PEDOMAN KEPALA BALAI BESAR SERTIFIKASI ELEKTRONIK

NOMOR 38 TAHUN 2026

TENTANG

PERNYATAAN PRAKTIK SERTIFIKASI ELEKTRONIK

BALAI BESAR SERTIFIKASI ELEKTRONIK (BSrE)

CERTIFICATION PRACTICE STATEMENT

BALAI BESAR SERTIFIKASI ELEKTRONIK (BSrE)

Versi 4.0

Nomor dokumen	38 Tahun 2026
Tanggal pembuatan	20 Januari 2022
Tanggal Efektif	27 April 2026
Jadwal Reviu	27 April 2027
Klasifikasi	Biasa
Disahkan oleh	

Lembar Catatan Review / Revisi

No.	Tanggal	Versi	Deskripsi	Oleh
1.	26 Juni 2022	1	Terbitan Pertama	*Policy Authority* BSrE
2.	23 September 2022	1.1	Terbitan Kedua - Penyelarasan CP PSrE Induk - Penghapusan akronim yang tidak digunakan	*Policy Authority* BSrE
3.	17 Januari 2023	1.2	Terbitan Ketiga - Perubahan profil sertifikat BSrE CA DS - Perubahan level verifikasi	*Policy Authority* BSrE
4.	20 Maret 2023	2.0	Terbitan Keempat - Penambahan nomor OID untuk segel elektronik (Instansi), repositori, level verifikasi, dan AATL - Perubahan OID pada acuan OID sertifikat Policy Root CA - Penyelarasan ketentuan *backup off-site* dengan CP Induk - Penyelarasan ketentuan pemeriksaan Keberlakukan Sertifikat Elektronik oleh Pengandal dengan CP Induk - Penyelarasan ketentuan Prosedur Pemeriksaan Latar Belakang dengan CP Induk - Perubahan ketetuan prosedur backup arsip dengan CP induk - Penyelarasan nomenklatur PSrE Berinduk menjadi PSrE Indonesia - Penyesuaian pembangkitan pasangan kunci untuk tanda tangan elektronik dan segel elektronik - Penyesuaian pengiriman pasangan kunci untuk tanda tangan elektronik dan segel elektronik - Penyesuaian penyimpanan kunci privat untuk tanda tangan elektronik dan segel elektronik - Perubahan standard FIPS 140-2 Level 2 menjadi FIPS 140-2 Level 3 pada pembangkitan kunci pemilik	*Policy Authority* BSrE
5.	2 Oktober 2023	2.1	Terbitan Kelima - Penyesuaian Hasil Audit Surveillance Berinduk	*Policy Authority* BSrE
6.	6 Desember 2023	2.2	Terbitan Keenam - Penyesuaian daftar nama trusted role	*Policy Authority* BSrE
7.	7 Maret 2024	2.3	Terbitan Ketujuh - Penambahan Profil Sertifikat pada Lampiran	*Policy Authority* BSrE
8.	22 Oktober 2024	2.4	Terbitan Kedelapan - Perubahan nomenklatur Balai Besar Sertifikasi Elektronik	*Policy Authority* BsrE

9	27 Maret 2025	3.0	Terbitan Kesembilan - Perubahan dasar hukum pembentukan Balai Besar Sertifikasi Elektronik - Perubahan Panjang kunci BSrE CA 4096 Bit - Penghapusan nomor telepon data yang disampaikan BSrE CA pada Autentikasi Identitas Individu	*Policy Authority* BsrE
10	27 April 2026	4.0	Terbitan Kesepuluh - Penyesuaian Hasil Reviu CPS oleh Kementerian Komunikasi dan Digital pada tanggal 28 Agustus 2025	*Policy Authority* BsrE

DAFTAR ISI

BAB I
PENGANTAR / INTRODUCTION

1.1. Ringkasan / Overview

Balai Besar Sertifikasi Elektronik (BSrE) adalah unit pelaksana teknis di bawah Badan Siber dan Sandi Negara (BSSN) Republik Indonesia yang menyelenggarakan layanan Sertifikasi Elektronik, yaitu BSrE CA. Tujuan layanan BSrE CA adalah untuk memenuhi aspek keamanan bagi informasi dan/atau dokumen elektronik yang dikelola, dipertukarkan, dan disimpan dalam sistem elektronik melalui penggunaan Sertifikat Elektronik. Cakupan aspek keamanan informasi dalam penggunaan Sertifikat Elektronik meliputi kerahasiaan, autentikasi, integritas, dan nir-penyangkalan.

Balai Besar Sertifikasi Elektronik (BSrE) is an organization under the National Cyber and Crypto Agency of Republic of Indonesia (BSSN) that carry out the service of Certification Authority namely BSrE CA. The goal of BSrE CA services is to fulfill security aspects with a high degree of certainty for electronic information and/or documents that are managed, exchanged and stored in electronic systems through the use of Certificates. The scope of information security aspects in the use of Certificates includes confidentiality, authentication, integrity and non-repudiation.

Dokumen ini adalah CPS yang berisi acuan teknis dalam penyelenggaraan sertifikasi elektronik BSrE CA. Dokumen CPS BSrE CA ini mengacu pada ketentuan-ketentuan dasar penyelenggaraan sertifikasi elektronik pada kerangka RFC 3647 dari IETF tentang Internet X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework*, *Reference Certificate Policy* NIST IR 7924, ketentuan mengenai identitas digital mengacu pada NIST 800-63-3, dan *Certificate Policy* (CP) PSrE Induk. Regulasi dalam penyelenggaraan sistem dan transaksi elektronik di Indonesia yakni Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Menteri Komunikasi dan Informatika Nomor 11 Tahun 2022 tentang Tata Kelola Penyelenggaraan Sertifikasi Elektronik, Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2024 tentang Organisasi dan Tata Kerja Balai Besar Sertifikasi Elektronik.

This Certificate Practice Statement (CPS) document presents BSrE CA practices and procedures in managing Certificate. This document refers to the basic provisions for managing Certificate in RFC 3647 framework from the IETF on Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework, NIST IR 7924 about Certificate Policy, NIST 800-63-3 about digital identity provisions, and Root CA Certificate Policy. Implementation of electronic systems and transactions in Indonesia, is regulated in Government Regulation Number 71 of 2019 regarding Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Informatics Number 11 of 2022 regarding Governance of Electronic Certification Implementation, Regulation of the National Cyber and Crypto Agency Number 6 of 2024 regarding Organization and Work Procedure of Balai Besar Sertifikasi Elektronik.

1.2. Nama dan Identifikasi Dokumen CPS BSrE CA / Document Name and Identification CPS BSrE CA

Nama dokumen ini adalah CPS BSrE CA. OID dokumen ini adalah 2.16.360.1.1.1.3.11.2.0.1 dan versi dokumen ini adalah CPS BSrE CA Versi 3.0.

Document Name is the CPS for BSrE CA. Document OID is 2.16.360.1.1.1.3.11.2.0.1 and version document is BSrE CA's CPS version 3.0.

OID	Penggunaan / Usage
2.16.360.1.1.1.3.11	Sertifikat Instansi
2.16.360.1.1.1.3.11.2	BSrE CA
2.16.360.1.1.1.3.11.2.0.1	CPS
2.16.360.1.1.1.3.11.2.1	https://bsre.bssn.go.id/repository
2.16.360.1.1.1.5.1.4.3	Individu Instansi Online Level 3
2.16.360.1.1.1.8.2	Sertifikat Segel Elektronik (Instansi)

1.3. Partisipan IKP / PKI Participants

1.3.1 Penyelenggara Sertifikasi Elektronik (PSrE) / Certification Authorities

1.3.1.1 Penyelenggara Sertifikasi Elektronik (PSrE) Induk Indonesia / Indonesia Root CA

PSrE Induk Indonesia adalah PSrE Induk dari IKP Indonesia yang dioperasikan oleh Kementerian Komunikasi dan Digital Republik Indonesia dan membawahi 2 (dua) jenis PSrE Indonesia yaitu PSrE Indonesia Non-Instansi dan PSrE Indonesia Instansi yang dalam hal ini termasuk BSrE CA. PSrE Induk Indonesia bertanggung jawab terhadap penerbitan dan pengelolaan sertifikat PSrE Indonesia, sebagaimana dirinci dalam CP PSrE Induk Indonesia.

Indonesia Root CA is the root CA from PKI Indonesia which is operated by the Ministry of Communication and Digital of the Republic of Indonesia and oversees 2 (two) types of Subordinate CAs, Non-Government CAs, and Government CAs where in this case including BSrE CA. Root CA Indonesia is responsible for all aspects of the issuance and management of those Subordinate CA certificates, as detailed in Indonesia Root CA's CP.

1.3.1.2 BSrE CA

BSrE CA merupakan Penyelenggara Sertifikasi Elektronik Berinduk Instansi yaitu PSrE yang menerbitkan sertifikat elektronik bagi warga negara indonesia yang merupakan pegawai instansi dan/atau instansi. BSrE CA terdiri dari kumpulan perangkat keras, perangkat lunak, dan personil yang bertugas membuat, menandatangani, dan menerbitkan Sertifikat Elektronik untuk pemohon/ pemilik Sertifikat Elektronik. BSrE CA beroperasi sesuai dengan ketentuan peraturan perundang-undangan di Indonesia tentang Sertifikasi Elektronik. BSrE CA tidak boleh berinduk kepada PSrE lain dan tidak boleh menjadi induk bagi PSrE lainnya. BSrE CA membuat dan memelihara CPS serta memastikan bahwa semua aspek layanan BSrE CA, operasi, dan infrastruktur dilakukan sesuai dengan CP PSrE Induk.

BSrE CA is an Agency-Based Electronic Certification Provider, which is a CA that issues digital certificates for Indonesian citizens who are employees of agencies and/or agencies. BSrE CA consist of set hardware, software and personnel that serve to make, sign certificates and issues certificates to applicant/subscribes certificates. BSrE CA operates in accordance with laws and regulations in Indonesia concerning digital certification. BSrE CA doesn't become the root CA of other Indonesia CA and not rooted under other Indonesia CA but only to Indonesia Root CA. BSrE CA creates and maintains CPS and ensures that all aspects of BSrE CA services, operations, and infrastructure are conducted in accordance with the CP's Root CA.

1.3.2 Otoritas Pendaftaran (RA) / Registration Authorities

RA adalah personil yang bertanggung jawab melakukan pemeriksaan, persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik (atau calon pemilik) Sertifikat Elektronik BSrE CA.

RA are personnel responsible examine, approve or reject any request for issuance, renewal, revocation of the digital certificate submitted by the subscriber (or prospective subscriber) of the BSrE CA Certificate.

Fungsi dari RA / Function of Registration Authorities

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

1. Memproses setiap permintaan layanan penerbitan, pembaruan dan pencabutan Sertifikat Elektronik;
2. Melakukan proses identifikasi, autentikasi dan pemeriksaan terhadap kelengkapan bukti dan berkas milik entitas yang mengajukan permintaan layanan Sertifikat Elektronik.
3. Menyusun laporan penyelenggaraan RA dalam hal pemanfaatan Sertifikat Elektronik di lingkungan institusinya setiap

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

1. Processing every service request for issuance, renewal, and revocation of Certificates
2. Perform identification, authentication and examination of the completeness of evidence and files belonging to the entity submitting the Certificate service request.
3. Prepare reports on the implementation of RA in terms of the use of Certificates within the institution once every 1(one)

1 (satu) tahun sekali dan disampaikan kepada Pimpinan Institusi dan BSSN.

year and submitted to the Head of the Institution and BSSN.

Proses pendelegasian wewenang RA dari BSrE kepada Instansi pemilik Sertifikat Elektronik dilaksanakan melalui Uji Kelaikan RA berdasarkan Pedoman Audit Penyelenggaraan Otoritas Pendaftaran Sertifikat Elektronik di Instansi Pemerintah dan dilakukan audit minimal 1 (satu) kali dalam setahun.

BSrE delegates RA's Authority to the subscriber's Institution carried out using RA Assessment based on the Audit Guidelines for Implementation Registration Authorities of Digital Certificate in Government Agencies and audits are carried out at least 1 (one) time a year.

Wewenang RA diberikan setelah instansi pemilik sertifikat elektronik mendapatkan surat pengesahan lulus Uji Kelaikan RA yang dikeluarkan oleh Kepala BSrE.

RA's Authority is granted after subscriber's institution receives a letter of acceptance the RA Assesment issued by the Head of BSrE.

1.3.3 Pemilik Sertifikat Elektronik / Subscribers

Pemilik adalah pihak yang sudah melalui proses verifikasi identitas dan identitasnya tertera dalam sertifikat yang diterbitkan oleh BSrE CA. Entitas Pemilik berarti subjek pemilik Sertifikat Elektronik sekaligus entitas yang terikat dengan BSrE CA penerbit Sertifikat Elektronik. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat Elektronik, Pemilik disebut sebagai Pemohon.

Subscribers are the party who has gone through the identity verification process and whose identity is stated in the certificate issued by BSrE CA. Subscribers entity means the subject of the Digital Certificate owner as well as the entity bound to BSrE CA issuing the Digital Certificate. Prior to identity verification and the issuance of a Digital certificate, a Subscriber is referred to as an Applicant.

1.3.4 Pengandal Sertifikat Elektronik / Relying Parties

Pengandal adalah pihak yang mengandalkan (mempercayai) informasi yang ada dalam Sertifikat Elektronik dan/atau Tanda Tangan Elektronik yang diterbitkan oleh BSrE CA.

Relying Parties are all parties that rely on the information contained in the Certificates and/or any digital signatures and/or other services using Certificates verified using that Certificate.

Pengandal terlebih dahulu memeriksa respon dari CRL atau OCSP BSrE CA yang sesuai sebelum memanfaatkan informasi yang ada dalam sertifikat.

Relying Parties check the appropriate response from the BSrE CA's CRL or OCSP before relying on information featured in the Certificate.

Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam sertifikat. Pengandal dapat menggunakan informasi dalam sertifikat untuk menentukan kecocokan penggunaan sertifikat. Pengandal menggunakan informasi dalam Sertifikat Elektronik untuk:

1. Memeriksa tujuan penggunaan sertifikat;
2. Melakukan verifikasi tanda tangan elektronik;
3. Memeriksa status pencabutan Sertifikat Elektronik menggunakan CRL dan/atau OCSP; dan
4. Penyetujuan batas tanggung jawab dan jaminan

The Relying Party is responsible for checking the status of the information in the Certificate. A Relying Party may use the information in the Certificate to determine the conformity of usage and purpose of the Certificate. Relying parties use information on the Certificate to:

1. Checking for which purpose a certificate is used
2. Verifying the digital signatures
3. Checking the revocation status of Digital certificates using CRL and/or OCSP; and
4. Acknowledgement of applicable liability caps and warranties.

Pengandal dapat meliputi Bank, Perusahaan *e-Commerce*, Instansi Penyelenggara Negara dan entitas lain.

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

1.3.5 Partisipan Lain / Other Participants

BSrE CA dalam bekerjasama dengan partisipan lain untuk operasional BSrE CA mendapat persetujuan dari Kementerian Komunikasi dan Digital.

BSrE CA in cooperating with other participants for the operation of the BSrE CA receives approval from the Ministry of Communications and Digital.

1.3.5.1 Verifikator / Verificator

Verifikator adalah personel yang bertanggung jawab melakukan proses verifikasi terhadap kelengkapan bukti dan berkas calon atau Pemilik Sertifikat Elektronik BSrE CA pada proses pendaftaran Sertifikat Elektronik.

Verificator is personnel who are responsible for carrying out verification process the completeness of evidence and files of candidates or BSrE CA's Subscribers in Certificate registration process.

1.3.5.2 Penyedia layanan Pusat Data / Data Center Vendor

Penyedia layanan Pusat Data adalah pihak yang menyediakan layanan Pusat Data untuk operasional BSrE CA.

Data Center vendor is a third party that provides Data Center service for BSrE CA operation.

1.4. Kegunaan Sertifikat Elektronik / Certificate Usage

Informasi yang diproses atau dilindungi menggunakan Sertifikat Elektronik yang diterbitkan oleh BSrE CA bervariasi ditinjau dari derajat kepentingan penggunaannya.

Information that is processed or protected using Certificates issued by BSrE CA varies in terms of the degree of importance of its use.

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 Elektronik BSrE CA dapat digunakan untuk transaksi yang memerlukan:

1. Autentikasi;
   Jenis Sertifikat yang disediakan adalah Sertifikat untuk otentikasi dua arah
2. Tanda Tangan Elektronik & Non-Repudiasi;
   Jenis Sertifikat yang disediakan BSrE CA adalah Sertifikat Tanda Tangan dokumen

Subscriber's certificate usage is restricted by the Key Usage and Extended Key Usage of the certificate extension. Subscriber's certificate can be used for public transactions that require:

1. Authentication
   The type of certificate provided is a certificate for two-way authentication.
2. Digital signature dan nonrepudiation
   The type of certificate provided BSrE CA is document signing certificate

Level Sertifikat	Level Verifikasi			Penggunaan	
	Verifikasi Rendah	Verifikasi Sedang	Verifikasi Tinggi	Autentikasi	Tanda tangan elektronik dan Nirsangkal
Level 3			✓	✓	✓

BSrE CA menyediakan tingkat Jaminan yang dapat disesuaikan dengan kebutuhan transaksi, layanan tertentu, ataupun Pengandal. Sertifikat yang diterbitkan oleh BSrE CA adalah sertifikat dengan level verifikasi identitas yang sesuai dengan peraturan perundang-undangan yang mengatur mengenai penyelenggaraan sertifikasi elektronik. Level sertifikat yang dimaksud adalah sebagai berikut:

BSrE CA provides level of assurance that can be tailored to the needs of a particular transaction, service, or Relying Party. The certificate issued by BSrE CA is a certificate with a level of identity verification in accordance with the laws and regulations governing the implementation of certification authority. The level of certificate is as follows:

Level 3 : sertifikat yang diterbitkan atas aktivitas verifikasi identitas yang dilakukan dengan membandingkan kesesuaian data demografi Pemohon terhadap data demografi yang tersedia pada sumber data Tepercaya

Level 3 : Certificate issued based on identity verification carried out by comparing the suitability of the Applicant's demographic data to the demographic data available on authoritative sources based on a process

berdasarkan proses yang dilakukan dengan keterlibatan manusia (verifikator).

carried out with human (verificator) involvement.

1.4.2 Penggunaan Sertifikat yang Dilarang / Prohibited Certificate Uses

Sertifikat Elektronik yang telah diterbitkan oleh BSrE CA tidak boleh digunakan selain untuk keperluan yang tercantum pada Bagian 1.4.1 di atas.

Subscriber certificates issued under this CPS are prohibited under any use not specified in Section 1.4.1.

Sertifikat yang diterbitkan oleh BsrE CA hanya digunakan oleh pegawai Instansi dan/atau Instansi dalam rangka pelaksanaan tugas dan/atau kewenangannya.

Certificates issued by BsrE CA are only used by employees of the Agency and/or the Agency in the context of carrying out their duties and/or authorities.

1.5. Administrasi Kebijakan / Policy Administration

PA BSrE CA adalah Kepala BSrE.

PA memiliki peran dan tanggung jawab sebagai berikut:

1. Menetapkan CPS; dan
2. Memastikan semua layanan, operasional dan infrastruktur BSrE CA yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk.

PA of BSrE CA is the Head of BSrE.

PA has roles and responsibilities as follows:

1. Approves the CPS; and
2. Ensures that all aspects of the CA operational as described in the CPS are well performed in accordance with the requirementsm representations, and warranties of the Root CA's CP.

1.5.1 Organisasi Pengelola Dokumen / Organization Administering the Document

CPS dan dokumen referensinya dikelola oleh:

Policy Authority (PA) Balai Besar Sertifikasi Elektronik

This CPS and documents referenced herein are maintained by :

Policy Authority (PA) Balai Besar Sertifikasi Elektronik

1.5.2 Kontak yang Dapat Dihubungi / Contact Person

Kepala Balai Besar Sertifikasi Elektronik
Web BSrE : https://bsre.bssn.go.id
Telegram: t.me/infobsre
Email: info.bsre@bssn.go.id
Jl. Harsono RM No.mor 70, RT.2/RW.4, Ragunan, Kec. Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550

Head of Balai Besar Sertifikasi Elektronik
Web BSrE : https://bsre.bssn.go.id
Telegram: t.me/infobsre
Email: info.bsre@bssn.go.id
Jl. Harsono RM No.mor 70, RT.2/RW.4, Ragunan, Kec. Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550

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

PA BSrE CA menentukan kesesuaian konten CPS dan kesesuaian antara CPS dengan CP PSrE Induk.

PA of BSrE CA determines suitability of this CPS and the conformance of the CPS to CP.

1.5.4 Prosedur Persetujuan CPS / CPS Approval Procedures

PA BSrE CA menyetujui CPS BSrE CA dan segala amandemen/perubahannya setelah mendapat persetujuan dari PA PSrE Induk. Amandemen dibuat dengan mengubah seluruh CPS atau sebagian CPS dan mempublikasikan seluruh perubahan atau adendum yang telah disetujui. PA BSrE CA menentukan apakah perubahan atas CPS membutuhkan pemberitahuan atau perubahan OID.

PA BSrE CA approves the BSrE CA CPS and any amendments/changes after approval by the PA Root CA. Amendments are made by changing the entire CPS or parts of the CPS and publishing all approved changes or addendums. PA BSrE CA determines whether changes to the CPS require notification or OID changes.

1.6. Definisi dan Akronim / Definitions and Acronyms

Lihat Lampiran A untuk tabel definisi dan akronim.

See Appendix A for a table of definitions and acronyms.

BAB II
TANGGUNG JAWAB PUBLIKASI DAN REPOSITORI / PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositori / Repositories

BSrE CA bertanggung jawab memelihara repositori daring yang dipublikasikan pada suatu sistem repositori, yang berisi :

1. Sertifikat BSrE CA;
2. CRL dan daftar responder OCSP*;*
3. CPS;
4. Kebijakan Privasi;
5. Perjanjian Pemilik;
6. Perjanjian Pengandal;
7. Kebijakan Jaminan; dan
8. Petunjuk teknis verifikasi tanda tangan digital pada dokumen PDF.

BSrE CA is responsible to maintaining publicly accessible online repositories which contain :

1. BSrE CA's Certificate;
2. CRL and OCSP responder lists*;*
3. CPS;
4. Privacy Policy;
5. User Agreement;
6. Relying Party Agreement;
7. Warranty Policy; and
8. Technical Document of digital signature validation on PDF.

2.2 Publikasi Informasi Sertifikat Elektronik / Publication of Certification Information

BSrE CA memelihara repositori yang dapat diakses melalui internet, sebagai tempat publikasi file atau dokumen yang disebutkan pada bagian 2.1. Repositori resmi dari BSrE CA dapat diakses pada https://bsre.bssn.go.id/repository.

BSrE CA maintains a repository that can be accessed via the internet. This repository serves as a place for publishing files or documents mentioned in section 2.1. The official repository of BSrE CA can be accessed at https://bsre.bssn.go.id/repository.

2.3 Waktu atau Frekuensi Publikasi / Time or Frequency of Publication

Versi terbaru dari dokumen CPS BSrE CA tersedia dalam jangka waktu maksimum 7 (tujuh) hari kerja sejak tanggal efektif. BSrE CA mempublikasikan informasi CRL secara reguler dan terjadwal sebagaimana diatur dalam bagian 4.9.7.

The latest version of BSrE CA's CPS will be publicly accessible within 7 (seven) days after approval. BSrE CA publishes CRL information on regular schedule as regulated in Section 4.9.7.

2.4 Kendali Akses Pada Sistem Repositori / Access Controls of Repositories System

Informasi yang terpublikasi pada repositori adalah informasi publik. BSrE CA memberikan akses baca yang tidak dibatasi pada repositori dan menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut. BSrE CA melindungi informasi yang tidak ditujukan untuk disebarkan kepada publik atau diubah oleh publik.

Information published in the repository is public information. BSrE CA provides unrestricted read access to the repository and applies logical and physical controls to prevent unauthorized write access to the repository. BSrE CA protects information that is not intended for public dissemination or public alteration.

BAB III
IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION

3.1 Penamaan / Naming

3.1.1 Tipe Nama / Types of Names

BSrE CA membangkitkan dan menandatangani Sertifikat dengan subjek *Distinguished Name* (DN) yang non-null dan mematuhi standar ITU X.500. Berikut tabel penjelasan DN BSrE CA dan DN pemilik sertifikat.

BSrE CA generates and sign Certificates with a non-null subject Distinguished Name (DN) that complies with the ITU X.500 standards. The following table describes the DN BSrE CA and the DN of the Subscriber.

Tipe Sertifikat	*Distinguished Name*
Sertifikat CA	CN= BSrE DS CA G1; O=Badan Siber dan Sandi Negara; C=ID
Sertifikat Perorangan	CN={Nama Orang}[1] C=ID Description={XXYYYYZZZZZZZZZZ_Tanda Tangan Elektronik}
Sertifikat Organisasi (Segel Elektronik)	CN={Nama Divisi/Unit Organisasi/Nama Sistem Elektronik}[2], O={Nama Organisasi} C=ID Description={XXYYYYZZZZZZZZZZ_Segel Elektronik}

Catatan:
1 = string maksimum 25 karakter sesuai Identitas Nasional (KTP), tanpa gelar
2 = string maksimum 25 karakter sesuai Surat Rekomendasi/Surat Keputusan
AMS ID = {XXYYYYZZZZZZZZZZ_produk}
XX = OID CA
Y = 4 Digit OID RA
Z = 10 Digit *random character* menggunakan *random generator*

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

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

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

Nama subjek dan penerbit yang terkandung dalam Sertifikat bermakna dalam arti bahwa BSrE CA memiliki cukup bukti yang menunjukkan keterkaitan antara nama dengan Pemilik. 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 the Certificate is meaningful in the sense that the BSrE CA has sufficient evidence demonstrating the link between the name and the Subscriber. To this end, the use of the name must be authorized by the legal Subscriber or an authorized representative of the legal Subscriber.

3.1.3 Penggunaan nama yang anonim dan Pseudonimitas oleh Pemilik Sertifikat Elektronik / Anonymity and Pseudonymity of Subscribers

BSrE CA tidak menerbitkan sertifikat elektronik anonim atau pseudonim.

BSrE CA not issue anonymous or pseudonymous Certificates.

3.1.4 Aturan untuk menginterpretasikan jenis penamaan lainnya / Rules for Interpreting Various Name Forms

DN dalam Sertifikat BSrE CA hanya mengacu pada ketentuan dalam standar ITU X.500.

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

3.1.5 Keunikan Nama / Uniqueness of Names

Semua DN adalah unik di dalam ranah BSrE CA.

All distinguished names issued by BSrE CA are unique.

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

Pemohon dan BSrE CA tidak mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. BSrE CA tidak memverifikasi hak Pemohon untuk penggunaan merek dagang. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih. BSrE CA menolak permohonan atau mencabut Sertifikat yang menjadi bagian dari sengketa merek dagang.

The Applicant and BSrE CA are not applying for a Certificate with content that infringes the intellectual property rights of others. BSrE CA does not verify the Applicant's right to use trademarks. The owner is responsible for ensuring the validity of the use of the chosen name. BSrE CA rejects applications or revokes Certificates that are part of a trademark dispute.

3.2 Validasi Identitas / Identity Validation

3.2.1 Metode untuk membuktikan kepemilikan Kunci Privat / Method to Prove Possession of Private Key

Pasangan Kunci Sertifikat Pemilik dibangkitkan oleh BSrE CA, dengan ketentuan Kunci Privat diamankan dengan menggunakan modul kriptografis FIPS 140-2 dan hanya dapat diakses oleh Pemilik menggunakan 2 (dua) faktor autentikasi.

The Subscriber Certificate Key Pair is generated by the BSrE CA, provided that the Private Key is secured using the FIPS 140-2 cryptographic module and can only be accessed by the Subscriber using two (2) authentication factors.

3.2.2 Autentikasi Identitas Organisasi / Authentication of Organization Identity

RA atau Verifikator melakukan pemeriksaan untuk setiap informasi identitas divisi/unit organisasi/sistem elektronik yang mengajukan permohonan Sertifikat Elektronik. Proses autentikasi identitas divisi/unit organisasi/sistem elektronik dapat dilakukan secara jarak jauh (*remote/online*) antara RA atau Verifikator dengan pemohon.

RA or verificator perfom verification to the division/ organization unit/electronic system that applies for a Digital Certificate. The verification process of identity about division/organization unit/electronic system can be conducted (remote/online) between RA and the applicant.

Pemeriksaan identitas wewenang/organisasi pemohon harus melampirkan Surat Tugas atau Surat Pernyataan yang menunjukkan bahwa pemohon memiliki kewenangan atau tanggung jawab terhadap organisasi.Pemohon wajib menyampaikan informasi berikut:

1. Surat permohonan yang memuat persetujuan untuk penerbitan Sertifikat Elektronik yang diajukan oleh pimpinan Instansi yang secara sah memiliki kewenangan untuk bertindak mewakili Instansi tersebut;
2. Peraturan perundang-undangan pembentukan Instansi;
3. Surat penugasan sebagai penanggung jawab atau perwakilan Instansi atau unit kerja yang mendaftar, berisi nomor identitas pegawai, nama, dan jabatan;
4. Nomor telepon penanggung jawab atau perwakilan Instansi; dan
5. Alamat email penanggung jawab atau perwakilan Instansi menggunakan nama domain Instansi atau alamat email resmi

For verification, the applicant must present an assignment letter indicating that the applicant has authority or responsibility toward the organization.
Applicant must submit this information:

1. A request letter containing approval for the issuance of an Electronic Certificate, submitted by the head of the Institution who is legally authorized to act on behalf of the Institution;
2. The laws and regulations concerning the establishment of the Institution;
3. A letter of assignment designating the person in charge or representative of the Institution or registering work unit, including employee identification number, name, and position;
4. The telephone number of the person in charge or representative of the Institution; and
5. The email address of the person in charge or representative of the Institution, using the Institution’s domain name or an official

Instansi.	institutional email address.

3.2.3 Autentikasi Identitas Individu / Authentication of Individual Identity

RA atau Verifikator harus melakukan pemeriksaan untuk setiap informasi identitas individu yang mengajukan permohonan Sertifikat Elektronik. Proses autentikasi identitas individu dapat dilakukan secara jarak jauh (*remote/online*) antara RA atau Verifikator dengan pemohon. Data yang diajukan terverifikasi dengan data dari *database* Kependudukan dan Pencatatan Sipil (Dukcapil) serta database Badan Kepegawaian Negara (BKN).	The RA or Verifier must perform a check for each individual identity information that applies for an Digital certificate. The individual identity authentication process can be done remotely (remote/online) between the RA or Verifier and the applicant. The data submitted is verified with data from the Population and Civil Registration (Dukcapil) database and the National Civil Service Agency (BKN) database.
Data yang disampaikan meliputi: 1. Nama; 2. Nomor Induk Kependudukan (NIK); 3. Nomor Induk Pegawai (NIP); 4. Nama Organisasi; 5. Unit Organisasi; 6. Jabatan; 7. Nomor Telepon; 8. Alamat surat elektronik (email) kedinasan; dan 9. Foto wajah.	The data submitted includes: 1. Name; 2. Single Identity Number (NIK); 3. Employee Identity Number (NIP); 4. Organization Name; 5. Organization Unit; 6. Position; 7. Number Phone; 8. Official e-mail Address; and 9. Face Photo.
BSrE CA menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi individu setidaknya untuk selama masa berlaku dari Sertifikat yang diterbitkan.	BSrE CA keeps records of the type and details of identification used to authenticate individuals for at least the validity period of the issued Certificate.
BSrE CA tidak menerbitkan Sertifikat bagi Pemohon yang tidak dapat diverifikasi.	BSrE CA does not issue Certificates to Applicants who cannot be verified.

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

Informasi yang tidak bisa diverifikasi tidak disertakan di dalam sertifikat.	Information that cannot be verified is not included in the certificate.

3.2.5 Validasi Otoritas / Validation of Authority

Validasi otoritas melibatkan penentuan apakah seseorang memiliki hak khusus, hak, atau izin khusus, termasuk izin untuk bertindak atas nama organisasi untuk mendapatkan sertifikat. Sertifikat yang mengandung afiliasi keorganisasian secara eksplisit atau implisit hanya dapat diterbitkan setelah memastikan bahwa Pemohon adalah benar memiliki kewenangan untuk bertindak dalam kapasitas yang diberikan organisasinya.	Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate. A Certificate that has explicit/implicit organization affiliation can only be issued after RA has verified that the applicant has authority based on the organization's mandate.

3.2.6 Kriteria Inter-Operasi / Criteria for Interoperation

Kriteria interoperasi BSrE CA mengacu pada standar interoperabilitas yang diterbitkan oleh PSrE Induk.	BSrE CA interoperability criteria refers to the interoperability standards issued by Root CA.

3.3 Identifikasi dan Autentikasi untuk Permintaan Re-key Sertifikat Elektronik / Identification and Authentication for Re-Key Requests

.

3.3.1 Identifikasi dan autentikasi untuk Re-Key rutin / Identification and Authentication for Routine Re-Key

Sebelum masa berlaku Sertifikat berakhir, Pemilik meminta penggantian kunci yang selanjutnya disebut re-key dan Pemilik diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau menggunakan proses pemeriksaan identitas awal sebagaimana diatur pada bagian 3.2.

Prior to the expiry of the Certificate, the Subscriber requests a key change referred to as a re-key and the Subscriber is authenticated by signing using the current Certificate or using the initial identity proofing process as set out in section 3.2.

3.3.2 Identifikasi dan autentikasi untuk Re-Key setelah pencabutan / Identification and Authentication for Re-Key after Revocation

Pemilik yang mengajukan permohonan re-key setelah sertifikat dicabut menjalani proses pembuatan sertifikat baru sesuai dengan bagian 3.2.

The subscriber who request a re-key after their certificate has been revoked must go through the new certificate creation process according to section 3.2.

3.4 Identifikasi dan Autentikasi untuk Permohonan Pencabutan Sertifikat Elektronik / Identification and Authentication for Revocation Request

RA melakukan identifikasi dan autentikasi permohonan pencabutan dengan memeriksa hal-hal sebagai berikut:

1. Identitas pemilik Sertifikat Elektronik;
2. Tipe, nomor seri, dan informasi pada Sertifikat Elektronik;
3. Alasan pengajuan permohonan pencabutan.

RA identify and authenticate the revocation request by checking the following:

1. Identity of Subscribers;
2. Type, serial number, and information on the Certificate;
3. Revocation reasons.

Proses pencabutan Sertifikat Elektronik dapat dilakukan secara tatap muka dengan RA atau secara jarak jauh (*remote/online*).

Revocation process of certicate can be carried out offline or online with RA.

BAB IV
PERSYARATAN OPERASIONAL SIKLUS HIDUP SERTIFIKAT ELEKTRONIK / CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Permohonan Sertifikat Elektronik / Certificate Application

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

BSrE CA menerbitkan sertifikat bagi pemohon warga negara Indonesia yang merupakan pegawai Instansi dan/atau Instansi. Pihak yang berhak mengajukan permohonan Sertifikat Elektronik adalah:

1. Individu; dan
2. Individu yang mewakili instansi (Divisi/Unit Organisasi/ Sistem Elektronik).

BSrE CA issues certificates for Government employees and/or Government. Those who can submit certificate application are:

1. individual; and
2. Individual representing Government (Division/organizations unit, electronic systems)

4.1.2 Proses Pendaftaran dan Tanggung Jawab / Enrollment Process and Responsibilities

BSrE CA memelihara sistem dan proses yang secara memadai mengautentikasi identitas Pemohon untuk semua jenis sertifikat yang menyajikan identitas kepada Pihak Pengandal. Pemohon mengirimkan informasi yang cukup untuk memungkinkan BSrE CA dan RA melakukan verifikasi yang diperlukan. BSrE CA dan RA melindungi komunikasi dan menyimpan informasi yang disajikan dengan aman oleh Pemohon selama proses pendaftaran sesuai dengan Kebijakan Privasi BSrE CA.

BSrE CA maintains systems and processes that adequately authenticate the identity of the Applicant for all types of certificates that present the identity to the Relying Party. The Applicant submits sufficient information to allow BSrE CA and RA to perform the necessary verification. BSrE CA and RA protect communications and store information submitted securely by the Applicant during the registration process in accordance with the BSrE CA Privacy Policy.

Secara umum, proses pendaftaran mencakup langkah-langkah berikut:

1. Pemohon melengkapi formulir pendaftaran dan menyiapkan informasi yang dibutuhkan dengan sebenarnya;
2. Pemohon menyetujui Perjanjian Kepemilikan dan syarat ketentuan lain yang berlaku bersamaan dengan pengiriman permintaan pendaftaran tersebut.

Generally, the enrollment process includes the following steps:

1. Applicant completes the registration form and prepare all appropriate information;
2. Applicant agrees to a Subscriber Agreement and other applicable terms and conditions while submitting the enrollment request.

4.2 Proses Permohonan Sertifikat Elektronik / Certificate Application Processing

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

Identifikasi dan autentikasi Pemilik memenuhi persyaratan yang ditentukan seperti yang tertera pada bagian 3.2.

The identification and authentication of the Subscribers meets the specified requirements as set out in section 3.2.

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

RA atau BSrE memiliki wewenang untuk menyetujui atau menolak permohonan Sertifikat Elektronik. Apabila hasil proses identifikasi dan autentikasi dinyatakan sah, maka permohonan Sertifikat Elektronik disetujui dan diproses sesuai ketentuan. Namun apabila hasil proses identifikasi dan autentikasi dinyatakan tidak sah, maka permohonan Sertifikat Elektronik ditolak. Penolakan permohonan Sertifikat Elektronik

RA or BSrE has an authority to approve or reject Certificate applications. If the identification and authentication process results are valid, then the Certificate application is approved and processed according to the provisions. However, if the identification and authentication process results are invalid, the Certificate application will be rejected. Rejection of an Certificate application can be made for the following

dapat dilakukan karena sebab-sebab sebagai berikut:

1. Informasi dalam permohonan Sertifikat Elektronik tidak dapat diidentifikasi atau tidak autentik.
2. Pemohon Sertifikat Elektronik tidak melengkapi dokumen-dokumen sesuai dengan ketentuan.
3. Pemohon Sertifikat Elektronik masih memiliki sertifikat aktif dengan subjek DN yang sama.

reasons:

1. The information in the Certificate application is unidentifiable or inauthentic.
2. The Certificate Applicant does not complete the documents in accordance with the provisions.
3. The Digital certificate Applicant still has an active certificate with the same DN subject.

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

BSrE CA memproses permohonan dan menerbitkan Sertifikat Elektronik dalam jangka waktu maksimal 3 (tiga) hari kerja semenjak disetujuinya permohonan sertifikat tersebut.

BSrE CA processes an applications and issues Certificates within a maximum period of 3 working days after approval of certificate applications.

4.3 Penerbitan Sertifikat Elektronik / Certificate Issuance

4.3.1 Tindakan BSrE CA selama Penerbitan Sertifikat / CA Actions during Certificate Issuance

BSrE CA memverifikasi sumber Permohonan Sertifikat sebelum diterbitkan. Sertifikat diperiksa untuk memastikan semua field dan ekstensi telah diisi dengan benar sesuai dengan CPS bagian 3.2.2 dan 3.2.3.

BSrE CA verifies the source of the Certificate Request before it is issued. The certificate is checked to ensure that all fields and extensions have been filled in correctly in accordance with CPS sections 3.2.2 and 3.2.3.

BSrE CA mengautentikasi Permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, kemudian membuat Sertifikat Pemohon. BSrE CA mempublikasikan Sertifikatnya ke suatu repositori sesuai pada bagian 2.2.

BSrE CA authenticates the Certificate Request, ensures that the Public Key is associated with the correct Applicant, obtains proof of ownership of the Private Key, and generates the Applicant's Certificate. The BSrE CA publishes the Certificate to a repository in accordance with section 2.2.

BSrE memastikan Pemilik menerima Sertifikat sebagaimana diatur pada Bagian 4.4 dan BSrE membuat Sertifikat tersedia bagi Pemilik setelah Pemilik secara formal menyetujui kewajibannya sebagaimana diatur pada Bagian 9.6.3

BSrE ensures the Subscriber receives the Certificate as set out in Section 4.4 and BSrE makes the Certificate available to the Owner once the Subscriber has formally agreed to its obligations as set out in Section 9.6.3.

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

BSrE CA memberitahu Pemilik dalam maksimum 5 (lima) hari kerja tentang berhasilnya penerbitan sertifikat melalui email.

BSrE CA notifies the Subscriber within a maximum of 5 (five) working days of successful issuance via email.

BSrE memberitahu Pemilik bahwa mereka tidak dapat menggunakan Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

BSrE informs the Subscriber that they cannot use the Certificate before checking all the information in the Certificate.

4.4 Penerimaan Sertifikat / Certificate Acceptance

4.4.1 Sikap yang Dianggap Menerima Sertifikat / Conduct Constituting Certificate Acceptance

BSrE CA memberikan informasi bahwa Sertifikat Elektronik Pemilik berhasil diterbitkan. Ketika tidak ada keluhan dari Pemilik dalam jangka waktu 7 (tujuh) hari kerja, Pemilik dianggap menerima semua informasi Sertifikat.

BSrE CA provides information that Subscriber was successfully issued. When there is no complaint from the Subscriber within a period of 7 (seven) working days, the Subscriber is deemed to accept all Certificate information.

4.4.2 Publikasi Sertifikat Elektronik oleh BSrE CA / Publication of the Certificate by the CA

Sertifikat Elektronik BSrE CA segera dipublikasikan setelah diterbitkan sebagaimana diatur dalam bagian 2.1. dan 2.2.	BSrE CA's Digital certificates are published immediately upon issuance as set out in sections 2.1. and 2.2.

4.4.3 Pemberitahuan Penerbitan Sertifikat Elektronik oleh BSrE CA Kepada Entitas Lain / Notification of Certificate Issuance by the CA to Other Entities

Tidak ada ketentuan.	No stipulation

4.5 Penggunaan Pasangan Kunci dan Sertifikat / Key Pair and Certificate Usage

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

Pemilik Sertifikat dapat menitipkan Kunci Privatnya kepada BSrE CA dalam rangka *remote signing*, sesuai dengan persetujuan pada Perjanjian Pemilik Sertifikat. BSrE CA akan mengamankan Kunci Privat tersebut dengan menggunakan modul kriptografi FIPS 140-2 Level 2 dan menerapkan kombinasi paling sedikit 2 faktor autentikasi bagi pemilik yang akan menggunakan Kunci Privatnya. Pemilik melindungi parameter autentikasi yang digunakan untuk mengaktifkan Kunci Privatnya. BSrE CA melakukan upaya pengamanan dan penyimpanan sesuai dengan prosedur dan penuh kehati-hatian terhadap Kunci Privat Pemilik Sertifikat agar Kunci Privat tersebut hanya dapat digunakan oleh Pemilik Sertifikat.	The Certificate Subscriber may entrust the Private Key to the BSrE CA for remote signing, as agreed in the Certificate Subscriber Agreement. The BSrE CA will secure the Private Key using FIPS 140-2 Level 2 cryptographic modules and apply a combination of at least 2 authentication factors for owners who will use their Private Key. The owner protects the authentication parameters used to activate the Private Key. The BSrE CA safeguards and stores the Certificate Subscriber's Private Key in a procedurally appropriate and prudent manner so that the Private Key can only be used by the Certificate Subscriber.
BSrE dan Pemilik hanya memakai Kunci Privatnya untuk tujuan yang sudah ditentukan. Tujuan penggunaan harus diatur melalui ekstensi Sertifikat, yang dinyatakan dalam KeyUsage dan/atau ExtendedKeyUsage.	BSrE and the Owner only use the Private Key for the specified purpose. The purpose of use must be set through Certificate extensions, expressed in KeyUsage and/or ExtendedKeyUsage.

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

Pengandal memvalidasi Sertifikat Elektronik yang sesuai dengan X.509 dan menggunakan aplikasi yang sudah ditentukan oleh BSrE CA serta PSrE Induk. BSrE CA menentukan penggunaan dan mekanisme keabsahan Sertifikat Elektronik melalui ekstensi yang berisi URL dari CRL dan OCSP. Pengandal harus menjalankan dan patuh kepada ketentuan ini sesuai dengan kewajiban mereka sebagai Pengandal.	Relying Parties validate Certificates that comply with X.509 and use applications that have been determined by the BSrE CA and Root CA. The BSrE CA specifies the use and validity mechanism of Digital certificates through extensions containing the URLs of the CRL and OCSP. Trustees must implement and comply with these provisions in accordance with their obligations as Relying Parties.

4.6 Pembaruan Sertifikat Elektronik / Certificate Renewal

4.6.1 Kondisi Pembaruan Sertifikat Elektronik / Circumstance for Certificate Renewal

Tidak ada ketentuan.	No Stipulation.

4.6.2 Pihak yang Dapat Mengajukan Pembaruan Sertifikat Elektronik / Entities May Request Renewal

Tidak ada ketentuan.	No Stipulation.

4.6.3 Proses Permohonan Pembaruan Sertifikat Elektronik / Processing Certificate Renewal

Tidak ada ketentuan.	No Stipulation.

4.6.4 Pemberitahuan Kepada Pemilik Sertifikat Elektronik / Notification to Subscriber

Tidak ada ketentuan. | No Stipulation.

4.6.5 Aturan Penerimaan Sertifikat Elektronik Setelah Pembaruan Sertifikat Elektronik / Policy of Acceptance After Renewal Certificate

Tidak ada ketentuan. | No Stipulation.

4.6.6 Publikasi Setelah Pembaruan Sertifikat Elektronik oleh BSrE CA / Publication After Renewal Certificate by BSrE CA

Tidak ada ketentuan. | No Stipulation.

4.6.7 Pemberitahuan Pembaruan Sertifikat Elektronik Milik BSrE CA Kepada Pihak Lain / Notification of Certificate Issuance by the BSrE CA to Other Entities

Tidak ada ketentuan. | No Stipulation.

4.7 Re-Key Sertifikat / Certificate Re-Key

Re-key merupakan pembuatan / penerbitan sertifikat baru dengan kunci publik, serial number, dan key identifier yang baru, sementara informasi lain terkait pemilik dalam sertifikat baru masih sama dengan sertifikat lama. Sertifikat baru dapat diisi masa berlaku yang baru, diisi dengan tempat publikasi CRL yang baru, dan/atau ditandatangani dengan kunci yang baru.

Re-key is the creation/issuance of a new certificate with a new public key, serial number, and key identifier, while other information of Subscriber in the new certificate is still same with the latest certificate. New certificates may be filled with a new validity period, new CRL publication, and/or signed with a new key.

4.7.1 Kondisi untuk Re-Key Sertifikat / Conditions for Certificate Re-Key

BSrE CA melakukan re-key bagi pemilik sertifikat selama:

1. Sertifikat lama yang akan diganti belum dicabut atau belum terkompromi atau belum kedaluwarsa;
2. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi; dan
3. Apabila kunci privat pemilik terkompromi atau sertifikat kedaluwarsa, pemilik dapat mengajukan permohonan sertifikat baru sebagaimana diatur pada bagian 4.1.
4. Sertifikat elektronik yang masa berlakunya 30 (tiga puluh) hari sebelum kedaluwarsa.

BSrE CA re-keys the certificate Subscriber during:

1. The old certificate to be re-keyed has not been revoked or compromised or expired;
2. All details in the Certificate remain accurate and do not require new or additional validations; and
3. If the Subscriber's private key is compromised or the certificate expires, the Subscriber can submit a new application as stipulated in section 4.1
4. Digital certificates with a validity period of 30 days before expiration.

4.7.2 Pihak yang Dapat Meminta Re-Key Sertifikat dari Sebuah Kunci Publik yang Baru / Entities May Request Certification of a New Public Key

Pemilik Sertifikat Elektronik atau perwakilan instansi, RA, dan BSrE CA dapat mengajukan *re-key* Sertifikat Elektronik pada waktu 30 (tiga puluh) hari menjelang berakhirnya masa berlaku Sertifikat Elektronik serta sudah memenuhi salah satu kondisi pada bagian 4.7.1.

The subscriber or a Government representative, RA, and BSrE CA may apply certificate re-key within 30 days prior to the expiration date of certificate and has fulfilled one of the conditions as stipulated in Section 4.7.1.

4.7.3 Pemrosesan Permintaan *Re-Key* Sertifikat / Processing Certificate Re-Keying Requests

Saat memproses permohonan *re-key* sertifikat, permohonan diperiksa keabsahannya sebelum permohonan tersebut diproses (sesuai bagian 4.3). Masa berlaku sertifikat baru sama seperti masa berlaku sertifikat sebelumnya.

When processing a re-key Certificate issuance application, the validity of the application is checked before being process (according to section 4.3). The validity period of the new certificate is the same as the validity period of the previous certificate.

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

Prosedur notifikasi terhadap penerbitan sertifikat dilakukan sebagaimana dinyatakan pada bagian 4.3.2.

The same notification procedure of the certificate issuance is followed, as stated in section 4.3.2.

4.7.5 Sikap yang dianggap sebagai Penerimaan Sertifikat *Re-key* / Conduct Constituting Acceptance of a Re-Keyed Certificate

Pemilik menerima sertifikat re-key sesuai dengan prosedur penerimaan sertifikat yang tercantum pada bagian 4.4.1.

The Subscriber should receive the re-keyed certificate following the same procedure of acceptance of a new certificate, as stated in section 4.4.1.

4.7.6 Publikasi Sertifikat *Re-key* oleh BSrE CA / Publication of the Re-Key Certificate by BSrE CA

BSrE CA tidak melakukan publikasi sertifikat pemilik.

BSrE CA does not publish Subscriber's Certificate.

4.7.7 Pemberitahuan Sertifikat *Re-key* oleh BSrE CA / Notification of the Re-Key Certificate by BSrE CA

Tidak ada ketentuan.

No stipulation.

4.8 Modifikasi Sertifikat / Certificate Modification

Modifikasi detil sertifikat tidak diperbolehkan. Apabila terjadi kesalahan selama penerbitan sertifikat, sertifikat akan dicabut dan dilanjutkan dengan proses penerbitan seperti yang dijelaskan pada bagian 4.3

Modification of certificate details is not permitted. In case there is a mistake during certificate issuance, the certificate is revoked and the issuance process is followed, as stated in section 4.3.

4.9 Pencabutan Sertifikat Elektronik / Certificate Revocation

4.9.1 Kondisi Pencabutan Sertifikat Elektronik / Circumstances for Revocation

BSrE CA melakukan pencabutan Sertifikat Elektronik jika terjadi paling tidak satu dari kondisi-kondisi berikut:

1. Pemilik Sertifikat Elektronik memiliki bukti-bukti bahwa secara sengaja atau tidak sengaja Kunci Privat miliknya telah hilang, telah dicuri, telah diketahui, atau telah disalahgunakan oleh pihak lain;
2. Pemilik Sertifikat Elektronik masih memiliki Sertifikat Elektronik dan kunci privat yang berelasi namun tidak mengingat/lupa *passphrase* untuk mengakses Sertifikat Elektronik miliknya;
3. Informasi apapun dalam sertifikat menjadi tidak valid;
4. Terdapat perubahan data identitas pada Sertifikat Elektronik;
5. Pemilik Sertifikat Elektronik sudah tidak berhak menggunakan Sertifikat Elektronik karena tidak lagi memiliki kewenangan;
6. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Kepemilikan;
7. Instansi dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Kerja Sama;
8. Pemilik atau instansi meminta sertifikatnya dicabut.
9. BSrE CA telah berhenti beroperasi;
10. Pemilik sudah tidak bisa lagi menggunakan

BSrE CA revokes Certificates if at least one of the following conditions occurs:

1. The Subscriber has evidence that intentionally or unintentionally his Private Key has been lost, stolen, known, or misused by another party;
2. The Subscriber still has Certificate and private key but does not remember the passphrase to access his Certificate;
3. Any information in the certificate becomes invalid
4. There is identity data change in the Certificate;
5. The Subscriber is no longer entitled to use the Certificate because he has no authority;
6. The Subscriber can be shown to have violated the stipulations of its Subscriber Agreement.
7. The Government Institution can be shown to have violated the stipulations of its Cooperation Agreement.
8. The Subscriber or Government Institution asks for his/her certificate to be revoked.
9. BSrE CA operation is terminated;
10. The Subscriber cannot use the certificate (eg death).

sertifikat (semisal: meninggal).

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

Information about the reason for the Certificate revocation is included in the CRL and/or OCSP responder. The revoked Certificate is included in all new publications about Certificate status information until the Certificate expires.

4.9.2 Pihak yang Dapat Meminta Pencabutan / Entities can Request Revocation

Permintaan pencabutan sertifikat dapat dilakukan oleh:
1. Pemilik;
2. Organisasi yang berafiliasi dengan pemilik;
3. Aparat penegak hukum; dan
4. Penasihat hukum.

Certificate revocation is requested by:
1. Subscriber;
2. Organization affiliated with the Subscriber;
3. Law enforcement officials; and
4. Lawyer.

4.9.3 Proses Permintaan Pencabutan Sertifikat Elektronik / Process for Revocation Request

BSrE CA memverifikasi identitas individu dan organisasi yang meminta pencabutan sertifikat. Validasi identitas yang meminta pencabutan dibutuhkan sesuai dengan bagian 3.4.

BSrE CA verifies the identity of the individual and organization requesting certificate revocation. Identity validation for requesting certificate revocation is required according to section 3.4.

Permintaan pencabutan sertifikat oleh entitas lain melampirkan bukti bahwa:
1. Kunci privat sertifikat telah terungkap, atau
2. Penggunaan sertifikat tersebut tidak sesuai dengan CPS atau
3. Terdapat alasan relevan lain yang diberikan oleh pemilik.

Certificate revocation request by an authorized representative, attach evidence that:
1. The certificate's private key has been compromised, or
2. The use of such certificates is not CPS compliant or
3. There are other relevant reasons given by the Subscriber.

Permintaan pencabutan sertifikat oleh pihak yang berwenang lainnya harus menyerahkan bukti bahwa:
1. Kunci Privat Sertifikat telah terungkap;
2. Penggunaan Sertifikat tidak sesuai dengan CP/CPS; dan
3. Pemilik sudah tidak terasosiasi dengan institusi yang bersangkutan.

Requests for certificate revocation by other entity is enclosed with evidence that:
1. The Private Key of the Certificate has been exposed;
2. The use of the Certificate does not conform to the CP/CPS; and
3. The Subscriber is no longer associated with the institution concerned.

Proses permintaan pencabutan Sertifikat dijelaskan lebih rinci dalam prosedur.

The steps involved in the process of requesting a Certification revocation detail in the procedure.

4.9.4 Masa tenggang permintaan pencabutan Sertifikat Elektronik / Revocation Request Grace Priod

Tidak ada tenggang waktu yang diizinkan setelah permintaan pencabutan diverifikasi. BSrE memproses pencabutan sertifikat segera setelah melakukan verifikasi permohonan pencabutan.

No grace period is permitted once a revocation request has been verified. BSrE CA will proceed to certificate revocation immediately after verifying the revocation request.

4.9.5 Jangka Waktu BSrE CA Memproses Permintaan Pencabutan / Time Within Which BSrE CA Must Process the Revocation Request

BSrE CA melakukan upaya terbaik untuk memproses permintaan pencabutan Sertifikat dalam waktu 3 (tiga) hari kerja setelah permohonan pencabutan yang valid diterima.

Root CA makes the best efforts to process revocation requests within 3 (three) business days after a valid revocation request is received

4.9.6 Pemeriksaan Keberlakukan Sertifikat Elektronik oleh Pengandal/ Revocation Checking Requirement for Relying Parties

Pengandal memvalidasi CRL dan/atau OCSP

Relying Parties validate Certificates BSrE CA's

milik BsrE CA dengan ketentuan sebagai berikut:

1. Pemeriksaan CRL dapat dilakukan 1x24 jam setelah proses pencabutan dilakukan; dan/atau
2. Pemeriksaan OCSP dapat dilakukan 1 jam setelah proses pencabutan dilakukan.

CRL and/or OCSP with the following :

1. CRL verification is performed within 24 hours after revocation; and/or;
2. OCSP verification is performed within 1 hour after revocation.

4.9.7 Frekuensi Penerbitan CRL / CRL Issuance Frequency

CRL harus diperbarui dan dipublikasikan:

1. Untuk sertifikat Pemilik, minimal sekali dalam 24 (dua puluh empat) jam.
2. Dalam kasus kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat BSrE CA, CRL terbaru dipublikasi dalam waktu maksimal 24 (dua puluh empat) jam semenjak stempel waktu (timestamp) pencabutan.
3. Untuk pencabutan Sertifikat Pemilik, waktu nextUpdate pada CRL BSrE CA paling lambat 48 (empat puluh delapan) jam setelah waktu penerbitan (*this Update time*). BSrE CA menjamin integritas CRL.

The CRL should be updated and published:

1. For Subscriber Certificate, minimum once in 24 hours.
2. In case of secret key exposure or of any other important security compromise incident, for example a BSrE CA revocation, an updated Certificate Revocation List must be published within 24 hours from the revocation timestamp.
3. For revocation of the Subscriber certificate, the value for nextUpdate field in BSrE CA's CRL is no later than 48 (forty eight) hours after the issuance time (this Update time). BSrE CA ensures the integrity of the CRL.

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

BSrE CA mempublikasikan CRL dalam waktu 30 (tiga puluh) menit setelah penerbitan.

BSrE CA publishes the CRL within 30 (thirty) minutes after issuance.

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

BSrE CA menyediakan layanan validasi daring menggunakan protokol OCSP.

BSrE CA provides online validation services using the OCSP protocol.

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

BSrE CA mengimplementasikan OCSP sesuai dengan standar IETF RFC 6960 yang dapat diakses di repository BSrE CA.

BSrE CA implements OCSP in accordance with the IETF RFC 6960 standard, which can be accessed in the BSrE CA repository.

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

Tidak ada ketentuan.

No stipulation.

4.9.12 Persyaratan Khusus Re-key apabila *compromise* / Special Requirements Re-Key Compromise

Jika Kunci Privat BSrE CA terkompromi, maka seluruh Sertifikat Elektronik yang telah diterbitkan oleh BSrE CA dicabut.

If BSrE CA's Private Key is compromised, then all Certificates that have been issued by the BSrE CA are revoked.

4.9.13 Keadaan untuk Pembekuan / Circumstances for Suspension

Tidak ada ketentuan.

No stipulation.

4.9.14 Siapa yang Dapat Meminta Pembekuan / Who can Request Suspension

Tidak ada ketentuan.

No stipulation.

4.9.15 Prosedur Permintaan Pembekuan / Procedure for Suspension Request

Tidak ada ketentuan.

No stipulation.

4.9.16 Batas Waktu Pembekuan / Limits on Suspension Period

Tidak ada ketentuan.

No stipulation.

4.10 Layanan Status Sertifikat / Certificate Status Services

4.10.1 Karakteristik Operasional / Operational Characteristics

Status keberlakuan Sertifikat Elektronik dapat diketahui berdasarkan informasi pada CRL dan/atau melalui OCSP.	The validity status of Certificates can be determined based on information on the CRL and/or through the OCSP.

4.10.2 Ketersediaan Layanan / Service Availability

BSrE CA melakukan semua tindakan yang diperlukan untuk ketersediaan layanan validasi status sertifikat.	BSrE CA takes all necessary measures to ensure the availability of the certificate status validation service.

4.10.3 Fitur Pilihan / Optional Features

Tidak ada ketentuan.	No stipulation.

4.11 Akhir Berlangganan / End of Subscription

Kepemilikan Sertifikat Elektronik oleh Pemilik Sertifikat Elektronik berakhir jika masa berlaku Sertifikat Elektronik tersebut telah habis atau jika Sertifikat Elektronik tersebut telah dicabut.	Ownership of an Certificate by Subscriber ends if the validity period of the Certificate has expired or has been revoked.
Pemilik dapat mengakhiri langganan dengan membiarkan sertifikatnya kedaluwarsa atau mencabut sertifikatnya tanpa meminta sertifikat yang baru.	Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12 Pemulihan dan Eskro Kunci / Key Escrow and Recovery

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

Kunci Privat BSrE CA dan pemilik tidak dieskrokan kepada pihak lain.	BSrE CA's and subscriber's Private Key is not escrowed to other parties.

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

Tidak ada ketentuan.	No stipulation.

BAB V
KENDALI FASILITAS, PENGELOLAAN DAN OPERASIONAL / FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Kendali Fisik / Physical Controls

5.1.1 Lokasi dan Konstruksi / Site Location and Contruction

Lokasi dan konstruksi bangunan yang menyimpan perangkat-perangkat sistem BSrE CA, berikut dengan perangkat-perangkat komputer untuk manajemen/ pengelolaan BSrE CA secara jarak jauh (*remote*), memenuhi kriteria sebagai tempat yang menyimpan informasi yang bernilai tinggi dan/atau informasi yang sangat sensitif.

The location and construction of the building that stores the BSrE CA system devices, along with computer devices for remote management of the BSrE CA, meet the criteria as a place that stores high-value and/or highly sensitive information.

Perangkat-perangkat komputer server tersimpan di dalam DC utama dan DRC dengan kondisi aktif secara bersamaan. BSrE melakukan identifikasi terhadap risiko yang muncul pada pengelolaan DC dan DRC untuk memitigasi kemungkinan dan/atau dampak yang terjadi agar layanan BSrE berjalan. Upaya mitigasi dilakukan dengan memastikan adanya perlindungan yang kuat terhadap upaya-upaya akses secara tidak sah pada setiap perangkat sistem BSrE CA dan informasi yang tersimpan di dalamnya (misal, menerapkan mekanisme penjagaan fisik, sensor untuk mendeteksi upaya penyusupan, dsb).

Computer devices are stored in the main DC and DRC with conditions being active simultaneously. BSrE identifies the risks that arise in the management of DC and DRC to mitigate the possibility and/or impact to keep BSrE services running. These mitigation efforts are carried out by ensuring strong protection against unauthorized access to each BSrE CA system device and the information stored therein (e.g. implementing physical guarding mechanisms, sensors to detect intrusion attempts, etc.).

5.1.2 Akses fisik / Physical Access

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

1. Memastikan tidak ada akses tidak resmi ke perangkat keras
2. Menyimpan semua removable media yang berisi informasi teks yang sensitif dalam tempat penyimpanan yang aman.
3. Memonitor akses yang tidak berwenang baik secara manual maupun elektronik.
4. Memelihara dan memeriksa log akses secara berkala.

BSrE CA equipment is always protected from unauthorized access. The physical security mechanisms for BSrE CA has been implemented to:

1. Ensure no unauthorized access to the hardware;
2. Store all removable media that contain sensitive plain-text information in secure containers;
3. Monitor unauthorized access, either manually or electronically;
4. Maintain and periodically inspect the access log.

Semua operasional BSrE yang sangat penting dan memiliki resiko tinggi harus dilakukan di dalam fasilitas yang aman dengan setidaknya memiliki empat lapis keamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif. Fasilitas tersebut harus terpisah secara fisik dari fasilitas organisasi yang lain, sehingga fasilitas tersebut membutuhkan kendali akses fisik dua orang untuk modul kriptografis dan sistem komputer BSrE.

All critical and high-risk BSrE operations must be conducted in a secure facility with at least four layers of security to access sensitive hardware and software. The facility must be physically segregated from the rest of the organization's facilities, requiring two-person physical access control for cryptographic modules and BSrE computer systems.

Modul kriptografis yang *removable* dinonaktifkan sebelum disimpan. Ketika tidak

Removable cryptographic modules are disabled before storage. When not in use,

digunakan, modul kriptografis yang *removable*, informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografis ditempatkan pada tempat penyimpanan yang aman. Data untuk aktivasi dihafal atau dicatat dan disimpan dengan pengamanan yang setara dengan pengamanan yang disediakan modul kriptografis, dan tidak boleh disimpan bersamaan dengan modul kriptografis.

removable cryptographic modules, the activation information used to access or activate the cryptographic module is placed in secure storage. Data for activation is memorized or logged and stored with security equivalent to that provided by the cryptographic module, and should not be stored with the cryptographic module.

Proses pemeriksaan keamanan fasilitas penyimpanan perangkat BSrE CA dilaksanakan jika fasilitas akan ditinggalkan tanpa adanya pengawasan. Setidaknya, proses pemeriksaan memverifikasi hal-hal berikut:

1. Semua *security container* (misal: lemari besi) sudah diamankan (dikunci);
2. Perangkat pemantauan terhadap fasilitas penyimpanan perangkat BSrE CA dipastikan selalu beroperasi dengan baik;
3. Sistem keamanan fisik (misalnya kunci pintu, pelindung ventilasi) berfungsi dengan baik; dan
4. Area diamankan dari akses yang tidak berhak.

The BSrE CA device storage facility security check process is performed if the facility is to be left unattended. At a minimum, the vetting process verifies the following:

1. All security containers (e.g. vaults) are secured (locked);
2. Monitoring devices for the BSrE CA device storage facility are in good working order;
3. Physical security systems (e.g. door locks, ventilation guards) are functioning properly; and
4. Areas are secured from unauthorized access.

BSrE CA menunjuk satu atau beberapa personel yang berperan dan bertanggung jawab untuk melakukan pemeriksaan tersebut. Pemeriksaan tersebut dibuktikan dengan log yang dapat dipertanggungjawabkan. Jika fasilitas tidak ditempati setiap waktu, maka orang terakhir yang meninggalkan fasilitas membuat lembaran *sign-out* yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

The BSrE CA designates one or more personnel whose role and responsibility it is to conduct such checks. The inspection is evidenced by an accountable log. If the facility is not occupied at any time, the last person to leave the facility creates a sign-out sheet indicating the date and time, and certifying that all physical protection mechanisms are in place and active.

5.1.3 Daya dan Penyejuk Udara / Power and Air Conditioning

Fasilitas perangkat sistem BSrE CA dilengkapi perangkat pendukung yaitu pembangkit listrik yang menjamin ketersediaan listrik dan sistem pendingin udara yang mengontrol suhu dan kelembaban.

BSrE CA system facility is equipped with supporting devices, specifically power plants that guarantees the availability of electricity and an air conditioning system that controls temperature and humidity.

BSrE CA memiliki cadangan listrik yang cukup agar dapat menyelesaikan aktivitas proses sertifikasi elektronik, mencatat keadaan/status terakhir dari perangkat-perangkat yang aktif, sebelum terjadinya pemutusan daya listrik yang menyebabkan sistem non-aktif/mati. Komponen perangkat sistem BSrE CA yang kritikal (misal: *Certificate Validation System*) dilengkapi dengan sumber daya listrik yang tidak terganggu dan dapat beroperasi minimal selama 6 (enam) jam tanpa adanya sumber listrik utama agar layanan kritikal dapat selalu tersedia.

BSrE CA has sufficient electricity backup to complete the electronic certification process activities, record the state/last status of active devices, before the power cut occurs which causes the system deactivate/shut down. Critical components of the BSrE CA system (ex: Certificate Validation System) are equipped with an uninterrupted power source for a minimum of 6 (six) hours without a main power source, in order to critical services are always available.

5.1.4 Keterpaparan Air / Water Exposures

BSrE CA menempatkan perangkat sistem pada tempat yang tidak terpapar air.

BSrE CA places system devices in facilities that are not exposed to water.

5.1.5 Pencegahan dan Perlindungan dari Kebakaran / Fire Preventation and Protection

BSrE CA menempatkan perangkat sistem di fasilitas dengan sistem deteksi kebakaran dan sistem pemadaman kebakaran yang memadai.

BSrE CA places system devices in facilities with adequate fire detection systems and fire suppression systems.

5.1.6 Media Penyimpanan / Media Storage

Media penyimpanan yang digunakan oleh BSrE CA terlindungi dari kerusakan akibat kecelakaan (misal: air, api, elektromagnetik, dsb). Media penyimpanan yang tidak berkaitan secara langsung dengan proses sertifikasi elektronik (misal: rekaman untuk audit, arsip, atau informasi cadangan) tersimpan pada lokasi yang terpisah dari lokasi utama. Media penyimpanan yang berisi Kunci Privat milik BSrE CA dikelola dan disimpan dalam fasilitas penyimpanan yang aman dan dilengkapi kendali akses baik fisik maupun logik untuk membatasi akses terhadap personil yang tidak berwenang.

Media storages that are used by BSrE CA is protected from accidental damage (eg water, fire, electromagnetic, etc). Media storages that are not directly related to the electronic certification process (ex: records for audits, archives, or backup information) are stored in a location separate from the main location. Media storages that contain BSrE CA's Private Keys are managed and saved in a secure storage facilities and equipped with both physical and logical access controls to limit access from unauthorized personnel.

5.1.7 Pembuangan Limbah / Waste Disposal

BSrE CA memastikan setiap dokumen dan material yang bersifat sensitif dihancurkan sebelum dibuang. Media yang digunakan untuk mengumpulkan dan membawa informasi sensitif diubah sampai informasi tersebut tidak dapat dibaca sebelum dibuang. Sebelum dibuang, materiil dan peralatan kriptografi dihancurkan secara fisik atau di-*zeroized* (dikosongkan). Limbah selain yang disebutkan di atas, dibuang sesuai dengan persyaratan pembuangan limbah normal. Tata cara pembuangan limbah diatur lebih rinci di prosedur mengenai pemusnahan Barang Milik Negara (BMN).

BSrE CA ensures that all sensitive documents and materials are destroyed before being disposed. The media that are used to collect and contain sensitive information is altered until the information is unreadable before being disposed. Before disposal, cryptographic material and equipment is physically destroyed or zeroized (emptied). Other waste except that mentioned above, disposed of in accordance with normal waste disposal requirements. The procedures for waste disposal are regulated in the procedures regarding the destruction of BMN.

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

BSrE CA melakukan *Backup off-site* dan hasil *backup off-site* tersebut disimpan di luar lokasi DC dan DRC secara berkala sesuai dengan penilaian risiko BSrE CA.

BSrE CAs perform off-site backups and their results be stored in a location outside of the DC and DRC periodically in accordance with the CAs' risk assessment.

BSrE CA menyimpan 1 (satu) set *backup* lengkap terkini di lokasi *off-site* dan dilindungi dengan pengamanan fisik serta prosedur yang setara dengan pengamanan pada operasional BSrE CA

BSrE CAs be stored 1 (one) set of full-backup an off-site location and be protected with physical and procedural controls commensurate to that of the operational of BSrE CA.

5.2 Kendali Prosedur / Procedural Controls

5.2.1 Peran Tepercaya / Trusted Roles

BSrE CA memiliki daftar dan catatan tentang personil yang bertugas sebagai Peran

BSrE CA has a list and records of personnel as Trusted Roles, which includes names,

Tepercaya, yang mencakup nama, informasi kontak, dan informasi lainnya yang diperlukan.
Peran Tepercaya PBSrE CA meliputi:

1. PA
   Pembuatan, revisi dan persetujuan CPS.
2. Staff PA
   Membantu PA dalam menyiapkan dokumen CPS.
3. Ketua Tim Operasional BSrE
   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan BSrE CA.
4. Administrator CA
   Melakukan operasional dan *maintenance* aplikasi manajemen BSrE CA.
5. Administrator VA
   Melakukan validasi aplikasi manajemen BSrE CA.
6. *DevOps Engineer*
   Melakukan operasional dan *maintenance* terkait DevOps di BSrE.
7. Administrator HSM
   Melakukan Operasional dan *maintenance* HSM BSrE CA.
8. *Network Engineer*
   Melakukan operasional dan *maintenance* jaringan sistem sertifikasi elektronik.
9. *Database & Log Engineer*
   Melakukan operasional, *maintenance* data, dan sinkronasinya antar *data center*.
10. RA
    Identifikasi dan Validasi identitas permohonan permintaan sertifikat.
11. Staff RA
    Membantu RA dalam menyiapkan dokumen identifikasi dan validasi identitas.
12. *Developer*
    Bertanggung jawab dalam mengembangkan aplikasi dan melakukan integrasi terkait dengan sistem PSrE.
13. *Security Engineer*
    Bertanggung jawab dalam keamanan *logic* operasional sistem BSrE CA
14. *Repository*
    Bertanggung jawab terhadap konten yang dipublikasikan pada repositori.
15. *Key Custodian*
    Mengelola penyimpanan dan pengamanan kunci.
16. *Internal Audit*
    Melakukan audit internal operasional BSrE CA.

Penjelasan lebih detil dapat dilihat pada dokumen *trusted role.*

contact information and other necessary information.
BSrE CA's Trusted roles includes :

1. PA
   Creation, revision, and approval of CPS
2. PA staff
   Assist PA in preparing CPS documents.
3. BSrE CA Operational Team Leader
   Overall responsibility for managing all BSrE CA security practices.
4. CA Administrator
   Conduct operasional and maintenance of CA management application.
5. VA Administrator
   Conduct validation of CA management application.
6. Devops Engineer
   Conduct operasional and maintenance related to DevOps at BSrE CA.
7. HSM Administrator
   Conduct operasional and maintenance related to HSM BSrE CA.
8. Network Engineer
   Conduct operasional and maintenance related to electronic certification system network.
9. Database & Log Engineer
   Conduct operasional, data maintenance and sinchronization between data centers.
10. RA
    Identification and validation of certificate application.
11. RA staff
    Assist RA in preparing identification and identity validation documents.
12. Developer
    Responsible for developing applications and performing integrations related to the PSrE systems.
13. Security Engineer
    Responsible for the security of the operational logic of the BSrE CA system.
14. Repository
    Responsible for the content published on the repository.
15. Key Custodian
    Manage storage and security of the keys .
16. Internal Auditor
    Conduct internal audits of BSrE CA operations.

More explanation about Trusted Role is detailed in the Trusted Role document.

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

Untuk kegiatan yang memerlukan kendali multi-pihak, semua partisipan harus memegang peran Tepercaya. Kendali multi-

Where multi-personnel control is required, all participants hold a trusted role. Multi-personnel control does not involve personnel

pihak tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan minimal tiga orang atau lebih:

1. Pembangkitan kunci BSrE CA
2. Pencabutan Sertifikat BSrE CA
3. Penandatanganan kunci BSrE CA
4. Pencadangan kunci privat BSrE CA
5. Penanganan perangkat keras kriptografi (pemasangan, pelepasan, pemeliharaan, pembongkaran dan penghapusan, serta *troubleshooting*)

that serve in an Auditor role. The following tasks require two or more persons:

1. BSrE CA key generation;
2. BSrE CA certificate revocation;
3. BSrE CA key signing;
4. BSrE Private Key backup;
5. Handling cryptographic hardware (installation, removal, maintenance, disassembly and disposal, and troubleshooting)

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

Semua individu yang ditugaskan dalam Peran Tepercaya akan menerima Surat Perintah. Autentikasi Peran Tepercaya dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi tersebut dilakukan berdasarkan identifikasi orang yang mengakses ruangan atau sistem dan hak akses yang diatur sesuai dengan peran dan tanggung jawab orang tersebut.

All individuals assigned to a Trusted Role will receive an Assignment Letter. Trusted Role Authentication is performed through physical access control and system-level access control. The authentication is based on the identification of the person accessing the room or system and the access rights are set according to the person's roles and responsibilities.

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

BSrE CA menerapkan pemisahan tugas baik berdasarkan perangkat BSrE CA, secara prosedural, maupun keduanya. Satu orang tidak boleh merangkap peran pada peran-peran berikut:

1. PA dan administrator operasional;
2. Auditor internal dan semua peran lain;
3. Pengembang aplikasi dan semua peran lain.

BSrE CA implements separation of duties based on BSrE CA's equipmet, procedures, or both. One person may not have multiple roles in the following roles:

1. PA and Operational Administrator;
2. Internal Auditor and all other roles;
3. Developer and all other roles.

5.3 Kendali Personel / Personnel Controls

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

Personil yang bertugas sebagai Peran Tepercaya adalah pegawai BSrE CA yang memiliki latar belakang, kualifikasi serta pengalaman dalam bidang keamanan informasi.

Personnel as Trusted Roles are BSrE CA employees who have backgrounds, qualifications and experience in the field of information security.

5.3.2 Prosedur Pemeriksaan Latar Belakang / Background Check Procedures

Semua personil di BSrE CA telah menyelesaikan pemeriksaan latar belakang sesuai dengan aturan kepegawaian di lingkungan pemerintah. Lingkup pemeriksaan latar belakang yang berlaku dalam 5 (lima) tahun terakhir.

All BSrE CA personnel have completed a background check consistent with Government Employment Regulations. The scope of the background check include the following areas covering in the past 5 (five) years.

5.3.3 Persyaratan Pelatihan / Training Requirements

BSrE CA menjamin bahwa seluruh personil telah mendapatkan pelatihan yang dibutuhkan. Pelatihan tersebut meliputi 3 (tiga) hal yaitu: keamanan informasi, teknis operasional dan teknis prosedural. Pelatihan tersebut mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras,

BSrE CA ensures that all personnel have received the required training. Such training will address relevant topics, such as: information security, operational techniques and procedural techniques. It should cover the minimum operations of the Indonesian IKP (including management of CA hardware,

perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil PSrE dilakukan minimal 1 (satu) kali dalam setahun.

software and operating system), operational procedures and security, CP and applicable CPS. An evaluation of the adequacy of the competence of PSrE personnel is carried out at least once a year.

5.3.4 Frekuensi dan Persyaratan Pelatihan Ulang / Retraining Frequency and Requirements

Personil yang bertugas sebagai Peran Tepercaya dalam BSrE CA akan selalu mendapatkan informasi terbaru tentang operasional BSrE CA. Setiap perubahan siginifikan terhadap operasional akan diikuti oleh program pelatihan yang terkait serta didokumentasikan dengan baik. BSrE akan mengevaluasi dan memperbaharui program pelatihannya minimal 1 (satu) tahun sekali.

Personnel as Trusted Roles in BSrE CA will always get the latest information about BSrE CA operations. Any significant changes to operations will be followed by a related and well-documented training program. BSrE will evaluate and update its training program at least 1 (one) time a year.

5.3.5 Frekuensi dan Urutan Rotasi Pekerjaan / Job Rotation Frequency Sequence

BSrE CA memastikan bahwa perubahan pegawai tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem.

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

5.3.6 Sanksi untuk Tindakan Tidak Terotorisasi / Sanctions for Unauthorized Actions

BSrE CA akan mengambil tindakan tegas dan sanksi yang jelas berupa hukuman administratif dan disiplin bagi personil yang melakukan aksi melanggar ketentuan dan kebijakan di dalam CPS atau prosedur operasional BSrE CA.

BSrE CA will take firm action and clear sanctions in the form of administrative and disciplinary to personnel violating provisions and policies within CPS, or BSrE CA operational procedures.

5.3.7 Persyaratan Kontraktor Independen / Independent Contractor Requirements

Apabila terdapat penyedia pihak ketiga/kontraktor yang terlibat dalam fungsi BSrE CA akan dikenakan aturan yang sama dengan personil BSSN sesuai 5.3.2.

If any third party provider/contractor involved in the BSrE CA function, it will be subject to the same rules as BSSN personnel according to 5.3.2.

5.3.8 Dokumentasi yang diberikan kepada Personil / Documentations Supplied to Personnel

BSrE CA menjamin ketersediaan dokumen CPS dan dokumen lain yang terkait dengan penyelenggaraan BSrE CA bagi personil-personilnya yang terlibat dalam operasional BSrE CA.

BSrE CA ensures the availability of CPS documents and other documents related to the implementation of BSrE CA for its personnel who are involved in BSrE CA operations.

BSrE CA menyediakan repositori internal yang memuat seluruh dokumen yang diperlukan oleh para personil untuk menunjang tugas dan kewajibannya.

The BSrE CA provides an internal repository that contains all documents required by personnel to support their duties and obligations.

5.4 Prosedur Log Audit / Audit Logging Procedures

BSrE CA membuat berkas *log audit* untuk semua kejadian yang terkait dengan keamanan BSrE CA, VA, dan RA. *Log audit* keamanan dikumpulkan secara manual serta dapat menggunakan buku *log*, kertas formulir, atau mekanisme fisik lain. Semua *log audit* keamanan, elektronik dan non elektronik, disimpan dan tersedia selama audit kepatuhan. *Log audit* keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan dalam bagian ini dipelihara sesuai dengan bagian 5.5.2.

The BSrE CA maintains audit log files for all events related to the security of the BSrE CA, VA, and RA. Security audit logs are collected manually and may use log books, paper forms, or other physical mechanisms. All security audit logs, electronic and non-electronic, are retained and made available during compliance audits. Security audit logs for each auditable event defined in this section are maintained in accordance with section 5.5.2.

5.4.1 Jenis Kejadian yang Direkam / Types of Events Recorded

BSrE CA mengaktifkan semua fitur audit keamanan dari sistem operasi BSrE CA dan RA, serta aplikasi BSrE CA, VA, dan RA yang dipersyaratkan oleh CPS ini. BSrE CA memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat dicatat dalam log sehingga setiap tindakan peran terpecaya dalam operasional BSrE CA dapat dilacak.

BSrE CA enables all security audit features of the BSrE CA and RA operating systems, as well as the BSrE CA, VA, and RA applications required by this CPS. BSrE CA should ensure all events relating to the lifecycle of certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for BSrE CA operations.

Setiap *record* audit minimal memuat poin-poin sebagai berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian yang dapat diaudit):

1. Jenis kejadian,
2. Nomor seri atau urutan rekaman,
3. Tanggal dan waktu terjadi rekaman,
4. Sumber perekaman,
5. Indikator sukses atau gagal yang sesuai,
6. Identitas dari entitas dan/atau operator yang menyebabkan kejadian tersebut

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

1. The type of event;
2. Serial or sequence number of entry;
3. The date and time the event occurred;
4. Source of entry;
5. Success or failure where appropriate;
6. The identity of the entity and/or operator that caused the event.

Waktu diselaraskan memakai Network Time Protocol (NTP) untuk fasilitas yang terkoneksi dengan internet. Penyelerasan waktu dilakukan dengan tingkat ketelitian 1 menit.

Time is synchronized using NTP for internet-connected facilities. Time synchronization is performed with a precision level of 1 minute

5.4.2 Frekuensi pemrosesan *log* / Frequency of Processing Log

BSrE CA memastikan bahwa *audit log* diperiksa minimal 1 (satu) kali setiap bulan. BSrE CA menindaklanjuti setiap aktivitas yang mencurigakan atau tidak biasa berdasarkan insiden dalam sistem BSrE CA.

BSrE CA ensures that audit logs were reviewed at least monthly. BSrE CA follows up on any suspicious or unusual activity based on incidents in the BSrE CA system.

5.4.3 Masa Retensi untuk *Audit Log* / Retention Period for Audit Log

BSrE CA menyimpan seluruh *audit log* dari sistem BSrE CA yang dihasilkan secara elektronik maupun yang dibuat manual untuk jangka waktu tidak kurang dari 12 (dua belas) bulan sejak *audit log* tersebut dibuat. Jangka waktu ini dapat berubah sesuai dengan ketentuan yang berlaku.

BSrE CA keeps all audit logs from the BSrE CA system that are generated electronically or manually for a period at least 12 (twelve) months since the audit log was created. This time period may change according to applicable regulations.

5.4.4 Perlindungan terhadap audit log / Protection of Audit Log

BSrE CA melindungi dengan sistem *audit log* elektronik dari pihak-pihak yang tidak berhak melihat, memodifikasi, menghapus atau gangguan lainnya.

BSrE CA protects the electronic log audit systems from parties who have no rights to view, modify, delete or tampering.

5.4.5 Prosedur pembuatan audit log cadangan (*backup*) / Audit Log Backup Procedures

BSrE CA mem-backup seluruh *log* sedikitnya sebulan sekali. Media backup disimpan dan diamankan di tempat terpisah.

BSrE CA backs up all logs at least once a month. Backup media is stored and secured in a separate place.

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

Sistem pengumpulan *log audit* dilakukan sejak sistem berjalan dan dimonitor secara internal

The audit log collection system has been done since the system up and running and

BSrE CA.

monitored internally by BSrE CA.

5.4.7 Notifikasi kepada Subjek Penyebab Kejadian / Notification to Event-Causing Subject

Tidak ditentukan.

No stipulation.

5.4.8 Penilaian kerentanan / Vulnerability Assessments

BSrE CA melakukan penilaian kerentanan (*vulnerability assessment*) secara rutin terhadap kendali keamanan yang telah dibuat oleh BSrE CA minimal 1 (satu) kali dalam 6 (enam) bulan atau ketika terjadi perubahan signifikan pada sistem BSrE CA. Jika terdapat temuan pada saat asesmen kerentanan, BSrE CA akan memastikan bahwa kerentanan valid dan memperbaiki kerentanan tersebut.

BSrE CA conducts periodically vulnerability assessments of security controls that have implemented by BSrE CA at least 1 (one) time in 6 (six) months or when significant changes occur to the BSrE CA system. If a finding is made during a vulnerability assessment, the BSrE CA will confirm that the vulnerability is valid and then fix the vulnerability.

5.5 Pengarsipan Record / Records Archival

5.5.1 Tipe Record yang Diarsipkan / Types of Records Archived

BSrE CA mengimplementasikan metode pencadangan untuk operasional BSrE CA yang terletak di Pusat Data. Minimal, data berikut disimpan pada arsip:

1. Siklus hidup sertifikat termasuk di dalamnya permohonan penerbitan, pembaruan, *re-key*, serta pencabutan sertifikat;
2. Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh BSrE CA;
3. Data konfigurasi sistem BSrE CA;
4. Dokumen CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.
5. Data Audit;
6. Data pendukung Sistem Manajemen Keamanan Informasi (SMKI):
   a. Penunjukan dan pencabutan peran dan kewenangan;
   b. Akses pengunjung ke fasilitas BSrE CA;
   c. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak system;
   d. Deteksi dan tindakan terhadap insiden keamanan;
   e. Latihan keadaan darurat;
   f. Tindakan dan penilaian risiko;
   g. Perubahan asset, prosedur, dan tanggung jawab; dan
   h. Perubahan dokumentasi.

BSrE CA implements a backup method for BSrE CA operations which is located at the Data Center. At a minimum, the following data is stored in the archive:

1. Certificate life cycle operations including certificate issuance request, renewal, re-key, and certificate revocation;
2. All certificates and CRLs as issued or published by the BSrE CA;
3. BSrE CA system configuration data;
4. Applicable CPS document, including modifications and amendments to the document;
5. Audit Data;
6. Supporting data for the Information Security Management System (ISMS):
   a. Designation and revocation of roles and authorities;
   b. Visitor access to BSrE CA facilities
   c. System hardware and software changes and maintenance;
   d. Detection and response to security incidents;
   e. Emergency drills;
   f. Risk measures and assessments;
   g. Changes to assets, procedures, and responsibilities; and
   h. Changes to documentation.

5.5.2 Periode Retensi Arsip / Retention Period for Archive

BSrE CA menyimpan catatan arsip mengenai kepemilikan Sertifikat Elektronik selama minimal 5 (lima) tahun. Media yang dibutuhkan untuk membaca arsip ini dipelihara selama masa retensi.

BSrE CA maintains archival records regarding the subscribership of Certificates for at least 5 (five) years. The media required to read this archive is maintained during the retention period.

5.5.3 Pelindungan Arsip / Protection of Archive

BSrE CA melindungi dokumen arsip sehingga

BSrE CA protects archived documents so that

hanya pihak-pihak sebagaimana tercantum dalam kebijakan privasi yang dapat memperoleh akses terhadap arsip tersebut. Setiap dokumen arsip dilindungi dari upaya pembacaan, pengubahan, atau penghapusan secara tidak sah dan upaya perusakan lainnya. Media penyimpanan dokumen arsip dan aplikasi yang diperlukan untuk memproses dokumen arsip dikelola untuk memastikan bahwa dokumen arsip tersebut dapat diakses selama masa retensi arsip yang telah ditentukan. Muatan arsip tidak diungkap kecuali berdasarkan ketentuan pada Bagian 9.3 dan 9.4.

only parties listed in the privacy policy can access them. Each archived documents are protected against unauthorized viewing, modification, deletion, or tampering. The media holding the archive documents and the applications required to process the archive documents are managed to ensure that the archivedl documents can be accessed during the specified archival retention period. The contents of the archive are not disclosed except in accordance with the provisions of Sections 9.3 and 9.4.

5.5.4 Prosedur Backup Arsip / Archive Backup Procedures

Tidak ada ketentuan.

No stipulation.

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

Rekaman arsip BSrE CA diberi stempel waktu (timestamp) ketika mereka dibuat.

BSrE CA archive records are time-stamped as they are created.

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

Sistem pengumpul arsip BSrE CA merupakan sistem internal, kecuali arsip RA yang berada diluar BSrE.

Archive Collection System is conducted by BSrE CA internally, except RA archives that are outside of BSrE CA.

5.5.7 Prosedur untuk Mendapatkan dan Memeriksa Informasi Arsip / Procedures to Obtain and Verify Archive Information

Penyimpanan media untuk informasi arsip BSrE CA diperiksa saat pembuatan. Sampel informasi yang diarsipkan diuji minimal sekali dalam setahun untuk memeriksa integritas dan keterbacaan informasinya.

Media storing of BSrE CA archive information is checked upon creation. The samples of archived information are tested at least once a year to check the integrity and readability of the information.

Hanya pihak atau personil yang memiliki kewenangan yang dapat memperoleh akses ke suatu arsip. Integritas (keutuhan) informasi harus diperiksa kembali setelah arsip tersebut dikembalikan oleh personil yang telah mengakses dokumen arsip tersebut. Permintaan untuk mendapatkan dan memverifikasi informasi arsip dikoordinasikan oleh Ketua Tim Operasional.

Only authorised personnel are allowed to access the archive. The integrity of information must be checked again after the archive is returned by personnel who have accessed the archive document. Requests to obtain and verify archive information are coordinated by The Operation Team Leader.

5.6 Pergantian kunci/ Key Changeover

Untuk meminimalisir risiko terhadap bocornya Kunci Privat BSrE CA, kunci privat diubah secara berkala. Kunci tersebut diganti dengan kunci baru yang digunakan untuk penanda tangan Sertifikat. BSrE CA melakukan pemberitahuan kepada Pemilik Sertifikat dan Pengandal dalam hal terjadi penggantian kunci baru BSrE CA tersebut.

To minimize risk from compromise of a BSrE CA's private signing key, the private key is changed periodically. The key replaced with the new key used for the Certificate signer. BSrE CA will make a notification to the Certificate Subscriber and Relying Parties if there is a replacement of the new BSrE CA key.

Sertifikat lama yang masih berlaku tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat pada Sertifikat lama

Old certificates that are still valid are available to verify old signatures until all certificates signed using the private key on the old certificate expire. If the old private key is used

tersebut kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka Kunci Privat lama disimpan dan dilindungi sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat lama habis masa berlakunya. Tabel penjelasan Kunci BSrE CA dan masa berlakunya dijelaskan pada bagian 6.3.2. Apabila BSrE CA memperbarui Kunci Privat dan menghasilkan Kunci Publik baru, maka BSrE CA memberitahu semua Pemilik yang mengandalkan Sertifikat BSrE CA bahwa telah terjadi perubahan. BSrE CA tidak membangkitkan Sertifikat Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat BSrE CA. Dengan demikian, pasangan kunci BSrE CA dibangkitkan lagi paling lambat 2 (dua) tahun sebelum Sertifikat BSrE CA kedaluwarsa.

to sign the CRL, then the old private key is stored and protected until all certificates signed using the old private key expire. The explanation table of BSrE CA keys and their validity periods is explained in section 6.3.2. If BSrE CA updates the private key and generates a new public key, then BSrE CA notifies all owners who rely on the BSrE CA certificate that a change has occurred. BSrE CA does not generate owner certificates that have a validity period longer than the validity period of the BSrE CA certificate. Thus, the BSrE CA key pair is generated again no later than 2 (two) years before the BSrE CA certificate expires.

5.7 Pemulihan Bencana dan Kondisi Terkompromi / Compromise and Disaster Recovery

5.7.1 Prosedur Penanganan Insiden dan Keadaan Terkompromi / Incident and Compromise Handling Procedure

BSrE CA memiliki rencana penanganan insiden dan rencana pemulihan bencana.

BSrE CA has an incident response plan and a disaster recovery plan.

Jika BSrE CA mendeteksi adanya percobaan peretasan terhadap sistem BSrE CA, maka BSrE CA melakukan investigasi untuk menentukan sifat dan tingkat kerusakan. Jika Kunci Privat milik BSrE CA diduga bocor, maka prosedur pencabutan seluruh Sertifikat Elektronik dilakukan.

If BSrE CA detects an attempted hack on the BSrE CA system, BSrE CA will conduct an investigation to determine the nature and extent of the damage. If the BSrE CA's Private Key is suspected to have been leaked, a procedure for revoking all Certificates will be carried out.

Jika Kunci Privat BSrE CA dicurigai sudah bocor/terkompromi, prosedur penanganan dilakukan sebagaimana diatur pada Bagian 5.7.3.

If the BSrE CA's Private Key is suspected to have been leaked/compromised, the handling procedure will be carried out as set out in Section 5.7.3.

Informasi cadangan terkait BSrE CA tersimpan di luar lokasi penyimpanan utama dan tersedia saat terjadi keadaan membahayakan atau bencana. Informasi cadangan tersebut minimal meliputi data permohonan Sertifikat Elektronik, *audit log* dan pangkalan data yang mencatat seluruh Sertifikat Elektronik yang telah dikeluarkan BSrE. Kunci Privat cadangan milik BSrE CA disimpan dan dikelola sesuai dengan ketentuan yang berlaku sebagaimana Kunci Privat utama.

Backup information regarding BSrE CA is stored in the outside of main storage location and available when an emergency or disaster occurs. The backup information at least includes Certificate application data, audit logs and databases that record all Certificates that have been issued by BSrE CA. Backup BSrE CA's Private Keys are stored and managed in accordance with the applicable stipulation as the main Private Key.

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

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

The BSrE CA informs the Root CA of any incidents, including but not limited to:

1. Detection or indication that the BSrE CA's systems are compromised;
2. An attempt to penetrate the BSrE CA's systems, either physically or electronically;
3. Denial of Service (DoS) attacks on the BSrE CA system;
4. Any incident that prevents or hinders the

4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam field "*next update*" pada CRLnya yang valid saat ini. BSrE CA harus segera memulihkan penerbitan CRL secepat mungkin; dan/atau
5. CRL dan/atau OCSP responder tidak dapat diakses oleh publik.

issuance of a CRL within 24 (twenty-four) hours of the time specified in the "next update" field of its currently valid CRL. The BSrE CA must restore CRL issuance as soon as practicable; and/or
5. The CRL and/or OCSP responder are not publicly accessible.

Prosedur diperbarui secara berkala sesuai kebutuhan. Semua sistem pencadangan/ pemulihan diuji minimal setahun sekali.

Procedures are regularly updated as required. All backup/restore systems are tested at least once a year.

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

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

1. Memberitahu PA atau PSrE Induk sesegera mungkin.
2. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.
3. Mengoperasikan kembali BSrE CA, dengan memprioritaskan kemampuan untuk membangkitkan informasi status sertifikat sesuai jadwal penerbitan CRL.
   - Jika kemampuan untuk membangkitkan informasi status Sertifikat tidak beroperasi atau rusak, BSrE CA memulihkan kemampuan untuk membangkitkan informasi status Sertifikat sesegera mungkin sesuai dengan prosedur yang ditetapkan dalam CPS. Jika kemampuan BSrE CA untuk membangkitkan informasi status Sertifikat tidak bisa dipulihkan dalam jangka waktu yang wajar, BSrE CA menentukan apakah perlu untuk meminta pencabutan Sertifikat miliknya kepada PSrE Induk.
4. Bila kunci penandatanganan BSrE CA rusak, operasional BSrE CA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci BSrE CA baru sesuai dengan prosedur yang ditetapkan dalam CPS.

When computer resources, software, and/or data are damaged, BSrE CA does the following:

1. Notify the PA or Root CA as soon as possible;
2. 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;
3. Re-establish BSrE CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule;
   - If the ability to generate Certificate status information is inoperative or damaged, the BSrE CA restores the ability to generate Certificate status information as soon as possible in accordance with the procedures set out in the CPS. If the BSrE CA's ability to generate Certificate status information cannot be restored within a reasonable period of time, the BSrE CA determines whether it is necessary to request revocation of its Certificate to the Root CA.
4. If BSrE CA signing keys are destroyed, reestablish BSrE CA operations as quickly as possible, giving priority to the generation of a new BSrE CA signing key pair in accordance with the procedures stipulated in the CPS.

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

If both primary and disaster recovery sites cannot be used for revocation capability in a reasonable time-frame, the CA systems will be treated as compromised.

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

Jika Kunci Privat dari BSrE CA terkompromi, maka BSrE CA:

If the Private Key of BSrE CA is compromised, then BSrE CA:

1. Memberitahu PA dan PSrE Induk sesegera mungkin agar dapat melakukan pencabutan Sertifikat;
2. Memberitahu semua Pemilik;
3. Mencabut Sertifikat Pemilik yang terkait dengan Kunci Privat yang terkompromi tersebut;
4. BSrE CA meminta penerbitan Sertifikat baru ke Menteri Komunikasi dan Digital sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CP PSrE Induk;
5. Memberitahu Pengandal, kontak-kontak yang relevan, dan seluruh Pemilik melalui pengumuman publik. Selanjutnya BSrE CA menghentikan layanan, memberitahu semua Pemilik dan Pengandal agar mengeluarkan Sertifikat BSrE CA dari rantai kepercayaannya, dilanjutkan dengan pencabutan semua Sertifikat, menerbitkan CRL terakhir, dan memberi tahu kontak-kontak yang relevan; dan
6. Menyiapkan Infrastruktur Kunci Publik BSrE CA dengan Pasangan Kunci yang baru.

1. Notify the PA and Root CA as soon as possible in order to to be able to revoke the Certificate;
2. Notify all Subscribers;
3. Revoke Subscriber Certificate related with the compromised private keys;
4. The BSrE CA requests the issuance of a new Certificate to the Minister of Communications and Information Technology in accordance with the initial registration process as specified in the Root CA's CP;
5. Notifies the Relying Parties, relevant contacts, and all Subscriber through a public announcement. The BSrE CA then discontinues service, notifies all Subscribers and Relying Parties to remove the BSrE CA's Certificate from its chain of trust, followed by revocation of all Certificates, issues a final CRL, and notifies relevant contacts; and
6. Set up the BSrE CA's Public Key Infrastructure with the new Key Pair.

BSrE CA membangkitkan Pasangan Kunci BSrE CA baru sesuai dengan prosedur yang ditetapkan dalam CPS. Penerbitan ulang Kunci Privat Pemilik akibat terkompromi dapat dilakukan Pemilik dengan mengajukan permohonan Sertifikat sebagaimana diatur pada Bagian 4.1. BSrE CA menyelidiki penyebab kompromi atau kerugian dan tindakan yang diambil untuk mencegah kompromi tersebut terulang kembali.

The BSrE CA generates the new BSrE CA Key Pair in accordance with the procedures set out in the CPS. Reissuance of an Subscriber's Private Key as a result of a compromise may be made by the Subscriber applying for a Certificate as set out in Section 4.1. The BSrE CA investigates the cause of the compromise or loss and the actions taken to prevent the compromise from recurring.

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

Untuk memelihara integritas layanan BSrE CA, diimplementasikan backup data dan prosedur-prosedur pemulihan. BSrE CA membuat sebuah Rencana Pemulihan Bencana (*Disaster Recovery Plan*/DRP). DRP ditinjau ulang dan diuji secara berkala (minimal setahun sekali) dan diperbaharui jika dibutuhkan. Fasilitas *Disaster Recovery Center* BSrE CA tersedia bila fasilitas utama berhenti beroperasi.

To maintain the integrity of the BSrE CA services, it implements data backup and recovery procedures. BSRE CA has developed a Disaster Recovery Plan (DRP). The DRP and supporting procedures are reviewed and tested periodically (at least once a year) and are revised and updated as needed. The BSrE CA Disaster Recovery Center facilitiy is available when the primary node (main site) should cease operation.

BSrE CA memiliki rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus- menerus diperbaharui. Layanan harus kembali pulih dalam kurun waktu 24 (dua puluh empat) jam bila ada bencana. Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan BSrE CA rusak secara fisik dan semua salinan kunci penandatangan milik BSrE CA hancur, BSrE CA akan meminta agar Sertifikat Elektronik-nya dicabut dan mengikuti ketentuan sebagaimana diatur

BSrE CA has a disaster recovery plan that has been tested, verified, and continuously updated. Services must be restored within 24 hours in case of disaster. If disaster that causes physical damage to all BSrE CA facilities and equipment, and the destruction of all copies of the BSrE CA's signing keys, the BSrE CA will request its Digital Certificate to be revoked and follow the provisions as regulated in section 5.7.3.

pada bagian 5.7.3.

5.8 Penghentian CA atau RA / CA or RA Termination

Bila ada keadaan yang menyebabkan diakhirinya layanan BSrE CA dengan persetujuan dari PA dan PSrE Induk, BSrE CA akan memberitahu RA, pemilik, dan semua Pengandal. Rencana aksi adalah sebagai berikut:

1. BSrE CA memastikan segala gangguan yang diakibatkan oleh penutupan BSrE CA diminimalisasi;
2. BSrE CA memastikan agar rekaman arsip tetap dipertahankan;
3. BSrE CA memberitahu ke RA, pemilik, dan semua Pengandal bahwa status operasional BSrE CA dihentikan;
4. BSrE CA menyediakan dukungan berkelanjutan operasional hingga semua sertifikat pemilik kadaluarsa;
5. BSrE CA melakukan pencabutan seluruh sertifikat pemilik; dan
6. BSrE CA menyimpan informasi BSrE CA dan Pemilik selama periode pemberitahuan untuk tujuan pengalihan tanggung jawab serta periode pengarsipan.
7. BSrE CA memberitahu Menteri, Pengawas Penyelenggaraan Sertifikasi Elektronik (P2SE), PSrE Induk, LS PSrE, dan pihak berwenang lainnya.

If there is any circumstance to terminate the services of BSrE CA with the approval of the PA and Root CA, BSrE CA will notify the RA, Subscribers, and all Relying Parties. The action plan is as follows:

1. BSrE CA ensure that any disruption caused by the termination of an Issuing BSrE CA is minimized as much as possible;
2. BSrE CA ensure that archived records are maintained;
3. BSrE CA notifies the RA, Subscribers, and all Relying Parties the status of the operational BSrE CA has been stopped;
4. BSrE CA provides ongoing operational support until all subscriber certificates expired;
5. BSrE CA revokes all Subscriber Certificates; and
6. Keep the BSrE CA and Subscriber informations during the notification period for the purpose of transferring responsibility and archiving periods.
7. BSrE CA notifies the Minister, Pengawas Penyelenggaraan Sertifikasi Elektronik (P2SE), Root CA, LS PSrE, and other relevant authorities.

BAB 6
KENDALI KEAMANAN TEKNIS / TECHNICAL SECURITY CONTROLS

6.1 Pembangkitan dan Instalasi Pasangan Kunci / Key Pair Generation and Installation

6.1.1 Pembangkitan Pasangan Kunci / Key Pair Generation

1. Pembangkitan Pasangan Kunci BSrE CA / BSrE CA Key Pair Generations

Pasangan Kunci BSrE CA dibangkitkan melalui sistem PKI BSrE CA. Material kunci kriptografi yang digunakan oleh BSrE CA untuk menandatangani Sertifikat Elektronik, CRL atau informasi status Sertifikat Elektronik dihasilkan dalam modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 3.	The BSrE CA key pair is generated using the BSrE CA PKI system. The cryptographic key material used by BSrRE CA to sign Digital Certificates, CRLs or digital certificate status information is generated in a cryptographic module that is certified at least FIPS 140-2 Level 3.

2. Pembangkitan Pasangan Kunci Pemilik Sertifikat / Subscriber Key Pair Generation

Material kunci kriptografi Pemilik Sertifikat dengan kegunaan tanda tangan elektronik dan segel elektronik dihasilkan dalam modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 3. Modul kriptografi untuk pembangkitan kunci pemilik dengan kegunaan segel elektronik dapat dikelola oleh pemilik.	Subscriber's cryptographic key material with the product is digital signatures and electronic seals is generated in a cryptographic module that is certified at least FIPS 140-2 Level 3. Cryptographic module for Subsriber's key pair generation with the use of electronic seals can be managed by Subscriber.

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

BSrE CA tidak melakukan pengiriman Kunci Privat kepada Pemilik Sertifikat.	BSrE CA does not send private keys to Subscriber.

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

BSrE CA tidak menerima permohonan penerbitan sertifikat berdasarkan CSR dari luar lingkungan BSrE CA untuk Tanda Tangan Elektronik. Sedangkan, untuk segel elektronik BSrE CA dapat menerima permohonan penerbitan sertifikat berdasarkan CSR dari luar lingkungan BSrE CA.	BSrE CA has not received a certificate issuance application based on CSR from outside of the BSrE CA's system environment for digital signature. Meanwhile for electronic seals, BSrE CA can received a certificate issuance application based on CSR from outside of the BsrE CA's system environment.

6.1.4 Pengiriman Kunci Publik BSrE CA ke Pengandal / BSrE CA Public Key Delivery to Relying Parties

Setiap sertifikat yang diterbitkan oleh BSrE CA berisi Kunci Publik. BSrE CA menyediakan mekanisme publikasi terhadap sertifikat BSrE CA yang aktif melalui repositori yang dapat diakses oleh Pihak Pengandal. Penjelasan tentang publikasi dan repositori sertifikat mengacu pada Bagian 2.1	Each certificate issued by BSrE CA contains a Public Key. BSrE CA provides a publication mechanism for active BSrE CA certificates through a repository that can be accessed by the Relying Party. Certificate publication and repository are referred to Section 2.1.

6.1.5 Ukuran Kunci / Key Sizes

Sertifikat	Panjang Kunci/Key Length	Encryption Algorithm	Digest Algorithm
BSrE CA	4096 bit	RSA	SHA-256
Pemilik - Tanda Tangan Elektronik	2048 bit	RSA	SHA-256

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

Parameter kunci publik dibangkitkan dan divalidasi sesuai FIPS 186-4.	Public key parameters are generated and validated in accordance with FIPS 186-4

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

Kunci BSrE CA hanya digunakan untuk membuat tanda tangan elektronik dengan key usage dan extended key usage yang dispesifikasikan dalam Sertifikat, yaitu untuk menandatangani Sertifikat (keyCert Sign) dan menerbitkan CRL (CRLSign).	The Private Keys of the BSrE CA are only used for creating digital signatures in accordance with the key usages and extended key usages specified in the Certificate, which is to sign Certificates (keyCert Sign) and issue CRL (CRLSign).

6.2 Kendali Kunci Privat dan Kendali Teknis Modul Kriptografis / Private Key Protection and Cryptographic Module Engineering Controls

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

Pasangan kunci BSrE CA menggunakan modul kriptografi yang sudah sesuai standard FIPS 140-2 level 3 untuk operasional BSrE CA. Sedangkan, pasangan kunci Pemilik menggunakan modul kriptografis sesuai standar FIPS 140-2 level 3 dan hanya dapat diakses oleh Pemilik dengan menerapkan kombinasi paling sedikit 2 (dua) faktor autentikasi.	The BSrE CA key pair uses a cryptographic module that complies with FIPS 140-2 level 3 standards for BSrE CA operations. Meanwhile, the Owner's key pair uses a cryptographic module that complies with FIPS 140-2 level 3 standards and can only be accessed by the Owner by applying a combination of at least 2 (two) authentication factors.

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

Semua Kunci Privat BSrE CA diakses melalui kendali multipersonel sebagaimana diatur pada Bagian 5.2.2.	All BSrE CA Private Keys accessed through multi-person control as specified in Section 5.2.2.
Kunci Privat BSrE CA telah mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran Tepercaya untuk melaksanakan operasi kriptografis yang sensitif. Suatu jumlah minimum dari Secret Shares (m) dari sejumlah total Secret Shares yang dibuat dan didistribusikan untuk dipakai di modul kriptografis tertentu (n) diperlukan untuk mengaktifkan sebuah Kunci Privat BSrE CA yang disimpan di dalam modul	BSrE CA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive cryptographic operations. A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a BSrE CA Private Key stored in the module.
Angka ambang yang diperlukan untuk pembuatan kunci adalah 2 dari 4 (dimana n=2 dan m=4), aktivasi kunci penandatanganan adalah 2 dari 4, dan backup serta pemulihan kunci privat adalah 2 dari 4. Peran Tepercaya yang terlibat dalam kendali multi personil ini dicatat untuk keperluan audit.	The threshold number of shares needed for key generation is 2 of 2 (where n=2 and m=2) signing key activation is 2 of 2 and Private Key backup and restore is 2 of 2

6.2.3 Eskro Kunci Privat / Private Key Escrow

Kunci Privat BSrE CA tidak dieskrokan. Kunci Privat Pemilik dititipkan di BSrE CA.	BSrE CA’s Private Key is not escrowed. Subscriber's Private Key deposited at BSrE CA.

6.2.4 *Backup* Kunci Privat / Private Key Backup

Kunci privat BSrE CA di-backup di bawah kendali multi-pihak yang sama dengan kunci privat asli. Paling tidak satu salinan dari kunci privat disimpan off-site. Semua salinan kunci privat BSrE CA dilindungi dengan cara yang sama dengan aslinya. Kunci Privat Pemilik yang dititipkan pada BSrE CA dapat di-	The BSrE CA private key is backed up under the same multi-party control as the original private key. At least one copy of the private key is stored off-site. All copies of the BSrE CA private key are protected in the same way as the original. The Subscriber's Private Key deposited with BSrE CA can be backed up. All

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

backups of the Subscriber's Public Key are recorded and protected in the same way as the original Public Key.

6.2.5 Arsip Kunci Privat / Private Key Archival

Setelah masa berlaku Kunci Privat BSrE CA berakhir, Kunci Privat dihancurkan dan tidak diarsipkan. Kunci Privat Pemilik tidak diarsipkan.

At the end of the validity period, BSrE CA's private key is destroyed and is not archived. Subscriber's Private Key is not archived.

6.2.6 Pemindahan Kunci Privat ke/dari Modul Kriptografi / Private Key Transfer Into or From a Cryptographic Module

Kunci Privat milik BSrE CA dihasilkan di dalam dan tetap berada dalam perangkat kriptografi yang sama. Pasangan Kunci Publik/Privat milik BSrE CA dibuat salinannya untuk cadangan keamanan. Pemindahan kunci dari perangkat keras modul kriptografi utama dilakukan secara langsung ke perangkat keras modul kriptografi cadangan dengan menggunakan mekanisme yang diatur dalam prosedur pengiriman kunci. Pasangan kunci BSrE CA tidak boleh disimpan dalam perangkat lunak, baik sementara ataupun permanen untuk tujuan apapun.

BSrE CA's Private Keys are generated, activated, and stored in a cryptographic module. BSrE CA's Public/Private Key pair is copied for security backup. Key transfer from the main cryptographic module hardware is carried out directly to the backup cryptographic module hardware using the mechanism according to key transport procedure. BSrE CA's key pair may not be stored in the software, either temporarily or permanently for any purpose.

Proses pemindahan Kunci Privat ke/dari modul kriptografi dalam kondisi terenkripsi dan proses tersebut diatur dalam prosedur pengiriman kunci privat.

Privat Key transfer to/from cryptographic module hardware is encrypted and the process is organized in the private key transmission procedure.

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

Material kunci kriptografi (Kunci Privat) yang digunakan oleh BSrE CA untuk menandatangani Sertifikat Elektronik, CRL atau informasi status Sertifikat Elektronik disimpan dalam pengamanan modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 3 dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

Cryptographic key material used by BSRE CA to sign certificates, CRLs or status information stored in cryptographic modules validated minimum to FIPS 140-2 level 3 in encrypted form and protected with key-shared mechanism and password.

Material kunci kriptografi Pemilik Sertifikat dengan kegunaan tanda tangan elektronik dan segel elektronik disimpan dalam modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 2. Modul kriptografi untuk penyimpanan kunci privat pemilik dengan kegunaan segel elektronik dapat dikelola oleh pemilik.

Subscriber's cryptographic key material with the product is digital signatures and electronic seals is stored in a cryptographic module that is certified at least FIPS 140-2 Level 2. Cryptographic module for Subsriber's private key storage with the use of electronic seals can be managed by Subscriber.

6.2.8 Metode Aktivasi Kunci Privat / Method of Activating Private Key

Metode aktivasi Kunci Privat milik BSrE CA dilakukan oleh personil yang berwenang dan memerlukan kendali multi pihak sesuai kendali yang tercantum dalam Bab 5.2.2.

Activation of BSRE CA's Private Key operations is performed by authorized persons and requires multiparty control as specified in Section 5.2.2

Pengaktifan Kunci Privat Pemilik dilakukan dengan cara mengautentikasi Pemilik ke modul kriptografis sebelum melakukan aktivasi

The user must be authenticated to the cryptographic module before the activation of any Private Key(s). Acceptable means of

Kunci Privat terkait. Cara otentikasi yang diterima termasuk namun tidak terbatas pada frasa sandi, PIN, atau biometrik. Entri data aktivasi dilindungi dari pengungkapan (data tidak ditampilkan saat dimasukkan).	authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs), or biometrics. Activation data entries are protected from disclosure (data is not displayed when entered).
Pemilik bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemilik.	Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Metode Penonaktifan Kunci Privat / Method of Deactivating Private Key

Modul kriptografis yang sudah diaktivasi tidak ditinggal tanpa pengawasan atau diakses secara tidak sah. Dalam hal modul kriptografis akan dinonaktifkan, modul kriptografis dinonaktifkan oleh personel yang berwenang sebagaimana didefinisikan dalam CPS. Ketika BSrE CA tidak lagi beroperasi, Kunci Privat BSrE CA dan pemilik tersebut dihapus dari modul kriptografis.	The cryptographic modules that have been activated not be left unattended or otherwise available to unauthorized access. When the cryptographic module is about to be deactivated, the cryptographic module be deactivated by an authorized person as defined in the applicable CPS. When a BSrE CA is no longer operational, the Private Key of BSrE CA and subscribers are removed from the cryptographic module.

6.2.10 Metode Penghancuran Kunci Privat / Method of Destroying Private Key

Kunci Privat BSrE CA dihancurkan oleh para individu dalam Peran Tepercaya ketika Kunci Privat tidak diperlukan lagi atau ketika Sertifikat yang terkait dengan Kunci Privat tersebut telah dicabut atau kedaluwarsa. Penghancuran Kunci Privat dan salinannya dilakukan dengan menimpa (overwrite) Kunci Privat atau menginisialisasi modul dengan fungsi factory reset dari modul kriptografi sehingga tidak ada lagi informasi yang dapat digunakan untuk memulihkan Kunci Privat. Jika fungsi-fungsi atau perintah dalam modul kriptografis tidak dapat diakses untuk menghancurkan kunci yang ada di dalam modul kriptografis tersebut, maka modul kriptografis tersebut dihancurkan secara fisik. Proses penghancuran dilakukan pada lingkungan fisik yang aman.	The BSrE CA's Private Key is destroyed by the trusted roles when they are no longer needed or when the Certificate to which they correspond is expired or revoked. All the Private Keys and their backups are destroyed by overwriting the data or by initiating a factory reset function in the cryptographic modules, in a manner that any information cannot be used to recover any part of the Private Key. If the functions of cryptographic modules are not accessible in order to destroy the key contained inside, then the cryptographic modules will be physically destroyed. The destruction operation is carried out in a physically secure environment.
Kejadian penghancuran Kunci Privat BSrE CA harus dicatat. Penghancuran kunci privat Pemilik dapat dilakukan dengan menimpa lalu menghapusnya dari media penyimpanan. Metode penghancuran kunci pemilik diatur dalam prosedur penghancuran kunci pemilik.	The event of destroying BSrE CA's Private Key must be recorded. Destruction of the Subscriber's private key can be done by overwriting and then deleting it from the storage media. The method of destroying the subscriber's key is regulated in the subscriber's key destruction procedure.

6.2.11 Peringkat Modul Kriptografis / Cryptographic Module Rating

Sesuai dengan ketentuan yang diatur pada Bagian 6.2.1.	As described in Section 6.2.1.

6.3 Aspek-Aspek Lain Dalam Pengaturan Pasangan Kunci / Other Respects of Key Pair Management

6.3.1 Pengarsipan Kunci Publik / Public Key Archival

Kunci Publik BSrE CA dan Pemilik diarsipkan selama 5 (lima) tahun sebagai bagian dari	BSrE CA's and Subcriber's Public Keys are archived as integral parts of the Certificates

proses pengarsipan Sertifikat Elektronik. Rincian tentang pengarsipan diatur pada Bagian 5.5.

issued for at least 5 (five) years. Detail on archival is described in Section 5.5.

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

Periode operasi pasangan kunci ditentukan oleh periode operasional Sertifikat Elektronik yang sesuai. Jangka waktu operasional maksimum kunci ditentukan selama 10 (sepuluh) tahun untuk BSrE CA. Sementara untuk kunci Pemilik memiliki periode 2 (dua) tahun.

The key pair operational period is defined by the operational period of the corresponding Certificate. The maximum operational period of the keys is defined as 10 (ten) years for BSrE CA, and 2 (two) year for Subscriber certificates.

6.4 Data Aktivasi / Activation Data

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

Data Aktivasi untuk HSM yang sesuai dibuat pada saat key ceremony oleh Peran Tepercaya (merujuk pada Bagian 6.1.1). Data aktivasi untuk mengaktifkan Kunci Privat Pemilik dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan.

Activation data for the corresponding HSM generate during a key ceremony by Trusted Role (refer to Section 6.1.1). The activation data to activate the Subscriber's Private Key is protected based on the security level commensurate with the cryptographic module used.

6.4.2 Pelindungan Data Aktivasi / Activation Data Protection

Data aktivasi untuk perangkat HSM dilindungi seperti yang diuraikan pada bagian 6.2.2. BSrE CA menyimpan data aktivasi dalam bentuk smartcard dengan perlindungan kata sandi.

Activation data for HSM tools protected as described in Section 6.2.2. BSrE CA stores activation data in the form of smart card with password protection.

Setelah mengalami kegagalan login sebanyak jumlah yang ditentukan, disediakan kemampuan untuk mengunci sementara akun tersebut. Data aktivasi Kunci Privat BSrE CA dilakukan oleh Peran Tepercaya.

After experiencing a certain number of failed login attempts, the ability to temporarily lock the account is provided. BSrE CA Private Key activation data is processed by Trusted Role.

Pemilik diwajibkan untuk selalu menjaga kerahasiaan data aktivasi.

The subscriber is required to always keep the activation data confidential.

6.4.3 Aspek Lain dari Aktivasi Data / 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 disediakan oleh sistem operasi atau melalui suatu kombinasi dari sistem operasi, perangkat lunak, dan perlindungan fisik. BSrE CA menyertakan fungsionalitas berikut:

1. Mewajibkan login terautentikasi bagi Peran Tepercaya;
2. Menyediakan kendali akses dengan kewenangan yang minimal;
3. Menyediakan kapabilitas audit keamanan (dilindungi integritasnya);
4. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;

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

1. Require authenticated logins for trusted roles;
2. Provide Access Control with least privilege;
3. Provide a security audit capability (protected in integrity);
4. Require use of cryptography for communication session and database security;

5. Menyediakan perlindungan mandiri untuk sistem operasi;
6. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
7. Mewajibkan penggunaan saluran Tepercaya untuk identifikasi dan autentikasi;
8. Menyediakan perlindungan terhadap kode jahat (*malicious code*);
9. Menyediakan cara untuk menjaga integritas perangkat lunak; dan
10. Mewajibkan pemeriksaan mandiri (*self-test*) terhadap layanan-layanan BSrE CA (seperti: pemeriksaan integritas audit log).

5. Provide self-protection for the operating system;
6. Require use of strong password policy;
7. Require trusted path for identification and authentication;
8. Provide means for malicious code protection;
9. Provide means to maintain software integrity; and
10. Require self-test security related BSrE CA services (e.g., check the integrity of the audit logs).

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

The BSrE CA's computer system must be configured with minimum of the required accounts and network services.

6.5.2 Penilaian 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

Diatur dalam pedoman pengembangan sistem aplikasi BSrE CA.

Regulated in the BSrE CA system application development guidelines.

6.6.2 Kendali Pengelolaan Keamanan / Security Management Controls

BSrE CA menggunakan perangkat lunak untuk mendeteksi perubahan konfigurasi sistem manajemen BSrE CA. BSrE CA memiliki prosedur dan personil yang bertanggung jawab melakukan monitoring dan pemeriksaan secara rutin.

BSrE CA uses software to detect configuration changes in the BSrE CA management system. BSrE CA has procedures and personnel who are responsible for routine monitoring and inspection.

6.6.3 Siklus Hidup Kendali Keamanan / Security Control Life Cycle

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

BSrE 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

BSrE CA melakukan tindakan keamanan jaringan yang sesuai untuk memastikan keamanan dari tindakan DoS dan serangan intrusi. Langkah langkah tersebut termasuk penggunaan firewall dan router. BSrE CA mematikan port dan layanan jaringan yang tidak digunakan.

BSrE CA employs appropriate network security measures to ensure they are guarded against Denial of Service and intrusion attacks. Such measures include the use of firewalls and filtering routers. Unused network ports and services are turned off.

6.8 Stempel Waktu / Time Stamping

BSrE CA memastikan akurasi dari tanggal dan jam yang digunakan dalam proses *Time-Stamping*. Jam server *online* BSrE CA disinkronkan menggunakan NTP. Waktu yang didapat dari layanan waktu di atas akan digunakan untuk menentukan waktu pada saat:

1. Validitas waktu berlakunya Sertifikat Elektronik milik BSrE CA;

All BSrE CA components are regularly synchronized with a time service using a NTP service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service must be used for establishing the time of:

1. Initial validity time of BSrE CA certificate;

2. Pencabutan Sertifikat Elektronik milik BSrE CA;
3. Pembaruan CRL dan OCSP responder; dan
4. Penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik Pemilik Sertifikat Elektronik.

Prosedur secara elektronik atau manual dapat digunakan untuk mempertahankan akurasi waktu pada sistem. Dalam menyelenggarakan layanan Penanda Waktu Elektronik tersertifikasi, BSrE CA mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

2. Revocation of BSRE CA certificate;
3. Posting of CRL and OCSP updates; and
4. Issuance, renewal, and revocation of Subscriber certificates.

Electronic or manual procedures may be used to maintain system time. When providing a certified electronic timestamp service, BSrE CA must refer to the national timestamp provided by a government agency whose authority concerns meteorology, climatology, and geophysics.

BAB VII
PROFIL OCSP, *CRL,* DAN *SERTIFIKAT / CERTIFICATE, CRL, AND OCSP PROFILES*

7.1 Profil Sertifikat Elektronik /Certificate Profile

Profil Sertifikat mengikuti standar RFC 5280 "*Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*". BSrE CA melakukan reviu terhadap profil Sertifikat secara berkala minimal setahun sekali. Lihat Lampiran B untuk tabel profil sertifikat.

A Certificate profile according to RFC 5280 "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile" is used. BSrE CA review Certificate profiles periodically at least once a year. See Appendix B for the table of certificate profile.

7.2 Profil CRL / CRL Profile

Profil CRL BSrE CA mematuhi Standar Interoperabilitas PSrE Indonesia. BSrE CA menggunakan CRL dan CRL *entry extension* RFC 5280.

BSrE CA's CRL Profile comply with Indonesian CA Interoperability Standard. BSrE CA operating under this CP use the RFC 5280 CRL and CRL entry extension.

7.3 Profil OCSP / OCSP Profile

BSrE CA mengoperasikan *Online Certificate Status Protocol responder* (responder OCSP) mengacu ke Standar Interoperabilitas PSrE Indonesia.

BSrE CA operate an Online Certificate Status Protocol (OCSP) referring to Indonesian CA Interoperability Standard.

BAB VIII
AUDIT KEPATUHAN DAN PENILAIAN KELAIKAN LAINNYA / COMPLIANCE AUDIT AND OTHER ASSESSMENTS

BSrE CA menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh Kementerian Komunikasi dan Digital tentang Penyelenggaraan Sertifikasi Elektronik. BSrE CA diaudit untuk kepatuhan kepada Webtrust CA dan untuk kepentingan memperoleh pengakuan dari Kementerian Komunikasi dan Digital. BSrE CA telah memenuhi audit untuk memastikan semua persyaratan pada CPS ini telah diimplementasikan dan diaudit berdasarkan standar Webtrust for CA dan ISO 27001.

BSrE CA performs a compliance audit and submits periodic reports required by the Ministry of Communication and Informatics regarding the Implementation of Certificate Authority. BSrE CA is audited for Webtrust for CA compliance and for the purpose of obtaining recognition from the Ministry of Communication and Informatics. BSrE CA has complied with an audit to ensure all requirements in this CPS have been implemented and audited according to Webtrust for CA and ISO 27001 standards.

8.1 Frekuensi atau Lingkup Penilaian / Frequency and Circumstances of Assessment

BSrE CA diaudit secara periodik minimal 1 kali dalam 12 bulan untuk memastikan bahwa seluruh kegiatan operasional BSrE CA sesuai dengan yang ditetapkan dalam dokumen CPS. BSrE CA menindak lanjuti setiap hasil audit berdasarkan rekomendasi yang dibuat oleh Auditor. BSrE CA menjalani audit kepatuhan dan menyampaikan laporan berkala minimal sekali setahun yang dipersyaratkan oleh Kementerian Komunikasi dan Digital.

BSrE CA is audited periodically at least 1 time in 12 months to ensure that all BSrE CA operational activities are in accordance as stipulated in the CPS document. BSrE CA follows up on each audit result based on the recommendations made by the Auditor. BSrE CA performs a compliance audit and submits periodic reports at least once a year as required by the Ministry of Communication and Digital.

8.2 Identitas/Kualifikasi Penilai / Identity/Qualifications of Assessor

Penilai menunjukkan kompetensi pada bidang audit kepatuhan, dan benar-benar memahami persyaratan CPS ini. Penilai kepatuhan melakukan audit kepatuhan sebagai tanggung jawab utama. Penilai kepatuhan memiliki kualifikasi sebagai berikut:

1. Penilai dilaksanakan oleh tim asesmen independen yang *qualified;*
2. Penilai memiliki pengetahuan yang cukup tentang tanda tangan elektronik, Sertifikat Elektronik, X.509 versi 3 PKI *Certificate Policy and Certification Practices Framework*, serta Undang-Undang tentang informasi dan transaksi elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Kementerian Komunikasi dan Digital terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik;
3. Penilai memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
4. Penilai harus memiliki bukti bahwa dirinya memenuhi kualifikasi penilai untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah;
5. Penilai menguasai set keahlian tertentu,

Assessors demonstrate competence in the compliance auditing area, and have a thorough understanding of the requirements of this CPS. Assessor performs compliance audits as a primary responsibility. Assessors have the following qualifications:

1. The assessment is carried out by a qualified independent assessment team;
2. Assessors have sufficient knowledge of digital signatures, Certificates, X.509 version 3 of PKI Certificate Policy and Certification Practices Framework, as well as Laws on electronic information and transactions, Government Regulations on the Implementation of Electronic Systems and Transactions, and Regulation of the Minister of Communication and Informatics regarding the Implementation of Certification Authorities.
3. The assessor has proficiency in information security auditing including security techniques, equipment, and Public Key Infrastructure technology.
4. The assessors have evidence that show their qualification for a specific audit scheme, in form of certification, accreditation, license or other valid assessment;
5. Assessors master certain skill sets,

pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan professional;
6. Penilai tidak memiliki konflik kepentingan terhadap BSrE CA; dan
7. Penilai patuh terhadap hukum, kebijakan pemerintah, atau kode etik professional.

competency evaluation, quality assurance measures such as peer review, standards regarding the proper assignment of staff, and requirements for continuing professional education;
6. The assessor has no conflict of interest with BSrE CA; and
7. Assessors comply with laws, government policies, or professional codes of ethics

8.3 Hubungan Penilai dengan Entitas yang Dinilai / Assessor's Relationship to Assessed Entity

BSrE CA memilih Penilai/asesor yang independen. Penilai juga dapat memberikan evaluasi independent yang tidak memihak.

BSrE CA selects independent assessors. The assessors can also provide unbiased independent evaluations.

8.4 Topik Penilaian / Topics Covered by Assessment

Audit yang dilaksanakan harus memenuhi kebutuhan dari skema audit yang digunakan dalam asesmen. Kebutuhan-kebutuhan tersebut bisa berbeda seiring dengan diperbaruinya skema audit. Sebuah skema audit akan berlaku pada tahun berikutnya setelah BSrE CA mengadopsi skema yang terbaru. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen BSrE CA.

The audit that is carried out must meet the requirements of the audit scheme used in the assessment. These requirements may change as the audit scheme is updated. An audit scheme will be applied in the following year after BSrE CA PSrE adopts the latest scheme. This assessment covers at least the organization, operations, personnel training, and management of BSrE CA.

8.5 Tindakan yang Diambil Akibat Ketidaksesuaian / Actions Taken as a Result of Deficiency

BSrE CA akan menyusun rencana tindakan perbaikan yang akan dilaksanakan untuk memperbaiki kekurangan yang tercatat berdasarkan masukan dari Penilai.
Tindakan yang dilakukan sebagai berikut:
1. Penilai kepatuhan harus memberitahu BSrE CA dan Kementerian Komunikasi dan Digital tentang ketidaksesuaian; dan
2. BSrE menentukan pemberitahuan atau tindak lanjut apa yang diperlukan disesuaikan dengan persyaratan CPS dan kontrak terkait, kemudian melaksanakan pemberitahuan dan tindakan tersebut tanpa penundaan.

BSrE CA will develop a corrective action plan that will be implemented to remove deficiencies based on input from the Assessor. Corrective action as follows:
1. Assessor must inform BSRE CA and the Ministry of Communication and Informatics regarding of deficiencies; and
2. BSrE determines what notification or follow-up is needed in accordance with the requirements of the CPS and related contracts, then implements the notification and action without delay.

8.6 Laporan Hasil Penilaian / Communications of Results

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

Results of the audit are reported to the Policy Authority as specified in section 8.1 for analysis and resolution of any deficiency through a subsequent corrective action plan. The result identifies the version of the Root CA's CP and CPS used on the assessment. Furthermore, the result is also made available as specified in section 8.5.

8.7 Audit Internal / Self-Audit

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan risiko gangguan pada proses bisnis dilaksanakan secara berkala 1 (satu) tahun sekali.

Audits on operational systems are planned and agreed to minimize the risk of business processes which carried out regularly once a year.

Audit internal juga memeriksa kesesuaian dengan CP PSrE Induk, CPS ini dan ketentuan peraturan perundangan-undangan terkait PSrE.

Internal audit also checks the compliance with CP Root CA, this CPS and laws and regulations concerning CA.

BSrE CA melakukan audit mandiri setiap tahun sekali terhadap sampel yang dipilih secara acak dari setidaknya 1 (satu) persen keseluruhan Sertifikat yang diterbitkan di tahun berjalan.

The BSrE CA conducts a self-audit once every year of a randomly selected sample of at least 1 (one) percent of all Certificates issued in the year.

BAB IX
BISNIS LAIN DAN MASALAH HUKUM / OTHER BUSINESS AND LEGAL MATTERS

9.1 Biaya / Fees

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

Seluruh proses/kegiatan yang berhubungan dengan permintaan, penerbitan dan pembaruan tidak dipungut biaya.	BSrE CA does not charge for any processes related to request, issuance and re-key of Certificate.

9.1.2 Biaya Pengaksesan Sertifikat Elektronik / Certificate Access Fees

Seluruh proses/kegiatan yang berhubungan dengan akses terhadap Sertifikat Elektronik tidak dikenakan biaya.	BSrE CA does not charge for any access to Certificate from the repository of BSrE CA.

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

Seluruh proses/kegiatan yang berhubungan dengan pencabutan Sertifikat Elektronik atau akses terhadap status keberlakuan Sertifikat Elektronik tidak dikenakan biaya.	BSrE CA does not charge for any access to revocation status information through CRL or OCSP.

9.1.4 Biaya Layanan Lainnya / Fees for Other Services

Seluruh proses/kegiatan dalam konteks penerapan sertifikat elektronik BSrE CA tidak dikenakan biaya.	BSrE CA does not charge for any processes related to implementation of Certificate.

9.1.5 Kebijakan Pengembalian Biaya

Tidak ada ketentuan.	No stipulation.

9.2 Tanggung Jawab Keuangan / Financial Responsibility

9.2.1 Cakupan Asuransi / Insurance Coverage

Apabila terjadi *compromised* pada BSrE CA, BSSN dapat mengambil alih operasional BSrE CA.	In case of compromise, the National Cyber and Crypto Agency can take over the operations of BSrE CA.

9.2.2 Aset Lainnya / Other Assets

BSrE CA mengupayakan pengelolaan keuangan secara wajar yang diperoleh dari DIPA BSSN untuk menjalankan operasional BSrE CA dalam memenuhi kewajiban kepada Partisipan IKP sebagaimana diatur pada Bagian 1.3.	BSrE CA also maintain reasonable and sufficient financial resources from DIPA BSSN to maintain operations, fulfill duties, and reasonable liability obligations to PKI Participants described in Section 1.3.

9.2.3 Jaminan Asuransi atau Garansi untuk Pemilik / Insurance or Warranty Coverage for Subscribers

BSrE CA menyediakan kebijakan jaminan untuk para Pemilik sertifikat atas kerusakan yang disebabkan oleh kesengajaan atau kelalaian BSrE CA karena kegagalan dalam mematuhi kewajibannya sebagaimana diatur dalam peraturan perundang-undangan.	BSrE CA provides a guarantee policy for certificate subscribers for damages caused by the deliberate act or negligence of BSrE CA due to failure to comply with its obligations as regulated in laws and regulations.

9.3 Kerahasiaan Informasi Bisnis / Confidentiality of Business Information

9.3.1 Cakupan Informasi Rahasia / Scope of Confidential Information

BSrE CA memperhatikan dan menyediakan penanganan khusus untuk kategori informasi rahasia. Yang termasuk dalam kategori informasi rahasia antara lain: 1. Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4; 2. Kunci Privat Pemilik Sertifikat yang	BSrE CA keeps and classifies the following items that are classified as being confidential information and therefore are subject to reasonable care and attention: 1. Personal information of CA's personnels as detailed in Section 9.4; 2. Subscriber's Private Key stored by BSrE

disimpan oleh BSrE CA, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
3. Catatan Permohonan Sertifikat;
4. Hasil penilaian kerentanan;
5. Rekam jejak audit (*audit logs*) dari sistem BSrE CA;
6. Data aktivasi pada saat pengaktifan Kunci Privat BSrE CA sebagaimana dijabarkan pada Bagian 6.4;
7. Dokumentasi bisnis proses PSrE termasuk dokumen DRP dan BCP;
8. Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8; dan
9. Kontrol keamanan untuk perangkat keras dan perangkat lunak BSrE CA.

CA and the information required to use Privat Key by the Subscriber;
3. Certificate Application Records;
4. Vulnerability Assessment Results;
5. Audit logs from BSrE CA's systems;
6. Activation data used to active BSrE CA Private Keys as detailed in Section 6.4;
7. BSrE CA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP);
8. Audit Reports from an independent auditor and internal auditor as detailed in Section 8; and
9. Security Control for BSrE CA's hardware and software.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, sebelum pengungkapan informasi di atas memerlukan persetujuan tertulis dari Pemilik.

Unless required by law or court order, any disclosure of such information requires the Subscriber's written prior consent.

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

Informasi yang tidak dikategorikan rahasia dalam dokumen CPS dianggap informasi publik, seperti:
1. Sertifikat BSrE CA;
2. CRL BSrE CA;
3. CPS BSrE CA;
4. Kebijakan Privasi untuk Pengguna Layanan BSrE;
5. Perjanjian Pemilik Sertifikat Elektronik BSrE CA;
6. Perjanjian Pengandal Layanan BSrE;
7. Kebijakan Jaminan BSrE CA; dan
8. Petunjuk Teknis Verifikasi Tanda Tangan Digital pada Dokumen PDF.

Any information not defined as confidential within this CPS is deemed as public, such as:
1. BSrE CA's certificate;
2. BSrE CA's CRL;
3. BSrE CA's CPS;
4. Privacy Policy;
5. Subscriber Agreement;
6. Relying Party Agreement;
7. Warranty Policy; and
8. Technical Instructions for Verifying Digital Signatures on PDF Documents.

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

BSrE CA melindungi informasi rahasia. BSrE CA menjaga kerahasiaan informasi bisnis rahasia yang secara jelas ditandai atau diberi label sebagai rahasia atau menurut sifatnya dipahami secara wajar sebagai rahasia, dan memperlakukan informasi tersebut dengan tingkat perhatian dan keamanan yang sama seperti BSrE CA memperlakukan informasi rahasia milik sendiri. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:
1. Pelatihan dan peningkatan *awareness*;
2. Perjanjian kontrak pegawai; dan
3. NDA dengan pegawai, pegawai *outsource*, dan rekanan.

BSrE CA safeguards the confidentiality of business information that is clearly marked or labeled as confidential or is reasonably understood to be confidential by its nature, and treats such information with the same level of care and security as BSrE CA treats its own confidential information. The forms of implementation of responsibility for the protection of confidential information include but are not limited to:
1. Training and awareness;
2. Contracts with employees; and
3. NDA with employees, outsource and contractors.

9.4 Privasi Informasi Pribadi / Privacy of Personal Information

9.4.1 Rencana Privasi / Privacy Plan

BSrE CA melindungi informasi pribadi dalam kaitan dengan Kebijakan Privasi yang dipublikasikan pada website BSrE CA, https://bsre.bssn.go.id/repository.

BSrE CA protect personal information in accordance with a Privacy Policy published on BSrE CA's website at https://bsre.bssn.go.id/repository.

Kebijakan Privasi sesuai dengan ketentuan peraturan perundangan-undangan Indonesia mengenai pelindungan data pribadi dan informasi dan transaksi elektronik. Kebijakan Privasi mendokumentasikan informasi pribadi yang dikumpulkan, bagaimana informasi tersebut disimpan dan diproses, dan kondisi yang membolehkan informasi tersebut untuk dibuka.

The Privacy Policy conform to the Indonesian laws and regulations concerning personal data protection and electronic information and transactions. The Privacy Policy document collected personal information, how it is stored and processed, and under what conditions the information may be disclosed.

Pemilik diberikan akses dan kemampuan untuk mengoreksi atau mengubah informasi pribadi atau organisasi melalui permintaan yang sah kepada BSrE CA. Informasi tersebut hanya bisa diberikan setelah BSrE CA melakukan langkah-langkah untuk mengautentikasi identitas dari pihak yang meminta.

The subscriber is given access and the ability to correct or change personal or organizational information through a legitimate request to BSrE CA. The information can only be given after BSrE CA takes steps to authenticate the identity of the requesting party.

BSrE CA hanya mengumpulkan data yang diperlukan untuk pendaftaran dan sertifikasi serta hanya menggunakan untuk tujuan tersebut. Secara khusus, BSrE CA tidak menggunakan data tersebut untuk tujuan komersial apapun.

BSrE CA only collects data necessary for registration and certification and only uses it for those purposes. Specifically, BSrE CA does not use such data for any commercial purposes.

9.4.2 Informasi yang Diperlakukan sebagai Privat / Information Treated as Private

BSrE CA melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Informasi pribadi dapat diungkapkan atas persetujuan Pemilik terhadap Pengandal. Arsip yang dikelola oleh BSrE CA tidak dirilis kecuali yang diizinkan pada bagian 9.4.1.

BSrE CA will protect all Subscribers personally identifiable information from unauthorized disclosure. Records of individual transactions may be released upon request of any Subscribers to BSrE CA or RA. The contents of the archives maintained by BSrE CA shall not be released except as allowed by Section 9.4.1.

BSrE CA menghapus secara langsung informasi pribadi Pemohon yang ditolak. BSrE CA hanya dapat menyimpan nama, email dan organisasi Pemohon disertai alasan penolakan.

BSrE CA immediately deletes the personal information of rejected Applicants. BSrE CA may only retain the name, email and organization of the Applicant along with the reason for rejection.

9.4.3 Informasi yang tidak Dianggap Privat / Information not Deemed Private

Informasi yang termasuk dalam Bagian 7 (Informasi sertifikat, CRL, dan Profil OCSP) dari CPS ini tidak termasuk dalam bagian 9.4.2.

Information of certificate, CRL and OCSP Profiles described in Section 7 is not subject to protection outlined in Section 9.4.2 above.

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

BSrE CA bertanggung jawab untuk menyimpan informasi privat sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan dapat berbentuk fisik maupun elektronik. *Backup* informasi privat dienkripsi setiap akan dipindahkan ke media backup.

BSrE CA is 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 Pemberitahuan dan Persetujuan untuk Menggunakan Informasi Privat / Notice and Consent to Use Private Information

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran termasuk informasi rahasia sehingga perlu persetujuan dari Pemohon supaya dapat menggunakan informasi tersebut. BSrE CA mengakomodir semua ketentuan terkait penggunaan informasi privat ke dalam Kebijakan Privasi untuk Pengguna Layanan BSrE. Kebijakan Privasi untuk Pengguna Layanan BSrE juga mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh BSrE CA.

Private information obtained from Applicants during the enrollment process is deemed private and permission is required from the Applicant to allow the use of such information. BSrE CA incorporates 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 BSrE CA.

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

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

BSrE CA does not disclose private information to any third party unless authorized by this policy, required by laws and regulations, or court order.

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 BSrE CA termasuk semua merek dagang dan hak cipta dari semua dokumen BSrE CA tetap menjadi milik tunggal dari BSrE CA. BSrE CA tidak melanggar hak kekayaan intelektual pihak lain.

BSrE CA's Intellectual Property Rights including trademarks, copyright and all documents remain as sole property of BSrE CA. BSrE CAs not violate intellectual property rights held by others.

9.6 Pernyataan dan Jaminan / Representations and Warranties

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

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

1. BSrE CA mematuhi ketentuan yang diatur dalam CPS ini;
2. BSrE CA menerbitkan dan memperbarui CRL sesuai ketentuan dalam CPS ini;
3. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CPS ini dan hanya Informasi yang telah diverifikasi yang ditampilkan di Sertifikat;
4. BSrE CA menampilkan informasi yang dapat diakses secara publik melalui repositori;
5. Kunci Privat BSrE CA terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;
6. Semua pernyataan yang dibuat oleh BSrE CA dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh BSrE CA; dan
7. Setiap Pemilik telah diwajibkan untuk

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

1. BSrE CA complies, in all material aspects, with the CPS;
2. BSrE CA publishes and updates CRL according to stipulations in this CPS;
3. All Certificates issued meet the minimum requirements and verified in accordance with this CPS and only verified information appears in the Certificate;
4. BSrE CA display information that can be accessed publicly through its repositories;
5. BSrE CA signing private key is protected and that no unauthorized person has ever had access to that private key;
6. All representations made by the BSrE CA in any applicable agreements are true and accurate, to the best knowledge of the applicable CA; and
7. Each Subscriber has been required to represent and warrant that all information

menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

supplied by the Subscriber in connection with, and/or contained in the Certificate is true.

9.6.2 Pernyataan dan Jaminan RA / RA Representations and Warranties

RA yang menjalankan fungsi pendaftaran seperti yang dijelaskan dalam klausul ini mematuhi ketentuan peraturan perundang-undangan, kebijakan ini, dan mematuhi CPS yang disetujui oleh *Policy Authority*. RA yang diketahui bertindak dengan cara yang tidak sesuai dengan kewajiban ini dapat dicabut tanggung jawabnya sebagai RA. RA menyatakan dan menjamin, bahwa:

1. Tidak ada kekeliruan dalam Sertifikat yang diketahui atau berasal dari entitas yang menyetujui permohonan pendaftaran Sertifikat;
2. Tidak ada kesalahan informasi dalam Sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran Sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat. RA memelihara bukti bahwa pemeriksaan (*due diligence*) telah dilakukan dalam memvalidasi informasi yang terdapat dalam Sertifikat;
3. BSrE CA mengharuskan semua RA untuk menjamin bahwa kegiatan registrasi yang dilakukan RA sesuai dengan CPS dan dituangkan dalam perjanjian RA; dan
4. Pemilik dikenakan kewajiban sebagaimana disebutkan dalam Bagian 9.6.3. Pemilik mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

RA carrying out the registration function as described in this clause shall comply with the provisions of laws and regulations, this policy, and comply with the CPS approved by the Policy Authority. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RAs responsibilities. An RA represents and warrants:

1. There are no fallacies on Certificate that have been known or came from the entity who gives an acknowledgement on Certificate application;
2. 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. RA maintains evidence that due diligence was exercised in validating the information contained in the Certificate;
3. BSrE CAs required all RAs to guarantee all registration activities that have been done by RAs comply with CPS and stated at the RA agreement; and
4. Obligations are imposed on Subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

9.6.3 Pernyataan dan Jaminan Pemilik Sertifikat Elektronik / Subcriber Representations and Warranties

Pemilik Sertifikat menjamin bahwa:

1. Setiap Sertifikat Elektronik yang dibuat menggunakan kunci privat serta berkorespondensi dengan kunci publik yang tercantum pada Sertifikat adalah merupakan tanda tangan elektronik pemilik dan sertifikat yang sudah disetujui serta secara operasional (tidak kadaluarsa dan telah dicabut) saat tanda tangan elektronik dibuat;
2. Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;
3. Sudah melakukan review terhadap informasi dari sertifikat;
4. Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;
5. Sertifikat Elektronik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS

Subscribers warrant that:

1. Each digital signature created using the Private Keys corresponding to the Public Key listed in the certificate is the digital signature of the Subscriber and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
2. Private Key is protected and that no unauthorized person has ever had access to the Subscriber's Private Key;
3. Have thoroughly reviewed the certificate information;
4. All information supplied by the Subscriber and contained in the certificate is true;
5. The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of

ini;
6. Segera memberitahukan BSrE CA dalam hal:
   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;
   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; dan
   c. menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam Sertifikat Elektronik setelah sertifikat dicabut;
7. Menanggapi instruksi BSrE CA terkait compromise atau penyalahgunaan Sertifikat Elektronik dalam kurun waktu 48 (empat puluh delapan) jam;
8. Menyetujui dan menerima bahwa BSrE CA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Kontrak Perjanjian atau jika BSrE CA menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti phising, penipuan atau pendistribusian *malware*;
9. Pemilik sertifikat adalah pengguna akhir yang bukan merupakan BSrE CA, serta tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat Elektronik untuk tujuan penandatangan Sertifikat Elektronik PSrE lain.

this CPS;
6. Immediately notify BSrE CA in the event that:
   a. request the revocation and termination of the use of the certificate and associated private key, if there are suspicious circumstances and misuse or leakage of the private key of the Subscriber associated with the Public Key included in the Certificate;
   b. submit a request for revocation of the Certificate and stop using it if any information in the Certificate is incorrect or becomes incorrect; and
   c. stop using the private key whose public key is listed in the Electronic Certificate after the Certificate is revoked;
7. Respond to BSrE CA instructions regarding compromise or certificates misuses within 48 (fourty eight) hours;
8. Acknowledges and accepts that BSrE CA is entitled to revoke the certificate immediately if the Subscriber violates the terms of the Subscriber Agreement or if BSrE CA discovers that the certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware; and
9. The Subscriber does not use the private key whose public key is mentioned in the Certificate to sign another PSrE because they are end users rather than BSrE CAs.

9.6.4 Pernyataan dan Perjanjian Pengandal / Relying Statements and Agreements

Pengandal menjamin bahwa:
1. Memiliki kemampuan teknis untuk menggunakan sertifikat;
2. Apabila perwakilan dari Pengandal menggunakan suatu sertifikat yang diterbitkan oleh BSrE CA, Pengandal harus secara benar memverifikasi informasi yang tercantum di dalam sertifikat sebelum digunakan dan menanggung akibat apapun yang terjadi jika lalai dalam melakukan hal tersebut;
3. Melaporkan langsung kepada RA yang berwenang ataupun BSrE CA, jika Pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat;

Relying Party warrants that :
1. Have the technical capability to use certificates;
2. If the representative from the Relying Party uses a certificate issued by BSrE 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;
3. Notify the appropriate RA or BSrE CA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised;

4. Mewajibkan 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 Pengandal yang ada pada CPS ini; dan
5. Mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

4. Required Relying Party to acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the certificate, that they are fully responsible for deciding to rely on the information or not, and they will carry the legal consequences from the failure to fulfil the obligation of the Relying Party as mentioned in this CPS; and
5. Comply with the provisions of this CPS and related agreements.

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

Tidak ada ketentuan.

No Stipulation

9.7 Pelepasan Jaminan / Disclaimers of Warranties

BSrE CA tidak menjamin:

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

BSrE CA does not warrant:

1. Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, BSrE CA disclaims any and all other possible warranties, conditions, or representations (express, implied, oral or written), including any warranty of merchantability or fitness for a particular use;
2. Misuse of a certificate that is inconsistent with its usage as shown in section 4.5;
3. The accuracy, authenticity, completeness or fitness of any information contained in test or demo certificates.

9.8 Pembatasan Tanggung Jawab / Limitations of Liability

9.8.1 Pembatasan Tanggung Jawab PSrE / CA Limitations of Liability

BSrE tidak bertanggung jawab atas penggunaan sertifikat yang tidak tepat, termasuk:

1. Kerugian yang diakibatkan oleh penggunaan Sertifikat Elektronik atau pasangan kunci yang tidak sesuai dengan yang ditetapkan dalam dokumen CPS ini;
2. Kerugian yang disebabkan oleh kondisi *force majeure*;
3. Semua kerusakan yang disebabkan oleh malware (seperti virus atau Trojans) diluar perangkat BSrE CA.

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

1. Losses caused by the use of Digital Certificates or key pairs that do not comply with those set forth in this CPS document;
2. Losses caused by the force majeure condition;
3. All damage caused by the Malware (i.e virus or Trojan) outside BSrE CA devices.

9.8.2 Pembatasan Tanggung Jawab RA / RA Limitation of Liability

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara BSrE CA kepada RA. Secara khusus, RA bertanggung jawab atas pendaftaran Pemilik.

The cap on RA liability is specified in the frame contract between BSrE CA and RA. In particular, the RA is liable for the registration of Subscribers

9.8.3 Pembatasan Tanggung Jawab Pemilik / Subscriber Limitation of Liability

Tanggung jawab Pemilik dan/atau batasannya diuraikan dalam perjanjian pemilik, dengan

The Subscriber's responsibilities and/or limitations are described in the subscribers

mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak. Pemilik secara khusus bertanggung jawab atas kerugian yang disebabkan oleh pelanggaran kelaikan (~~*due diligence*~~), seperti memindahtangankan passphrase dan token kepada orang lain ataupun tidak mencabut Sertifikatnya yang terkompromi.

agreement, with reference to the provisions of laws and regulations governing the relationship between the parties. In particular, the Subscriber is liable for damages caused by a breach of their due diligence, such as handing over a token and PIN to somebody else or not revoking his compromised Certificate.

9.9 Ganti Rugi / Indemnities

Penggantian kerugian diatur dalam perjanjian antar para pihak yang terlibat sebelum menggunakan layanan.

Compensation is regulated in the agreement between the parties involved before using the service.

9.9.1 Ganti Rugi oleh BSrE CA / Indemnification by an CAs

Kewajiban ganti rugi BSrE CA ditetapkan pada Kebijakan Jaminan BSrE CA.

BSrE CA indemnification obligation is stipulated in the BSrE CA Guarantee Policy.

9.9.2 Ganti Rugi oleh Pemilik Sertifikat / Indemnification by Subscriber

BSrE CA menyertakan persyaratan ganti rugi oleh Pemilik dalam CPS dan perjanjian pemilik. Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pemilik setuju untuk mengganti rugi dan membebaskan BSrE CA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya, dan segala tuntutan yang diakibatkan oleh:

1. Pelanggaran yang dilakukan oleh Pemilik terhadap perjanjian pemilik, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
2. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik;
3. Penggunaan Sertifikat oleh Pemilik untuk melakukan perbuatan melawan hukum;
4. Kegagalan Pemilik untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu pihak manapun;
5. Kegagalan Pemilik untuk melindungi Kunci Privat, menggunakan sistem elektronik yang tepercaya, atau mengambil langkah-langkah yang wajar untuk mencegah kebocoran, kehilangan, pengungkapan, perubahan, atau penggunaan tidak sah Kunci Privat; atau
6. Penggunaan nama oleh Pemilik (termasuk namun tidak terbatas pada *common name*, nama domain, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

BSrE CA include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements. To the extent permitted by applicable laws and regulations, Subscriber agrees to indemnify and hold CA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that CA may incur as a result of:

1. Violations committed by the Subscriber against the owner agreement, this CPS, or applicable laws, whether committed intentionally or unintentionally;
2. Invalid Private Key Usage due to Subscriber's negligence;
3. Use of the Certificate by the Subscriber to commit unlawful acts;
4. Failure of the Subscriber to disclose evidence in the Certificate application with the intent to deceive any party;
5. Failure of the Subscriber to protect the Private Key, use a trusted electronic system, or take reasonable steps to prevent leakage, loss, disclosure, alteration, or unauthorized use of the Private Key; or
6. Use of a name by the Subscriber (including but not limited to common name, domain name, or email address) that violates the Intellectual Property Rights of a third party.

9.9.3 Ganti Rugi oleh Pengandal / Indemnification by Relying Parties

BSrE CA menyertakan persyaratan ganti rugi oleh Pengandal dalam CPS dan Perjanjian

BSrE CA include its indemnification requirements for Relying Parties in its CPS

Pengandal. Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan BSrE CA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya dan segala tuntutan yang diakibatkan oleh:

1. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pihak Pengandal, CPS ini, atau hukum yang berlaku; dan
2. Pengandal tidak memeriksa status Sertifikat untuk menentukan apakah Sertifikat tersebut sudah kedaluwarsa atau sudah dicabut.

and its Relying Party Agreements. To the extent permitted by applicable laws and regulations, and any applicable contractual agreements, Relying Party agrees to indemnify and hold Airbus harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that Airbus may incur as a result of:

1. The Relying Party's failure to perform the obligations of a Relying Party; and
2. The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10 Jangka Waktu dan Pengakhiran / Term and Termination

9.10.1 Jangka Waktu / Term

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh BSrE CA melalui laman atau repositorinya.

This CPS is declared valid until there is further notification by BSrE CA through its website or repository.

9.10.2 Pengakhiran / Termination

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

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

Dalam hal terdapat perubahan CP PSrE Induk, dokumen Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan lainnya yang berdampak pada OID PSrE Indonesia, maka OID dalam CPS ini berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan dengan ketentuan CP PSrE Induk, Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan terkini lainnya.

When there are changes in Root CA's CP, OID Hierarchy document for Indonesian PKI, and/or other regulations which implicate the Indonesian CAs' OID, then OID in this CPS valid for maximum 12 (twelve) months or sooner, after adjusting to the new stipulation in Root CA's CP, OID Hierarchy document for Indonesian PKI, and/or other latest regulations.

9.10.3 Dampak Pengakhiran dan Ketentuan yang tetap Berlaku / Effect of Termination and Survival

BSrE CA mengomunikasikan kondisi, dampak dari pengakhiran CPS, dan juga kondisi keberlangsungan dari Sertifikat yang masih berlaku melalui laman situs web BSrE CA atau repositori BSrE CA.

BSrE CA will communicate the conditions and effect of this CPS termination and continuity of the issued certificate on its website or repository.

Meskipun CPS sudah tidak berlaku lagi, aturan terkait pelindungan data dan arsip informasi tetap dipatuhi.

Even once the CPS is no longer valid, the regulations pertaining to the laws on data protection and on archival of information are still observed.

9.11 Pemberitahuan Individu dan Komunikasi dengan Partisipan / Individual Notices and Communications with Participants

BSrE CA menyediakan media komunikasi bagi para pihak terkait melalui publikasi pada laman, email, dan dokumen baik dalam bentuk elektronik maupun kertas. BSrE CA memberi tanggapan paling lama 20 (dua puluh) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke BSrE CA

BSrE CA provides a communication medium for related parties through publication on the website, email, and documents in both electronic and paper form. BSrE CA will provide a response no later than 20 (twenty) working days through the same communication medium. Communication made to BSrE CA is

dialamatkan sesuai dengan yang tercantum pada Bagian 1.5.2.

addressed in accordance with the provisions in Section 1.5.2.

9.12 Perubahan atau Amendemen / Amendments

9.12.1 Prosedur untuk Amendemen / Procedure for Amendments

BSrE CA akan meninjau CPS ini setidaknya 1 (satu) kali setiap tahun. Perbaikan, pembaruan atau perubahan terhadap dokumen CPS dipublikasikan.
Segala perubahan CPS direviu dan disetujui oleh PA PSrE Induk. Perubahan CPS dilakukan sesuai dengan prosedur reviu dokumen.

BSrE CA will review this CPS at least 1 (one) time every year. Corrections, updates or changes to the CPS document are published.
All changes are reviewed and approved by the Policy Authority before insertion. CPS amendments are carried in accordance with the document reviewal procedure.

9.12.2 Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

BSrE CA menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika terjadi perubahan, CPS dipublikasikan paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.

BSrE CA announces appropriate notice on its website of any major or significant changes to this CPS as well as information about the period by when the revised CPS becomes effectively applicable. These CPS changes are made publicly available within 7 (seven) business days since approval.

9.12.3 Keadaan dimana OID harus diubah / Circumstances Under Which OID Must be Changed

Jika *Policy Authority* (PA) memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, maka PA akan memberitahukan terlebih dahulu kepada PA PSrE Induk. BSrE CA akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

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

9.13 Ketentuan Penyelesaian Perselisihan/Sengketa / Dispute Resolution Provisions

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara BSrE CA dengan pemilik sertifikat atau dengan entitas lain.

In case of dispute or controversy related performance, execution or the interpretation of the CPS, all parties will try to reach a peaceful settlement. The official provisions of the dispute are part of the contract agreed upon between BSrE CA and the Subscriber or other entities.

9.14 Hukum yang Mengatur / Governing Law

CPS ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan sertifikat BSrE CA ataupun produk/ layanan lainnya. Termasuk apabila sertifikat BSrE CA dipakai untuk kebutuhan komersil di negara lain tetap menerapkan aturan hukum di Indonesia.

This CPS applies Indonesian law to ensure a common understanding, regardless of the location of domicile or location of use of the BSrE CA certificate or other products/services. This includes the application of Indonesian law even if the BSrE CA certificate is used for commercial purposes in another country.

Para pihak, termasuk rekan BSrE CA, pemilik, Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.

The parties, including BSrE CA partners, subscribers, relying parties, may not waive the legal references specified above.

9.15 Kepatuhan atas Hukum yang Berlaku / Compliance with Applicable Law

BSrE CA mematuhi hukum yang berlaku di Indonesia. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data,

BSrE CA complies with applicable laws of Indonesia. Compliance includes, but is not limited to, hardware, software, systems, business information, data processes and all

dan semua kegiatan sehari-hari terkait operasi praktik bisnis.

related undertakings during the daily operations of business practices.

9.16 Ketentuan yang Belum Diatur / Miscellaneous Provisions

9.16.1 Seluruh Perjanjian / Entire Agreement

BSrE CA secara kontraktual mewajibkan semua RA yang terlibat dalam penerbitan Sertifikat untuk mematuhi CPS ini dan semua panduan yang terkait.

BSrE CA contractually obligate every RA involved with Certificate issuance to comply with this CPS and all related guidelines.

9.16.2 Pengalihan Hak / Assignment

Entitas yang beroperasi di bawah CPS ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari BSrE CA.

Entities operating under this CPS must not assign their rights or obligations without the prior consent of BSrE CA.

9.16.3 Keterpisahan / Severability

Jika ada pengaturan dalam CPS ini yang dinyatakan tidak sah oleh pengadilan, maka ketentuan lain tetap berlaku hingga CPS diperbarui. Proses pembaruan CPS dijelaskan pada Bagian 9.12.

If any provision of this CPS is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect until the CPS is updated. The process for updating this CPS is described in Section 9.12

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

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

BSrE CA can request compensation and reimbursement of attorney's fees from parties proven to have committed damages, losses and other losses caused by that party. BSrE CA's failure to implement this clause in one case does not eliminate the BSrE CA's right to continue to use this clause in the future or the right to use other clauses in this CPS. All matters related to waiver in court must be submitted in writing and signed by BSrE CA.

9.16.5 Keadaan Memaksa / Force Majeure

BSrE CA tidak bertanggung jawab atas kegagalan atau keterlambatan dalam kinerjanya dikarenakan penyebab yang berada di luar kendali yang wajar, termasuk namun tidak terbatas pada, bencana alam, tindakan otoritas sipil atau militer, kebakaran, wabah, banjir, gempa bumi, kerusuhan, keadaan perang, perang; kegagalan peralatan; listrik dan kegagalan jalur telekomunikasi; kurangnya akses Internet; sabotase; terorisme; tindakan pemerintahan atau setiap kejadian yang tidak terduga; dan tidak tersedianya, gangguan, atau keterlambatan telekomunikasi atau layanan pihak ketiga.

BSrE CA not be liable for any loss, cost, expenses, obligations, damages, or claims for failure or delay in its performance under this CPS due to causes that are beyond its reasonable control, including, but not limited to 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 and unavailability of interruption or delay in telecommunications or third party services.

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

BSrE CA has BCP and DRP with reasonable control in accordance with the capabilities of the BSrE CA.

9.17 Ketentuan Lain / Other Provisions

9.17.1 Versi CPS yang memiliki kekuatan hukum / Legally Binding Version of CPS

Versi Bahasa Indonesia dari CPS ini mengikat secara hukum. Versi Bahasa Inggris dari CPS ini hanya untuk tujuan informasi.	This Indonesian version of the CPS is legally binding. An English version of this CPS serves for informational purposes only.

Ditetapkan di Jakarta
Pada tanggal 27 April 2026

Lampiran A
DEFINISI / DEFINITIONS

Istilah / Term	Definisi / Definition
Sertifikat Certificate	Sertifikat Elektronik yang selanjutnya disebut Sertifikat adalah Sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh PSrE. Certificate is a digital certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions.
Penyelenggara Sertifikasi Elektronik (PSrE) Certification Authority (CA)	Penyelenggara Sertifikasi Elektronik berbentuk badan hukum Indonesia, berdomisili di Indonesia, dan telah mendapatkan pengakuan dari Menteri. A CA which possesses Indonesian legal entity, located in Indonesia, and recognized by the Minister.
Otoritas Pendaftaran Registration Authority	Pihak yang bekerja sama dengan PSrE Indonesia untuk meneruskan permohonan kepada PSrE Indonesia dalam hal pemeriksaan kebenaran identitas, perpanjangan masa berlaku, dan pemblokiran dan/atau pencabutan Sertifikat Elektronik memenuhi persyaratan. An entity which cooperates with an Indonesian CA to forward Certificate applications to the Indonesian CA on the condition that the identity verification, extension of validity period, and suspension and/or revocation of the Certificates fulfill the requirements.
Pemilik Subscriber	Pihak yang identitasnya tertera dalam Sertifikat Elektronik yang diterbitkan oleh PSrE dan sudah melalui proses verifikasi. An entity whose identity is stated in an Digital certificate issued by the CA and has been through a verification process.
Instansi Agency/ Government	Instansi Penyelenggara Negara yang selanjutnya disebut Instansi adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah, dan instansi lain yang dibentuk dengan peraturan perundang-undangan. A legislative, executive, and judicial institution at the central and regional levels and such other agencies established under laws and regulations.
Pengandal Relying Party	Setiap orang, organisasi, badan usaha, atau entitas yang mengandalkan keabsahan dari Sertifikat. Means a person, organisation, business entity, or entity relying on the validity of a certificate.
Kebijakan Sertifikat Elektronik Certificate Policies	Tata cara dan/atau prosedur yang ditulis dan digunakan oleh PSrE untuk penggunaan, pendaftaran, penerbitan, dan pencabutan Sertifikat Elektronik. Written procedures used by CA's for the use, registration, issuance, and revocation of Digital certificates.
Pernyataan Praktik Sertifikat Elektronik Certification Practice Statement	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat. One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Pasangan Kunci	Kunci Privat dan Kunci Publik yang mengacu ke entitas yang sama, yang memiliki karakteristik khusus, sehingga suatu pesan yang

	dienkripsi memakai Kunci Privat hanya dapat didekripsi dengan Kunci Publik pasangannya, dan sebaliknya.
Key Pair	Private Key and Public Key referring to the same entity, which possess certain characteristics, so that a message encrypted by a Private Key can only be decrypted by the corresponding Public Key, and vice versa.
Kunci Privat	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Digital dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait.
Private Key	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	Kunci dari Pasangan Kunci yang dapat diungkapkan secara terbuka oleh pemegang Kunci Pribadi terkait dan yang digunakan oleh Pihak yang Mengandalkan untuk memverifikasi Tanda Tangan Digital yang dibuat dengan Kunci Pribadi dan / atau untuk mengenkripsi pesan pemiliknya sehingga dapat didekripsi hanya dengan Private Key yang sesuai.
Public Key	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 corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Peran Tepercaya	Peran-peran yang melakukan fungsi yang sangat penting, dimana jika fungsi tersebut tidak dilakukan dengan benar dan sesuai, dapat menimbulkan dampak yang sangat buruk bagi tingkat kepercayaan PSrE.
Trusted Roles	Roles that perform critical functions which, if performed unsatisfactorily, can have an adverse impact upon the degree of trust provided by the CA
Kebocoran Kunci	Kunci Privat dikatakan dikompromikan jika nilainya telah diungkapkan kepada orang yang tidak berkepentingan, orang yang tidak sah memiliki akses ke sana, atau ada praktek teknis yang memungkinkan orang yang tidak berwenang mendapatkan nilainya.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.
Object Identifier	A unique alphanumeric or numeric identifier yang terdaftar di bawah Object Identifier standar International Organization for Standardization untuk objek atau kelas objek tertentu.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization’s applicable standard for a specific object or object class.
Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat.
Online Certificate Status Protocol	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Pemohon	Individu atau Badan Usaha atau Instansi yang mengajukan permohonan pembuatan atau perubahan Sertifikat. Setelah

Applicant	Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik atau PSrE Indonesia. The natural person or Business Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber or Subordinate CA
Penilaian Kelaikan Compliance Audit	Penilaian Kelaikan atau audit kepatuhan adalah suatu proses yang dilaksanakan oleh LS PSrE atau P2SE terhadap PSrE Indonesia, dengan mengacu kepada beberapa standar tentang PSrE yang telah diterbitkan oleh Kementerian Komunikasi dan Digital. A Compliance Audit is a process conducted by CA CAB or Root CA upon Indonesian CA, by referring to CA standards issued by Ministry of Communication and Digital.

AKRONIM

BCP	Business Continuity Plans
BSrE	Balai Besar Sertifikasi Elektronik
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DRP	Disaster Recovery Plans
EV	Extended Validation
FIPS	Federal Information Processing Standards (US Government)
FQDN	Fully-Qualified Domain Name
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IKP	Infrastruktur Kunci Publik
ITU	International Telecommunication Union
NDA	Non-Disclosure Agreement
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PSrE	Penyelenggara Sertifikat Elektronik
RA	Registration Authority
RFC	Request for Comment
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
VA	Validation Authority

Lampiran B
PROFIL SERTIFIKAT / CERTIFICATE PROFILE

1. Sertifikat BSrE CA / BSrE CA Certificate

Basic Certificate Fields	Value
Version	3
Signature Algorithm	SHA-384 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	BSRE CA DS G1
Subject: OrganizationName	Badan Siber dan Sandi Negara
Subject: CountryName	ID
Subject Alternative Name	N / A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Digital Signature Sign CRL Sign Certificate (CA)
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	CA: Yes Path Length Constraint: None
Public Key	RSA 4096 bits

2. Sertifikat Pemilik / Subscriber Certificate

Basic Certificate Fields	Value
Version	3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	BSRE CA DS G1
Issuer: O	Badan Siber dan Sandi Negara
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar)
Subject: OrganizationName	Nama Instansi Kerja
Subject: CountryName	ID
Description	AMS ID_Tanda Tangan Elektronik BSRE CA
Subject Alternative Name	N / A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Digital Signature Non-Repudiation
Extended Key Usage	Acrobat Authentic Documents
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	URI = https://va.bsre.go.id/bsrecadsg1.crl
Authority Info Access	Method = Certification Authority Issuer URI = https://va.bsre.go.id/bsrecadsg1.crt Method = OCSP URI = https://va.bsre.go.id/bsrecadsg1/ocsp
Certificate Policies	Policy OID: 2.16.360.1.1.1.5.1.4.3 Notice: Individu Instansi Online Level 3

	Policy OID: 2.16.360.1.1.1.3.11.2.0.1 URL: https://bsre.bssn.go.id/repository/kebijakan Policy OID: 2.16.360.1.1.1.9.1 Notice: Adobe Approved Trust List (AATL)
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	CA: No / Path Length Constraint: None
Public Key	RSA 2048 bits

3. Sertifikat Organisasi / Organization Certificate

Basic Certificate Fields	**Value**
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	BSRE CA DS G1
Issuer: O	Badan Siber dan Sandi Negara
Issuer: C	ID
Subject: CommonName	Nama Divisi / Unit Organisasi / Nama Sistem
Subject: OrganizationName	Nama Organisasi
Subject: CountryName	ID
Description	AMS ID_Segel Elektronik BSRE CA
Subject Alternative Name	N / A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Digital Signature, Non-Repudiation (c0)
Enhanced Key Usage	Unknown Key Usage (1.2.840.113583.1.1.5)
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	URL=https://va.bsre.go.id/bsrecadsg1.crl
Authority Information Access	Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://va.bsre.go.id/bsrecadsg1.crt Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://va.bsre.go.id/bsrecadsg1/ocsp
Certificate Policies	Certificate Policy: Policy Identifier=2.16.360.1.1.1.8.2 Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Segel Elektronik Instansi Certificate Policy: Policy Identifier=2.16.360.1.1.1.3.11.2.0.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://bsre.bssn.go.id/repository/kebijakan Certificate Policy: Policy Identifier=2.16.360.1.1.1.9.1 Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Adobe Approved Trust List (AATL)
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Subject Type=End Entity / Path Length Constraint=None
Public Key	RSA 2048 bits