



PERURI CA

Nomor	:	002/KRC/KBJ/CP/XII/2018
Mulai Berlaku	:	23 November 2018
Versi	:	3.0
Tanggal Perubahan	:	08 Desember 2020
OID	:	2.16.360.1.1.1.3.12.3.1
Klasifikasi	:	Biasa

Peruri CA

Certificate Policy

Disetujui Oleh / Approved By:

Policy Authority

CATATAN REVISI / REVISION NOTES

NO	TANGGAL / DATE	VERSI / VERSION	DESKRIPSI / DESCRIPTION	OLEH / BY
1	23 November 2018	1.0	Initial Release	CA Organization
2	14 December 2018	1.1	Minor Update: <ul style="list-style-type: none"> - Revise statement in section 1.4 - Revise statement in section 9.16.5 - Cosmetics change 	CA Organization
3	16 January 2019	1.2	Minor Update: <ul style="list-style-type: none"> - Revise statement in section 1.4.1 - Add section 5.6.1 - Cosmetics change 	CA Organization
4	13 February 2019	1.3	Minor Update: <ul style="list-style-type: none"> - Root CA Indonesia Alignment - Bilingual Bahasa Indonesia 	CA Organization
5	6 May 2019	2.0	Major Update: <ul style="list-style-type: none"> - Footer - Writing Format - CRL Interval - Limitation of Peruri CA Responsibility - Point 4.12.1, 4.9.7, 6.1.2, 6.2.1, 6.2.5, and 9.81 	CA Organization
6	10 July 2019	2.1	Minor Update: <ul style="list-style-type: none"> - CRL Interval (Point 4.9.7) 	CA Organization
7	6 March 2020	2.2	Minor Update: <ul style="list-style-type: none"> - Archive retention period - Authentication of Individual Identity 	CA Organization
8	10 October 2020	2.3	Minor Update: <ul style="list-style-type: none"> - Alignment Webtrust For CA 	CA Organization
9	08 December 2020	3.0	Major Update: <ul style="list-style-type: none"> - Improvements to the Kominfo Audit Findings 	Policy Authority

DAFTAR ISI / TABLE OF CONTENTS

CATATAN REVISI / REVISION NOTES.....	2
DAFTAR ISI / TABLE OF CONTENTS.....	3
1. PENGANTAR / INTRODUCTION.....	12
1.1 RINGKASAN / OVERVIEW.....	12
1.2 IDENTIFIKASI DAN NAMA DOKUMEN / DOCUMENT NAME AND IDENTIFICATION.....	12
1.3 PARTISIPAN IKP / PKI PARTICIPANTS.....	12
1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE) / Certification Authorities.....	12
1.3.2 Otoritas Pendaftaran (RA) / Registration Authorities.....	13
1.3.3 Pemilik / Subscribers.....	14
1.3.4 Pihak Pengandal / Relying Parties.....	14
1.3.5 Partisipan Lain / Other Participants.....	15
1.4 KEGUNAAN SERTIFIKAT / CERTIFICATE USAGE.....	15
1.4.1 Penggunaan Sertifikat yang Semestinya / Appropriate Certificate Uses.....	15
1.4.2 Penggunaan Sertifikat yang Dilarang / Prohibited Certificate Uses.....	16
1.5 ADMINISTRASI KEBIJAKAN / POLICY ADMINISTRATION.....	16
1.5.1 Organisasi Pengaturan Dokumen / Organization Administering the Document.....	17
1.5.2 Narahubung / Contact Person.....	17
1.5.3 Personil yang menentukan Kesesuaian CPS dengan Kebijakan / Person Determining CPS Suitability for the Policy.....	17
1.5.4 Prosedur Persetujuan CP & CPS / CP & CPS Approval Procedures.....	17
1.6 DEFINISI DAN AKRONIM / DEFINITIONS AND ACRONYMS.....	18
1.6.1 Definisi / Definitions.....	18
1.6.2 Akronim / Acronyms.....	18
2. TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI / PUBLICATION AND REPOSITORY RESPONSIBILITIES.....	20
2.1 REPOSITORI / REPOSITORIES.....	20
2.2 PUBLIKASI INFORMASI SERTIFIKASI / PUBLICATION OF CERTIFICATION INFORMATION.....	20
2.3 WAKTU ATAU FREKUENSI PUBLIKASI / TIME OR FREQUENCY OF PUBLICATION.....	20
2.4 KENDALI AKSES PADA REPOSITORI / ACCESS CONTROLS ON REPOSITORIES.....	20
3. IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION.....	22
3.1 PENAMAAN / NAMING.....	22
3.1.1 Tipe Nama / Types of Names.....	22
3.1.2 Kebutuhan Nama yang Bermakna / Need for Names to be Meaningful.....	22
3.1.3 Anonimitas atau Pseudonimitas Pemilik / Anonymity or Pseudonymity of Subscribers.....	22

3.1.4	Aturan Interpretasi Berbagai Bentuk Nama / Rules for Interpreting Various Name Forms.....	22
3.1.5	Keunikan Nama / Uniqueness of Names.....	23
3.1.6	Pengakuan, Autentikasi, dan Peran Merek Dagang / Recognition, Authentication, and Role of Trademarks.....	23
3.2	VALIDASI IDENTITAS AWAL / INITIAL IDENTITY VALIDATION	23
3.2.1	Pembuktian Kepemilikan Kunci Privat / Method to Prove Possession of Private Key	23
3.2.2	Autentikasi Identitas Organisasi / Authentication of Organization Identity.....	23
3.2.3	Autentikasi Identitas Individu / Authentication of Individual Identity	24
3.2.4	Informasi Pemilik yang Tidak Terverifikasi / Non-Verified Subscriber Information	24
3.2.5	Validasi Otoritas / Validation of Authority.....	24
3.2.6	Kriteria Inter-Operasi / Criteria for Interoperation / Kriteria Inter-Operasi	24
3.3	IDENTIFIKASI DAN AUTENTIKASI UNTUK PERMINTAAN PENGGANTIAN KUNCI (RE-KEY) / IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS.....	24
3.3.1	Identifikasi dan Autentikasi untuk kegiatan Penggantian Kunci / Identification and Authentication for Routine Re-Key.....	25
3.3.2	Identifikasi dan Autentikasi untuk Re-Key setelah Pencabutan / Identification and Authentication for Re-Key after Revocation	25
3.4	IDENTIFIKASI DAN OTENTIKASI UNTUK PERMINTAAN PENCABUTAN / IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	25
4.	PERSYARATAN OPERASIONAL SIKLUS SERTIFIKAT / CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	26
4.1	PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION	26
4.1.1	Siapa yang dapat mengajukan permohonan sertifikat / Who can submit a Certificate Application	26
4.1.2	Proses Pendaftaran dan Tanggung Jawab / Enrollment Process and Responsibilities	26
4.2	PEMROSESAN PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION PROCESSING	26
4.2.1	Melaksanakan Fungsi-fungsi Identifikasi dan Autentikasi / Performing Identification and Authentication Functions	26
4.2.2	Persetujuan atau Penolakan Permohonan Sertifikat / Approval or Rejection of Certificate Applications	27
4.2.3	Waktu Pemrosesan Permohonan Sertifikat / Time to Process Certificate Applications.....	27
4.3	PENERBITAN SERTIFIKAT / CERTIFICATE ISSUANCE	27
4.3.1	Tindakan PSrE Selama Penerbitan Sertifikat / CA Actions during Certificate Issuance.....	27
4.3.2	Pemberitahuan ke Pemilik oleh PSrE tentang Diterbitkannya Sertifikat / Notification to Subscriber by the CA of Issuance of Certificate.....	27
4.4	PENERIMAAN SERTIFIKAT / CERTIFICATE ACCEPTANCE.....	28
4.4.1	Sikap Yang Dianggap Sebagai Menerima Sertifikat / Conduct Constituting Certificate Acceptance	28
4.4.2	Publikasi Sertifikat oleh Peruri CA / Publication of the Certificate by the Peruri CA	28
4.4.3	Pemberitahuan Penerbitan Sertifikat oleh Peruri CA ke Entitas Lain / Notification of Certificate Issuance by Peruri CA to Other Entities	28

4.5	PASANGAN KUNCI DAN PENGGUNAAN SERTIFIKAT / KEY PAIR AND CERTIFICATE USAGE	28
4.5.1	Kunci Privat Pemilik dan Penggunaan Sertifikat / Subscriber Private Key and Certificate Usage	28
4.5.2	Kunci Publik Pihak Pengandal dan Penggunaan Sertifikat / Relying Party Public Key and Certificate Usage	29
4.6	PEMBARUAN SERTIFIKAT / CERTIFICATE RENEWAL.....	29
4.6.1	Kondisi untuk Pembaruan Sertifikat / Circumstance for Certificate Renewal	29
4.6.2	<i>Siapa Yang Dapat Meminta Pembaruan / Who May Request Renewal</i>	30
4.6.3	Pemrosesan Permintaan Pembaruan Sertifikat / Processing Certificate Renewal Requests	30
4.6.4	Pemberitahuan Penerbitan Sertifikat Baru kepada Pemilik / Notification of New Certificate Issuance to Subscriber	30
4.6.5	Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui / Conduct Constituting Acceptance of a Renewal Certificate	30
4.6.6	Publikasi Sertifikat yang Diperbarui oleh Peruri CA / Publication of the Renewal Certificate by the Peruri CA	30
4.6.7	Pemberitahuan Penerbitan Sertifikat oleh Peruri CA ke Entitas Lain / Notification of Certificate Issuance by Peruri CA to Other Entities	31
4.7	PENGGANTIAN KUNCI SERTIFIKAT / CERTIFICATE RE-KEY	31
4.7.1	Lingkup Penggantian Kunci Sertifikat / Circumstance for Certificate Re-Key	31
4.7.2	Siapa yang Dapat Meminta Sertifikasi dari sebuah Kunci Publik Baru / Who May Request Certification of a New Public Key.....	31
4.7.3	Pemrosesan Permintaan Penggantian Kunci Sertifikat / Processing Certificate Re-Keying Requests	32
4.7.4	Pemberitahuan Penerbitan Sertifikat Baru ke Pemilik / Notification of New Certificate Issuance to Subscriber	32
4.7.5	Sikap yang Dianggap Sebagai Menerima Sertifikat yang Kuncinya Digantikan / Conduct Constituting Acceptance of a Re-Keyed Certificate	32
4.7.6	Publikasi Sertifikat yang Kuncinya Digantikan oleh Peruri CA / Publication of the Re-Keyed Certificate by Peruri CA	32
4.7.7	Pemberitahuan Penerbitan Sertifikat oleh Peruri CA ke Entitas Lain / Notification of Certificate Issuance by Peruri CA to Other Entities	32
4.8	MODIFIKASI SERTIFIKAT / CERTIFICATE MODIFICATION	32
4.8.1	Kedaaan Bagi Modifikasi Sertifikat / Circumstance for Certificate Modification.....	32
4.8.2	Siapa yang Berhak Meminta Modifikasi Sertifikat / Who May Request Certificate Modification	33
4.8.3	Pemrosesan Permintaan Modifikasi Sertifikat / Processing Certificate Modification Requests	33
4.8.4	Pemberitahuan tentang Penerbitan Sertifikat Baru ke Pemilik / Notification of New Certificate Issuance to Subscriber	33
4.8.5	Sikap yang Dianggap Sebagai Menerima Sertifikat yang Dimodifikasi / Conduct Constituting Acceptance of Modified Certificate	33
4.8.6	Publikasi Sertifikat yang Dimodifikasi oleh PSrE / Publication of the Modified Certificate by the CA	33
4.8.7	Pemberitahuan Penerbitan Sertifikat oleh PSrE ke Entitas Lain / Notification of Certificate	

	Issuance by the CA to Other Entities	33
4.9	PENCABUTAN DAN PEMBEKUAN SERTIFIKAT / CERTIFICATE REVOCATION AND SUSPENSION	33
4.9.1	Keadaan untuk Pencabutan / Circumstances for Revocation	33
4.9.2	Siapa yang Dapat Meminta Pencabutan / Who can Request Revocation	34
4.9.3	Prosedur Permintaan Pencabutan / Procedure for Revocation Request	34
4.9.4	Masa Tenggang Permintaan Pencabutan / Revocation Request Grace Period	34
4.9.5	Waktu Dimana Peruri CA Harus Memproses Permintaan Pencabutan / Time Within which Peruri CA Must Process the Revocation Request	35
4.9.6	Persyaratan Pemeriksaan Pencabutan bagi Pihak Pengandal / Revocation Checking Requirement for Relying Parties	35
4.9.7	Frekuensi Penerbitan CRL (bila berlaku) / CRL Issuance Frequency (if applicable).....	35
4.9.8	Latensi Maksimum CRL (bila berlaku) / Maximum Latency for CRLs (if applicable)	35
4.9.9	Ketersediaan Pemeriksaan Pencabutan/Status Daring / On-Line Revocation/Status Checking Availability	36
4.9.10	Pemeriksaan Pencabutan Daring / On-Line Revocation Checking Requirements	36
4.9.11	Bentuk Lain dari Pengumuman Pencabutan yang Tersedia / Other Forms of Revocation Advertisements Available.....	36
4.9.12	Kompromi Re-Key Persyaratan Khusus / Special Requirements Re-Key Compromise	36
4.9.13	Keadaan untuk Pembekuan / Circumstances for Suspension.....	36
4.9.14	Siapa yang Dapat Meminta Pembekuan / Who can Request Suspension.....	36
4.9.15	Prosedur Permintaan Pembekuan / Procedure for Suspension Request.....	36
4.9.16	Batas Waktu Pembekuan / Limits on Suspension Period	36
4.10	LAYANAN STATUS SERTIFIKAT / CERTIFICATE STATUS SERVICES.....	36
4.10.1	Karakteristik Operasional / Operational Characteristics.....	36
4.10.2	Ketersediaan Layanan / Service Availability.....	36
4.10.3	Fitur Opsional / Optional Features	37
4.11	AKHIR BERLANGGANAN / END OF SUBSCRIPTION.....	37
4.12	PEMULIHAN DAN PENITIPAN KUNCI / KEY ESCROW AND RECOVERY	37
4.12.1	Kebijakan dan Praktik Pemulihan dan Penitipan Kunci / Key Escrow and Recovery Policy and Practices	37
4.12.2	Kebijakan dan Praktik Pemulihan dan Enkapsulasi Kunci Sesi / Session Key Encapsulation and Recovery Policy and Practices	37
5.	FASILITAS, MANAJEMEN, DAN KENDALI OPERASI / FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	38
5.1	KENDALI FISIK / PHYSICAL CONTROLS	38
5.1.1	Lokasi dan Konstruksi / Site Location and Construction	38
5.1.2	Akses Fisik / Physical Access	38
5.1.3	Daya dan Penyejuk Udara / Power and Air Conditioning	38
5.1.4	Pemaparan Air / Water Exposures	39

5.1.5	Pencegahan dan Perlindungan dari Kebakaran / Fire Prevention and Protection.....	39
5.1.6	Penyimpanan Media / Media Storage	39
5.1.7	Pembuangan Limbah / Waste Disposal	39
5.1.8	Backup Off-Site / Off-Site Backup	39
5.2	KENDALI PROSEDUR / PROCEDURAL CONTROLS	40
5.2.1	Peran-Peran Terpercaya / Trusted Roles	40
5.2.2	Jumlah Orang yang Dibutuhkan per Tugas / Number of Persons Required per Task	41
5.2.3	Identifikasi dan Autentikasi untuk Setiap Peran / Identification and Authentication for Each Role	41
5.2.4	Peran yang Membutuhkan Pemisahan Tugas / Roles Requiring Separation of Duties	41
5.3	KENDALI PERSONIL / PERSONNEL CONTROLS	41
5.3.1	Persyaratan Kualifikasi, Pengalaman, dan Perizinan / Qualifications, Experience, and Clearance Requirements	41
5.3.2	Background Check Procedures / Prosedur Pemeriksaan Latar Belakang	41
5.3.3	Persyaratan Pelatihan / Training Requirements	42
5.3.4	Frekuensi dan Persyaratan Pelatihan Ulang / Retraining Frequency and Requirements	42
5.3.5	Frekuensi dan Urutan Rotasi Pekerjaan / Job Rotation Frequency and Sequence	42
5.3.6	Sanksi untuk Tindakan Tidak Terotorisasi / Sanctions for Unauthorized Actions.....	42
5.3.7	Persyaratan Kontraktor Independen / Independent Contractor Requirements	42
5.3.8	Dokumentasi yang Diberikan kepada Personil / Documentation Supplied to Personnel	43
5.4	PROSEDUR LOG AUDIT / AUDIT LOGGING PROCEDURES.....	43
5.4.1	Jenis Kejadian yang Direkam / Types of Events Recorded	43
5.4.2	Frekuensi Pemrosesan Log / Frequency of Processing Log.....	44
5.4.3	Periode Retensi Log Audit / Retention Period for Audit Log.....	44
5.4.4	Proteksi Log Audit / Protection of Audit Log.....	44
5.4.5	Prosedur Backup Log Audit / Audit Log Backup Procedures.....	44
5.4.6	Sistem Pengumpulan Audit (Internal vs Eksternal) / Audit Collection System (Internal vs. External)	45
5.4.7	Pemberitahuan ke Subyek Penyebab Kejadian / Notification to Event-Causing Subject.....	45
5.4.8	Penilaian Kerentanan / Vulnerability Assessments	45
5.5	PENGARSIPAN CATATAN / RECORDS ARCHIVAL	46
5.5.1	Tipe Catatan yang Diarsipkan / Types of Records Archived.....	46
5.5.2	Periode Retensi Arsip / Retention Period for Archive	46
5.5.3	Perlindungan Arsip / Protection of Archive.....	46
5.5.4	Prosedur Backup Arsip / Archive Backup Procedures.....	46
5.5.5	Kewajiban Pemberian Label Waktu pada Rekaman Arsip / Requirements for Time-Stamping of Records	47
5.5.6	Sistem Pengumpulan Arsip (Internal atau Eksternal) / Archive Collection System (Internal or External)	47

5.5.7	Prosedur untuk Memperoleh dan Memverifikasi Informasi Arsip / Procedures to Obtain and Verify Archive Information	47
5.6	PERGANTIAN KUNCI / KEY CHANGE OVER.....	47
5.6.1	Skema Interlock / Interlock Scheme	48
5.7	PEMULIHAN BENCANA DAN KEBOCORAN / COMPROMISE AND DISASTER RECOVERY.....	48
5.7.1	Prosedur Penanganan Insiden dan Kebocoran / Incident and Compromise Handling Procedures 48	
5.7.2	Sumber Daya Komputasi, Perangkat Lunak, dan/atau Data Rusak / Computing Resources, Software, and/or Data are Corrupted.....	48
5.7.3	Prosedur Kunci Privat Entitas Terkompromi / Entity Private Key Compromise Procedures	49
5.7.4	Kapabilitas Keberlangsungan Bisnis setelah suatu Bencana / Business Continuity Capabilities after a Disaster.....	49
5.8	PENUTUPAN CA ATAU RA / CA OR RA TERMINATION	49
6.	KENDALI KEAMANAN TEKNIS / TECHNICAL SECURITY CONTROLS.....	50
6.1	PEMBANGKITAN DAN INSTALASI PASANGAN KUNCI / PAIR GENERATION AND INSTALLATION	50
6.1.1	Pembangkitan Pasangan Kunci / Key Pair Generation	50
6.1.2	Pengiriman Kunci Privat ke Pemilik / Private Key Delivery to Subscriber.....	50
6.1.3	Pengiriman Kunci Publik ke Penerbit Sertifikat / Public Key Delivery to Certificate Issuer	51
6.1.4	Pengiriman Kunci Publik Peuri CA kepada Pihak Pengandal / Peruri CA Public Key Delivery to Relying Parties	51
6.1.5	Ukuran Kunci / Key Sizes	52
6.1.6	Parameter Pembangkitan dan Pengujian Kualitas Kunci Publik / Public Key Parameters Generation and Quality Checking.....	52
6.1.7	Tujuan Penggunaan Kunci (pada field key usage - X509 v3) / Key Usage Purposes (as per X.509 v3 key usage field).....	52
6.2	KENDALI KUNCI PRIVATE DAN KENDALI TEKNIS MODUL KRIPTOGRAFI / PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	52
6.2.1	Kendali dan Standar Modul Kriptografi / Cryptographic Module Standards and Controls	52
6.2.2	Kendali Multi Personil (n dari m) Kunci Privat / Private Key (n out of m) Multi-Person Control.	52
6.2.3	Penitipan Kunci Privat / Private Key Escrow.....	53
6.2.4	Backup Kunci Privat / Private Key Backup.....	53
6.2.5	Pengarsipan Kunci Privat / Private Key Archival.....	53
6.2.6	Perpindahan Kunci Privat ke dalam atau dari Modul Kriptografi / Private Key Transfer into or from a Cryptographic Module	53
6.2.7	Penyimpanan Kunci Privat pada Modul Kriptografis / Private Key Storage on Cryptographic Module	54
6.2.8	Metode Pengaktifan Kunci Privat / Method of Activating Private Key	54
6.2.9	Metode Penonaktifan Kunci Privat / Method of Deactivating Private Key	54
6.2.10	Metode Penghancuran Kunci Privat / Method of Destroying Private Key	54
6.2.11	Pemeringkatan Modul Kriptografis / Cryptographic Module Rating.....	54

6.3	ASPEK LAIN DARI MANAJEMEN PASANGAN KUNCI / OTHER ASPECTS OF KEY PAIR MANAGEMENT ..	54
6.3.1	Pengarsipan Kunci Publik / Public Key Archival.....	54
6.3.2	Periode Operasional Sertifikat dan Periode Penggunaan Pasangan Kunci / Certificate Operational Periods and Key Pair Usage Periods.....	55
6.4	DATA AKTIVASI / ACTIVATION DATA.....	55
6.4.1	Pembuatan dan Instalasi Data Aktivasi / Activation Data Generation and Installation	55
6.4.2	Aktivasi Perlindungan Data / Activation Data Protection	55
6.4.3	Aspek Lain Mengenai Data Aktivasi / Other Aspects of Activation Data.....	55
6.5	KENDALI KEAMANAN KOMPUTER / COMPUTER SECURITY CONTROLS.....	55
6.5.1	Persyaratan Teknis Keamanan Komputer Spesifik / Specific Computer Security Technical Requirements	55
6.5.2	Peringkat Keamanan Komputer / Computer Security Rating	56
6.6	KENDALI TEKNIS SIKLUS HIDUP / LIFE CYCLE TECHNICAL CONTROLS	56
6.6.1	Kendali Pengembangan Sistem / System Development Controls	56
6.6.2	Kendali Manajemen Keamanan / Security Management Controls	56
6.6.3	Kendali Keamanan Siklus Hidup / Life Cycle Security Controls	57
6.7	KENDALI KEAMANAN JARINGAN / NETWORK SECURITY CONTROLS	57
6.8	STEMPEL WAKTU / TIME-STAMPING	57
7.	PROFIL OCSP, CRL, DAN SERTIFIKAT / CERTIFICATE, CRL, AND OCSP PROFILES	58
7.1	PROFIL SERTIFIKAT / CERTIFICATE PROFILE	58
7.1.1	Nomor Versi / Version Number(s)	58
7.1.2	Ekstensi Sertifikat / Certificate Extensions.....	58
7.1.3	Pengidentifikasi Objek Algoritma / Algorithm Object Identifiers.....	60
7.1.4	Format Nama / Name Forms.....	60
7.1.5	Batasan Nama / Name Constraints.....	60
7.1.6	Pengidentifikasi Objek Kebijakan Sertifikat / Certificate Policy Object Identifier.....	60
7.1.7	Penggunaan Ekstensi Batasan Kebijakan / Usage of Policy Constraints Extension.....	60
7.1.8	Kualifikasi Kebijakan Sintaksis dan Semantik / Policy Qualifiers Syntax and Semantics	60
7.1.9	Memproses Semantik untuk Ekstensi Kebijakan Sertifikat Kritis / Processing Semantics for the Critical Certificate Policies Extension.....	60
7.2	PROFIL CRL / CRL PROFILE.....	60
7.2.1	Nomor Versi / Verion Number(s).....	60
7.2.2	CRL dan Ekstensi Entri CRL / CRL and CRL Entry Extension.....	60
7.3	OCSP PROFILE / PROFIL OCSP	61
7.3.1	Nomor Versi / Version Number(s)	61
7.3.2	OCSP Extensions / Ekstensi OCSP	61
8.	AUDIT KEPATUHAN DAN ASESMEN LAIN / COMPLIANCE AUDIT AND OTHER ASSESSMENTS	62
8.1	FREKUENSI ATAU KEADAAN ASESMEN / FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	62

8.2	IDENTITAS/KUALIFIKASI ASESOR / IDENTITY/QUALIFICATIONS OF ASSESSOR.....	62
8.3	HUBUNGAN ASESOR DENGAN BADAN YANG DINILAI / ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	62
8.4	TOPIK YANG DICAKUP OLEH ASESMEN / TOPICS COVERED BY ASSESSMENT.....	62
8.5	TINDAKAN YANG DIAMBIL SEBAGAI HASIL DARI KEKURANGAN / ACTIONS TAKEN AS A RESULT OF DEFICIENCY	63
8.6	KOMUNIKASI HASIL / COMMUNICATION OF RESULTS	63
8.7	AUDIT INTERNAL / INTERNAL AUDIT	63
9.	BISNIS LAIN DAN MASALAH HUKUM / OTHER BUSINESS AND LEGAL MATTERS.....	64
9.1	BIAYA / FEES	64
9.1.1	Biaya Penerbitan atau Pembaruan Sertifikat / Certificate Issuance or Renewal Fees	64
9.1.2	Biaya Pengaksesan Sertifikat / Certificate Access Fees	64
9.1.3	Biaya Pengaksesan Informasi atau Pencabutan Sertifikat / Revocation or Status Information Access Fees	64
9.1.4	Biaya Layanan Lainnya / Fees for Other Services	64
9.1.5	Kebijakan Pengembalian Biaya / Refund Policy	64
9.2	TANGGUNG JAWAB KEUANGAN / FINANCIAL RESPONSIBILITY	64
9.2.1	Cakupan Asuransi / Insurance Coverage.....	64
9.2.2	Aset Lainnya / Other Assets.....	64
9.2.3	Jaminan Asuransi atau Garansi untuk Entitas Akhir / Insurance or Warranty Coverage for End-Entities	65
9.3	KERAHASIAAN INFORMASI BISNIS / CONFIDENTIALITY OF BUSINESS INFORMATION	65
9.3.1	Cakupan Informasi Rahasia / Scope of Confidential Information	65
9.3.2	Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia / Information Not Within the Scope of Confidential Information.....	65
9.3.3	Tanggung Jawab untuk Melindungi Informasi yang Rahasia / Responsibility to Protect Confidential Information	65
9.4	PRIVASI INFORMASI PRIBADI / PRIVACY OF PERSONAL INFORMATION.....	66
9.4.1	Rencana Privasi / Privacy Plan	66
9.4.2	Informasi yang Dianggap Pribadi / Information Treated as Private	66
9.4.3	Informasi tidak Dianggap Pribadi / Information not Deemed Private.....	66
9.4.4	Tanggung Jawab Melindungi Informasi Pribadi / Responsibility to Protect Private Information	66
9.4.5	Catatan dan Persetujuan untuk memakai Informasi Pribadi / Notice and Consent to use Private Information.....	67
9.4.6	Pengungkapan Berdasarkan Proses Peradilan atau Administratif / Disclosure Pursuant to Judicial or Administrative Process	67
9.4.7	Keadaan Pengungkapan Informasi Lain / Other Information Disclosure Circumstances.....	67
9.5	HAK ATAS KEKAYAAN INTELEKTUAL / INTELLECTUAL PROPERTY RIGHTS	67
9.6	PERNYATAAN DAN JAMINAN / REPRESENTATIONS AND WARRANTIES	67
9.6.1	Pernyataan dan Jaminan Peruri CA / Peruri CA Representations and Warranties	67

9.6.2	Pernyataan dan Jaminan RA / RA Representations and Warranties	68
9.6.3	Pernyataan dan Jaminan Pemilik Sertifikat / Subscriber Representations and Warranties.....	68
9.6.4	Pernyataan dan Perjanjian Pihak Pengandal / Relying Party Representations and Warranties..	70
9.6.5	Representations and Warranties of other Participants / Pernyataan dan Jaminan Partisipan Lain	70
9.7	PELEPASAN JAMINAN / DISCLAIMER OF WARRANTIES.....	70
9.8	PEMBATASAN TANGGUNG JAWAB / LIMITATIONS OF LIABILITY	71
9.8.1	Pembatasan Tanggung Jawab Peruri CA / Peruri CA Limitations of Liability	71
9.8.2	Pembatasan Tanggung Jawab RA / RA Limitation of Liability	71
9.9	GANTI RUGI / INDEMNITIES	72
9.9.1	Ganti Rugi oleh Peruri CA / Indemnification by Peruri CA	72
9.9.2	Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Subscriber	72
9.9.3	GantiRugi oleh Pihak Pengandal / Indemnification by Relying Parties.....	72
9.10	SYARAT DAN PENGAKHIRAN / TERM AND TERMINATION	72
9.10.1	Syarat / Term	72
9.10.2	Pengakhiran / Termination.....	72
9.10.3	Efek Pengakhiran dan Keberlangsungan / Effect of Termination and Survival.....	72
9.11	PEMBERITAHUAN INDIVIDU DAN KOMUNIKASI DENGAN PARTISIPAN / INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	72
9.12	AMANDEMEN / AMENDMENTS	73
9.12.1	Prosedur untuk Amandemen / Procedure for Amendment	73
9.12.2	Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period	73
9.12.3	Keadaan Dimana OID Harus Diubah / Circumstances Under Which OID Must be Changed	73
9.13	PROVISI PENYELESAIAN KETIDAKSEPAHAMAN / KETENTUAN PENYELESAIAN SENGKETA / DISPUTE RESOLUTION PROVISIONS	73
9.14	HUKUM YANG MENGATUR / GOVERNING LAW	74
9.15	KEPATUHAN ATAS HUKUM YANG BERLAKU / COMPLIANCE WITH APPLICABLE LAW	74
9.16	KETENTUAN YANG BELUM DIATUR / MISCELLANEOUS PROVISIONS	74
9.16.1	Seluruh Perjanjian / Entire Agreement	74
9.16.2	Pengalihan Hak / Assignment.....	74
9.16.3	Keterpisahan / Severability	74
9.16.4	Penegakan Hukum (Biaya Pengacara dan Pengalihan Hak-hak) / Enforcement (Attorneys' Fees and Waiver of Rights).....	75
9.16.5	Keadaan Memaksa / Force Majeure	75
9.17	PROVISI LAIN / OTHER PROVISIONS	76

1. PENGANTAR / INTRODUCTION

1.1 RINGKASAN / OVERVIEW

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

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

Dokumen ini, "Certificate Policy Peruri CA" (CP) diatur oleh CP PSrE Induk Indonesia dan mendefinisikan persyaratan prosedural dan operasional yang dianut oleh Peruri CA saat menerbitkan dan mengelola objek yang ditandatangani secara digital dalam Peruri CA.

This document, "Peruri CA Certificate Policy" (CP) is governed under the Root CA Indonesia CP and defines the procedural and operational requirements that Peruri CA adheres to when issuing and managing digitally signed objects within PeruriCA

CP 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 CP is consistent with Request for Comments 3647 (RFC 3647) of the Internet Engineering Task Force (IETF) 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 Certificate Policy (CP) Peruri CA. Object Identifier (OID) yang digunakan untuk sertifikat (tidak termasuk Extended Validation Certificate) ini adalah: 2.16.360.1.1.1.3.12.3.1

The document is Certificate Policy of Peruri CA. Object Identifier (OID) used for certificates (not including Extended Validation Certificate) for this CP is: 2.16.360.1.1.1.3.12.3.1

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

1.3 PARTISIPAN IKP / PKI PARTICIPANTS

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE) / Certification Authorities

1.3.1.1 PSrE Induk Indonesia / Root CA Indonesia

PSrE Induk Indonesia adalah PSrE Induk dari *Root CA Indonesia is the root CA of Indonesia*

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

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

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

PKI. Root CA Indonesia issues and revokes certificates to Peruri CA as a Non-Government CA based on the status of recognition given by MCIT.

Root CA Indonesia is responsible for all aspects of the issuance and management, as detailed in this CP, including:

- *The control over the registration process,*
- *The identification and authentication process,*
- *The Certificate manufacturing process,*
- *The publication of Certificates,*
- *The revocation of Certificates, and*
- *Ensuring that all aspects of the services, operations, and infrastructure related to Peruri CA Certificates issued under this CP were performed in accordance with the requirements, representations, and warranties of this CP.*

1.3.1.2 Peruri CA

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

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

1.3.2 Otoritas Pendaftaran (RA) / Registration Authorities

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

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

1.3.2.1 Fungsi dari RA / Function of Registration Authorities

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

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

- Menyusun prosedur pendaftaran untuk
- *Establish enrollment procedures for end-*

Pemohon sertifikat;	<i>user certificate applicants,</i>
• Melakukan identifikasi dan otentikasi Pemohon sertifikat;	• <i>Perform identification and authentication of certificate applicants,</i>
• Memulai atau meneruskan proses permohonan pembatalan sertifikat; dan	• <i>Initiate or pass along revocation requests for certificates, and</i>
• Menyetujui permohonan untuk memperbaharui sertifikat atau pembaharuan kunci atas nama Peruri CA.	• <i>Approve applications for certificates renewal or re-keying on behalf of a Peruri CA.</i>

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

Tidak ada ketentuan.	<i>No stipulation.</i>
----------------------	------------------------

1.3.3 Pemilik / Subscribers

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

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

1.3.4 Pihak Pengandal / Relying Parties

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

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

Pihak Pengandal adalah entitas yang mempercayai keabsahan keterkaitan antara nama pemilik dengan kunci publik. Pihak Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat.

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

Pihak Pengandal menggunakan informasi dalam Sertifikat Digital untuk:

Relying party uses the information in the Digital Certificate to:

- | | |
|---|--|
| • Memeriksa tujuan penggunaan sertifikat | • <i>Check the intended use of the certificate</i> |
| • Melakukan verifikasi tanda tangan digital | • <i>Perform digital signature verification</i> |

- Memeriksa apakah Sertifikat Digital termasuk di dalam CRL
- *Checks whether a Digital Certificate is included in the CRL*
- Penyetujuan batas tanggung jawab dan jaminan.
- *Approval of limits of liability and guarantees.*

1.3.5 Partisipan Lain / Other Participants

1.3.5.1 Otoritas Kebijakan / Policy Authority

Peran Otoritas Kebijakan (PA) memiliki tanggung jawab yang berkaitan dengan CP yaitu sebagai berikut:

The role of the Policy Authority (PA) has responsibilities related to CP, which are as follows:

- Mendapatkan persetujuan untuk Certificate Policy (CP) dari Management Peruri
- *Obtain approval for the Certificate Policy (CP) from Peruri Management*
- Memastikan bahwa semua aspek layanan, operasional, dan infrastruktur Peruri CA seperti yang dijelaskan dalam CPS dilakukan sesuai dengan persyaratan, representasi, dan jaminan CP.
- *Ensures that all aspects of the Peruri CA services, operations, and infrastructure as described in the CPS are performed in accordance with the requirements, representations, and warranties of the CP.*
- Memastikan bahwa CP dan CPS selaras dengan CP dan CPS PSrE Induk Indonesia.
- *Ensures that the CP and CPS is aligned with the Root CA Indonesia CP and CPS.*

1.4 KEGUNAAN SERTIFIKAT / CERTIFICATE USAGE

1.4.1 Penggunaan Sertifikat yang Semestinya / Appropriate Certificate Uses

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

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

- Autentikasi;
- *Authentication;*
- Tanda Tangan Elektronik & Nir-Sangkal; serta
- *Digital Signature & Non-Repudiation; and*
- Enkripsi
- *Encryption*

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

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

- Level 3: Sertifikat dengan Tingkat Jaminan Sedang Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap Data identitas yang dimiliki oleh pemerintah.
- *Level 3: Medium Assurance Certificate Medium Assurance Certificate, which verifies identities with Government-owned identity data.*

- Level 4: Sertifikat dengan Tingkat Jaminan Tinggi Verifikasi identitas dilakukan dengan membandingkan kesesuaian terhadap data identitas yang dimiliki oleh pemerintah dan data biometrik.
- *Level 4: High Assurance Certificate High Assurance Certificate, which verifies identities with Government-owned identity data and biometric data.*

Penggunaan yang tidak sesuai dapat berakibat pada hilangnya jaminan yang diberikan oleh Peruri CA kepada Pemilik dan Pihak Pengandal. *Unauthorised use of Certificates may result in the voiding of warranties offered by Peruri CA to Subscribers and their Relying Parties.*

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

Sertifikat yang diterbitkan di bawah CP ini dapat digunakan untuk tujuan yang ditentukan dalam field key usage dan extended key usage yang ditemukan dalam sertifikat. *Certificate issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate.*

1.4.2 Penggunaan Sertifikat yang Dilarang / Prohibited Certificate Uses

Sertifikat yang diterbitkan di bawah CP ini dilarang dipakai untuk penggunaan yang tidak dinyatakan dalam Bagian 1.4.1. *Certificate issued under this CP are prohibited under any use not specified in Section 1.4.1.*

1.5 ADMINISTRASI KEBIJAKAN / POLICY ADMINISTRATION

Policy Authority (PA) adalah entitas yang ada di dalam Peruri CA. PA memiliki peran dan tanggung jawab sebagai berikut: *Policy Authority (PA) is an internal entity of a Peruri CA. The PA has roles and responsibilities as follows:*

- Menetapkan Certificate Policy (CP);
- Memastikan semua layanan, operasional, dan infrastruktur PSrE yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan
- *Approves the Certificate Policy (CP);*
- *Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are well performed in accordance with the requirements,*

dari CP; dan

representations, and warranties of the CP; dan

- Menyetujui terjalannya hubungan kepercayaan dengan IKP eksternal yang memiliki Tingkat Jaminan yang kurang lebih setara.
- *Approves the establishment of trust relationships with external PKIs that approximately have equivalent Level of Assurance.*

1.5.1 Organisasi Pengaturan Dokumen / Organization Administering the Document

CP dan dokumen referensinya dikelola oleh: *This CP and the document referenced herein are maintained by:*

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

1.5.2 Narahubung / Contact Person

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

1.5.3 Personil yang menentukan Kesesuaian CPS dengan Kebijakan / Person Determining CPS Suitability for the Policy

Peruri CA mempekerjakan Otoritas Kebijakan (PA) untuk memastikan kesesuaian CPS dengan CP ini dan bahwa CPS ini sejalan dengan CP Peruri CA. *Peruri CA employs a Policy Authority (PA) to ensure conformance of the CPS to this CP and that this CPS is inline with the Peruri CA's CP.*

1.5.4 Prosedur Persetujuan CP & CPS / CP & CPS Approval Procedures

Otoritas Kebijakan Peruri CA menyetujui CP/CPS dan segala perubahannya. Perubahan dibuat dengan mengubah seluruh CP/CPS atau dengan mempublikasikan addendum. Otoritas Kebijakan Peruri CA menentukan apakah perubahan atas CP ini membutuhkan pemberitahuan atau perubahan OID. *Peruri CA Policy Authority approves the CP/CPS and any amendments. Amendments are made by either updating the entire CP/CPS or by publishing an addendum. Peruri CA Policy Authority determines whether an amendment to this CP requires notice or an OID change.*

1.6 DEFINISI DAN AKRONIM / DEFINITIONS AND ACRONYMS

1.6.1 Definisi / Definitions

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

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

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

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

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

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

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

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

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

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

“Pihak Penghandal” entitas yang mempercayai pada informasi yang terkandung dalam sertifikat atau token stempel waktu.

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

1.6.2 Akronim / Acronyms

CA	: Certificate Authority or Certification Authority
CP	: Certificate Policy
CPS	: Certification Practice Statement
CRL	: Certificate Revocation List
CSR	: Certificate Signing Request
IETF	: Certificate Signing Request
ITU	: International Telecommunication Union
ITU-T	: ITU Telecommunication Standardization Sector
OCSP	: Online Certificate Status Protocol
OID	: Object Identifier
PKI	: Public Key Infrastructure
PKCS	: Public Key Cryptography Standard

RA : *Registration Authority*
SSL : *Secure Sockets Layer*
TLS : *Transport Layer Security*
X.509 : *The ITU-T standard for Certificates and their corresponding authentication framework*

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

2.1 REPOSITORI / REPOSITORIES

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

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

2.2 PUBLIKASI INFORMASI SERTIFIKASI / PUBLICATION OF CERTIFICATION INFORMATION

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

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

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

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

Repositori dokumen Peruri dapat diakses pada <https://ca.peruri.co.id/ca/legal>.

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

2.3 WAKTU ATAU FREKUENSI PUBLIKASI / TIME OR FREQUENCY OF PUBLICATION

CP ini dan tiap perubahan selanjutnya harus dapat diakses publik dalam tujuh (7) hari kalender setelah disetujui. Peruri CA harus mempublikasikan sertifikat Pemilik dan data pencabutan sertifikat dalam waktu tiga puluh (30) menit setelah penerbitan.

This CP and any subsequent changes shall be made publicly available within seven (7) calendar days after its approval. Peruri CA shall publish Subscriber certificates and revocation data within thirty (30) minutes after issuance.

CRL diperbaharui sesuai pengaturan pada bagian 4.9.7.

CRL diperbaharui sesuai pengaturan pada bagian 4.9.7.

2.4 KENDALI AKSES PADA REPOSITORI / ACCESS CONTROLS ON REPOSITORIES

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

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

Peruri CA harus melindungi informasi yang tidak ditujukan untuk disebarkan kepada

Peruri CA shall protect information not intended for public dissemination or

publik atau diubah oleh publik *modification (adding, deleting, or modifying repository entries)*.
(menambahkan, menghapus, atau mengubah entri repositori).

3. IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION

3.1 PENAMAAN / NAMING

3.1.1 Tipe Nama / Types of Names

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

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

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

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

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

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

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

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

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

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

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

3.1.3 Anonimitas atau Pseudonimitas Pemilik / Anonymity or Pseudonymity of Subscribers

Peruri CA tidak akan menerbitkan sertifikat anonim atau pseudonim.

Peruri CA shall not issue anonymous or pseudonymous certificates.

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

Distinguished Name (DN) dalam sertifikat diinterpretasikan menggunakan standar X.500. *Distinguished Name (DN) in Certificates are interpreted using X.500 standards.*

3.1.5 Keunikan Nama / Uniqueness of Names

Distinguished Name (DN) dalam sertifikat harus unik di dalam ranah Peruri CA. *Distinguished Names in Certificates shall be unique within Peruri CA domain.*

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

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. Peruri CA tidak perlu memverifikasi hak Pemohon untuk penggunaan merek dagang. Merupakan tanggung jawab Pemilik untuk memastikan penggunaan nama-nama pilihan yang sah. *Subscriber may not request certificates with any content that infringes the intellectual property rights of another parties. Peruri CA is not required to verify an applicant's right to use a trademark. It is the sole responsibility of the subscriber to ensure lawful use of chosen names.*

Peruri CA dapat menolak setiap permohonan atau melakukan pencabutan Sertifikat apapun yang menjadi bagian dari konflik merek dagang. *Peruri CA may reject any application or require revocation of any certificate that is part of a trademark dispute.*

3.2 VALIDASI IDENTITAS AWAL / INITIAL IDENTITY VALIDATION

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

Metode untuk membuktikan kepemilikan kunci privat harus PKCS#10, atau permintaan lain yang ekuivalen secara kriptografi (permintaan ditandatangani secara digital dengan kunci privat). Pasangan kunci dibuat oleh Peruri Digital Bisnis. *The method to prove possession of a private key shall be PKCS #10, or another cryptographically equivalent request (digitally signed request with private key). The key pair is generated by Peruri Digital Business.*

- Pemilik menyerahkan kunci publik
- Pemilik menyerahkan CSR secara luring
- *Subscribers submit public key*
- *Subscribers submit CSR offline*

3.2.2 Autentikasi Identitas Organisasi / Authentication of Organization Identity

Permohonan dari organisasi untuk menjadi pemilik sertifikat harus dibuat oleh orang yang berwenang mewakili organisasi tersebut. Permohonan ini harus mengikuti persyaratan seperti yang tercantum dalam CPS Peruri CA dan menyertakan rincian tentang organisasi dan Salinan surat-surat pendirian perusahaan yang dilegalisir. *An application for organization to become a Subscriber shall be made by a person authorized to act on behalf of the organization. The details of this application shall conform to the requirements as set forth in the issuer Peruri CA's CPS and include details about the organization and include a certified true copy of their incorporation papers.*

Peruri CA memverifikasi identitas dan status kepegawaian dari individu yang membuat permohonan dan otorisasinya untuk menerima sertifikat untuk organisasi tersebut.

Peruri CA verifies the identity and employment status of the individual making the application and their authority to receive the keys for that organization.

Peruri CA menyimpan dokumen dan catatan jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

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

3.2.3 Autentikasi Identitas Individu / Authentication of Individual Identity

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

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

Peruri CA harus menyimpan dokumen dan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya untuk selama masa berlaku dari sertifikat yang diterbitkan.

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

Autentikasi identitas individu pemohon sertifikat pengguna harus sesuai dengan Peraturan Menteri Komunikasi dan Informatika No. 11/2018. Untuk informasi lebih detail bisa dilihat pada CPS bagian 3.2.3.

Authentication of applicant's individual identity shall comply with Ministry Regulation of Communication and Informatics No. 11/2018. Detailed information as described in CPS poin 3.2.3.

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

Informasi yang tidak bisa diverifikasi tidak boleh disertakan pada sertifikat.

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

3.2.5 Validasi Otoritas / Validation of Authority

Sertifikat yang mencantumkan afiliasi organisasi secara eksplisit atau implisit harus diterbitkan hanya setelah memastikan bahwa Pemohon memiliki otorisasi untuk bertindak atas nama organisasinya.

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

3.2.6 Kriteria Inter-Operasi / Criteria for Interoperation / Kriteria Inter-Operasi

Tidak ada ketentuan.

No stipulation.

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

3.3.1 Identifikasi dan Autentikasi untuk kegiatan Penggantian Kunci / Identification and Authentication for Routine Re-Key

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

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

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

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

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

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

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

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

Pencabutan sertifikat harus memenuhi salah satu dari proses berikut:

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

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

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

Prosedur bagaimana permintaan pencabutan dapat diajukan dijelaskan di bagian 4.9.3.

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

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

4.1 PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION

4.1.1 Siapa yang dapat mengajukan permohonan sertifikat / Who can submit a Certificate Application

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

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

4.1.2 Proses Pendaftaran dan Tanggung Jawab / Enrollment Process and Responsibilities

Peruri CA harus memelihara sistem dan proses yang mampu mengautentikasi identitas Pemohon untuk semua jenis Sertifikat dimana Sertifikat yang dimaksud menampilkan identitas kepada Pihak Pengandal atau Pemilik. Pemohon harus memberikan informasi yang cukup sehingga memungkinkan Peruri CA dan RA untuk melakukan verifikasi atas identitas tersebut. Peruri CA dan RA harus melindungi komunikasi dan menyimpan dengan aman informasi yang diberikan oleh pemohon selama proses permohonan.

Peruri CA shall maintain systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties or Subscribers. Applicants should submit sufficient information to allow Peruri CA and RA to successfully perform the required verification. Peruri CA and RA shall protect communications and securely store information presented by the Applicant during the enrollment process.

Pemohon harus menyetujui kontrak berlangganan yang ditetapkan oleh Peruri CA sebelum melakukan pendaftaran. Untuk keterangan lebih rinci, harap mengacu pada CPS terkait.

Applicants shall accept a subscription agreement before the enrollment process. For further details, please refer to the related CPS.

4.2 PEMROSESAN PERMOHONAN SERTIFIKAT / CERTIFICATE APPLICATION PROCESSING

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

Identifikasi dan autentikasi Pemilik harus memenuhi persyaratan yang ditentukan seperti yang tertera pada Bagian 3.2 dari CP ini. Untuk keterangan lebih rinci, harap mengacu pada CPS terkait.

The identification and authentication of the Subscriber shall meet the requirements specified in Sections 3.2 of this CP. For further details, please refer to the related CPS.

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

Setelah semua pemeriksaan identitas dan atribut Pemohon, konten aplikasi untuk sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap sertifikat atau permohonannya mengandung kesalahan, Peruri CA harus menolak permohonan. Apabila tidak ada masalah, permohonan akan disetujui.

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

4.2.3 Waktu Pemrosesan Permohonan Sertifikat / Time to Process Certificate Applications

Semua pihak yang terlibat dalam pemrosesan permohonan sertifikat harus melakukan usaha untuk memastikan permohonan sertifikat diproses tepat waktu. Untuk keterangan lebih rinci, harap mengacu pada CPS terkait.

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. For further details, please refer to the related CPS.

4.3 PENERBITAN SERTIFIKAT / CERTIFICATE ISSUANCE

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

Peruri CA memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat harus diperiksa untuk memastikan semua isian dan keterangan tambahan telah diisi dengan benar.

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

Peruri CA harus mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, baru kemudian membuat Sertifikat milik Pemohon dan menyerahkan Sertifikat kepada Pemohon.

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

Peruri CA harus menerbitkan Sertifikat ke repositori sesuai dengan CP ini dan CPS yang berlaku. Ini harus dilakukan sesuai waktu dimana Peruri CA akan melakukan tindakannya selama proses penerbitan sertifikat secara aman.

Peruri CA shall publish the Certificate to a repository in accordance with this CP and the applicable CPS. This shall be done in a timely manner, which is Peruri CA shall perform its actions during the certificate issuance process in a secure manner.

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

Peruri CA harus memberitahu Pemilik dalam selang waktu yang wajar tentang berhasilnya penerbitan sertifikat sesuai dengan prosedur yang diatur dalam CPS terkait.

Peruri CA shall notify the Subscriber within a reasonable time of successful certificate issuance in accordance with procedures set forth in the applicable CPS.

4.4 PENERIMAAN SERTIFIKAT / CERTIFICATE ACCEPTANCE

4.4.1 Sikap Yang Dianggap Sebagai Menerima Sertifikat / Conduct Constituting Certificate Acceptance

Peruri CA harus memberitahu Pemilik bahwa mereka tidak dapat memakai Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

Peruri CA shall notify to the Subscriber that they cannot use the certificate before checking all the information of certificate.

Ketika tidak ada keluhan dari Pemilik dalam jangka waktu tujuh (7) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat.

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

Untuk penerbitan Sertifikat Pemilik, Peruri CA telah menyiapkan prosedur penerimaan yang mengindikasikan dan mendokumentasikan penerimaan atas Sertifikat yang diterbitkan pada CPS bagian 4.4.1.

For the issuance of Subscribers Certificates, Peruri CA shall follow the acceptance procedure indicating and documenting the acceptance of the issued Subscribers Certificate defined in CPS Section 4.4.1.

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

Peruri CA harus mempublikasikan Sertifikat dalam suatu repositori, termasuk ketika menerbitkan informasi pencabutan terkait Sertifikat tersebut pada repositori yang didefinisikan pada CPS bagian 4.4.2.

Peruri CA shall publish certificates in a repository based on the certificate publishing practices of the Peruri CA (as defined in the CPS), as well as revocation information concerning such certificates in a repository as defined in CPS Section 4.4.2.

Semua sertifikat harus dipublikasikan dalam repositori, sesuai dengan bagian 2.2, segera setelah diterbitkan.

All certificates shall be published in repository according to section 2.2 as soon as they are issued.

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

Tidak ada ketentuan.

No stipulation.

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

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

Pemilik harus melindungi Kunci Privatnya dari penggunaan tanpa izin atau pengungkapan oleh pihak lain, menggunakan modul kriptografi yang dikendalikan oleh Pemilik. Pemilik yang menitipkan kunci privatnya kepada pihak ketiga, maka pihak ketiga tersebut harus melindungi kunci privat Pemilik dengan menggunakan Hardware Security Module. Pemilik harus memakai kunci privatnya hanya untuk tujuan yang sudah

Subscribers shall protect their Private Key from unauthorized use or disclosure by other parties using a cryptographic module that is controlled by the Subscribers. In case of Subscriber escrowed their private key to a third party, that third party is obliged to protect the subscriber's private key using Hardware Security Module. Subscribers shall use their private key only for the designated purpose.

ditentukan.

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

Pihak Pengandal harus menggunakan perangkat lunak yang sesuai standar X.509. Peruri CA harus menyatakan pembatasan penggunaan Sertifikat melalui ekstensi sertifikat dan harus menyatakan mekanisme untuk menentukan keabsahan sertifikat (CRL dan OCSP). Pihak Pengandal harus memproses dan patuh kepada informasi ini sesuai dengan kewajiban mereka sebagai Pihak Pengandal.

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

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

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

4.6 PEMBARUAN SERTIFIKAT / CERTIFICATE RENEWAL

4.6.1 Kondisi untuk Pembaruan Sertifikat / Circumstance for Certificate Renewal

Peruri CA dapat memperbarui Sertifikat Pemilik selama:

- Sertifikat asli yang akan diperbarui belum dicabut;
- Kunci Publik dari Sertifikat asli belum masuk daftar hitam karena alasan apa pun; dan
- Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan.
- Peruri CA dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya.
- Berisi informasi yang sama (identitas, domain, dll.) Seperti sertifikat lama.

Peruri CA may renew a Subscriber Certificate so long as:

- *The original Certificate to be renewed has not been revoked;*
- *The Public Key from the original Certificate has not been blacklisted for any reason; and*
- *All details within the Certificate remain accurate and no new or additional validation is required.*
- *Peruri CA may renew Certificates which have either been previously renewed.*
- *Contains the same information (identity, domain, etc.) as the old certificate.*

- Memiliki periode validitas baru yang berakhir setelah periode validitas sertifikat lama.
- Berisi kunci publik yang sama dengan sertifikat lama.
- *Has a new validity period which ends after the old certificate validity period.*
- *Contains the same public key as the old certificate.*

Selain itu, periode validitas Sertifikat tidak boleh melebihi masa berlaku Kunci Privat, sebagaimana ditentukan dalam Bagian 5.6. Persyaratan pemeriksaan identitas yang tercantum dalam Bagian 3.3.1 juga harus dipenuhi.

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

4.6.2 Siapa Yang Dapat Meminta Pembaruan / Who May Request Renewal

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

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

4.6.3 Pemrosesan Permintaan Pembaruan Sertifikat / Processing Certificate Renewal Requests

Perpanjangan sertifikat harus menggunakan salah satu dari proses berikut:

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

- Proses pendaftaran awal seperti yang dijelaskan dalam Bagian 3.2; atau
- Identifikasi & Otentikasi untuk Re-key seperti yang dijelaskan dalam Bagian 3.3, kecuali kunci lama masih dapat digunakan sebagai kunci baru.
- *Initial registration process as described in Section 3.2; or*
- *Identification & Authentication for Re-key as described in Section 3.3, except the old key can also be used as the new key.*

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

Prosedur penerbitan sertifikat baru sebagaimana dinyatakan pada bagian 4.3.2.

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

4.6.5 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Diperbarui / Conduct Constituting Acceptance of a Renewal Certificate

Pemilik dapat menerima sertifikat yang telah diperbarui sesuai dengan prosedur pendaftaran dan penerimaan sertifikat yang dinyatakan dalam bagian 4.4.1.

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

4.6.6 Publikasi Sertifikat yang Diperbarui oleh Peruri CA / Publication of the Renewal Certificate by the Peruri CA

Sertifikat baru diterbitkan sesuai prosedur yang tercantum dalam bagian 4.4.2. *The new certificate is published according to the procedures stated in section 4.4.2.*

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

Tidak ada Ketentuan. *No Stipulation.*

4.7 PENGGANTIAN KUNCI SERTIFIKAT / CERTIFICATE RE-KEY

Penggantian kunci sertifikat adalah penerbitan kembali sertifikat menggunakan informasi subjek dan tanggal kadaluarsa ("validTo" field) yang sama tetapi dengan pasangan kunci yang baru. Namun, Peruri CA tidak melakukan penggantian kunci sertifikat Pemilik. *Certificate re-key is the re-issuance of a certificate using the same subject information and expiration date ("validTo" field) but with a new key pair. However, Peruri CA does not re-key from subscriber.*

4.7.1 Lingkup Penggantian Kunci Sertifikat / Circumstance for Certificate Re-Key

Penggantian kunci (*re-key*) sertifikat adalah penerbitan ulang suatu sertifikat yang memakai informasi subyek dan tanggal kadaluarsa yang sama (*field "validTo"*) tetapi dengan pasangan kunci yang baru. *Certificate re-keying is the re-issuance of a certificate using the same subject information and expiration date ("validTo" field) but with a new key-pair.*

Peruri CA dapat melakukan penggantian kunci selama: *Peruri CA may re-key a Certificate as long as:*

- Sertifikat asli yang diganti belum pernah dibatalkan/dicabut;
- Kunci Publik yang baru tidak pernah didaftarkan ke daftar hitam dengan alasan apa pun;
- Seluruh rincian yang terkait dengan Sertifikat tersebut tetap akurat dan tidak dibutuhkan validasi baru dan tambahan; dan
- Kunci Privat Peruri CA bocor.
- *The original Certificate to be re-keyed has not been revoked;*
- *The new public key has not been blacklisted for any reason;*
- *All details within the Certificate remain accurate and no new or additional validation is required; and*
- *Peruri CA private key compromise.*

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

Sesuai dengan kondisi yang ditentukan pada bagian 4.7.1, hanya Peruri CA yang dapat meminta dan melakukan penggantian kunci publik yang baru. *According to the conditions specified in section 4.7.1, only CA Peruri may request and perform a new public key replacement.*

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

Berlaku prosedur Penerbitan Sertifikat seperti yang dinyatakan pada bagian 4.3. *The same re-key issuance procedure is followed, as stated in section 4.3.*

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

Berlaku prosedur yang sama dengan yang dinyatakan pada bagian 4.3.2. *The same re-key issuance procedure is followed, as stated in section 4.3.2.*

4.7.5 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Kuncinya Digantikan / Conduct Constituting Acceptance of a Re-Keyed Certificate

Pemilik harus menerima sertifikat dengan kunci baru, mengikuti prosedur penerimaan yang sama, sebagaimana diuraikan dalam bagian 4.4.1. *The subscriber MUST receive the certificate with the new key, following the same acceptance procedure, as described in section 4.4.1.*

4.7.6 Publikasi Sertifikat yang Kuncinya Digantikan oleh Peruri CA / Publication of the Re-Keyed Certificate by Peruri CA

Sertifikat dengan kunci baru dipublikasikan, sesuai dengan prosedur repositori, yang dinyatakan dalam bagian 4.4.2. *The certificate with the new key is published, according to the repository procedures, as stated in section 4.4.2.*

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

Tidak ada ketentuan. *No Stipulation.*

4.8 MODIFIKASI SERTIFIKAT / CERTIFICATE MODIFICATION

Modifikasi rincian sertifikat tidak diizinkan. Dalam hal terjadi kesalahan selama penerbitan sertifikat (contohnya ejaan), sertifikat dicabut dan diikuti dengan proses penerbitan ulang kunci, seperti yang dinyatakan pada bagian 4.3. *Modification of certificate details is not permitted. In case there is a mistake during certificate issuance (e.g. spelling), the certificate is revoked and the re-key issuance process is followed, as stated in section 4.3.*

4.8.1 Keadaan Bagi Modifikasi Sertifikat / Circumstance for Certificate Modification

Modifikasi informasi sertifikat tidak diizinkan. *Modification of certificate information is not permitted.*

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

Tidak ada ketentuan. *No stipulation.*

4.8.3 Pemrosesan Permintaan Modifikasi Sertifikat / Processing Certificate Modification Requests

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

4.8.5 Sikap yang Dianggap Sebagai Menerima Sertifikat yang Dimodifikasi / Conduct Constituting Acceptance of Modified Certificate

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

4.9 PENCABUTAN DAN PEMBEKUAN SERTIFIKAT / CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Keadaan untuk Pencabutan / Circumstances for Revocation

Peruri CA harus mencabut sertifikat Pemilik dalam keadaan berikut: *Peruri CA shall revoke a subscriber's certificate in the following circumstances:*

- Komponen informasi identifikasi atau afiliasi dari nama dalam sertifikat menjadi tidak valid. *Identifying information or affiliation components of any names in the certificate becomes invalid.*
- Informasi apapun dalam sertifikat menjadi tidak valid. *Any information in the certificate becomes invalid.*
- Pemilik dapat ditunjukkan telah melanggar ketentuan dalam kontrak berlangganannya. *The subscriber can be shown to have violated the stipulations of its subscriber agreement.*
- Ada alasan untuk meyakini bahwa kunci privat telah dikompromikan/rusak. *There is reason to believe the private key has been compromised.*
- Pemilik atau pihak berwenang lainnya *The subscriber or other authorized party*

meminta sertifikatnya dicabut.

(as defined in the CPS) asks for his/her certificate to be revoked.

- PSrE Berindak berhenti beroperasi.
- Sertifikat yang dibuat untuk uji coba.
- Peruri CA termination.
- The certificate is issued for trial run.

Sertifikat harus dicabut ketika hubungan antara subyek dan kunci publiknya yang didefinisikan dalam sertifikat sudah tidak valid lagi. Ketika hal ini terjadi sertifikat seharusnya dicabut dan diletakkan pada CRL dan/atau ditambahkan pada responder OCSP.

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. When this occurs the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder.

Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status sertifikat sampai sertifikat kadaluwarsa.

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

4.9.2 Siapa yang Dapat Meminta Pencabutan / Who can Request Revocation

Sertifikat dapat diminta untuk dicabut oleh Pemilik atau entitas lain yang dapat membuktikan terungkapnya kunci privat atau penyalahgunaan sertifikat sesuai dengan *Certification Policy*.

The certificate can be requested to be revoked by the subscriber or by another entity that can prove the exposure or the misuse of the certificate according to the Certification Policy.

4.9.3 Prosedur Permintaan Pencabutan / Procedure for Revocation Request

Peruri CA harus memverifikasi identitas dan wewenang (untuk entitas penegak hukum) dari Pemilik yang mengajukan pencabutan sertifikat. Validitas identitas Pemilik dibutuhkan sesuai dengan bagian 3.4.

Peruri CA shall verify the identity and authority (for juridical entity) of a subscriber making the request for revocation. The validation of the subscriber's identity is required according to section 3.4.

Permintaan pencabutan Sertifikat oleh entitas lain harus menyerahkan bukti bahwa:

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

- Kunci privat sertifikat telah terungkap, atau
- Penggunaan sertifikat tidak sesuai dengan *Certification Policy*, atau
- Pemilik sertifikat tidak memiliki hubungan dengan institusi
- The private key of the certificate has been exposed, or
- The use of the certificate does not conform to the Certification Policy or
- The certificate owner's relationship with the institution does not exist

Langkah-langkah pada proses permintaan pembatalan sertifikat dijelaskan lebih rinci dalam CPS.

The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.9.4 Masa Tenggang Permintaan Pencabutan / Revocation Request Grace Period

Tidak ada masa tenggang untuk pembatalan dalam kebijakan ini.

There is no grace period for revocation under this policy.

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

Peruri CA harus memulai permintaan investigasi dalam satu (1) hari kerja kecuali dalam hal *force majeure*. Permintaan pencabutan yang memberikan bukti pendukung yang cukup akan diproses sesegera mungkin.

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

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

Pihak Pengandal harus memvalidasi sertifikat terhadap CRL terbaru yang ditentukan dalam poin distribusi CRL pada sertifikat.

Relying parties should validate any presented certificate against the most updated CRL defined in the certificate's CRL distribution point.

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

Relying parties should validate any presented certificate against the Peruri CA's provided OCSP server according to CPS Section 4.9.9.

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

CRL harus diperbarui dan dipublikasi:

The CRL must be updated and published:

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

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

CRL harus disimpan pada lingkungan yang dilindungi untuk menjamin integritas dan keotentikannya.

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

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

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

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

Pelanggan dan orang yang bertanggung jawab atas keamanan Peruri CA diberitahukan jika ada kebocoran kunci privat selama pencabutan sertifikat.

The subscriber and the person in charge of Peruri CA security are notified in case of exposure of the private key during the certificate revocation.

Peruri CA harus mengoperasikan dan memelihara CRL dan OCSP-nya dengan sumber daya yang cukup untuk memberikan waktu respon sepuluh (10) detik atau kurang

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

dalam kondisi operasi normal.

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

Peruri CA menyediakan layanan validasi daring sesuai dengan CPS Bagian 4.9.9. *Peruri CA provides online validation service according to CPS Section 4.9.9.*

4.9.10 Pemeriksaan Pencabutan Daring / On-Line Revocation Checking Requirements

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

4.9.12 Kompromi Re-Key Persyaratan Khusus / Special Requirements Re-Key Compromise

Tidak ada ketentuan. *No stipulation.*

4.9.13 Keadaan untuk Pembekuan / Circumstances for Suspension

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

4.9.14 Siapa yang Dapat Meminta Pembekuan / Who can Request Suspension

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

4.9.15 Prosedur Permintaan Pembekuan / Procedure for Suspension Request

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

4.9.16 Batas Waktu Pembekuan / Limits on Suspension Period

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

4.10 LAYANAN STATUS SERTIFIKAT / CERTIFICATE STATUS SERVICES

4.10.1 Karakteristik Operasional / Operational Characteristics

Status sertifikat publik tersedia dari CRL di dalam repositori. *The status of public certificates is available from CRL's in the repositories.*

4.10.2 Ketersediaan Layanan / Service Availability

Peruri CA harus melakukan semua tindakan yang diperlukan untuk menjamin ketersediaan layanan validasi status sertifikat. *Peruri CA shall take all necessary measures to ensure availability of 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 sertifikatnya kadaluarsa atau mencabut sertifikatnya tanpa meminta sertifikat yang baru. Terdapat prosedur pencabutan sertifikat pada Peruri CA.

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

4.12 PEMULIHAN DAN PENITIPAN KUNCI / KEY ESCROW AND RECOVERY

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

Kebijakan dan Praktik Pemulihan dan Penitipan Kunci diatur pada CPS bagian 4.12.1.

Key Escrow and Recovery Policy and Practices as defined at CPS section 4.12.1.

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

Tidak ada ketentuan.

No stipulation.

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

5.1 KENDALI FISIK / PHYSICAL CONTROLS

5.1.1 Lokasi dan Konstruksi / Site Location and Construction

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

The location and construction of the facility housing Peruri CA equipment as well as sites housing remote workstations used to administer the Peruri CA, shall be 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 intrusion sensors, shall provide robust protection against unauthorized access to the Peruri CA equipment and records.

5.1.2 Akses Fisik / Physical Access

Peralatan Peruri CA selalu terlindungi dari akses yang tidak sah. Mekanisme keamanan fisik minimal Peruri CA yang harus dilakukan :

The Peruri CA equipment shall always be protected from unauthorized access. The physical security mechanisms for Peruri CA at a minimum shall be in place to:

- Memastikan tidak ada akses ke perangkat keras tanpa izin.
- Menyimpan semua media dan kertas yang berisi informasi sensitif dalam wadah yang aman.
- Memonitor, baik secara manual maupun elektronik, dari intrusi tidak sah setiap saat.
- Memelihara dan memeriksa log akses secara berkala.
- *Ensure no unauthorized access to the hardware is permitted*
- *Store all removable media and paper containing sensitive plain-text information in secure containers.*
- *Monitor, either manually or electronically, for unauthorized intrusion at all times.*
- *Maintain and periodically inspect an access log.*

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

All critical Peruri CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software.

5.1.3 Daya dan Penyejuk Udara / Power and Air Conditioning

Peruri CA harus memiliki daya cadangan yang cukup untuk mengunci masukan secara otomatis, menyelesaikan setiap tindakan yang tertunda, dan merekam status peralatan

Peruri CA shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air

sebelum kekurangan daya atau AC yang menyebabkan peralatan mati. Repositori IKP harus dilengkapi Daya Tak Terputus dan Generator Listrik yang cukup untuk beroperasi paling sedikit enam (6) jam saat tidak adanya daya komersial, untuk mendukung keberlangsungan operasional.

conditioning causes a shutdown. PKI Repositories shall be provided with Uninterrupted Power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to support continuity of operations.

5.1.4 Pemaparan Air / Water Exposures

Peralatan Peruri CA ditempatkan pada tempat yang tidak terpapar air.

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

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

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

5.1.5 Pencegahan dan Perlindungan dari Kebakaran / Fire Prevention and Protection

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

Peruri CA equipment is placed in facilities with adequate fire detection and suppression systems.

5.1.6 Penyimpanan Media / Media Storage

Media Peruri CA harus disimpan untuk melindunginya dari kerusakan yang tidak disengaja (air, api, elektromagnetik), pencurian, dan akses tidak sah. Media yang berisi informasi audit, arsip, atau cadangan harus digandakan dan disimpan di lokasi yang terpisah dari lokasi Peruri CA.

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

5.1.7 Pembuangan Limbah / Waste Disposal

Bahan limbah yang sensitive dibuang dengan cara yang aman.

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

5.1.8 Backup Off-Site / Off-Site Backup

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

System backups of the Peruri CA, sufficient to recover from system failure, shall be made on a periodic schedule, described in the Peruri CA - CPS. Backups shall be performed and stored offsite not less than once every seven (7) days. At least one (1) full backup copy shall be stored at an offsite location (at a location separate from the Peruri CA equipment). Only the latest full backup need be retained. The backup data shall be protected with physical and

dengan kendali fisik dan kontrol prosedur.

procedural controls.

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

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

5.2 KENDALI PROSEDUR / PROCEDURAL CONTROLS

5.2.1 Peran-Peran Terpercaya / Trusted Roles

Peran-peran terpercaya meliputi:

- **Koordinator**
Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan Peruri CA.
- **Policy Administrator (Compliance Officer)**
Pembuatan atau revisi *Certificate Policy* dan *Certification Practice Statement*.
- **Security Officer / Internal Auditor**
Melihat dan memelihara arsip sistem CA dan log audit Peruri.
- **Key Manager / Key Custodian**
Pembuatan dan pencabutan pasangan kunci Peruri CA.
- **CA Administrator (CA)**
Akses sistem CA, persetujuan siklus penerbitan sertifikat, pencabutan dan penangguhan sertifikat.
- **RA Administrator (RA)**
Akses dan manajemen Sistem RA, Persetujuan untuk identifikasi dilakukan oleh *Validation Specialist*.
- **Validation Specialist**
Identifikasi Pengguna dan verifikasi dokumen.
- **Repository (WEB)**
Manajemen halaman WEB, publikasi.
- **Developer**
Pengembangan CA / RA / OCSP dan sistem terkait lainnya.
- **Operator**
Operasi sehari-hari sistem Peruri CA dan pencadangan serta pemulihan sistem.

Trusted roles including:

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

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

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

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

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

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require three or more persons:

- Pembuatan kunci Peruri CA
- Pengaktifan kunci Peruri CA
- Pencadangan kunci Peruri CA
- Peruri CA key generation
- Peruri CA key activation
- Peruri CA key backup

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

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

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

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

Setiap individu Peruri CA secara khusus ditunjuk untuk peran yang ditentukan dalam bagian 5.2.1 dari CP ini dan tidak ada individu yang ditugaskan lebih dari satu Peran Terpercaya.

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

5.3 KENDALI PERSONIL / PERSONNEL CONTROLS

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

Semua personil Peruri CA harus warga negara Indonesia dan dipilih atas dasar keterampilan, pengalaman, kesetiaan, kepercayaan, dan integritas. Personil yang ditunjuk untuk peran terpercaya harus:

All persons shall be citizens of Indonesia and selected based on skills, experience, loyalty, trustworthiness, and integrity. Personnel appointed to trusted roles shall:

- Tidak memiliki catatan kriminal
- Tidak dalam kebangkrutan
- Have no criminal record
- Not in bankruptcy

5.3.2 Background Check Procedures / Prosedur Pemeriksaan Latar Belakang

Semua personil di Peruri CA harus lulus pemeriksaan latar belakang. Lingkup pemeriksaan latar belakang mencakup area berikut, yang paling sedikit lima (5) tahun:

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

- Kontak Referensi Pekerjaan
- Employment Contact Reference

- Pendidikan atau sertifikasi
- Identifikasi Kependudukan (KTP)
- Catatan Kepolisian
- *Education or certification*
- *Residential Identification*
- *Police Certificate of Good Conduct*

Prosedur pemeriksaan latar belakang harus dijelaskan pada CPS.

Background check procedures shall be described in the CPS.

5.3.3 Persyaratan Pelatihan / Training Requirements

Semua personil Peruri CA harus dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan ini akan membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional, dan prosedur terkait.

All Peruri CA personnel shall be appropriately trained to perform their duties. Such training will address relevant topics, such as security requirements, operational responsibilities and associated procedures.

Pelatihan tersebut harus mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras, perangkat lunak dan sistem operasi Peruri CA), prosedur operasional dan keamanan, CP ini, dan CPS yang berlaku.

The training shall include minimum operations of the PKI (including CA hardware and software), operational and security procedures, this CP and the applicable CPSes.

5.3.4 Frekuensi dan Persyaratan Pelatihan Ulang / Retraining Frequency and Requirements

Peruri CA memberikan penyegaran pelatihan dan pembaruan pada personilnya sejauh dan sesering yang dibutuhkan untuk memastikan personil tersebut mempertahankan tingkat kemampuan yang dipersyaratkan untuk melakukan tanggung jawab pekerjaannya secara kompeten dan memuaskan.

The Peruri CA shall provide refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and 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 ensure that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanksi untuk Tindakan Tidak Terotorisasi / Sanctions for Unauthorized Actions

Sanksi disiplin yang sesuai berlaku pada personel yang melanggar ketentuan dan kebijakan dalam CP ini, CPS, atau prosedur operasional Peruri CA. Sanksi disiplin disesuaikan dengan tingkat keparahan pelanggaran yang dilakukan dan termasuk pemutusan hubungan kerja.

Appropriate disciplinary actions are taken for unauthorized actions or other violations of relevant policies and procedures. Disciplinary actions are commensurate with the frequency and severity of the unauthorized actions and may include measures up to and including termination.

5.3.7 Persyaratan Kontraktor Independen / Independent Contractor Requirements

Personel sub-kontraktor yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional Peruri CA harus memenuhi persyaratan yang berlaku yang ditetapkan dalam CP ini (misalnya, semua persyaratan pada bagian 5.3).

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

5.3.8 Dokumentasi yang Diberikan kepada Personil / Documentation Supplied to Personnel

Peruri CA menyediakan untuk setiap personil Certificate Policy yang mereka gunakan, CPS dan setiap undang – undang yang relevan, kebijakan atau kontrak apapun. Dokumen teknis, operasi dan dokumen administratif lainnya disediakan agar personil yang dipercaya dapat menjalankan tugasnya.

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

5.4 PROSEDUR LOG AUDIT / AUDIT LOGGING PROCEDURES

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

Audit log files shall be generated for all events relating to the security of the CA, VA 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

Semua kapabilitas audit keamanan dari sistem operasi Peruri CA dan RA serta aplikasi Certificate Authority, Validation Authority dan Registration Authority yang telah dipersyaratkan oleh CP ini telah aktif. Sebagai hasilnya, seluruh kejadian yang teridentifikasi harus direkam secara otomatis.

All security auditing capabilities of the Peruri CA and RA operating system and the CA, VA and RA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded.

Setiap rekaman audit minimal harus memuat poin – poin sebagai berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian) :

At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- Tipe kejadian;
- Nomor rekaman atau urutan rekaman;
- The type of event;
- Serial or sequence number of entry;

- Tanggal dan waktu terjadi;
- Asal perekaman;
- Indikator berhasil atau gagal jika perlu; dan
- Identitas dari entitas dan/atau operator yang menyebabkan kejadian.
- *The date and time the event occurred;*
- *Source of entry;*
- *Success or failure where appropriate; and*
- *The identity of the entity and/or operator that caused the event.*

5.4.2 Frekuensi Pemrosesan Log / Frequency of Processing Log

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

Audit logs shall be reviewed at least monthly. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log.

Tindakan yang diambil sebagai hasil dari peninjauan didokumentasikan.

Actions taken as a result of these reviews shall be documented.

5.4.3 Periode Retensi Log Audit / Retention Period for Audit Log

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

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

5.4.4 Proteksi Log Audit / Protection of Audit Log

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

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

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

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

5.4.5 Prosedur Backup Log Audit / Audit Log Backup Procedures

Log audit Peruri CA harus di-backup sedikitnya sebulan sekali. Media backup harus disimpan di tempat lokal pada lokasi yang aman. Salinan kedua dari log audit harus diletakkan pada

Peruri CA's Audit logs shall be backed up at least monthly. Backup media shall be stored locally in a secure location. A second copy of the audit log shall be sent off-site on a monthly

tempat yang lain setiap bulan. *basis.*

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

Sistem pengumpulan log audit adalah internal ke sistem Peruri CA. *The audit log collection systems were internal to the Peruri CA system.*

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

Tidak ada ketentuan. *No stipulation.*

5.4.8 Penilaian Kerentanan / Vulnerability Assessments

Peruri CA harus menilai kerentanan sistem CA atau komponennya paling tidak sekali setahun. *Peruri CA shall assess the vulnerability of its CA system or its components at least on a yearly basis.*

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 operasi yang benar dan validitas sertifikat yang dikeluarkan oleh Peruri CA. Data berikut tercatat di arsip:

- Siklus operasi sertifikat termasuk permintaan sertifikat, permintaan pencabutan, permintaan pembangkitan ulang pasangan kunci.
- Semua sertifikat dan CRL yang telah diterbitkan.
- Log audit.
- Data konfigurasi sistem IKP.
- Dokumen CP dan CPS yang berlaku termasuk modifikasi dan amandemen terhadap dokumen ini.

Peruri CA archive records shall be sufficiently detailed to determine the proper operation of the Peruri CA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

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

5.5.2 Periode Retensi Arsip / Retention Period for Archive

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

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

5.5.3 Perlindungan Arsip / Protection of Archive

Catatan yang diarsipkan harus dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan yang diarsipkan dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan harus dipelihara dan dilindungi sesuai peraturan yang ditentukan dalam CP ini dan CPS yang berlaku.

The archived records shall be protected against unauthorized viewing, modification, deletion, or tampering. The media holding the archive records and the applications required to process the archive records shall be maintained and protected as per the rules specified in this CP and applicable CPSs.

Peruri CA tidak akan mengeluarkan arsip kecuali atas permintaan oleh Kominfo sebagai Penyelenggara Sertifikasi Elektronik (PSrE) Induk Indonesia atau seperti yang disyaratkan oleh hukum.

Peruri CA shall not release archives except upon request by Root CA Indonesia or as required by law.

5.5.4 Prosedur Backup Arsip / Archive Backup Procedures

Prosedur *backup* arsip yang memadai dan teratur harus dilakukan agar jika terjadi

Adequate and regular backup procedures shall be in place so that in the event of loss or

kehilangan atau kerusakan arsip utama, tersedia satu set lengkap salinan *backup* di lokasi terpisah. CPS atau dokumen yang diacu harus menguraikan bagaimana rekaman arsip di-*backup*, dan bagaimana backup arsip dikelola.

destruction of the primary archives, a complete set of backup copies held in a separate location will be available. The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

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

Catatan arsip Peruri CA diberikan label waktu secara otomatis.

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

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

Tidak ada ketentuan.

No stipulation.

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

Media penyimpanan informasi arsip CA diperiksa setelah dibuat. Secara berkala, sampel dari informasi arsip diuji untuk memeriksa integritas dan kemampuan dalam membaca informasi. Hanya yang diijinkan yang dapat mengakses arsip. Permintaan untuk mendapat dan memverifikasi informasi arsip dikoordinasikan oleh operator pada peran terpercaya.

Media storing of CA archive information is checked upon creation. Periodically, samples of archived information are tested to check the continued integrity and readability of the information. Only authorised CA, trusted role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by operators in trusted roles.

5.6 PERGANTIAN KUNCI / KEY CHANGE OVER

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

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

Apabila Peruri CA memperbarui kunci privat dan menghasilkan kunci publik baru, Peruri CA memberitahu semua pemilik sertifikat yang mengandalkan Sertifikat Peruri CA bahwa

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

telah terjadi perubahan.

5.6.1 Skema Interlock / Interlock Scheme

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

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

5.7 PEMULIHAN BENCANA DAN KEBOCORAN / COMPROMISE AND DISASTER RECOVERY

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

Peruri CA memiliki rencana tanggap darurat dan rencana pemulihan bencana.

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

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

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

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

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

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

- Memberitahu Policy Authority, Security Officer, Key Manager, Head of Peruri CA dan Kominfo selaku Root CA.
 - Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi backup terakhir.
 - Mengoperasikan kembali Peruri CA, memprioritaskan kemampuan membangkitkan informasi status sertifikat untuk penerbitan CRL sesuai jadwal.
 - Apabila kunci penandatanganan Peruri CA rusak, mengembalikan operasional Peruri CA secepat mungkin, dengan memberikan
- *Notify PA, Security Officer, Key Manager, PSrE Head and ROOT CA Indonesia as soon as possible.*
 - *Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.*
 - *Reestablish Peruri CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.*
 - *If Peruri CA's signing keys are destroyed, reestablish Peruri CA operations as quickly as possible, giving priority to the*

prioritas ke pembangkitan pasangan kunci Peruri CA yang baru.

generation of a new Peruri CA signing key pair.

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

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

In case of loss of private keys or compromise of the algorithms and parameters used to generate the private key and certificate, all related subscriber/device certificates are revoked by the Peruri CA and new keys and certificates are issued without interruption of the service

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

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

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

If the private key of the Root CA Indonesia is lost, Root CA Indonesia is expected to notify Peruri CA's PA officially and relying parties via public announcement. Peruri CA MUST stop service, notify all subscribers of Peruri CA, proceed with the revocation of all certificates, issue a final CRL and then notify the relevant security contacts. Then the Public Key Infrastructure will be set up again with new Certification Authorities starting with a new Root Certification Authority.

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

Peruri CA harus menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbarui. Suatu pemulihan layanan secara penuh harus terlaksana dalam 24 jam bila ada bencana.

Peruri CA shall prepare a disaster recovery plan which have been tested, verified and continually updated. A full restoration of services shall be done within 24 hours in case of disaster.

5.8 PENUTUPAN CA ATAU RA / CA OR RA TERMINATION

Dalam kasus Peruri CA mengakhiri operasinya, mereka harus memberitahu ke Root CA Induk Indonesia, PA, dan para Pemilik sebelum penutupan agar mematuhi Peraturan Pemerintah.

In the event that Peruri CA terminates its operation, it shall provide notice to Root CA Indonesia, PA, and subscriber prior to termination in compliance with Government regulation.

6. KENDALI KEAMANAN TEKNIS / TECHNICAL SECURITY CONTROLS

6.1 PEMBANGKITAN DAN INSTALASI PASANGAN KUNCI / PAIR GENERATION AND INSTALLATION

6.1.1 Pembangkitan Pasangan Kunci / Key Pair Generation

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

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

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

Pembangkitan pasangan kunci Peruri CA harus menghasilkan jejak audit yang dapat diverifikasi yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. Dokumentasi prosedur harus cukup rinci untuk menunjukkan bahwa pemisahan peran yang tepat digunakan. Pihak ketiga yang independen harus memvalidasi pelaksanaan prosedur pembangkitan kunci baik dengan menyaksikan pembangkitan kunci atau dengan memeriksa rekaman yang ditandatangani dan didokumentasikan saat pembangkitan kunci.

Peruri CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. An independent third party shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 Pembangkitan Pasangan Kunci Pemilik / Subscriber Key Pair Generation

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

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

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

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

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

Jika Pemilik membangkitkan sendiri Pasangan Kuncinya, maka tidak ada kebutuhan pengiriman Kunci Privat, dan bagian ini tidak berlaku.

If Subscribers generate their own Key Pairs, then there is no need to deliver Private Keys, and this section does not apply.

Bila Peruri CA membangkitkan kunci atas

When Peruri CA generates keys on behalf of

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

- Siapapun yang membuat kunci privat penandatanganan untuk Pemilik tidak boleh menyimpan salinan kunci apapun setelah pengiriman Kunci Privat ke Pemilik.
- Kunci Privat harus dilindungi terhadap aktivasi, *compromise*, atau perubahan selama proses pengiriman.
- Pemilik harus memberikan pernyataan penerimaan Kunci Privat.
- Peruri CA harus menyimpan pernyataan penerimaan Pemilik atas Kunci Privat.
- *Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber.*
- *The Private Key shall be protected from activation, compromise, or modification during the delivery process.*
- *The Subscriber shall acknowledge receipt of the Private Key(s).*
- *The CA shall maintain a record of the Subscriber acknowledgement of receipt of the private key.*

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

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

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

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

Setiap sertifikat digital yang diterbitkan oleh Peruri CA berisi kunci publik.

Public Key is included in the digital certificate issued by the Peruri CA.

Peruri CA harus menyediakan mekanisme pengiriman secara digital (*digital delivery*) yang aman bagi semua sertifikat yang diterbitkan. Sebagai contoh, semua sertifikat dari setiap Peruri CA dipublikasikan melalui suatu situs web yang aman, yang identitasnya disertifikasi oleh penyedia SSL terpercaya.

Peruri CA shall provide mechanisms for securing digital delivery of all certificates. This may include publication through a trusted SSL secured website.

Pada jangka waktu tertentu sebelum kunci publik Peruri CA kadaluarsa, suatu pasangan

A suitable time before the expiration of a Peruri CA public key, a new certificate signing

kunci penandatanganan sertifikat yang baru akan dibangkitkan untuk menjaga operasional Peruri CA berjalan normal.

key pair will be generated in order to avoid disruptions to the normal Peruri CA operations.

Penjelasan tentang publikasi dan repositori sertifikat mengacu pada Bagian 2.1.

Peruri CA publishes its certificate at the certificate store described in section 2.1.

6.1.5 Ukuran Kunci / Key Sizes

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

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

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

Tidak ada ketentuan.

No stipulation.

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

Kunci publik yang terikat pada suatu sertifikat harus disertifikasi, agar kunci publik tersebut bisa digunakan untuk autentikasi, penandatanganan, atau enkripsi, tapi tidak semua, kecuali yang sudah ditentukan oleh Peruri CA. Penggunaan sebuah kunci spesifik ditentukan oleh *key usage extension* dalam sertifikat X.509.

Public keys that are bound into certificates shall be certified for use in authenticating, signing or encrypting, but not all, except as specified by Peruri CA. The use of a specific key is determined by the key usage extension in the X.509 certificate.

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

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

Peruri CA menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 *Security* minimal Level 1 untuk pembangkitan kunci, proses penandatanganan, dan enkripsi.

Peruri CA uses a FIPS 140-2 Security minimum Level 1 cryptographic module for key generation, signing operations and encryption.

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

Semua kunci privat Peruri CA harus diakses melalui kendali multi-personil seperti yang ditentukan pada Bagian 5.2.2 (Sejumlah orang dibutuhkan dalam setiap tugas) dari CP dan CPS yang berlaku.

All Peruri CA private keys shall be accessed through multi-person control as specified in Section 5.2.2 (Number of Persons Required Per Task) from applicable CP and CPS.

6.2.3 Penitipan Kunci Privat / Private Key Escrow

Kunci private Peruri CA tidak akan pernah dititipkan. *Peruri CA private keys shall never be escrowed.*

Kunci privat Pemilik boleh dititipkan di Peruri CA. *Subscriber private keys may be escrowed at Peruri CA.*

6.2.4 Backup Kunci Privat / Private Key Backup

Kunci privat Peruri CA harus di-backup di bawah kendali multi-pihak yang sama dengan kunci tanda tangan asli. Paling tidak satu salinan dari kunci privat harus disimpan off-site. Semua salinan kunci privat Peruri CA harus dilindungi dengan cara yang sama dengan aslinya. *Peruri CA's private signature key shall be backed up under the same multiparty control as the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.*

Untuk backup kunci privat Pemilik, Pemilik dapat memilih untuk melakukan backup kunci mereka, tapi backup kunci harus berada di bawah kendali Pemilik. *For the backup of Subscriber private keys, Subscribers may choose to backup their keys, but must be held in the Subscriber's control.*

6.2.5 Pengarsipan Kunci Privat / Private Key Archival

Sebelum kunci privat Peruri CA dimusnahkan, kunci harus diarsipkan sesuai dengan ketentuan pengarsipan Peruri CA. Pengarsipan dilakukan dengan cara menyimpan salinan kunci pada media penyimpanan yang disimpan terpisah. Sementara itu, kunci privat Pemilik tidak boleh diarsipkan. *Before Peruri CA private signature keys are destroyed, the key shall be archived in accordance to Peruri CA policy. Archiving is accomplished by storing a copy of the key on a separate storage. Meanwhile, subscriber private signature keys shall not be archived.*

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

Kunci privat Peruri CA boleh diekspor dari modul kriptografis hanya untuk melaksanakan prosedur backup kunci Peruri CA. Kunci privat Peruri CA tidak pernah sekalipun boleh berada dalam bentuk *plaintext* di luar modul kriptografis. *Peruri CA private keys may be exported from the cryptographic module only to perform CA key backup procedure. At no time shall the Peruri CA private key exist in plaintext outside the cryptographic module.*

Bila sebuah kunci privat akan dipindahkan dari satu modul kriptografis ke yang lain, kunci privat harus dienkrpsi selama pemindahan. Token yang dipakai untuk enkripsi kunci privat harus dilindungi dengan tingkat keamanan 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 shall be handled in the same way as the private key.*

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

Kunci Privat Peruri CA harus disimpan pada modul kriptografis FIPS 140-2 Security Level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi. *Peruri CA Private Keys shall be stored on FIPS 140-2 Security Level 3 cryptographic module, in encrypted form and password-protected.*

6.2.8 Metode Pengaktifan Kunci Privat / Method of Activating Private Key

Aktivasi operasi kunci privat Peruri CA dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak seperti yang dinyatakan dalam bagian 5.2.2. *Activation of Peruri CA's private key operations is performed by authorized persons and requires multiparty control as specified in Section 5.2.2.*

6.2.9 Metode Penonaktifan Kunci Privat / Method of Deactivating Private Key

Setelah dipakai atau ketika tidak dipakai, modul kriptografis harus dinonaktifkan oleh personil yang berwenang, misalnya, melalui prosedur *logout manual*, atau secara otomatis setelah suatu selang waktu ketidakaktifan sebagaimana didefinisikan dalam CPS yang berlaku. *After use or when not in use, the cryptographic module shall be deactivated by authorized persons, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS.*

6.2.10 Metode Penghancuran Kunci Privat / Method of Destroying Private Key

Ketika kunci privat Peruri CA tidak diperlukan lagi, para individu dalam peran terpercaya harus menghapus kunci privat dari Modul Kriptografi dan *backup*-nya dengan menimpa kunci privat atau menginisialisasi modul dengan fungsi *factory reset* dari Modul Kriptografi. *When Peruri CA's private signature keys are no longer needed, individuals in trusted roles shall delete the private keys from Cryptographic Module and its backup by overwriting the private key or initialize the module with the destroy function of Cryptographic Module.*

Kejadian penghancuran kunci privat Peruri CA harus dicatat ke dalam barang bukti sesuai dengan bagian 5.4. *The event of destroying Peruri CA's private key must be recorded into evidence under section 5.4.*

6.2.11 Pemingkatan Modul Kriptografis / Cryptographic Module Rating

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

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

6.3.1 Pengarsipan Kunci Publik / Public Key Archival

Kunci Publik diarsipkan sebagai bagian dari pengarsipan Sertifikat. *The Public Key is archived as part of the Certificate archival.*

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

Periode operasional pasangan kunci didefinisikan oleh periode operasional dari sertifikat digital yang berkaitan. Periode operasional maksimum dari kunci didefinisikan sebagai dua puluh (20) tahun bagi PSrE Induk, sepuluh (10) tahun bagi PSrE Berinduk, dan satu (1) tahun untuk sertifikat pengguna. Periode operasional harus didefinisikan menurut ukuran kunci dan perkembangan teknologi terkini di bidang kriptografi, sehingga tingkat terbaik untuk keamanan dan efisiensi penggunaan terjamin.

The key pair operational period is defined by the operational period of the corresponding digital certificate. The maximum operational period of the keys is defined as twenty (20) years for the Root CA, ten (10) years for a Subordinate CA, and one (1) year for Subscriber certificates. The operational period must be defined according to the size of the keys and the current technological developments at the field of cryptography, so that the best level of security and efficiency of use is guaranteed.

6.4 DATA AKTIVASI / ACTIVATION DATA

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

Data aktivasi seperti *Personal Identification Number* (PIN) dan kata sandi untuk mengakses sistem CA dipilih dan dilindungi oleh banyak orang sesuai dengan *Key Ceremony Procedure*.

Activation data such as Personal Identification Number (PIN) and passwords for accessing the CA systems are user-selected and protected under multi-person in accordance with the Key Ceremony Procedure.

6.4.2 Aktivasi Perlindungan Data / Activation Data Protection

Data yang digunakan untuk membuka kunci privat harus dilindungi dari pengungkapan. Data aktivasi harus dihafal, bersifat biometrik, atau direkam dan diamankan pada tingkat jaminan yang terkait dengan aktivasi modul kriptografi.

Data used to unlock a private key shall be protected from disclosure. Activation data shall be memorized, biometric in nature, or recorded and secured at the level of assurance associated with the activation of the cryptographic module.

Perlindungan Data Aktivasi untuk CA harus sesuai dengan *Key Ceremony Procedure*.

Activation Data Protection for CAs shall be in accordance with the Key Ceremony Procedure.

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 Spesifik / Specific Computer Security Technical Requirements

Fungsi-fungsi keamanan komputer berikut dapat disediakan oleh sistem operasi, atau melalui suatu kombinasi dari sistem operasi, perangkat lunak, dan perlindungan fisik.

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. Peruri CA

Peruri CA harus menyertakan fungsionalitas berikut: *shall include the following functionality:*

- Membutuhkan *login* terautentikasi • *Require authenticated logins*
- Menyediakan *Discretionary Access Control* • *Discretionary Access Control*
- Menyediakan kapabilitas audit keamanan • *Security audit capability*
- Melarang penggunaan ulang objek yang sama • *Prohibit object re-use*
- Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data • *Use of cryptography for communication session and database security*
- Membutuhkan jalur terpercaya untuk identifikasi dan autentifikasi • *Require a trusted path for identification and authentication*
- Isolasi domain untuk proses • *Domain isolation for process*
- Menyediakan perlindungan mandiri untuk sistem operasi • *Self-protection for the operating system*
- Pengujian keamanan mandiri yang berhubungan dengan layanan peruri CA (contohnya: memeriksa integritas dari catatan audit) • *Self-test security related CA services (e.g., check the integrity of the audit logs)*

Ketika peralatan Peruri CA ditempatkan pada suatu *platform* terevaluasi dalam mendukung persyaratan penjaminan keamanan komputer maka sistem (perangkat keras, perangkat lunak, sistem operasi) harus, kalau mungkin, beroperasi dalam konfigurasi terevaluasi. Paling tidak, *platform* tersebut harus memakai versi yang sama dari sistem operasi komputer dengan yang menerima perangkat evaluasi.

When Peruri CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating.

Sistem komputer Peruri CA harus dikonfigurasi dengan akun yang diperlukan dan layanan jaringan yang minimum.

The Peruri CA-computer system shall be configured with minimum of the required accounts, network services.

6.5.2 Peringkat Keamanan Komputer / Computer Security Rating

Tidak ada ketentuan.

No stipulation.

6.6 KENDALI TEKNIS SIKLUS HIDUP / LIFE CYCLE TECHNICAL CONTROLS

6.6.1 Kendali Pengembangan Sistem / System Development Controls

Tidak ada ketentuan.

No stipulation.

6.6.2 Kendali Manajemen Keamanan / Security Management Controls

Konfigurasi dari sistem Peruri CA serta seluruh modifikasi dan pembaharuan didokumentasikan dan dikontrol oleh Manajemen Peruri CA. Ada mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi milik Peruri CA.

The configuration of the Peruri CA system as well as any modifications and upgrades are documented and controlled by the Peruri CA management. There is a mechanism for detecting unauthorized modification to the Peruri CA software or configuration.

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.

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 harus menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa mereka terjaga dari *denial of service* dan serangan intrusi. Langkah-langkah sedemikian harus termasuk penggunaan *firewall* dan *router* penyaring. *Port* jaringan dan layanan yang tidak dipakai harus dimatikan. Setiap perangkat lunak jaringan yang ada harus perlu bagi berfungsinya Peruri CA.

Peruri CA shall employ appropriate network security measures to guard against denial of service and intrusion attacks. Such measures shall include the use of firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the Peruri CA.

6.8 STEMPEL WAKTU / TIME-STAMPING

Jam internal server Peruri CA harus disinkronkan menggunakan *Network Time Protocol* (NTP). Waktu yang didapat dari layanan waktu tersebut akan digunakan untuk menentukan waktu pada saat:

Peruri CA servers' internal clock shall be synchronized using Network Time Protocol (NTP). Time derived from the time service shall be used for establishing the time of:

- Validitas waktu permulaan untuk sebuah sertifikat PsrE
- Pencabutan sertifikat PsrE
- Pembaruan CRL, dan
- Penerbitan sertifikat pemilik dan entitas
- *Initial validity time of a CA Certificate;*
- *Revocation of a CA Certificate;*
- *Posting of CRL updates; and*
- *Issuance of Subscriber end entity Certificates*

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

7.1 PROFIL SERTIFIKAT / CERTIFICATE PROFILE

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

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

Peruri CA melakukan *Review* Profil Sertifikat secara berkala minimal satu tahun sekali yang dilakukan oleh CA Admin dengan cara menyesuaikan profil sertifikat dengan peraturan yang berlaku dan/atau kebutuhan bisnis.

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

7.1.1 Nomor Versi / Version Number(s)

Peruri CA seharusnya menerbitkan sertifikat X.509 v3 (mengisi versi *field* dengan *integer* “2”).

Peruri CA shall issue X.509 v3 certificates (populate version field with integer “2”).

7.1.2 Ekstensi Sertifikat / Certificate Extensions

Peruri CA harus memakai ekstensi sertifikat standar yang mematuhi RFC 5280.

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

7.1.2.1 Penggunaan Kunci / Key Usage

Sertifikat X.509 Versi 3 biasanya diisi sesuai dengan RFC 5280: *Internet X.509 Public Key Infrastructure Certificate* dan Profil CRL. Bidang kritis dari ekstensi *Key Usage* biasanya diisi *TRUE*.

X.509 Version 3 Certificates are generally populated in accordance with RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile. The criticality field of the Key Usage extension is generally set to TRUE.

7.1.2.2 Perluasan Kebijakan Sertifikat / Certificate Policies Extension

Ekstensi *certificate policies* dari Sertifikat X.509 Versi 3 diisi dengan identifier objek dari CP ini sesuai dengan bagian 7.1.6 dan dengan pengkualifikasi kebijakan yang ditentukan dalam bagian 7.1.8. *Field criticality* dari ekstensi ini harus diisi *FALSE*.

Certificate Policies extension of X.509 Version 3 Certificates are populated with the object identifier of this CP in accordance with Section 7.1.6 and with policy qualifiers set forth in Section 7.1.8. The criticality field of this extension shall be set to FALSE.

7.1.2.3 Batasan Dasar / Basic Constraint

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

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

TRUE untuk Sertifikat CA, tapi boleh diisi *TRUE* atau *FALSE* bagi Sertifikat Pemilik.

extension shall be set to TRUE for CA Certificates, but may be set to TRUE or FALSE for end-user Subscriber Certificates.

7.1.2.4 Penggunaan Kunci Tambahan / Extended Key Usage

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

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

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

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

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

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

7.1.2.5 Titik Distribusi CRL / CRL Distribution Points

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

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

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

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

7.1.2.6 Authority Key Identifier / Authority Key Identifier

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

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

7.1.2.7 Pengidentifikasi Kunci Subjek / Subject Key Identifier

Bila ada dalam Sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini harus diisi dengan *FALSE* dan metode untuk menghasilkan *keyIdentifier* yang berbasis pada kunci publik

If present in X.509 Version 3 Certificates, the critically field of this extension shall be set to FALSE and the method for generating the key identifier based on the public key of the

Subyek Sertifikat harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280. *subject of the certificate shall be calculated in accordance with one of the methods described in RFC 5280.*

7.1.3 Pengidentifikasi Objek Algoritma / Algorithm Object Identifiers

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

7.1.4 Format Nama / Name Forms

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1. *As per the naming conventions and constraints listed in section 3.1.*

7.1.5 Batasan Nama / Name Constraints

Sesuai dengan konvensi penamaan dan batasan yang tercantum pada bagian 3.1. *As per the naming conventions and constraints listed in section 3.1.*

7.1.6 Pengidentifikasi Objek Kebijakan Sertifikat / Certificate Policy Object Identifier

Sertifikat yang diterbitkan di bawah CP ini harus menggunakan nomor OID Joint-ISO-ITU yang mengacu pada PSrE yang benar dan sesuai dengan Certificate Policy. *Certificates issued under this CP shall use the Joint-ISO-ITU OID number that points to the correct CA as well as Certificate Policy.*

7.1.7 Penggunaan Ekstensi Batasan Kebijakan / Usage of Policy Constraints Extension

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

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

Tidak ada ketentuan. *No stipulation.*

7.2 PROFIL CRL / CRL PROFILE

7.2.1 Nomor Versi / Version Number(s)

Peruri CA yang beroperasi di bawah CP ini harus menerbitkan CRL X.509 versi 2. *Peruri CA shall issue X.509 version 2 and CRL entry extension.*

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

Peruri CA menggunakan standar RFC 5280 CRL dan ekstensi entri CRL.

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

7.3 OCSP PROFILE / PROFIL OCSP

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

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

7.3.1 Nomor Versi / Version Number(s)

Peruri CA harus menerbitkan respon OCSP versi 1.

Peruri CA shall issue OCSP responses Version 1.

7.3.2 OCSP Extensions / Ekstensi OCSP

Tidak ada ketentuan.

No stipulation.

8. AUDIT KEPATUHAN DAN ASESMEN LAIN / COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Peruri CA harus menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika No 11/2018.

Peruri CA shall undergo a compliance audit and submit reports periodically as required by Indonesia Ministry of Communication and Informatics Regulation No 11 Year 2018.

8.1 FREKUENSI ATAU KEADAAN ASESMEN / FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Peruri CA harus menjalani audit kepatuhan berkala terhadap skema yang telah ditetapkan dan juga setiap setelah terjadi perubahan yang signifikan terhadap prosedur dan teknik yang diterapkan.

Peruri CA shall undergo a compliance audit of the currently established scheme, both on regular basis as well as each time after undergo significant changes to the established procedures and techniques.

Peruri CA harus menjalani audit kepatuhan dan menyampaikan laporan berkala minimal sekali setahun yang dipersyaratkan oleh Peraturan Menteri Komunikasi dan Informatika No 11/2018.

Peruri CA shall undergo a compliance audit and submit periodical reports at least once a year as required by Indonesia Ministry of Communication and Informatics Regulation No 11 Year 2018.

8.2 IDENTITAS/KUALIFIKASI ASESOR / IDENTITY/QUALIFICATIONS OF ASSESSOR

Auditor kepatuhan harus menunjukkan kompetensi dalam bidang audit kepatuhan, dan harus benar-benar memahami persyaratan CP ini. Auditor kepatuhan harus melakukan audit kepatuhan tersebut sebagai tanggung jawab utama. CPS yang berlaku harus mengidentifikasi auditor kepatuhan dan membenarkan kualifikasi auditor kepatuhan.

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with the requirements of this CP. The compliance auditor must perform such compliance audits as a primary responsibility. The applicable CPS shall identify the compliance auditor and justify the compliance auditor's qualifications.

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

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

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 TOPIK YANG DICAKUP OLEH ASESMEN / TOPICS COVERED BY ASSESSMENT

Audit yang dilaksanakan harus memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema

The audit must meet the requirements of the audit scheme under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to the CA in the year

audit akan berlaku pada tahun berikutnya *following the adoption of the updated scheme.* setelah PSrE mengadopsi skema yang terbaru.

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

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

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

- Auditor kepatuhan harus memberitahu Kominfo tentang ketidaksesuaian.
 - Pihak yang bertanggung jawab untuk memperbaiki ketidaksesuaian harus menentukan pemberitahuan atau tindakan lebih lanjut apa yang diperlukan sesuai dengan persyaratan CP dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan tersebut tanpa penundaan.
- *The compliance auditor shall notify Peruri CA of the discrepancy.*
 - *The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and the respective contracts, and then proceed to make such notifications and take such actions without delay.*

8.6 KOMUNIKASI HASIL / COMMUNICATION OF RESULTS

Laporan Kepatuhan Audit, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh komponen, harus diberikan kepada PA sebagaimana diatur dalam bagian 8.1. Laporan tersebut harus mengidentifikasi versi CP dan CPS yang digunakan dalam penilaian. Selain itu, hasilnya harus dikomunikasikan seperti yang ditetapkan pada bagian 8.5 di atas.

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, shall be provided to the PA as set forth in section 8.1. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in 8.5 above.

8.7 AUDIT INTERNAL / INTERNAL AUDIT

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan resiko gangguan pada proses business.

Audits of operational systems are planned and agreed such as to minimise the risk of disruptions to business processes.

9. BISNIS LAIN DAN MASALAH HUKUM / OTHER BUSINESS AND LEGAL MATTERS

9.1 BIAAYA / FEES

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

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

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

9.1.2 Biaya Pengaksesan Sertifikat / Certificate Access Fees

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

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

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

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

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

9.1.4 Biaya Layanan Lainnya / Fees for Other Services

Peruri CA dapat mengenakan biaya untuk mendapatkan layanan tambahan lainnya.

Peruri CA may charge fees for other additional services.

9.1.5 Kebijakan Pengembalian Biaya / Refund Policy

Peruri CA dapat menyediakan kebijakan pengembalian biaya kepada para Pemilik. Bagi pemilik sertifikat yang mengajukan permohonan pengembalian biaya, semua sertifikatnya dicabut.

Peruri CA may provide a refund policy to Subscribers. For Subscribers who submit a refund request, all certificates are revoked.

9.2 TANGGUNG JAWAB KEUANGAN / FINANCIAL RESPONSIBILITY

9.2.1 Cakupan Asuransi / Insurance Coverage

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

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

9.2.2 Aset Lainnya / Other Assets

Tidak ada ketentuan

No stipulation.

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

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

9.3 KERAHASIAAN INFORMASI BISNIS / CONFIDENTIALITY OF BUSINESS INFORMATION

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

9.3.1 Cakupan Informasi Rahasia / Scope of Confidential Information

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

- Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
- Rekam jejak audit (*audit logs*) dari sistem PSrE dan RA;
- Data aktivasi pada saat pengaktifan Kunci Privat PSrE sebagaimana dijabarkan pada Bagian 6.4;
- Dokumentasi bisnis proses PSrE termasuk dokumen Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); dan
- Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8.0.
- *Personal Information as detailed in Section 9.4;*
- *Audit logs from CA and RA systems;*
- *Activation data used to active CA Private Keys as detailed in Section 6.4;*
- *CAs business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and*
- *Audit Reports from an independent auditor as detailed in Section 8.0.*

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

Informasi yang tidak dikategorikan rahasia dalam dokumen CP dianggap informasi publik. Sertifikat dan informasi mengenai status sertifikat termasuk kategori informasi publik. *Any information not defined as confidential within the CP shall be deemed public. Certificate status information and Certificates themselves are deemed public.*

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

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

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

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

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

9.4 PRIVASI INFORMASI PRIBADI / PRIVACY OF PERSONAL INFORMATION

9.4.1 Rencana Privasi / Privacy Plan

Peruri CA akan mengembangkan, menerapkan, dan memelihara rencana privasi. Rencana privasi harus mendokumentasikan informasi yang dapat diidentifikasi secara pribadi yang dikumpulkan, bagaimana itu disimpan dan diproses, dan dalam kondisi apa informasi tersebut dapat diungkapkan.

Peruri CA shall develop, implement and maintain a privacy plan. The privacy plan shall document what personally identifiable information is collected, how it is stored and processed, and under what conditions the information may be disclosed.

Peruri CA harus melindungi informasi pribadi dalam kaitan dengan “Kebijakan Informasi Pribadi” yang dipublikasikan sesuai dengan ketentuan repositori pada Bagian 2.1.

Peruri CA shall protect personal information in accordance with a Privacy Policy published on a suitable Repository along with this CP. Section 2.1.

9.4.2 Informasi yang Dianggap Pribadi / Information Treated as Private

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

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

9.4.3 Informasi tidak Dianggap Pribadi / Information not Deemed Private

Informasi yang termasuk dalam Bagian 7 (Sertifikat, CRL, Profil OCSP) dari CP ini tidak termasuk dalam Bagian 9.4.2.

Information included in Section 7 (Certificate, CRL and OCSP Profiles) of this CP is not subject to protection outlined in Section 9.4.2 (Information Treated as Private) above.

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

Peruri CA bertanggung jawab untuk menyimpan informasi pribadi sesuai dengan Kebijakan “Perlindungan Data Pribadi” secara aman. Informasi yang disimpan dapat berbentuk digital maupun kertas. Backup informasi pribadi harus dienkripsi setiap akan dipindahkan ke media *backup*.

Peruri CA are responsible for securely storing private information in accordance with a published privacy policy document and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media.

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

Informasi pribadi yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. Peruri CA akan mengakomodir semua ketentuan terkait penggunaan informasi pribadi ke dalam Kontrak Berlangganan yang juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh Peruri CA.

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

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

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

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

9.4.7 Keadaan Pengungkapan Informasi Lain / Other Information Disclosure Circumstances

Tidak ada ketentuan.

No stipulation.

9.5 HAK ATAS KEKAYAAN INTELEKTUAL / INTELLECTUAL PROPERTY RIGHTS

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

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

9.6 PERNYATAAN DAN JAMINAN / REPRESENTATIONS AND WARRANTIES

9.6.1 Pernyataan dan Jaminan Peruri CA / Peruri CA Representations and Warranties

Peruri CA menyatakan dan menjamin, sejauh

Peruri CA represents and warrants, to the

yang ditentukan dalam CP, bahwa:

- Peruri CA mematuhi ketentuan yang diatur dalam CP ini,
- Peruri CA menerbitkan dan memperbarui CRL secara berkala,
- Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP ini,
- Peruri CA akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya.

extent specified in this CP, that:

- *Peruri CA complies, in all material aspects, with the CP,*
- *Peruri CA publishes and updates CRL on a regular basis,*
- *All certificates issued will meet the minimum requirements and verified in accordance with this CP and,*
- *Peruri CA will display information that can be accessed publicly through its repositories.*

9.6.2 Pernyataan dan Jaminan RA / RA Representations and Warranties

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

RA's warrant that:

- Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran Sertifikat atau penerbitan Sertifikat,
- Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat,
- Peruri CA mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CP dan dituangkan dalam kontrak.

- *There are no fallacy on Certificate that have been known or came from the entity who gives an acknowledgement on Certificate application or Certificate issuance,*
- *There are no false information in the Certificate carried by the entity that approves the registration of the Certificate as a result of inaccuracy in the Certificate Registration Management,*
- *CAs required all RAs to guarantee all registration activity that have been done by Ras comply with CP and stated at the contract.*

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat / Subscriber Representations and Warranties

Pemilik Sertifikat menjamin bahwa:

Subscribers warrant that:

- Setiap sertifikat digital yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah merupakan tanda tangan digital pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan digital dibuat;
- Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;

- *Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;*
- *Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key;*

- Sudah melakukan *review* terhadap informasi dari sertifikat;
- Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;
- Sertifikat Digital digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CP ini;
- Segera:
 - a) melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat; dan
 - b) mengajukan permohonan untuk melakukan pencabutan Sertifikat, dan berhenti menggunakannya, jika ada informasi apa pun yang tidak sesuai atau menjadi tidak sesuai di dalam sertifikat tersebut;
 - c) menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam sertifikat digital setelah sertifikat dicabut;
- Akan menanggapi instruksi Peruri CA terkait kebocoran atau penyalahgunaan sertifikat digital dalam kurun waktu empat puluh delapan (48) jam;
- Menyetujui dan menerima bahwa Peruri CA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika Peruri CA menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan atau pendistribusian *malware*;
- Pengguna akhir dan bukan merupakan PSrE, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat Digital untuk tujuan
 - a) *request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;*
 - b) *request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;*
 - c) *stop using the private key whose public key is listed in a digital certificate after the certificate is revoked;*
- *Have thoroughly reviewed the certificate information;*
- *All information supplied by the Subscriber and contained in the Certificate is true;*
- *The Certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CP and the applicable CPS, and*
- *Promptly:*
 - a) *request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;*
 - b) *request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;*
 - c) *stop using the private key whose public key is listed in a digital certificate after the certificate is revoked;*
- *Will respond to Peruri CA's instructions regarding compromise or digital certificates misuses within forty eight (48) hours,*
- *Acknowledges and accepts that Peruri CA is entitled to revoke the Certificate immediately if the subscriber violates the terms of the Subscriber Agreement or Terms of Use or if Peruri CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware, and*
- *The Subscriber is an end-user Subscriber and not a CA and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally*

penandatanganan sertifikat digital PSrE lain.

signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

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

Pihak yang mengandalkan Sertifikat Peruri CA menjamin bahwa:

Peruri CA's Certificate relying party guarantee that:

- Memiliki kemampuan teknis untuk menggunakan sertifikat,
 - Apabila perwakilan dari pihak pengandal menggunakan suatu sertifikat yang diterbitkan oleh Peruri CA, pihak pengandal harus secara benar memverifikasi informasi yang tercantum di dalam sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut,
 - Melaporkan langsung kepada RA yang berwenang, jika pihak pengandal menyadari atau mencurigai bahwa telah terjadi compromise pada Kunci Privat
 - Mewajibkan Pihak Pengandal untuk mengakui bahwa mereka memiliki cukup informasi untuk membuat keputusan berdasarkan informasi sejauh mana mereka memilih untuk bergantung pada informasi dalam Sertifikat, bahwa mereka sepenuhnya bertanggung jawab untuk memutuskan apakah bergantung atau tidak pada informasi tersebut, dan mereka akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pihak Pengandal yang ada pada CP ini,
 - Harus mematuhi ketentuan yang ditetapkan di CP dan perjanjian lain yang terkait.
- *Have the technical capability to use certificates,*
 - *If the representative from the Relying Party uses a certificate issued by Peruri CA, the relying party should verify the information contained in the certificate before use and carry all the consequences that happened if the relying party fails to apply it,*
 - *Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised,*
 - *Required relying party to acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the Certificate, that they are fully responsible for deciding to rely on the information or not, and they will carry the legal consequences from the failure to fulfill the obligation of the Relying Party as mentioned in the CP,*
 - *Must compliance with the provisions of this CP and related agreements.*

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

Tidak ada ketentuan.

No stipulation.

9.7 PELEPASAN JAMINAN / DISCLAIMER OF WARRANTIES

Peruri CA harus membuat pernyataan dalam

Peruri CA should make statements in their CPS

CPS bahwa Peruri CA tidak menjamin:	<i>that they do not warrant:</i>
<ul style="list-style-type: none"> 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, 	<ul style="list-style-type: none"> <i>Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, Peruri CA disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use.</i>
<ul style="list-style-type: none"> Penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (Certificate Usage), 	<ul style="list-style-type: none"> <i>Misuse of a certificate that is inconsistent with its usage as shown in section 4.5 (Certificate Usage),</i>
<ul style="list-style-type: none"> Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau testing Sertifikat. 	<ul style="list-style-type: none"> <i>The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo Certificates.</i>

9.8 PEMBATASAN TANGGUNG JAWAB / LIMITATIONS OF LIABILITY

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

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

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

- semua kerusakan yang dihasilkan dari penggunaan sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CP, kontrak pemilik sertifikat, atau yang diatur dalam sertifikat itu sendiri,
- semua kerusakan yang disebabkan oleh *force majeure*,
- semua kerusakan yang disebabkan oleh malware (seperti virus atau Trojans) diluar perangkat Peruri CA,
- semua kesalahan data informasi sertifikat yang berasal dari pemilik sertifikat setelah periode verifikasi data selesai,
- sertifikat yang tidak diterbitkan atau dikelola sesuai dengan Persyaratan ini atau *Certificate Policy* Peruri CA dan / atau *Certificate Practice Statement*.
- all damage caused by the misuse of certificates or key pairs beside the proper use that have been defined in CP, subscriber agreement, or all provision which have been mentioned in The Certificate,*
- all damage caused by the force majeure condition,*
- all damage caused by the Malware (i.e virus or Trojan) outside Peruri CA devices,*
- all incorrect certificate information that comes from subscriber after data verification period is complete,*
- certificates not issued or administered in accordance with Peruri CA Certificate Policy and/or Certificate Practice Statement.*

9.8.2 Pembatasan Tanggung Jawab RA / RA Limitation of Liability

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan Peruri CA.

The cap on Registration Agent's liability is specified in the frame contract between

Secara khusus, RA bertanggung jawab atas pendaftaran pemilik sertifikat.

Registration Agent and CAs. In particular, the Registration Agent is liable for the registration of subscribers.

9.9 GANTI RUGI / INDEMNITIES

9.9.1 Ganti Rugi oleh Peruri CA / Indemnification by Peruri CA

Kewajiban ganti rugi Peruri CA harus ditetapkan dalam CPS, Kontrak Berlangganan, atau Perjanjian Pihak Pengandal termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.

Peruri CA's indemnification obligations must be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Subscriber

Peruri CA harus menyertakan persyaratan ganti rugi untuk Pemilik Sertifikat dalam CPS dan dalam Kontrak Berlangganannya.

Peruri CA shall include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3 GantiRugi oleh Pihak Pengandal / Indemnification by Relying Parties

Peruri CA harus menyertakan persyaratan ganti rugi untuk Pihak Pengandal dalam CPS.

Peruri CA's shall include its indemnification requirements for Relying Parties in its CPS.

9.10 SYARAT DAN PENGAKHIRAN / TERM AND TERMINATION

9.10.1 Syarat / Term

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

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

9.10.2 Pengakhiran / Termination

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

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

9.10.3 Efek Pengakhiran dan Keberlangsungan / Effect of Termination and Survival

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

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

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

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

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

9.12 AMANDEMEN / AMENDMENTS

9.12.1 Prosedur untuk Amandemen / Procedure for Amendment

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

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

9.12.2 Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

PSrE harus menerbitkan pemberitahuan di situs web terkait perubahan besar atau signifikan dari CP ini termasuk juga keterangan waktu ketika CP efektif berlaku. Ketika terjadi perubahan, CP harus dipublikasikan paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.

CAs should post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted. When there is a change, CP must be published no later than 7 (seven) working days from the date it was signed.

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

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

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

9.13 PROVISI PENYELESAIAN KETIDAKSEPAHAMAN / KETENTUAN PENYELESAIAN SENGKETA / DISPUTE RESOLUTION PROVISIONS

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CP ini, para pihak akan berusaha untuk mencapai penyelesaian

In case of dispute or controversy related performance, execution or the interpretation of the CP, all parties will try to reach a peaceful settlement. The official provisions of the

damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara Peruri CA dengan pemilik sertifikat.

dispute are part of the contract agreed upon between Peruri CA and the certificate owner.

9.14 HUKUM YANG MENGATUR / GOVERNING LAW

CP ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat Peruri CA ataupun produk/ layanan lainnya. Termasuk apabila sertifikat Peruri CA dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia. Para pihak, termasuk partners Peruri CA, pemilik, pihak pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

This CP is governed, construed and interpreted in accordance with the laws of Indonesia. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Certificates or other products and services. The laws of Indonesia also apply to all Peruri CA commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to Peruri CA products and services where Peruri CA acts as a provider, supplier, beneficiary receiver or otherwise. Each party, including Peruri CA partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Indonesia.

9.15 KEPATUHAN ATAS HUKUM YANG BERLAKU / COMPLIANCE WITH APPLICABLE LAW

Peruri CA mematuhi hukum yang berlaku di Indonesia. Ekspor berbagai jenis perangkat lunak tertentu yang digunakan dalam beberapa produk dan layanan manajemen Sertifikat publik Peruri CA dapat memerlukan persetujuan dari otoritas publik atau pihak swasta yang berwenang. Para Pihak (termasuk Peruri CA, Pemilik, dan Pihak Pengandal) setuju untuk mematuhi undang-undang dan regulasi ekspor yang berlaku di Indonesia.

Peruri CA complies with applicable laws of Indonesia. Export of certain types of software used in certain Peruri CA public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including Peruri CA, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Indonesia.

9.16 KETENTUAN YANG BELUM DIATUR / MISCELLANEOUS PROVISIONS

9.16.1 Seluruh Perjanjian / Entire Agreement

Tidak ada ketentuan.

No stipulation.

9.16.2 Pengalihan Hak / Assignment

Entitas yang beroperasi dibawah CP ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari PSrE.

Entities operating under this CP may not assign their obligations without the prior written consent of PeruriCA.

9.16.3 Keterpisahan / Severability

Jika terdapat ketentuan dari dari CP ini, termasuk pembatasan dari klausul pertanggunggaan, ditemukan tidak sah atau tidak dapat dilaksanakan, bagian CP ini selanjutnya akan ditafsirkan sedemikian rupa sehingga dapat mendukung maksud awal dari semua pihak. Setiap dan seluruh ketentuan dari CPS ini yang menjelaskan batasan tanggung jawab, dimaksudkan dapat dipisahkan dan bersifat independen dari ketentuan lain dan harus diberlakukan dengan sebagaimana harusnya.

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

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

Peruri CA dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan Peruri CA dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak Peruri CA untuk tetap menggunakan klausul ini di kemudian hari atau hak untuk menggunakan klausul lain dalam CP ini. Segala hal terkait pelepasan hak dalam pengadilan harus disampaikan secara tertulis dan ditandatangani Peruri CA.

Peruri CA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Peruri CA's failure to enforce a provision of this CP does not waive Peruri CA's right to enforce the same provisions later or right to enforce any other provisions of this CP. 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 CP 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, kerusakan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga. Peruri CA wajib menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Peruri CA.

Peruri CA shall not be liable for any failure or delay in its performance under this CP 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.

9.17 PROVISI LAIN / OTHER PROVISIONS

Tidak ada ketentuan.

No stipulation.