PEDOMAN KEPALA BALAI BESAR SERTIFIKASI ELEKTRONIK

NOMOR 2 TAHUN 2024

TENTANG

KEBIJAKAN SERTIFIKAT DAN PERNYATAAN PRAKTIK SERTIFIKASI ELEKTRONIK *SECURE SOCKET LAYER* (SSL) BALAI BESAR SERTIFIKASI ELEKTRONIK

***CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT SECURE SOCKET LAYER* (SSL) BALAI BESAR SERTIFIKASI ELEKTRONIK**

Versi 2.1

Nomor dokumen	2 Tahun 2024
Tanggal pembuatan	20 Januari 2022
Tanggal Efektif	25 Oktober 2024
Jadwal Reviu	25 Oktober 2025
Klasifikasi	Biasa
Disahkan oleh	Dokumen Ini ditandatangani secara elektronik oleh: Kepala Balai Besar Sertifikasi Elektronik JONATHAN GERHARD T, S.ST Pembina (IV/a)

LEMBAR CATATAN REVIU

No.	Tanggal	Versi	Deskripsi	Oleh
1.	26 Juni 2022	1.0	Terbitan Pertama	*Policy Authority* BSrE
2.	9 Desember 2022	1.1	Terbitan Kedua - Penambahan Penamaan Sertifikat Root TLS/SSL - Penambahan Metode Validasi Otorisasi Domain	*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 repositori, level verifikasi, dan sertifikat badan usaha - 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 - Penambahan produk sertifikat klien	*Policy Authority* BSrE
5	22 Oktober 2024	2.1	Terbitan Kelima - Reviu Substansi	*Policy Authority* BSrE

DAFTAR ISI

BAB I
PENGANTAR / INTRODUCTION

1.1. Ringkasan / Overview

Dalam rangka mendukung pelaksanaan tugas dan fungsi Badan Siber dan Sandi Negara (BSSN) dalam upaya meningkatkan keamanan nasional di bidang siber dan sandi melalui pelayanan sertifikasi elektronik, BSSN membentuk Balai Besar Sertifikasi Elektronik (BSrE) sebagai unit pelaksana teknis penyelenggara sertifikasi elektronik yang dinamakan BSrE CA. Tujuan penyelenggaraan layanan BSrE CA adalah untuk memenuhi aspek-aspek keamanan dengan derajat kepastian dan risiko tinggi atas informasi dan/atau dokumen elektronik yang dikelola, dipertukarkan dan disimpan pada sistem-sistem elektronik melalui pemanfaatan Sertifikat Elektronik. Cakupan aspek keamanan informasi pada pemanfaatan Sertifikat Elektronik meliputi kerahasiaan, autentikasi, integritas dan anti penyangkalan.

Dokumen ini adalah CP/CPS TLS/SSL yang berisi acuan teknis dalam penyelenggaraan sertifikasi elektronik BSrE CA. Dokumen CP/CPS TLS/CCL 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, EV SSL Guidelines v1.6.2, dan ketentuan mengenai identitas digital mengacu pada NIST 800-63-3. BSrE CA mematuhi versi terkini dari Persyaratan Dasar dan Pedoman EV SSL pada Forum CA/Browser (http://www.cabforum.org).

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.

This document presents BSrE CA practices and procedures in managing BSrE CA 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, EV SSL Guidelines v1.6.2, and NIST 800-63-3 about digital identity provisions. BSrE CA complies with the latest version of the SSL Baseline and EV SSL Guidelines on the CA/Browser Forum (http://www.cabforum.org).

Persyaratan Dasar tersebut menjelaskan tentang persyaratan minimum yang harus dipenuhi BSrE CA untuk menerbitkan Sertifikat TLS/SSL. 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.

The baseline requirements explain the minimum requirement that should be met by BSrE CA to issue a TLS/SSL certificate. 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 Implementation of Electronic Certification, Regulation of the National Cyber and Crypto Agency Number 6 of 2024 regarding Organization and Work Procedure of the Balai Besar Sertifikasi Elektronik.

1.2. Nama dan Identifikasi Dokumen CP/CPS TLS/SSL BSrE CA / Document Name and Identification BSrE CA's TLS/SSL CP/CPS

Nama dokumen ini adalah CP/CPS TLS/SSL BSrE CA . OID dokumen ini adalah 2.16.360.1.1.1.3.11.2.0.2 dan versi dokumen ini adalah CP/CPS TLS/SSL BSrE CA Versi 2.1.

This Document's name is BSrE CA's TLS/SSL CP/CPS. Document's OID is 2.16.360.1.1.1.3.11.2.0.2 and version 2.1.

OID	Penggunaan / Usage
2.16.360.1.1.1.3.11	Sertifikat Instansi
2.16.360.1.1.1.3.11.2	BSrE CA
2.16.360.1.1.1.3.11.2.0.2	CP/CPS TLS/SSL
2.16.360.1.1.1.3.11.2.1.1	Sertifikat TLS/SSL
2.16.360.1.1.1.3.11.2.1.2	Sertifikat EV SSL
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
2.16.360.1.1.1.7.2	Sertifikat Badan Usaha/Organisasi

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

Tidak ada ketentuan

No stipulation.

1.3.1.2 BSrE CA

BSrE CA merupakan Penyelenggara Sertifikasi Elektronik Berinduk Instansi yaitu PSrE yang menerbitkan sertifikat kepada Pemilik yang merupakan entitas pemerintah Indonesia. 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 perundang-undangan yang berlaku di Indonesia tentang Sertifikasi Elektronik. BSrE CA tidak boleh berinduk kepada PSrE lain dan tidak boleh menjadi induk bagi PSrE lainnya.

BSrE CA is a Government Certification Authorities which issues certificates to Subscriber who are Indonesian Citizens that are employees of Government, or for the Government Institution itself. 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 pursuant to the prevailing 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.

1.3.2 Otoritas Pendaftaran (RA) / Registration Authorities

RA adalah personil yang bertanggung jawab melakukan pemeriksaan, penyetujuan 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 Electronic Certificate submitted by the owner (or prospective owner) of the BSrE CA Certificate.

1.3.2.1 Fungsi dari RA / Function of Registration Authorities

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

a. Memproses setiap permintaan layanan penerbitan, pembaruan dan pencabutan Sertifikat Elektronik;
b. Melakukan proses identifikasi, autentikasi dan pemeriksaan terhadap kelengkapan bukti dan berkas milik entitas yang mengajukan permintaan layanan Sertifikat Elektronik.

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

a. Processing every service request for issuance, renewal, and revocation of Certificates
b. Perform identification, authentication and examination of the completeness of evidence and files belonging to the entity submitting the Certificate service request.

1.3.2.2 Persyaratan Khusus RA untuk Sertifikat EV SSL / RA's Specific Requirement for EV SSL Certificate

Tidak ada ketentuan.

No stipulation

1.3.3 Pemilik Sertifikat Elektronik / Subscribers

Pemilik adalah pihak yang memohon dan berhasil mendapatkan Sertifikat Elektronik yang ditandatangani 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 Digital, Pemilik disebut sebagai Pemohon.

Subscribers are the party who request and successfully acquire a certificate signed by BSrE CA. Subscriber refers to the subject of the certificate that is contracted with the BSrE CA for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a subscriber is called 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.

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

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:

The "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.

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

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:

a. Checking for which purpose a certificate is

a. Memeriksa tujuan penggunaan sertifikat;
b. Melakukan verifikasi tanda tangan elektronik;
c. Memeriksa status pencabutan Sertifikat Elektronik termasuk di dalam CRL dan/atau OCSP; dan
d. Penyetujuan batas tanggung jawab dan jaminan

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

used
b. Verifying the digital signatures
c. checking certificate revocation status whether using CRL or OCSP; and
d. Acknowledgement of applicable liability caps and warranties.

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

1.3.5 Partisipan Lain / Other Participants

BSrE CA dapat menentukan Partisipan Lain yang berhubungan dengan operasional sertifikat.

BSrE CA may designate Other Participants that are related to the CA Operation.

1.3.4.1 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.

1.3.4.2 Penyedia layanan Pusat ata / 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 Elektronik / 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:

a. Autentikasi;
   Jenis Sertifikat yang disediakan adalah Sertifikat untuk otentikasi dua arah.
b. Tanda Tangan Elektronik & Non-Repudiasi;
   Jenis Sertifikat yang disediakan BSrE CA adalah Sertifikat Tanda Tangan elektronik.
c. Enkripsi;
   .

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:

a. Authentication
   The type of certificate provided is a certificate for two-way authentication.

b. Digital signature dan nonrepudiation
   The type of certificate provided BSrE CA is digital signature certificate.

Layanan BSrE CA yang menggunakan enkripsi adalah pengiriman elektronik tercatat

c. Encryption
BSrE CA services that use encryption are registered electronic transmissions.

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

BSrE CA menyediakan tingkat Jaminan yang dapat disesuaikan dengan kebutuhan transaksi, layanan tertentu, ataupun Pihak Pengandal. Sertifikat yang diterbitkan oleh BSrE CA adalah sertifikat dengan level verifikasi identitas yang sesuai denganperaturan 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 terpercaya berdasarkan proses yang dilakukan dengan keterlibatan manusia.

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 carried out with human 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 Bab 1.4.1 di atas.

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

1.5. Administrasi Kebijakan / Policy Administration

PA BSrE CA adalah Kepala BSrE.

PA of BSrE CA is the Head of BSrE

PA memiliki peran dan tanggung jawab sebagai berikut:

a. Menetapkan CP/CPS TLS/SSL; dan
b. Memastikan semua layanan, operasional dan infrastruktur BSrE CA yang didefinisikan dalam CP/CPS TLS/SSL telah dilakukan sesuai dengan persyaratan, representasi, dan
c. Menyetujui terjalinnya hubungan kepercayaan dengan IKP eksternal yang memiliki level verifikasi yang kurang lebih setara.

PA has roles and responsibilities as follows:

a Approves the TLS/SSL CP/CPS;
b Ensures that all aspects of the CA operational as described in the TLS/SSL CP/CPS are well performed in accordance with the requirements, representations; and
c. Approved the establishment of a trust relationship with external IKP which has a more or less equal level of verification.

1.5.1 Organisasi Pengelola Dokumen / Organization Administering the Document

CP, CPS, dan dokumen referensinya dikelola oleh: Balai Besar Sertifikasi Elektronik Jl. Harsono RM No.mor 70, RT.2/RW.4, Ragunan, Kec. Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550 E-mail : info.bsre@bssn.go.id	This CP, CPS, and documents referenced herein are maintained by : Balai Besar Sertifikasi Elektronik Jl. Harsono RM No.mor 70, RT.2/RW.4, Ragunan, Kec. Ps. Minggu, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12550 E-mail : info.bsre@bssn.go.id

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	Head of Balai Besar Sertifikasi Elektronik Web BSrE : https://bsre.bssn.go.id Telegram: t.me/infobsre Email: info.bsre@bssn.go.id

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

PA BSrE CA menentukan kesesuaian konten CPS dan kesesuaian antara CPS dengan CP.	PA of BSrE CA determines suitability of this CPS and the conformance of the CPS to CP.

1.5.4 Prosedur Persetujuan CP/CPS TLS/SSL / TLS/SSL CP/CPS Approval Procedures

PA menyetujui CP/CPS TLS/SSL dan segala amandemen / perubahannya. Amandemen / perubahan dibuat dengan mengubah seluruh CP/CPS TLS/SSL atau dengan mempublikasikan adendum. BSrE CA menentukan apakah amandeman / perubahan ke CP/CPS TLS/SSL ini memerlukan pemberitahuan atau perubahan OID.	PA approves TLS/SSL CP/CPS and any amendments. Amendments are made by either updating the entire TLS/SSL CP/CPS or by publishing an addendum. BSrE CA determines whether an amendment to this TLS/SSL CP/CPS requires notice or an OID change.

1.6. Definisi dan Akronim / Definitions and Acronyms

Lihat Lampiran A untuk tabel akronim dan definisi.	See Appendix A for a table of acronyms and definitions.

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

2.1 Repositori / Repositories

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

a. Sertifikat BSrE CA;
b. CRL;
c. CP/CPS TLS/SSL; dan
d. Dokumen kebijakan lainnya.

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

a. BSrE CA's Certificate;
b. CRL;
c. TLS/SSL CP/CPS; and
d. The other policy document.

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 pad https://bsre.bssn.go.id/repository.

BSrE CA maintains a repository accessible through the Internet, in which it publishes the certificate of BSrE CA (type X.509.v3), the current CRL, the document of CP/CPS. Authorized BSrE CA's repository can be accessed at https://bsre.bssn.go.id/repository.

2.3 Periode Waktu Publikasi / Time Period of Publication

Versi terbaru dari dokumen CP/CPS TLS/SSL BSrE CA tersedia dalam jangka waktu maksimum 7 hari sejak ditetapkan. BSrE CA mempublikasikan informasi CRL secara reguler dan terjadwal sebagaimana diatur dalam bagian 4.9.7.

The latest version of BSrE CA's TLS/SSL CP/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 memberikan akses baca yang tidak dibatasi pada repositori dan menerapkan kendali logis dan fisik untuk mencegah akses penulisan yang tidak berhak pada repositori tersebut

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

BAB III
IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION

3.1 Penamaan / Naming

3.1.1 Tipe Nama / Types of Names

BSrE CA akan membuat dan menandatangani Sertifikat Elektronik dengan subyek nama yang berbeda / DN yang tidak boleh kosong dan memenuhi standar ITU X.500. Berikut tabel penjelasan DN BSrE CA dan DN pemilik sertifikat.

BSrE CA will generate 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 Root TLS/SSL	C=ID O= Badan Siber dan Sandi Negara; CN=Root BSrE CA TLS/SSL G1
Sertifikat CA	C=ID O=Badan Siber dan Sandi Negara; CN= BSrE CA TLS/SSL G1;
Sertifikat TLS/SSL	C=ID O={Nama Organisasi}[1] CN={Nama Hostname} D={XXYYYYZZZZZZZZZZ_TLS}
Sertifikat EV SSL	C=ID O={Nama Organisasi}[1] CN={Nama Hostname} SERIALNUMBER={Dasar Hukum Pendirian Instansi} BUSINESSCATEGORY={Instansi Pemerintah} JURISDICTIONOFINCORPORATIONCOUNTRY=ID D={XXYYYYZZZZZZZZZZ_EV TLS}
Sertifikat Klien	CN={Nama Sistem}[2] O={Nama Organisasi} C=ID Description={XXYYYYZZZZZZZZZZ_Sertifikat Klien}

Catatan:
AMS ID = {XXYYYYZZZZZZZZZZ_produk}
XX = OID CA
Y = 4 Digit OID RA
Z = 10 Digit random character menggunakan random generator
1 = string maksimum 25 karakter sesuai Dasar Hukum Pendirian Instansi
2 = string maksimum 25 karakter sesuai Surat Rekomendasi/Surat Keputusan

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

Sertifikat yang diterbitkan sesuai dengan CP/CPS TLS/SSL 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 TLS/SSL CP/CPS are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates shall identify the person or object to which they are assigned in a meaningful way.
Nama subjek dan penerbit yang terkandung dalam Sertifikat bermakna dalam arti bahwa PSrE Induk memiliki cukup bukti yang menunjukkan keterkaitan antara nama dengan PSrE Indonesia. Untuk mencapai tujuan ini, penggunaan nama diotorisasi oleh PSrE Indonesia yang sah atau perwakilan resmi dari PSrE Indonesia yang sah.	The subject and issuer name contained in a Certificate is meaningful in the sense that the Root CA has proper evidence of the existent association between these names and the entities to which they belong. To achieve this goal, the use of a name is authorized by the rightful owner (Indonesian CA) or its legal representative

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 shall 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 Penggunaan Merk Dagang dalam Sertifikat Elektronik / Use of Trademarks in Electronic Certification

Pemilik tidak diperbolehkan mengajukan permohonan sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. BSrE CA tidak perlu memverifikasi hak pemohon untuk penggunaan merek dagang. Pemilik bertanggung jawab untuk memastikan keabsahan penggunaan dari nama yang dipilih.	Subscriber may not request certificates with any content that infringes the intellectual property rights of another party. BSrE CA will not verify trademark use during certificate application processing. The owner is responsible for ensuring the legitimacy of the use of the chosen name.
BSrE CA dapat menolak permohonan atau melakukan pencabutan Sertifikat yang menjadi bagian dari konflik merek dagang.	BSrE CA may reject any application or require revocation of any certificate that is 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

Metode untuk membuktikan kepemilikan kunci privat pemilik adalah dengan membandingkan nomor seri sertifikat Pemilik dengan data yang tercatat pada server aplikasi untuk mendapatkan PKCS#10 sehingga selanjutnya dapat dibandingkan antara Kunci Publik pada sertifikat dengan Kunci Publik pada PKCS#10.	The method to prove possession of a Subscriber's private key is by comparing the Subscriber's serial number certificate with the data recorded on the application server to get PKCS #10 so that it can be compared between the public key on the certificate and the public key on PKCS # 10.

3.2.2 Autentikasi Identitas Organisasi / Authentication of Organization Identity

RA atau Verifikator melakukan pemeriksaan untuk setiap informasi identitas wewenang / organisasi yang mengajukan permohonan Sertifikat Elektronik. Proses autentikasi identitas wewenang / organisasi dapat dilakukan secara jarak jauh (*remote/online*) antara RA atau Verifikator dengan pemohon.	RA performs verification of the applicant's information. The verification process may be conducted online between RA and the applicant.
Pemohon wajib menyampaikan surat rekomendasi dari organisasi. Autentikasi identitas organisasi pemohon terdiri dari:	The applicant must submit a letter of recommendation from his organization. Authentication of the applicant's organizational identity consists of:

3.2.2.1 Identitas / Identity

RA akan memverifikasi identitas organisasi yang diajukan oleh pemohon. RA akan menetapkan apakah identitas, alamat, dan nama domain sesuai dengan informasi yang ada pada database pihak ketiga dan atau sumber terpercaya.	RA verifies the identity of applicant's organization. RA determine conformity identity, address and domain name with the information contained in third party databases and/or trusted sources

3.2.2.2 DBA/Tradename

Jika dalam informasi identitas termasuk juga DBA / Tradename, RA memverifikasi DBA / Tradename pemohon.	If the identity information also includes a DBA/Tradename, the RA verifies the applicant's DBA/Tradename.

3.2.2.3 Verifikasi Negara

Verifikasi negara dilakukan pada bagian 3.2.2.1.	Country verification is carried out in section 3.2.2.1.

3.2.2.4 Validasi Otoritas Domain

BSrE CA memvalidasi setiap FQDN menggunakan minimal satu cara/metode di bawah ini.	BSrE CA validates each FQDN using at least one method below.

3.2.2.4.1 Validasi Kontak Domain / Validating the Applicant as a Domain Contact

Tidak ada ketentuan.

No stipulation.

3.2.2.4.2 Email, Fax, SMS dari Kontak Domain / Email, Fax, SMS to Domain Contact

Tidak ada ketentuan.

No stipulation.

3.2.2.4.3 Nomor Telepon dari Kontak Domain / Phone Contact with Domain Contact

Tidak ada ketentuan.

No stipulation.

3.2.2.4.4 Email ke Kontak Domain / Email to Domain Contact

a. BSrE CA mengirimkan email berisi link approval ke alamat email Registrant Domain.
b. Jika Email Registrant Domain tidak dapat dibaca di Whois record, maka Pemohon diharuskan menghubungi pengelola domain untuk mempublikasi sementara hingga dapat terbaca di Whois Record dan BSrE CA mengirimkan ulang link approval ke email Registrant Domain tersebut.
c. Jika Email Registrant Domain tetap tidak bisa terbaca, maka Pemohon dapat menggunakan email alternatif yang disarankan di bawah ini:
   - admin@namadomain.com
   - administrator@namadomain.com
   - hostmaster@namadomain.com
   - postmaster@namadomain.com
   - webmaster@namadomain.com

a. BSrE CA sends an email containing an approval link to The Registrant Domain email address.
b. If the Registrant Domain Email cannot be seen in the Whois record, then the Applicant should contact the domain management to publish the Registrant Domain email address in Whois record.
c. If the Registrant Domain Email is still unreadable, then the Applicant may use the alternative email suggested below:
   - admin@namadomain.com
   - administrator@namadomain.com
   - hostmaster@namadomain.com
   - postmaster@namadomain.com
   - webmaster@namadomain.com

3.2.2.4.5 Dokumen Otorisasi Domain

Tidak ada ketentuan.

No stipulation.

3.2.2.4.6 *Agreed-Upon Change to Website*

Tidak ada ketentuan.

No stipulation.

3.2.2.4.7 Perubahan DNS

Tidak ada ketentuan.

No stipulation.

3.2.2.4.8 Alamat IP

Mengonfirmasi kepemilikan Pemohon atas FQDN dengan memastikan bahwa pemohon memiliki Alamat IP yang berasal dari DNS Lookup, sesuai dengan ketentuan pada bagian 3.2.2.5.

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP Address returned from a DNS lookup in accordance with 3.2.2.5

Setelah FQDN divalidasi menggunakan metode ini, BSrE CA mungkin tidak menerbitkan Sertifikat untuk FQDN untuk tingkat domain di atasnya. Metode ini tidak cocok untuk memvalidasi Nama Domain Wildcard.	Once the FQDN has been validated using this method, the BSrE CA also issue Certificates for FQDNs for higher level domain levels that end in the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 *Test Certificate*

Tidak ada ketentuan.	No stipulation.

3.2.2.4.10 TLS Menggunakan Nomor Acak / TLS Using a Random Number

Tidak ada ketentuan.	No stipulation.

3.2.2.4.11 *Any Other Method*

Tidak ada ketentuan.	No stipulation.

3.2.2.4.12 *Validating Applicant as a Domain Contact*

Tidak ada ketentuan.	No stipulation.

3.2.2.4.13 Email ke CAA DNS / Email to DNS CAA

Tidak ada ketentuan.	No stipulation.

3.2.2.4.14 Email ke TXT DNS / Email to DNS TXT

a. BSrE CA mengirimkan email berisi random value (bsreca tls/ssl-domain-verification=[kodeCA])	a. BSrE CA sends email that contain random value (bsreca tls/ssl-domain-verification=[kodeCA])
b. Pemohon menambahkan random value yang diberikan BSrE CA pada record DNS nya.	b. The applicant adds the random value provided by the BSrE CA to their DNS record.
c. BSrE CA mengecek record tersebut dengan tools dnschecker, dan memastikan bahwa random value yang dimasukan sudah sesuai.	c. BSrE CA checks the record with the dnschecker tool, and ensures the random value entered is correct.

3.2.2.4.15 Kontak Telepon ke Domain / Phone with Domain Contact

Tidak ada ketentuan.	No stipulation.

3.2.2.4.16 Kontak Telepon TXT DNS Record

Tidak ada ketentuan.	No stipulation.

3.2.2.4.17 Kontak Telepon CAA DNS

Tidak ada ketentuan.	No stipulation.

3.2.2.4.18 *Agreed Upon Change to Website* – V2

Tidak ada ketentuan.	No stipulation.

3.2.2.4.19 *Agreed Upon Change to Website* – ACME

Tidak ada ketentuan.	No stipulation.

3.2.2.4.20 TLS Using ALPN

Tidak ada ketentuan.	No stipulation.

3.2.2.5 Otentikasi dari Alamat IP / Authentication of an IP Address

Bagian ini mendefinisikan proses dan prosedur untuk memvalidasi kepemilikan Pemohon atas Alamat IP yang tercantum dalam Sertifikat.	This section defines the permitted processes and procedures for validating the Applicant's ownership or control of an IP Address listed in a Certificate.
BSrE CA akan mengonfirmasi bahwa sebelum penerbitan, BSrE CA telah memvalidasi setiap Alamat IP yang tercantum dalam Sertifikat menggunakan setidaknya satu metode yang ditentukan di bagian ini.	The BSrE CA will confirm that prior to issuance, the BSrE CA has validated each IP Address listed in the Certificate using at least one of the methods specified in this section.

3.2.2.5.1 Agreed-Upon Change to Website

Tidak ada ketentuan.	No stipulation.

3.2.2.5.2 Email, Fax, SMS dari Kontak Domain / Email, Fax, SMS to Domain Contact

Tidak ada ketentuan.	No stipulation.

3.2.2.5.3 *Reverse Address Lookup*

Mengkonfirmasi kepemilikan pemohon atas Alamat IP dengan mendapatkan nama domain yang terkait dengan alamat IP melalui lookup reverse-IP pada alamat IP dan kemudian memverifikasi kepemilikan atas FQDN menggunakan metode pada bagian 3.2.2.4.	Confirm the Applicant's control over the IP Address by obtaining a Domain Name associated with the IP Address through a reverse-IP lookup on the IP Address and then verifying control over the FQDN using a method permitted under Baseline Requirements section 3.2.2.4.

3.2.2.5.4 *Any Other Method*

Tidak ada ketentuan.	No stipulation.

3.2.2.5.5 Nomor Telepon dari Kontak Domain / Phone Contact with Domain Contact

Tidak ada ketentuan.	No stipulation.

3.2.2.5.6 Metode ACME "http-01" untuk Alamat IP / ACME "http-01" method for IP Address

Tidak ada ketentuan.	No stipulation.

3.2.2.5.7 Metode ACME "tls-alpn-01" untuk Alamat IP / ACME "tls-alpn-01" method for IP Addresses

Tidak ada ketentuan.	No stipulation.

3.2.2.6 Validasi *Wildcard* / Wilcard Validation

Memastikan FQDN memiliki tanda bintang berada di sebelah kiri dari nama domain, sebagai contoh *.bssn.go.id.	Ensure that the FQDN has an asterisk to the left of the domain name, for example *.bssn.go.id.

3.2.2.7 Akurasi Sumber Data / Data Source Accuracy

Sebelum menggunakan sumber data, RA harus mengevaluasi sumber data tersebut untuk realibilitas, akurasi dan ketahanan dari penambahan atau pemalsuan.	Before using a data source, the RA must evaluate the data source for reliability, accuracy and robustness from addition or falsification.

3.2.2.8 CAA *Records*

CAA records diatur ketentuannya pada bagian 4.2.4.	CAA records Policy is stated in section 4.2.4

3.2.2.9 Otentikasi Alamat Email / Authentication of Email Address

BSrE CA mengkonfirmasi kepemilikan pemohon atas alamat email menggunakan metode di bawah ini. a. Mengirimkan URL termasuk nilai acak ke alamat email dan menerima link acknowledgement, kemudian masuk ke dalam URL tersebut. b. Menggunakan proses validasi domain pada bagian 3.2.2.4 untuk menunjukkan kepemilikan atas FQDN. Ketika terverifikasi, RA dapat menyetujui penerbitan Sertifikat yang berisi alamat email untuk FQDN atau nama domain terkait.	BSrE CA confirms the applicant's ownership of the email address using the method below. a. Sending a URL including a random value to the email address and then receiving an acknowledgement click-through with passphrase on the web page utilizing the random value URL; b. Using a domain validation process from section 3.2.2.4 to demonstrate control over or right to use an FQDN. Once verified, the Enterprise RA can approve issuance of Certificates containing email addresses under that FQDN or associated Base Domain Name

3.2.2.10 Otentikasi *Registered Trademark*

Tidak ada ketentuan	No stipulation.

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.	The RA or Verifier must carry out checks for any identifying information of individuals applying for Certificates. The individual identity authentication process can be carried out remotely/online between the RA or Verifier and the applicant.

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

Informasi yang tidak bisa diverifikasi tidak boleh disertakan di dalam sertifikat.	Information that is not verified shall not be included in certificates.

3.2.5 Validasi Otoritas / Validation of Authority

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

Re-key Pemilik diperkenankan untuk mengajukan permohonan rekey sebelum sertifikat kedaluwarsa sesuai bagian 4.7. BSrE CA dapat melakukan validasi ulang terhadap Pemohon sesuai bagian 3.2.	Subscribers may request re-key of a certificate prior to a certificate's expiration as per section 4.7. BSrE CA may perform some revalidation of the Applicant according to section 3.2.

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

Sebelum masa berlaku Sertifikat berakhir, Pemilik dapat meminta penggantian kunci yang selanjutnya disebut re-key dan Pemilik harus diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau menggunakan proses pemeriksaan identitas awal sebagaimana diatur pada bagian 3.2.	Before the validity period of the Certificate expires, The Subscriber may request a key replacement, hereinafter referred to as a re-key and the Owner must be authenticated by signing using a valid Certificate or using the initial identity check process as stipulated in section 3.2.

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

Jika suatu sertifikat elektronik telah dicabut, maka tidak dapat dilakukan pembaruan sertifikat elektronik. Pemilik Sertifikat Elektronik harus melakukan permohonan penerbitan ulang berdasarkan ketentuan BSrE CA.	If an certificate has been revoked, it cannot be renewed. The subscriber should make a request for reissuance based on the provisions of the BSrE CA.

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: a. Identitas pemilik Sertifikat Elektronik; b. Tipe, nomor seri, dan informasi pada Sertifikat Elektronik; c. Alasan pengajuan permohonan pencabutan.	RA identify and authenticate the revocation request by checking the following: a. Identity of Subscribers; b. Type, serial number, and information on the Certificate; c. 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 menerbitkan sertifikat bagi pemohon warga negara Indonesia yang merupakan pegawai Instansi dan/atau Instansi. Pihak yang berhak mengajukan permohonan sertifikat elektronik adalah Individu yang mewakili sistem elektronik/aplikasi.	BSrE issues certificates for applicants who are Indonesian citizens who are employees of Government and/or Government. Parties entitled to apply for certificates are individuals who represent electronic systems / applications.

4.1.2 Proses Pendaftaran dan Tanggung Jawab / Enrollment Process and Responsibilities

Seluruh komunikasi yang dilakukan pada proses pendaftaran dapat diautentikasi dan terlindungi dari ancaman-ancaman terkait modifikasi informasi secara tidak sah. Data yang disampaikan terkait dengan informasi pribadi dilindungi oleh BSrE CA. Jika menggunakan komunikasi elektronik, maka digunakan mekanisme kriptografi dengan kekuatan pasangan Kunci Publik/Privat yang sepadan. Namun jika komunikasi menggunakan media non elektronik, tetap harus melindungi kerahasiaan dan keutuhan data.	All communication during the registration process can be authenticated and protected from threats related to unauthorized modification of information. The submitted data related to personal information is protected by BSrE CA. In electronic communication, a cryptographic mechanism is used with adequate strength of the Public/Private Key pair. However, in non-electronic communication, the confidentiality and integrity of the data should be protected.
Proses pendaftaran meliputi langkah-langkah sebagai berikut: a. Pemohon sertifikat elektronik harus melengkapi berkas pendaftaran dan dokumen lain yang dibutuhkan secara akurat; dan b. Pembuatan CSR menggunakan aplikasi pembuat file CSR dari BSrE CA.	The registration process includes the following steps: a. The applicant have to complete the registration files and other documents required accurately; and b. Creating a CSR uses the CSR file generator application from BSrE CA.

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 harus memenuhi persyaratan yang ditentukan seperti yang tertera pada bagian 3.2.	The identification and authentication of the Subscriber shall meet the requirements specified in sections 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 dapat dilakukan karena sebab-sebab sebagai berikut:

a. Informasi dalam permohonan Sertifikat Elektronik tidak dapat diidentifikasi atau tidak autentik.
b. Pemohon Sertifikat Elektronik tidak melengkapi dokumen-dokumen sesuai dengan ketentuan.
c. Pemohon Sertifikat Elektronik tidak melakukan respon atas suatu pemberitahuan dari BSrE dalam jangka waktu tertentu.
d. Hal-hal lain yang berpotensi dapat merugikan pihak BSrE.

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 reasons:

a. The information in the Certificate application is unidentifiable or inauthentic.
b. The Certificate Applicant does not complete the documents in accordance with the provisions.
c. The Certificate Applicant does not respond to a notification from BSrE within a certain period of time.
d. Other potentially harmful things to BSrE.

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

Tidak ada ketentuan batas waktu bagi Pemohon untuk melakukan permohonan sertifikat elektronik. BSrE CA memproses permohonan dan menerbitkan Sertifikat Elektronik dalam jangka waktu maksimal 3 hari kerja semenjak disetujuinya permohonan sertifikat tersebut.

There is no time limit for the Applicant to apply for a certificate. BSrE CA processes an applications and issues Certificates within a maximum period of 3 working days after approval of certificate applications.

4.2.4 CAA *Records*

Sebelum menerbitkan Sertifikat TLS/SSL atau Sertifikat EV SSL, BSrE CA memeriksa CAA Records untuk setiap DNS Name pada ekstensi subjectAltName dari Sertifikat TLS/SSL atau Sertifikat EV SSL, sesuai dengan RFC 8659.

Before issuing a TLS/SSL Certificate or EV SSL Certificate, BSrE CA checks the CAA Records for each DNS Name in the subjectAltName extension of the TLS/SSL Certificate or EV SSL Certificate, according to RFC 8659.

Jika di dalam CAA record belum terdapat BSrE CA, maka sebelum Sertifikat TLS/SSL dan EV SSL diterbitkan, pemohon dapat menambahkan BSrE CA pada CAA record. Jika di dalam CAA record pemohon tidak menambahkan BSrE CA, dan Sertifikat TLS/SSL pada FQDN sudah terdaftar di CA lain, maka permohonan penerbitan Sertifikat TLS/SSL dan EV SSL akan ditolak.	If the CAA record does not yet contain a BSrE CA, then before the TLS/SSL and EV SSL certificates are issued, the applicant may add the BSrE CA to the CAA record. If in the CAA record the applicant does not add the BSrE CA, and the TLS/SSL Certificate on the FQDN has already been registered with another CA, then the application for the issuance of TLS/SSL and EV SSL Certificates will be rejected.

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 harus diperiksa untuk memastikan semua field dan ekstensi telah diisi dengan benar sesuai bagian 3.2.3.	BSrE CA verifies the source of a Certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated according to section 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 dengan pada bagian 2.2.	BSrE CA authenticates the Certificate request, ensures that the Public Key is bound to the correct Applicant, obtains a proof of possession of the Private Key, then generates a certificate applicant. BSrE CA publishes its Certificate to a repository according to in section 2.2.

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.

4.4 Penerimaan Sertifikat / Certificate Acceptance

4.4.1 Sikap yang Dianggap Menerima Sertifikat / Conduct Constituting Certificate Acceptance

BSrE CA mendapatkan 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 received the 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 dipublikasikan sesuai dengan bagian 2.1. dan 2.2.	BSrE CA's Certificate is published in accordance with section 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

Penggunaan kunci privat mengacu pada bagian 9.6.3.	The Subscriber may entrust his Private Subscriber shall conform to section 9.6.3.

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

Tidak Ada Ketentuan.	No stipulation.

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:

a. Sertifikat lama yang akan diganti belum dicabut atau belum terkompromi atau belum kadaluarsa;
b. BSrE CA menerbitkan Sertifikat baru setelah Pemilik memberi persetujuan untuk membangkitkan Pasangan Kunci baru dan terasosiasi dengan Sertifikat tersebut;
c. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi; dan
d. Apabila kunci privat pemilik terkompromi atau sertifikat kadaluarsa, pemilik dapat mengajukan permohonan baru sebagaimana diatur pada bagian 4.1.

BSrE CA re-keys the certificate Subscriber during:

a. The old certificate to be re-keyed has not been revoked or compromised or expired;
b. BSrE CA issues a new Certificate after the subscriber approve the generation new Key Pair that is associated with the Certificate;
c. All details in the Certificate remain accurate and do not require new or additional validations; and
d. 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.

4.7.2 Pihak yang Dapat Meminta Sertifikasi 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 dalam waktu 30 hari ke depan masa berlaku Sertifikat Elektroniknya akan habis.

Subscriber or a Government representative, RA, and BSrE CA may apply certificate re-key within the next 30 days the validity period of the Certificate expired.

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).

When processing a re-key Certificate issuance application, the validity of the application is checked before being process (according to section 4.3).

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

Setelah re-key Sertifikat berhasil dilakukan, maka BSrE CA akan memberitahukan Pemohon Sertifikat bahwa penerbitan Sertifikat telah berhasil dilakukan melalui media komunikasi yang ditentukan BSrE CA, selambatnya dalam jangka waktu 5 (lima) hari kerja.	After the Certificate re-key, BSrE CA notifies the Applicant that the Certificate has been successfully issued through communication media specified by BSrE CA, no later than 5 (five) working days.

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

BSrE CA tidak mengizinkan modifikasi detil sertifikat. Apabila terjadi kesalahan dalam penerbitan Sertifikat, maka BSrE CA akan melakukan pencabutan Sertifikat dan menerbitkan Sertifikat baru yang sesuai dengan ketentuan yang diatur pada CP/CPS TLS/SSL ini.	BSrE CA does not allow modification of certificate details. If an error occurs in the issuance of the Certificate, BSrE CA revoke the Certificate and issue a new Certificate in accordance with the provisions stipulated in this CP/CPS TLS/SSL.

4.8.1 Keadaan yang Menyebabkan Modifikasi Sertifikat / Circumstance for Certificate Modification

Tidak ada ketentuan.	No stipulation.

4.8.2 Pihak yang Dapat Mengajukan Permohonan Modifikasi Sertifikat / Entities May Request Certificate Modification

Tidak ada ketentuan.	No stipulation.

4.8.3 Pemrosesan Permohonan Modifikasi Sertifikat / Processing Certificate Modification Request

Tidak ada ketentuan.	No stipulation.

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

Tidak ada ketentuan.	No stipulation.

4.8.5 Sikap yang dianggap sebagai Penerimaan Modifikasi Sertifikat / Conduct Constituting Acceptance of Modified Certificate

Tidak ada ketentuan. | No stipulation.

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

Tidak ada ketentuan. | No stipulation.

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

Tidak ada ketentuan. | No stipulation.

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:

a. 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.
b. Pemilik Sertifikat Elektronik masih memiliki Sertifikat Elektronik dan kunci privat yang berelasi namun tidak mengingat/lupa *passphrase* untuk mengakses Sertifikat Elektronik miliknya;
c. Informasi apapun dalam sertifikat menjadi tidak valid;
d. Terdapat perubahan data identitas pada Sertifikat Elektronik;
e. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Kepemilikan;
f. Instansi dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Kerja Sama;
g. Pemilik atau instansi meminta sertifikatnya dicabut.
h. BSrE CA telah berhenti beroperasi;

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

a. The Subscriber has evidence that intentionally or unintentionally his Private Key has been lost, stolen, known, or misused by another party;
b. The Subscriber still has Certificate and private key but does not remember the passphrase to access his Certificate;
c. Any information in the certificate becomes invalid
d. There is identity data change in the Certificate;
e. The Subscriber can be shown to have violated the stipulations of its Subscriber Agreement.
f. The Government Institution can be shown to have violated the stipulations of its Cooperation Agreement.
g. The Subscriber or Government Institution asks for his/her certificate to be revoked.
h. BSrE CA operation is terminated;

i. BSrE CA mengetahui keadaan yang menunjukkan bahwa penggunaan Nama Domain atau alamat IP tidak diizinkan secara hukum (misalnya pengadilan atau arbiter telah mencabut hak Pendaftaran Nama Domain, perjanjian lisensi atau layanan Nama Domain telah berakhir, atau Pendaftar Nama Domain gagal memperpanjang Nama Domain); dan
j. BSrE CA diberitahu bahwa Sertifikat Wildcard telah digunakan untuk mengautentikasi FQDN secara curang.
k. Alasan lain yang dapat mempengaruhi integritas, keamanan, atau kepercayaan dari Sertifikat atau BSrE CA.

i. The CA is made aware of any circumstance indicating that use of a FQDN or IP Address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
j. The CA is made aware that a Certificate with a Wildcard Domain Name has been used to authenticate a fraudulently misleading subordinate FQDN.
k. Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of a Certificate or CA.

4.9.2 Pihak yang Dapat Meminta Pencabutan / Entities can Request Revocation

Permintaan pencabutan sertifikat dapat dilakukan oleh:
a. Pemilik;
b. Pihak berwenang lainnya (seperti Contract Signer, Certificate Approver, or Certificate Requester).

Certificate revocation is requested by:
a. Subscriber;
b. other authorities (example Contract Signer, Certificate Approver, or Certificate Requester)

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.

Permintaan pencabutan sertifikat oleh entitas lain melampirkan bukti bahwa:
a. Kunci privat sertifikat telah terungkap, atau
b. Penggunaan sertifikat tersebut tidak sesuai dengan CP/CPS TLS/SSL atau
c. Terdapat alasan relevan lain yang diberikan oleh pemilik.

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

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.

Certificate revocation request by an authorized representative attach evidence that:
a. The certificate's private key has been compromised, or
b. The use of such certificates is not TLS/SSL CP/CPS compliant or
c. There are other relevant reasons given by the Subscriber.

Requests for certificate revocation by other entity is enclosed with evidence that:

1) Kunci Privat Sertifikat telah terungkap;
2) Penggunaan Sertifikat tidak sesuai dengan CP/CPS TLS/SSL; dan
3) Pemilik sudah tidak terasosiasi dengan institusi yang bersangkutan.

1) The Private Key of the Certificate has been exposed;
2) The use of the Certificate does not conform to the TLS/SSL 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 ketentuan.

No stipulation.

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

BSrE CA memproses permintaan pencabutan Sertifikat dalam waktu 1 (satu) hari kerja setelah permohonan pencabutan yang valid diterima.

BSrE CA process revocation requests within 1 (one) working days after a valid revocation request is received

4.9.6 Pemeriksaan Keberlakukan Sertifikat Elektronik oleh Pengandal

Pengandal memvalidasi CRL dan/atau OCSP 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.

Relying Parties validate Certificates BSrE CA's 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:

a. Untuk sertifikat Pemilik, minimal sekali dalam 24 jam.
b. Dalam kasus kebocoran kunci privat atau insiden keamanan penting lainnya, contohnya pencabutan sertifikat BSrE CA, CRL terbaru dipublikasi dalam waktu maksimal 24 jam semenjak stempel waktu (timestamp) pencabutan.

The CRL should be updated and published:

a. For Subscriber Certificate, minimum once in 24 hours.
b. 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.

c. 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.

c. 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 dan dapat diunduh dalam waktu 3 (tiga) detik. BSrE CA tidak menghapus entri pencabutan dalam CRL atau respons OCSP sampai setelah Tanggal Kedaluwarsa Sertifikat yang dicabut.

BSrE CA publishes the CRL within 30 (thirty) minutes after issuance and can be downloaded within 3 (three) seconds. BSrE CA does not remove the revocation entry in the CRL or OCSP response until after the Expiration Date of the revoked Certificate.

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

BSrE CA menyediakan layanan validasi daring menggunakan protokol OCSP yang memberikan waktu respons 10 detik atau kurang dalam kondisi operasi normal dengan menggunakan metode GET.

BSrE CA provides online validation services using the OCSP protocol which provides a response time of 10 seconds or less under normal operating conditions using the GET method.

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

BSrE CA mengimplementasikan OCSP sesuai dengan standar IETF RFC 6960. Pembaruan informasi OCSP dilakukan setiap empat hari dan respon OCSP memiliki kadaluarsa selama 10 hari.

BSrE CA implements OCSP according to IETF RFC 6960 standard. OCSP information is updated every four days and OCSP responses have an expiration date of 10 days.

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.	The BSrE CA shall take all necessary measures to ensure availability of 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 kadaluwarsa 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

a. BSrE CA tidak menitipkan kunci privat kepada pihak lain. b. Kunci privat sertifikat pemilik tidak dititipkan kepada BSrE CA	a. BSrE CA's Private Key is not escrowed to other parties. b. Subscriber's Private Key does not entrusted to BSrE CA.

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
FASILITAS, PENGELOLAAN DAN KENDALI 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. BSrE CA 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).

The location and construction of the building that store BSrE CA systems dan computer devices for remote BSrE CA management, have fullfiled the criteria as facilities that stores high-value information and/or very sensitive information. BSrE CA ensures strong protection against unauthorized access attempts on each BSrE CA system and information stored on it (ex: implementing physical security 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:

a. Memastikan tidak ada akses tidak resmi ke perangkat keras
b. Menyimpan semua removable media yang berisi informasi teks yang sensitif dalam tempat penyimpanan yang aman.
c. Memonitor akses yang tidak berwenang baik secara manual maupun elektronik.
d. 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:

a. Ensure no unauthorized access to the hardware;
b. Store all removable media that contain sensitive plain-text information in secure containers;
c. Monitor unauthorized access, either manually or electronically;
d. 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 terpisah dari fasilitas organisasi yang lain, sehingga hanya pegawai BSrE yang memiliki otoritas yang bisa mengakses fasilitas tersebut.	All critical and high-risk BSrE operations take place within a physically secured facility with at least 4 (four) layers of security to allow access to sensitive hardware and software. Such facilities are physically separated from the organization's other systems, so only authorized trusted roles of the BSrE CA can access them.

5.1.3 Listrik dan AC / 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 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 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 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 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 diatas, dibuang sesuai dengan persyaratan pembuangan limbah normal.	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.

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

Data backup dilindungi dengan pengamanan fisik dan prosedur yang setara dengan pengamanan pada operasional BSrE CA.

The backup data is 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 yang Dipercaya / Trusted Roles

BSrE CA memiliki daftar dan catatan tentang personil yang bertugas sebagai Peran Terpercaya, yang mencakup nama, informasi kontak, dan informasi lainnya yang diperlukan.

BSrE CA has a list and records of personnel as Trusted Roles, which includes names, contact information and other necessary information.

Peran terpercaya BSrE CA meliputi:

a. PA
   Pembuatan, revisi dan persetujuan CPS.
b. Staff PA
   Membantu PA dalam menyiapkan dokumen CPS.
c. Ketua Tim Operasional BSrE
   Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan BSrE CA.
d. Administrator Aplikasi CA
   Melakukan operasional dan *maintenance* aplikasi manajemen BSrE CA.
e. DevOps *Engineer*
   Melakukan operasional dan *maintenance* terkait DevOps di BSrE.
f. Administrator HSM
   Melakukan Operasional dan *maintenance* HSM BSrE CA.
g. *Network Engineer*
   Melakukan operasional dan *maintenance* jaringan sistem sertifikasi elektronik.
h. RA
   Identifikasi dan Validasi identitas permohonan permintaan sertifikat.
i. Staff RA
   Membantu RA dalam menyiapkan dokumen identifikasi dan validasi identitas.
j. *Developer*
   Bertanggung jawab dalam mengembangkan aplikasi dan melakukan integrasi terkait dengan sistem PSrE.

BSrE CA's Trusted roles includes :

a. PA
   Creation, revision, and approval of CPS
b. PA staff
   Assist PA in preparing CPS documents.
c. BSrE CA Operational Team Leader
   Overall responsibility for managing all BSrE CA security practices.
d. CA Administrator
   Conduct operasional and maintenance of CA management application.
e. Devops Engineer
   Conduct operasional and maintenance related to DevOps at BSrE CA.
f. HSM Administrator
   Conduct operasional and maintenance related to HSM BSrE CA.
g. Network Engineer
   Conduct operasional and maintenance related to electronic certification system network.
h. RA
   Identification and validation of certificate application.
i. RA staff
   Assist RA in preparing identification and identity validation documents.
j. Developer
   Responsible for developing applications and performing integrations related to the PSrE systems.

k. *Repository*
Bertanggung jawab terhadap konten yang dipublikasikan pada repositori.
l. *Key Custodian*
Mengelola penyimpanan dan pengamanan kunci.
m. Internal Audit
Melakukan audit internal operasional BSrE CA

k. Repository
Responsible for the content published on the repository.
l. Key Custodian
Manage storage and security of the keys .
m. Internal Auditor
Conduct internal audits of BSrE CA operations.

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

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 terpercaya. Kendali multi-pihak tidak boleh dilakukan dengan melibatkan personil yang bertugas dalam peran Auditor. Tugas berikut memerlukan minimal tiga orang atau lebih:
a. Pembangkitan kunci BSrE CA
b. Pencabutan Sertifikat BSrE CA
c. Penandatanganan kunci BSrE CA
d. Pencadangan kunci privat BSrE CA
e. Penanganan perangkat keras kriptografi (pemasangan, pelepasan, pemeliharaan, pembongkaran dan penghapusan, serta troubleshooting)

Where multi-personnel control is required, all participants hold a trusted role. Multi-personnel control does not involve personnel that serve in an Auditor role. The following tasks require two or more persons:
a. BSrE CA key generation;
b. BSrE CA certificate revocation ;
c. BSrE CA key signing
d. BSrE Private Key backup;
e. 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 Terpercaya akan menerima Surat Perintah.

All individuals assigned to a Trusted Role will receive an Assignment Letter.

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:

a. PA dan administrator operasional;
b. Auditor internal dan semua peran lain;
c. 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:
a. PA and Operational Administrator;
b. Internal Auditor and all other roles;
c. Developer and all other roles.

5.3 Kontrol Personil / Personnel Controls

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

Personil yang bertugas sebagai Peran Terpercaya 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 harus mencakup operasional minimum dari IKP Indonesia (termasuk perangkat keras, perangkat lunak dan sistem operasi PSrE), prosedur operasional dan keamanan, CP, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil PSrE harus dilakukan minimal 1 (satu) kali dalam setahun.

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, software and operating system), operational procedures and security, CP and applicable CPS. The adequacy of the competence of CA personnel shall be conducted at least 1 (one) time a year.

5.3.4 Frekuensi Pelatihan Ulang dan Persyaratannya / Retraining Frequency and Requirements

Personil yang bertugas sebagai Peran Terpercaya 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 aksi legal diluar kewenangan / 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 CP, 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 CP, 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 disediakan untuk 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.

5.4 Prosedur Pencatatan untuk Audit / Audit Logging Procedures

BSrE CA membuat berkas *log audit* untuk semua kejadian yang terkait dengan keamanan BSrE CA, VA, dan RA. Bila memungkinkan, *log audit* keamanan dikumpulkan secara otomatis. Bila tidak mungkin, 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.

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

5.4.1 Jenis kegiatan yang dicatat / 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 *trusted role* dalam operasional BSrE CA dapat dilacak.

All available security auditing capabilities of the CA, RA, and VA operating system and applications shall be enabled. 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 harus memuat poin-poin sebagai berikut (baik direkam secara otomatis atau secara manual untuk setiap kejadian yang dapat diaudit):

a. Jenis kejadian,
b. Nomor seri atau urutan rekaman,
c. Tanggal dan waktu terjadi rekaman,
d. Sumber perekaman,
e. Indikator sukses atau gagal yang sesuai,
f. 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) :

a. The type of event;
b. Serial or sequence number of entry;
c. The date and time the event occurred;
d. Source of entry;
e. Success or failure where appropriate;
f. The identity of the entity and/or operator that caused the event.

5.4.2 Frekuensi pemrosesan *audit 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:

a. Untuk Sertifikat TLS/SSL tidak kurang dari 2 (dua) tahun sejak audit log tersebut dibuat.
b. Untuk Sertifikat EV SSL tidak kurang dari 7 (tujuh) tahun sejak audit log tersebut dibuat.

BSrE CA keeps all audit logs from the BSrE CA system that are generated electronically or manually for a period at

a. For TLS/SSL Certificates no less than 2 (two) years since the audit log was created.
b. For EV SSL Certificates no less than 7 (seven) years since the audit log was created.

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 BSrE CA.	The audit log collection system has been done since the system up and running and monitored internally by BSrE CA.

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

Tidak ada ketentuan.	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.	BSrE CA conducts periodically vulnerability assessments of security controls that have implemented by BSrE CA at least 1 (one) time in 6 (six) months

5.5 Pengarsipan Catatan / Records Archival

5.5.1 Jenis Catatan yang Diarsipkan / Types of Records Archived

BSrE CA mengimplementasikan metode pencadangan untuk operasional BSrE CA yang terletak di Pusat Data. Minimal, data berikut harus disimpan pada arsip: a. Siklus hidup sertifikat termasuk di dalamnya permohonan penerbitan, pembaruan, *re-key*, serta pencabutan sertifikat; b. Semua sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh BSrE CA; c. Data konfigurasi sistem BSrE CA; d. Dokumen CPS yang berlaku, termasuk juga segala modifikasi dan amandemen terhadap dokumen-dokumen tersebut.	BSrE CA implements a backup method for BSrE CA operations which is located at the Data Center. At a minimum, the following data shall be recorded for archive: a. Certificate life cycle operations including certificate issuance request, renewal, re-key, and certificate revocation; b. All certificates and CRLs as issued or published by the BSrE CA; c. BSrE CA system configuration data; d. Applicable CPS document, including modifications and amendments to the document.

5.5.2 Masa Retensi untuk Arsip / Retention Period for Archive

BSrE CA menyimpan catatan arsip mengenai kepemilikan Sertifikat Elektronik selama minimal 7 (tujuh) tahun. Media yang dibutuhkan untuk membaca arsip ini dipelihara selama masa retensi.	BSrE CA maintains archival records regarding the ownership of Certificates for at least 7 (seven) years. The media required to read this archive is maintained during the retention period.

5.5.3 Perlindungan Terhadap Dokumen Arsip / Protection of Archive

BSrE CA melindungi dokumen arsip sehingga hanya pihak yang berwenang 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.	BSrE CA protects archived documents, only authorized parties have access to these archives. 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.

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. Secara berkala, sampel informasi yang diarsipkan diuji untuk memeriksa integritas dan keterbacaan informasinya.	Media storing of BSrE CA archive information is checked upon creation. Periodically, samples of archived information are tested to check the continued integrity and readability of the information.
Hanya pihak atau personil yang memiliki kewenangan yang dapat memperoleh akses ke suatu arsip.	Only authorised personnel are allowed to access the archive.

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.

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 akan diganti dengan kunci baru yang digunakan untuk penanda tangan Sertifikat. BSrE CA akan 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 will be 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.

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.

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 harus dilakukan. Jika prosedur pencabutan Sertifikat Elektronik tidak dilakukan, lingkup potensi kerusakan harus dinilai untuk menentukan apakah sertifikat perlu dibangun kembali, hanya beberapa sertifikat harus ditarik, dan/atau kunci sertifikat perlu dinyatakan telah bocor.

If BSrE CA detects an attempted attacking to the BSrE CA system, BSrE CA will conduct an investigation to determine the nature and the degree of damage. If BSrE CA private signing key is suspected of compromise, then the revocation procedures for the entire Certificate shall be followed. If the Certificate revocation procedure is not folowed, the scope of potential damage must be assessed to determine whether the certificate needs to be rebuilt, or only some certificates affected to be withdrawn, and/or certificate keys need to be declared leaked.

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

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

disimpan dan dikelola sesuai dengan ketentuan yang berlaku sebagaimana Kunci Privat utama.

Keys are stored and managed in accordance with the applicable stipulation as the main Private Key.

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:

a. Memberitahu PA atau PSrE Induk sesegera mungkin.
b. Memastikan integritas sistem telah dipulihkan sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data sejak posisi terakhir backup.
c. Mengoperasikan kembali BSrE CA, dengan memprioritaskan kemampuan untuk membangkitkan informasi status sertifikat sesuai jadwal penerbitan CRL
d. Bila kunci penandatanganan BSrE CA rusak, operasional BSrE CA dilakukan kembali secepat mungkin, dengan memberikan prioritas ke pembangkitan pasangan kunci BSrE CA baru.

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

a. Notify the PA or Root CA as soon as possible;
b. Ensure that the system's integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup;
c. Re-establish BSrE CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule;
d. 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.

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

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

a. Memberitahu PA dan PSrE Induk sesegera mungkin agar dapat melakukan pencabutan Sertifikat;
b. Memberitahu semua Pemilik; dan
c. Mencabut Sertifikat Pemilik yang terkait dengan Kunci Privat yang terkompromi tersebut.

If the Private Key of the Root CA is compromised, BSrE CA shall respond as follow :

a. Notify the PA and Root CA as soon as possible in order to to be able to revoke the Certificate;
b. Notify all Subscribers; and
c. Revoke Subscriber Certificate related with the compromised private keys.

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

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).

(*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.

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 menyiapkan suatu rencana pemulihan bencana yang telah diuji, diverifikasi, dan terus-menerus diperbaharui. Layanan harus kembali pulih dalam kurun waktu 24 jam bila ada bencana.

BSrE CA prepares a disaster recovery plan that has been tested, verified, and continuously updated. Services must be restored within 24 hours in case of disaster.

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:

a. BSrE CA memberitahu ke RA, pemilik, dan semua Pengandal bahwa status operasional BSrE CA dihentikan;
b. BSrE CA menyediakan dukungan berkelanjutan operasional hingga semua sertifikat pemilik kadaluarsa;
c. BSrE CA melakukan pencabutan seluruh sertifikat pemilik; dan
d. Menyimpan informasi BSrE CA dan Pemilik selama periode pemberitahuan untuk tujuan pengalihan tanggung jawab mengikuti ketentuan yang akan diberlakukan.

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:

a. BSrE CA notifies the RA, Subscribers, and all Relying Parties the status of the operational BSrE CA has been stopped;
b. BSrE CA provides ongoing operational support until all subscriber certificates expired;
c. BSrE CA revokes all Subscriber Certificates; and
d. Keep the BSrE CA and Subscriber informations during the notification period for the purpose of transferring responsibility following the provisions that will be applied.

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

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

Pasangan Kunci BSrE CA harus 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.	BSRE CA's Key Pair shall be generated via the BSrE CA PKI system. Cryptographic keying material used by BSRE CA to sign certificates, CRLs or status information shall be generated in cryptographic modules validated to FIPS 140-2 level 3.

b. Pembangkitan Pasangan Kunci Pemilik Sertifikat TLS/SSL dan Sertifikat EV SSL / TLS/SSL and EV SSL Subscribers Key Pair Generation

BSrE CA tidak membangkitkan pasangan kunci pemilik dan tidak menerima permohonan sertifikat menggunakan pasangan kunci yang sebelumnya dibangkitkan oleh BSrE CA.	The BSrE CA does not generate the Subscriber's key pair and neither accept certificate requests using a key pair that was previously generated by BSrE CA.

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

Tidak ketentuan	No stipulation.

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

CSR dari Pemilik Sertifikat Elektronik disampaikan kepada BSrE CA dengan menggunakan protokol keamanan HTTPS. Kunci Publik dalam bentuk X. 509 dikirimkan BSrE CA kepada Pemilik Sertifikat Elektronik dengan menggunakan protokol keamanan HTTPS.	The CSR from the Subscriber's Certificate is submitted to the BSrE CA using the HTTPS security protocol. The X.509 Public Key is sent by BSrE CA to the Subscriber using the HTTPS security protocol.

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

Pengandal dapat mengakses Kunci Publik BSrE CA yang terdapat dalam Sertifikatmelalui saluran publikasi sebagaimana dijelaskan pada Bagian 2.2.	Relying Parties can access BSrE CA Public Key in the Certificate by the published channel as described in Section 2.2.

6.1.5 Ukuran Kunci / Key Sizes

Sertifikat	Panjang Kunci	Encryption Algorithm	Digest Algorithm
BSrE CA	4096 bit	RSA	SHA-256
Pemilik – Sertifikat TLS/SSL dan EV SSL	2048 bit	RSA	SHA-256

Panjang kunci dan periode penggunaan kunci dilakukan reviu secara periodik setiap tahun sesuai dengan kebijakan PSrE Induk.	The key length and period of key usage are reviewed periodically every year in accordance with the policy of root CA.

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

Pembangkitan pasangan kunci BSrE Perangkat kriptografi sesuai standar FIPS 140-2 level 3.	Key pair generation use cryptographic device according to FIPS 140-2 level 3 standard.

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 digunakan untuk penandatanganan sertifikat (keyCertSign) dan penandatanganan CRL (cRLSign). Secara lebih lengkap akan dijelaskan pada bagian ekstensi Key Usage.	The BSrE CA key is used for certificate signing (keyCertSign) and CRL signing (cRLSign). More details explained in the Key Usage extension section.

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

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

BSrE CA menggunakan modul kriptografi yang sudah sesuai standard FIPS 140-2 level 3 untuk operasional BSrE CA.	BSrE CA uses a cryptographic module that complies with FIPS 140-2 level 3 standards

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

Kunci Privat BSrE CA telah mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif. Suatu jumlah minimum dari Secret Shares (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.	The threshold number of shares needed for key generation is 2 of 4 (where n=2 and m=4) signing key activation is 2 of 4 and Private Key backup and restore is 2 of 4.

6.2.3 Eskro Kunci Privat / Private Key Escrow

Kunci Privat BSrE CA dan Pemilik tidak dititipkan.	Neither BSrE CA nor Subscriber Private Key are not be escrowed.

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 harus disimpan *off-site.* Semua salinan kunci privat BSrE CA dilindungi dengan cara yang sama dengan aslinya.	The BSrE CA Private Key is backed up under the same multiparty control as the main Private Key. At least one copy of the private key was stored off-site All backups of the Root CA Private Key shall be accounted for and protected in the same manner as the main Private 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 shall not be archived

6.2.6 Pemindahan Kunci Privat ke/dari Modul Kriptografi / Private / 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.	Privat Key transfer to/from cryptographic module hardware is encrypted.

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, atau sertifikasi lain yang ditetapkan dalam peraturan BSSN.	Cryptographic keying 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 or other certifications stipulated in the BSSN regulations
Material kunci privat pemilik disimpan dalam pengamanan modul kriptografi yang tersertifikasi minimal FIPS 140-2 Level 2.	Subcriber's Private Key is stored in a secure cryptographic module that is certified at least FIPS 140-2 Level 2.

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.

6.2.9 Metode Penonaktifan Kunci Privat / Method of Deactivating Private Key

Kunci Privat milik seluruh pihak yang terlibat dalam BSrE CA secara otomatis tidak aktif pada saat peralatan kriptografi penyimpan Kunci Privat dinon-aktifkan/dimatikan.	All Private Keys involved in BSrE CA are automatically inactivated when the cryptographic equipment storing the Private Key is deactivated / turned off.

6.2.10 Metode Penghancuran Kunci Privat / Method of Destroying Private Key

Kunci Privat BSrE CA dihancurkan oleh para individu dalam Peran Terpercaya 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.

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 tahun sebagai bagian dari proses pengarsipan Sertifikat Elektronik.	BSrE CA's and Subcriber's Public Keys are archived as integral parts of the Certificates issued for at least 5 (five) years.

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 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 harus dibuat pada saat key ceremony oleh personil Peran Terpercaya.	Activation data for the corresponding HSM shall be generated during a key ceremony by Trusted Role personnel

6.4.2 Aktivasi Perlindungan Data / 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.
Data aktivasi Kunci Privat BSrE CA dilakukan oleh personil Peran Terpercaya.	BSrE CA's Private Key activation data is performed by Trusted Role personnel

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 Tertentu / Specific Computer Security Technical Requirements

BSrE CA memastikan bahwa sistem yang menjaga perangkat lunak BSrE CA dan file data aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem BSrE CA telah dikonfigurasi dan diperkuat keamanannya menggunakan praktik terbaik (*best practices*).	BSrE CA ensures that the systems maintaining the BSrE CA software and data files are secure from unauthorized access. All computers that are part of the BSrE CA system have been configured and hardened using industry best practices.
Fungsi-fungsi keamanan komputer dapat diberikan oleh sistem operasi, atau melalui kombinasi sistem operasi, perangkat lunak, dan pengamanan fisik, mencakup namun tidak terbatas pada fungsi berikut: a. Memerlukan login terautentikasi untuk akses logikal; b. Menyediakan kontrol akses terbatas; c. Menyediakan kapabilitas audit keamanan; d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data; e. Menyediakan perlindungan mandiri untuk sistem operasi.	The following operational component security functions may be provided by a combination of operating system, software, and physical safeguards include but not limited to the following functionality: a. Require authenticated logins for logical access; b. Provide discretionary access control; c. Provide a security audit capability; d. Require use of cryptography for communication session and database security; e. Provide self-protection for the operating system.

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 aplikasi sistem 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 Kontrol 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 *Network Time Protocol*. Waktu yang didapat dari layanan waktu di atas akan digunakan untuk menentukan waktu pada saat:

a. Validitas waktu berlakunya Sertifikat Elektronik milik BSrE CA;
b. Pencabutan Sertifikat Elektronik milik BSrE CA;
c. Pembaruan CRL dan OCSP responder; dan
d. Penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik Pemilik Sertifikat Elektronik.

Prosedur secara elektronik atau manual dapat digunakan untuk mempertahankan akurasi waktu pada sistem.

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

a. Initial validity time of BSrE CA certificate;
b. Revocation of BSRE CA certificate;
c. Posting of CRL and OCSP responder updates; and
d. Issuance, renewal, and revocation of Subscriber certificates;

Electronic or manual procedures may be used to maintain system time.

BAB VII
PROFIL SERTIFIKAT ELEKTRONIK, *CERTIFICATE REVOCATION LIST, & ONLINE CERTIFICATE STATUS PROTOCOL / CERTIFICATE, CRL, AND OCSP PROFILES*

7.1 Profil Sertifikat Elektronik /Certificate Profile

Sertifikat Elektronik X.509 versi 3 sesuai dengan RFC 5280. BSrE CA melakukan tinjauan terhadap profil sertifikat secara berkala minimal setahun sekali.

The X.509 version 3 Certificate according to RFC 5280. BSrE CA shall review certificate profiles periodically at least once a year.

7.1.1 Nomor Versi / Version Number (s)

BSrE CA menerbitkan sertifikat X.509 v3.

BSrE CA issues X.509 v3 certificate

7.1.2 *Certificate Extension*

BSrE CA memakai ekstensi sertifikat standar yang mematuhi RFC 5280. Nomor seri sertifikat yang dihasilkan oleh BSrE-CA berisi setidaknya 64 bit keluaran dari Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

BSrE CA uses standard certificate extentions that comply with RFC 5280. The certificate serial number generated by BSrE-CA contains at least 64 bits output from the Cryptographically Secure Pseudorandom Number Generator (CSPRNG).

7.1.2.1 Penggunaan Kunci / Key Usage

Field	Sertifikat BSrE CA	Sertifikat TLS/SSL / EV SSL
Critical	True	True
digitalSignature	True	True
nonRepudiation	False	False
KeyEnchiperment	False	False
dataEnchiperment	False	False
Key Agreement	False	True
keyCertSign	False	False
cRLSign	True	False
enchiperOnly	False	False
dechiperOnly	False	False

7.1.2.2 *Certificate Policies Extension*

Ekstensi *certificate Policies* dari sertifikat X.509 Versi 3 diisi dengan identifier objek sesuai dengan bagian 7.1.6. *Field criticality* dari ekstensi ini diisi FALSE.

The Certificate Policies Extension of the X.509 version 3 certificate is filled with an object identifier according to section 7.1.6. Field Criticality of this extention is set to FALSE.

7.1.2.3 *Basic Constraint*

Ekstensi *Basic Constraints* sertifikat X.509 Versi 3 bagi sertifikat BSrE CA memiliki field CA yang diisi TRUE. Ekstensi *Basic Constraints* sertifikat Pemilik memiliki field CA yang diisi FALSE. *Field criticality* dari ekstensi ini diisi TRUE untuk sertifikat BSrE, tapi boleh diisi TRUE atau FALSE bagi sertifikat Pemilik.

The X.509 version 3 certificate Basic Constrain Extension for BSrE CA certificate has CA field TRUE. Basic Constrain Extension for Subscriber certificate has CA field FALSE. Field criticality for this extension is set to TRUE for BSrE CA certificate, but can be set to TRUE or FALSE for Subscriber certificate.

7.1.2.4 *Extended Key Usage*

Secara baku, *Extended Key Usage* diatur sebagai ekstensi non-critical. Sertifikat BSrE CA dapat memuat ekstensi *extended key usage* sebagai suatu bentuk dari pembatasan teknis pada penggunaan sertifikat-sertifikat yang BSrE CA terbitkan. Semua sertifikat Pemilik boleh mengandung sebuah ekstensi *extended key usage* sesuai tujuan penerbitan sertifikat, namun tidak boleh memuat nilai anyEKU.

By default, Extended Key Usage is set to Non-Critical Extension. BSrE CA's Certificate may contain an extended key usage extensions as a form of technical restriction on the use of certificates issued by BSrE CA. All certificate subscriber may contain an extended key usage extension according to an objective of certificate issuance, but may not contain anyEKU.

7.1.2.5 CRL *Distribution Points*

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

The X.509 version 3 certificate populated with a CRLDistributionPoints extension that contain URL i.e a location where the Relying Party can obtain the CRL to check certificate status. Field Critically of this extension must be set with FALSE.

7.1.2.6 *Authority Key Identifier*

Sertifikat X.509 Versi 3 secara umum diisi dengan ekstensi *authorityKeyIdentifier*. Metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik dari BSrE CA, harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280. *Field criticality* dari ekstensi ini harus diisi FALSE.

The X.509 Version 3 certificates are generally assigned the authorityKeyIdentifier extension. The method for generating a keyIdentifier based on a Public Key from a BSrE CA, must be calculated according to the method described in RFC 5280. The criticality field of this extension must be set to FALSE.

7.1.2.7 *Subject Key Identifier*

Bila ada dalam sertifikat X.509 Versi 3, *field criticality* dari ekstensi ini harus diisi dengan FALSE dan metode untuk menghasilkan *keyIdentifier* yang berbasis pada Kunci Publik subjek sertifikat harus dihitung sesuai dengan metode yang diuraikan dalam RFC 5280.	If present in the X.509 Version 3 certificate, field criticality of this extension must be set to FALSE and the method for generating a keyIdentifier based on a Public Key subject of the Certificate shall calculating according to the method described in RFC 5280.

7.1.3 Identifier Objek Algoritma / Algorithm Object Identifier (OID)

Pengidentifikasi objek algoritma kriptografi diisi sesuai dengan standar dan rekomendasi RFC 5280.	Cryptographic algorithm OID are set in according to RFC 5280 standards and reccommendations.
OID standar X.509v3 digunakan. Algoritma enkripsi RSA untuk kunci subjek dan SHA384 dengan enkripsi RSA untuk tanda tangan sertifikat.	X.509v3 standard OIDs shall be used. RSA encryption algorithm for subject key and SHA384 with RSA Encryption for digital signature algorithm.
SHA384 With RSA Encryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}	SHA384 With RSA Encryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}

7.1.4 Format Nama / Name Forms

BSrE CA tidak menerbitkan sertifikat dengan nama domain yang berisi Reserved IP Address atau Nama Domain Internal.	BSrE CA does not issue certificates with domain names that contain Reserved IP Addresses or Internal Domain Names.

7.1.5 Batasan Nama / Name Constrains

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

7.1.6 Identifier Objek Kebijakan Sertifikat / Certificate Policy Object Identifier

OID CP yang tercantum di dalam sertifikat adalah sesuai dengan daftar OID pada bagian 1.2.	The CP OID listed in the certificate is in accordance with the OID list in section 1.2.

7.1.7 Usage of Policy Costraints Extension

Tidak ada ketentuan.	No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Tidak ada ketentuan.	No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies *Extension*

Tidak ada ketentuan.	No stipulation.

7.2 Profil CRL / CRL Profile

7.2.1 Nomor Versi / Version Number (s)

BSrE CA menerbitkan CRL dengan standar X.509 versi 2.	The BSrE CA published CRLs with the X.509 version 2 standard.

7.2.2 CRL dan Ekstensi Entri CRL / CRL dan CRL Entry Extensions

BSrE CA menggunakan CRL dan CRL entry extension sesuai RFC 5280.	BSrE CA uses CRL and CRL entry extension according to RFC 5280.

7.3 Profil OCSP / OCSP Profile

BSrE mengoperasikan suatu responder OCSP yang sesuai dengan RFC 6960 atau RFC 5019.	BSrE operates an OCSP responder that complies with RFC 6960 or RFC 5019.

7.3.1 Nomor Versi / Version Number (s)

BSrE menerbitkan responder OCSP versi 1.	BSrE published version 1 of the OCSP responder.

7.3.2 Ekstensi OCSP / OCSP Extensions

Ekstensi OCSP merujuk ke standar interoperabilitas PSrE Instansi.	The OCSP extension refers to the Government PSrE 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 Informatika tentang Penyelenggaraan Sertifikasi Elektronik. BSrE CA diaudit untuk kepatuhan kepada Webtrust TLS/SSL dan EV SSL.

BSrE CA performs a compliance audit and submits periodic reports required by the Ministry of Communication and Informatics regarding the operational of Certificate Authority. BSrE CA is audited by Webtrust for TLS/SSL and EV SSL.

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 CP/CPS TLS/SSL. 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 Informatika.

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 TLS/SSL CP/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 Informatics.

8.2 Identitas/Kualifikasi Penilai / Identity/Qualifications of Assessor

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

a. Penilai dilaksanakan oleh tim asesmen independen yang *qualified*.
b. 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 Kominfo terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik.

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

a. The assessment is carried out by a qualified independent assessment team.
b. 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.

c. Penilai memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
d. Penilai harus memiliki bukti bahwa dirinya memenuhi kualifikasi penilai untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi, akreditasi, lisensi, atau asesmen lain yang sah;
e. Penilai menguasai set keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan professional;
f. Penilai tidak memiliki konflik kepentingan terhadap BSrE CA; dan
g. Penilai patuh terhadap hukum, kebijakan pemerintah, atau kode etik professional.

c. The assessor has proficiency in information security auditing including security techniques, equipment, and Public Key Infrastructure technology.
d. The assessors have evidence that show their qualification for a specific audit scheme, in form of certification, accreditation, license or other valid assessment;
e. Assessors master certain skill sets, competency evaluation, quality assurance measures such as peer review, standards regarding the proper assignment of staff, and requirements for continuing professional education;
f. The assessor has no conflict of interest with BSrE CA; and
g. 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.

BSrE CA has selected an auditor/assessor who is completely independent.

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. Asesmen mencakup persyaratan dasar dan Pedoman EV SSL pada Forum CA/Browser (http://www.cabforum.org) versi terkini.

The audit meets the requirements of the audit schemes under which the assessment is being made. These requirements may vary as audit schemes are updated. The assessment covers the basic requirements and the latest version of the SSL EV Guidelines on the CA/Browser Forum (http://www.cabforum.org).

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.

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:

Tindakan yang dilakukan sebagai berikut:

a. Penilai kepatuhan harus memberitahu BSrE CA dan Kominfo tentang ketidaksesuaian; dan

a. Assessor must inform BSRE CA and Kominfo regarding of deficiencies.

b. BSrE menentukan pemberitahuan atau tindak lanjut apa yang diperlukan disesuaikan dengan persyaratan CPS dan kontrak terkait, kemudian melaksanakan pemberitahuan dan tindakan tersebut tanpa penundaan.

b. BSRE CA define notification and actions that need to be carried out in accordance with CPS and related contracts.

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/CPS TLS/SSL 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 TLS/SSL CP/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 resiko 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 ketentuan peraturan perundangan-undangan terkait PSrE.

Internal audit also checks the compliance with laws and regulations concerning Certification Authority

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 re-key sertifikat elektronik tidak dikenakan biaya	All processes/activities 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.	All processes/activities 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.	All processes/activities 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.	All processes/activities does not charge for any processes related to implementation of Certificate .

9.1.5 Kebijakan Pengembalian Biaya / Refund Policy

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. BSrE CA mematuhi persyaratan asuransi mengenai Penyelenggaraan Sertifikasi Elektronik sesuai dengan Peraturan Menteri yang terkait.	In case of compromise, the National Cyber and Crypto Agency can take over the operations of BSrE CA. BSrE CA comply with the insurance requirements regarding the Certification Practice in accordance with the relevant Ministry Regulations.

9.2.2 Aset Lainnya / Other Assets

Tidak ada ketentuan.	No stipulation

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

BSrE CA menyediakan kebijakan jaminan untuk para Pemilik sertifikat.	BSrE CA will offer an insurance or warranty policy to Subscribers

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:

a. Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
b. Kunci Privat Pemilik Sertifikat yang disimpan oleh BSrE CA, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
c. Catatan Permohonan Sertifikat;
d. Hasil penilaian kerentanan;
e. Rekam jejak audit (audit logs) dari sistem BSrE CA;
f. Data aktivasi pada saat pengaktifan Kunci Privat BSrE CA sebagaimana dijabarkan pada Bagian 6.4;
g. Dokumentasi bisnis proses PSrE termasuk dokumen DRP dan BCP;
h. Laporan audit dari auditor independen sebagaimana dijabarkan pada Bagian 8; dan
i. Kontrol keamanan untuk perangkat keras dan perangkat lunak BSrE CA.

BSrE CA keeps and classifies the following items that are classified as being confidential information and therefore are subject to reasonable care and attention:

a. Personal information of CA's personnels as detailed in Section 9.4;
b. Subscriber's Private Key stored by BSrE CA and the information required to use Privat Key by the Subscriber;
c. Certificate Application Records;
d. Vulnerability Assessment Results;
e. Audit logs from BSrE CA's systems;
f. Activation data used to active BSrE CA Private Keys as detailed in Section 6.4;
g. BSrE CA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP);
h. Audit Reports from an independent auditor and internal auditor as detailed in Section 8; and
i. Security Control for BSrE CA's hardware and software.

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

Informasi yang tidak dikategorikan rahasia dalam dokumen CP/PS TLS/SSL dianggap informasi publik. Sertifikat dan informasi mengenai status sertifikat termasuk kategori informasi publik. Berikut daftar dokumen yang dipublikasikan ke dalam repository BSrE CA:

a. Sertifikat BSrE CA
b. CRL BSrE CA
c. CP/PS TLS/SSL BSrE CA
d. Kebijakan Privasi untuk Pengguna Layanan BSrE
e. Perjanjian Pemilik Sertifikat Elektronik BSrE CA
f. Perjanjian Pengandal Layanan BSrE
g. Kebijakan Jaminan BSrE CA

Any information not defined as confidential within this TLS/SSL CP/CPS is deemed as public, such as:

a. BSrE CA's certificate;
b. BSrE CA's CRL;
c. BSrE CA's TLS/SSL CP/PS;
d. Privacy Policy;
e. Subscriber Agreement;
f. Relying Party Agreement;
g. Warranty Policy;

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

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

a. Pelatihan dan peningkatan *awareness*;
b. Perjanjian kontrak pegawai;
c. NDA dengan pegawai, pegawai *outsource*, dan rekanan.

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

a. training and awareness;
b. contracts with employees;
c. 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 shall protect personal information in accordance with a Privacy Policy published on BSrE CA's website at https://bsre.bssn.go.id/repository.

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 boleh 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.

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 pribadi sesuai dengan Kebijakan Privasi secara aman. Informasi yang disimpan dapat berbentuk fisik maupun elektronik. *Backup* informasi pribadi 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 pribadi 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 pribadi 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.

Personal 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 pribadi 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's Intellectual Property Rights including trademarks, copyright and all documents remain as sole property of BSrE CA.

9.6 Pernyataan dan Jaminan / Representations and Warranties

9.6.1 Pernyataan dan Jaminan BSrE CA / CA Representations and Warranties

BSrE CA menyatakan dan menjamin bahwa:

a. BSrE CA mematuhi ketentuan yang diatur dalam CP/CPS TLS/SSL ini;
b. BSrE CA menerbitkan dan memperbarui CRL secara berkala;

BSrE CA represents and warrants that:

a. BSrE CA complies, in all material aspects, with the TLS/SSL CP/CPS,
b. BSrE CA publishes and updates CRL on a regular basis,

c. Seluruh sertifikat yang diterbitkan akan memenuhi syarat yang diatur berdasarkan CP/CPS TLS/SSL ini;

d. BSrE CA akan menampilkan informasi yang dapat diakses secara publik melalui repositorinya;
e. Kunci Privat BSrE CA terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang; dan
f. Hanya informasi yang diverifikasi yang dapat muncul dalam Sertifikat.

in accordance with this TLS/SSL CP/CPS,
d. BSrE CA will display information that can be accessed publicly through its repositories,
e. BSrE CA's signing Private Key is protected and no unauthorized person has ever had access to that Private Key; and
f. Only verified information appears in the Certificate.

c. All certificates issued will meet the minimum requirements and verified

9.6.2 Pernyataan dan Jaminan RA / RA Representations and Warranties

RA menyatakan dan menjamin, bahwa:
a. Tidak ada kekeliruan fakta dalam sertifikat yang diketahui oleh atau berasal dari entitas yang menyetujui pendaftaran sertifikat atau penerbitan sertifikat;
b. Tidak ada kesalahan informasi dalam sertifikat yang dilakukan oleh entitas yang menyetujui pendaftaran sertifikat sebagai akibat dari ketidakcermatan dalam pengelolaan pendaftaran Sertifikat;
c. Kegiatan registrasi yang dilakukan RA sesuai dengan CP/CPS TLS/SSL ini dan Perjanjian RA.

RAs warrant that:
a. There are no fallacy on certificate that have been known or came from the entity who gives an acknowledgement on certificate application or certificate issuance
b. There is 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.
c. Registration activity that have been done by RAs comply with this TLS/SSL CP/CPS and other agreed agreement.

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

Pemilik Sertifikat menjamin bahwa:
a. 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;

a. 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;

b. Setiap kunci privat harus diamankan dan hanya pemilik sertifikat yang memiliki akses terhadap kunci privat tersebut;

Subscribers warrant that:

c. Sudah melakukan review terhadap informasi dari sertifikat;
d. Semua informasi yang diberikan oleh pemilik sertifikat dan informasi yang berada di dalam sertifikat adalah benar;
e. Sertifikat Elektronik digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
f. Segera:

b. Private Key is protected and that no unauthorized person has ever had

1) Melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan sertifikat dan kunci privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari kunci privat pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat; dan
2) 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
3) Menghentikan penggunaan kunci privat yang kunci publiknya tercantum dalam Sertifikat Elektronik setelah sertifikat dicabut;

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

1) Request revocation of the certificate, and cease using it and its

access to the Subscriber's Private Key;
c. Have thoroughly reviewed the certificate information;
d. All information supplied by the Subscriber and contained in the certificate is true,
e. The certificate is being used exclusively for authorized and legal purposes, consistent with all material requirements of this CPS;
f. Promptly :

associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
2) Request revocation of the certificate, and cease using it, if any information in the certificate is or becomes incorrect or inaccurate;
3) Stop using the Private Key whose Public Key is listed in a certificate after the certificate is revoked;

g. Will respond to BSrE CA instructions regarding compromise or certificates misuses within 48 (forty eight) hours;

h. 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*;

i. Pemilik sertifikat adalah pengguna akhir dan bukan merupakan BSrE CA, dan tidak menggunakan kunci privat yang kunci publiknya tercantum dalam Sertifikat Elektronik untuk tujuan penandatangan Sertifikat Elektronik PSrE lain.

j. Sertifikat TLS/SSL dan EV SSL akan diinstall hanya pada server yang dapat diakses pada nama domain (subjectAltName(s)) yang terdapat pada Sertifikat.

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

i. The Subscriber is an end-user and not a CA and does not use the private key whose public key is listed in the Certificate for the purpose of signing another PSrE.

j. TLS/SSL and EV SSL Certificates will be installed only on servers that can be accessed on the domain name (subjectAltName(s)) contained in the Certificate.

h. Acknowledges and accepts that BSrE CA is entitled to revoke the certificate immediately if the

9.6.4 Pernyataan dan Perjanjian Pengandal / Relying Party Representations and Warranties

Pengandal menjamin bahwa:

a. Memiliki kemampuan teknis untuk menggunakan sertifikat;

b. 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;

c. 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 :

a. Have the technical capability to use certificates;

b. 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;

c. Notify the appropriate RA or BSrE CA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised;

d. 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;

e. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

d. Required Relying Party to acknowledge that they have enough information to make a decision based on the extent whether they choose to rely on the information in the 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;

e. Must 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:

a. 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,
b. Penyalahgunaan sertifikat yang tidak sesuai dengan peruntukannya seperti yang tertera pada bagian 4.5 (*Certificate Usage*)
c. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam *demo* atau *testing* Sertifikat.

BSrE CA does not warrant:

a. 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;
b. Misuse of a certificate that is inconsistent with its usage as shown in section 4.5;
c. 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:

a. Kerugian yang diakibatkan oleh penggunaan Sertifikat Elektronik atau pasangan kunci yang tidak sesuai dengan yang ditetapkan dalam dokumen CPS ini;
b. Kerugian yang disebabkan oleh kondisi *force majeure*;
c. Kerugian yang disebabkan oleh kode yang tidak sah (malicious code) pada infrastruktur yang digunakan oleh Pemilik Sertifikat Elektronik;
d. 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:

a. all damage caused by the misuse of Certificates or Key Pairs besides the proper use that have been defined in CP/CPS;
b. all damage caused by the force majeure condition;
c. Losses caused by malicious code on the infrastructure used by Subscriber;
d. 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

9.9 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

Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pemilik Sertifikat sepakat untuk mengganti rugi BSrE CA berikut dengan para pihak terkait terhadap kerugian, kerusakan, dan biaya, yang diakibatkan oleh

a. Setiap kekeliruan penggunaan sertifikat oleh pemilik baik disengaja atau tidak disengaja.

Based on laws and regulations, the Subscriber agrees to indemnify the BSrE CA along with the related parties against losses, damages and costs, which are caused by :

a. Any misuse of the certificate by the Subscriber intentional or unintentional ;
b. Pelanggaran yang dilakukan oleh Pemilik Sertifikat terhadap Perjanjian Pemilik

Sertifikat, CP/CPS TLS/SSL ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;

c. Penggunaan Kunci Privat Pemilik Sertifikat yang tidak sah karena kelalaian Pemilik Sertifikat; atau
d. Penggunaan Sertifikat oleh Pemilik Sertifikat untuk kegiatan melawan hukum.

b. Violation of subscriber agreement, this TLS/SSL CP/CPS, or applicable law, intentionally or unintentionally;

c. Invalid use of the subscriber Private Key due to the subscriber negligence; or
d. The usage of Certificate by subscriber for activities against the law.

9.9.3 Ganti Rugi oleh Pengandal / Indemnification by Relying Parties

BSrE CA menyertakan persyaratan ganti rugi untuk Pengandal dalam Perjanjian Pengandal.

BSrE CA will include its indemnification requirements for Relying Parties in its Relying Party Agreement.

9.10 Jangka Waktu dan Pengakhiran / Term and Termination

9.10.1 Jangka Waktu / Term

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

This TLS/SSL CP/CPS is declared valid until there is further notification by BSrE CA through its website or repository

9.10.2 Pengakhiran / Termination

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

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

9.10.3 Efek Pengakhiran dan Keberlangsungan / Effect of Termination and Survival

BSrE CA mengkomunikasikan kondisi, dampak dari pengakhiran CP/CPS TLS/SSL, 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 TLS/SSL CP/CPS termination and continuity of the issued certificate on its website or repository.

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

Even once the TLS/SSL CP/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, telepon, 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 dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 CP/CPS TLS/SSL.

BSrE CA provides communication media for related parties through printed documents or electronic documents that are manually or electronically signed. Communication media for related parties are provided through telephone and/or electronic mail. BSrE CA will respond for a maximum of 20 (twenty) business days through the same communication media. Communications made to BSrE CA must be addressed in accordance with those listed in Section 1.5.2.

9.12 Perubahan atau Amandemen / Amandments

9.12.1 Prosedur untuk Amandemen / Procedure for Amendments

BSrE CA akan meninjau CP/CPS TLS/SSL ini setidaknya 1 (satu) kali setiap tahun. Perbaikan, pembaruan atau perubahan terhadap dokumen CP/CPS TLS/SSL dipublikasikan. Amandemen CP/CPS TLS/SSL dilakukan sesuai dengan prosedur persetujuan CP/CPS TLS/SSL.

BSrE CA will review this TLS/SSL CP/CPS at least 1 (one) time every year. Corrections, updates or changes to the TLS/SSL CP/CPS document are published. TLS/SSL CP/CPS amendments are carried out following the TLS/SSL CP/CPS approval procedure

9.12.2 Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

BSrE CA menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CP/CPS TLS/SSL ini termasuk juga keterangan waktu ketika CP/CPS TLS/SSL efektif berlaku. Ketika terjadi perubahan, CP/CPS TLS/SSL 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 TLS/SSL CP/CPS as well as information about the period by when the revised TLS/SSL CP/CPS becomes effectively applicable. These TLS/SSL CP/CPS changes are made publicly available within 7 (seven) business days since approval.

9.12.3 Kondisi dimana OID harus berubah / Circumstances Under Which OID Must be Chaned

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 Provisi Penyelesaian Perselisihan / Dispute Resolution Provisions

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CP/CPS TLS/SSL 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 pihak pengandal.	In case of dispute or controversy related performance, execution or the interpretation of the TLS/SSL CP/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 Relying Party.

9.14 Hukum yang Mengatur / Governing Law

CP/CPS TLS/SSL 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 TLS/SSL CP/CPS is governed, construed and interpreted in accordance with the laws of Indonesia to ensure uniform interpretation of this TLS/SSL CP/CPS, regardless of the place of residence or place of use of BSrE CA's certificates or other products and services. Including if the BSrE CA certificate is used for commercial needs in other countries, it still applies the rule of law in Indonesia.
Para pihak, termasuk rekan BSrE CA, pemilik, pihak Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.	Each party, including BSrE CA's partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Indonesia

9.15 Kepatuhan atas Hukum yang Berlaku / Compliance with Applicable Law

BSrE CA mematuhi hukum yang berlaku di Indonesia. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.	BSrE CA complies with applicable laws of Indonesia. Compliance includes, but is not limited to, hardware, software, systems, business information, data processes and all related undertakings during the daily operations of business practices.

9.16 Ketentuan yang Belum Diatur / Miscellaneous Provisions

9.16.1 Seluruh Perjanjian / Entire Agreement

Tidak ada ketentuan.	No Stipulation

9.16.2 Pengalihan Hak / Assignment

Entitas yang beroperasi di bawah CP/CPS TLS/SSL ini tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari BSrE CA.	Entities operating under this TLS/SSL CP/CPS must not assign their rights or obligations without the prior consent of BSrE CA.

9.16.3 Keterpisahan / Severability

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

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

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

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 CP/CPS TLS/SSL 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 TLS/SSL CP/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 shall 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

Tidak ada ketentuan.	No Stipulation

Ditetapkan di Jakarta
Pada tanggal 22 Oktober 2024

Dokumen Ini ditandatangani secara elektronik oleh:
Kepala Balai Besar Sertifikasi Elektronik

JONATHAN GERHARD T, S.ST
Pembina (IV/a)

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 an electronic certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions.
Penyelenggara Sertifikasi Elektronik (PSrE) 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 Electronic 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.
Pihak 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 Electronic Certificates.
Pernyataan Praktik Sertifikat	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan

Elektronik Certification Practice Statement	Sertifikat. One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Pasangan Kunci Key Pair	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. 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 Private Key	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. 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 Public Key	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. 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 Terpercaya Trusted Roles	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. 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 Key Compromise	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. 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 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. 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 Online Certificate Status Protocol	Protokol pemeriksaan Sertifikat secara online bagi Pihak Pengandal yang berisi informasi mengenai status Sertifikat. An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Pemohon Applicant	Individu atau Badan Usaha atau Instansi yang mengajukan permohonan pembuatan atau perubahan Sertifikat. Setelah 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 Kominfo. A Compliance Audit is a process conducted by CA CAB or Root CA upon Indonesian CA, by referring to CA standards issued by Kominfo.
Sertifikat TLS/SSL TLS/SSL Certificate	Sertifikat TLS/SSL adalah sertifikat yang diterbitkan oleh BSrE CA untuk penggunaan pengamanan pada web server. TLS/SSL certificate is a Certificate issued by a BSrE CA for use on secure servers.
Sertifikat EV SSL EV SSL Certificate	Sertifikat EV SSL adalah sertifikat TLS/SSL yang diterbitkan oleh BSrE CA dengan persyaratan EV SSL. EV SSL certificate is a SSL Certificate issued by a BSrE CA meeting the requirements of the EV SSL Guidelines.
FQDN FQDN	FQDN adalah nama domain lengkap yang terdiri dari hostname dan nama domain. FQDN is a complete domain name consisting of hostname and domain name.

AKRONIM

BCP	*Business Continuity Plans*
BSrE	Balai Besar Sertifikasi Elektronik
CA	*Certificate Authority*
CAA	*Certification Authority Authorization*
CP	*Certificate Policy*
CPS	*Certificate 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 Sertifikasi Elektronik
RA	*Registration Authority*
RFC	*Request for Comment*
SHA	*Secure Hashing Algorithm*
SSL	*Secure Sockets Layer*
VA	*Validation Authority*