) established through Government Regulation (GR) Number 60 of 1971. Throughout its journey, the government has made several amendments to the GR that governs Peruri, with the most recent change being GR Number 6 of 2019. Under GR Number 6 of 2019, Peruri's business activities include: printing Indonesian Rupiah currency to meet the demand of Bank Indonesia, producing security documents for the state and other security documents, providing services with security features, and digital security services.

Sejalan dengan tugas Peruri untuk dapat menyediakan jasa digital sekuriti, Peruri telah mendapatkan Surat Keputusan (SK) Pengakuan Berinduk Nomor 340 Tahun 2022 sebagai Penyelenggara

In line with Peruri's task of providing digital security services, Peruri has obtained recognition as Subordinated CA with Decree Number 340 of 2022. As regulated in Ministerial Regulation (PM) of

Sertifikasi Elektronik - Berinduk. Sebagaimana diatur dalam Peraturan Menteri (PM) Kominfo No 11 tahun 2022, Peruri merupakan Penyelenggara Sertifikasi Elektronik (PSrE) non instansi yang disebut dengan Peruri CA.

Communication and Information No. 11 of 2022, Peruri is a non-institutional Certificate Authority (CA) called Peruri CA.

Dokumen ini ditujukan kepada:

This document is addressed to:

1. Peruri CA agar beroperasi sesuai dengan *Certification Practice Statement* (CPS) di mana CPS tersebut mengacu pada persyaratan yang diatur di dalam *Certificate Policy* (CP) PSrE Induk;

1. *Peruri CA who have to operate in terms of their own Certification Practice Statement (CPS) that complies with the requirements stated by Root CA Certificate Policy (CP);*

2. Pemilik perlu memahami bagaimana mereka diautentikasi dan apa kewajiban mereka sebagai pemegang Sertifikat Elektronik yang diterbitkan oleh Peruri CA dan bagaimana mereka dilindungi oleh Peruri CA.

2. *Subscribers who need to understand how they are authenticated and what their obligations are as Electronic Certificate holders issued by Peruri CA and how they are protected by Peruri CA.*

3. Pengandal yang perlu memahami seberapa besar tingkat kepercayaan terhadap Sertifikat Elektronik Pemilik atau Tanda Tangan Elektronik tersertifikasi dan layanan yang memanfaatkan Sertifikat Elektronik lain yang menjadi bagian dari rantai kepercayaan (*trust chain*) Sertifikat Elektronik PSrE Induk.

3. *Relying Parties who need to understand how much trust to place in Root CA Indonesia Electronic Certificate or Digital Signature and other services using Electronic Certificates which constitute a part of Root CA's trust chain.*

1.1 Ringkasan/*Overview*

Infrastruktur Kunci Publik (IKP) Peruri CA adalah hierarki IKP dengan rantai kepercayaan yang dimulai dari Penyelenggara Sertifikasi Elektronik (PSrE) Induk Indonesia. Kementerian Komunikasi dan Digital Republik Indonesia (Kemenkomdigi) mengoperasikan PSrE Induk Indonesia. Peruri CA merupakan PSrE non-Instansi di bawah PSrE Induk Indonesia. CPS ini mengacu kepada CP PSrE Induk Indonesia.

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

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

This CPS defines the procedural and operational requirements that Peruri CA adheres to when issuing and managing electronically signed objects within Peruri CA's PKI. This CPS also complies with the current version of Indonesia Root CA policies.

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

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

1.2 Identifikasi dan Nama dokumen/*Document Name and Identification*

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

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

OID	Objek/*Object*
Peruri CA	2.16.360.1.1.1.3.12.3
CPS	2.16.360.1.1.1.3.12.3.2
Individu WNI non-Instansi Online Verifikasi Level 2	2.16.360.1.1.1.5.1.2.2
Individu WNA Online Verifikasi Level 2	2.16.360.1.1.1.5.2.2.2
Segel Elektronik Badan Usaha	2.16.360.1.1.1.8.1

1.3 Partisipan IKP/*PKI Participants*

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

1.3.1.1 PSrE Induk Indonesia/*Indonesia Root CA*

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia yang dioperasikan oleh Kementerian Komunikasi dan Digital Republik Indonesia (Kemenkomdigi).

Indonesia Root CA is the root CA of Indonesia PKI which is operated by the Ministry of Communications and Digital Affairs of the Republic of Indonesia.

PSrE Induk Indonesia bertanggung jawab ter-

Indonesia Root CA is responsible for all aspects of

hadap penerbitan dan pengelolaan Sertifikat Elektronik PSrE Berinduk, sebagaimana dirinci dalam CP PSrE Induk Indonesia.

the issuance and management of those Subordinate CA Electronic Certificates, as detailed in Indonesia Root CA's CP.

1.3.1.2 PSrE Berinduk/*Subordinate CA*

Peruri CA merupakan PSrE Berinduk Non-Instansi yang menerbitkan Sertifikat Elektronik, Tanda Tangan Elektronik, dan Segel Elektronik kepada orang, badan usaha atau badan hukum selain instansi.

Peruri CA is a Subordinate Non-Government CA that issues Electronic Certificate, Digital Signature, and Electronic Seal to a person, business entity or legal entity other than a non-government entity.

Peruri CA tidak menjadi induk dari PSrE lainnya dan tidak berinduk kepada PSrE lain.

Peruri CA will not have further subordinate CA and not become others subordinate CA.

Peruri CA bertanggung jawab terhadap semua aspek penerbitan dan pengelolaan Sertifikat Elektronik, sebagaimana dirinci dalam CPS ini, termasuk namun tidak terbatas pada:

Peruri CA is responsible for all aspects of the issuance and management of those Electronic Certificates, as detailed in this CPS, including but not limited to:

1. Pengendalian terhadap proses pendaftaran Pemohon;
2. Proses identifikasi dan autentikasi;
3. Proses penerbitan Sertifikat Elektronik;
4. Proses penerbitan Daftar Pencabutan Sertifikat *(Certificate Revocation List*/CRL);
5. Publikasi Sertifikat Elektronik dan CRL;
6. Validasi Sertifikat Elektronik;
7. Pencabutan Sertifikat Elektronik;
8. Membangun dan memelihara sistem Peruri CA; dan
9. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan Sertifikat Elektronik Peruri CA yang diterbitkan sesuai dengan CPS ini dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

1. *Control over the registration process;*
2. *Identification and authentication process;*
3. *Process of Electronic Certificate issuance;*
4. *The Certificate Revocation List (CRL) issuance process;*
5. *Publication of Electronic Certificates and CRL;*
6. *Validation of Electronic Certificates;*
7. *Revocation of Electronic Certificates;*
8. *Establishing and maintaining Peruri CA system; and*
9. *Ensuring that all aspects of the services, operations and infrastructure related to Peruri CA Electronic Certificates issued under this CPS were performed in accordance with the requirements, representations, and warranties of this CPS.*

Peruri CA memiliki kewajiban untuk membuat laporan kerja dan menyampaikannya kepada Kementerian Komunikasi dan Digital Republik Indonesia (Kemenkomdigi).

Peruri CA has the obligation to make a work report and submit it to the Ministry of Communication and Digital Affairs of the Republic of Indonesia.

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

Peruri CA dapat menunjuk Otoritas Pendaftaran (RA) tertentu untuk melakukan identifikasi dan autentikasi Pemohon dan Pemilik, serta permohonan dan pencabutan Sertifikat Elektronik sesuai dengan yang telah didefinisikan pada CPS dan dokumen terkait. Peruri CA memiliki RA sendiri di internal, dan tidak melakukan proses verifikasi melalui mitra bisnis.

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

RA berkewajiban untuk melaksanakan fungsi tertentu atas nama Peruri CA, meliputi hal-hal sebagai berikut:

The RA is obliged to perform certain functions on behalf of Peruri CA, including the following:

1. Menyusun dan melaksanakan prosedur pendaftaran untuk Pemohon Sertifikat Elektronik;
2. Melakukan identifikasi dan autentikasi Pemohon Sertifikat Elektronik;
3. Memulai atau meneruskan proses permohonan pencabutan Sertifikat Elektronik; dan
4. Menyetujui permohonan untuk memperbarui Sertifikat Elektronik atau penggantian kunci atas nama Peruri CA.

1. *Establish and execute enrollment procedures for end-user Electronic Certificate Applicants;*
2. *Perform identification and authentication of Electronic Certificate Applicants;*
3. *Initiate or pass along revocation requests for Electronic Certificates; and*
4. *Approve applications for Electronic Certificates renewal or re-keying on behalf of Peruri CA.*

1.3.3 Pemilik/*Subscribers*

Pemilik adalah orang, badan usaha, atau badan hukum yang memohon dan berhasil mendapatkan Sertifikat Elektronik yang ditandatangani oleh Peruri CA. Pemilik berarti subjek pemegang Sertifikat Elektronik sekaligus entitas yang terikat dengan Peruri CA. Sebelum dilakukan verifikasi

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

identitas dan diterbitkannya Sertifikat Elektronik, Pemilik disebut sebagai Pemohon.

Pemohon terdiri atas 2 (dua) yaitu:

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

suance of an Electronic Certificate, a Subscriber is an Applicant.

There are 2 (two) Applicants namely:

1. *Individual Applicants consist of Indonesian Citizens (WNI) or Foreign Citizens (WNA);*
2. *Business entity Applicants consist of organizations or non-governmental entities.*

1.3.4 Pengandal/*Relying Parties*

Pengandal adalah pihak yang bertindak mengandalkan (mempercayai) informasi yang ada dalam Sertifikat Elektronik dan/atau Tanda Tangan Elektronik tersertifikasi dan/atau layanan yang memanfaatkan Sertifikat Elektronik lainnya yang diterbitkan oleh Peruri CA.

Relying Parties are parties that rely on the information contained in the Electronic Certificates and/or any Certified Electronic Signatures and/or other services using Electronic Certificates issued by Peruri CA.

Pengandal harus terlebih dahulu memeriksa respon *Certificate Revocation Lists* (CRL) dan/atau *Online Certificate Status Protocol* (OCSP) yang sesuai sebelum memanfaatkan informasi yang ada dalam Sertifikat Elektronik.

Relying Parties must check the appropriate Certificate Revocation Lists (CRL) and/or Online Certificate Status Protocol (OCSP) response prior to relying on information featured in an Electronic Certificate.

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

The Relying Party relies on the validity of the binding of the Subscriber's name to the Public Key. The Relying Party is responsible for checking the status of the information in the Electronic Certificate.

Pengandal menggunakan informasi dalam Sertifikat Elektronik untuk:

1. Memeriksa tujuan penggunaan Sertifikat Elektronik;
2. Melakukan verifikasi Tanda Tangan Elektronik dan layanan lain yang memanfaatkan Sertifikat Elektronik;
3. Memeriksa status pencabutan Sertifikat Electronic (*revocation*) menggunakan CRL

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

1. *Check the usage purpose of the Electronic Certificate;*
2. *Perform digital signature verification and other services using Electronic Certificates;*
3. *Checks whether an Electronic Certificate is included in the CRL; and*

dan/atau OCSP; dan

4. Penyetujuan batas tanggung jawab dan jaminan.

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

4. *Approval of limits of liability and guarantees.*

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

1.3.5 Partisipan Lain/*Other Participants*

Partisipan Lain adalah Penyelenggara Sistem Elektronik yang bekerja sama dengan Peruri CA dalam penyelenggaraan sebagian infrastruktur atau layanan terkait Penyelenggaraan Sertifikasi Elektronik, yaitu penyedia layanan pusat data adalah pihak ketiga yang menyediakan layanan pusat data untuk operasional Peruri CA.

Other Participant is any Electronic System Operator that participates with Peruri CA in provision of some of the infrastructures or services related to CA operation, namely data center service is a third party who provide data center services for Peruri CA operations.

1.4 Kegunaan Sertifikat Elektronik/*Certificate Usage*

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

Penggunaan Sertifikat Elektronik Pemilik dibatasi sesuai key usage dan extended key usage pada certificate extension. Sertifikat Elektronik Peruri CA dapat digunakan untuk menerbitkan Sertifikat Elektronik untuk transaksi yang memerlukan:

1. Autentikasi;
2. Tanda Tangan Elektronik & nir-sangkal.

Pemilik dapat memilih kelas Sertifikat Elektronik yang sesuai sebagai identitas yang akan mereka tunjukkan kepada Pengandal. Peruri CA memberikan layanan Sertifikat Elektronik dengan pembedaan kelas sebagai berikut:

1. Kelas 2: Sertifikat Elektronik dengan jaminan menengah bagi individu WNI non-Instansi secara online dan individu WNA secara online. Verifikasi identitas level 2 dit-

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

1. *Authentication;*
2. *Digital Signature & non-repudiation.*

Subscribers can choose the appropriate class of Electronic Certificate as the identity they will present to the Relying Party. Peruri CA provides Electronic Certificate services with class distinctions as follows:

1. *Class 2: Electronic Certificate with medium warranty for Indonesian Citizens who are non-government online and Foreign Citizen online. Level 2 identity verification is imple-*

erapkan dengan dengan cara memastikan *liveness detection* dari Pemohon, membandingkan data kartu identitas, dan data biometrik terhadap data identitas yang dimiliki oleh pemerintah.

2. Kelas 3: Sertifikat Elektronik dengan jaminan tinggi bagi badan usaha secara online. Verifikasi identitas level 3 diterapkan dengan membandingkan data badan usaha terhadap basis data Instansi yang berwenang memberikan pengesahan Badan Usaha sesuai dengan ketentuan peraturan perundang-undangan atau dengan meminta surat/dokumen penunjukan Perwakilan Badan Usaha yang dibandingkan terhadap situs resmi Badan Usaha.

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

mented by ensuring the liveness detection of the Applicant, comparing identity card data, and biometric data to identity data owned by the government.

2. *Class 4: high assurance Electronic Certificates for business entities online. Level 3 identity verification is implemented by comparing the business entity's data against the agency database authorized to authorize business entities in accordance with statutory provisions or by requesting a letter/document for appointing a Business Entity Representative compared to the official website of the Business Entity.*

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

Kelas Sertifikat Elektronik / *Electronic Certificate Class*	**Pengguna / *Users***	**Tingkat Jaminan / *Assurance Level***		**Penggunaan/ *Usage***		
		Jaminan Sedang/ *Medium Assurance*	**Jaminan Tinggi / *High Assurance***	**Tanda Tangan Elektronik/ *Digital Signature***	**Segel-Elektronik/ *Electronic Seal***	**Autentikasi/ *Authentication***
Kelas 2 / *Class 2*	**WNI tidak berafiliasi dengan badan usaha level 2 *online* / *Indonesian citizens not affiliated with business entities level 2 online***	✓		✓		✓
	WNI berafiliasi dengan badan usaha level 2 *online* / *Indonesian citizens affiliated with business entities level 2 online*	✓		✓		✓
	WNA berafiliasi dengan badan usaha level 2 *online* / *Foreign citizens affiliated with business entities level 2 online*	✓		✓		✓
Kelas 3 / *Class 3*	**Badan Usaha *Business Entities***		✓		✓	✓

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

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

Electronic Certificates issued by Peruri CA are prohibited under any use not specified in section 1.4.1

Pegawai Instansi atau Instansi dilarang menggunakan Sertifikat Elektronik yang diterbitkan oleh Peruri CA dalam rangka pelaksanaan tugas dan/atau kewenangannya. Dalam hal pegawai Instansi membutuhkan Sertifikat Elektronik bukan dalam rangka pelaksanaan tugas dan/atau kewenangannya, dapat menggunakan Sertifikat Elektronik yang diterbitkan Peruri CA.

Employees of Government Institution or Government Institutions are prohibited from using Electronic Certificates issued by Peruri CA in the context of carrying out their duties and/or authorities. In the event that an Employees of Government Institution requires an Electronic Certificate not in the context of carrying out their duties and/or authorities, they may use an Electronic Certificate issued by Peruri CA.

1.5 Administrasi Kebijakan/*Policy Administration*

Policy Authority (PA) adalah entitas yang ada di dalam Peruri CA. PA memiliki peran dan tanggung jawab sebagai berikut:

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

1. Menetapkan *Certification Practice Statement* (CPS);
2. Memastikan semua layanan, operasional, dan infrastruktur Peruri CA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk; dan
3. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang setara.

1. *Approves the Certificate Practice Statements (CPS);*
2. *Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are well performed in accordance with the requirements, representations, and warranties of the Root CA's CP; and*
3. *Approves the establishment of trust relationships with external PKIs that have equivalent verification level.*

1.5.1 Organisasi Pengaturan Dokumen/*Organization Administering the Document*

CPS ini dan dokumen referensinya dikelola oleh PA Peruri CA.

This CPS and the documents referenced herein are maintained by Peruri CA's PA.

1.5.2 Narahubung/Contact Person

Pemilik, Pengandal, dan pihak ketiga lainnya dapat menghubungi Peruri CA melalui surat elek-

Subscribers, Relying Parties, and other third parties may contact Peruri CA via email and/or

tronik (surel) dan/atau melalui dokumen fisik bertandatangan basah untuk melaporkan dugaan penyalahgunaan Sertifikat Elektronik yang diterbitkan Peruri CA.

through wet-signed physical documents to report suspected misuse of Electronic Certificates issued by Peruri CA.

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

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

Policy Authority (PA) Peruri CA menentukan kesesuaian konten CPS ini dan kesesuaian antara CPS ini dengan CP PSrE Induk. PA menerima masukan dari anggota Peran Terpercaya, regulator, dan auditor eksternal untuk melakukan perubahan terhadap dokumen CPS, kemudian menentukan kesesuaian dan penerapannya.

Policy Authority (PA) Peruri CA determines suitability of this CPS and the conformance of the CPS to Root CA's CP. PA receives input from Trusted Role members, regulators, and external auditors to make changes to the CPS document, then determining the suitability and application of the document.

1.5.4 Prosedur Persetujuan CPS/*CPS Approval Procedures*

Policy Authority (PA) Peruri CA menyetujui CPS dan segala perubahannya setelah mendapat persetujuan dari *Policy Authority* (PA) PSrE Induk.

Policy Authority (PA) Peruri CA approves the CPS and any amendments after the CPS is approved by Root CA's Policy Authority (PA).

Perubahan dibuat dengan mengubah seluruh CPS atau dengan mempublikasikan addendum. PA Peruri CA menentukan apakah perubahan atas CPS ini membutuhkan pemberitahuan atau perubahan OID.

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

1.6 Definisi dan Akronim/Definitions and Acronyms

Lihat Lampiran untuk tabel akronim dan definisi.

See Appendix for a table of acronyms and definitions.

SECTION 2

Tanggung Jawab Publikasi dan Repositori/*Publication and Repository Responsibilities*

Peruri CA melaksanakan prosedur yang mengatur ketentuan tentang tanggung jawab publikasi dan repositori.

Peruri CA perform procedures that regulate the rules concerning the responsibility of publication and repository.

2.1 Repositori/*Repositories*

Peruri CA bertanggung jawab memelihara repositori yang dapat diakses publik. Dokumen yang dipublikasikan antara lain, namun tidak terbatas pada:

1. Sertifikat Elektronik Peruri CA;
2. CRL;
3. Responder OCSP;
4. CPS ;
5. Perjanjian Pemilik;
6. Kebijakan Privasi;
7. Perjanjian Pengandal; dan

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

1. *Peruri CA Electronic Certificate;*
2. *CRL;*
3. *OCSP Responder;*
4. *CPS ;*
5. *Subscriber Agreement;*
6. *Privacy Policy;*
7. *Relying Party Agreement; and*

8. Kebijakan Jaminan.

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

Peruri CA berhak untuk tidak mengunggah dokumen penunjang operasional lainnya yang tidak bersifat publik.

8. *Warranty Policy.*

Documents are made using bilingual, namely Indonesian and English. In the event of a discrepancy between the Indonesian version and the English version, the Indonesian version will take precedence.

Peruri CA reserves the right not to upload other operational supporting documents that are not public.

2.2 Publikasi Informasi Sertifikat Elektronik/*Publication Of Electronic Certificate Information*

Peruri CA memelihara repositori yang dapat diakses melalui internet, yang mempublikasikan Sertifikat Elektronik dari Peruri CA, CRL terakhir, dokumen CP/CPS, dan dokumen lainnya yang berkaitan dengan operasional Peruri CA.

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

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

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

2.3 Waktu Atau Frekuensi Publikasi/*Time Of Frequency Of Publication*

Dokumen CPS dan setiap perubahan yang dilakukan dapat diakses secara publik dalam waktu selambat-lambatnya 7 (tujuh) hari kalender setelah disetujui.

Peruri CA mempublikasikan Sertifikat Elektronik Pemilik dan data pencabutan Sertifikat Elektronik dalam waktu 30 (tiga puluh) menit setelah penerbitan.

CRL diperbarui sesuai dengan frekuensi penerbitan CRL pada bagian 4.9.7

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

Peruri CA publishes Subscriber's Electronic Certificates data and revocation data within 30 (thirty) minutes after issuance.

The CRL is updated in accordance with the issuance frequency of CRL in section 4.9.7.

2.4 Kendali Akses pada Repositori/*Access Controls on Repositories*

Informasi yang terpublikasi pada repositori adalah informasi publik (biasa). Peruri CA mem-

Information published on a repository is public information (general). Peruri CA provides unre-

berikan akses baca yang tidak dibatasi pada repositori dan menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut.

stricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

Peruri CA melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

Peruri CA protects information not intended for public dissemination or modification.

SECTION 3

Identifikasi Dan Autentikasi/*Identification And Authentication*

Sertifikat Elektronik yang diterbitkan oleh Peruri CA dapat diidentifikasi berdasarkan sistem penamaan berikut ini.

Electronic Certificates issued by Peruri CA can be identified based on the following naming system.

3.1 Penamaan/*Naming*

3.1.1 Tipe Nama/*Types of Names*

Peruri CA men-*generate* (membangkitkan) dan menandatangani Sertifikat Elektronik dengan subjek *Distinguished Name* (DN) yang *non-null* dan mematuhi standar ITU X.500.

Peruri CA generates and sign Electronic Certificates with a non-null subject Distinguished Name (DN) that complies with the ITU X.500 standards.

Sertifikat Elektronik Peruri CA mematuhi ketentuan atribut sebagaimana ditetapkan dalam ITU-T X.520, yang mencakup atribut *organizationName* (O) dengan value sesuai nama badan hukum resmi.

Peruri CA Electronic Certificates comply with the attribute requirements as specified in ITU-T X.520, which include the organizationName (O) attribute with a value corresponding to the official registered legal entity name.

Tabel di bawah meringkas DN minimum dari Sertifikat Elektronik yang diterbitkan oleh Peruri CA.

The table below summarizes the minimum DNs of the Electronic Certificates issued by Peruri CA.

Tipe Sertifikat Elektronik/ ***Electronic Certificate Type***		**Distinguished Name (DN) /** ***Distinguished Name (DN)***
Sertifikat Elektronik Peruri CA/ *Peruri CA Electronic Certificate*		CN=<Nama Peruri CA>, O=<Peruri>, C=ID
Sertifikat Elektronik Pemilik/ *Subscriber Electronic Certificate*	Individual/ *Individual*	CN=<Nama>, OU=PERSONAL, O=Public, C=ID
	Individual dengan Afiliasi/ *Affiliated Individual*	CN=<Nama>, OU=<Unit Organisasi Badan Usaha>, O=<Nama Badan Usaha>, C=ID
	Badan Usaha untuk Segel Elektronik/ *Business Entity for Electronic Seal*	CN=<Nama Badan Usaha>, C=ID

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

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

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

Nama subjek dan penerbit yang terkandung dalam Sertifikat Elektronik memiliki arti bahwa Peruri CA memiliki bukti keterkaitan yang cukup antara nama dengan Pemilik. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh Pemilik yang sah atau perwakilan resmi dari Pemilik yang sah.

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

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

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

Peruri CA shall not issue end-entity anonymous or pseudonymous Electronic Certificates.

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

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

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

3.1.5 Keunikan Nama/*Uniqueness of Names*

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

Distinguished Names in Electronic Certificates are unique within the Peruri CA domain.

3.1.6 Pengakuan, Autentikasi dan Peran Merek Dagang/*Recognition, Authentication, and Role of Trademarks*

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

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

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

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

3.2 Validasi Identitas Awal/*Initial Identity Validation*

Peruri CA memiliki prosedur dan dokumen yang mengatur rincian proses verifikasi identitas Pemohon baik itu organisasi atau individu. Prosedur dan dokumen dimaksud mengacu pada ketentuan peraturan perundang-undangan, Standar Verifikasi Identitas, dan CPS ini. Peruri CA dapat menolak untuk menerbitkan Sertifikat Elektronik atas dasar ketidaksesuaian dengan peraturan perundang-undangan yang berlaku.

Peruri CA has procedures and documents that regulate the details of the Applicant's identity verification process, whether it is an organization or an individual. These procedures and documents refer to the provisions of laws and regulations, Identity Verification Standards, and this CPS. Peruri CA may refuse to issue an Electronic Certificate on the basis of non-compliance with applicable laws and regulations.

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

Untuk Sertifikat Elektronik Pemilik, Pasangan Kunci dibangkitkan oleh Peruri CA, dengan syarat

For Subscriber Electronic Certificate, Key Pairs generated by Peruri CA, that the Private Key is se-

Kunci Privat dibangkitkan dengan menggunakan modul kriptografis yang memenuhi persyaratan FIPS 140-2 Level 3 dan hanya dapat diakses oleh Pemilik dengan minimal menggunakan 2 (dua) faktor autentikasi.

cured using a cryptographic module that meets FIPS 140-2 Level 3 requirements and can only be accessed by Subscriber using a minimum of 2 (two) factor authentication.

3.2.2 Autentikasi Identitas Organisasi/*Authentication of Organization Identity*

Permohonan Sertifikat Elektronik untuk organisasi hanya dapat dilakukan oleh Badan Usaha yang telah bekerja sama dengan Peruri CA dan diajukan oleh pihak yang berwenang untuk mewakili organisasi tersebut dibuktikan dengan dokumen Badan Usaha apabila diwakilkan oleh Pimpinan tertinggi organisasi atau Direktur Utama atau yang mewakili yang dibuktikan dengan surat kuasa.

Applications for Electronic Certificates for organizations can only be made by a Business Entity that has agreement with Peruri CA and is submitted by an authorized party to represent the organization as evidenced by a Business Entity document if it is represented by the organization's highest leadership or the President Director or who represents the organization evidenced by a power of attorney.

Peruri CA akan memeriksa identitas (KTP) dan jabatan dari Pemohon disesuaikan dengan dokumen Badan Usaha termasuk namun tidak terbatas kepada Akta Pendirian Perusahaan dan perubahannya, NIB, SIUP, NPWP, dan khusus organisasi yang dimaksud adalah Badan Usaha Milik Negara (BUMN) maka melampirkan SK Penunjukan Pejabat yang memohonkan dari Otoritas Pengatur dan Pengawas Sektor. Bagi Pemohon yang diwakilkan harus melampirkan surat kuasa yang ditandatangani oleh Direktur Perusahaan dan Kartu Identitas Pegawai.

Peruri CA will check the residential identification (KTP) and position of the Applicant in accordance with the legalized Business Entity documents including but not limited to the Company Establishment Deed, NIB, SIUP, NPWP, and in terms of the Organization such as State-Owned Enterprise, The Applicant can attach a Letter of CEO Appointment from Regulatory Authority and Sector. Applicants who are represented are required to attach a power of attorney signed by the Director of the Company and an Employee Identity Card.

Peruri CA menyimpan dokumen terkait identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya selama masa berlaku dari Sertifikat Elektronik yang diterbitkan.

Peruri CA maintains a record of the type and details of the identification, which is used for authentication for the organization at least during the validity period of the issued Electronic Certificate.

Peruri CA tidak menerbitkan Sertifikat Elektronik bagi Pemohon yang tidak dapat diverifikasi.

Peruri CA does not issue Electronic Certificate to unverifiable Applicants.

3.2.3 Autentikasi Identitas Individu/*Authentication of Individual Identity*

Autentikasi identitas warga negara Indonesia dan warga negara asing (individu) yang mengajukan permohonan Sertifikat Elektronik untuk individu atau individu penanggung jawab Badan Usaha mengikuti persyaratan sesuai dengan ketentuan peraturan perundang-undangan terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik, Standar Verifikasi Identitas, dan CPS ini.

Authentication of the identity of Indonesian citizens and foreign citizens (individuals) who apply for an Electronic Certificate for individuals or individuals responsible for a Business Entity follows the requirements in accordance with the provisions of laws and regulations related to the Governance of the Implementation of Electronic Certification, Identity Verification Standards, and this CPS.

3.2.3.1 Autentikasi Identitas Individu yang Berafiliasi dengan Perusahaan/*Identity Authentication of Individual who are Affiliated with a Company*

Peruri CA melakukan verifikasi identitas individu WNI yang berafiliasi dengan perusahaan sebagai pegawai internal atau merupakan bagian dari perusahaan (kemudian disebut dengan *Corporate Users*) dan WNI yang memanfaatkan Pengandal dari Peruri CA untuk menerbitkan Sertifikat Elektronik sebagai pengguna layanan (kemudian disebut dengan *Corporate Clients*) dengan cara memastikan *liveness detection* dari Pemohon serta membandingkan data kartu identitas dan data biometrik terhadap data identitas yang dimiliki oleh pemerintah. Peruri CA kemudian menerbitkan Sertifikat Elektronik kelas 2.

Peruri CA verifies the identity of Indonesian citizens who are affiliated with related companies as internal employees or are part of the company (later referred to as Corporate Users) and Indonesian citizens who use Peruri CA's Relying Party to issue Electronic Certificates as service users (later referred to as Corporate Clients) by ensuring the liveness detection of the Applicant and obtaining the results of matching data, including biometric data, which is managed by the government agency administering the population administration. Peruri CA then issues a class 2 Electronic Certificate.

Untuk tujuan identifikasi dan autentikasi, Pemohon Sertifikat Elektronik WNI *Corporate Users* harus memberikan informasi sebagai berikut:

1. Persetujuan terhadap Perjanjian Pemilik untuk penerbitan Sertifikat Elektronik;
2. Data NIK, Nama, tanggal lahir;
3. Salinan Kartu Tanda Penduduk (KTP);
4. Salinan kartu identitas resmi yang dikeluarkan oleh perusahaan;

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

1. *Consent to the Subscriber's Agreement for the issuance of Electronic Certificates;*
2. *NIK data, name, date of birth;*
3. *Copy of Identity Card (KTP);*
4. *Copy of official identity card issued by the corporate;*

5. Foto wajah;
6. Nomor *handphone*; dan
7. Alamat *email* perusahaan.

Untuk Pemohon WNI *Corporate Clients* harus memberikan informasi sebagai berikut:

1. Persetujuan terhadap Perjanjian Pemilik untuk penerbitan Sertifikat Elektronik;
2. Data NIK, Nama, tanggal lahir;
3. Salinan Kartu Tanda Penduduk (KTP);
4. Foto wajah;
5. Nomor *handphone*; dan
6. Alamat *email*.

Sementara bagi Pemohon WNA (Warga Negara Asing) harus memberikan;

1. Mengisi Formulir Pendaftaran Sertifikat Elektronik;
2. KTP atau bagi yang tidak memiliki KTP menggunakan Kartu izin Tinggal Sementara (KITAS);
3. Paspor;
4. Foto wajah;
5. Nomor *handphone*;
6. Alamat *email*; dan
7. Surat jaminan dari perusahaan yang ditandatangani oleh penanggung jawab perusahaan dimana Pemohon bekerja.

Peruri CA kemudian menerbitkan Sertifikat Elektronik level 2.

5. *Face photo;*
6. *Phone number; and*
7. *Corporate email address.*

For Indonesian Citizen Applicant Corporate Clients are required to provide the following information:

1. *Consent to the Subscriber's Agreement for the issuance of Electronic Certificates;*
2. *NIK data, name, date of birth;*
3. *Copy of Identity Card (KTP);*
4. *Face photo;*
5. *Phone number; and*
6. *Email address*

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

1. *Fill out the Electronic Certificate Registration Form;*
2. *KTP or for those who do not have a KTP, use a Temporary Residence Permit Card (KITAS);*
3. *Passport;*
4. *Face photo;*
5. *Phone number;*
6. *Email Address; and*
7. *Guarantee letter from the corporate signed by the person in charge of the corporate where the Applicant works.*

Peruri CA then issues a level 2 Electronic Certificate.

3.2.3.2 Autentikasi Identitas Individu yang Tidak Berafiliasi dengan Perusahaan/*Identity Authentication of Individual who are Not Affiliated with a Company*

Peruri CA melakukan verifikasi identitas individu WNI umum yang tidak berafiliasi dengan perusahaan dengan cara memastikan *liveness detection* dari Pemohon serta membandingkan data kartu identitas atau data biometrik terhadap data identitas yang dimiliki oleh pemerintah. Peruri CA kemudian menerbitkan Sertifikat Elektronik kelas 2.

Peruri CA verifies the identity of Indonesian citizens who are not affiliated with a company by ensuring the liveness detection of the Applicant and obtaining the results of matching data, including biometric data, which is managed by the government agency administering the population administration. Peruri CA then issues a class 2 Electronic Certificate.

Untuk tujuan identifikasi dan autentikasi, Pemohon WNI harus memberikan informasi sebagai berikut:

1. Persetujuan terhadap Perjanjian Pemilik untuk penerbitan Sertifikat Elektronik;
2. Data NIK, Nama, tanggal lahir;
3. Salinan Kartu Tanda Penduduk (KTP);
4. Foto wajah;
5. Nomor *handphone*; dan
6. Alamat *email*.

For the purpose of identification and authentication Indonesian Citizen Applicant are required to provide the following information:

1. *Consent to the Subscriber's Agreement for the issuance of Electronic Certificates;*
2. *NIK data, name, date of birth;*
3. *Copy of Identity Card (KTP);*
4. *Face photo;*
5. *Phone number; and*
6. *Email Address.*

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

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

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

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

Peruri CA tidak menerbitkan Sertifikat bagi Pemohon yang tidak dapat diverifikasi.

Peruri CA shall not issue Certificate to univerifiable Applicants.

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

Informasi yang tidak bisa diverifikasi tidak disertakan di dalam Sertifikat Elektronik.

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

3.2.5 Validasi Otoritas/*Validation of Authority*

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

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

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

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

3.2.6 Kriteria Inter-operasi/*Criteria for Interoperation*

Tidak ada ketentuan.

No stipulation.

3.3 Identifikasi Dan Autentikasi Untuk Permintaan Penggantian Kunci (Re-Key)/ *Identification And Authentication For Re-Key Requests*

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

Sebelum masa berlaku Sertifikat Elektronik berakhir, Pemilik dapat meminta penggantian kunci *(re-key)* kepada Peruri CA dan Peruri CA akan menerbitkan Sertifikat Elektronik dan kunci baru dengan masa berlaku yang baru. Pemilik harus diautentikasi melalui penandatanganan menggunakan Sertifikat Elektronik yang berlaku atau menggunakan proses pemeriksaan identitas awal sebagaimana diatur pada Bagian 3.2.

Before the validity period of the Electronic Certificate expires, Subscriber may request for re-key from Peruri CA and Peruri CA will issue a new Electronic Certificate and a new key with a new validity period. Subscriber must be authenticated by signing using a valid Electronic Certificate or using the initial identity check process as set out in Section 3.2.

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

Setelah Sertifikat Elektronik dicabut selain karena alasan penggantian kunci (*re-key*) pada bagian 3.3.1 untuk mendapatkan Sertifikat Elektronik baru dengan kunci yang baru, Pemilik mengulang proses permohonan seperti yang dijelaskan pada bagian 3.2.2 dan 3.2.3.

After an Electronic Certificate has been revoked during a renewal action in section 3.3.1, the Subscriber is required to go through the initial registration process described in section 3.2.2 and 3.2.3 to obtain a new Electronic Certificate with new keys.

3.4 Identifikasi Dan Autentikasi Untuk Permintaan Pencabutan/*Identification And Authentication For Revocation Request*

Permintaan pencabutan selalu diautentikasi. Permintaan untuk mencabut Sertifikat Elektronik dapat diautentikasi menggunakan Kunci Publik yang terhubung dengan Sertifikat Elektronik atau memvalidasi formulir permohonan pencabutan yang ditandatangani dengan tanda tangan elektronik oleh Pemilik atau pihak yang berwenang, dan memastikan keabsahan permintaan, terlepas dari apakah Kunci Privat telah terkompromi.

Revocation requests shall always be authenticated. Requests to revoke an Electronic Certificate may be authenticated using that Electronic Certificate's associated Public Key or validate the revocation request form which is signed with an electronic signature by the Subscriber or the authorized party, and ensuring the validity of the request, regardless of whether the Private Key has been compromised.

Prosedur bagaimana permintaan pencabutan dijelaskan di bagian 4.9.3.

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

4

SECTION

Persyaratan Operasional Siklus Sertifikat Elektronik/*Electronic Certificate Life-Cycle Operational Requirements*

Siklus hidup Sertifikat Elektronik meliputi pendaftaran, penerbitan, perubahan, dan pencabutan Sertifikat Elektronik. Untuk perubahan Sertifikat terdiri atas 3 macam cara, yaitu:

1. Pembaruan Sertifikat Elektronik *(Electronic Certificate Renewal)*: Sertifikat Elektronik berisikan informasi dan kunci yang sama. Perubahan terletak pada masa berlaku Sertifikat Elektronik. Pengaturan lebih lengkap dibahas pada Bagian 4.6.

2. Penggantian kunci *(Electronic Certificate Re-key)*: Sertifikat Elektronik berisikan informasi yang sama dan masa berlaku yang dapat berbeda. Perubahan terletak pada kunci yang berasosiasi dengan Sertifikat Elektronik. Pengaturan lebih lengkap dibahas pada Bagian 4.7.

An Electronic Certificate life cycle consists of registration, issuance, modification, and revocation. Electronic Certificate modification is further classified into three modes:

1. *Electronic Certificate Renewal: The key and information contained in the Electronic Certificate remain the same. The alteration is only on the validity period of the Electronic Certificate. Further stipulation on Electronic Certificate renewal is described in Section 4.6.*

2. *Electronic Certificate Re-key: Information contained in the Electronic Certificate remains the same, however the validity period may be different. The alteration is only on the keys associated with the Electronic Certificate. Further stipulation on Electronic Certificate Re-Key is described in Section 4.7.*

3. Perubahan Sertifikat Elektronik *(Electronic Certificate Modification)*: Sertifikat Elektronik berisikan kunci yang sama namun sebagian isi Sertifikat Elektronik berubah. Pengaturan lebih lengkap dibahas pada Bagian 4.8

Setelah Sertifikat Elektronik Peruri CA diterbitkan, Peruri CA memiliki kewajiban untuk:

1. Melindungi Kunci Privat dengan aman;
2. Mendapatkan persetujuan PA PSrE Induk terhadap perubahan CPS;
3. Melakukan operasional PSrE sebagaimana diatur dalam ketentuan peraturan perundang-undangan, CP PSrE Induk, dan CPS;
4. Membarui CPS ketika terjadi perubahan pada kebijakan CP PSrE Induk atau sebagaimana diatur dalam panduan yang diterbitkan oleh PA PSrE Induk;
5. Mengumumkan informasi nama dan kontak dari pihak yang bertanggungjawab terhadap Peruri CA;
6. Mengelola website dan menampilkan Surat Keputusan Pengakuan PSrE Indonesia, Sertifikat Elektronik Peruri CA, Sertifikat Elektronik Pemilik, dan otoritas validasi; dan
7. Mencabut semua Sertifikat Elektronik Pemilik dan menerbitkan CRL sesegera mungkin dalam hal terjadi kebocoran kunci penandatanganan dan melaporkannya ke PSrE Induk sesegera mungkin.

3. *Electronic Certificate Modification: The Key contained in Electronic Certificate remains the same, but some contents of the Electronic Certificate are changed. Further stipulation on Electronic Certificate modification is described in Section 4.8.*

After the Peruri CA Electronic Certificate is issued, Peruri CA has the obligation to:

1. *Protect their Private Key in a secure manner;*
2. *Have CPS approved by Root CA's PA;*
3. *Perform the CA operation as stipulated in laws and regulations, Root CA's CP, and CPS;*
4. *Update the CPS when the Root CA's CP policy changes or in accordance with the Root CA PA guidelines;*
5. *Publish a name and contact information of the party responsible for Peruri CA;*
6. *Maintain a website and publish the Recognition Letter of the Indonesian CA, Peruri CA Electronic Certificate, Subscriber Electronic Certificates, and validation authorities; and*
7. *Revoke all the Electronic Certificates of Subscribers and publish the CRL immediately in the case of compromise of the signing key and this is to be reported to Root CA immediately.*

4.1 Permohonan Sertifikat Elektronik/*Electronic Certificate Application*

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

Permohonan dari Badan Usaha untuk menjadi Pemilik kepada Peruri CA diajukan oleh orang yang berwenang mewakili Badan Usaha tersebut.

Application from a Business Entity to become a Subscriber to Peruri CA is submitted by a person authorized to represent the Business Entity.

Permohonan dari warga negara Indonesia dan warga negara asing (individu) hanya dapat dilakukan oleh individu tersebut atau oleh orang lain atau organisasi yang secara resmi memiliki wewenang untuk mewakili Pemohon tersebut.

Application from Indonesian citizens and foreign citizens (individuals) can only be made by the individual or by another person or organization that officially has the authority to represent the Applicant.

Permohonan Sertifikat Elektronik hanya dapat dilakukan oleh individu atau entitas non-instansi pemerintah. Proses pendaftaran disertai dengan identitas Pemohon yang dapat diverifikasi. Pemohon harus menyetujui syarat dan ketentuan Peruri CA dan memberikan informasi yang cukup sehingga Peruri CA melakukan verifikasi atas dokumen tersebut.

Applications for Electronic Certificates can only be made by individuals or non-government entities. The registration process is accompanied by a verifiable identity of the Applicant. The Applicant is required to agree to the terms and conditions of Peruri CA and provide sufficient information so that Peruri CA verify the document.

RA Peruri CA melakukan verifikasi terhadap seluruh permohonan yang diterima sesuai dengan ketentuan peraturan perundang-undangan terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik dan Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk.

Peruri CA's RA carry out verification of all applications received in accordance with the provisions of laws and regulations related to CA Governance and Identity Verification Standards issued by Root CA.

Verifikasi dan Validasi Dokumen / Verification and Document Validation	Pemohon / Applicant				
	Individu / Individual				Badan Usaha / Business Entity
	Warga Negara Indonesia (WNI*) / Indonesia Citizen			Warga Negara Asing (WNA*) / Foreign Citizen	
	Terafiliasi dengan Sebuah Perusahaan / Affiliated with a Company		Tidak Terafiliasi dengan Perusahaan/ Not Affiliated with a Company		
	Corporate User	Corporate Client			
KTP/ *Residential Identification*	✓	✓	✓	✓ (jika memiliki/ *if any)*	✓
Paspor *Passport*				✓	
KITAS*/KITAP*/ ID Nasional *(National ID)*				✓	
Informasi: NIK, Nama Lengkap & TTL/ *Information: Resident Number, Full Name* & *Date of Birth*	✓	✓	✓		✓
Kartu Pegawai/ *Company ID Card*	✓			✓ (jika memiliki/ *if any)*	✓
Kartu Identitas Lain/ *Other ID Card*				✓ (opsional/ *optional)*	
Surel Perusahaan / *Corporate Email*	✓			✓ (jika memiliki/ *if any)*	✓
Surel Pribadi / *Private Email*		✓	✓	✓	
Nomor Telepon Seluler/ *Handphone Number*	✓	✓	✓	✓ (jika memiliki/ *if any)*	
Formulir Pendaftaran Sertifikat/ *Certificate Registration Form*				✓	

Verifikasi dan Validasi Dokumen / Verification and Document Validation	Pemohon / Applicant				
	Individu / Individual				Badan Usaha / Business Entity
	Warga Negara Indonesia (WNI*) / Indonesia Citizen			Warga Negara Asing (WNA*) / Foreign Citizen	
	Terafiliasi dengan Sebuah Perusahaan / Affiliated with a Company		Tidak Terafiliasi dengan Perusahaan/ Not Affiliated with a Company		
	Corporate User	Corporate Client			
Surat Jaminan dari Perusahaan/ *Guarantee Letter from The Corporate*				✓	
Foto Wajah/ *Face Photo*	✓	✓	✓	✓	✓
Verifikasi Data Biometrik/ *Biometric Data Verification/*	✓	✓	✓	✓	✓
Deteksi Kehidupan/ *Liveness Detection/*	✓	✓	✓	✓	✓
Akta Pendirian Perusahaan/ *Deed of Incorporation*					✓
NIB*, SIUP*, NPWP*					✓
SK Penunjukan Pejabat/ *Statement of Appointment*					✓
Surat Kuasa (apabila diwakilkan)/ *Power of Attorney (if represented)*					✓

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

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

Pemohon bertanggung jawab untuk menyediakan informasi yang akurat serta menyetujui Perjanjian Pemilik atau kontrak berlangganan dan Kebijakan Privasi sebelum melakukan permohonan Sertifikat Elektronik.

The Applicant must be responsible for providing accurate information and agreeing to a subscription contract before applying for an Electronic Certificate.

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

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

1. Memberikan formulir Permohonan Pendaftaran Sertifikat kepada Pemohon;
2. Menerima formulir permohonan pendaftaran Sertifikat Elektronik yang telah diisi oleh Pemohon;
3. Memastikan bahwa Pemohon telah menyetujui Perjanjian Pemilik atau kontrak berlangganan yang berlaku; dan
4. Memastikan bahwa Pemohon telah menyetujui Kebijakan Privasi.

1. *Provide an Electronic Certificate Registration Application form to the Applicant;*
2. *Receive the Electronic Certificate registration application form which has been filled out by the Applicant;*
3. *Ensure that the Applicant has agreed to the Subscriber Agreement or subscription contract; and*
4. *Ensure that the Applicant has agreed to the Privacy Policy.*

Pemohon harus membayar biaya yang berlaku sesuai dengan kontrak berlangganan.

The Applicant is required to pay the applicable fees in accordance with the subscription contract.

Peruri CA memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat Elektronik. Sertifikat Elektronik yang dimaksud menampilkan identitas kepada Pengandal atau Pemilik.

Peruri CA maintains systems and processes capable of authenticating Applicant identity for all types of Electronic Certificates. The Electronic Certificate in question displays identity to the Relying Party or Subscriber.

Peruri CA melindungi komunikasi dan menyimpan informasi yang diberikan oleh Pemohon selama proses pendaftaran dengan aman.

Peruri CA protects communications and securely stores information provided by Applicants during the registration process.

4.2 Pemrosesan Permohonan Sertifikat Elektronik/*Certificate Application Processing*

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

Identifikasi dan autentikasi Pemohon memenuhi persyaratan yang ditentukan untuk autentikasi Pemilik sebagaimana dalam CPS bagian 3.2.

Identification and authentication The Applicant meets the requirements specified for Subscriber authentication as set out in CPS section 3.2.

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

Setelah semua pemeriksaan identitas dan atribut Pemohon yang mengacu pada poin 4.1 dipenuhi maka Sertifikat Elektronik dapat diterbitkan.

After all checking of the identity and attributes of the Applicant referring to point 4.1 is fulfilled the Electronic Certificate can be issued.

Apabila Pemohon tidak memenuhi syarat untuk penerbitan Sertifikat Elektronik atau permohonannya mengandung kesalahan, Peruri CA langsung menolak proses permohonan tersebut. Peruri CA meminta tambahan informasi lainnya seperti SIM, paspor, dan/atau dokumen lainnya yang menjelaskan identitas serta memuat foto Pemohon untuk dilakukan proses verifikasi lebih lanjut dan selanjutnya permohonan disetujui apabila proses verifikasi dan validasi telah sesuai.

If the Applicant does not meet the requirements for the issuance of Electronic Certificate or the application contains errors, Peruri CA rejects the application process directly. Peruri CA request additional information such as driver's license, passport, and/or other documents that explain identity and contain photo of the Applicant for further verification process and then the application is approved if the verification and validation process is appropriate.

Peruri CA memiliki prosedur terkait proses pendaftaran Sertifikat Elektronik dan terkait verifikasi data Pemohon.

Peruri CA has procedures related to the Electronic Certificate registration process and related to verification of Applicant data.

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

Semua pihak yang terlibat dalam proses permohonan Sertifikat Elektronik melakukan usaha untuk memastikan permohonan Sertifikat Elektronik diproses tepat waktu.

All parties involved in the Electronic Certificate application process make efforts to ensure that the Electronic Certificate application is processed in a timely manner.

Peruri CA akan menyelesaikan proses validasi

Peruri CA will complete the validation process and

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

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

4.3 Penerbitan Sertifikat Elektronik/*Electronic Certificate Issuance*

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

Pada proses penerbitan Sertifikat Elektronik, Peruri CA melakukan tindakan-tindakan sebagai berikut:

1. Memastikan identitas Pemohon sebagaimana diatur pada Bagian 3.2.2 dan 3.2.3;
2. Memverifikasi otoritas Pemohon sebagaimana diatur pada Bagian 3.2.5;
3. Mempersiapkan dan menandatangani Sertifikat Elektronik saat semua persyaratan telah dipenuhi;
4. Memastikan bahwa Pemilik menerima Sertifikat Elektronik sebagaimana diatur pada Bagian 4.4; dan
5. Membuat Sertifikat tersedia bagi Pemilik setelah Pemilik secara formal menyetujui kewajibannya sebagaimana diatur pada Bagian 9.6.3.

In the Electronic Certificate issuance process, Peruri CA perform the following actions:

1. *Ensure the Applicant's identity as regulated in Sections 3.2.2 and 3.2.3;*
2. *Verifying the Applicant's authority as regulated in Section 3.2.5;*
3. *Prepare and sign the Electronic Certificates when all requirements have been met;*
4. *Ensure that the Subscriber receives the Electronic Certificate as regulated in Section 4.4; And*
5. *Make the Certificate available to the Subscriber after the Subscriber formally agrees to its obligations as provided in Section 9.6.3.*

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

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

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

Pemilik tidak dapat menggunakan Sertifikat Elek-

Subscriber cannot use the Electronic Certificate be-

tronik sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat Elektronik.

fore checking all the information in the Electronic Certificate.

4.4 Pernyataan Persetujuan Sertifikat Elektronik/*Certificate Acceptance*

4.4.1 Sikap yang Dianggap sebagai Menyetujui Sertifikat Elektronik/*Conduct Constituting Electronic Certificate Acceptance*

Pemilik memeriksa semua informasi tentang Sertifikat Elektronik dan melakukan penerimaan Sertifikat Elektronik sebelum menggunakan Sertifikat Elektronik tersebut.

The Subscriber checks all information about the Electronic Certificate and receives the Electronic Certificate before using the Electronic Certificate.

Bila tidak ada keluhan dari Pemilik dalam waktu 7 (tujuh) hari kerja atau Pemilik telah menggunakan Sertifikat Elektronik tersebut, Pemilik dianggap menerima semua informasi Sertifikat Elektronik.

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

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

In the case of Electronic Certificate issuance, Peruri CA makes acceptance procedures and documents receipt of issued Electronic Certificates.

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

Peruri CA mempublikasikan Sertifikat Elektroniknya dalam sebuah Repositori sebagaimana tercantum pada bagian 2.2 paling lambat 1 (satu) hari setelah Sertifikat Elektronik diterbitkan, termasuk ketika menerbitkan informasi pencabutan terkait Sertifikat Elektronik tersebut pada Repositori. Peruri CA mempublikasikan Sertifikat Elektronik Pemilik dengan mengirimkannya ke Pemilik tersebut.

Peruri CA publishes its Electronic Certificate in a Repository as stated in section 2.2 no later than 1 (one) day after the Electronic Certificate is issued, including when issuing revocation information regarding the Electronic Certificate in the Repository. Peruri CA publishes the Subscriber's Electronic Certificate by sending it to the Subscriber.

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

Tidak ada ketentuan.

No stipulation.

4.5 Penggunaan Pasangan Kunci Dan Sertifikat Elektronik/*Key Pair And Electronic Certificate Usage*

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

Peruri CA melindungi Kunci Privat Pemilik dari penggunaan tanpa izin atau pengungkapan oleh pihak lain dengan menggunakan *Hardware Security Module* (HSM) dan *Self-encrypting Drives* (SED) milik Peruri CA.

Peruri CA protects the Subscriber's Private Key from unauthorized use or disclosure by others by using Peruri CA's Hardware Security Module (HSM) and Peruri CA's Self-encrypting Drives (SED).

Peruri CA menerapkan kombinasi minimal 2 (dua) faktor autentikasi bagi Pemilik yang akan menggunakan Kunci Privatnya. Pemilik melindungi parameter autentikasi yang digunakan untuk mengaktifkan Kunci Privatnya.

Peruri CA applies a combination of at least 2 (two) factor authentication for Subscriber who will use their Private Keys. The Subscriber protects the authentication parameters used to activate his Private Key.

Pemilik memakai Kunci Privatnya hanya untuk tujuan yang sudah ditentukan.

The Subscriber uses Private Key only for the specified purpose.

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

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

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

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

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

inan tambahan, Pengandal mendapatkan jaminan tersebut sebelum menggunakan Sertifikat Elektronik.

before using the Electronic Certificate.

4.6 Pembaruan Sertifikat Elektronik/*Electronic Certificate Renewal*

Pembaruan Sertifikat Elektronik (*renewal*) adalah penerbitan Sertifikat Elektronik baru dengan menggunakan nama, kunci, dan informasi yang sama dengan Sertifikat Elektronik lama yang belum kedaluwarsa, namun masa berlaku dan *serial number* Sertifikat Elektronik yang diperbarui.

Electronic Certificate renewal is the issuance of a new Electronic Certificate using the same name, key and information as the old Electronic Certificate that has not expired, but the validity period and serial number of the Electronic Certificate are renewed.

Peruri CA tidak melakukan proses pembaruan Sertifikat Elektronik Pemilik. Dalam hal masa berlaku Sertifikat Elektronik Pemilik akan berakhir, Pemilik dapat meminta Penerbitan ulang Sertifikat Elektronik dengan penggantian kunci (*re-key*) sesuai dengan poin 4.7.

Peruri CA does not renew the Subscriber's Electronic Certificate. In the event that the validity period of the Subscriber's Electronic Certificate expires, Subscriber may request Reissuance of the Electronic Certificate with re-key in accordance with point 4.7.

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

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

4.6.5 Sikap yang Dianggap sebagai Menerima Sertifikat Elektronik yang Diperbarui/*Conduct Constituting Acceptance of a Renewal Electronic Certificate*

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

4.7 Penggantian Kunci Sertifikat Elektronik/*Electronic Certificate Re-Key*

Penerbitan ulang Sertifikat Elektronik dengan penggantian kunci (*re-key*) adalah pembuatan/penerbitan Sertifikat Elektronik baru dengan Kunci Publik, *serial number*, dan *key identifier* yang baru, sementara informasi pribadi Pemilik yang terverifikasi dalam Sertifikat Elektronik baru masih sama dengan Sertifikat Elektronik lama. Sertifikat Elektronik baru dapat diisi masa berlaku yang baru, diisi dengan tempat publikasi CRL yang baru, dan/atau ditandatangani dengan kunci yang baru.

Re-issuance of Electronic Certificate with key replacement (re-key) is the creation/issuance of a new Electronic Certificate with a new Public Key, serial number, and key identifier, while the verified Subscriber's personal information in the new Electronic Certificate is still the same as the old Electronic Certificate. A new Electronic Certificate can be filled with a new validity period, filled with a new CRL publication place, and/or signed with a new key.

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

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

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

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

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

Pemilik dapat meminta *re-key* selama Sertifikat Elektronik yang akan diterbitkan memiliki karakteristik (misalnya *key usage*) dan level verifikasi yang sama dengan Sertifikat Elektronik yang

Subscriber may request a re-key as long as the Electronic Certificate to be issued has the same characteristics (eg key usage) and level of verification as the old Electronic Certificate.

lama.

Peruri CA melakukan penggantian kunci Sertifikat Elektronik selama:

1. Sertifikat Elektronik yang akan diganti belum dicabut, terkompromi, atau kedaluwarsa;
2. Pemilik telah memberi persetujuan untuk pembangkitan Pasangan Kunci baru dan terasosiasi dengan Sertifikat Elektronik tersebut; dan
3. Seluruh rincian yang terkait dengan Sertifikat Elektronik tersebut tetap akurat dan tidak dibutuhkan validasi baru dan tambahan.

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

1. *The old Electronic Certificate to be re-keyed has not been revoked, compromised, or expired;*
2. *Subscriber has or given approval to a generation of a new Key Pair and is associated to the Certificate; and*
3. *All details within the Electronic Certificate remain accurate and no new or additional validation is required.*

Apabila Kunci Privat Pemilik terkompromi atau Sertifikat Elektronik kedaluwarsa atau dicabut, maka Pemilik dapat mengajukan permohonan baru sebagaimana diatur pada Bagian 4.1.

If the Subscriber's Private Key is compromised or the Electronic Certificate expires or is revoked, then Subscriber can submit a new application as regulated in 4.1.

4.7.2 Siapa yang Dapat Meminta *Re-Key* Sertifikas Elektronik/*Who May Request Electronic Certificate Re-Key*

Sesuai dengan kondisi yang ditentukan pada bagian 4.7.1, Pemilik dapat meminta penggantian kunci kepada Peruri CA.

In accordance with the conditions specified in section 4.7.1, the Subscriber can request a key replacement to Peruri CA.

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

Berlaku prosedur yang dinyatakan pada bagian 3.3.

The procedure as stated in section 3.3.

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

Sertifikat Elektronik baru diterbitkan sesuai prosedur yang dinyatakan dalam bagian 4.3.2.

The new Electronic Certificate is published according to the procedures stated in section 4.3.2.

4.7.5 Sikap yang Dianggap Sebagai Menyetujui Sertifikat Elektronik yang di *Re-key*/*Conduct Constituting Acceptance of a Re-Keyed Certificate*

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

The Subscriber receives the Electronic Certificate with a new key following the same acceptance procedure as described in section 4.4.1.

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

Sertifikat Elektronik dengan kunci baru dipublikasikan sesuai dengan prosedur yang dinyatakan pada bagian 4.4.2.

The Electronic Certificate with the new key is published according to the procedures as stated in section 4.4.2.

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

Tidak ada ketentuan.

No Stipulation.

4.8 Modifikasi Sertifikat Elektronik/*Electronic Certificate Modification*

Peruri CA tidak melakukan modifikasi rincian Sertifikat Elektronik. Dalam hal terjadi kesalahan selama penerbitan Sertifikat Elektronik (contohnya ejaan), Sertifikat Elektronik yang sudah terbit dicabut dan diikuti dengan proses penerbitan Sertifikat Elektronik sebagaimana diatur pada Bagian 4.3.

Peruri CA does not modify the details of the Electronic Certificate. In the event of an error during the issuance of the Electronic Certificate (for example spelling), the Electronic Certificate that has been issued is revoked and followed by the process of issuing the Electronic Certificate as regulated in Section 4.3.

4.9 Pencabutan Dan Pembekuan Sertifikat Elektronik/*Electronic Certificate Revocation And Suspension*

4.9.1 Kondisi untuk Pencabutan/*Circumstances for Revocation*

Peruri CA mencabut Sertifikat Elektronik Pemilik ketika hubungan antara subjek dan Kunci Publik yang didefinisikan dalam Sertifikat Elektroniknya sudah tidak valid lagi, antara lain ketika:

1. Informasi yang berafiliasi dengan nama dalam Sertifikat Elektronik menjadi tidak valid;

Peruri CA revokes the Subscriber's Electronic Certificate when the relation between the Electronic Certificate and the subject is no longer valid, such as:

1. *Information affiliated with the name in the Electronic Certificate becomes invalid;*

2. Setiap informasi dalam Sertifikat Elektronik menjadi tidak valid;
3. Pemilik terbukti melanggar ketentuan dalam Perjanjian Pemilik;
4. Ada alasan untuk meyakini bahwa Kunci Privat telah bocor;
5. Pemilik atau pihak lain yang berwenang (sesuai ketentuan peraturan perundang-undangan seperti kepolisian, kejaksaan, perintah pengadilan) meminta agar Sertifikat Elektroniknya dicabut;
6. Peruri CA berhenti beroperasi;
7. Kunci hilang;
8. Pemilik sudah tidak bisa lagi menggunakan Sertifikat Elektronik (misal: meninggal – salinan sertifikat kematian harus ditunjukkan kepada Peruri CA); dan
9. Sertifikat Elektronik yang dibuat untuk uji coba.

Informasi pencabutan Sertifikat Elektronik tersebut dimasukkan dalam CRL dan/atau ditambahkan pada *responder* OCSP. Sertifikat Elektronik yang dicabut disertakan dalam semua publikasi baru tentang informasi status Sertifikat Elektronik sampai masa berlaku Sertifikat Elektronik berakhir.

2. *Any information in the Electronic Certificate becomes invalid;*
3. *The Subscriber is proven to have violated the stipulations of the Subscriber Agreement;*
4. *There is reason to believe the private key has been compromised;*
5. *The subscriber or other authorized party (in accordance with the provisions of laws and regulations such as the police, prosecutors, court orders) asks for its Electronic Certificate to be revoked;*
6. *Peruri CA termination;*
7. *Key lost;*
8. *Subscriber is not in a position to use the Electronic Certificate (for example: death – copy of death certificate must be shown to Peruri CA); and*
9. *The Electronic Certificate is issued for trial run.*

The Electronic Certificate revocation information is included in the CRL and/or added to the OCSP responder. Electronic Certificates that have been revoked are included in all new publications regarding Electronic Certificate status information until the Electronic Certificate validity period expires.

4.9.2 Pihak yang Dapat Meminta Pencabutan/*Who can Request Revocation*

Sertifikat Elektronik dapat diminta untuk dicabut oleh:

1. Pemilik;
2. Organisasi yang berafiliasi dengan Pemilik yang dapat membuktikan hilangnya hubungan Pemilik;

Electronic Certificates may be requested to be revoked by:

1. *Subscriber;*
2. *Organizations affiliated with the Subscriberwho can prove the loss of the Subscriber relationship;*

3. Entitas lain seperti lembaga penegak hukum yang dapat membuktikan terungkapnya Kunci Privat atau penyalahgunaan Sertifikat Elektronik sesuai CPS;
4. Peruri CA; atau
5. Ahli waris Pemilik.

3. *Other entities such as law enforcement agencies that can prove the disclosure of Private Keys or misuse of Electronic Certificates according to CPS;*
4. *Peruri CA; or*
5. *Heirs of the Subscribers.*

4.9.3 Prosedur Permintaan Pencabutan/*Procedure for Revocation Request*

Peruri CA melakukan verifikasi identitas dan kewenangan (untuk entitas penegak hukum) yang meminta pencabutan Sertifikat Elektronik. Validasi identitas dan wewenang pihak yang meminta pencabutan diperlukan sesuai dengan bagian 3.2.5 dan 3.4.

Peruri CA verifies the identity and authority (for juridical entity) whom makes request for Electronic Certificate revocation. The validation of the identity and authority is required according to Section 3.2.5 and 3.4.

Permintaan pencabutan Sertifikat Elektronik oleh Pemilik harus menyerahkan bukti bahwa:

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

Electronic Certificate revocation request by Subscriber shall attach evidences that:

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

Permintaan pencabutan Sertifikat oleh pihak yang berwenang lainnya harus menyerahkan bukti bahwa:

1. Kunci Privat dari Sertifikat Elektronik telah terungkap;
2. Penggunaan Sertifikat Elektronik tidak sesuai dengan CP/CPS, Perjanjian Pemilik, dan perjanjian lainnya; dan/atau
3. Pemilik tidak memiliki hubungan dengan institusi.

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

1. *The Private Key of the Electronic Certificate has been exposed;*
2. *The use of the Electronic Certificate does not conform to the CP/CPS, Subscriber Agreement, and other agreements; and/or*
3. *Subscriber's relationship with the institution does not exist.*

Permintaan pencabutan Sertifikat Elektronik dapat dilakukan dengan menghubungi Peruri CA

Requests for revocation of Electronic Certificates can be made by contacting Peruri CA via email to

melalui email ke cs.digital@peruri.co.id, kemudian mengisi formulir permintaan pencabutan dan menandatanganinya menggunakan tanda tangan elektronik tersertifikasi. Selanjutnya Peruri CA akan melakukan proses verifikasi atas permintaan pencabutan untuk kemudian memproses permintaan tersebut.

cs.digital@peruri.co.id, then filling out the revocation request form and signing it using a certified electronic signature. Furthermore, Peruri CA will carry out the verification process for the revocation request and then process the request.

4.9.4 Masa Tenggang Permintaan Pencabutan/*Revocation Request Grace Period*

Tidak ada tenggang waktu yang diizinkan setelah permintaan pencabutan terverifikasi.

No grace period is permitted once a revocation request has been verified.

Pihak yang disebutkan dalam bagian 4.9.2 harus meminta pencabutan segera setelah mengidentifikasi perlunya pencabutan Sertifikat Elektronik.

The parties identified in section 4.9.2 must request for revocation promptly after identifying the need for revocation.

Peruri CA akan mencabut Sertifikat Elektronik segera setelah proses verifikasi permintaan pencabutan dilaksanakan.

Peruri CA will revoke Electronic Certificates immediately after the revocation request verification process is carried out.

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

Peruri CA memulai penyelidikan permintaan pencabutan dalam waktu 1 (satu) hari kerja kecuali pada kasus *force majeure*. Permintaan pencabutan yang disertai dengan bukti pendukung yang memadai segera diproses sehingga dapat dipublikasikan pada CRL berikutnya, kecuali jika permintaan tersebut diterima dan disetujui dalam waktu kurang dari 2 (dua) jam sebelum penerbitan CRL berikutnya.

Peruri CA begins an investigation of the revocation request within 1 (one) working day except in the case of force majeure. Revocation requests accompanied by sufficient supporting evidence will be processed immediately so that the revocation can be published on the next CRL, unless the revocation request is accepted and approved within 2 (two) hours before the next CRL release.

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

Penggunaan Sertifikat Elektronik yang sudah dicabut dapat menimbulkan kerugian bagi Pengandal. Oleh karena itu, Pengandal harus melakukan validasi setiap Sertifikat Elektronik yang sudah dicabut terhadap CRL terbaru minimal 1x24 jam

The use of revoked Electronic Certificate may cause detriment to Relying Parties. Therefore, The Relying Party must validate each revoked Electronic Certificate against the most recent CRL within 24 hours after revocation and/or against OCSP server

setelah proses pencabutan dilakukan dan/atau terhadap server OCSP yang disediakan oleh Peruri CA minimal 1 jam setelah proses pencabutan dilakukan.

provided by Peruri CA within 1 hour after revocation.

Frekuensi validasi Sertifikat Elektronik terhadap CRL dan/atau OCSP milik Peruri CA ditentukan oleh Pengandal.

The frequency of Electronic Certificate validation against Peruri CA's CRL and/or OCSP is determined by the Relying Party.

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

Peruri CA mempublikasikan CRL dengan ketentuan sebagai berikut:

Peruri CA publish the CRL according to the following conditions:

Kondisi/ ***Condition***	**Publikasi CRL/** ***CRL Issuance***
Rutin/ *Routine*	Minimal sekali dalam 24 (dua puluh empat) jam/ *At least once every 24 (twenty-four) hours*
Kunci Privat hilang atau terkompromi/ *Loss or compromise of Private Key*	Maksimal 24 (dua puluh empat) jam setelah Peruri CA menerima permintaan pencabutan/ *Maximum 24 (twenty-four) hours after Peruri CA accepts the revocation request*
Peruri CA terkompromi atau insiden keamanan lainnya/ *Peruri CA compromise or other security incident*	Sesegera mungkin, namun tidak lebih dari 24 (dua puluh empat) jam setelah Peruri CA menerima notifikasi kompromi/ *Immediately, but not more than 24 (twenty-four) hours after Peruri CA accepts the compromise incident notification*

Untuk pencabutan Sertifikat Pemilik, waktu *nextUpdate* pada CRL Peruri CA paling lambat 72 (tujuh puluh dua) jam setelah waktu penerbitan (*thisUpdate time*).

For Subscriber's Electronic Certificate revocation, the value for nextUpdate field in Peruri CA's CRL is no later than 72 (seventy two) hours after the issuance time (thisUpdate time).

CRL disimpan dan dilindungi untuk menjamin integritas dan keautentikannya.

CRLs are stored and protected to ensure their integrity and authentication.

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

Peruri CA mempublikasikan CRL paling lama 30 (tiga puluh) menit setelah penerbitan.

Peruri CA publish the Certificate Revocation List within 30 (thirty) minutes after Certificate issuance.

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

Peruri CA memberikan layanan validasi daring. Pengandal dapat menggunakan layanan tersebut untuk memeriksa status pencabutan Sertifikat Elektronik.

Peruri CA provides online validation service. Relying Party may use the service to check the revocation status of the Electronic Certificate.

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

Repositori Peruri CA berisi dan mempublikasi daftar semua responder OCSP yang dioperasikan.

Peruri CA Repository contain and publish a list of all OCSP responders operated by Peruri CA.

Semua layanan OCSP yang diimplementasikan sesuai dengan standar internet *Engineering Task Force* (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas.

All OCSP services comply with the Internet Engineering Task Force (IETF) RFC 6960 standard to meet security and interoperability requirements.

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

Tidak ada ketentuan.

No stipulation.

4.9.12 Persyaratan Khusus terkait Kebocoran Kunci/*Special Requirements Related to Key Compromise*

Tidak ada ketentuan.

No stipulation.

4.9.13 Kondisi untuk Pembekuan/*Circumstances for Suspension*

Tidak ada ketentuan.

No stipulation.

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

Tidak ada ketentuan.

No stipulation.

4.9.15 Prosedur untuk Permintaan Pembekuan/*Procedure for Suspension Request*

Tidak ada ketentuan.

No stipulation.

4.9.16 Batas Masa Pembekuan/*Limits on Suspension Period*

Tidak ada ketentuan.

No stipulation.

4.10 Layanan Status Sertifikat Elektronik/*Electronic Certificate Status Services*

4.10.1 Karakteristik Operasional/*Operational Characteristics*

Status Sertifikat Elektronik publik tersedia dalam CRL di repositori atau responder OCSP.

The status of public Electronic Certificates are available from CRL's in the repositories or an OCSP responder.

4.10.2 Ketersediaan Layanan/*Service Availability*

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

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

4.10.3 Fitur Opsional/*Optional Features*

Tidak ada ketentuan.

No stipulation.

4.11 Akhir Berlangganan/*End Of Subscription*

Pemilik dapat mengakhiri langganan dengan membiarkan Sertifikat Elektroniknya kedaluwarsa atau mencabut Sertifikat Elektroniknya tanpa meminta Sertifikat Elektronik yang baru. Terdapat prosedur pencabutan Sertifikat Elektronik pada Peruri CA.

Subscriber may end a subscription by allowing its Electronic Certificate to expire or revoking its Electronic Certificate without requesting a new Electronic Certificate. There is an Electronic Certificate revocation procedure at Peruri CA.

4.12 Pemulihan Dan Eskro Kunci/*Escrow And Recovery*

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

Kunci Privat Peruri CA dan Kunci Privat Pemilik yang terasosiasi dengan Sertifikat Elektronik yang berisi key *usage digital Signature* tidak dieskro.

Peruri CA's Private Key and Subscriber's Private Key associated with an Electronic Certificate that asserts a digitalSignature key usage are not escrowed.

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

Tidak ada ketentuan.

No stipulation.

SECTION 5

Fasilitas, Manajemen, Dan Kendali Operasi/*Facility, Management, And Operational Controls*

5.1 Kendali Fisik/*Physical Controls*

5.1.1 Lokasi dan Konstruksi/*Site Location and Construction*

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

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

Sistem cadangan Peruri CA disiapkan di *Data Center* (DC) cadangan (yaitu DC yang difungsikan sebagai *Disaster Recovery Center* (DRC)), dan mampu memulihkan layanan sistem ketika terjadi kegagalan di DC utama.

The Peruri CA backup system is set up in a backup Data Center (DC) (ie a DC that functions as a Disaster Recovery Center (DRC)), and is capable of restoring system services when a failure occurs at the main DC.

DRC berada di lokasi yang ketika terjadi bencana alam pada DC utama, DRC tidak ikut terkena dampaknya.

DRC is in a location where when a natural disaster occurs in the main DC, DRC is not affected.

Lokasi fisik DC dan DRC berada di Indonesia. Peruri CA telah mengukur risiko untuk menentukan jarak antara DC dan DRC yang mempertimbangkan *availability* layanan Peruri CA.

The physical location of DC and DRC is in Indonesia. Peruri CA has measured the risk to determine the distance between DC and DRC by considering the availability of Peruri CA services.

5.1.2 Akses Fisik/*Physical Access*

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

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

1. Memastikan tidak ada akses tidak resmi yang diizinkan ke perangkat keras;
2. Menyimpan semua media dan kertas yang berisi informasi teks yang bernilai tinggi dan sensitif dalam media yang aman;
3. Monitor, baik secara manual maupun elektronik, untuk gangguan yang tidak sah setiap saat;
4. Menjaga dan memeriksa log akses secara berkala; dan
5. Menerapkan kendali akses fisik dua orang untuk modul kriptografis dan sistem komputer PSrE.

1. *Ensure no unauthorized access to the hardware is permitted;*
2. *Store all media and paper containing high-value and sensitive textual information in secure media;*
3. *Monitor, either manually or electronically, for unauthorized intrusion at all times;*
4. *Maintain and periodically inspect an access log; and*
5. *Implement two-person physical access control to CA's cryptographic modules and computer systems.*

Semua operasional Peruri CA yang sangat penting dan memiliki risiko tinggi dilakukan di dalam fasilitas yang aman dengan memiliki setidaknya empat lapis keamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif. Fasilitas tersebut terpisah secara fisik dari fasilitas organisasi yang lain. Hanya Peran Terpercaya Peruri CA yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

All Peruri CA operations which are very important and have a high risk are carried out in a secure facility with at least four layers of security to be able to access sensitive hardware and software. The facility is physically separated from other organizational facilities. Only Peruri CA Trusted Roles who have the authority can access the facility.

Modul kriptografis yang *removable* dinonaktifkan

Removable cryptographic modules are deactivated

sebelum disimpan. Ketika tidak digunakan, modul kriptografis yang *removable*, informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografis harus ditempatkan pada tempat penyimpanan yang aman.

before being stored. When not in use, the removable cryptographic module, the activation information used to access or activate the cryptographic module must be placed in a secure storage area.

Data untuk aktivasi diingat atau dicatat dan disimpan dengan pengamanan yang setara dengan pengamanan yang disediakan modul kriptografis, dan tidak disimpan bersamaan dengan modul kriptografis.

Data for activation is remembered or recorded and stored with security equivalent to that provided by the cryptographic module, and is not stored together with the cryptographic module.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat Peruri CA dilaksanakan jika fasilitas akan ditinggalkan. Pemeriksaan memverifikasi hal-hal berikut:

A security check of the facility housing the Peruri CA equipment occurs if the facility is to be left unattended. The check verifies the following:

1. Semua perangkat luring dimatikan;
2. Semua *security container* (brankas) sudah diamankan (dikunci);
3. Sistem keamanan fisik (kunci pintu, kunci rak, kunci brankas) berfungsi dengan baik; dan
4. Area diamankan dari akses yang tidak berhak.

1. *All devices are turned off.*
2. *Any security containers are properly secured (locked)*
3. *Physical security systems (e.g., door locks, rack locks, safe locks) are functioning properly; and*
4. *The area is secured against unauthorized access.*

Peran Terpercaya ditunjuk untuk melakukan pemeriksaan di atas. Pemeriksaan tersebut dibuktikan dengan log yang dapat dipertanggungjawabkan. Ketika fasilitas tidak ditempati, maka personel terakhir yang meninggalkan fasilitas harus memiliki log yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

Trusted Roles are appointed for making such checks. The check is proven by reliable logs. When the facility is not occupied, the last personnel to depart the facility shall have a log showing the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Listrik dan AC/*Power and Air Conditioning*

Peruri CA memiliki daya listrik cadangan yang cukup ketika listrik utama mati, dan menyelesaikan setiap aksi yang tertunda, dan merekam

Peruri CA has sufficient backup power when the main power fails, and completes any pending actions, and records the status of the device before a

status perangkat sebelum kekurangan daya atau AC yang menyebabkan *shutdown*. Fasilitas Peruri CA telah dilengkapi dengan *uninterrupted power* dan generator listrik yang cukup untuk pengoperasian minimal 6 (enam) jam tanpa adanya listrik/daya dari PLN, untuk mendukung kelangsungan operasi.

lack of power or AC causes shutdown. The Peruri CA facility has been equipped with uninterrupted power and sufficient electric generators to operate for a minimum of 6 (six) hours without electricity/power from PLN, to support continuity of operations.

5.1.4 Keterpaparan Air/*Water Exposures*

Peralatan Peruri CA ditempatkan pada tempat yang tidak terpapar air.

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

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

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

5.1.5 Pencegahan dan Perlindungan Kebakaran/*Fire Prevention and Protection*

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

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

5.1.6 Media Penyimpanan/*Media Storage*

Media penyimpanan 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 DC/DRC Peruri CA.

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

5.1.7 Pembuangan Limbah/*Waste Disposal*

Dokumen yang mengandung informasi sensitif dihancurkan sampai tidak dapat direkonstruksi kembali.

Documents containing sensitive information will be destroyed until they could not be reconstructed.

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

All sensitive information contained on items that are no longer in use are destroyed prior to disposal.

Seluruh informasi dalam perangkat kriptografi yang sudah tidak digunakan dihapus, lalu perangkat kriptografi tersebut dihancurkan fisiknya sampai tidak dapat digunakan kembali sebelum dibuang.

All information on a cryptographic device that is no longer in use is deleted, then the cryptographic device is physically destroyed until it cannot be used again before being disposed of.

Tata cara pembuangan limbah diatur dalam prosedur terkait penghancuran informasi dan media.

Procedures for waste disposal are regulated in the procedure regarding the destruction of information and media.

5.1.8 Backup Off-Site/*Off-Site Backup*

Backup off-site sistem dari Peruri CA cukup untuk memulihkan kegagalan sistem, yang dilakukan secara berkala dan telah dijelaskan pada CPS ini. *Backup off-site* data dilakukan dan disimpan di luar lokasi tidak kurang dari sekali setiap 7 (tujuh) hari. Setidaknya 1 (satu) salinan *backup* lengkap disimpan. Hanya *backup* lengkap terbaru yang perlu dipertahankan. Data *backup* dilindungi dengan kendali fisik dan kontrol prosedur.

Off-site backup from Peruri CA's system is sufficient to restore system failures, which is done regularly and has been explained in this CPS. Off-site backup data is performed and stored off-site not less than once every 7 (seven) days. At least 1 (one) full backup copy is kept. Only the most recent full backup should be maintained. Backup data is protected by physical controls and procedural controls.

Backup off-site berada di lokasi yang ketika terjadi bencana alam baik pada DC dan DRC, *backup off-site* tidak ikut terkena dampaknya.

Off-site backups are in locations where when natural disasters occur on both DC and DRC, off-site backups are not affected.

5.2 Kendali Prosedur/*Procedural Controls*

5.2.1 Peran Terpercaya/*Trusted Roles*

Peran Terpercaya meliputi:

1. *Head of Peruri CA*
   Bertanggung jawab secara keseluruhan dalam operasional Peruri CA.
2. *Policy Authority*
   Bertanggung jawab dalam memastikan Peruri CA berjalan sesuai regulasi yang berlaku serta sesuai dengan CPS Peruri CA yang sudah selaras dengan CP milik PSrE Induk.

Trusted Roles include:

1. *Head of Peruri CA*
   Responsible for overall operations of Peruri CA.
2. *Policy Authority*
   Responsible for ensuring that Peruri CA runs in accordance with applicable regulations and in accordance with Peruri CA's CPS which are already in line with Root CA's CP.

3. *Policy Authority Officer*
   Bertanggung jawab membantu *Policy Authority* dalam menjalankan tugasnya.
4. *Internal Auditor*
   Bertanggung jawab menentukan ruang lingkup audit internal dan rencana audit tahunan.
5. *Administrator Application (RA, VA, and TSA)*
   Bertanggung jawab melakukan dan menjaga administrasi RA, VA, dan TSA.
6. *Verificator Team*
   Bertanggung jawab melakukan kegiatan *Know Your Customer* (manual KYC) sesuai dengan prosedur.
7. *Share Holder Manager*
   Menjalankan peran sebagai salah satu pemegang (*custodianship*) perlengkapan aktivasi Peruri CA.
8. *Administrator Application of CA*
   Melakukan kegiatan operasional dan pemeliharaan terhadap sistem Infrastruktur Kunci Publik (IKP) yang terkait dengan CA.
9. *Administrator of Network*
   Menjamin ketersediaan jaringan dan sumberdaya dalam seluruh sistem IKP Peruri CA.
10. *Security Officer*
    Bertanggung jawab terhadap keamanan fisik, logikal, dan jaringan pada operasional Peruri CA.
11. *Administrator of Repository*
    Bertanggung jawab terhadap penempatan dan publikasi Sertifikat Elektronik Peruri CA, *Certificate Practice Statement*(CPS),

3. *Policy Authority Officer*
   Responsible for assisting Policy Authority in carrying out its duties.
4. *Internal Auditor*
   Responsible for determining the scope of the internal audit and the annual audit plan
5. *Administrator Application (RA, VA, and TSA)*
   Responsible for conducting and maintaining RA, VA, and TSA administration.
6. *Verificator Team*
   Responsible for carrying out Know Your Customer (manual KYC) activities in accordance with procedures
7. *Share Holder Manager*
   Carrying out the role as one of the holders (custodianship) of Peruri CA activation equipment.
8. *Administrator Application of CA*
   Perform operational and maintenance activities on the Public Key Infrastructure (PKI) system related to CA.
9. *Administrator of Network*
   Ensuring the availability of networks and resources in all Peruri CA PKI systems.
10. *Security Officer*
    Responsible for physical, logical, and network security in Peruri CA operations.
11. *Administrator of Repository*
    Responsible for the placement and publication of the Peruri CA Electronic Certificate, Certificate Practice Statement (CPS),

Subscriber Agreement, Privacy Policy, Relying Party Agreement, dan *Warranty Policy* pada situs repository.

12. *Administrator of Operating System*
    Bertanggung jawab terhadap administrasi sistem operasi dalam seluruh sistem IKP.
13. *Administrator of Appliance and HSM*
    Bertanggung jawab terhadap administrasi Perangkat Keras dan HSM dalam seluruh sistem IKP.
14. *Support Team*
    Memberikan masukan bagi *Administrator Application* (RA, VA, dan TSA), *Administrator Application of CA, Network and Security, Administrator of Appliance* and HSM, *Administrator of Repository, Administrator of Operating System, Administrator of Repository* dalam menjalankan tugasnya.

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

Subscriber Agreement, Privacy Policy, Relying Party Agreement, and Warranty Policy on the repository site.

12. *Administrator of Operating System*
    Responsible for Operating System administration in the entire PKI system.
13. *Administrator of Appliance and HSM*
    Responsible for hardware and HSM administration in the entire PKI system.
14. *Support Team*
    Provide input for Application Administrators (RA, VA, and TSA), Application Administrators of CA, Network and Security, Administrators of Appliance and HSM, Administrators of Repositories, Administrators of Operating Systems, Administrators of Repositories in carrying out their duties.

Other Trusted Roles may be defined in other documents, which describe or impose requirements on Peruri CA operation.

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

Untuk kegiatan yang memerlukan kendali multi-pihak, semua partisipan memegang Peran Terpercaya. Kendali multi-pihak tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan 2 (dua) orang atau lebih:

1. Pembuatan kunci Peruri CA;
2. Penandatanganan Sertifikat Elektronik Peruri CA;
3. Pencabutan Sertifikat Elektronik Peruri CA; dan

Where multi-party control is required, all participants shall hold a Trusted Role. Multi-party control shall not be achieved using personnel that serve in an Internal Auditor role with the exception of audit functions. The following tasks requires two or more persons:

1. *Peruri CA key generation;*
2. *Peruri CA key signing;*
3. *Peruri CA Electronic Certificate Revocation; and*

4. Pencadangan kunci Peruri CA.

4. *Peruri CA key backup.*

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

Semua individu yang ditugaskan dalam Peran Terpercaya merupakan karyawan Peruri yang telah diidentifikasi dan diautentikasi, kemudian diberikan mandat melalui Surat Penugasan atau Surat Keputusan.

All individuals assigned to the Trusted Roles are Peruri employees who have been identified and authenticated, then given a mandate through an Assignment Letter or Decree.

Autentikasi Peran Terpercaya dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi tersebut dilakukan berdasarkan identifikasi orang yang mengakses ruangan atau sistem dan hak akses yang diatur sesuai dengan peran dan tanggung jawab orang tersebut.

Trusted Roles authentication is performed through physical access controls and system-level access controls. Authentication is carried out based on the identification of the person accessing the room or system and access rights which are regulated according to the person's role and responsibilities.

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

Setiap personel Peruri CA disusun secara khusus untuk peran yang telah ditentukan pada bagian 5.2.1

Individual Peruri CA personnel are specifically designated to roles defined in section 5.2.1 of this CPS.

Ketentuan mengenai pemisahan tugas Peran Terpercaya lebih lanjut diatur dalam Panduan Seremoni Pembangkitan Kunci (*Key Generation Ceremony*).

Trusted Roles segregation of duties are further stipulated in the Key Generation Ceremony Guidelines.

5.3 Kendali Personel/*Personnel Controls*

5.3.1 Persyaratan Kualifikasi, Pengalaman, dan Penugasan/*Qualification, Experience, and Assignment Requirements*

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

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

Personel untuk Peran Terpercaya secara resmi ditunjuk oleh Direksi Peruri.

Personnel for Trusted Roles are officially appointed by the Board of Directors of Peruri.

5.3.2 Prosedur Pemeriksaan Latar Belakang/*Background Check Procedures*

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

1. Kontak Referensi Pekerjaan;
2. Pendidikan atau sertifikasi;
3. Identifikasi Kependudukan (KTP);
4. Surat Keterangan Catatan Kepolisian (SKCK); dan
5. Informasi finansial dari sistem pengecekan finansial yang dikeluarkan oleh otoritas yang berwenang.

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

1. *Curriculum Vitae;*
2. *Education and certification;*
3. *Residential Identification;*
4. *Police Certificate of Good Conduct; and*
5. *Financial information from the authorized Financial information system.*

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

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

5.3.3 Persyaratan Pelatihan/*Training Requirements*

Semua personil Peruri CA dilatih untuk menjalankan tugasnya. Pelatihan semacam itu membahas topik yang relevan, paling sedikit mencakup topik-topik sebagai berikut:

1. Mekanisme dan prinsip keamanan IKP/PSrE/RA;
2. Seluruh versi perangkat lunak, perangkat keras, dan sistem operasi dalam lingkup

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.

1. *Security principles and practices of PKI/CA/RA;*
2. *All softwares, hardwares, and operating systems within the scope of the CA's PKI;*

IKP yang digunakan dalam sistem PSrE/RA;

3. Seluruh kewajiban masing-masing personel terkait operasional PSrE/RA;
4. Prosedur pemulihan bencana dan keberlangsungan bisnis; dan
5. CP dan CPS yang berlaku.

Peruri CA menyimpan catatan pelatihan semua personel. Evaluasi terhadap kecukupan kompetensi personel Peruri CA dilakukan minimal 1 (satu) kali dalam setahun.

3. *Obligations of each personnel related to CA/RA;*
4. *Business continuity and disaster recovery procedures; and*
5. *The applied CP/CPS.*

Peruri CA stores all the training records of all their personnel. The adequacy of the competence of Peruri CA personnel is evaluated at least once a year.

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

Peruri CA memberikan pelatihan ulang yang sifatnya memberi penyegaran dan memutakhirkan kemampuan para personelnya sesuai tingkatan dan frekuensi pelatihan yang dibutuhkan. Hal ini dilakukan untuk memastikan bahwa personel tersebut mempertahankan kompetensi yang dipersyaratkan untuk melakukan tugas dan tanggung jawab pekerjaan secara memuaskan.

Peruri CA provides retraining which is meant to refresh and update the capabilities of its personnel according to the level and frequency of training required. This is done to ensure that these personnel maintain the competencies required to perform their job duties and responsibilities satisfactorily.

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

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

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

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

Sanksi disipliner yang sesuai diberikan pada personil yang melanggar ketentuan dan kebijakan di dalam CP, CPS, atau prosedur operasional Peruri CA.

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

5.3.7 Persyaratan Kontraktor Independen/*Independent Contractor Requirements*

Personil sub kontraktor yang dipekerjakan untuk melaksanakan fungsi-fungsi yang terkait dengan

Sub-Contractor personnel employed to perform functions pertaining to Peruri CA operations have

operasi Peruri CA telah memenuhi persyaratan yang berlaku yang diatur dalam CPS ini pada poin 5.3.1 dan 5.3.2.

complied with the applicable requirements set forth in this CPS in section 5.3.1 and 5.3.2.

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

Peruri CA menyediakan dokumen kepada para personilnya meliputi CP, CPS, setiap undang-undang yang relevan, kebijakan, kontrak yang relevan, dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

Peruri CA provides documents to its personnel including CP, CPS, all relevant laws, policies, relevant contracts, other technical, operational and administrative documents (for example, Administrator's Guide, User's Guide, etc.) provided so that trusted personnel can carry out their duties.

5.4 Prosedur Log Audit/*Audit Logging Procedures*

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

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

5.4.1 Jenis Kejadian yang Direkam/*Types of Events Recorded*

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

1. Tipe Kejadian;
2. Nomor rekaman atau urutan rekaman;

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

1. *The type of event;*
2. *Serial or sequence number of entry;*

3. Tanggal dan waktu kejadian;
4. Asal perekaman;
5. Indikator keberhasilan atau kegagalan jika perlu; dan
6. Identitas dan entitas dan/atau operator yang menyebabkan kejadian tersebut.

Waktu diselaraskan memakai NTP untuk fasilitas yang terkoneksi dengan internet. Waktu disinkronkan dengan otoritas sumber waktu dengan ketelitian paling lama 1 (satu) menit.

3. *The date and time of the incident;*
4. *Source of entry;*
5. *A success or failure indicator, where appropriate; and*
6. *The identity of the entity and/or operator that caused the event.*

For online facilities, the time is synchronized using NTP. Time is synchronized with the time source authority with a maximum accuracy of 1 (one) minute.

5.4.2 Frekuensi Pemrosesan Log/*Frequency of Processing Log*

Log audit ditinjau sedikitnya 3 (tiga) bulan sekali, termasuk verifikasi bahwa log tersebut tidak dirusak, tidak ada diskontinuitas atau hilangnya data audit, dan kemudian secara singkat memeriksa semua entri log, dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan dalam log.

Audit logs were reviewed every 3 (three) months including verification that the log has not been tampered with, there is no discontinuity or other loss of audit data, and brief inspection of all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Tindakan yang diambil sebagai hasil dari peninjauan ini didokumentasikan.

Actions taken as a result of these reviews were documented.

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

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

Peruri CA audit log were retained for 1 (one) year in order to be available for any lawful control. This period may be modified depending on developments of relevant laws.

5.4.4 Proteksi Log Audit/*Protection of Audit Log*

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

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

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

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

Sistem dapat menimpa (*overwrite*) log audit setelah log audit tersebut di-*backup*.

The system may overwrite audit logs after they have been backed up.

5.4.5 Prosedur Backup Log Audit/*Audit Log Backup Procedures*

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

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

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

Sistem pengumpulan log audit adalah internal ke sistem Peruri CA. Pengumpulan log audit eksternal tidak berlaku.

The audit log collection systems were internal to the Peruri CA system. The external audit log collection systems were not applicable.

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

Tidak ada ketentuan.

No stipulation.

5.4.8 Asesmen Kerentanan/*Vulnerability Assessments*

Peruri CA melaksanakan asesmen kerentanan sistem atau komponennya 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem Peruri CA. Dalam hal terdapat temuan pada saat asesmen kerentanan, Peruri CA memperbaiki temuan tersebut.

Peruri CA conducts a vulnerability assessment of the system or its components once a year or when there is a significant change in the Peruri CA system. In the event that there are findings during the vulnerability assessment, Peruri CA corrects these findings.

Uji penetrasi ke sistem Peruri CA dilakukan minimal 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem Peruri CA.

Penetration tests into the Peruri CA system are carried out at least once a year or when significant changes occur to the Peruri CA system.

Asesmen kerentanan dan uji penetrasi sistem dilakukan pada sistem yang terkoneksi ke internet.

Vulnerability assessments and system penetration tests are performed on systems connected to the internet.

5.5 Pengarsipan Catatan/*Records Archival*

5.5.1 Tipe Catatan yang Diarsipkan/*Types of Records Archived*

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

1. Siklus hidup Sertifikat Elektronik termasuk permohonan Sertifikat Elektronik, permintaan pencabutan Sertifikat Elektronik, dan permintaan *re-key*;
2. Semua Sertifikat Elektronik dan CRL yang telah diterbitkan atau dipublikasikan oleh Peruri CA;
3. Data konfigurasi sistem Peruri CA;
4. Dokumen CP dan CPS, termasuk juga segala modifikasi dan amendemen terhadap dokumen tersebut;
5. Data audit; dan
6. Data pendukung Sistem Manajemen Pengamanan Informasi (SMPI):
    - Penunjukan dan pencabutan peran dan kewenangan;
    - Akses pengunjung ke fasilitas Peruri CA;
    - Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
    - Deteksi dan tindakan terhadap insiden keamanan;
    - Latihan keadaan darurat;
    - Tindakan dan penilaian risiko;

Peruri CA's archival records are detailed enough to determine the correct operation of the CA and the validity of any Electronic Certificate (including revoked or expired) issued by Peruri CA. The following data is recorded on the archive:

1. *The Electronic Certificate life cycle includes Electronic Certificate requests, Electronic Certificate revocation requests, and re-key requests;*
2. *All Electronic Certificates and CRLs that have been issued or published by Peruri CA;*
3. *Peruri CA system configuration data;*
4. *CP and CPS documents, including all modifications and amendments to these documents;*
5. *Audit data; and*
6. *Supporting data for the Information Security Management System (ISMS):*
    - *Assignment and withdrawal of rolesand privileges;*
    - *Visitor access to Peruri CA facilities;*
    - *Change and maintenance of system hardware and software;*
    - *Detection and action against security incidents;*
    - *Emergency drills;*
    - *Risk assessment and treatment;*

- Perubahan aset, prosedur, dan tanggung jawab; dan
- Perubahan dokumentasi.

- *Changes in assets, procedures and responsibilities; And*
- *Changes of documentation.*

5.5.2 Periode Retensi Arsip/*Retention Period for Archive*

Catatan yang diarsipkan disimpan setidaknya selama 5 (lima) tahun. Perangkat lunak dan perangkat keras yang dibutuhkan untuk membaca arsip ini dipelihara selama masa retensi.

Archived records are kept for at least 5 (five) years. Software and hardware required to read these files must be maintained throughout the retention period.

5.5.3 Perlindungan Arsip/*Protection of Archive*

Catatan yang diarsipkan dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan arsip dan aplikasi yang dibutuhkan untuk memproses catatan arsip dipelihara dan dilindungi.

The archived records were protected against unauthorized viewing, modification, deletion, or tampering. The media holding the archive records and the applications required to process the archive records will be maintained and protected.

Muatan arsip tidak boleh diungkap kecuali berdasarkan ketentuan pada Bagian 9.3 dan 9.4. Catatan dari transaksi individu boleh diungkap berdasarkan permintaan dari Pemilik yang terlibat dalam transaksi atau berdasarkan permintaan dari agen Pemilik yang dikenali oleh hukum.

The contents of the archive shall not be released except in accordance with Sections 9.3 and 9.4. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally recognized agents.

5.5.4 Prosedur Backup Arsip/*Archive Backup Procedures*

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

Adequate and regular backup procedures are in place so that in the event of loss or destruction of the primary archives, a complete set of backup copies held in a separate location is available in accordance with the Backup Management SOP.

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

Catatan arsip Peruri CA diberikan penanda waktu/*timestamp* secara otomatis.

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

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

Dilakukan oleh internal Peruri CA sendiri. Peruri CA tidak mengumpulkan arsip eksternal.

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

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

Media penyimpanan informasi arsip Peruri CA diperiksa setelah dibuat. Sedikitnya 1 (satu) kali dalam setahun, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya Peruri CA, Peran Terpercaya dan pihak-pihak lain yang berwenang yang diizinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada Peran Terpercaya.

Peruri CA archive information storage media are checked after they are created. Periodically, samples of archival information are tested to check the integrity and readability of the information. Only Peruri CA, Trusted Roles and other authorized parties are allowed to access the archives. Requests to obtain and verify archive information are coordinated by operators in Trusted Roles.

5.6 Pergantian Kunci/*Key Changeover*

Untuk meminimalkan risiko dari kebocoran Kunci Privat Peruri CA, Kunci Privat dapat diubah secara berkala setiap sepuluh (10) tahun atau jika ada kebutuhan khusus apabila ada risiko kebocoran kunci. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat Elektronik.

To minimize the risk of Peruri CA's private key leak, the Private Key can be changed periodically every ten (10) years or if there is a special need if there is a risk of key leakage. From that time on, only the new Key Private shall be used for Electronic Certificate signing purposes.

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

The older, but still valid, Electronic Certificate will be available to verify old signatures until all of the Electronic Certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

Apabila Peruri CA memperbarui Kunci Privat dan menghasilkan Kunci Publik baru, Peruri CA memberitahu semua Pemilik Sertifikat Elektronik yang mengandalkan Sertifikat Elektronik Peruri

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

CA bahwa telah terjadi perubahan melalui surel atau situs web.

Peruri CA tidak membangkitkan (*generate*) Sertifikat Elektronik Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat Elektronik Peruri CA. Dengan demikian, pasangan kunci Peruri CA dibangkitkan lagi paling lambat pada saat Sertifikat Elektronik Peruri CA kedaluwarsa dikurangi masa berlaku Sertifikat Elektronik Pemilik.

Peruri CA does not generate the Subscriber's Electronic Certificate whose validity period exceeds the validity period of the Peruri CA Electronic Certificate. Thus, the Peruri CA key pair are regenerated no later than when the Peruri CA Electronic Certificate expires minus the validity period of the Subscriber's Electronic Certificate.

5.7 Pemulihan Bencana Dan Kebocoran/*Compromise And Disaster Recovery*

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

Peruri CA memiliki rencana tanggap darurat dan rencana pemulihan bencana.
Apabila dicurigai telah terjadi kebocoran kunci Peruri CA, penerbitan Sertifikat Elektronik oleh Peruri CA dihentikan seketika. Investigasi independen oleh pihak ketiga dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup dari kerusakan dinilai untuk menentukan prosedur perbaikan yang tepat. Apabila Kunci Privat Peruri CA dicurigai mengalami kebocoran, prosedur pada bagian 5.7.3 diikuti.

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 investigation by a third party was carried out to determine the nature and extent of the damage. The scope of potential damage shall be assessed in order to determine appropriate remediation procedures. If Peruri CA's private signing key is suspected of compromise, the procedures outlined in section 5.7.3 shall be followed.

Peruri CA menginformasikan PSrE Induk apabila mengalami insiden, termasuk namun tidak terbatas pada:

1. Terdeteksinya atau adanya indikasi sistem Peruri CA terkompromi;
2. Adanya upaya untuk menembus sistem Peruri CA, baik secara fisik maupun elektronik;
3. Serangan *Denial of Service* pada sistem Peruri CA;

Peruri CA informs the Root CA if it experiences an incident, including but not limited to:

1. *Suspected or detected compromise of Peruri CA system;*
2. *There are attempts to penetrate the Peruri CA system, both physically and electronically;*
3. *Denial of Service attack on the Peruri CA system;*

4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam *field "next update"* pada CRL yang valid saat ini. Peruri CA segera memulihkan penerbitan CRL secepat mungkin; dan/atau

4. *Any incident that prevents or hinders the issuance of a CRL within 24 (twenty four) hours from the time specified in the "next update" field on the currently valid CRL. Peruri CA immediately restores CRL issuance as quickly as possible; and/or*

5. CRL dan/atau OCSP responder tidak dapat diakses oleh publik.

5. *The CRL and/or OCSP responder is not accessible to the public.*

Prosedur diperbarui secara berkala sedikitnya 1 (satu) kali dalam setahun atau sesuai kebutuhan.

Procedures are updated periodically at least 1 (one) time a year of as needed.

Semua sistem pencadangan/pemulihan diuji minimal setahun sekali.

All backup/restore systems are tested at least once a year.

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

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

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

1. Memberitahu *Policy Authority* dan PSrE Induk sesegera mungkin;

1. *Notify Policy Authority and Root CA as soon as possible;*

2. Jika Kunci Privat Peruri CA masih tetap berfungsi dan tidak mengalami kerusakan, maka:

2. *If the Peruri CA Private Key is still functional and not damaged, then:*

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

    - *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;*

    - Mengoperasikan kembali Peruri CA, memprioritaskan kemampuan membangkitkan informasi status Sertifikat Elektronik untuk penerbitan CRL sesuai jadwal.

    - *Re-establish Peruri CA operations, giving priority to the ability to generate Electronic Certificate status information within the CRL issuance schedule.*

Jika kemampuan untuk membangkitkan informasi status Sertifikat Elektronik tidak beroperasi atau rusak, Peruri CA memulihkan kemampuan untuk membangkitkan informasi status Sertifikat Elektronik sesegera mungkin. Jika kemampuan Peruri CA untuk membangkitkan informasi status Sertifikat Elektronik tidak bisa dipulihkan dalam jangka waktu yang wajar, Peruri CA kemudian menentukan apakah perlu untuk meminta pencabutan Sertifikat Elektronik Peruri CA kepada PSrE Induk.

If the ability to generate Electronic Certificate status information is inoperative or damaged, Peruri CA restores the ability to generate Electronic Certificate status information as soon as possible. If Peruri CA's ability to generate Electronic Certificate status information cannot be restored within a reasonable period of time, Peruri CA then determines whether it is necessary to request revocation of the Peruri CA Electronic Certificate from the Parent PSrE.

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

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

Jika DC dan DRC tidak dapat memulihkan kemampuan pencabutan Sertifikat Elektronik dalam jangka waktu yang wajar, maka sistem Peruri CA akan diperlakukan sebagai PSrE terkompromi.

If DC and DRC are unable to restore Electronic Certificate revocation capabilities within a reasonable time, then the Peruri CA system will be treated as a compromised CA.

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

Dalam kasus terjadi kehilangan Kunci Privat atau terjadi kebocoran/kompromi terhadap parimeter yang digunakan untuk membangkitkan Kunci Privat dan Sertifikat Elektronik, semua Sertifikat Elektronik yang terkait dicabut oleh Peruri CA dan kunci serta Sertifikat Elektronik baru diterbitkan tanpa menghentikan layanan.

In case of loss of Private Keys or leakage/compromise of the parameters used to generate Private Keys and Electronic Certificates, all related Electronic Certificates are revoked by Peruri CA and new keys and Electronic Certificates are issued without stopping the service.

Bila Kunci Privat Peruri CA hilang, terjadi kebo-

If the Peruri CA Private Key is lost, there is a leak/-

coran/kompromi, atau terindikasi terjadi kebocoran/kompromi, Peruri CA akan:

1. Memberitahu PSrE Induk sesegera mungkin agar dapat melakukan pencabutan Sertifikat Elektronik;
2. Memberitahu semua Pemilik;
3. Mencabut Sertifikat Elektronik Pemilik yang terkait dengan Kunci Privat yang terkompromi tersebut;
4. Menerbitkan suatu CRL akhir; dan
5. Infrastruktur Kunci Publik akan disiapkan lagi dengan membangkitkan Pasangan Kunci Peruri CA yang baru.

Peruri CA segera meminta penerbitan Sertifikat Elektronik baru kepada PSrE Induk.

Penerbitan ulang Kunci Privat Pemilik akibat terkompromi dapat dilakukan Pemilik dengan mengajukan permohonan Sertifikat Elektronik sebagaimana diatur pada Bagian 4.1.

Peruri CA menyelidiki penyebab kompromi atau kerugian dan tindakan yang harus diambil untuk mencegah kompromi tersebut terulang kembali.

compromise, or there are indications that a leak/-compromise has occurred, Peruri CA will:

1. *Notify the Root CA as soon as possible so that the Electronic Certificate can be revoked;*
2. *Notify all Subscribers;*
3. *Revoke the Subscribers's Electronic Certificate associated with the compromised Private Key;*
4. *Publish a final CRL; and*
5. *The Public Key Infrastructure will be prepared again by generating a new Peruri CA Key Pair.*

Peruri CA immediately requests the issuance of a new Electronic Certificate to Root CA.

Subscribers can re-issue the Subscriber's Private Key as a result of a compromise by submitting an Electronic Certificate application as regulated in Section 4.1.

Peruri CA investigates the cause of the compromise or loss and the actions that must be taken to prevent the compromise from happening again..

5.7.4 Kapabilitas Keberlangsungan Bisnis Setelah Terjadi Bencana/*Business Continuity Capabilities after a Disaster*

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

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

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

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

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

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

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

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

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan Peruri CA rusak secara fisik dan semua salinan kunci penandatangan milik Peruri CA hancur, Peruri CA akan meminta agar Sertifikat Elektronik-nya dicabut dan mengikuti ketentuan sebagaimana diatur pada bagian 5.7.3.

In the event of a disaster which results in all of Peruri CA's facilities and equipment being physically damaged and all copies of Peruri CA's signing keys being destroyed, Peruri CA will request that its Electronic Certificate be revoked and follow the provisions as stipulated in section 5.7.3.

5.8 Penutupan PSrE Atau RA/*CA or RA Termination*

Bila ada keadaan yang menyebabkan diakhirinya layanan Peruri CA dengan persetujuan *Policy Authority* dan PSrE Induk, maka Peruri CA:

1. Memberitahu Pemilik, Pengandal, dan pihak lain yang terkait dengan siklus hidup Sertifikat Elektronik melalui surel dan/atau pengumuman publik;
2. Mencabut semua Sertifikat Elektronik;
3. Menjamin agar proses pencabutan semua Sertifikat Elektronik pada saat penutupan dilakukan sampai selesai;
4. Menyimpan dalam jangka panjang in-

If there is any circumstance to terminate the services of Peruri CA with the approval of Policy Authority and Root CA, then Peruri CA:

1. *Notify the Subscribers, Relying Parties, and other parties related to the life cycle of Electronic Certificates via email and/or public announcement;*
2. *Revoke all Electronic Certificates;*
3. *Ensure that the process of revoking all Electronic Certificates at the time of termination is carried out to completion;*
4. *Keep in the long term Peruri CA and Elec-*

formasi Peruri CA dan Pemilik Sertifikat Elektronik dalam periode yang dinyatakan dalam poin 5.5.2;

5. Menyediakan dukungan hak dan kewajiban berlaku sesuai dengan perjanjian yang berlaku dan menjawab pertanyaan;
6. Menangani dengan tepat Pasangan Kunci Peruri CA dan perangkat keras yang terkait;
7. Memastikan agar layanan informasi status Sertifikat Elektronik tetap tersedia dan dipelihara selama kurun waktu tertentu setelah penutupan, termasuk jika memungkinkan, memindahkan layanan informasi status Sertifikat Elektronik kepada PSrE Indonesia lain; dan
8. Memberitahu Menteri Komunikasi dan Digital, Pengawas Penyelenggaraan Sertifikasi Elektronik (P2SE), PSrE Induk, LS PSrE, dan pihak berwenang lainnya.

Ketentuan lebih rinci terkait penutupan PSrE diatur lebih lanjut dalam prosedur mengenai penutupan PSrE Peruri CA.

tronic Certificate Subscribers information for the period stated in point 5.5.2

5. *Provide support for applicable rights and obligations in accordance with applicable agreements and answer questions;*
6. *Properly handle Peruri CA Key Pair and associated hardware;*
7. *Ensure Electronic Certificate status information services are provided and maintained for the applicable period after termination, including, if applicable, transferring Electronic Certificate status information services to another Indonesian CA; and*
8. *Notify the Minister of Communication and Digital, Root CA, CA Certification Bodies, and other relevant authorities.*

Detailed provisions regarding the closure of CA are further regulated in the procedures regarding the closure of Peruri CA.

SECTION 6

Kendali Keamanan Teknis/ *Technical Security Controls*

6.1 Pembangkitan Dan Instalasi Pasangan Kunci/*Key Pair Generation And Installation*

6.1.1 Pembangkitan Pasangan Kunci/*Key Pair Generation*

Tabel berikut berisi persyaratan minimal untuk pembangkitan Pasangan Kunci pada sistem Peruri CA.

Tabel berikut berisi persyaratan minimal untuk pembangkitan Pasangan Kunci pada sistem Peruri CA.

Entitas / *Entity*	**FIPS 140-2 Level**	**Perangkat Keras atau Perangkat Lunak (Modul Kriptografis) / *Hardware or Software***	**Dibangkitkan di dalam Modul Kriptografis / *Generated in Cryptographic Module***
Peruri CA	3	Perangkat Keras / *Hardware*	Ya / *Yes*
Time Stamp Authority	3	Perangkat Keras / *Hardware*	Ya / *Yes*
OCSP *Responder*	3	Perangkat Keras / *Hardware*	Ya / *Yes*
Pemilik untuk TTE / *Subscriber for Signature*	2	Perangkat Keras / *Hardware*	Ya / *Yes*

Kontrol multi-pihak dibutuhkan untuk pembangkitan Pasangan Kunci Peruri CA, seperti yang ditentukan pada bagian 6.2.2.

Multi-party control is required for Peruri CA Key Pair generation, as specified in section 6.2.2.

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

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

Pembangkitan Pasangan Kunci Pemilik dilakukan oleh Peruri CA atas persetujuan Pemilik dan Kunci Privat Pemilik dititipkan kepada Peruri CA.

Subscriber Key Pairs are generated by Peruri CA with Subscriber concent and the Subscriber's Private Key is entrusted to Peruri CA.

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

Peruri CA tidak melakukan pengiriman Kunci Privat kepada Pemilik.

Peruri CA does not deliver Private Keys to Subscribers.

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

Peruri CA hanya menerima Kunci Publik dalam format PKCS#10 (CSR) yang berasal dari lingkungan Peruri.

Peruri CA only accepts Public Key in PKCS#10 (CSR) format from Peruri environment.

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

Peruri CA menyediakan repositori untuk mengakses Kunci Publik Peruri CA.

Peruri CA provides a repository for accessing Peruri CA's Public Keys.

Mekanisme tersebut diamankan menggunakan TLS.

That mechanism is secured using TLS.

Penjelasan tanggung jawab tentang publikasi dan repositori Sertifikat Elektronik mengacu pada bagian 2.1.

Electronic Certificate publication and repository responsibilities are referred to section 2.1.

6.1.5 Ukuran Kunci/*Key Sizes*

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

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

Parameter kunci publik dibangkitkan dan divalidasi sesuai FIPS 186-4.

Public key parameters are generated and validated in accordance with FIPS 186-4.

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

Penggunaan kunci dibatasi oleh ekstensi *Key Usage* pada Sertifikat X.509. Semua Sertifikat Elektronik menyertakan ekstensi KeyUsage dan ditandai sebagai *Critical*.

The use of a specific key is constrained by the key usage extension in the X.509 Certificate. All Electronic Certificates include a keyUsage extension and be marked as critical.

Kunci yang terikat dengan Sertifikat Elektronik Pemilik digunakan hanya untuk menandatan-

Keys that are bound into Subscriber Electronic Certificates is used only for signing.

gani.

Kunci-kunci Peruri CA dipakai untuk penandatanganan Sertifikat Elektronik (*keyCertSign*) dan penandatanganan CRL (*cRLSign*).

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

6.2 Kendali Kunci Privat Dan Kontrol Teknis Modul Kriptografi/*Private Key Protection And Cryptographic Module Engineering Controls*

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

Peruri CA menggunakan modul kriptografi yang sudah sesuai standar FIPS untuk pembangkitan kunci Peruri CA, pembangkitan kunci Pemilik, proses penandatanganan, dan enkripsi dengan level sesuai tabel pada bagian 6.1.1.

Peruri CA uses a cryptographic module that complies with FIPS standards for Peruri CA key generation, Subscriber key generation, signing process, and encryption with levels according to the table in section 6.1.1.

Pemilik hanya dapat mengakses Kunci Privat melalui kombinasi 2 (dua) faktor autentikasi.

Subscriber can only access the Private Key through a combination of 2 (two) factors authentication.

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

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

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

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

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

Kendali multipersonel diterapkan untuk akses dan pencadangan kunci penandatanganan Sertifikat Elektronik Pemilik.

Multipersonnel control is implemented for access and backup of the Subscriber's Electronic Certificate signing keys.

Modul kriptografis yang memuat seluruh kunci penandatanganan Peruri CA tidak dapat diaktivasi atau diakses hanya oleh 1 (satu) orang. Kunci penandatanganan Peruri CA dicadangkan hanya melalui kendali multipersonel. Akses ke kunci penandatanganan Peruri CA yang dicadangkan untuk pemulihan bencana melalui kendali multipersonel. Nama-nama pihak yang terlibat dalam kendali multipersonel dicatat dalam sebuah daftar yang tersedia untuk pemeriksaan selama Audit.

The cryptographic module containing all Peruri CA signing keys cannot be activated or accessed by only 1 (one) person. Peruri CA signing keys are backed up only through multipersonnel control. Access to Peruri CA signing keys that are backed up for disaster recovery is through multipersonnel control. The names of the parties involved in the multipersonnel control are recorded in a list available for inspection during the Audit.

6.2.3 Eskro Kunci Privat/*Private Key Escrow*

Kunci Privat Peruri CA tidak dieskro. Peruri CA tidak melakukan eskro terhadap Kunci Privat Pemilik.

Peruri CA Private Key is not escrowed. Peruri CA does not escrow Subscribers Private Keys.

Kunci Privat Pemilik yang terasosiasi dengan Sertifikat Eektronik yang berisi key usage digitalSignature tidak dieskro.

Subscriber's Private Key associated with a Electronic Certificate that asserts a digitalSignature key usage is not escrowed.

6.2.4 Backup Kunci Privat/*Private Key Backup*

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

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

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

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

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

All backups of the Subscriber's Public Key accounted for and protected in the same manner as the original.

6.2.5 Pengarsipan Kunci Privat/*Private Key Archival*

Kunci Privat Peruri CA dan Kunci *Privat Signing* Pemilik tidak boleh diarsipkan.

The Peruri CA Private Key and Owner Signing Private Key must not be archived.

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

Kunci Privat Peruri CA boleh diekspor dari modul kriptografis hanya untuk melaksanakan prosedur *backup* kunci Peruri CA. Kunci Privat Peruri CA tidak pernah sekalipun boleh berada dalam bentuk *plaintext* di luar modul kriptografi. Kunci Privat Peruri CA di-*backup* sesuai ketentuan pada Bagian 6.2.4.

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 existed in plaintext outside the cryptographic module. Peruri CA Private Key is backed up according to the provisions in Section 6.2.4.

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

If a Private Key is to be transported from one cryptographic module to another, the Private Key must be encrypted during transport. Transport keys used to encrypt Private Keys will be handled in the same way as the Private Key

Ketika Peruri CA mengetahui bahwa Kunci Privat Pemilik telah disampaikan kepada orang atau entitas yang tidak berwenang dan berafiliasi dengan Pemilik tersebut, maka Peruri CA akan mencabut semua Sertifikat Elektronik yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.

When Peruri CA finds out that the Subscriber's Private Key has been communicated to an unauthorized person or entity affiliated with the Subscriber, Peruri CA will revoke all Electronic Certificates containing the Public Key associated with the Private Key that has been communicated.

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

Kunci Privat Peruri CA disimpan pada modul kriptografis FIPS 140-2 Level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi. Kunci Privat Pemilik disimpan minimal dalam perangkat FIPS 140-2 Level 2. Kunci Privat tidak dapat diakses tanpa mekanisme autentikasi.

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

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

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

Activation of Peruri CA's Private Key operations is performed by authorized person and requires multiparty control as specified in section 5.2.2.

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

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

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

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

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

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

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

Ketika Peruri CA tidak lagi beroperasi Kunci Privat Peruri CA tersebut dihapus dari modul kriptografis.

When Peruri CA is no longer operational, its Private Keys are removed from the cryptographic module.

Penonaktifan Kunci Privat Pemilik dilakukan dengan cara Pemilik melakukan logout akun.

Deactivating the Subscriber's Private Key is carried out by the Subscriber logging out of the account.

6.2.10 Metode Penghancuran Kunci Privat/*Method of Destroying Private Key*

Kunci Privat Peruri CA dihancurkan oleh para individu dalam Peran Terpercaya ketika Kunci Privat tidak diperlukan lagi, atau Sertifikat Elektronik yang terkait dengan Kunci Privat tersebut dicabut, atau kedaluwarsa. Penghancuran Kunci Privat dari modul kriptografi dan *backup*-nya dilakukan dengan menimpa Kunci Privat atau menginisialisasi modul dengan fungsi *factory reset* dari modul kriptografi sehingga tidak ada lagi informasi yang dapat digunakan untuk memulihkan Kunci Privat. Jika fungsi-fungsi atau perintah dalam modul kriptografis tidak dapat diakses untuk menghancurkan kunci yang ada di dalam modul kriptografis tersebut, maka

Peruri CA Private Keys are destroyed by individuals in Trusted Roles when the Private Key is no longer needed, or the Electronic Certificate associated with the Private Key is revoked, or expires. Destruction of the Private Key from a cryptographic module and its backups is accomplished by overwriting the Private Key or initializing the factory reset function of the cryptographic module so that no information can be used to recover the Private Key. If the functions or commands within the cryptographic module are not accessible to destroy the keys contained within the cryptographic module, then the cryptographic module will be physically destroyed. The destruction process is carried out in

modul kriptografis tersebut akan dihancurkan secara fisik. Proses penghancuran dilakukan pada lingkungan fisik yang aman.

a secure physical environment.

Saat Kunci Privat Pemilik yang sudah tidak diperlukan lagi, sudah melebihi batas masa pakai, atau Sertifikat Elektronik dicabut, Peruri CA melakukan penghancuran Kunci Privat Pemilik dengan menimpa lalu menghapusnya dari media penyimpanan.

When the Subscriber's Private Key is no longer needed, has exceeded its expiration date, or the Electronic Certificate is revoked, Peruri CA destroy the Subscriber's Private Key by overwriting and then deleting it from the storage media.

Peruri CA memiliki prosedur yang mengatur terkait penghancuran kunci Peruri CA.

Peruri CA has procedures regarding the destruction of Peruri CA's key.

6.2.11 Pemeringkatan Modul Kriptografis/*Cryptographic Module Rating*

Seperti diuraikan dalam bagian 6.2.1.

As described in section 6.2.1.

6.3 Aspek Lain Dari Manajemen Pasangan Kunci/*Other Aspects Of Key Pair Management*

6.3.1 Pengarsipan Kunci Publik/*Public Key Archival*

Kunci Publik diarsipkan setidaknya selama 5 (lima) tahun sebagai bagian dari pengarsipan Sertifikat Elektronik. Rincian tentang pengarsipan diatur pada bagian 5.5.

The Public Key is archived for at least 5 (five) years as part of the Electronic Certificate archival. Details on archival are described in section 5.5.

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

Periode operasi Pasangan Kunci sama dengan periode operasional Sertifikat Elektronik yang terkait. Jangka waktu operasional maksimum Pasangan Kunci ditentukan sebagai berikut:

The Key Pair operational period is the same as the operational period of the corresponding digital certificate. The maximum operational period of a Key Pair is determined as follows:

Kunci / *Key*	**Algoritma / *Algorithm***			
	2048 *Bit Keys* (RSA)		**4096 *Bit Keys* (RSA)**	
	Kunci Privat / *Private Key*	**Sertifikat / *Certificate***	**Kunci Privat / *Private Key***	**Sertifikat / *Certificate***
Peruri CA	N/A	N/A	10 tahun / 10 *years*	10 tahun / 10 *years*
Time Stamp Authority	2 tahun / 2 *years*	2 tahun / 2 *years*	N/A	N/A
OCSP *Responder*	2 tahun / 2 *years*	2 tahun / 2 *years*	N/A	N/A
Pemilik untuk TTE / *Subscriber for Signature*	1 tahun / 1 *year*	1 tahun / 1 *year*	N/A	N/A

6.4 Aktivasi Data/*Data Activation*

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

Pembangkitan dan penggunaan data aktivasi Peruri CA untuk mengaktifkan Kunci Privat Peruri CA dibuat pada saat *key ceremony* (merujuk pada Bagian 6.1.1). Aktivasi data dibuat secara otomatis oleh HSM yang sesuai dan dikirimkan ke *shareholder*, dimana *shareholder* tersebut merupakan orang yang memiliki Peran Terpercaya.

Generation and use of Peruri CA activation data used to activate Peruri CA Private Keys are made during a key ceremony (refer to Section 6.1.1). Data activation is created automatically by the appropriate HSM and sent to the shareholder, where the shareholder is a person who has a Trusted Role.

Data aktivasi untuk mengaktifkan Kunci Privat dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan.

Activation data to activate the Private Key is protected based on the security level appropriate to the cryptographic module used.

Jika data aktivasi harus ditransmisikan, transmisi tersebut dilakukan melalui saluran yang dilindungi dengan perlindungan yang sesuai dan dapat diketahui tempat dan waktu transmisi dari modul kriptografis yang terasosiasi dengan data aktivasi tersebut.

If activation data must be transmitted, such transmission is carried out over a channel protected by appropriate protection and the place and time of transmission can be known from the cryptographic module associated with the activation data.

Penggunaan data aktivasi Kunci Privat Pemilik harus dimasukkan oleh Pemilik saat aktivasi.

Use of the Subscriber's Private Key activation data must be entered by the Subscriber during activation.

6.4.2 Perlindungan Data Aktivasi/*Activation Data Protection*

Data aktivasi Kunci Privat Peruri CA dilindungi dari pengungkapan kerahasiaan melalui kombinasi antara kriptografi dan mekanisme kendali akses fisik. Data aktivasi Kunci Privat Peruri CA disimpan dalam token fisik.

Peruri CA Private Key activation data is protected from confidentiality disclosure through a combination of cryptography and physical access control mechanisms. Peruri CA Private Key activation data is stored in a physical token.

Token fisik dapat diakses menggunakan kata sandi yang dihafal. Catatan tulisan kata sandi diamankan pada tingkat yang setara dengan pengamanan modul kriptografis dan tidak disimpan bersama dengan modul kriptografis.

Physical token can be accessed using a memorized password. Password writing records are secured at a level equivalent to that of the cryptographic module and are not stored together with the cryptographic module.

Setelah mengalami kegagalan *login* sebanyak 3 (tiga) kali, akun tersebut terkunci sementara.

After experiencing login failure 3 (three) times, the account was temporarily locked.

Pemilik harus selalu menjaga kerahasiaan data aktivasi.

Subscribers are obliged to keep the activation data secret at all times.

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

Tidak ada ketentuan.

No stipulation.

6.5 Kendali Keamanan Komputer/*Computer Security Controls*

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

Peruri CA memastikan bahwa sistem yang menjaga perangkat lunak Peruri CA dan file data aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem Peruri CA telah dikonfigurasi dan dikeraskan/dikuatkan menggunakan praktik terbaik industri. Peruri CA menyertakan fungsionalitas berikut:

Peruri CA ensures that the systems maintain Peruri CA software and data files are secure from unauthorized access. All computers that are part of the Peruri CA system have been configured and hardened using industry best practices. Peruri CA includes the following functionality:

1. Mewajibkan login terautentikasi bagi Peran Terpercaya;
2. Menyediakan kendali akses dengan kewenangan yang minimal;
3. Menyediakan kapabilitas audit keamanan

1. *Require authenticated logins for Trusted Roles;*
2. *Provide Access Control with least privilege;*
3. *Provide a security audit capability (pro-*

(dilindungi integritasnya);

4. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;
5. Menyediakan perlindungan mandiri untuk sistem operasi;
6. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
7. Mewajibkan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
8. Menyediakan perlindungan terhadap kode jahat (*malicious code*);
9. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
10. Mewajibkan pemeriksaan mandiri (*self-test*) terhadap layanan-layanan Peruri CA.

Sistem komputer Peruri CA dikonfigurasi dengan meminimalisir jumlah akun dan layanan jaringan yang diperlukan.

Server Peruri CA yang terkait dengan kunci penandatanganan pribadi dioperasikan menggunakan Kunci Privat.

tected in integrity);

4. *Require use of cryptography for communication session and database security;*
5. *Provide self-protection for the operating system;*
6. *Require use of strong password policy;*
7. *Require trusted path for identification and authentication;*
8. *Provide means for malicious code protection;*
9. *Provide means to maintain software integrity; and*
10. *Require self-test security related Peruri CA services.*

Peruri CA computer system is configured with minimum of the required accounts and network services.

The Peruri CA server associated with the private signing key is operated using the Private Key.

6.5.2 Peringkat Keamanan Komputer/*Computer Security Rating*

Tidak ada ketentuan.

No stipulation.

6.6 Kendali Teknis Siklus Hidup/*Life Cycle Of Technical Controls*

6.6.1 Kendali Pengembangan Aplikasi/*System Development Controls*

Kendali pengembangan sistem Peruri CA adalah sebagai berikut:

1. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;

Peruri CA system development controls are as follows:

1. *Using software designed and developed through a formal and documented methodology;*

2. Pengadaan perangkat keras dan perangkat lunak dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen-komponen yang terdapat dalam perangkat lunak dirusak;

3. Pengembangan perangkat keras dan perangkat lunak dilakukan dalam sebuah lingkungan yang terkendali, dan proses pengembangan didefinisikan dan didokumentasikan. Syarat ini tidak berlaku bagi perangkat lunak maupun perangkat keras komersil siap-pakai yang dibeli;

4. Perangkat keras dan perangkat lunak didedikasikan untuk melaksanakan aktivitas IKP. Tidak ada aplikasi lain, perangkat lunak, koneksi jaringan, atau komponen perangkat lunak yang diinstall yang bukan bagian dari operasional IKP;

5. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya untuk dimuat ke perangkat. Perangkat keras dan perangkat lunak Peruri CA selalu di-*scan* untuk kode-kode berbahaya pada penggunaan pertama dan secara periodik; dan

6. Pembaruan perangkat keras dan perangkat lunak dibeli atau dikembangkan dengan cara yang sama dengan perangkat aslinya dan diinstal oleh personel yang terpercaya dan terlatih melalui langkah-langkah yang terdokumentasi.

Perangkat lunak siap pakai maupun perangkat lunak yang dikembangkan sendiri oleh Peruri CA yang digunakan untuk manajemen Sertifikat Elektronik, sepenuhnya diuji di lingkungan non-produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem atau komponen-

2. *Procurement of hardware and software is carried out with efforts to reduce the possibility of components contained in the software being damaged;*

3. *Hardware and software development is carried out in a controlled environment, and the development process is defined and documented. These terms do not apply to commercial off-the-shelf software or hardware purchased;*

4. *Hardware and software are dedicated to carrying out PKI activities. There are no other applications, software, network connections, or software components installed that are not part of PKI operations;*

5. *Sufficient care is taken to prevent malicious software from being loaded onto the device. Peruri CA hardware and software is always scanned for malicious code upon first use and periodically; and*

6. *Hardware and software updates are purchased or developed in the same manner as the original device and installed by trusted and trained personnel through documented steps.*

Both ready-to-use software and software developed in-house by Peruri CA used for Electronic Certificate management, are fully tested in a non-production environment before being implemented in the production environment. Any changes to the system or its components must go

nya harus melalui proses reviu Kontrol Manajemen Perubahan dan persetujuan.

through a Change Management Control review and approval process.

6.6.2 Kendali Manajemen Keamanan/*Security Management Controls*

Konfigurasi dari sistem Peruri CA serta seluruh modifikasi dan *upgrades* didokumentasikan dan dikontrol oleh Manajemen Peruri CA. Peruri CA menggunakan perangkat lunak untuk mendeteksi perubahan konfigurasi sistem manajemen CA. Untuk menjamin integritas perangkat keras, Peruri CA menggunakan *anti-tempered bag.*

The configuration of the Peruri CA system as well as all modifications and upgrades are documented and controlled by Peruri CA Management. Peruri CA uses software to detect changes to the CA management system configuration. To ensure hardware integrity, Peruri CA uses anti-tempered bag.

Peruri CA menggunakan metodologi manajemen konfigurasi resmi untuk instalasi dan pemeliharaan sistem Peruri CA. Peruri CA melakukan verifikasi terhadap perangkat lunak ketika dimuat pertama kali, untuk memastikan bahwa perangkat lunak tersebut benar berasal dari penyedia, tanpa modifikasi, dan benar merupakan versi yang ingin digunakan.

Peruri CA uses an official configuration management methodology for the installation and maintenance of the Peruri CA system. Peruri CA verifies the software when it is first loaded, to ensure that the software really comes from the provider, without modification, and is the correct version you want to use.

Peruri CA memiliki prosedur dan jadwal untuk pemeliharaan sistem. Personel Peruri CA yang bertanggung jawab, melakukan *monitoring* dan pemeriksaan sistem secara rutin. Sebagai tambahan dari *monitoring* secara manual, Peruri CA menambahkan proses otomatis yang menginformasikan Peran Terpercaya ketika ada aktivitas yang tidak wajar pada sistem.

Peruri CA has procedures and schedules for the system, as well as maintenance of these procedures and schedules. Responsible Peruri CA personnel carry out routine monitoring and system checks. In addition to manual monitoring, Peruri CA adds an automated process that notifies Trusted Roles when there is unusual activity on the system.

6.6.3 Kendali Keamanan Siklus Hidup/*Life Cycle Security Controls*

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

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

6.7 Kendali Keamanan Jaringan/*Network Security Controls*

Peruri CA menggunakan tindakan keamanan jaringan yang sesuai untuk memastikannya dijaga dari *denial-of-service* (DoS) dan serangan intrusi. Langkah-langkah tersebut termasuk penggunaan *firewall* dan menyaring *router*. Port dan layanan jaringan yang tidak digunakan telah dimatikan. Perangkat lunak jaringan apa pun diperlukan untuk memfungsikan Peruri CA.

Peruri CA employs appropriate network security measures to ensure it is guarded against denial-of-service (DoS) and intrusion attacks. Such measures include the use of firewalls and filtering routers. Unused network ports and services have been turned off. Any network software present was necessary to the functioning of Peruri CA.

6.8 Tanda Waktu/*Time-Stamping*

Semua komponen Peruri CA secara berkala disinkronisasikan dengan sebuah layanan waktu *Network Time Protocol* (NTP).

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

Sistem ini digunakan sebagai stempel waktu untuk:

This system is used as a timestamp for:

1. Validasi waktu awal penerbitan Sertifikat Peruri CA;
2. Waktu pencabutan Sertifikat;
3. Penjadwalan penerbitan CRL;
4. Validasi waktu penerbitan Sertifikat Pemilik; dan
5. Respon OCSP.

1. *Validation of the initial time of issuance of the Peruri CA Certificate;*
2. *Certificate revocation time;*
3. *CRL issuance scheduling;*
4. *Validate the time of issuance of the Owner's Certificate; and*
5. *OCSP response.*

Prosedur secara elektronik atau manual digunakan untuk tetap mempertahankan akurasi waktu pada sistem. Pencocokan jam merupakan sebuah aktivitas yang diaudit sebagaimana diatur pada Bagian 5.4.1.

Electronic or manual procedures are used to maintain time accuracy in the system. Hour matching is an audited activity as provided in Section 5.4.1.

Dalam menyelenggarakan layanan Penanda Waktu Elektronik tersertifikasi, Peruri CA mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

In providing certified Electronic Time-Stamping services, Peruri CA refers to national time marks distributed by institutions that carry out government affairs in the fields of meteorology, climatology and geophysics.

SECTION 7

Profil OCSP, CRL, Dan Sertifikat Elektronik/ *Certificate, CRL, And OCSP Profiles*

7.1 Profil Sertifikat Elektronik/ *Certificate Profile*

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

Peruri CA meninjau profil Sertifikat Elektronik secara berkala minimal setahun sekali yang dilakukan oleh *Administrator Application of CA* dengan menyesuaikan profil Sertifikat Elektronik dengan regulasi dan/atau persyaratan bisnis.

Rincian ketentuan profil Sertifikat Elektronik ini mengacu ke Standar Interoperabilitas PSrE Indonesia.

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

Peruri CA reviews Electronic Certificate profile periodically at least once a year done by Administrator Application of CA by adjusting the Electronic Certificate profile with regulations and/or business requirements.

The specifications for this Electronic Certificate profile refer to the Indonesian CA Interoperability Standard.

Basic Field

Field	Type	M	Peruri CA	Pemilik/*Subscriber*
Certificate (seq)				
tbsCertificate	TBSCertificate	M		
signatureAlgorithm	AlgorithmIdentifier	M		
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.13 (SHA512WithRSA-Encryption)	1.2.840.113549.1.1.13 (SHA512withRSA-Encryption)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL
signatureValue	BIT STRING	M	Tanda tangan PSrE Induk	Tanda tangan Peruri CA
TBSCertificate (seq)				
version	INTEGERv1(0), v2(1), v3(3)	M	Versi 3	Versi 3
serialNumber	INTEGER	M	Serial number sertifikat sesuai dengan RFC 5280	Serial number sertifikat sesuai dengan RFC 5280
signature	AlgorithmIdentifier	M		
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.13 (SHA512WithRSA-Encryption)	1.2.840.113549.1.1.13 (SHA512withRSA-Encryption)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL
issuer	Name	M	DN PSrE Induk (CN=Root CA Indonesia DS {Issuance Number}, O=Kementerian Komunikasi dan Informatika, C=ID)	DN Peruri CA (CN=Peruri CA - {Issuance Number}, O=Peruri, C=ID)
validity	Validity	M	10 tahun	1 tahun
Validity(seq)				
notBefore	UTCTime		Waktu mulai validitas	Waktu mulai validitas

Continued on next page

continued from previous page

Field	Type	M	Peruri CA	Pemilik/*Subscriber*
notAfter	Name		Waktu validitas berakhir	Waktu validitas berakhir
subject	Name	M	DN Peruri CA (CN=Peruri CA - {Issuance Number}, O=Peruri, C=ID)	DN untuk Tanda Tangan Elektronik minimal memuat: • Orang-perseorangan Pribadi (CN={Nama Orang}, OU=Personal, C=ID) • Orang-perseorangan berafiliasi ke perusahaan (CN={Nama Orang}, O={Nama Badan Usaha}, C=ID) DN untuk Segel Elektronik minimal memuat: (CN={Nama Badan Usaha}, C=ID)
subjectPublicKeyInfo	SubjectPublicKeyInfo	M		
SubjectPublicKeyInfo (seq)				
algorithm	AlgorithmIdentifier			
AlgorithmIdentifier (seq)				
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 4096)	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL

Continued on next page

continued from previous page

Field	Type	M	Peruri CA	Pemilik/*Subscriber*
subjectPublicKey	BIT STRING		Kunci Publik Peruri CA	Kunci Publik Subscriber
extensions	EXPLICIT Extensions	M		
Extensions (seq size (1...MAX))				
extension	EXTENSION			
EXTENSION (seq)				
extnID	OBJECT IDENTIFIER		OID dari extension	OID dari extension
critical	BOOLEAN DEFAULT FALSE			
extnValue	OCTET STRING		Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

Standard Extension Field

Field	**Type**	**OID**	**Peruri CA**			**Pemilik/*Subscriber***		
			M	**C**	**Information**	**M**	**C**	**Information**
AuthorityKeyIdentifier (seq)		**2.5.29.35**	**M**	**N**		**M**	**N**	
keyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik PSrE Induk			Hash SHA-1 160 bit dari kunci publik Peruri CA
authorityCertIssuer	GeneralNames							
authorityCert-SerialNumber	INTEGER							
SubjectKeyIdentifier		**2.5.29.14**	**M**	**N**		**M**	**N**	
subjectKeyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik Peruri CA			Hash SHA-1 160 bit dari kunci publik Pemilik
KeyUsage		**2.5.29.15**	**M**	**C**		**M**	**C**	

Continued on next page

continued from previous page

Field	Type	OID	Peruri CA			Pemilik/*Subscriber*		
			M	C	Information	M	C	Information
keyUsage	BIT STRING				keyCertSign (5), cRLSign (6) Nilai key usage (00001100)			digitalSignature, nonRepudiation
CertificatePolicies (seq size (1...MAX))		**2.5.29.32**	**M**	**C**		**M**	**C**	
policyInformation	Policy Information							
PolicyInformation (seq)								
policyIdentifier	OBJECT IDENTIFIER				"Peruri CA" OID: 2.16.360.1. 1.1.3.12.3			"Individu WNI non-Instansi Online Verifikasi Level 2" OID: 2.16.360.1.1.1.5.1.2.2 "Individu WNA Online Verifikasi Level 2" OID: 2.16.360.1.1.1.5.2.2.2 "Segel Elektronik Badan Usaha" OID: 2.16.360.1.1.1.8.1
policyQualifiers	Sequence Size (1...MAX) PolicyQualifierInfo							
SubjectAlternativeName		**2.5.29.17**	**O**	**N**		**O**	**N**	

Continued on next page

continued from previous page

Field	Type	OID	Peruri CA			Pemilik/*Subscriber*		
			M	C	Information	M	C	Information
subjectAlternative-Name	GeneralNames							1. NIK Pemilik menggunakan informasi virtual ID (VID), sesuai ketentuan Subject Identification Method (SIM) pada RFC 4683, disimpan dalam bentuk otherName dari struktur GeneralName menggunakan SII Type=2.16.360.1.1.1.6.1 untuk tipe NIK. 2. Email address Pemilik, sesuai RFC 5280 disimpan di Subject Alternative Name Extension dengan mengikuti ketentuan rfc822Name.
IssuerAlternativeName		**2.5.29.18**	**O**	**N**		**O**	**N**	
issuerAlternative-Name	GeneralNames							
BasicConstraint (seq)		**2.5.29.19**	**M**	**C**		**M**	**C**	
cA	BOOLEAN				TRUE			FALSE
pathLenConstraint	INTEGER				0			
NameConstraint		**2.5.29.30**	**X**	**-**		**X**	**-**	
permittedSubtrees	General Subtrees							
excludedSubtrees	General Subtrees							

Continued on next page

continued from previous page

Field	Type	OID	Peruri CA			Pemilik/*Subscriber*		
			M	C	Information	M	C	Information
ExtendedKeyUsage (seq size (1...MAX))		**2.5.29.37**	**X**	**-**		**O**	**N**	1.2.840.113583.1.1.5
keyPurposeId	Object Identifier							PDF Signing
CRLDistributionPoints (seq size (1...MAX))		**2.5.29.31**	**M**	**N**		**M**	**N**	
DistributionPoint-(seq)								
distribution Point	Distribution Point Name				`http://crl.peruri.co.id/PeruriCA-G1.crl`			`http://crl.peruri.co.id/PeruriCA-G1.crl`
reasons	ReasonFlags							
cRLIssuer	GeneralNames							
FreshestCRL		**2.5.29.46**	**O**	**N**		**O**	**N**	
freshestCRL	CRL Distribution Point							
AuthorityInfoAccess (seq size (1..MAX))		**2.5.29.1**						
Access Description (seq)								
access Method	OBJECT IDENTIFIER		**X**	**-**		**M**	**N**	1.3.6.1.5.5.7.48.1
access Location	GeneralName							OCSP URL
AccessDescription (seq)								
access Method	OBJECT IDENTIFIER		**X**	**-**		**M**	**N**	1.3.6.1.5.5.7.48.2
access Location	GeneralName		**X**	**-**		**M**	**N**	ca Issuer URL

7.2 Profil CRL/*CRL Profile*

Profil CRL Peruri CA mematuhi Standar Interoperabilitas PSrE Indonesia.

Peruri CA's CRL Profile comply with Indonesian CA Interoperability Standard.

Peruri CA menerbitkan CRL X.509 versi 2 dan menggunakan CRL dan CRL entry extension RFC

Peruri CA issue X.509 CRL version 2 and using RFC 5280 CRL and CRL entry extension.

5280.

CRL Profile

Field	ASN.1 Type	Note	M
version	Integer	1 (version2)	M
issuer	Name	CN = Peruri CA - G1 O = Peruri C = ID	M
thisUpdate	UTCTime	Issuing date	M
nextUpdate	UTCTime	According CA's policy	M
revokedCertificates			M
userCertificate	Integer		M
revocationDate	UTCTime		M
crlEntryExtension	Extensions		O
crlExtensions			M

CRL Extension Field

CRL Extension Field				
Field	**ASN.1 Type**	**Note**	**C**	**M**
authorityKeyIdentifier		e558ccf6fa456fb74ed4321f07b 7c3edabce6582	N	M
issuerAltName	otherName		N	O
cRLNumber	Integer	Issuing date	C	M
issuingDistributionPoint	UTCTime	According CA's policy	C	O

7.3 Profil OCSP/*OCSP Profile*

Peruri CA mengoperasikan Online *Certificate Status Protocol responder* (responder OCSP) mengacu ke Standar Interoperabilitas PSrE Indonesia.

Peruri CA operate an Online Certificate Status Protocol responder (OCSP responder) referring to Indonesian CA Interoperability Standard.

Basic Field

Field	Type	M	OCSP Certificate
Certificate (seq)			
Continued on next page			

continued from previous page

Field	Type	M	OCSP Certificate
tbsCertificate	TBSCertificate	M	
signatureAlgorithm, memiliki subfield	AlgorithmIdentifier	M	
AlgorithmIdentifier (seq)			
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL
signatureValue	BIT STRING	M	Tanda tangan PSrE Indonesia penerbit Sertifikat
TBSCertificate (seq)			
version	INTEGER{v1(0), v2(1), v3(3)}		V3
serialNumber	INTEGER		Serial number sertifikat
signature, memiliki subfield	AlgorithmIdentifier		
AlgorithmIdentifier (seq)			
algorithm	OBJECT IDENTIFIER		RSA algorithm identifier (1.2.840.113549.1.1.11)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL
issuer	Name	M	CN = Peruri CA - {Issuance Number} O = Peruri C = ID
validity, memiliki subfield	Validity	M	2 tahun
Validity(seq)			
notBefore	UTCTime		Waktu mulai validitas
notAfter	Name		Waktu validitas berakhir

Continued on next page

continued from previous page

Field	Type	M	OCSP Certificate
subject	Name	M	DN Pemilik Sertifikat (CN=OCSP Peruri Responder, OU=OCSP Responder, O=Peruri, C=ID)
subjectPublicKeyInfo memiliki subfield	SubjectPublicKeyInfo	M	
SubjectPublicKeyInfo(seq)			
algorithm	AlgorithmIdentifier		
AlgorithmIdentifier (seq)			
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL
subjectPublicKey	BIT STRING		Kunci Publik End Entity
extensions, memiliki subfield	EXPLICIT Extensions	M	
EXTENSION (seq size (1...MAX))			
extension	EXTENSION		
EXTENSION (seq)			
extnID	OBJECT IDENTIFIER		OID dari extension
critical	BOOLEAN DEFAULT FALSE		
extnValue	OCTET STRING		Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

Standard Extension Field

Field	Type	OID	Peruri CA		
			M	C	
AuthorityKeyIdentifier (seq)		**2.5.29.35**	**M**	**N**	
keyIdentifier	OCTET STRING				e558ccf6fa456fb74e d4321f07b7c3edabce 6582
authorityCertIssuer	GeneralNames				
authorityCert-SerialNumber	INTEGER				
SubjectKeyIdentifier		**2.5.29.14**	**M**	**N**	
subjectKeyIdentifier	OCTET STRING				SHA-1 160 bit
KeyUsage		**2.5.29.32**	**M**	**C**	
keyUsage	BIT STRING				digitalSignature
CertificatePolicies (seq size (1...MAX))		**2.5.29.32**	**M**	**C**	
policyInformation, memilik subfield	PolicyInformation				
PolicyInformation (seq)					
policyIdentifier	OBJECT IDENTI-FIER				
policyQualifiers	Sequence Size (1...MAX) PolicyQualifi-erInfo				
SubjectAlternativeName		**2.5.29.17**	**X**	**-**	
subjectAlternativeName	GeneralNames				
IssuerAlternativeName		**2.5.29.18**	**O**	**N**	
issuerAlternativeName	GeneralNames				
BasicConstraint (seq)		**2.5.29.19**	**M**	**C**	FALSE
cA	BOOLEAN				
pathLenConstraint	INTEGER				
NameConstraint		**2.5.29.30**	**X**	**-**	
permittedSubtrees	GeneralSubtrees				
excludedSubtrees	GeneralSubtrees				
ExtendedKeyUsage (seq size (1...MAX))		**2.5.29.37**	**O**	**N**	

Continued on next page

continued from previous page

Field	Type	OID	OCSP Certificate		
			M	C	
keyPurposeId	ObjectIdentifier				1.3.6.1.5.5.7.3.9 (OCSP Signing)
FreshestCRL		**2.5.29.46**	**X**	**-**	
freshestCRL	CRLDistributionPoint				
AuthorityInfoAccess (seq size (1..MAX)), memiliki subfield:		**2.5.29.1**			
AccessDescription (seq)					
access Method	OBJECT IDENTIFIER		**X**	**-**	
access Location	GeneralName				

SECTION

8

Audit Kepatuhan Dan Penilaian Lainnya/ *Compliance Audit And Other Assessments*

Peruri CA memiliki mekanisme Penilaian Kelaikan atau Audit Kepatuhan untuk memastikan ketentuan yang diatur dalam CPS ini diterapkan dan diawasi.

Peruri CA menjalani Penilaian Kelaikan dan menyampaikan laporan berkala yang dipersyaratkan oleh ketentuan peraturan perundang-undangan.

Peruri CA juga telah menjalani audit untuk memastikan semua persyaratan pada CPS ini telah diimplementasikan dan diaudit berdasarkan standar:

1. SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi; dan
2. *WebTrust for Certification Authorities.*

Peruri CA has a Feasibility Assessment or Compliance Audit mechanism to ensure that the provisions regulated in this CPS are implemented and monitored.

Peruri CA undergoes a Feasibility Assessment and submits periodic reports required by statutory provisions.

Peruri CA has also undergone an audit to ensure that all requirements in this CPS have been implemented and audited based on:

1. *SNI ISO/IEC 27001 Information Security Management System; and*
2. *WebTrust for Certification Authorities.*

8.1 Frekuensi Atau Lingkup Penilaian/*Frequency Or Circumstances Of Assessment*

Peruri CA menjalani Penilaian Kelaikan berkala sesuai ketentuan peraturan perundang-undangan minimal sekali dalam setahun dan setiap terjadinya perubahan yang signifikan terhadap CPS, prosedur, dan teknik yang diterapkan.

Peruri CA undergoes a periodic Feasibility Assessment in accordance with statutory provisions at least once a year and every time there are significant changes to the CPS, procedures and techniques applied.

Peruri CA menjalani audit berdasarkan standar SNI ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi dan *WebTrust for Certification Authorities* sekali dalam setahun.

Peruri CA undergoes an audit based on the SNI ISO/IEC 27001:2022 Information Security Management System and WebTrust for Certification Authorities standard once a year.

8.2 Identitas/Kualifikasi Penilai/Identity/*Qualifications of Auditor*

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

Auditor demonstrates competence in the field of compliance audit and shall thoroughly understand the requirements in this CPS. Compliance auditors shall perform compliance audit as their main responsibility.

Penilai kepatuhan memiliki kualifikasi sebagai berikut:

1. Tidak memiliki konflik kepentingan terhadap Peruri CA;
2. Memiliki kemampuan untuk melakukan audit berdasarkan standar audit dalam ketentuan peraturan perundang-undangan termasuk pengetahuan terkait pemanfaatan layanan yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik, X.509 versi 3 IKP *Certificate Policy and Certification Practices Framework*, Undang undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Komdigi terkait

Compliance auditors must possess these qualifications:

1. *Have no conflict of interest with Peruri CA;*
2. *Auditors shall possess abilities to perform audit based on audit standards stipulated on laws and regulations, including have a sufficient knowledge related the use of services using Electronic Certificate such as Digital Signature, Electronic Seal, X.509 PKI version 3 Certificate Policy and Certificate Practice Framework, Indonesian Law of Electronic Information and Transactions, Indonesian Government Regulation on Electronic System and Transaction Operations, and Indonesia Ministry of Communication and Digital Affairs Regulation on Certifica-*

Tata Kelola Penyelenggaraan Sertifikasi Elektronik;

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

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

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

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

tion Authority Governance;

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

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

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

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

8.3 Hubungan Penilai Dengan Badan Yang Dinilai/*Auditor's Relationship To Assessed Entity*

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

Selain larangan konflik kepentingan di atas, dalam melaksanakan audit, Penilai memiliki hubungan kontrak yang jelas dengan Peruri CA untuk menjaga independensi/ketidakberpihakan para Penilai. Penilai mempertahankan standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan pelaksanaan pe-

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.

In addition to the prohibition on conflicts of interest above, in carrying out audits, the Auditor has a clear contractual relationship with Peruri CA to maintain the independence/impartiality of the Auditor. Auditor maintain high ethical standards designed to ensure impartiality and the exercise of independent professional judgment, subject to

nilaian profesional yang independen, dengan tunduk padai ketentuan peraturan perundang-undangan.

statutory and regulatory requirements.

8.4 Topik Penilaian/*Topics Covered By Assessment*

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa Peruri CA beroperasi sesuai dengan CP PSrE Induk yang berlaku dan ketentuan peraturan perundang-undangan. Penilaian Kelaikan mencakup penilaian CPS Peruri CA yang berlaku terhadap CP PSrE Induk, untuk menentukan bahwa CPS telah diimplementasikan dan ditegakkan. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen Peruri CA.

The Feasibility Assessment aims to verify that Peruri CA operates in accordance with the applicable Root CA's CP and statutory provisions. The Feasibility Assessment includes an assessment of the Peruri CA's CPS that applies to the Root CA's CP, to determine that the CPS has been implemented and enforced. This assessment covers at least the organization, operations, personnel training and management of Peruri CA.

Penilaian yang dilaksanakan telah memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema audit akan berlaku pada tahun berikutnya setelah Peruri CA mengadopsi skema yang terbaru.

The audit carried out has met the needs of the audit scheme used in the assessment. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to Peruri CA in the year following the adoption of the updated scheme.

8.5 Tindakan Yang Diambil Sebagai Hasil Dari Kekurangan/*Actions Taken As A Result Of Deficiency*

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

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

1. Penilai mencatat ketidaksesuaian tersebut;
2. Penilai kepatuhan memberitahu KKementerian Komunikasi dan Digital Republik Indonesia tentang ketidaksesuaian yang ada;
3. Peruri CA bertanggung jawab untuk

1. *The auditor shall note the discrepancy;*
2. *The compliance auditor notifies the Ministry of Communication and Digital Affairs of The Republic of Indonesia of any nonconformities;*
3. *Peruri CA is responsible for correcting the*

memperbaiki ketidaksesuaian dan harus menentukan tindak lanjut yang diperlukan agar sesuai dengan persyaratan CP/CPS dan/atau kontrak masing-masing, kemudian melaksanakan perbaikan tanpa penundaan.

discrepancy shall and determine what further notifications or actions are necessary pursuant to the requirements of this CP/CPS and the respective contracts, and then proceed to make such notifications and take such actions without delay.

8.6 Komunikasi Hasil/*Communication of Results*

Laporan Penilaian Kelaikan, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh Peruri CA, diberikan kepada Policy Authority. Laporan tersebut mengidentifikasi versi CP dan CPS yang digunakan dalam penilaian. Selain itu, hasilnya dikomunikasikan sebagaimana diatur pada bagian 8.5.

An Audit Compliance Report, including identification of corrective measures taken or being taken by Peruri CA, provided to the Policy Authority. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, the results are communicated as provided in section 8.5.

8.7 Audit Internal/*Internal Audit*

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan resiko gangguan pada proses bisnis.

Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.

Peruri CA memantau kepatuhannya terhadap CP PSrE Induk, CPS Peruri CA, dan ketentuan peraturan perundang-undangan dan secara ketat mengontrol kualitas layanannya dengan melakukan audit mandiri setidaknya setiap setahun sekali terhadap sampel yang dipilih secara acak dari setidaknya 1 persen keseluruhan Sertifikat Elektronik yang diterbitkan di tahun berjalan.

Peruri CA monitors its compliance with the Root CA's CP, Peruri CA's CPS, and statutory provisions and strictly controls the quality of its services by conducting an independent audit at least once a year on a randomly selected sample of at least 1 percent of all Electronic Certificates issued in the current year .

SECTION 9

Bisnis dan Masalah Hukum Lainnya/ *Other Business and Legal Matters*

9.1 Biaya/*Fees*

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

Peruri CA mengenakan biaya layanan dalam menerbitkan atau memperbarui Sertifikat Elektronik termasuk dalam hal penerbitan ulang Sertifikat Elektronik dan penggantian kunci (*re-key*). Terdapat syarat dan ketentuan terkait biaya bagi para Pemohon sertifikat. Mengenai detail biaya permohonan penerbitan atau pembaruan Sertifikat Elektronik tercantum pada setiap dokumen terkait *Manual Marketing, Sales, and Product.*

Peruri CA charges service fees for Electronic Certificate issuance or renewal, including charge for re-issuance or re-key. There are terms and conditions related to fees for certificate applicants. The details of the application fee for certificate issuance or renewal are listed in each document related to Manual Marketing, Sales, and Product.

9.1.2 Biaya Pengaksesan Sertifikat Elektronik/*Electronic Certificate Access Fees*

Peruri CA tidak mengenakan biaya pengaksesan Sertifikat Elektronik.

Peruri CA does not charges fees for accessing Electronic Certificates.

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

Peruri CA tidak mengenakan biaya terhadap pencabutan Sertifikat Elektronik atau pengecekan status keabsahan Sertifikat Elektronik melalui CRL.

Peruri CA does not charge fees for revocation of Electronic Certificates or checking the validity status of Electronic Certificates through CRL.

9.1.4 Biaya Layanan Lainnya/*Fees for Other Services*

Peruri CA dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya di luar penerbitan dan pembaruan Sertifikat Elektronik.

Peruri CA may charge fee for other additional services beyond Electronic Certificate issuance and renewal.

9.1.5 Kebijakan Pengembalian Biaya/*Refund Policy*

Peruri CA dapat memberikan pengembalian biaya kepada Pemilik sesuai dengan syarat dan ketentuan yang diatur dalam Kebijakan Jaminan yang tersedia pada repositori Peruri CA.

Peruri CA can provide a refund to the Subscriber in accordance with the terms and conditions set out in the Warranty Policy available in the Peruri CA repository.

Tidak ada pengembalian biaya dalam hal terjadi penutupan layanan Peruri CA, namun Peruri CA menjamin Sertifikat Elektronik tetap valid hingga masa berlakunya habis

There is no refund in the event of a Peruri CA service closure, but Peruri CA guarantees that the Electronic Certificate remains valid until its validity period expires.

9.2 Tanggung Jawab Keuangan/*Financial Responsibility*

9.2.1 Cakupan Asuransi/*Insurance Coverage*

Peruri CA menjamin kerugian akibat kegagalan layanan Penyelenggaraan Sertifikasi Elektronik akibat kelalaian Peruri CA dalam mematuhi kewajiban sebagai PSrE sesuai dengan ketentuan perundang-undangan yang diatur dalam dokumen Kebijakan Jaminan.

Peruri CA guarantees losses due to failure of Certification Authority services due to their failure to comply with obligations as CA in accordance with the provisions of the legislation as stipulated in the Warranty Policy document.

9.2.2 Aset Lainnya/*Other Assets*

Peruri CA mempertahankan kemampuan keuangan yang wajar untuk menjalankan operasional dalam memenuhi kewajibannya kepada Partisipan IKP sebagaimana diatur pada bagian 1.3.

Peruri CA maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and reasonable liability obligations to PKI Participants described in section 1.3.

9.2.3 Jaminan Asuransi atau Garansi untuk Pemilik/*Insurance or Warranty Coverage for End-Entities*

Peruri CA menyediakan Jaminan Asuransi atau Garansi untuk para Pemilik yang diatur dalam dokumen Kebijakan Jaminan.

Peruri CA provides insurance or warranty for Subscriber as regulated in the Guarantee Policy document.

9.3 Kerahasiaan Informasi Bisnis/*Confidentiality of Business Information*

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

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

9.3.1 Cakupan Informasi Rahasia/*Scope of Confidential Information*

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

1. Informasi pribadi data Pemilik sebagaimana dijabarkan pada bagian 9.4;
2. Rekam jejak audit (*audit logs*) dari sistem Peruri CA dan RA;
3. Data aktivasi pada saat pengaktifan Kunci Privat Peruri CA sebagaimana dijabarkan pada bagian 6.4;
4. Dokumentasi bisnis proses Peruri CA termasuk dokumen *Disaster Recovery Plans* (DRP) dan *Business Continuity Plans* (BCP);
5. Laporan audit dari auditor independen dan auditor internal sebagaimana dijabarkan pada bagian 8;
6. Hasil penilaian kerentanan; dan
7. Dokumen terkait Business Plan, hasil

1. *Personal Information from Subscriber as detailed in section 9.4;*
2. *Audit logs from Peruri CA and RA systems;*
3. *Activation data used to active Peruri CA Private Keys as detailed in section 6.4;*
4. *Peruri CA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP);*
5. *Audit reports from independent auditor and internal auditor as described in section 8;*
6. *Vulnerability assessment results; and*
7. *Documents related to the Business Plan, VA*

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

/ pentest results, network topology with IP Address, employee work assessment results, system administrator logs, and other documents mentioned in the SOP for Document and Records Control.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, sebelum pengungkapan informasi di atas memerlukan persetujuan tertulis dari Pemilik.

Unless required by law or court order, prior disclosure of the above information requires written consent from the Subscriber.

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

Informasi yang tidak dikategorikan rahasia dalam dokumen CPS dianggap informasi publik (biasa). Informasi mengenai status Sertifikat Elektronik dan Sertifikat Elektronik itu sendiri termasuk kategori informasi publik.

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

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

Peruri CA melindungi informasi rahasia. Peruri CA menjaga kerahasiaan informasi bisnis rahasia yang secara jelas ditandai atau diberi label sebagai rahasia atau menurut sifatnya harus dipahami secara wajar sebagai rahasia, dan memperlakukan informasi tersebut dengan tingkat perhatian dan keamanan yang sama seperti Peruri CA memperlakukan informasi rahasia miliknya sendiri.

Peruri CA protects confidential information. Peruri CA maintains the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should be reasonably understood to be confidential, and treats such information with the same level of care and security as Peruri CA treats its own confidential information.

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

1. Pelatihan atau peningkatan *awareness*;
2. Perjanjian kontrak pegawai; dan
3. *Non-Disclosure Agreement* (NDA) dengan

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

1. *Training or increase awareness;*
2. *Contracts with employees; and*
3. *Non-Disclosure Agreement (NDA) with em-*

pegawai, pegawai *outsource*, dan rekanan.

ployees, outsourcers and contractors.

9.4 Privasi Informasi Pribadi/*Privacy Of Personal Information*

9.4.1 Rencana Privasi/*Privacy Plan*

Peruri CA melindungi informasi pribadi sesuai dengan ketentuan yang diatur dalam Kebijakan Privasi yang dipublikasikan dalam repositori sebagaimana diatur pada Bagian 2.1 bersamaan dengan CPS ini.

Peruri CA protect personal information in accordance with a Privacy Policy published on a suitable Repository along with this CPS, as mentioned in Section 2.1.

Kebijakan Privasi dibuat sesuai dengan ketentuan peraturan perundangan- undangan Indonesia mengenai pelindungan data pribadi dan informasi dan transaksi elektronik. Kebijakan Privasi mendokumentasikan informasi pribadi yang dikumpulkan, bagaimana informasi tersebut disimpan dan diproses, dan kondisi yang membolehkan informasi tersebut untuk dibuka.

The Privacy Policy conform to the Indonesian laws and regulations concerning personal data protection and electronic information and transactions. The Privacy Policy document collected personal information, how it is stored and processed, and under what conditions the information may be disclosed.

Peruri CA memberikan akses dan kemampuan kepada Pemilik untuk mengoreksi atau mengubah informasi pribadi atau organisasi melalui permintaan yang sah kepada Peruri CA. Informasi tersebut hanya bisa diberikan setelah Peruri CA melakukan langkah-langkah untuk mengautentikasi identitas dari pihak yang meminta.

Peruri CA provides Subscribers with access and the ability to correct or modify their personal or organization information upon appropriate request to Peruri CA. Such information shall be provided only after taking proper steps to authenticate the identity of the requesting party.

Peruri CA hanya mengumpulkan data yang diperlukan untuk pendaftaran dan sertifikasi dan hanya menggunakan untuk tujuan tersebut. Secara khusus, Peruri CA tidak menggunakan data tersebut untuk tujuan komersial apa pun.

Peruri CA only collect Subscriber data necessary for registration and certification and use it for these purposes exclusively. In particular, Peruri CA does not use subscriber data for any commercial purposes.

9.4.2 Informasi yang Diperlakukan Sebagai Privat/*Information Treated as Private*

Peruri CA melindungi semua informasi pribadi Pemohon dari pengungkapan yang tidak sah, baik terhadap Pemohon yang Sertifikatnya berhasil diterbitkan (Pemilik) maupun yang ditolak. Peruri CA menghapus informasi pribadi

Peruri CA protect all Applicant's personal information from unauthorized disclosure, regardless of the acceptance of their applications approval. Peruri CA delete personal information of the rejected Applicants in no later than 30 (thirty) days

Pemohon yang ditolak paling lama 30 (tiga puluh) hari kalender dan hanya dapat menyimpan nomor identitas kependudukan (NIK) Pemohon disertai alasan penolakan.

thereafter. Peruri CA can only keep Applicant's national Identity number (NIK) and the reason for application's rejection.

Informasi pribadi dapat diungkapkan atas persetujuan Pemilik terhadap Pengandal. Arsip yang dikelola oleh Peruri CA tidak boleh dirilis kecuali yang diizinkan pada bagian 9.4.1.

Personal information may be disclosed with the Subscriber's consent to the Relying Parties. The contents of the archives maintained by Peruri CA shall not be released except as allowed by section 9.4.1.

9.4.3 Informasi tidak Dianggap Privat/*Information not Deemed Private*

Informasi yang ada pada Sertifikat Elektronik, profil OCSP dan CRL tidak dianggap privat.

Information contained in Electronic Certificates, OCSP profiles and CRLs is not considered private.

9.4.4 Tanggung Jawab Melindungi Informasi Privat/*Responsibility to Protect Private Information*

Peruri CA telah menerapkan tindakan keamanan untuk melindungi informasi privat. Informasi yang disimpan berbentuk elektronik maupun fisik. *Backup* informasi pribadi dienkripsi setiap akan dipindahkan ke media *backup*.

Peruri CA has implemented security measures to protect private information. The information stored in the debate is in digital or physical form. Backup personal information is encrypted every time it is moved to the backup media.

Pelaksanaan perlindungan terhadap informasi privat mencakup mengikat pegawai, pegawai outsource, dan rekanan dengan *Non-Disclosure Agreemen*t (NDA).

Implementation of protection for private information includes binding employees, outsourced employees and partners with a Non-Disclosure Agreement (NDA).

9.4.5 Pemberitahuan dan Persetujuan untuk Menggunakan Informasi Privat/*Notice and Consent to use Private Information*

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. Peruri CA mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Perjanjian Pemilik dan Kebijakan Privasi mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk

Personal information obtained from Applicants during the application and enrolment process is deemed private and permission is required from the Applicant to allow the use of such information. Peruri CA accommodates all provisions related to the use of personal information into the Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by Peruri CA. The use of private in-

atau layanan yang disediakan oleh Peruri CA. Penggunaan informasi privat harus didasarkan pada Kebijakan Privasi dan ketentuan peraturan perundang-undangan yang berlaku.

formation must be based on the Privacy Policy and the provisions of applicable laws and regulations.

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

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

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

9.4.7 Keadaan Pengungkapan Informasi Lain/*Other Information Disclosure Circumstances*

Tidak ada ketentuan.

No stipulation.

9.5 Hak Atas Kekayaan Intelektual/Intellectual Property Rights

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

Peruri CA's intellectual property rights including trademarks, copyright and all Peruri CA documents remain as sole property of Peruri CA.

Peruri CA tidak melanggar hak kekayaan intelektual pihak lain.

Peruri CA does not violate intellectual property rights held by others.

9.6 Pernyataan dan Jaminan/*Representations and Warranties*

9.6.1 Pernyataan dan Jaminan CA/*CA Representations and Warranties*

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

1. Peruri CA mematuhi ketentuan yang diatur dalam CPS ini;
2. Peruri CA menerbitkan dan memperbarui CRL sesuai ketentuan CPS ini;
3. Seluruh Sertifikat Elektronik yang diterbitkan memenuhi syarat yang diatur berdasarkan CPS ini dan hanya Informasi

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

1. *Peruri CA complies with the provisions set out in this CPS;*
2. *Peruri CA issues and updates the CRL in accordance with the provisions of this CPS;*
3. *All Electronic Certificates issued meet the requirements regulated under this CPS and only verified information is displayed on the*

yang telah diverifikasi yang ditampilkan di Sertifikat Elektronik;

4. Peruri CA menampilkan informasi yang dapat diakses secara publik melalui situs repositori;
5. Kunci Peruri CA terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;
6. Semua pernyataan yang dibuat oleh Peruri CA dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh Peruri CA; dan
7. Setiap Pemilik telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik yang terkait dengan atau yang dimuat dalam Sertifikat Elektronik adalah benar.

Electronic Certificate;

4. *Peruri CA displays information that can be accessed publicly through the repository site;*
5. *Peruri CA's key is protected and cannot be accessed by unauthorized parties;*
6. *All statements made by Peruri CA in all applicable agreements are true and accurate, as far as Peruri CA knows; and*
7. *Each Subscriber is required to represent and warrant that all information provided by the Subscriber related to or contained in the Electronic Certificate is correct.*

9.6.2 Pernyataan dan Jaminan RA/*RA Representations and Warranties*

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

1. Tidak ada kekeliruan dalam Sertifikat Elektronik yang diketahui atau berasal dari entitas yang menyetujui permohonan pendaftaran Sertifikat Elektronik;
2. Tidak ada kesalahan informasi dalam Sertifikat Elektronik yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat Elektronik sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat Elektronik. RA memelihara bukti bahwa pemeriksaan (*due diligence*) telah dilakukan dalam memvalidasi informasi yang terdapat dalam Sertifikat Elektronik;
3. Dalam hal Peruri CA menunjuk RA tertentu, Peruri CA mengharuskan RA men-

RA represents and warrants, to the extent specified in the CPS, that:

1. *There are no fallacies on Electronic Certificate that have been known or came from the entity who gives an acknowledgement on Electronic Certificate application;*
2. *There are no false information in the Electronic Certificate carried by the entity that approves the registration of the Electronic Certificate as a result of inaccuracy in the Electronic Certificate Registration Management. RA maintains evidence that due diligence was exercised in validating the information contained in the Electronic Certificate;*
3. *In the event that Peruri CA appoints a particular RA, Peruri CA requires the RA to guar-*

jamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP PSrE Induk, CPS ini dan dituangkan dalam kontrak dengan Peruri CA; dan

4. Pemilik dikenakan kewajiban sebagaimana disebutkan dalam Bagian 9.6.3. Pemilik mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

RA yang diketahui bertindak dengan cara yang tidak sesuai dengan kewajiban ini dapat dicabut tanggung jawabnya sebagai RA.

antee that the registration activities carried out by the RA are in accordance with the Parent PSrE CP, this CPS and as stated in the contract with Peruri CA; and

4. *Obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.*

RAs who act in a manner inconsistent with these obligations may be stripped of their responsibilities as RAs.

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

Peruri CA mengharuskan Pemilik dan/atau Pemohon untuk menyetujui dokumen yang berisi persyaratan yang harus dipenuhi terkait perlindungan Kunci Privat dan penggunaan Sertifikat Elektronik, sebelum Sertifikatnya Elektronik diterbitkan. Pemilik dan/atau Pemohon harus menyetujui hal-hal sebagai berikut:

1. Setiap Sertifikat Elektronik yang dibuat menggunakan Kunci Privat serta berkorespondensi dengan Kunci Publik yang tercantum pada Sertifikat Elektronik adalah merupakan Tanda Tangan Elektronik Pemilik dan Sertifikat Elektronik yang sudah disetujui serta secara operasional (tidak kedaluwarsa dan telah dicabut) saat Tanda Tangan Elektronik dibuat;
2. Setiap Kunci Privat diamankan dan hanya Pemilik yang memiliki akses terhadap Kunci Privat tersebut;
3. Sudah melakukan peninjauan terhadap informasi dalam Sertifikat Elektronik yang telah diterima untuk memastikan akurasi;

Peruri CA requires the Subscriber and/or Applicant to approve a document containing the requirements that must be fulfilled regarding the protection of the Private Key and the use of the Electronic Certificate, before the Electronic Certificate is issued. Subscriber and/or Applicant must agree to the following:

1. *Each Electronic Certificate created using the Private Key corresponding to the Public Key listed in the Electronic Certificate is the Digital Signature of the Subscriber and the Electronic Certificate has been accepted and is operational (not expired or revoked) at the time the Digital Signature is created;*
2. *Each Private Key must be secured and only the Subscriber has access to the Private Key;*
3. *Have thoroughly reviewed the Electronic Certificate information;*

4. Semua informasi yang diberikan oleh Pemilik dan informasi yang berada di dalam Sertifikat Elektronik adalah akurat;
5. Sertifikat Elektronik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini, Perjanjian Pemilik, atau kontrak berlangganan;
6. Segera memberitahukan Peruri CA dalam hal:
    i. permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat Elektronik dan Kunci Privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari Kunci Privat Pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat Elektronik;
    ii. Permohonan untuk melakukan pencabutan Sertifikat Elektronik, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam Sertifikat Elektronik tersebut; dan
    iii. Penghentian penggunaan Kunci Privat yang Kunci Publik-nya tercantum dalam Sertifikat Elektronik setelah dicabut.
7. Akan menanggapi instruksi Peruri CA terkait kebocoran atau penyalahgunaan Sertifikat Elektronik dalam kurun waktu 48 (empat puluh delapan) jam;
8. Menyetujui dan menerima bahwa Peruri CA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat Elek-

4. *All information supplied by the Subscriber and contained in the Electronic Certificate is accurate;*
5. *The Electronic Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CPS, or Subscriber Agreement;*
6. *Immediately notify Peruri CA in the event of:*
    i. *Request revocation of the Electronic Certificate and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Electronic Certificate;*
    ii. *Request revocation of the Electronic Certificate, and cease using it, if any information in the Electronic Certificate is or becomes incorrect or inaccurate; and*
    iii. *Stop using the Private Key whose Public Key is listed in an Electronic Certificate after revoked.*
7. *Will respond to Peruri CA's instructions regarding compromise or Electronic Certificates misuses within 48 (forty eight) hours;*
8. *Acknowledges and accepts that Peruri CA is entitled to revoke the Electronic Certificate immediately if the Subscriber violates the*

tronik jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Pemilik atau jika Peruri CA menemukan bahwa Sertifikat Elektronik tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware*; dan

terms of the Subscriber Agreement or terms of use or if Peruri CA discovers that the Electronic Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware; and

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

9. *Subscriber of the Electronic Certificate is the end user and is not the provider of the Electronic Certificate, and does not use the private key whose Public Key is listed in the digital certificate for the purpose of signing the Electronic Certificate of another Certification Authority.*

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

Dengan mengandalkan Sertifikat Elektronik dari Peruri CA, Pengandal menyatakan dan menjamin bahwa:

By relying on the Electronic Certificate, the Relying Party assures that:

1. Memiliki kemampuan teknis untuk menggunakan Sertifikat Elektronik;

1. *Have the technical capability to use Electronic Certificates;*

2. Apabila perwakilan dari Pengandal menggunakan suatu Sertifikat Elektronik yang diterbitkan oleh Peruri CA, Pengandal secara benar memverifikasi informasi yang tercantum di dalam Sertifikat Elektronik sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut;

2. *If the representative from the relying party use an Electronic Certificate issued by Peruri CA, Relying Party should verify the information contained in the Electronic Certificate before use and carry all the consequences that happened if the relying party fail to applied it;*

3. Melaporkan langsung kepada Peruri CA yang berwenang, jika Pengandal menyadari atau mencurigai bahwa telah terjadi kebocoran/penyalahgunaan pada Kunci Privat;

3. *Notify the appropriate Peruri CA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been compromised;*

4. Mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat Elektronik, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pengandal yang ada pada CPS ini; dan

4. *Acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the Electronic Certificate, that they are fully responsible for deciding to rely on the information or not, and they will carry the legal consequences from the failure to fulfill the obligation of the Relying Party as mentioned in the CPS; and*

5. Mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

5. *Must comply with the provisions of this CPS and related agreements.*

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

Tidak ada ketentuan.

No stipulation.

9.7 Pelepasan Jaminan/*Disclaimers of Warranties*

Peruri CA dalam CPS ini tidak menjamin bahwa:

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

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;

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

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

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

3. Keakuratan, keaslian, kelengkapan atau ke-

3. *The accuracy, authenticity, completeness or*

sesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat Elektronik.

fitness of any information contained in, free, test or demo Electronic Certificates.

9.8 Pembatasan Tanggung Jawab/*Limitations of Liability*

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

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

1. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat Elektronik atau Pasangan Kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Pemilik, atau yang diatur dalam Sertifikat Elektronik itu sendiri;
2. Semua kerusakan yang disebabkan oleh *force majeure*;
3. Semua kerusakan yang disebabkan oleh *malware* (seperti virus atau trojan) diluar perangkat Peruri CA;
4. Semua kesalahan data informasi Sertifikat Elektronik yang berasal dari Pemilik setelah periode verifikasi data selesai; dan
5. Sertifikat Elektronik yang penerbitan atau pengelolaannya tidak sesuai dengan CPS Peruri CA.

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

1. *All damage caused by the misuse of Electronic Certificate 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 Electronic Certificates;*
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 Electronic Certificate information that comes from Subscriber after data verification period is complete; and*
5. *Electronic Certificates whose issuance or management is not in accordance with CPS Peruri CA.*

9.8.2 Pembatasan Tanggung Jawab RA/*RA Limitation of Liability*

Tidak ada ketentuan.

No stipulation.

9.8.3 Pembatasan Tanggung Jawab Pemilik/*Subscriber Limitation of Liability*

Tanggung jawab Pemilik dan/atau batasannya diuraikan dalam kontrak berlangganan atau Perjanjian Pemilik, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur

The liability and/or limitation thereof of Subscribers shall be as set forth in the applicable Subscriber Agreement, subject to the applicable law governing the relationship between the parties.

hubungan kedua belah pihak.

Pemilik secara khusus bertanggung jawab atas kerugian yang disebabkan oleh pelanggaran kelaikan (*due diligence*), seperti memindahtangankan token dan PIN kepada orang lain ataupun tidak mencabut Sertifikat Elektroniknya yang terkompromi.

In particular, the Subscriber is liable for damages caused by a breach of their due diligence, such as handing over a token and PIN to somebody else or not revoking his compromised Electronic Certificate.

9.9 Ganti Rugi/*Indemnities*

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

Kewajiban ganti rugi Peruri CA ditetapkan dalam CPS, Perjanjian Kerja Sama (PKS) dengan klien, atau Perjanjian Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat yang diatur dalam Kebijakan Jaminan.

Peruri CA's indemnification obligations must be set forth in its CPS, Subscription Contract with clients, or Relying Party Agreement including any obligation to third party beneficiaries as set in Warranty Policy.

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

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

9.9.2 Ganti Rugi oleh Pemilik/*Indemnification by Subscribers*

Persyaratan ganti rugi oleh Pemilik diatur pula dalam Perjanjian Kerja Sama (PKS) dan/atau Kebijakan Jaminan.

Requirements for compensation by the Subscriber are also regulated in the Cooperation Agreement (PKS) and/or Warranty Policy.

Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pemilik setuju untuk mengganti rugi dan membebaskan Peruri CA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya, dan segala tuntutan yang diakibatkan oleh:

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold Peruri CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Peruri CA may incur as a result of:

1. Pelanggaran yang dilakukan oleh Pemilik terhadap perjanjian pemilik atau kontrak berlangganan, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
2. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik;

1. *Any violation by the Owner of the owner's agreement or subscription contract, this CPS, or applicable law, whether committed intentionally or unintentionally;*
2. *Fraudulent or negligent use of Private Key by the Subscriber;*

3. Penggunaan Sertifikat Elektronik oleh Pemilik untuk melakukan perbuatan melawan hukum;
4. Kegagalan Pemilik untuk mengungkapkan alat bukti pada permohonan Sertifikat Elektronik dengan maksud untuk menipu pihak manapun;
5. Kegagalan Pemilik untuk melindungi Kunci Privat, menggunakan sistem elektronik yang terpercaya, atau mengambil langkah-langkah yang wajar untuk mencegah kebocoran, kehilangan, pengungkapan, perubahan, atau penggunaan tidak sah Kunci Privat; atau
6. Penggunaan nama oleh Pemilik (termasuk namun tidak terbatas pada *common name*, nama domain, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

3. *Unauthorised use of the Electronic Certificates by Subscribers;*
4. *Failure by the Subscriber to disclose a material fact on the Electronic Certificate Application with intent to deceive any party;*
5. *The Subscriber's failure to protect the Subscriber's Private Key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key; or*
6. *The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.*

9.9.3 Ganti Rugi oleh Pengandal/*Indemnification by Relying Parties*

Persyaratan ganti rugi oleh Pengandal diatur pula dalam Perjanjian Pengandal.

Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan Peruri CA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya, dan segala tuntutan termasuk biaya pengacara yang wajar yang mungkin ditanggung Peruri CA yang diakibatkan oleh:

1. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pengandal, CPS ini, atau hukum yang berlaku; dan
2. Pengandal tidak memeriksa status Ser-

Requirements for compensation by Relying Party are also regulated in the Relying Party Agreement.

To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold Peruri CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorney's fees that Peruri CA may incur as a result of:

1. *Relying Party does not carry out its obligations as regulated in the Relying Party Agreement, this CPS, or applicable law; and*
2. *The Relying Party's failure to check the status*

tifikat Elektronik untuk menentukan apakah Sertifikat Elektronik tersebut sudah kedaluwarsa atau sudah dicabut.

of such Electronic Certificate to determine if the Electronic Certificate is expired or revoked.

9.10 Jangka Waktu Dan Pengakhiran/*Term And Termination*

9.10.1 Jangka Waktu/*Term*

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

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

9.10.2 Pengakhiran/*Termination*

Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 (tiga puluh) kalender hari setelah dipublikasikan.

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

Dalam hal terdapat perubahan CP PSrE Induk, dokumen Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan lainnya yang berdampak pada OID Peruri CA, maka OID dalam CPS Peruri CA tetap berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan dengan ketentuan CP PSrE Induk, Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan terkini lainnya.

When there are changes in Root CA's CP, OID Hierarchy document for Indonesian PKI, and/or other regulations which implicate the Peruri CA's OID, then Peruri CA's OID in the CPS remain valid for maximum 12 (twelve) months or sooner, after adjusting to the new stipulation in Root CA's CP, OID Hierarchy document for Indonesian PKI, and/or other latest regulations.

9.10.3 Dampak Pengakhiran dan Ketentuan yang Tetap Berlaku/*Effect of Termination and Survival*

Peruri CA mengkomunikasikan kondisi, akibat dari penghentian CPS, dan juga kondisi keberlangsungan dari Sertifikat Elektronik yang telah terbit melalui situs web atau laman repositorinya.

Peruri CA communicates the conditions, consequences of terminating the CPS, as well as the state of sustainability of the Electronic Certificates that have been issued via the website or repository.

Meski CPS sudah tidak berlaku lagi, aturan terkait perlindungan data dan arsip informasi harus tetap dipatuhi.

Even once CPS may no longer be valid, the regulations pertaining to the laws on data protection and on archival of information are still observed.

9.11 Pemberitahuan Individu dan Komunikasi Dengan Partisipan/*Individual Notices and Communications with Participants*

Peruri CA menyediakan media komunikasi bagi para pihak terkait melalui dokumen elektronik, surat elektronik, baik yang ditandatangani secara elektronik, telepon atau surel. Peruri CA memberikan tanda terima yang valid sebagai bukti bagi pengirim. Peruri CA memberi tanggapan paling lama 7 (tujuh) hari kerja melalui media komunikasi yang sama.

Peruri CA provides communication media for related parties through electronic documents, electronic mail, whether electronically signed, telephone or email. Peruri CA provides a valid receipt as proof for the sender. Peruri CA will respond within 7 (seven) working days through the same communication media.

Komunikasi yang dibuat ke Peruri CA dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS.

Communications made to Peruri CA must be addressed as stated in section 1.5.2 of the CPS.

9.12 Amendemen/*Amendments*

9.12.1 Prosedur untuk Amendemen/*Procedure for Amendment*

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

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

9.12.2 Periode dan Mekanisme Pemberitahuan/*Notification Mechanism and Period*

Setiap kali CPS diubah, CPS akan diumumkan dalam waktu 7 (tujuh) hari kerja sejak ditandatangani dan semua pihak yang berkepentingan dianggap mengetahui perubahan yang telah diumumkan. Salinan CPS terbaru dapat dilihat pada situs web `https://ca.peruri.co.id/ca/legal`.

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

9.12.3 Keadaan Dimana OID Diubah/*Circumstances Under Which OID Changed*

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

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

Jika PA Peruri CA menambah atau mengubah OID di bawah kebijakan OID Peruri CA, Peruri CA akan menginformasikan kepada PA PSrE Induk sebelum OID tersebut diimplementasikan.

If Peruri CA's PA adds or changes the OID of which is within the boundary of the Peruri CA's OID regulation, Peruri CA will inform the Root CA's PA prior to its implementation.

9.13 Ketentuan Penyelesaian Perselisihan/Sengketa/*Dispute Resolution Provisions*

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai dengan cara musyawarah. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara Peruri CA dengan Pemilik Sertifikat Elektronik.

In case of dispute or controversy related performance, execution or the interpretation of the CPS, all parties will try to reach a peaceful settlement by way of deliberation. The official provisions of the dispute are part of the contract agreed upon between Peruri CA and the Electronic Certificate Subscriber.

Apabila sengketa tidak dapat diselesaikan dengan cara musyawarah, maka para pihak sepakat bahwa penyelesaian sengketa dilakukan oleh Badan Arbitrase Nasional Indonesia (BANI).

If the dispute cannot be resolved by means of deliberation, the parties agree that the dispute settlement shall be carried out by the Indonesian National Arbitration Board (BANI).

9.14 Hukum Yang Mengatur/Governing Law

CPS ini diatur, ditafsirkan, dan dipahami sesuai dengan aturan hukum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat dari Peruri CA ataupun produk/ layanan lainnya. Termasuk apabila Sertifikat Elektronik Peruri CA dipakai untuk kebutuhan komersial atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan Peruri CA, tetap menerapkan aturan hukum di Indonesia.

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

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

Each party, including Peruri CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Indonesia.

9.15 Kepatuhan Atas Hukum Yang Berlaku/*Compliance with Applicable Law*

Partisipan IKP harus mematuhi semua persyaratan, hukum, dan ketentuan peraturan perundang-undangan Indonesia untuk penyediaan produk dan layanan yang dijelaskan dalam CPS ini. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.

PKI Participants shall comply with all applicable requirements, laws, and regulations pertaining in Indonesia for the provision of products and services described in this CPS. Compliance includes, but is not limited to, hardware, software, systems, business information, data processes and all related undertakings during the daily operations of business practices.

9.16 Ketentuan yang Belum Diatur/*Miscellaneous Provisions*

9.16.1 Seluruh Perjanjian/*Entire Agreement*

Tidak ada ketentuan.

No stipulation.

9.16.2 Pengalihan Hak/*Assignment*

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

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

9.16.3 Keterpisahan/*Severability*

Jika ada pengaturan dalam CPS ini yang dinyatakan tidak sah oleh pengadilan, maka ketentuan lain tetap berlaku hingga CPS diperbarui. Proses pembaruan CPS dijelaskan pada Bagian 9.12.

If any provision of this CPS is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect until the CPS is updated. The process for updating this CPS is described in Section 9.12.

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

Peruri CA meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan Peruri CA dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak Pe-

Peruri CA seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Peruri CA's failure to enforce a provision of this CP does not waive Peruri CA's right to enforce the same provisions later or right to enforce any other provisions of this CPS.

ruri CA untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CPS ini. Segala hal terkait pelepasan hak dalam pengadilan disampaikan secara tertulis dan ditandatangani oleh Peruri CA.

To be effective any waivers must be in writing and signed by Peruri CA.

9.16.5 Keadaan Memaksa/*Force Majeure*

Peruri CA tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada diluar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga. Peruri CA telah menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Peruri CA.

Peruri CAs shall not be liable for any failure or delay in its performance under this CPS due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, power and failure of telecommunications lines, lack of internet access, sabotage, terrorism, and governmental action or any unforeseeable events or situations.Peruri CA has provided BCP and DRP with reasonable control in accordance with Peruri CA's capabilities.

9.17 Provisi Lain/*Other Provisions*

9.17.1 Versi CPS yang memiliki kekuatan hukum/*Legally Binding Version of CPS*

Versi Bahasa Indonesia dari CPS ini mengikat secara hukum. Versi Bahasa Inggris dari CPS ini hanya untuk tujuan informasi.

This Indonesian version of the CPS is legally binding. An English version of this CPS serves for informational purposes only.

SECTION 10

LAMPIRAN TABEL AKRONIM DAN DEFINISI/*APPENDIX TABLE OF ACRONYMS AND DEFINITIONS*

Tabel Akronim/*Table of Acronyms*

Istilah/*Term*	**Definisi/*Definition***
BCP	Rencana Keberlangsungan Bisnis (*Business Continuity Planning*)
CP	Kebijakan Sertifikat Elektronik (*Certificate Policy*)
CPS	Pernyataan Penyelenggaraan Sertifikasi Elektronik (*Certification Practice Statement*)
CRL	Daftar Pencabutan Sertifikat (*Certificate Revocation List*)
CSR	Permohonan Penandatangan Sertifikat (*Certificate Signing Request*)
DC	Pusat Data (*Data Center*)
DRC	Pusat Pemulihan Bencana (*Disaster Recovery Center*)
DRP	Rencana Pemulihan Bencana (*Disaster Recovery Planning*)
EV	*Extended Validation*
FIPS	(*US Government*) *Federal Information Processing Standards*
HSM	*Hardware Security Module*
Continued on next page	

continued from previous page

Istilah/*Term*	**Definisi/*Definition***
IKP PKI	Infrastruktur Kunci Publik *Public Key Infrastructure*
LS PSrE CAB	Lembaga Sertifikasi PSrE *Conformity Assessment Body*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PA	*Policy Authority*
PSrE CA	Penyelenggara Sertifikasi Elektronik *Certification Authority*
P2SE	Pengawas Penyelenggaraan Sertifikasi Elektronik (*CA Certification Bodies*)
RA	Otoritas Pendaftaran (*Registration Authority*)
RFC	*Request For Comment*
VA	*Validation Authority*

Definisi/*Definitions*

- **Pemohon** adalah orang, badan usaha, atau badan hukum yang mengajukan permohonan penerbitan Sertifikat Elektronik kepada Peruri CA.
- ***Applicant*** *is a person, business entity, or legal entity that submits an application for the issuance of Electronic Certificates to Peruri CA.*

- **Pemilik** adalah orang, badan usaha, atau badan hukum yang sudah diterbitkan dan memiliki Sertifikat Elektronik.
- ***Subscriber*** *is a person or business entity that has been issued and has an Electronic Certificate.*

- **Pelanggan** adalah orang atau badan usaha yang menggunakan layanan Peruri CA tetapi tidak memiliki atau diterbitkan Sertifikat Elektronik.
- ***Customer*** *is a person or business entity that uses Peruri CA services but does not have or issue Electronic Certificates.*

- **Peran Terpercaya** adalah peran-peran yang melakukan fungsi yang sangat penting, dimana jika fungsi tersebut tidak dilakukan dengan benar dan sesuai, dapat menimbulkan dampak yang sangat buruk bagi tingkat kepercayaan PSrE.
- ***Trusted Roles*** *are roles that perform critical actions, which, when those actions are not performed correctly and appropriately, can result in a detrimental effect for CA's trustworthiness.*

- **Sertifikat Elektronik** adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Peruri CA sebagai Penyelenggara Sertifikasi Elektronik (PSrE).
- ***Electronic Certificate*** *is an electronic certificate containing a Digital Signature and identity indicating the status of the legal subjects of the parties in the Electronic Transaction issued by Peruri CA as Certificate Authority (CA)*

- **Tanda Tangan Elektronik** adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
- ***Digital Signature*** *is a signature consisting of electronic information that is attached, associated, or related to other electronic information used as a means of verification and authentication.*

- **Segel Elektronik** adalah data elektronik yang dilekatkan, terasosiasi, atau terkait dengan informasi elektronik dan/atau dokumen elektronik untuk menjamin asal, integritas dan keutuhan dari informasi
- ***Electronic Seal*** *is electronic data attached, associated, or related to electronic information and/or electronic documents to guarantee the origin, integrity and integrity of electronic information and/or electronic*

elektronik dan/atau dokumen elektronik yang digunakan oleh Badan Usaha atau Instansi.

- **OCSP Responder** adalah aplikasi perangkat lunak online yang dioperasikan di bawah wewenang Peruri CA dan terhubung ke Repositori untuk memproses status permintaan Sertifikat Elektronik.
- **Hardware Security Module** adalah perangkat komputasi fisik yang melindungi dan mengelola kunci digital untuk autentikasi yang kuat dan menyediakan operasi kriptografi yang sesuai dengan FIPS 140-2 Level 3.
- **Pasangan Kunci** adalah Kunci Privat dan Kunci Publik yang mengacu ke entitas yang sama, yang memiliki karakteristik khusus, sehingga suatu pesan yang dienkripsi memakai Kunci Privat hanya dapat didekripsi dengan Kunci Publik pasangannya, dan sebaliknya.
- **Kunci Privat** adalah kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Elektronik dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.
- **Kunci Publik** adalah kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Privat terkait dan yang digunakan oleh Pengandal untuk memverifikasi Tanda Tangan Elektronik yang dibuat oleh pemegangnya.
- **Pengandal** adalah orang, badan usaha, atau badan hukum yang mempercayai

documents used by Business Entities or Institutions.

- ***OCSP Responder*** *is an online software application operated under the authority of Peruri CA and connected to its repository for processing Electronic Certificate status requests.*
- ***Hardware Security Module*** *is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptographic operations that conform to FIPS 140-2 Level 3.*
- ***Key Pair*** *is Private Key and Public Key referring to the same entity, which possess certain characteristics, so that a message encrypted by a Private Key can only be decrypted by the corresponding Public Key, and vice versa.*
- ***Private Key*** *is the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.*
- ***Public Key*** *is the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder.*
- ***Relying Party*** *is a person, business entity, or legal entity that relies upon either the infor-*

pada informasi yang terkandung dalam Sertifikat Elektronik atau token stempel waktu.

- **Peruri CA** adalah unit bisnis Peruri yang memberikan layanan Tanda Tangan Elektronik, Sertifikat Elektronik, dan Segel Elektronik.
- **Kebijakan Jaminan** adalah dokumen yang berisikan ketentuan pemberian ganti rugi yang dialami Pemilik Sertifikat akibat kegagalan penyelenggaraan layanan.
- **Perjanjian Pemilik** adalah perjanjian yang melibatkan Pemilik sebagai pihak yang telah diterbitkan Tanda Tangan Elektronik, Sertifikat Elektronik, dan Stempel Elektronik oleh Peruri CA.

mation contained within an Electronic Certificate or a time-stamp token.

- ***Peruri CA** is Peruri's business unit that provides Digital Signature, Electronic Certificate, and Electronic Seal services.*
- ***Warranty Policy** is a document which contains the provision of compensation experienced by the Subscriber as a result of the failure to provide services.*
- ***Subscriber Agreement** is an agreement involving the Subscriber as a party that has been issued a Digital Signature, Electronic Certificate, and Electronic Seal by Peruri CA.*