CERTIFICATION PRACTICE STATEMENT
PENYELENGGARA SERTIFIKASI ELEKTRONIK (PSrE)
PT INDONESIA DIGITAL IDENTITY (VIDA)

Nomor Dokumen	SOP-COM-P-001
Tanggal Berlaku	21 November 2023
Versi	3.0
Klasifikasi	**PUBLIK**

Disetujui oleh :

Policy Authority

LEMBAR CATATAN REVISI / REVIEW

Tanggal	Rev	Uraian	Oleh
1 Desember 2018	1.0	Initial Release	Policy authority
13 May 2019	2.0	* Daring dan Luring * Penyesuaian berdasarkan Audit Checklist PSrE Kominfo	Policy authority
19 July 2019	2.1	* Penyesuaian pernyataan pada Bagian 6.1.1.2	Policy authority
2 September 2019	2.2	* Penyempurnaan OID pada Bagian 1.2 * Perbaikan redaksional pada Bagian 2.3 * Perbaikan redaksional pada Bagian 3.2.3 * Perbaikan redaksional pada Bagian 4.1.2 * Perbaikan redaksional pada Bagian 4.2.1 * Perbaikan redaksional pada Bagian 4.9.8 * Perbaikan redaksional pada Bagian 6.1.5	Policy authority

8 Juni 2020	2.3	* Penyesuaian berdasarkan ketentuan Webtrust CA 2.2	Policy authority
8 Juli 2020	2.4	* Penyesuaian definisi istilah pada Appendix	Policy authority
5 Agustus 2020	2.5	*Penyesuaian mengenai level Sertifikat yang berlaku pada Bagian 1.4.1 , 3.2.1, 3.2.3, 4.1.2	Policy authority
17 Maret 2021	2.6	*Perbaikan redaksional * Penyesuaian berdasarkan standar operabilitas	Policy authority
18 October 2022	2.7	*Penyesuaian mengenai - level sertifikat yang berlaku pada bagian 1 - metode identifikasi Pemilik pada bagian 3 - pengelolaan kunci Pemilik dan sertifikat Pemilik pada bagian 4, 6 *Perbaikan redaksional dan penyesuaian kalimat	Policy authority
21 November 2023	3.0	* Penyesuaian berdasarkan CP Kominfo 3.3 *menghapus keterangan mengenai penyimpanan pasangan kunci pada perangkat *smartphone* *Penyesuaian mengenai - level sertifikat yang berlaku pada bagian 1 *Perbaikan redaksional dan penyesuaian kalimat	Policy authority

DAFTAR ISI / TABLE OF CONTENT

1. PENGANTAR / INTRODUCTION

1.1. Ringkasan / Overview

PT Indonesia Digital Identity adalah Penyelenggara Sertifikasi Elektronik ("**PSrE**") yang beroperasi mengacu pada ketentuan peraturan perundang-undangan terkait penyelenggaraan sertifikasi elektronik (untuk selanjutnya disebut "**VIDA**"). Pada hierarki Infrastruktur Kunci Publik (IKP) Indonesia, VIDA merupakan PSrE Non-Instansi yang menerbitkan Sertifikat selain yang diterbitkan oleh PSrE Instansi.

PT Indonesia Digital Identity is a Certification Authority ("**CA**") operating by virtue of laws and regulations concerning CA operation, (hereinfer "**VIDA**"). In Indonesia PKI hierarchy, VIDA is a Non-Government CA that issues certificates to anyone other than those issued by Government CAs.

Dokumen *Certification Practice Statement* (CPS) ini mendefinisikan persyaratan prosedural dan operasional yang dianut oleh VIDA saat menerbitkan dan mengelola Sertifikat Elektronik ("Sertifikat"). Dokumen ini ditujukan bagi:

1. Pemilik yang perlu memahami bagaimana mereka diautentikasi, apa kewajiban mereka sebagai pemegang Sertifikat yang diterbitkan oleh VIDA, dan bagaimana mereka dilindungi oleh VIDA sesuai dengan ketentuan CPS ini;
2. Pengandal yang perlu memahami tingkat kepercayaan terhadap Sertifikat Pemilik atau tanda tangan elektronik tersertifikasi (tanda tangan digital) dan layanan yang memanfaatkan sertifikat elektronik lain yang menjadi bagian dari rantai kepercayaan (*trust chain*) IKP Indonesia.
3. siapa saja yang perlu memahami mengenai penyelenggaraan sertifikasi elektronik yang dijalankan oleh VIDA.

This Certification Practice Statement (CPS) defines the procedural and operational requirements that VIDA adheres to when issuing and managing Digital Certificate ("Certificate"). This document is intended for:

1. Subscriber who need to understand how they are authenticated,what their obligations are as VIDA's Subscribers, and how they are protected by VIDA as per this CPS;
2. Relying Parties who need to understand how much trust to place in a VIDA's Certificate, or digital signatures and other services using electronic Certificates which constitute a part of Indonesia's PKI trust chain
3. anyone who needs to understand how VIDA runs the certification authority practices.

CPS ini sesuai dengan standar *Request for Comments* 3647 (RFC 3647) dari *Internet Engineering Task Force* (IETF) tentang *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework* serta sejalan dengan *Certificate Policy* dari PSrE Induk Indonesia. Dalam hal terjadi inkonsistensi antara dokumen ini dan persyaratan tersebut, persyaratan tersebut didahulukan dari dokumen ini.

This CPS is consistent with Request for Comments 3647 (RFC 3647) of the Internet Engineering Task Force (IETF) Internet X.509 version 3 Public Key Infrastructure Certificate Policy and Certification Practices Framework and aligned with Root CA Indonesia's Certificate Policy. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

1.2. Identifikasi dan Nama Dokumen / Document Name and Identification

Dokumen ini adalah dokumen *Certification Practice Statement* (CPS) VIDA.

The document is the Certification Practice Statement (CPS) for VIDA.

OID	Penggunaan / Usage
2.16.360.1.1.1.12.4	OID VIDA untuk Webtrust
2.16.360.1.1.1.12.4.4.1	CP VIDA
2.16.360.1.1.1.12.4.4.2	CPS VIDA sebelum pembaruan OID
2.16.360.1.1.1.12.4.5	Subscriber certificate
2.16.360.1.1.1.12.4.6	Development
2.16.360.1.1.1.12.4.7	OCSP Signer
2.16.360.1.1.1.12.4.8	VIDA Root Certificate Authority
2.16.360.1.1.1.12.4.9.1	VIDA Sign Certificate Authority
2.16.360.1.1.1.2.1	CP PSrE Induk
2.16.360.1.1.1.3.12.4	OID PSrE Non-Instansi VIDA sesuai panduan Kemenkominfo pada Hierarki OID untuk IKP Indonesia versi 1.2
2.16.360.1.1.1.3.12.4.4.2	CPS VIDA Indonesia
2.16.360.1.1.1.5.1.2.2	Sertifikat untuk individu Warga Negara Indonesia (WNI) non-Instansi Online Level 2 sesuai panduan Kemenkominfo pada Hierarki OID untuk IKP Indonesia versi 1.2
2.16.360.1.1.1.5.2.2.2	Sertifikat untuk individu Warga Negara Asing (WNA) non-Instansi Online Level 2 sesuai panduan Kemenkominfo pada Hierarki OID untuk IKP Indonesia versi 1.2
2.16.360.1.1.1.8.1	Sertifikat untuk Segel Elektronik Badan Usaha Online Level 3 sesuai panduan Kemenkominfo pada Hierarki OID untuk IKP Indonesia versi 1.2
2.16.360.1.1.1.7.1	Sertifikat untuk individu sesuai standar interoperabilitas Kemenkominfo versi 1.5
2.16.360.1.1.1.7.2	Sertifikat untuk badan usaha sesuai standar interoperabilitas Kemenkominfo versi 1.5
2.16.360.1.1.1.4.3	Verifikasi Level 3 sesuai standar interoperabilitas Kemenkominfo versi 1.5
2.16.360.1.1.1.4.4	Verifikasi Level 4 sesuai standar interoperabilitas Kemenkominfo versi 1.5

1.3. Partisipan IKP / PKI Participants

1.3.1. Penyelenggara Sertifikasi Elektronik (PSrE) / Certification Authorities

1.3.1.1. PSrE Induk Indonesia / Root CA Indonesia

PSrE Induk Indonesia adalah Induk dari PSrE Indonesia di dalam ranah IKP Indonesia sebagaimana diatur dalam ketentuan peraturan perundang-undangan yang dioperasikan oleh Kementerian Komunikasi dan Informatika Republik Indonesia (Kominfo). PSrE Induk Indonesia membawahi 2 (dua) jenis PSrE Indonesia yaitu PSrE Indonesia Instansi dan PSrE Indonesia Non-Instansi yang

Root CA Indonesia is the root from Indonesian CAs within Indonesia PKI according to laws and regulations which is operated by the Ministry of Communication and Informatics of the Republic of Indonesia (Kominfo). Root CA Indonesia oversees 2 (two) types of Subordinate CAs, Indonesia Government CAs and Indonesia Non-Government CAs where in this case including VIDA. Root CA Indonesia is

dalam hal ini termasuk VIDA. PSrE Induk Indonesia bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Indonesia, sebagaimana dirinci dalam CP PSrE Induk Indonesia.

responsible for all aspects of the issuance and management of those Subordinate Indonesia CA certificates, as detailed in Root CA Indonesia's CP.

1.3.1.2. PSrE Indonesia / Indonesian CAs

VIDA merupakan PSrE Indonesia Non-Instansi yaitu PSrE yang menerbitkan Sertifikat kepada Pemilik yang merupakan warga negara Indonesia, warga negara asing, dan entitas sekaligus menyediakan layanan pemanfaatan Sertifikat elektronik tersebut. VIDA beroperasi sesuai dengan ketentuan peraturan perundang-undangan terkait penyelenggaraan sertifikasi elektronik. Di wilayah IKP Indonesia, VIDA tidak menjadi induk bagi PSrE Indonesia lain dan tidak berinduk kepada PSrE Indonesia lain kecuali PSrE Induk Indonesia.

VIDA bertanggung jawab terhadap pengelolaan Sertifikat VIDA dan Sertifikat Pemilik, sebagaimana dirinci dalam CPS ini termasuk:

a. Pengendalian terhadap proses pendaftaran;
b. Proses identifikasi dan autentikasi;
c. Proses penerbitan Sertifikat;
d. Proses pembaruan Sertifikat;
e. Proses *re-key* Sertifikat;
f. Proses pencabutan Sertifikat,
g. Publikasi Sertifikat,
h. Publikasi CRL;
i. Validasi Sertifikat;
j. Membangun dan memelihara sistem PSrE;
k. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan VIDA dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CPS ini.

VIDA is a Subordinate Non-Government CA which issues certificates to Subscriber who are Indonesia citizens, foreigners, and entities as well as provides the services utilizing such certificates. VIDA operates pursuant to the prevailing laws and regulations in Indonesia concerning CA operation. In Indonesia PKI, VIDA does not become the root CA of other Indonesia CA and not rooted under other Indonesia CA but only to Root CA Indonesia.

VIDA shall be responsible for all aspects of the issuance and management of its own VIDA's certificate and Subscriber's certificate, as per detailed in this CPS including:

a. The control over the registration process;
b. The identification and authentication process;
c. The certificate issuance process;
d. The certificate renewal process;
e. The certificate re-key process;
f. The certificates revocation process;
g. The certificates publication;
h. CRLs publication;
i. The certificate validation;
j. Build and maintain CA system;
k. Ensuring that all aspects of the services, operations, and infrastructures related to VIDA are performed in accordance with the requirements, representations, and warranties of this CPS.

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

Dalam hal VIDA bertindak secara langsung untuk menerima permohonan pemrosesan Sertifikat dari Pemohon, maka VIDA berperan sebagai RA bagi dirinya sendiri.

In the event that VIDA acts directly to accept the request for certificate processing from the Applicant, VIDA acts as RA for itself.

VIDA juga menunjuk Otoritas Pendaftaran tertentu (RA eksternal) untuk melakukan identifikasi dan autentikasi Pemilik, penerimaan permohonan pemrosesan Sertifikat seperti penerbitan dan pencabutan Sertifikat sesuai dengan yang telah didefinisikan pada CPS ini dan melaporkan hasil kegiatan kepada VIDA. VIDA memiliki hak untuk melakukan audit dan pemeriksaan terhadap keamanan dan kesesuaian fungsi yang dijalankan sesuai perjanjian antara VIDA dengan RA eksternal. Kerja sama dengan RA eksternal tidak melepaskan tanggung jawab VIDA sebagai PSrE Indonesia sesuai dengan ketentuan peraturan perundang-undangan.

RA, baik yang diselenggarakan oleh VIDA maupun oleh pihak RA eksternal, menyelenggarakan fungsi otoritas pendaftaran sesuai dengan ketentuan peraturan perundang-undangan.

VIDA also designates a specific Registration Authority (external RA) to perform identification and authentication of Subscribers, as well as accepting certificate processing requests such as issuance and revocation requests as defined in this CPS, and report the activity to VIDA. VIDA has the right to carry out audits and checks on the security and conformity of functions performed by RA in accordance with the agreement between VIDA and the external RA. Cooperation with external RA does not waive VIDA's responsibilities as a CA in accordance with the provisions of laws and regulations.

The RA, whether performed by VIDA or by the external RA, carries out the function of the registration authority in accordance with the provisions of laws and regulations.

1.3.2.1. Fungsi dari RA / Function of Registration Authorities

RA berkewajiban untuk melaksanakan fungsi otoritas pendaftaran sesuai dokumen prosedur yang ditetapkan oleh VIDA, meliputi hal-hal sebagai berikut:

a. melakukan identifikasi dan autentikasi Pemohon Sertifikat;
b. memulai, meneruskan, memeriksa permohonan pemrosesan Sertifikat; dan
c. menyetujui atau menolak permohonan pemrosesan Sertifikat.

The RA is obliged to perform certain functions pursuant to procedure specified by VID, including the following:

a. perform identification and authentication of Applicants;
b. initiate,pass along, or check certificate processing request; and
c. approve or reject requests for certificate processing.

1.3.3. Pemilik / Subscribers

Pemilik adalah pihak yang identitasnya tertera dalam Sertifikat yang diterbitkan oleh VIDA dan sudah melalui proses verifikasi. Pemilik berarti subjek pemegang Sertifikat yang terikat dengan VIDA dalam penerbitan Sertifikat. Sebelum dilakukan verifikasi identitas dan diterbitkannya Sertifikat,

Subscribers are entities whose identity has been verified and is displayed in a Certificate issued by VIDA. Subscriber refers to the subject of the certificate that is contracted with the VIDA for the certificate's issuance. Prior to verification of identity and issuance

Pemilik disebut sebagai Pemohon. VIDA boleh menerbitkan Sertifikat kepada Pemilik mana saja yang tidak terkait dengan keperluan dinas Kementerian/Instansi pemerintah Indonesia. Kewajiban Pemilik terkait dengan penyelenggaraan Sertifikasi Elektronik dideskripsikan pada Perjanjian Kepemilikan *(Subscriber Agreement)*.

of a certificate, a Subscriber is called an Applicant.
VIDA may issue certificates to any Subscriber which are not for Indonesia Ministry or Government institution purposes. Subscriber's obligations regarding the Certification Authority governance are described in the Subscriber Agreement.

1.3.4. Pengandal / Relying Parties

Pengandal adalah pihak yang mempercayai Sertifikat, tanda tangan elektronik dan/atau layanan lainnya yang memanfaatkan Sertifikat yang disediakan oleh VIDA. Pengandal harus terlebih dahulu memeriksa respon yang sesuai dari *Online Certificate Status Protocol* (OCSP) atau *Certificate Revocation Lists* (CRL) yang disediakan oleh VIDA sebelum memanfaatkan informasi yang ada dalam Sertifikat.
Pengandal mengandalkan keabsahan keterkaitan antara nama Pemilik dengan Kunci Publik. 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 untuk:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi tanda tangan elektronik;
c. Memeriksa status pencabutan Sertifikat baik melalui CRL atau OCSP; dan
d. Penyetujuan batas tanggung jawab dan jaminan.

Pengandal meliputi lembaga keuangan, perusahaan swasta, institusi pemerintah dan pihak lainnya yang mengandalkan Sertifikat, tanda tangan elektronik, dan/atau layanan lainnya yang memanfaatkan Sertifikat yang disediakan oleh VIDA.

Relying Parties are parties that rely on certificates, digital signatures, and/or other services utilizing such certificates provided by VIDA. Relying Parties must check the appropriate response from the Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRL) provided by VIDA before relying on information featured in a certificate.

A Relying Party relies on the validity of the Subscriber's name attached to the Public Key. The Relying Party is responsible for checking the status of the information in the certificate. A Relying Party may use the information in the certificate to determine the conformity of the certificate to particular use and purposes such as:

a. Checking for which purpose a certificate is 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 financial institutions, private companies, government institutions and other party which rely on certificate, digital signatures, and/or other services utilizing such certificates provided by VIDA

1.3.5. Partisipan Lain / Other Participants

VIDA menentukan partisipan lain yang berhubungan dengan penyelenggaraan sertifikasi elektronik. Dalam hal VIDA bekerja sama dengan partisipan lain untuk menyelenggarakan layanannya, VIDA mendapat persetujuan dari Kominfo.

VIDA designates other participants that are related to the CA operation. In the event that VIDA cooperates with other participants to provide its services, VIDA shall get approval from Kominfo.

1.3.5.1. Penyedia Layanan Pusat data / Data Center Vendor

Penyedia layanan Pusat Data adalah pihak ketiga yang menyediakan layanan Pusat Data untuk operasional VIDA. VIDA menunjuk penyedia Pusat Data yang menerapkan standar keamanan yang tinggi dan memenuhi persyaratan keamanan informasi yang relevan serta melaksanakan audit reguler.

Data Center vendor is a third party that provides Data Center service for VIDA Operation. VIDA will appoint a highly secure Data Center provider and ensure it complies with all relevant security requirements and undergo regular audits.

1.4. Kegunaan Sertifikat / Certificate Usage

1.4.1. Penggunaan Sertifikat yang Semestinya / Appropriate Certificate Uses

Sertifikat VIDA hanya dapat digunakan untuk menandatangani Sertifikat Pemilik, CRL, OCSP, dan Sertifikat penanda waktu, serta untuk verifikasi Sertifikat.

VIDA's Certificate can only be used for signing Certificates, CRLs, OCSP and time stamp Certificates, as well as for verification of Certificates

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

a. Tanda Tangan Elektronik;
b. Nirsangkal;

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. Digital Signature;
b. Non-Repudiation;

VIDA menyediakan tingkat jaminan yang dapat disesuaikan dengan kebutuhan transaksi, layanan tertentu, ataupun kebutuhan Pengandal. Sertifikat Pemilik yang diterbitkan oleh VIDA dibedakan menjadi beberapa level Sertifikat sesuai aturan yang ditetapkan pada Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk. Adapun VIDA telah menentukan level sertifikat yang akan diterima Pemilik sesuai dengan layanan yang disediakan oleh VIDA. Level Sertifikat yang dimaksud adalah sebagai berikut:

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

VIDA provides a level of assurance that can be tailored to the needs of a particular transaction, service, or Relying Party's need. Subscriber's Certificates issued by VIDA are divided into several levels of certificates in accordance with the rules stipulated in the Identity Verification Standards issued by Root CA Indonesia. Meanwhile, VIDA has determined the level of certificate that the Subscriber will receive in accordance with the services provided by VIDA.The level of Certificate is as follows:

Inappropriate use of certificates may result in the voiding of warranties offered by VIDA to Subscribers and their Relying Parties.

Tipe Pengguna / Subscriber Type	**Metode Verifikasi / Verification Method**	**Level Sertifikat / Certificate Level**	**Tingkat Jaminan/ Identity Assurance Level**	**Penggunaan / Utilization**
Individu WNI/ Individual of Indonesia citizen	online	Level 2	medium	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNI / Individual of Indonesia citizen	offline	Level 3	tinggi / high	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNI yang berafiliasi dengan badan usaha/ Individual of Indonesia citizen with business entity affiliation	online	Level 2	medium	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNI yang berafiliasi dengan badan usaha/ Individual of Indonesia citizen with business entity affiliation	offline	Level 3	tinggi / high	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNA/ Individual of foreign citizen	online	Level 2	medium	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNA / Individual of foreign citizen	offline	Level 3	tinggi / high	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature

Individu WNA yang berafiliasi dengan badan usaha/ Individual of foreign citizen with business entity affiliation	online	Level 2	medium	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Individu WNA yang berafiliasi dengan badan usaha/ Individual of foreign citizen with business entity affiliation	offline	Level 3	tinggi / high	tanda tangan elektronik tersertifikasi (tanda tangan digital) / digital signature
Badan usaha di wilayah Indonesia / Business entity in Indonesia	online	Level 3	high	segel elektronik / e-seal

1.4.2. Penggunaan Sertifikat yang Dilarang / Prohibited Certificate Uses

Sertifikat Pemilik yang diterbitkan sesuai CPS ini dilarang dipakai untuk penggunaan yang tidak dinyatakan pada bagian 1.4.1.

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

1.5. Administrasi Kebijakan / Policy Administration

Dokumen CPS VIDA dikelola oleh *Policy Authority* (PA) VIDA. PA VIDA adalah bagian dari Peran Terpercaya VIDA yang memiliki peran dan tanggung jawab sebagai berikut:

a. Menyusun dan menetapkan dokumen CPS;
b. Memastikan semua layanan, operasional, dan infrastruktur PSrE yang didefinisikan dalam CPS telah dilakukan sesuai dengan CP PSrE Induk; dan

CP and CPS of VIDA are managed by VIDA's Policy Authority (PA). VIDA's PA is part of VIDA Trusted Roles who has roles and responsibilities as follows:

a. Composes and approves the CPS document;
b. Ensures that all aspects of the CA services, operations, and infrastructure as described in the CPS are well performed in accordance with Root CA Indonesia's CP;

1.5.1. Organisasi Pengelola Dokumen / Organization Administering the Document

CPS dan dokumen referensi lainnya dikelola oleh PA VIDA.

PA dapat dihubungi melalui
compliance@vida.id
Telepon: 021 2598 3275

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

PA can be contacted via
compliance@vida.id
Phone: 021 2598 3275

1.5.2. Kontak / Contact Person

Pemilik, Pengandal, maupun pihak ketiga lainnya dapat menghubungi VIDA melalui *email* untuk melaporkan dugaan kompromisasi Kunci Privat, penyalahgunaan Sertifikat, maupun penyalahgunaan lainnya terhadap Sertifikat.
Alamat: WTC 1 Lantai 13 Jl. Jenderal Sudirman Kav. 29-31, Kota Jakarta Selatan, DKI Jakarta, 12920
Email: support@vida.id
URL: https://www.vida.id
Telp: 021 2598 3275

Subscribers, Relying Parties, and other third parties can contact VIDA by email to report suspected Private Key compromise, certificate misuse, or other types of fraud, inappropriate conduct, or any other matter related to certificates.
Mailing address: WTC 1 13th Floor Jl. Gen. Sudirman Kav. 29-31, South Jakarta, DKI Jakarta, 12920
Email: support@vida.id
URL: https://www.vida.id
Telp: 021 2598 3275

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

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

Policy Authority (PA) determines suitability of this CPS and the conformance of the CPS to Root CA Indonesia's CP. PA receives input from Trusted Role members, regulators, and external auditors to make changes to tCPS documents, and then monitor the suitability and applicability of the document together with other Trusted Role members.

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

PA VIDA menyetujui CPS VIDA dan segala perubahannya setelah mendapat persetujuan dari PA PSrE Induk. Perubahan dibuat dengan mengubah seluruh atau sebagian isi dari CPS dan mempublikasikan dokumen versi terbaru dari CPS yang telah disetujui. PA VIDA menentukan apakah perubahan atas CPS ini membutuhkan pemberitahuan atau perubahan OID.

VIDA's PA approves VIDA's CPS and any amendments after getting acknowledgement from Root CA Indonesia's PA. Amendments are made by either updating the entire or partial content of the CPS and publishing the updated version of the CPS document. VIDA's PA determines whether an amendment to this 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.

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

2.1. Repositori / Repositories

VIDA memelihara repositori daring yang dapat diakses publik melalui internet sebagai tempat publikasi *file* atau dokumen yang bersifat publik. *File* atau dokumen yang dimaksud antara lain namun tidak terbatas pada:

a. Sertifikat VIDA,
b. CRL,
c. CP/CPS,
d. Perjanjian Kepemilikan Sertifikat,
e. Perjanjian Pengandal,
f. Kebijakan Privasi,
g. Kebijakan Jaminan.

Dokumen dapat dibuat menggunakan dwibahasa. Dalam hal terjadi ketidaksesuaian antara versi bahasa Indonesia dengan versi bahasa Inggris, maka versi bahasa Indonesia didahulukan.

VIDA berhak untuk tidak mengunggah dokumen penunjang VIDA lainnya yang tidak bersifat publik.

VIDA maintains an online repository that is publicly accessible via the internet as a place for publication of files or documents intended for the public. The files or documents are but not limited to:

a. VIDA certificate,
b. CRL,
c. CP/CPS,
d. Subscriber Agreement,
e. Relying Party Agreement,
f. Privacy Policy,
g. Warranty Policy.

Documents can be made bilingual. In the event of a mismatch between the Indonesian version and the English version, the Indonesian version takes precedence.

VIDA has rights not to publish other documents which are not for the public.

2.2. Publikasi Informasi Sertifikat / Publication of Certification Information

VIDA mempublikasikan Sertifikat VIDA beserta *file* atau dokumen yang disebutkan pada bagian 2.1 di repositori resmi milik VIDA dapat diakses pada laman https://www.repo.vida.id yang dilengkapi dengan pengamanan SSL/TLS yang terpercaya.

VIDA publishes the files and documents stipulated in section 2.1 in the authorized VIDA's repository which can be accessed at https://www.repo.vida.id that is equipped with trusted SSL/TLS security.

2.3. Waktu atau Frekuensi Publikasi / Time or Frequency of Publication

VIDA mempublikasikan Sertifikat VIDA dalam repositori VIDA segera setelah diserahkan oleh PSrE Induk Indonesia kepada VIDA.

Perubahan pada CPS dan dokumen penunjang sesuai bagian 2.1 harus dapat diakses publik dalam 7 (tujuh) hari kalender setelah disetujui.

VIDA publishes VIDA certificates on VIDA's repository immediately after being handed over from Indonesia Root CA Indonesia to VIDA.

The changes of CPS and other supporting documents mentioned in Section 2.1 shall be made publicly available within 7 (seven) calendar days after its approval.

CRL diperbaharui dan dipublikasikan secara reguler dan terjadwal sesuai pengaturan pada bagian 4.9.7.

The CRL is updated and published regularly as per schedule according to section 4.9.7.

2.4. Kendali Akses pada Repositori / Access Controls on Repositories

Informasi yang terpublikasi pada repositori adalah informasi publik. VIDA 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. VIDA provides unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

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

VIDA protects information not intended for public dissemination or modification.

Manajer repositori mengoperasikan repositori dan bertanggung jawab atas kendali akses pada repositori VIDA.

Repository manager operates the repository and responsible for the access control of VIDA's repository.

3. IDENTIFIKASI DAN AUTENTIKASI / IDENTIFICATION AND AUTHENTICATION

3.1. Penamaan / Naming

3.1.1. Tipe Nama / Types of Names

VIDA membuat dan menandatangani Sertifikat dengan subjek *Distinguished Name (DN)* yang *non-null* dan mematuhi standar ITU X.500 serta mengacu pada pengaturan parameter sesuai Standar Interoperabilitas PSrE Indonesia. Tabel di bawah meringkas DN dari Sertifikat yang diterbitkan oleh VIDA.

VIDA generates and signs certificates with a non-null subject Distinguished Name (DN) that complies with the ITU X.500 standards, and also refer to Certificate parameters stipulated in Indonesian CA Interoperability Standard. The table below summarizes the DN of the certificates issued by the VIDA.

Tipe Pemilik Sertifikat/ Subscriber Type		**Distinguished Name (DN)**
Sertifikat VIDA / VIDA Certificate		(CN=<Certification Authority Name>, OU=CA, O=PT Indonesia Digital Identity, C=ID)
Sertifikat Pemilik / Subscriber Certificate	Individual	(CN={Name} , OU=Personal, O=<empty>, C=ID,)
	Individual with affiliation	(CN={Name} , OU={organization unit*}, O={organization name*}, C=ID, T={title*})
	Business Entity	(CN={Business Entity Legal Name} , C=ID)

*field opsional yang dapat diisi apabila verifikasi dilakukan hingga level tersebut

*optional fields that can only be filled if verification is carried out up to that level

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

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

Nama Pemilik yang terkandung dalam Sertifikat harus bermakna dalam arti bahwa VIDA memiliki bukti keterkaitan yang cukup antara nama Pemilik dengan dokumen

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

The Subscriber's name contained in a certificate must be meaningful in the sense that the VIDA has proper evidence of the existent association between the Subscriber

identitasnya. Untuk mencapai tujuan ini, penggunaan nama harus diotorisasi oleh Pemilik yang sah atau perwakilan resmi dari Pemilik yang sah.

name with the identity document to which they belong. To achieve this goal, the use of a name must be authorized by the rightful Subscriber or a formal representative of the rightful Subscriber.

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

VIDA tidak menerbitkan Sertifikat anonim atau pseudonim.

VIDA does not issue anonymous or pseudonymous certificates.

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

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

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

3.1.5. Keunikan Nama / Uniqueness of Names

Distinguished name (DN) untuk Sertifikat VIDA harus unik.

Distinguished names (DN) for VIDA certificate shall be unique.

Sertifikat Pemilik yang diterbitkan oleh VIDA akan selalu unik yang dibuktikan lewat nomor seri Sertifikat yang unik.

Subscriber Certificates issued by VIDA will always be unique which is indicated by the unique certificate serial number.

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

Pemilik tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. VIDA tidak memverifikasi penggunaan merek dagang sepanjang pemrosesan permohonan Sertifikat.

Subscriber may not request certificates with any content that infringes the intellectual property rights of another party. VIDA will not verify trademark use during certificate application processing

VIDA dapat menolak setiap permohonan atau melakukan pencabutan Sertifikat apapun yang menjadi bagian dari sengketa merek dagang.

VIDA may reject any application or require revocation of any certificate that is part of a trademark dispute

3.2. Validasi Identitas Awal / Initial Identity Validation

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

Metode untuk membuktikan kepemilikan Kunci Privat Pemilik yang dilakukan oleh VIDA adalah sebagai berikut:

The method to prove possession of a Subscriber;s Private Key performed by VIDA is as follows:

Metode untuk membuktikan kepemilikan Kunci Privat pada *secure usb token* adalah dengan membandingkan Kunci Publik pada Sertifikat dengan Kunci Publik pada PKCS#10.

The method to prove possession of a Private Key in a secure usb token is by comparing the public key on the certificate with the public key in PKCS # 10.

Metode untuk membuktikan kepemilikan Kunci Privat lewat aplikasi *smartphone* maupun aplikasi web untuk penyimpanan Kunci Privat Pemilik pada *VIDA Vault* 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 the possession of the Private Key on the smartphone application and web application for Subscriber’s Private Key that is stored in VIDA vault 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.

Metode untuk membuktikan kepemilikan Kunci Privat juga dapat dilakukan oleh Pemilik dengan menunjukkan keberhasilan penggunaan Kunci Privat dan Sertifikat Pemilik sesuai bagian 4.5.1.

The method to prove the possession of the Private Key can also be carried out by the Subscriber by demonstrating the successful use of the Private Key and Certificate as per section 4.5.1.

3.2.2. Autentikasi dari Identitas Organisasi / Authentication of Organization Identity

VIDA menyediakan layanan yang memungkinkan suatu badan usaha yang memiliki izin usaha untuk beroperasi di wilayah Republik Indonesia menjadi Pemilik. Autentikasi Badan Usaha yang mengajukan permohonan Sertifikat mengikuti persyaratan sesuai aturan yang ditetapkan pada Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk dan menyertakan rincian tentang Badan Usaha dan salinan surat-surat pendirian Badan

VIDA provides a service where an entity operating in Indonesia can become Subscriber. Authentication of the Business Entity submitting
Certificate applications follow the requirements in accordance with the rules stipulated in the Identity Verification Standards issued by Root CA Indonesia and submit copies of the Business Entity establishment documents.

Usaha. Badan usaha yang mengajukan permintaan pemrosesan Sertifikat dari VIDA, maka Pemohon wajib menyampaikan informasi berikut:

Business Entity who submits a request for certificate processing from VIDA, the Applicant must submit the following information:

Tipe Pemilik/ ***Subscriber type***	**Detil Permohonan/** ***Request detail***
Badan Usaha di wilayah Indonesia / Business Entity located in Indonesia	1. NPWP badan usaha *Entity tax* 2. SIUP *entity operation permit* 3. apabila SIUP tidak tersedia maka dokumen alternatif dapat berupa: *If SIUP is not available, alternative documents can be in the form of:* a. NIB b. Akta Pendirian dan SK Menkumham *Deed of Establishment and Decree of the Minister of Law and Human Rights* c. Akta Perubahan anggaran dasar *Deed of Amendment to Articles of Association* d. Akta daftar direksi terbaru *Latest deed of board of directors* e. Company Domicile Letter Surat Domisili Perusahaan 4. Identitas dari perwakilan entitas sesuai dengan bagian 3.2.3 *Identity of the entity's representative in accordance with section 3.2.3* 5. surat keterangan kerja dari perwakilan entitas *employment certificate from the entity's representative* dengan persetujuan Pemohon, dan dengan pernyataan dari pemohon bahwa setiap informasi yang disampaikan sudah benar dan akurat. *upon the consent of the applicant, and upon the applicant's statement that all information submitted is true and accurate.*

VIDA melakukan verifikasi terhadap keberadaan entitas, verifikasi terhadap identitas perwakilan entitas sesuai dengan bagian 3.2.3, serta kebenaran atas hubungan perwakilan entitas dengan entitas tersebut sesuai dengan bagian 3.2.5.

VIDA verifies the existence of the entity, the identity of the entity's representative in accordance with sections 3.2.3 as well as the correctness of the relationship of the entity's representative with the entity they belong to in accordance with sections 3.2.5.

3.2.3. Autentikasi Identitas Individu / Authentication of Individual Identity

Perbedaan level Sertifikat berdasarkan aktivitas verifikasi identitasnya dapat mengacu pada bagian 1.4.1.

The differentiation level of certificates obtained based on such identity verification activity can be referred to section 1.4.1.

Terkait identifikasi dan autentikasi identitas Pemilik yang mengajukan permintaan pemrosesan Sertifikat dari VIDA, maka Pemohon wajib menyampaikan informasi berikut:

For the purpose of identification and authentication of the Subscriber who submits certificate processing request to VIDA, the Applicant shall submit following information:

Tipe Pemilik ***Subscriber type***	**WNI** ***Indonesia citizen***	**WNA** ***foreigner***
Individu/ *Individual*	1. nama; *name;* 2. nomor kartu identitas NIK dari KTP; *Identity card number NIK from KTP;* 3. tanggal lahir; *date of birth;* 4. alamat surat elektronik (email) dan/atau nomor telepon; *electronic mail address and/or phone number;* 5. foto wajah; dan *face photo; dan* 6. VIDA berhak meminta dokumen pendukung identitas seperti foto KTP, paspor, dan SIM apabila diperlukan; *VIDA has right to request identity supporting document such as KTP image, passport and driver license if necessary;* dengan persetujuan pemohon, dan dengan pernyataan dari pemohon bahwa setiap informasi yang disampaikan sudah benar dan akurat. *upon the consent of the applicant, and upon the applicant's statement that all information submitted is true and accurate.*	1. nama; *name;* 2. paspor dan dokumen pendukung identitas; *passport and identity supporting document;* 3. tanggal lahir; *date of birth;* 4. alamat surat elektronik (email) dan/atau nomor telepon; *email address and/or phone number;* 5. foto wajah; *face photo;* 6. VIDA berhak meminta dokumen pendukung identitas berupa: *VIDA has right to request identity supporting document such as:* a. izin tinggal (KITAS/KITAP), atau *living permit , or* b. kartu identitas nasional dan surat keterangan kerja, atau *National ID card and employment letter, or* c. kartu identitas nasional dan bukti alamat surat menyurat, atau *National ID card and mailing address proof, or* d. kartu identitas nasional dan surat keterangan dari pihak berwenang *National ID card and attestation letter from authorities,* dengan persetujuan pemohon, dan dengan pernyataan dari pemohon bahwa setiap informasi yang disampaikan sudah benar dan akurat. *upon the consent of the applicant, and upon the applicant's statement that all information submitted is true and accurate.*
Individu dengan afiliasi /	1. verifikasi terhadap identitas Pemohon sesuai dengan bagian 3.2.3 untuk jenis Pemilik individu sesuai kewarganegaraannya;	

Individual with affiliation	*verify the identity of the Applicant in accordance with section 3.2.3 of individual subscriber verification based on the nationality;* 2. verifikasi terhadap kewenangan atau afiliasi Pemohon sesuai dengan bagian 3.2.5; *verify the authority or affiliation of the Applicant in accordance with section 3.2.5;* 3. verifikasi terhadap keabsahan badan usaha: *verify the entity existence:* a. Pemohon menyertakan nama organisasi dan alamat dalam permohonan Sertifikat untuk memverifikasi keberadaan organisasi tersebut. *Applicant include the information of entity's name and address to verify its existence;* b. Untuk tujuan identifikasi dan autentikasi identitas organisasi tersebut, VIDA dapat meminta dokumentasi resmi badan usaha sesuai bagian 3.2.2 dan/atau memanfaatkan berbagai sarana yang ada termasuk dengan menjalin komunikasi dengan perwakilan badan usaha, memeriksa informasi yang terdapat pada institusi yang mengatur pengakuan hukum badan usaha, atau memanfaatkan rujukan ke basis data pihak ketiga yang andal. *For the purpose of identification and authentication of the organization's identity, VIDA may request for official entity documentation in accordance with section 3.2.2 and/or utilize any channel to communicate with the entity representatives, check the information residing in the institution governing the entity's legal recognition, or making reference to reliable third-party database.*
Badan usaha / *Business entity*	lihat bagian 3.2.2 see section 3.2.2

Selanjutnya VIDA melakukan verifikasi identitas individu dengan melakukan pencocokan data demografi serta pencocokan data biometrik dalam bentuk swafoto yang diuji secara *liveness*, terhadap basis data kependudukan yang dikelola oleh lembaga pemerintah yang menyelenggarakan administrasi kependudukan, sesuai aturan yang ditetapkan pada Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk.

Hereinafter, VIDA verifies individual identities by matching demographic data and matching biometric data in the form of selfie photo tested with liveness detection, against population data managed by government agencies that carry out population administration, in accordance with the rules stipulated in the Identity Verification Standards issued by Root CA Indonesia.

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

Informasi yang tidak bisa diverifikasi tidak boleh disertakan di dalam Sertifikat. VIDA tidak akan menerbitkan Sertifikat bagi Pemohon yang datanya tidak terverifikasi,

Information that is not verified shall not be included in certificates. VIDA will not issue the certificate for the Applicant if the data is not

informasi tersebut akan disimpan sebagai bagian dari *audit trail*.

verified, the information will be stored as part of the audit trail.

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 badan usaha 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 a business entity to obtain a certificate.

Sertifikat dapat mencantumkan afiliasi badan usaha secara eksplisit apabila sudah dipastikan bahwa Pemohon memiliki otorisasi untuk bertindak atas kapasitas tertentu di badan usaha tersebut.

Certificates may contain explicit business entity affiliation only after ascertaining the Applicant has the authorisation to act on its capacity in the business entity.

VIDA bertanggung jawab untuk memverifikasi dan mengautentikasi perwakilan resmi dengan memeriksa dokumen berikut:

a. Surat penunjukan / surat keterangan kerja / surat kuasa, atau
b. Cara lainnya ataupun tantangan yang mampu membuktikan afiliasi dengan badan usaha.

VIDA is responsible for verifying and authenticating an authorized representative by checking the following documents:

a. Appointment Letter/ employment letter / power of attorney, or
b. Any means or challenge that may prove the affiliation with the business entity.

3.2.6. Kriteria Inter-Operasi / Criteria for Interoperation

Interoperasi antar PSrE Indonesia diatur dalam Standar Interoperabilitas PSrE Indonesia yang diterbitkan oleh PA PSrE Induk.

Interoperability between Indonesian CAs are elaborated in CA Interoperability Standards issued by Root CA's PA.

3.3. Identifikasi dan Autentikasi untuk Permintaan Penggantian Kunci (Re-Key) / Identification and Authentication for Re-Key Requests

Sebelum masa berlaku Sertifikat berakhir, Pemilik dapat meminta penggantian kunci yang selanjutnya disebut re-key dan Pemilik diautentikasi melalui penandatanganan menggunakan Sertifikat yang berlaku atau metode pembuktian kepemilikan Kunci Pemilik sebagaimana diatur pada Bagian 3.2.1 dan/atau 4.5.1.

Prior to the expiry of a Certificate, Subscribers may request for a re-key and Subscribers is authenticated through signing using their current Certificates or by demonstrating possession of Subscriber Private Key as described in Section 3.2.1 and/or 4.5.1

3.3.1. Identifikasi dan Autentikasi untuk kegiatan Re-Key Rutin / Identification and Authentication for Routine Re-Key

Re-key dilakukan secara *adhoc* sesuai dengan bagian 4.7, penggantian Sertifikat secara rutin tidak disediakan.

Re-key is performed on an adhoc basis as specified in section 4.7, certificate routine re-key is not provided for Subscriber.

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

Pemilik yang mengajukan permohonan *re-key* setelah Sertifikat dicabut harus menjalani proses pembuatan Sertifikat baru sesuai dengan bagian 3.2 dan 4.2.1.

A Subscriber requesting re-key after a certificate is revoked shall undergo the initial registration process as specified in section 3.2 and 4.2.1.

3.4. Identifikasi dan Autentikasi untuk Permintaan Pencabutan / Identification and Authentication for Revocation Request

Permintaan pencabutan Sertifikat selalu diautentikasi oleh VIDA menggunakan Kunci Publik yang terhubung dengan Sertifikat, memvalidasi kepemilikan Kunci Privat Pemilik dengan cara mengautentikasi Pemilik terhadap akun VIDA miliknya dan memastikan keabsahan permohonan. Apabila Permintaan pencabutan dilakukan oleh Pemohon yang merupakan perwakilan Pemilik, maka VIDA melakukan autentikasi terhadap Pemohon untuk memastikan Pemohon tersebut memiliki otorisasi yang sesuai, sesuai dengan bagian 3.2.5.

Revocation requests are always authenticated by VIDA using that certificate's associated Public Key, validating Subscriber's Private Key possession by authenticating the Subscriber to their VIDA account, and ensuring the validity of the request. If the revocation request is raised by an Applicant who is a representative of the Subscriber, then VIDA authenticates the Applicant to ensure that the Applicant has the appropriate authorization, in accordance with section 3.2.5.

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

4.1. Permohonan Sertifikat / Certificate Application

4.1.1. Siapa yang dapat mengajukan sebuah permohonan Sertifikat / Who can Submit a Certificate Application

Pihak yang dapat mengajukan permohonan Sertifikat ke VIDA adalah

a. individu perorangan;
b. individu dengan afiliasi dengan badan usaha (bukan institusi pemerintah).
c. badan usaha.

Those who can submit certificate application to VIDA are

a. individual person;
b. individual with entity affiliation (non-government institution).
c. business entity

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

VIDA memelihara sistem dan memiliki proses yang memadai agar dapat mengautentikasi identitas Pemohon untuk semua jenis Sertifikat. Pemohon harus mengirimkan informasi yang cukup dan akurat sehingga memungkinkan VIDA dan/atau RA melakukan verifikasi yang diperlukan. VIDA dan RA harus melindungi jalur komunikasi dan menyimpan secara aman informasi yang diperoleh dari Pemohon sesuai dengan Kebijakan Privasi VIDA.

Secara umum, proses pendaftaran mencakup langkah-langkah berikut sesuai dengan bagian 3.2:

a. Pemohon melengkapi formulir pendaftaran dan menyiapkan informasi yang dibutuhkan dengan sebenar-benarnya;
b. Pemohon menyetujui Perjanjian Kepemilikan dan syarat ketentuan lain yang berlaku bersamaan dengan pengiriman permintaan pendaftaran tersebut.

VIDA maintains systems and sufficient processes to be able to perform authentication against the Applicant's identity for all certificate types. Applicants must submit sufficient and accurate information to enable VIDA and/or RA to successfully perform the required verification. VIDA and RA shall protect communication channels and securely store information presented by the Applicant during the enrollment process in compliance with the VIDA CA Privacy Policy.

Generally, the enrollment process includes the following steps in accordance with section 3.2:

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

4.2. Pemrosesan Permohonan Sertifikat / Certificate Application Processing

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

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

The identification and authentication of the Subscriber shall meet the requirements specified in sections 3.2.

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

Setelah semua pemeriksaan identitas dan atribut Pemohon, konten permohonan untuk Sertifikat juga diperiksa. Dalam hal Pemohon tidak berhak terhadap Sertifikat atau permohonannya terdapat kesalahan, VIDA harus menolak permohonan tersebut. Apabila tidak ada masalah, permohonan disetujui.

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

VIDA menolak permintaan pendaftaran yang validasi persyaratannya tidak lengkap, termasuk untuk alasan berikut;

a. VIDA dapat menolak permintaan pendaftaran berdasarkan pada potensi rusaknya merek VIDA.
b. VIDA juga dapat menolak permohonan pemrosesan Sertifikat yang sebelumnya melanggar kebijakan VIDA.

VIDA rejects requests for certificates where validation of all items cannot successfully be completed, including for the following reasons:

a. VIDA may reject requests based on potential brand damage to VIDA in accepting the request.
b. VIDA may also reject certificate processing requests from Applicants who have violated a provision of VIDA's policy.

VIDA tidak wajib untuk memberikan alasan kepada Pemohon terkait penolakan permohonan Sertifikat.

VIDA is under no obligation to provide a reason to an Applicant for rejection of a certificate request.

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

Semua pihak yang terlibat dalam proses permohonan Sertifikat harus melakukan usaha untuk memastikan permohonan Sertifikat diproses tepat waktu. Dalam hal Pemohon tidak berhak terhadap Sertifikat

All parties involved in certificate applications processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. In case the applicant is not eligible for a certificate or the

atau permohonannya mengandung kesalahan, Pemohon akan mendapatkan penolakan yang dapat diinformasikan melalui *email* atau media lainnya tidak lebih dari 4 (empat) hari kerja sejak permohonan diterima.

application contains faults, Applicant will accept the rejection that may be informed through email or via other media no more than 4 (four) working days after application is received.

Sertifikat harus diterbitkan tidak lebih dari 8 (delapan) hari kerja semenjak disetujuinya permohonan Sertifikat tersebut.

Certificate shall be issued no more than 8 (eight) working days after approval of certificate applications.

4.3. Penerbitan Sertifikat / Certificate Issuance

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

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

VIDA verifies the source of a certificate request before issuance. Certificates shall be checked to ensure that all fields and extensions are properly populated.

VIDA harus mengautentikasi permohonan Sertifikat, memastikan bahwa Kunci Publik memang terkait dengan Pemohon yang benar, mendapatkan bukti kepemilikan Kunci Privat, selanjutnya menerbitkan Sertifikat, dan memberikan Sertifikat ke Pemilik. Semua ini harus dilaksanakan secara tepat waktu, yang diuraikan pada bagian 4.2.

VIDA authenticates a 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, and provides the certificate to the Subscriber. This is done in a timely manner, which is detailed in section 4.2.

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

VIDA memberitahu Pemilik dalam selang waktu maksimum 2 (dua) hari kerja tentang berhasilnya penerbitan Sertifikat melalui *email* ataupun cara lainnya.

VIDA notifies the Subscriber within 2 (two) days of successful certificate issuance via email or other means.

4.4. Penerimaan Sertifikat / Certificate Acceptance

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

VIDA memberitahu Pemilik bahwa mereka perlu melakukan pemeriksaan atas semua informasi dalam Sertifikat sebelum menggunakan Sertifikat tersebut.
Sertifikat yang diterbitkan dianggap diterima dan Pemilik dianggap menerima semua informasi Sertifikat apabila

a. Pemilik menerima pemberitahuan penerbitan oleh VIDA, atau
b. tidak ada keluhan dari Pemilik dalam jangka waktu 7 (tujuh) hari kerja sebelum Pemilik menggunakan Sertifikat, atau
c. Pemilik menggunakan Sertifikat sesuai dengan peruntukannya, misalnya untuk pembubuhan tanda tangan digital.

VIDA notifies the Subscriber that they need to check all the information of the certificate prior to usage.

The issued Certificate is deemed accepted by Subscriber and Subscriber is deemed to accept all certificate information when:

a. Subscriber receive issuance notification from VIDA, or
b. there is no complaint from Subscriber within 7 (seven) working days, or
c. Subscriber uses the certificate according to its designation, for example for performing digital signing.

Pemilik dapat mengajukan permohonan pencabutan Sertifikat apabila Pemilik mendapati adanya ketidaksesuaian informasi atau kesalahan apapun pada Sertifikat sesuai dengan bagian 4.9.

Subscriber may raise revocation request if Subscriber finds that there is any discrepancy in the information or errors in the Certificate in accordance with section 4.9.

4.4.2. Publikasi Sertifikat oleh PSrE / Publication of the Certificate by the CA

VIDA mempublikasikan Sertifikat VIDA dalam suatu repositori sesuai dengan bagian 2, termasuk juga menerbitkan informasi pencabutan terkait Sertifikat Pemilik.

VIDA publishes VIDA's certificates in a repository based on section 2, as well as revocation information concerning Subscriber Certificates.

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

Tidak ditentukan.

No stipulation.

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

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

Pemilik harus melindungi Kunci Privat mereka dari penggunaan tanpa izin atau pengungkapan kepada atau oleh pihak lain, dan harus memakai Kunci Privat mereka hanya untuk tujuan yang sudah ditentukan sesuai bagian 7.

Subscriber shall protect their Private Key from unauthorized use or disclosure to or by other parties and shall use their Private Keys only for the intended purpose as per section 7.

Untuk Sertifikat Pemilik, pasangan kunci dapat dibangkitkan oleh VIDA lewat layanan *secure usb token,* aplikasi *smartphone,* dan aplikasi *web*, dengan syarat bahwa Kunci Privat diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS 140-2 sesuai bagian 6.1.1.2. VIDA melakukan upaya pengamanan yang wajar untuk melindungi Kunci Privat Pemilik dengan menggunakan modul kriptografi yang dikendalikan oleh Pemilik.

For Subscriber certificates, key pairs can be generated by VIDA, utilizing secure usb token service, smartphone application, and web application, given the condition that the Private Key is secured using a cryptographic module that meets the requirements of FIPS 140-2 in accordance to section 6.1.1.2. VIDA takes reasonable security measures to protect Subscriber's Private Key by using a cryptographic module which is controlled by the Subscriber.

VIDA menerapkan kombinasi paling sedikit 2 (dua) faktor autentikasi bagi Pemilik yang akan menggunakan Kunci Privatnya. Penggunaan Kunci Privat Pemilik tersebut hanya dapat diinisiasi oleh Pemilik setelah Pemilik berhasil melewati mekanisme autentikasi sebagai berikut:

a. akses kepada perangkat *usb token* dan pengetahuan atas *password* perangkat;
b. kepemilikan akun VIDA untuk *remote signing*, pengetahuan atas *username* dan *password* akun VIDA, verifikasi biometrik dan/atau *one time password* (OTP) yang dikirimkan ke perangkat seluler.

VIDA applies a combination of at least 2 (two) authentication factors for Subscribers who will use their Private Keys. Usage of the subscriber Private Key is initiated by Subscriber after Subscriber passed the authentication mechanism as follows:

a. access to usb token devices and knowledge of device passwords;
b. ownership of VIDA accounts for remote signing, knowledge of username and password of VIDA account, biometric verification and/or one time password (OTP) sent to mobile phone number.

Pemilik berkewajiban untuk senantiasa menjaga kerahasiaan faktor autentikasi di atas untuk melindungi dari penggunaan yang tidak sah.

Subscribers are obliged to constantly make the authentication factor private in order to protect from unauthorized use.

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

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

Relying Parties shall use software that is compliant with X.509. VIDA specifies restrictions on the use of a certificate through certificate extensions and the mechanism to determine certificate validity (using CRL and/or OCSP). Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties.

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

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

4.6. Pembaruan Sertifikat / Certificate Renewal

4.6.1. Kondisi untuk Pembaruan Sertifikat / Circumstance for Certificate Renewal

Pembaruan Sertifikat (renewal) didefinisikan sebagai penerbitan Sertifikat baru dengan menggunakan nama, kunci, dan informasi yang sama dengan Sertifikat lama yang belum kedaluwarsa, dimana masa berlaku dan *serial number* diperbarui. VIDA mengidentifikasi produk dan layanan di mana pembaruan dapat diterima. VIDA dapat memperbarui Sertifikat selama:

a. Sertifikat asli yang akan diperbarui belum dicabut, belum kedaluwarsa, atau tidak terkompromi;

Certificate renewal is defined as an issuance of a new Certificate with same name, keys, and information with the original unexpired Certificate, where validity and serial number is updated. VIDA will identify the products and services under which renewals can be accepted. VIDA may renew a Certificate so long as:

a. The original Certificate to be renewed has not been revoked, not expired, or not compromised;

b. Semua rincian dalam Sertifikat tetap akurat dan tidak diperlukan validasi baru atau tambahan.

b. All details within the Certificate remain accurate and no new or additional validation is required.

c. VIDA dapat memperbaharui Sertifikat yang sudah pernah diperbaharui sebelumnya selama masa berlaku Kunci Privat Pemilik belum berakhir.

c. VIDA may renew Certificates which have either been previously renewed as long as Subscriber's Private Key is within the validity period.

Apabila Kunci Privat Pemilik terkompromi atau sertifikat kedaluwarsa, maka Pemilik dapat mengajukan permohonan penerbitan Sertifikat baru sebagaimana diatur pada bagian 4.1.

If Subscriber's Private Key was compromised or the Certificate has expired, then the Subscriber can submit a new Certificate issuance as regulated in section 4.1.

VIDA menyediakan dukungan untuk pembaruan sertifikat terhadap sertifikat dalam perangkat USB token yang memenuhi kondisi di atas.

VIDA provides Certificate renewal for Certificates that are delivered in USB token devices which meet the above conditions.

VIDA tidak menyediakan pembaruan sertifikat terhadap sertifikat dengan masa berlaku pendek (30 menit) untuk tujuan penggunaan sekali pakai.

VIDA does not support Certificate renewal of short-term Certificates (30 minutes) for one-time use purposes.

4.6.2. Who May Request Renewal / Siapa Yang Dapat Meminta Pembaruan

Pembaruan Sertifikat hanya dapat diinisiasi atas permintaan Pemilik ke VIDA.

Certificate renewal may be initiated upon a subscriber's request to VIDA.

4.6.3. Processing Certificate Renewal Requests / Pemrosesan Permintaan Pembaruan Sertifikat

VIDA melakukan identifikasi dan autentifikasi permohonan pembaruan Sertifikat sesuai dengan bagian 3.2, 3.3, 4.5.1 dan penerbitan sesuai dengan bagian 4.3.

VIDA must identify and authenticate the Certificate renewal request as per section 3.2, 3.3, 4.5.1 and issuance as per section 4.3.

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

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

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

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

Pemilik menerima Sertifikat yang telah diperbarui sesuai dengan prosedur penerimaan Sertifikat yang tercantum pada bagian 4.4.1.	The Subscriber should receive the renewed Certificate following the same procedure of acceptance of a new Certificate, as stated in section 4.4.1.

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

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

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

Tidak ditentukan.	No stipulation.

4.7. Re-Key Sertifikat / Certificate Re-Key

4.7.1. Kondisi Re-Key Sertifikat / Circumstance for Certificate Re-Key

Penerbitan ulang Sertifikat dengan penggantian kunci (*re-key*) didefinisikan sebagai 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.	Certificate re-key is defined as an issuance of a new Certificate with a new Public Key, serial number and key identifier while retaining the other information from the original Certificate that describe the Subscriber. The new Certificate may be assigned a new validity period, specify a new CRL distribution point, and/or be signed with a different key.
Setelah *re-key* Sertifikat selesai dilakukan, VIDA dapat mencabut Sertifikat yang lama maupun membiarkan Sertifikat hingga kedaluwarsa dengan sendirinya.	After re-keying a certificate, VIDA may revoke the old certificate or let it expire eventually.
VIDA dapat melakukan *re-key* selama: a. Sertifikat lama yang akan diganti belum dicabut, belum kedaluwarsa atau tidak terkompromi;	VIDA may perform re-key if: a. The original certificate has not been revoked, not expired, or not compromised;

b. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi.
c. apabila diperlukan akibat adanya penggantian layanan yang disediakan oleh VIDA untuk Pemilik atau pelanggan.

b. All details relating to the Certificate are still accurate and do not require new or additional validation.
c. if necessary due to replacement of services provided by VIDA to the Subscriber or customer.

Apabila Kunci Privat Pemilik terkompromi atau sertifikat kedaluwarsa, maka Pemilik dapat mengajukan permohonan penerbitan Sertifikat baru sebagaimana diatur pada bagian 4.1.

VIDA tidak menyediakan *re-key* sertifikat terhadap sertifikat dengan masa berlaku pendek (30 menit) untuk tujuan penggunaan sekali pakai.

If Subscriber's Private Key was compromised or the certificate has expired, then the Subscriber can submit a new certificate issuance as regulated in section 4.1.

VIDA does not support certificate re-key for short-term certificates (30 minutes) for one-time use purposes.

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

Re-key certificate dapat diinisiasi atas permintaan Pemilik kepada VIDA atau diinisiasi oleh VIDA lalu disetujui oleh Pemilik.

Certificate re-key may be initiated upon a Subscriber's request to VIDA or initiated by VIDA and approved by the Subscriber.

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

VIDA melakukan identifikasi dan autentifikasi permohonan *re-key* sesuai dengan bagian 3.2, 4.5.1 dan penerbitan sesuai dengan bagian 4.3.

VIDA identifies and authenticates the certificate re-key request as per section 3.2 and 4.5.1 and issuance as per section 4.3.

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

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

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

4.7.5. Sikap yang Dianggap Sebagai Menerima Sertifikat yang Kuncinya Digantikan / 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 yang Kuncinya Digantikan oleh PSrE / Publication of the Re-Keyed Certificate by the CA

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

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

Tidak ditentukan.	No stipulation.

4.8. Modifikasi Sertifikat / Certificate Modification

Modifikasi Sertifikat tidak diperbolehkan. Apabila terjadi kesalahan selama penerbitan Sertifikat (misalnya, ejaan), Sertifikat akan dicabut dan dilanjutkan dengan proses penerbitan seperti yang dijelaskan pada bagian 4.3.	Modification of certificate is not permitted. In case there is a mistake during certificate issuance (e.g. spelling), the certificate is revoked and the issuance process is followed, as stated in section 4.3.

4.9. Pencabutan dan Pembekuan Sertifikat / Certificate Revocation and Suspension

4.9.1. Keadaan untuk Pencabutan / Circumstances for Revocation

VIDA mencabut Sertifikat Pemilik dalam keadaan berikut: a. Komponen informasi identifikasi atau afiliasi dari nama dalam Sertifikat menjadi tidak valid	VIDA shall revoke a Subscriber's certificate in the following circumstances: a. Identifying information or affiliation components of any names in the certificate becomes invalid.

b. Informasi apapun dalam Sertifikat menjadi tidak valid.
c. Pemilik dapat ditunjukkan telah melanggar ketentuan dalam Perjanjian Kepemilikan.
d. Ada alasan untuk meyakini bahwa Kunci Privat rusak/terkompromi.
e. Pemilik atau pihak berwenang lainnya yang diacu pada bagian 4.9.2 meminta Sertifikat dicabut.
f. Alasan operasional VIDA termasuk apabila ada salah satu layanan yang tutup atau VIDA berhenti beroperasi.
g. Kunci Privat dilaporkan telah hilang.
h. apabila diketahui dan terbukti bahwa Pemilik meninggal dunia.

b. Any information in the certificate becomes invalid.
c. The Subscriber can be shown to have violated the stipulations of its Subscriber Agreement.
d. There is reason to believe the Private Key has been lost or compromised.
e. The Subscriber or other authorized party as defined in section 4.9.2 asks for the certificate to be revoked.
f. Operational reason in VIDA including if VIDA terminates some of its service or when VIDA operation is terminated.
g. The Private Key is reported to have been lost.
h. if it is known and proven that the Subscriber passed away.

Sertifikat harus dicabut ketika hubungan antara subjek dan Kunci Publiknya yang didefinisikan dalam Sertifikat sudah tidak valid lagi. Ketika hal ini terjadi Sertifikat seharusnya dicabut dan diletakkan pada CRL dan/atau ditambahkan pada responder OCSP. Sertifikat yang dicabut harus disertakan dalam semua publikasi baru tentang informasi status Sertifikat sampai Sertifikat kedaluwarsa.
VIDA tidak menyediakan pencabutan sertifikat terhadap sertifikat dengan masa berlaku pendek (30 menit) untuk tujuan penggunaan sekali pakai.

A certificate shall be revoked when the binding between the subject and the subject's Public Key defined within the certificate is no longer considered valid. When this occurs, the associated certificate shall be revoked and placed on the CRL and/or added to the OCSP responder. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.
VIDA does not support certificate revocation for short-term certificates (30 minutes) for one-time use purposes.

4.9.2. Siapa yang Dapat Meminta Pencabutan / Who can Request Revocation

Sertifikat dapat diminta untuk dicabut oleh
a. Pemilik;
b. Badan usaha yang berafiliasi dengan Pemilik yang dapat membuktikan hilangnya hubungan Pemilik, atau lembaga penegak hukum yang dapat membuktikan terungkapnya Kunci Privat atau penyalahgunaan Sertifikat sesuai dengan CPS ini;
c. VIDA.

The certificate revocation can be requested by
a. the Subscriber;
b. affiliated business entity that can prove the binding between Subscriber and his affiliation ends, or law enforcement institution who can prove the Private Key exposure or the misuse of the certificate according to this CPS.
c. VIDA.

4.9.3. Prosedur Permintaan Pencabutan / Procedure for Revocation Request

VIDA memverifikasi identitas dan wewenang (untuk entitas penegak hukum) dari Pemilik yang mengajukan pencabutan Sertifikat. Validitas identitas Pemilik dibutuhkan sesuai dengan bagian 3.2.5 dan 3.4.

Permintaan pencabutan Sertifikat oleh entitas lain yang disebutkan pada bagian 4.9.2, harus menyerahkan bukti bahwa:

a. Kunci Privat Sertifikat telah terungkap;
b. penggunaan Sertifikat tidak sesuai dengan CP dan CPS, atau
c. Pemilik Sertifikat tidak memiliki hubungan dengan entitas atau hubungannya sudah berakhir.

VIDA shall verify the identity and authority (for juridical entity) of a Subscriber making the request for revocation. The validation of the Subscriber's identity is required according to section 3.2.5 and 3.4.

Request for revocation by other entity stated in the section 4.9.2, must have submission of proof that:

a. the Private Key of the certificate has been exposed;
b. the use of the certificate does not conform to the CP and CPS;
c. the Subscriber's affiliation with the entity does not exist or ends.

4.9.4. Masa Tenggang Permintaan Pencabutan / Revocation Request Grace Period

Pihak yang disebutkan dalam bagian 4.9.2 harus meminta pencabutan segera setelah mengidentifikasi perlunya pencabutan Sertifikat. Tidak ada masa tenggang untuk pencabutan dalam proses ini.

A subscriber should request revocation as soon as possible after the need for revocation has been identified. There is no specified grace period for the subscriber in this process.

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

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

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

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

Penggunaan Sertifikat yang sudah dicabut dapat menimbulkan kerugian bagi Pengandal. Oleh karena itu, Pengandal harus memvalidasi Sertifikat terhadap CRL terbaru melalui repositori maupun terhadap *server* OCSP yang disediakan oleh VIDA.

The use of revoked Certificate may cause detriment to Relying Parties. Therefore, Relying parties should validate any Certificate against the most updated CRL via repository or against VIDA's OCSP server.

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

CRL harus diperbarui dan dipublikasi:

a. untuk Sertifikat Pemilik, segera setelah adanya proses yang memicu perubahan CRL atau paling sedikit sekali setiap 1 (satu) hari. CRL akan berdampak dalam waktu maksimum 72 jam.

b. untuk Sertifikat VIDA, sedikitnya setiap 6 (enam) bulan. CRL akan berdampak dalam waktu maksimum 6 (enam) bulan.

Dalam kasus kebocoran Kunci Privat atau insiden keamanan penting lainnya, contohnya pencabutan Sertifikat VIDA, CRL terbaru harus dipublikasi dalam waktu 24 jam semenjak stempel waktu *(timestamp*) pencabutan. CRL disimpan pada lingkungan yang dilindungi untuk menjamin integritas dan keotentikannya.

The CRL must be updated and published:

a. for Subscriber certificates, immediately after a process triggers a CRL update or at least once every 1 (one) day. The CRL will be in effect for a maximum time of 72 hours.

b. for VIDA certificates, at least every 6 (six) months. The CRL will be in effect for a maximum time of 6 (six) months.

In case of secret key exposure or of any other important security compromise incident, for example a VIDA's CA Certificate revocation, an updated CRL must be published within 24 hours from the revocation timestamp. CRL is stored in a protected environment in order to ensure their integrity and authenticity.

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

Pembaruan CRL dipublikasikan otomatis ke repositori paling lambat 30 menit setelah adanya perubahan atau akan dipublikasikan secara teratur sesuai dengan jadwal.

CRLs are posted automatically to the online repository within 30 minutes after any update otherwise they will be published regularly as per schedule.

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

VIDA memberikan layanan validasi daring. Jika validasi daring tersedia, diharapkan melakukan pengecekan menggunakan Server OCSP yang disediakan.	VIDA provides an online validation service. If online validation is available, it is expected to perform revocation checks using the OCSP Server provided.

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

Layanan OCSP yang disediakan VIDA sesuai dengan standar Internet Engineering Task Force (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas.	OCSP service provided by VIDA is compliant with the Internet Engineering Task Force (IETF) RFC 6960 to meet security and interoperability requirements.

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

Tidak ditentukan.	No stipulation.

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

Tidak ditentukan.	No stipulation.

4.9.13. Keadaan untuk Pembekuan / Circumstances for Suspension

Pembekuan Sertifikat tidak disediakan.	Certificate suspension is not provided.

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

Pembekuan Sertifikat tidak disediakan.	Certificate suspension is not provided.

4.9.15. Prosedur Permintaan Pembekuan / Procedure for Suspension Request

Pembekuan Sertifikat tidak disediakan.	Certificate suspension is not provided.

4.9.16. Batas Waktu Pembekuan / Limits on Suspension Period

Pembekuan Sertifikat tidak disediakan.	Certificate suspension is not provided.

4.10. Layanan Status Sertifikat / Certificate Status Services

4.10.1. Karakteristik Operasional / Operational Characteristics

Status Sertifikat publik tersedia dari CRL di dalam repositori dan layanan OCSP yang disediakan oleh VIDA.	The status of public certificates is available from CRL in the repositories and OCSP provided by VIDA.

4.10.2. Ketersediaan Layanan / Service Availability

VIDA melakukan segala tindakan yang diperlukan untuk menjamin ketersediaan layanan validasi status Sertifikat.	VIDA shall take all necessary measures to ensure availability of certificate status validation service.

4.10.3. Fitur Opsional / Optional Features

Tidak ditentukan.	No stipulation.

4.11. Akhir Berlangganan / End of Subscription

Pemilik dapat mengakhiri langganan dengan membiarkan Sertifikatnya kedaluwarsa atau mencabut Sertifikatnya tanpa meminta Sertifikat yang baru.	Subscriber may end a subscription by allowing its certificate to expire or revoking its certificate without requesting a new certificate.

4.12. Pemulihan dan Penitipan Kunci / Key Escrow and Recovery

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

VIDA tidak meng-eskro Kunci Privat VIDA maupun Kunci Privat Pemilik yang terasosiasi dengan Sertifikat yang berisi *key usage digitalSignature* ke pihak lain. VIDA	VIDA does not escrow CA Private Key nor Subscriber's Private Key associated to Certificate with key usage digitalSignature to

tidak menyediakan layanan eskro untuk Pemilik.

Kunci Privat Pemilik dapat disimpan dan dikelola di lingkungan VIDA sesuai dengan perjanjian kepemilikan dan dilakukan untuk tujuan penggunaan Sertifikat seperti yang dijelaskan di bagian 4.5.1.

other party. VIDA does not provide escrow service for Subscriber.

Subscriber's Private Key can be stored and managed in VIDA's environment as per subscriber agreement and conducted for the purpose of certificate usage as per specified in section 4.5.1.

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

Tidak ditentukan.

No stipulation.

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

5.1. Kendali Fisik / Physical Controls

5.1.1. Lokasi dan Konstruksi / Site Location and Construction

Guna menjamin keberlangsungan operasional PSrE, lokasi dan konstruksi bangunan dimana fasilitas, peralatan, dan infrastruktur PSrE ditempatkan, telah memiliki spesifikasi khusus mekanisme perlindungan yang kuat dan memberikan jaminan fasilitas pengelolaan informasi yang bernilai tinggi.

VIDA memiliki pusat data utama (DC) dan pusat data pendukung sebagai pusat pemulihan bencana (DRC) yang terletak di Indonesia. Jarak antara DRC dengan DC utama dinilai cukup berdasarkan penilaian risiko dan pertimbangan ketersediaan layanan sehingga apabila terjadi peristiwa kahar pada lokasi DC utama maka DRC tidak ikut terkena dampaknya.

In order to ensure the continuity of CA operations, the location and construction of the building where the facilities, equipment and infrastructure of the PSrE are placed, have special specifications and strong protection mechanisms and guarantee high-value information management facilities.

VIDA has a main data center (DC) and a secondary data center meant for Disaster recovery center (DRC) which are located in Indonesia. The distance between DRC and the main DC is sufficient based on risk assessment and service availability consideration so that when a force majeure happens in the main DC location so the DRC remains unaffected.

5.1.2. Akses Fisik / Physical Access

VIDA selalu terlindungi dari akses yang tidak resmi. Mekanisme keamanan fisik untuk VIDA telah diimplementasikan untuk:

a. Memastikan tidak ada akses ke perangkat keras tanpa izin;
b. Menyimpan semua media dan kertas yang berisi informasi teks polos yang sensitif dalam wadah yang aman;
c. Memonitor, baik secara manual maupun elektronik, dari intrusi tanpa hak setiap saat;
d. Memelihara dan secara berkala memeriksa log akses;
e. Membutuhkan kendali akses fisik dua orang untuk mengakses rak

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

a. Ensure no unauthorized access to the hardware is permitted;
b. Store all removable media and paper containing sensitive plain-text information in secure containers;
c. Monitor, either manually or electronically, for unauthorized intrusion at all times;
d. Maintain and periodically inspect an access log.
e. Require physical access control of two people to access the storage rack of cryptographic module and CA server.

penyimpanan modul kriptografi dan perangkat *server CA*;

f. Brankas dikunci;
g. Sistem keamanan fisik (misalnya kunci pintu, *alarm, CCTV*) berfungsi dengan baik;
h. Akses ke area peralatan sensitif operasional CA mengikuti kendali akses fisik dua orang atau terdapat mekanisme autentikasi multi faktor sehingga senantiasa terjaga dari akses tanpa izin.

f. The safebox is locked;
g. Physical security systems (e.g. door locks, alarms, CCTV) are functioning properly;
h. Access to the CA operational equipment sensitive area follows two-person physical access control or there is a multi-factor authentication mechanism applied so that it is always protected from unauthorized access.

Facility engineer bertanggung jawab untuk memastikan mekanisme keamanan fisik di atas dijalankan dengan baik dan melakukan pemeriksaan keamanan fasilitas penyimpanan perangkat. Proses pemeriksaan keamanan fasilitas penyimpanan perangkat harus dilaksanakan jika fasilitas akan ditinggalkan tanpa adanya pengawasan. Proses tersebut meliputi:

i. perangkat yang tidak digunakan boleh dimatikan;
ii. *security container* (misal: brankas) sudah dikunci;
iii. sistem keamanan fisik misalnya kunci pintu berfungsi dengan baik; dan
iv. area diamankan dari akses yang tidak berhak.

The facility engineer is responsible for ensuring that the above physical security mechanisms are implemented properly and conducting security checks of device storage facilities. Security check of the storage facility that storing CA equipment shall be done if the facility is to be left unattended. At a minimum, the check shall verify the following:

i. equipment that is not used may be shut down;
ii. security containers (e.g safebox) are locked;
iii. physical security systems (e.g., door locks) are functioning properly; and
iv. the area is secured against unauthorized access.

5.1.2.1. Pusat Data / Data Center

Semua kegiatan operasional PSrE yang sangat penting dan memiliki risiko tinggi harus ditempatkan pada fasilitas yang aman dengan memiliki setidaknya empat (4) lapis pengamanan untuk bisa mengakses perangkat keras dan perangkat lunak yang sensitif.

All critical CA operations and having high risk should take place within a physically secure facility with at least four (4) layers of security to access sensitive hardware or software.

Fasilitas dan peralatan operasional PSrE milik VIDA berlokasi di Pusat Data Tier-3 di Indonesia dan tersertifikasi ISO 27001. Hanya personil yang memiliki otoritas yang bisa mengakses fasilitas tersebut.

Facilities and equipment of CA operation owned by VIDA is located in a Tier 3 data center in Indonesia with ISO 27001 certification. Only authorized personnel who have authority can access the facility.

5.1.2.2. RA Operational Room/ Ruang Operasional RA

Operasi RA dilaksanakan pada area tersendiri yang dilindungi dengan kontrol akses fisik sehingga hanya dapat diakses oleh individu yang memiliki otorisasi.

RA operations are performed in dedicated areas which are protected using physical access controls making them accessible only to appropriately authorized individuals.

5.1.3. Power and Air Conditioning / Daya dan Penyejuk Udara

VIDA memiliki daya cadangan yang cukup untuk me-lockout secara otomatis, menyelesaikan beberapa hal/tindakan yang tertunda, dan mencatat keadaan peralatan sebelum kekurangan daya atau AC yang menyebabkan peralatan mati. Repositori IKP telah dilengkapi dengan *Uninterrupted Power Supply* dan Generator Listrik yang cukup untuk pengoperasian minimal 6 (enam) jam tanpa adanya listrik/daya dari PLN, untuk mendukung kelangsungan operasi.

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

5.1.4. Water Exposures / Pemaparan Air

VIDA dilindungi terhadap air dengan cara meletakkannya di atas tanah atau menggunakan raised floor. Sistem pencegahan kebakaran seperti sprinkler termasuk ke dalam pengecualian.

VIDA equipment is protected against water by having it located above ground or using raised flooring. Fire prevention systems such as sprinklers are considered as exceptions.

5.1.5. Pencegahan dan Perlindungan dari Kebakaran / Fire Prevention and Protection

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

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

5.1.6. Penyimpanan Media / Media Storage

Media penyimpanan yang digunakan oleh VIDA dikelola secara aman sehingga terlindungi dari kerusakan akibat kerusakan (akibat paparan air, api, atau gangguan elektromagnetik), pencurian, dan akses yang tidak sah. Media yang berisi informasi audit, arsip, atau backup diduplikasi dan disimpan dengan aman di DRC maupun di lokasi *offsite*.

Modul kriptografi yang bersifat *removable* dinonaktifkan sebelum disimpan. Ketika tidak digunakan, modul kriptografi yang *removable*, informasi aktivasi yang digunakan untuk mengakses atau mengaktifkan modul kriptografi tersebut harus ditempatkan pada tempat penyimpanan yang aman.

Storage media used by VIDA are managed with secure manner so that they are protected from damage (exposure to water, fire or electromagnetic interference), theft and unauthorized access. Media containing audit, archival, or backup information is duplicated and stored securely in DRC or in an offsite location.

Removable cryptographic modules are deactivated before being stored. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers.

5.1.7. Pembuangan Limbah / Waste Disposal

Seluruh dokumen, media penyimpanan, dan perangkat kriptografis milik VIDA yang mengandung informasi sensitif dan sudah tidak digunakan akan dihancurkan dan dibuang sesuai dengan prosedur yang ditetapkan oleh VIDA agar informasi didalamnya tidak dapat direkonstruksi kembali.

All documents, storage media, and cryptographic devices owned by VIDA which contain sensitive information and are no longer used will be destroyed and disposed in accordance with procedures defined by VIDA so that the information contained therein cannot be reconstructed.

5.1.8. Backup Off-Site / Off-Site Backup

VIDA memiliki setidaknya 1 (satu) set *backup* lengkap yang disimpan pada DRC. VIDA juga memiliki 1 (satu) salinan *backup* yang disimpan pada lokasi *off-site* yang terpisah dari lokasi DC maupun DRC yang diperbarui secara berkala sesuai dengan penilaian risiko agar dapat digunakan untuk pemulihan sistem. Salinan backup tersebut disimpan di dalam brankas. Pengamanan fisik dan prosedur yang diterapkan pada DRC dan *off-site* setara dengan pengamanan pada lokasi DC utama.

VIDA maintains at least 1 (one) full set of backups stored in a DRC. VIDA also has 1 (one) backup copy stored in an off-site location separate from the DC or DRC locations which is updated regularly according to risk assessment so that it can be used for system recovery. Backup copies are kept in a safe. The physical safeguards and procedures implemented at the DRC and off-site are equivalent to those at a primary DC location.

5.2. Kendali Prosedur / Procedural Controls

5.2.1. Peran Terpercaya / Trusted Roles

Peran Terpercaya meliputi tapi tidak terbatas pada:	Trusted Role includes, but not limited to:
a. CA Team Leader Bertanggung jawab secara keseluruhan dalam mengelola praktik keamanan PSrE	a. CA Team Leader Overall responsibility for managing all CA security practices
b. Key Manager Bertanggung jawab untuk menjaga token CA dan perangkat HSM	b. Key Manager Accountable for keeping the CA and HSM tokens
c. Administrator CA Melakukan operasional dan maintenance aplikasi manajemen PSrE	c. CA Administrator Conduct operasional and maintenance of CA management application
d. Administrator RA Identifikasi dan Validasi identitas permohonan Sertifikat	d. RA Administrator Identification and validation of certificate application
e. Administrator VA Bertanggung jawab dalam proses validasi Sertifikat dan ketersediaan layanan tersebut	e. VA Administrator Responsible for certificate validation process and ensure the services are available
f. Manajer Repositori Bertanggung jawab terhadap konten yang dipublikasikan pada repositori	f. Repository Manager Responsible for all contents that published in repository
g. Pengembang Piranti Lunak Bertanggung jawab dalam mengembangkan aplikasi dan melakukan integrasi terkait dengan sistem PSrE	g. Software Developer responsible for developing applications and performing integrations related to the CA organization systems
h. Facility Engineer Bertanggung jawab terhadap kelancaran perangkat CA termasuk mengelola perangkat *server*, jaringan, dan sistem operasi	h. Facility Engineer Responsible for the smooth running of CA equipments including managing server, network, and operating system
i. Policy Authority Bertanggung jawab untuk pembuatan, revisi dan persetujuan CPS	i. Policy Authority Responsible for creation, revision and approval of CPS

j. Security Officer

Bertanggung jawab terhadap keamanan fisik maupun logis dari sistem PSrE

k. Internal Auditor

Melakukan audit internal terhadap pelaksanaan operasional PSrE

Peran Terpercaya di atas dapat dibantu oleh peran lain yang penjelasan terhadap keterlibatan pada operasional VIDA dapat dilihat di dokumen internal lainnya.

j. Security Officer

Accountable for the Physical and Logical security of the CA organization and systems

k. Internal Auditor

Conduct internal audit of CA operational

Trusted roles above can be assisted by other roles for which an explanation of involvement in VIDA operations can be seen in other internal documents.

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

Untuk kegiatan yang memerlukan kendali multi-pihak, semua partisipan harus memegang peran terpercaya. Kendali multi-pihak tidak dapat dicapai dengan melibatkan personil yang bertugas dalam peran Auditor Keamanan. Tugas berikut memerlukan partisipasi tiga (3) orang atau lebih sesuai dengan peran dan tanggung jawab yang sudah ditentukan:

a. Pembangkitan kunci VIDA,
b. Penandatanganan kunci VIDA,
c. Pencabutan Sertifikat VIDA, atau
d. Pencadangan Kunci VIDA.

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks shall require three (3) or more persons according to the defined role and responsibilities:

a. VIDA's CA key generation,
b. VIDA's CA key signing,
c. VIDA's CA certificate revocation, or
d. VIDA's CA key backup.

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

Semua individu yang ditugaskan dalam Peran Terpercaya akan menerima Surat Penugasan. Individu dapat diautentikasi menggunakan kata sandi untuk menjalankan tugas pada sistem milik VIDA.

All individuals assigned to a Trusted Role will receive an Assignment Letter. Individuals authenticate themselves using passwords to perform the tasks in the VIDA's system.

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

Role yang tidak boleh diperankan bersamaan adalah:

a. Policy Authority dan administrator operasional;
b. Internal audit dan semua peran lain;
c. Pengembang sistem dan semua peran lain.

Same person was not assigned to another role for:

a. Policy authority and operational administrator;
b. Internal audit and any other role;
c. System developer and any other role.

5.3. Kendali Personil / Personnel Controls

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

Semua personil di VIDA dipilih atas dasar keahlian, pengalaman, kualifikasi, memiliki loyalitas, bersifat dapat dipercaya, dan memiliki integritas. Personil yang ditunjuk untuk peran terpercaya harus secara resmi diangkat oleh manajemen senior, sesuai dengan persyaratan sebagai berikut:

a. memiliki bukti latar belakang yang diperlukan sesuai bagian 5.3.2 serta kualifikasi dan pengalaman yang diyakini memadai untuk melaksanakan tanggung jawab pekerjaan secara efektif dan efisien; dan
b. memiliki bukti catatan kriminal yang bersih.

All VIDA personnel shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. Personnel appointed to trusted roles shall be formally appointed by senior management, pursuant to the following criteria:

a. has proof of the requisite background as per 5.3.2 as well as has qualifications and experience that are necessary to perform their job responsibilities effectively and efficiently; and
b. has proof of criminal record clearances.

5.3.2. Prosedur Pemeriksaan Latar Belakang / Background Check Procedures

Semua personil Peran Terpercaya harus lulus pemeriksaan latar belakang sesuai prosedur yang ditetapkan oleh VIDA. Lingkup pemeriksaan latar belakang mencakup pemeriksaan berkas terhadap area berikut, yang paling sedikit 5 (lima) tahun:

a. Pendidikan atau sertifikasi,
b. Identifikasi Kependudukan (KTP bagi WNI),

All VIDA Trusted Role personnel shall have completed a background check as per procedure specified by VIDA. The scope of the background check shall include the document check of following areas covering at least the past 5 (five) years:

a. Education or certification
b. Residential Identification (KTP for Indonesia citizen)

c. tidak memiliki catatan kriminal (SKCK atau yang ekuivalen),
d. Kontak Referensi Pekerjaan
e. tidak mengalami kebankrutan atau masalah finansial yang dapat berdampak pada kualitas kinerja.

c. not having criminal record (Police Certificate of Good Conduct/Police Clearance or equivalent)
d. Employment Contact Reference
e. not bankrupt or not having financial problems which may negatively impact on performance.

5.3.3. Persyaratan Training / Training Requirements

Semua personil VIDA harus dilatih dengan tepat untuk menjalankan tugasnya. Pelatihan ini akan membahas topik yang relevan, seperti persyaratan keamanan, tanggung jawab operasional (termasuk pengelolaan perangkat keras, perangkat lunak dan sistem operasi PSrE), serta prosedur, CP, dan CPS yang berlaku. Evaluasi terhadap kecukupan kompetensi personil PSrE harus dilakukan minimal 1 (satu) kali dalam setahun.

All VIDA personnel shall be appropriately trained to perform their duties. Such training will address relevant topics, such as security requirements, operational responsibilities (including management of CA hardware, software and operating system), and applicable procedure, CP, and CPS. The adequacy of the competence of CA personnel shall be conducted at least 1 (one) time a year.

5.3.4. Frekuensi dan Persyaratan Training Ulang / Retraining Frequency and Requirements

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

VIDA shall provide refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

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

VIDA memastikan bahwa perubahan staf tidak akan mempengaruhi efektivitas operasional layanan atau keamanan sistem dengan meninjau kontrol akses apabila personel mengundurkan diri dari organisasi serta menyiapkan personil pengganti.

VIDA should ensure that any change in the staff will not affect the operational effectiveness of the service or the security of the system by reviewing access controls when personnel leave the organization as well as preparing replacement personnel.

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

Sanksi disiplin yang sesuai dikenakan pada personel yang melanggar ketentuan dan kebijakan dalam CPS ini, CP, atau prosedur operasional VIDA yang terkait sesuai dengan prosedur pendisiplinan.

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within this CPS, CP, or VIDA related operational procedures as per disciplinary procedure.

5.3.7. Persyaratan Kontraktor Independen / Independent Contractor Requirements

Personel sub-kontraktor yang dipekerjakan untuk melakukan fungsi yang berkaitan dengan operasional VIDA harus memenuhi persyaratan yang berlaku yang ditetapkan pada bagian 5.3, serta prosedur tambahan dan kontrak lain yang telah disepakati.

Sub-Contractor personnel employed to perform functions pertaining to VIDA operations shall meet applicable requirements set forth in this CPS section 5.3, and other procedures and agreed contract.

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

VIDA menyediakan kepada para personilnya berupa CP, CPS, dan setiap undang-undang yang relevan, kebijakan, dan kontrak. Dokumen teknis, operasional, dan administratif lainnya (misalnya, Panduan Administrator, Panduan Pengguna, dll) harus disediakan agar para personil dapat menjalankan tugasnya.

VIDA has made available to its personnel the CP, CPS, and any relevant laws, policies, and contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) shall be provided in order for the personnel to perform their duties.

5.4. Prosedur Log Audit / Audit Logging Procedures

Berkas log audit harus dibuat untuk semua kejadian yang terkait dengan keamanan sistem PSrE dan RA milik VIDA. Bila memungkinkan, log audit keamanan harus dikumpulkan secara otomatis. Bila tidak memungkinkan, buku log, kertas formulir, atau mekanisme fisik lain harus dipakai. Semua log audit keamanan, elektronik dan non elektronik, harus dipertahankan dan

Audit log files shall be generated for all events relating to the security of the VIDA's CAand RA systems. 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

tersedia selama audit kepatuhan. Log audit keamanan untuk setiap kejadian yang dapat diaudit yang didefinisikan pada bagian ini dipelihara sesuai dengan bagian 5.5.2.

security audit logs for each auditable event defined in this section shall be maintained in accordance with section 5.5.2.

5.4.1. Jenis Kejadian yang Direkam / Types of Events Recorded

VIDA mengaktifkan semua kapabilitas audit keamanan yang tersedia pada sistem operasi serta aplikasi PSrE, RA, dan VA dimana waktu yang diacu disinkronkan dengan otoritas sumber waktu (*NTP*) dengan ketelitian 1 (satu) menit. VIDA memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat disimpan sedemikian rupa sehingga dapat memastikan keterlacakan setiap tindakan Trusted Role dalam operasional layanan PSrE.

Jenis kejadian yang direkam termasuk namun tidak terbatas pada:

i. Aktivitas Pengguna sistem CA, RA dan VA;
ii. Identitas Pemilik Sertifikat;
iii. kejadian yang berkaitan dengan siklus hidup Sertifikat seperti tanggal Sertifikat diterbitkan dan dicabut;

All available security auditing capabilities of the CA, RA, and VA operating system and applications shall be enabled where the referenced time is synchronized with the time source authority (NTP) with an accuracy of 1 (one) minute. VIDA 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 CA service operations.

The types of events recorded include but are not limited to:

i. User activities for CA, RA and VA systems;
ii. Subscriber Identity;
iii. events related with Certificate lifecycle such as issued and revoked date;

Setiap pencatatan log apabila memungkinkan dan tersedia dapat memuat poin-poin sebagai berikut (baik direkam secara otomatis atau secara manual):

a. jenis kejadian,
b. nomor seri atau urutan pencatatan,
c. tanggal dan waktu kejadian,
d. sumber pencatatan,
e. deskripsi seperti status atau indikator hasil kejadian misalnya sukses atau gagal,
f. identitas dari operator yang menjalankan kejadian.

Each audit log if possible may include the following record (either recorded automatically or manually:

a. type of event,
b. serial number of sequence of entry,
c. date time entry,
d. source of entry,
e. descriptions such as status or indicator of the event result such as success or failure,
f. the identity of the operator which triggers the event.

5.4.2. Frekuensi Pemrosesan Log / Frequency of Processing Log

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

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

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

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

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

5.4.4. Proteksi Log Audit / Protection of Audit Log

Log Audit dilindungi untuk mencegah perubahan dan mendeteksi gangguan serta untuk memastikan bahwa hanya individu dengan akses terpercaya yang berwenang yang mampu melakukan operasi apa pun tanpa memodifikasi integritasnya. Sistem dapat menimpa (*overwrite*) log audit setelah log audit tersebut di-backup atau diarsipkan.

The records of events are protected to prevent alteration and detect tampering and to ensure that only individuals with authorized trusted access are able to perform any operations without modifying integrity. The system can overwrite audit logs after they have been backed up or archived.

5.4.5. Prosedur Backup Log Audit / Audit Log Backup Procedures

Log audit dikumpulkan secara otomatis dan dicadangkanan setiap bulan dan diisimpan di lokasi yang aman.

Log audit is gathered automatically and backed up on a monthly basis and stored into the secure location.

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

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

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

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

Tidak ditentukan.

No stipulation.

5.4.8. Asesmen Kerentanan / Vulnerability Assessments

VIDA melakukan penilaian kerentanan sistem PSrE beserta komponen infrastruktur secara berkala. Uji penetrasi dilakukan paling tidak 1 (satu) tahun sekali atau ketika terjadi perubahan signifikan pada sistem PSrE. Hasil asesmen kerentanan akan digunakan untuk menjaga dan meningkatkan keamanan sistem dari VIDA.

VIDA shall carry out regular vulnerability assessments of CA systems and infrastructure components. Penetration tests are carried out at least once a year or when significant changes occur in the CA system. The results of the vulnerability assessment will be used to maintain and improve system security.

5.5. Pengarsipan Record / Records Archival

5.5.1. Tipe Record yang Diarsipkan/ Types of Records Archived /

VIDA mengimplementasikan metode pencadangan untuk operasional VIDA 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 VIDA;
c. Data konfigurasi sistem PSrE;
d. Dokumen CP dan CPS yang berlaku, termasuk juga segala modifikasi dan

VIDA implements a backup method for VIDA 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 request, re-key request, and revocation request;
b. All certificates and CRLs as issued or published by the VIDA;
c. CA system configuration data;
d. Applicable CP and CPS document including modifications and amendments to these documents;

amandemen terhadap dokumen-dokumen tersebut;

e. Data audit;
f. Catatan yang mendukung sistem manajemen keamanan informasi (SMKI) seperti penugasan dan penarikan peran dan hak istimewa, akses pengunjung ke fasilitas, perubahan dan pemeliharaan perangkat keras atau perangkat lunak sistem; deteksi dan pemrosesan insiden keamanan, latihan darurat, penilaian dan penanganan risiko, perubahan aset, prosedur atau tanggung jawab, dan perubahan dokumentasi publik.

e. Audit data;
f. Records supporting the information security management system (ISMS) such as assignment and withdrawal of roles and privileges, visitor access to facilities, changes and maintenance of system hardware or software; detection and processing of security incidents, emergency drills, risk assessment and treatment, changes of assets, procedures or responsibilities and changes of public documentation.

5.5.2. Periode Retensi Arsip / Retention Period for Archive

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

Archived records shall be retained for at least 5 (lima) years. Softwares and hardwares necessary to read these archives shall be maintained for the retention period.

5.5.3. Protection of Archive / Perlindungan Arsip

Catatan yang diarsipkan dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah. Media yang menyimpan catatan yang diarsipkan dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan harus dipelihara dan dilindungi.
Arsip tidak boleh diungkapkan kecuali untuk kepentingan audit, investigasi oleh lembaga penegak hukum, atau permintaan dari Pemilik yang bersangkutan serta sesuai dengan bagian 9.3 dan 9.4.

The archived records are protected against unauthorized viewing, modification, deletion, or tampering. The media holding the archived records and the applications required to process the archived records shall be maintained and protected.
Archives are not disclosed except for audits, investigations by law enforcement agencies, or requests from the relevant Subscribers and in accordance with section 9.3 and 9.4.

5.5.4. Prosedur Backup Arsip / Archive Backup Procedures

Prosedur backup arsip yang memadai dan teratur dilakukan agar jika terjadi kehilangan atau kerusakan arsip utama, tersedia satu set lengkap salinan *backup* di lokasi terpisah.	Adequate and regular backup procedures are in place so that in the event of loss or destruction of the primary archives, a complete set of backup copies held in a separate location will be available.

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

Rekaman arsip VIDA diberi label waktu saat dibuat.	VIDA archive records are time-stamped as they are created.

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

Pengumpulan arsip di VIDA dilakukan oleh internal PSrE.	Archive Collection Process is conducted by VIDA internally.

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

Media penyimpanan arsip informasi di VIDA diperiksa pada saat dibuat. Dalam waktu berkala, sampel informasi yang diarsip akan diperiksa untuk memastikan informasi tetap terintegrasi dan dapat dibaca. Hanya personil yang terotorisasi yang dapat mengakses arsip. Permintaan untuk mendapatkan dan memverifikasi informasi di arsip dikoordinasi oleh personil peran terpercaya.	Media storing of VIDA archive information is checked upon creation. Periodically, samples of archived information are tested to check the continued integrity and readability of the information. Only authorised personnel are allowed to access the archive. Requests to obtain and verify archive information are coordinated by trusted roles personnel.

5.6. Pergantian Kunci / Key Changeover

Untuk meminimalkan risiko dari kondisi Kunci Privat VIDA terkompromi, Kunci Privat dapat diubah. Sejak Kunci Privat diubah, hanya kunci baru yang bisa digunakan untuk penandatanganan Sertifikat. Sertifikat yang	To minimize risk from compromise of a VIDA's private signing key, that key may be changed; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to

lama, namun masih berlaku, akan tersedia untuk memverifikasi tanda tangan lama sampai seluruh Sertifikat yang ditandatangani menggunakan Kunci Privat terkait kedaluwarsa. Jika Kunci Privat lama digunakan untuk menandatangani CRL, maka kunci lama harus disimpan dan dilindungi.

verify old signatures until all of the certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs, then the old key shall be retained and protected.

Apabila VIDA memperbarui Kunci Privat dan dengan demikian menghasilkan Kunci Publik baru, VIDA harus memberitahu semua Pemilik dan Pengandal bahwa telah terjadi perubahan. Baik pasangan kunci lama maupun baru akan aktif secara bersamaan untuk mendukung Sertifikat Pemilik yang belum kedaluwarsa hingga periode berlakunya berakhir.

When VIDA updates its private signature key and thus generates a new Public Key, the VIDA will notify all Subscribers and Relying Parties that it has been changed. Both the old and the new Key Pairs are concurrently active to support Subscriber certificates that have not expired until their validity ends.

VIDA tidak menerbitkan Sertifikat Pemilik yang masa berlakunya melebihi masa berlaku Sertifikat VIDA. Ketentuan untuk masa berlaku Kunci Privat VIDA dapat dilihat pada bagian 6.3.2.

VIDA does not issue Subscriber Certificate whose validity exceeds VIDA's Certificate validity. Provision about VIDA Private Key can be checked in section 6.3.2.

5.7. Pemulihan Bencana dan Keadaan Terkompromi / Compromise and Disaster Recovery

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

VIDA memiliki rencana tanggap darurat dan rencana pemulihan bencana ditinjau setiap tahun dan diperbarui sesuai kebutuhan.

VIDA shall have an incident response plan and a disaster recovery plan which is reviewed annually and updated as needed

Jika VIDA dicurigai telah terkompromi, penerbitan Sertifikat oleh VIDA harus dihentikan seketika. Investigasi independen oleh pihak ketiga harus dilakukan untuk menentukan sifat dan tingkat kerusakan. Ruang lingkup potensi kerusakan harus dinilai untuk menentukan prosedur perbaikan yang tepat. Jika Kunci Privat VIDA dicurigai sudah terkompromi, prosedur pada Bagian 5.7.3 harus diikuti.

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

VIDA menginformasikan kepada PSrE Induk apabila mengalami insiden terkait keamanan

VIDA informs the Root CA Indonesia if it experiences an incident related to information security, including but not limited to:

informasi, termasuk namun tidak terbatas pada:

1. Terdeteksinya atau adanya indikasi sistem VIDAa terkompromi;
2. Adanya upaya untuk menembus sistem VIDA, baik secara fisik maupun elektronik;
3. Serangan Denial of Service pada sistem VIDA;
4. Setiap insiden yang mencegah atau menghambat penerbitan CRL dalam kurun waktu 24 (dua puluh empat) jam dari waktu yang telah ditentukan dalam field “next update” pada CRLnya yang valid saat ini. PSrE Indonesia harus segera memulihkan penerbitan CRL secepat mungkin; dan/atau
5. CRL dan/atau OCSP responder tidak dapat diakses oleh publik.

Semua sistem pencadangan dan/atau pemulihan diuji minimal setahun sekali.

1. Detected or indicated that VIDA system is compromised;
2. There are efforts to penetrate the VIDA system, both physically and electronically;
3. Denial of Service attacks on VIDA system;
4. Any incident that prevents or hinders the issuance of the CRL within 24 (twenty four) hours from the time specified in the "next update" field of the current valid CRL. VIDA must immediately restore the issuance of the CRL as soon as possible; and/or
5. CRL and/or OCSP responders are not publicly accessible.

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

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

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

a. Memberitahu PA PSrE Induk sesegera mungkin;
b. Memastikan integritas sistem telah direstorasi sebelum kembali beroperasi dan menentukan seberapa banyak kehilangan data terjadi sejak posisi terakhir backup;
c. Mengoperasikan kembali sistem PSrE milik VIDA, memprioritaskan fungsi validasi informasi status Sertifikat sesuai jadwal penerbitan CRL maupun OCSP;
d. Bila kunci penandatanganan VIDA rusak, pengoperasiaan kembali VIDA dilakukan secepat mungkin dengan memberikan prioritas ke pembangkitan pasangan kunci penandatanganan VIDA yang baru.

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

a. Notify the Policy Authority of Root CA Indonesia 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 VIDA’s CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule and also OCSP;
d. If VIDA signing keys are destroyed, reestablish VIDA operations as quickly as possible, giving priority to the generation of a new VIDA signing key pair.

VIDA dapat berkoordinasi dengan PSrE Induk dalam menentukan apakah perlu untuk meminta pencabutan Sertifikat VIDA kepada PSrE Induk, misalnya apabila VIDA tidak berhasil memulihkan fungsi validasi Sertifikat dalam jangka waktu yang wajar atau apabila fasilitas dan peralatan PSrE berikut semua salinan kunci penandatangan milik VIDA rusak atau hancur secara fisik akibat bencana.

VIDA may coordinate with the Root CA in determining whether it is necessary to request the revocation of the VIDA Certificate from the Root CA Indonesia, for example if VIDA fails to restore the Certificate validation function within a reasonable time or if facilities and equipment along with all copies of signing keys belonging to VIDA are physically damaged or destroyed after a disaster.

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

Dalam kasus PSrE Induk kehilangan Kunci Privat, PA ataupun CA Team Leader akan mendapatkan pemberitahuan dan bekerja sama dengan perwakilan dari PSrE Induk untuk melaksanakan tindakan yang dapat menyelesaikan isu tersebut.

If the Private Key of the Root CA is lost, Root CA shall notify the PA or CA Team leader will be notified and work closely with Root CA representative to take appropriate actions to resolve the issue.

Dalam kasus VIDA kehilangan Kunci Privat atau terkompromi, semua Pemilik dan Pengandal yang terkait mendapat pemberitahuan, semua Sertifikat Pemilik yang diterbitkan oleh VIDA yang terkompromi tersebut dicabut bersamaan dengan Sertifikat milik VIDA. VIDA membangkitkan pasangan kunci baru dan meminta penerbitan Sertifikat baru ke Menteri sesuai dengan proses registrasi awal sebagaimana disebutkan dalam CP PSrE Induk lalu kemudian pasangan kunci beserta Sertifikat baru bagi Pemilik dapat diterbitkan segera setelah kondisi kondusif.

In case VIDA's Private Key is compromised or lost, all related Subscribers and Relying Parties are notified, all related Subscriber certificates issued by the compromised VIDA’s Certificate are revoked along with VIDA’s Certificate. VIDA generates a new key pair and requests the issuance of a new Certificate to the Minister in accordance with the initial registration process as stated in the Root CA Indonesia and then new keypairs and Certificates for subscribers can be issued as soon as the condition is getting conducive.

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

Untuk memelihara ketersediaan dan keandalan layanan VIDA, *backup* data dan prosedur pemulihan tersedia. VIDA memiliki sebuah Rencana Keberlangsungan Bisnis (*Business Continuity Plan*/BCP) yang

To maintain the availability and reliability of the VIDA services, data backup and recovery procedures are made available. VIDA has a Business Continuity Plan (BCP) which includes Disaster Recovery Plan (DRP). The BCP is

mencakup Rencana Pemulihan Bencana (*Disaster Recovery Pla*n/DRP) di dalamnya. BCP ditinjau dan diuji minimal setahun sekali dan diperbaharui jika dibutuhkan.

reviewed and tested at least once a year and is updated as needed.

VIDA memelihara *backup* data baik secara *online* maupun *offline*. Fasilitas cadangan VIDA tersedia bila fasilitas utama berhenti beroperasi.

VIDA maintains the data backup both online and offline. The secondary node VIDA is readily available in the event that the primary node should cease operation.

5.8. Penutupan CA atau RA / CA or RA Termination

Bila ada keadaan yang menyebabkan diakhirinya layanan VIDA dengan persetujuan dari Kementerian Komunikasi dan Informatika, VIDA memberitahu RA, pemilik, Pengandal dan Partisipan lain yang terkait. Rencana aksi adalah sebagai berikut:

a. memastikan agar segala gangguan yang diakibatkan oleh penutupan VIDA sebagai PSrE dapat diminimalisasi;
b. menjaga rekaman arsip PSrE milik VIDA tetap dipertahankan hingga ketentuan pengalihan dijalankan;
c. Memberitahu status layanan ke Pemilik dan Pengandal yang terkena dampak dan menentukan periode pemberitahuan yang dibutuhkan;
d. Mencabut semua Sertifikat selama periode pemberitahuan ;
e. Menyimpan informasi VIDA dan para Pemilik selama periode pemberitahuan untuk tujuan pengalihan tanggung jawab mengikuti ketentuan yang akan diberlakukan;
f. Menyediakan dukungan berkelanjutan dan menjawab pertanyaan;
g. Menangani dengan tepat pasangan kunci VIDA dan perangkat keras yang terkait untuk dapat dialihkan kepada pihak yang ditunjuk.

If there is any circumstance to terminate the services of VIDA with the approval of the Ministry of Communications and Informatics, VIDA will notify the RAs, the Subscribers, Relying Parties, and other relevant Participants. The action plan is as follow:

a. ensure that any disruption resulting from VIDA as a CA terminated is minimized;
b. VIDA's CA archivals are retained until the transfer provisions are implemented;
c. Notify the status of the service to affected Subscribers and relying parties and define the notice period needed;
d. Revoke all certificates during the notice period;
e. store information of VIDA and Subscribers within the notice period for the take-over purpose according to the provision herein specified;
f. Provide ongoing support and answer questions;
g. Properly handle VIDA key pair and associated hardwares to be taken over by the appointed entity.

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

6.1.1.1. Pembangkitan Pasangan Kunci CA / CA Key Pair Generation

Material kunci kriptografi yang digunakan oleh VIDA untuk menandatangani Sertifikat, CRL atau informasi status dibuat di dalam modul kriptografi yang sesuai standar FIPS 140-2 level 3. Kendali multi-pihak dibutuhkan untuk pembangkitan pasangan kunci VIDA, seperti yang ditentukan pada bagian 6.2.2.

Cryptographic keying material used by VIDA to sign certificates, CRLs or status information shall be generated in cryptographic modules validated to FIPS 140-2 level 3. Multi-party control is required for VIDA key pair generation, as specified in section 6.2.2.

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

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

Entitas / Entity	FIPS 140-2 Level	Perangkat Keras atau Perangkat Lunak (Modul Kriptografi) / Hardware or Software	Dibangkitkan di dalam Modul Kriptografi / Generated in Cryptographic Module
PSrEVIDA / VIDA CA	3	Perangkat Keras / Hardware	Ya / Yes
Time Stamp Authority	3	Perangkat Keras / Hardware	Ya / Yes
OCSP Responder	3	Perangkat Keras / Hardware	Ya / Yes

6.1.1.2. Pembangkitan Pasangan Kunci Pemilik / Subscriber Key Pair Generation

Pasangan kunci Pemilik dibangkitkan pada modul kriptografi menggunakan fasilitas yang disediakan oleh VIDA yaitu sebagai berikut:

a. secure usb token, yang memenuhi persyaratan FIPS 140-2 level 3;

b. perangkat keras modul kriptografi, yang memenuhi persyaratan FIPS 140-2 level 3. Kunci Privat Pemilik kemudian disimpan pada VIDA *Vault* sesuai bagian 6.2.7.

Subscriber's key pairs are generated in cryptographic modules using the facilities provided by VIDA as follows:

a. secure usb tokens, which are in compliant with FIPS 140-2 level 3 requirements;
b. hardware cryptographic module, which are in compliant with FIPS 140-2 level 3 requirements. Subscriber's Private Key then stored in VIDA Vault in accordance with section 6.2.7.

Pemilik / Subscriber	**FIPS 140-2 Level**	**Dibangkitkan di dalam Modul Kriptografi / Generated in Cryptographic Module**	**Modul Kriptografi / Cryptographic Module**
Pemilik untuk TTE / Subscriber for Signature	3	Ya / Yes	Modul Kriptografi / Cryptographic Module : - HSM - Secure USB token

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

Kunci Privat Pemilik yang berada dalam *secure USB token* dapat dikirimkan oleh VIDA kepada Pemilik. Pengiriman perangkat fisik *secure USB token* dilakukan oleh VIDA melalui kurir yang terpercaya. Dalam semua kasus maka Kunci Privat dilindungi terhadap aktivasi, kebocoran, atau perubahan selama proses pengiriman. Pemilik mengkonfirmasi bahwa Pemilik telah menerima perangkat dan VIDA menyimpan catatan konfirmasi tersebut.

Pengiriman pin aktivasi dilakukan secara langsung kepada Pemilik melalui pesan elektronik yang terenkripsi.

The Subscriber's Private Key which resides in a secure USB token may be delivered by VIDA to Subscriber.

The delivery of the secure USB token physical device is carried out by VIDA through a trusted courier. In all cases the Private Key must be protected against activation, compromise, or change during the delivery process. Subscriber confirms that he has received the device and VIDA keeps a record of the confirmation.

The activation pin is sent directly to the Subscriber via an encrypted electronic message.

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

Pemilik melakukan proses inisiasi pembangkitan pasangan kunci kemudian mengirimkan Kunci Publik dalam bentuk *Certificate Signing Request (CSR)* sebagai bagian dari proses penggunaan layanan VIDA. Kunci Publik dan identitas Pemilik harus dikirimkan dengan aman menggunakan TLS minimal 1.2 dengan algoritma RSA dan panjang kunci 2048 bit.
Pada saat ini VIDA belum menerima permohonan penerbitan Sertifikat berdasarkan CSR dari luar layanan VIDA.

Subscribers initiate Key Pairs generation and CSR submission as part of the utilization of VIDA service. The Public Key and Subscriber's identity must be transmitted securely using a minimum of TLS 1.2 with the RSA algorithm and a key length of 2048 bits.
At this time VIDA has not received a certificate issuance application based on CSR from outside of the VIDA service.

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

Setiap Sertifikat yang diterbitkan oleh VIDA berisi Kunci Publik. VIDA menyediakan mekanisme publikasi terhadap Sertifikat VIDA yang aktif melalui repositori yang dapat diakses oleh Pengandal. Penjelasan tentang publikasi dan repositori Sertifikat mengacu pada Bagian 2.2.
Pada jangka waktu tertentu sebelum Kunci Publik VIDA kedaluwarsa, suatu pasangan kunci penandatanganan Sertifikat yang baru akan dibangkitkan untuk menjaga operasional VIDA berjalan normal.

Each certificate issued by VIDA contains a Public Key. VIDA provides a publication mechanism for active VIDA certificates through a repository that can be accessed by the Relying Party. Certificate publication and repository are referred to Section 2.2.

For a certain period before the expiry date of a VIDA's Public Key, a new key pair for certificate signing will be generated so that VIDA keep working normally.

6.1.5. Ukuran Kunci / Key Sizes

VIDA membuat Sertifikat menggunakan algoritma RSA dengan panjang kunci 2048 bit dan hash SHA384 ketika menandatangani Sertifikat Pemilik.

Pemilik Sertifikat harus menggunakan algoritma RSA dengan panjang kunci 2048 bit

VIDA generates certificates using the RSA algorithm with a key length of 2048 bit, and SHA384 hash algorithm when signing Subscriber certificates.

Subscribers should use the RSA algorithm with a key length of at least or equivalent to 2048

dengan hash SHA384 ketika membuat tanda tangan elektronik.

bit , and the SHA384 hash algorithm when generating digital signatures.

	Panjang Kunci	Algoritma Kunci
VIDA Root CA	4096	RSA
VIDA Issuing CA (PSrE Berinduk)	4096	RSA
VIDA Issuing CA	2048	RSA
Pemilik	2048	RSA

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

Pasangan Kunci VIDA dan Pemilik dibangkitkan oleh VIDA sesuai bagian 6.1.1 dan Kunci Publiknya divalidasi sesuai FIPS 186-4.

VIDA's keypair and Subscriber's keypairs are generated by VIDA as per section 6.1.1 and the Public Key is validated as per FIPS 186-4.

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

Kunci VIDA dipakai untuk digital signature, certificate sign, dan CRL sign.

VIDA key is used for digital signature, certificate sign, and CRL sign.

Kunci Pemilik yang dipakai untuk pemanfaatan tanda tangan elektronik bagi Pemilik individual dan segel elektronik bagi Pemilik entitas menggunakan key usage digital signature.

Subscriber Key used for digital signature utilization for individual Subscriber and electronic seal for entity Subscriber using key usage digital signature.

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

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

VIDA menggunakan modul kriptografi yang sudah sesuai standar FIPS 140-2 level 3 untuk operasional VIDA.
Modul kriptografi yang sudah beroperasi diawasi dan dijaga dari akses yang tidak sah. Pengaktifan maupun penonaktifannya modul kriptografi milik VIDA dilakukan oleh personel VIDA yang berwenang sesuai dengan mekanisme yang ditentukan. Apabila perangkat modul kriptografi sudah tidak akan digunakan dan diberhentikan untuk seterusnya, maka dilakukan *factory reset*.
Kunci Privat Pemilik disimpan dalam keadaan terenkripsi di lingkungan FIPS 140-2 sesuai bagian 6.1.1.2. Kendali terhadap perangkat modul kriptografi dikelola oleh VIDA dan hanya dapat dimanfaatkan oleh Pemilik sesuai bagian 4.5.1.

VIDA uses a FIPS 140-2 level 3 validated hardware cryptographic module for VIDA operation.
Cryptographic modules that are already in operation mode are monitored and protected from unauthorized access. The activation or deactivation of VIDA's cryptographic module is carried out by authorized VIDA personnel in accordance with the specified mechanism. If the cryptographic module device is no longer used and will be permanently discontinued, a factory reset is carried out.

Subscriber's Private Key is stored encrypted in a FIPS 140-2 environment as per section 6.1.1.2. Control of the cryptographic module device is managed by VIDA and can only be accessed by the Subscriber in accordance with section 4.5.1.

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

VIDA telah mengimplementasikan mekanisme teknis dan prosedural yang mempersyaratkan partisipasi dari beberapa peran terpercaya untuk melaksanakan operasi kriptografis yang sensitif sesuai dengan bagian 5.2.2. Suatu jumlah minimum dari *Secret Shares* (m) dari sejumlah total *Secret Shares* yang dibuat dan didistribusikan untuk dipakai di modul kriptografi tertentu (n) diperlukan untuk mengaktifkan sebuah Kunci Privat VIDA yang disimpan di dalam modul.

VIDA has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive cryptographic operations in accordance with section 5.2.2. 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 VIDA Private Key stored in the module.

6.2.3. Eskro Kunci Privat / Private Key Escrow

Lihat bagian 4.12.1.	Lihat bagian 4.12.1

6.2.4. Backup Kunci Privat / Private Key Backup

Kunci Privat VIDA dicadangkan di bawah kendali multi-pihak yang sama dengan kunci aslinya. Paling tidak satu salinan dari Kunci Privat harus disimpan dengan aman. Semua salinan Kunci Privat VIDA harus dilindungi dengan cara yang sama dengan aslinya.	VIDA's Private Key is backed up under the same multiparty control as the original key. At least one copy of the Private Key shall be stored securely. All copies of VIDA Private Keys shall be accounted for and protected in the same manner as the original.
Pemilik belum dimungkinkan untuk melakukan *backup* terhadap Kunci Privat mereka pada layanan VIDA. Untuk kunci Privat Pemilik yang diberikan kepada Pemilik melalui *secure USB token,* tidak dapat dicadangkan oleh VIDA atau disalin dengan cara apa pun. Kunci Privat Pemilik yang dititipkan pada VIDA melalui layanan *Vault* dapat dicadangkan oleh VIDA untuk keberlangsungan layanan.	Subscriber is not enabled with the Private Key backup option in VIDA service. In the case where the Subscriber's Private Key is given to the Subscriber via a secure USB token, the Private Key can not be backed up by VIDA or copied in any way. In the case where the Subscriber's Private Key is stored in the VIDA through the vault service, the Private Key can be backed up by the VIDA for service continuity purposes.

6.2.5. Pengarsipan Kunci Privat / Private Key Archival

Kunci Privat VIDA tidak diarsipkan. Kunci Privat Pemilik tidak diarsipkan.	VIDA Private Keys shall not be archived. Subscriber's Private Key shall not be archived.

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

Kunci Privat VIDA dicadangkan langsung menggunakan *backup HSM.* Kunci Privat VIDA tidak pernah sekalipun boleh berada dalam bentuk *plaintext* di luar modul kriptografi. Komponen modul kriptografi serta perangkat *backup HSM* dilindungi di dalam brankas yang terletak di area yang aman. Kunci Privat Pemilik disimpan dalam keadaan terenkripsi di lingkungan FIPS 140-2 sesuai bagian 6.1.1.2.	VIDA Private Keys are backed up directly using HSM backup. VIDA Private Key may never exist in plaintext outside of the cryptographic module. The components of the cryptographic module as well as the HSM backup device are protected in a safe located in a secure area. Subscriber's Private Key is stored in an encrypted form in a FIPS 140-2 environment in accordance with section 6.1.1.2

.

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

Kunci Privat VIDA disimpan pada modul kriptografi FIPS 140-2 level 3, dalam bentuk terenkripsi dan terlindungi oleh kata sandi.

VIDA Private Keys are stored on FIPS 140-2 level 3 cryptographic modules, in encrypted form and password-protected.

Kunci Privat Pemilik dibangkitkan sesuai bagian 6.1.1.2 dan disimpan dalam keadaan terenkripsi di lingkungan yang memenuhi kriteria FIPS 140-2 sesuai tabel di bawah ini. Kunci Privat tidak dapat diakses tanpa mekanisme autentikasi dari Pemilik sesuai bagian 4.5.1.

Subscriber Private Key is generated in accordance with section 6.1.1.2 and then stored in encrypted form in the environment that is in compliance with FIPS 140-2 criteria as per below table. The Private Key cannot be accessed without passing the authentication mechanism from the Subscriber in accordance with section 4.5.1.

Entitas / Entity	**Disimpan dalam / Stored in**	**FIPS 140-2 Level**
Kunci Privat CA / VIDA CA's Private Key	Perangkat Keras Modul Kriptografi / Hardware Cryptographic Module	3
Kunci Privat Pemilik / Subscriber's Private Key	VIDA Vault dengan keadaan terenkripsi di lingkungan yang memenuhi kriteria FIPS 140-2 level 2 / VIDA Vault in encrypted form in the environment that is in compliance with FIPS 140-2 level 2	2

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

Pengaktifan Kunci Privat VIDA dilakukan oleh personil yang berwenang dengan cara yang sesuai dengan petunjuk dan dokumentasi yang disediakan oleh penyedia modul kriptografi serta menerapkan kendali multi pihak sesuai bagian 5.2.2. Kunci Privat CA milik VIDA akan aktif hingga dinonaktifkan seperti pada bagian 6.2.9.

Pengaktifan Kunci Privat Pemilik dilakukan dengan cara mengautentikasi Pemilik sebelum Pemilik melakukan aktivasi Kunci Privat terkait sesuai bagian 4.5.1. Pemilik

Activation of VIDA Private Key operations is performed by authorized persons that meets the instructions and documentation provided by the cryptographic module provider and implements multi-party controls in accordance with section 5.2.2. VIDA's CA Private Key will be active until deactivated as in section 6.2.9.

Activation of Subscriber's Private Key is carried out by authenticating the Subscriber before the Subscriber is activating the relevant Private Key in accordance with section 4.5.1. The Subscriber is obliged to protect access to his

wajib melindungi akses terhadap Kunci Privatnya sesuai bagian 1.3.3 dan 4.5.1. Entri data aktivasi yang berupa PIN atau *password* dilindungi dari pengungkapan.

Private Key according to sections 1.3.3 and 4.5.1. Activation data entry in the form of a PIN or password is protected from disclosure.

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

Kunci Privat VIDA dinonaktifkan oleh personil yang berwenang melalui prosedur *logout* manual pada modul kriptografi sekaligus mencopot token aktivasi kunci. Kunci Privat VIDA yang sudah tidak digunakan di dalam modul kriptografi dinonaktifkan oleh personil VIDA yang berwenang.

VIDA's Private Key is deactivated by authorized persons via a manual logout procedure on the cryptographic module and unplugging the key activation token.Unused VIDA Private Keys within the cryptographic module are deactivated by authorized VIDA personnel.

Penonaktifan Kunci Privat Pemilik yang disimpan dan dikelola oleh VIDA dilakukan dengan cara Pemilik *logout* dari akun VIDA. Penonaktifan Kunci Privat Pemilik yang diserahkan kepada Pemilik dilakukan dengan cara mencabut USB token VIDA dari perangkat komputer (*workstation*) Pemilik.

.

Deactivating Subscriber's private key which is stored and managed by VIDA is performed by Subscriber logging out of the VIDA account Deactivating Subscriber's private key which is stored and managed by Subscriber is performed by Subscriber by unplugging VIDA USB token from the Subscriber's workstation.

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

Kunci Privat VIDA dihancurkan apabila

a. Kunci Privat VIDA tersebut tidak diperlukan lagi, atau
b. Sertifikat yang terkait dengan Kunci Privat tersebut telah dicabut atau kedaluwarsa, atau
c. VIDA berhenti beroperasi.

Para personil peran terpercaya menghapus Kunci Privat CA milik VIDA dari Modul Kriptografi dan menghapus *backup* yang terasosiasi dengan Kunci Privat tersebut dengan menimpa (*overwrite*) atau menginisialisasi ulang agar tidak ada lagi informasi yang dapat digunakan untuk memulihkan Kunci Privat CA milik VIDA yang telah dihapus tersebut. Kejadian penghancuran Kunci Privat PSrE VIDA harus dicatat sebagai barang bukti sesuai dengan bagian 5.4.

VIDA Private Key is destroyed when

a. VIDA Private Key is no longer needed, or
b. The certificate associated with the Private Key has been revoked or expired, or
c. if VIDA stops operating.

Trusted roles personnel shall delete the VIDA's CA Private Keys from Cryptographic Module and the backup associated with the Private Key by overwriting or re-initializing it so that no more information can be used to restore the deleted VIDA's CA Private Key. The event of destroying VIDA's Private Key must be recorded into evidence under section 5.4.

Penghancuran Kunci Privat Pemilik yang disimpan dan dikelola oleh VIDA dapat dilakukan dengan cara menghapusnya dari media penyimpanan.	Destruction of the Subscriber's Private Key which is stored and managed by VIDA can be done by deleting it from the storage media.
Penghancuran Kunci Privat Pemilik yang diserahkan kepada Pemilik dilakukan dengan cara USB token diinisialisasi ulang.	Destruction of the Subscriber's Private Key which is handed over to the Subscriber is carried out by re-initializing the USB token.

6.2.11. Pemeringkatan Modul Kriptografi / Cryptographic Module Rating

Seperti diuraikan pada bagian 6.2.1.	As described in section 6.2.1.

6.3. Aspek Lain dari Manajemen Pasangan Kunci / Other Aspects of Key Pair Management

6.3.1. Pengarsipan Kunci Publik / Public Key Archival

Kunci Publik diarsipkan sebagai sebagai satu kesatuan dari Sertifikat dan mengikuti mekanisme pengarsipan Sertifikat sesuai bagian 5.5.	The Public Key is archived as part of the certificate archival following the mechanism stipulated in section 5.5.

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

Periode operasional maksimum dari kunci dan Sertifikat dapat dilihat pada tabel di bawah ini. Periode operasional ditentukan dengan mengacu kepada ketentuan CP PSrE Induk serta mempertimbangkan ukuran kunci dan perkembangan teknologi terkini di bidang kriptografi, sehingga baik tingkat keamanan maupun efisiensi dapat diperoleh.	The maximum operational period of the keys and Certificates can be seen from below table. The operational period is defined by aligning with Root CA Indonesia CP as well as considering the size of the keys and the technological developments in cryptography, so that the best level of security and efficiency can be achieved.

Kunci/Key	Algoritma/Algorithm			
	4096 Bit Keys (RSA)		2048 Bit Keys (RSA) prime	
	Kunci	Sertifikat	Kunci	Sertifikat
VIDA/ VIDA CA	10 tahun/ 10 years	10 tahun/ 10 years	-	-
Time Stamp Authority	3 tahun/ 3 years	3 tahun/ 3 years	-	-
OCSP Responder	3 tahun/ 3 years	3 tahun/ 3 years	-	-
Subscriber for Signature / Pemilik untuk TTE	-	-	maksimal 2 tahun/ maximum 2 years	maksimal 2 tahun/ maximum 2 years
				1 tahun
				30 menit

6.4. Data Aktivasi / Activation Data

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

Pembangkitan dan penggunaan data aktivasi PSrE untuk mengaktifkan Kunci Privat PSrE dibuat pada saat *key ceremony* sesuai bagian 6.1.1. Data aktivasi harus dibangkitkan secara otomatis dengan modul kriptografi yang sesuai. Data aktivasi untuk mengaktifkan Kunci Privat dilindungi berdasarkan tingkat keamanan yang sesuai dengan modul kriptografi yang digunakan.

Generation and use of CA activation data used to activate CA Private Keys shall be made during a key ceremony as per section 6.1.1. Activation data shall be generated automatically by the appropriate cryptographic modules. The activation data used to activate Private Keys shall be protected based on an appropriate security level in accordance with the cryptographic module used.

6.4.2. Perlindungan Data Aktivasi / Activation Data Protection

Data aktivasi Kunci Privat VIDA disimpan dalam token fisik yang dilindungi dengan pengamanan modul kriptografi serta mekanisme kendali akses fisik sesuai bagian 6.2.

Private Key activation data is stored in a physical token which is protected by secure cryptographic modules and physical access control mechanisms according to section 6.2.

6.4.3. Aspek Lain dari Data Aktivasi / Other Aspects of Activation Data

Tidak ditentukan.

No stipulation.

6.5. Kendali Keamanan Komputer / Computer Security Controls

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

VIDA memastikan bahwa sistem yang menjaga perangkat lunak VIDA dan *data files* aman dari akses yang tidak sah. Semua komputer yang merupakan bagian dari sistem PSrE milik VIDA telah dikonfigurasi dan diperkuat keamanannya menggunakan praktik terbaik *(best practices)* industri. Sistem komputer PSrE harus dikonfigurasi dengan meminimalisisasi jumlah akun dan layanan jaringan yang diperlukan.

Fungsi keamanan komputer dapat tersedia melalui keamanan atas komponen yang terkait, seperti sistem operasi, perangkat lunak, perangkat keras, dan perlindungan fisik. CA harus menyertakan fungsi berikut dalam mencakup namun tidak terbatas pada fungsi berikut:

a. Memerlukan login terautentikasi untuk akses logikal;
b. Menyediakan kontrol akses terbatas dengan kewenangan yang sesuai;
c. Menyediakan kapabilitas audit keamanan;
d. Memerlukan penggunaan kriptografi untuk sesi komunikasi dan keamanan basis data;
e. Menyediakan perlindungan mandiri untuk sistem operasi;
f. Memerlukan penggunaan kebijakan kata sandi kuat;
g. Memerlukan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
h. Menyediakan perlindungan terhadap *malicious code;*

VIDA ensures that the systems maintaining the VIDA software and data files are secure from unauthorized access. All computers that are part of the VIDA's CA system have been configured and hardened using industry best practices.

CA's computer system should be configured to minimize the number of accounts and network services required.

Computer security functions may be provided by the security of its related component such as operating system, software, hardware, and physical safeguards. The CA shall include the following functionality include but not limited to the following:

a. Require authenticated logins for logical access;
b. Provide discretionary access control with appropriate privilege;
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;
f. Require use of a strong password policy;
g. Requires the use of trusted channels for identification and authentication;
h. Provides protection against malicious code;

i. Menyediakan cara untuk menjaga integritas perangkat lunak;
j. Memerlukan pemeriksaan mandiri terkait keamanan layanan.

i. Provides a way to maintain software integrity;
j. Requires self-test regarding the security of the service.

6.5.2. Peringkat Keamanan Komputer / Computer Security Rating

Tidak ditentukan.

No stipulation.

6.6. Kendali Teknis Siklus Hidup / Life Cycle Technical Controls

6.6.1. Kendali Pengembangan Sistem / System Development Controls

Kendali pengembangan sistem PSrE adalah sebagai berikut:

1. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;
2. Pengadaan perangkat keras dan perangkat lunak harus dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen-komponen yang terdapat dalam perangkat lunak dirusak;
3. Pengembangan perangkat keras dan perangkat lunak dilakukan dalam sebuah lingkungan yang terkendali, dan proses pengembangan harus didefinisikan dan didokumentasikan. Syarat ini tidak berlaku bagi perangkat lunak maupun perangkat keras komersil siap-pakai yang dibeli;
4. Perangkat keras dan perangkat lunak didedikasikan untuk melaksanakan aktivitas IKP. Tidak boleh ada aplikasi lain, perangkat lunak, koneksi jaringan, atau komponen perangkat lunak yang diinstall yang bukan bagian dari operasional IKP;
5. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya dimuat ke perangkat.

CA system development control is as follows:

1. Using software designed and developed through a formal and documented methodology;
2. Procurement of hardware and software must be carried out with efforts to reduce the possibility of components contained in the software being damaged;
3. Hardware and software development is carried out in a controlled environment, and the development process must be defined and documented. These terms do not apply to commercial off-the-shelf software or hardware purchased;
4. Hardware and software are dedicated to carrying out PKI activities. There may be no other applications, software, network connections, or software components installed that are not part of PKI operations;
5. Sufficient care is taken to prevent malicious software from being loaded onto the device.

6. Perangkat keras dan perangkat lunak PSrE harus selalu dipindai untuk mendeteksi adanya *malicious code*.

Perangkat lunak yang digunakan untuk manajemen Sertifikat, baik dikembangkan sendiri atau siap pakai, sepenuhnya diuji di lingkungan non-produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem berikut komponennya dilaksanakan sesuai proses manajemen perubahan.

6. CA hardware and software should always be scanned for malicious code.

Software used for Certificate management, whether in-house developed or off-the-shelf, is fully tested in a non-production environment before being deployed in a production environment. Every change to the system and its components is carried out according to the change management process.

6.6.2. Kendali Manajemen Keamanan / Security Management Controls

Konfigurasi dari sistem PSrE milik VIDA serta seluruh modifikasi dan *upgrade* didokumentasikan dan dikelola oleh VIDA. Terdapat mekanisme untuk mendeteksi modifikasi yang tidak sah ke perangkat lunak maupun konfigurasi sistem PSrE milik VIDA. Manajemen konfigurasi dijalankan dalam melakukan instalasi dan pemeliharaan sistem PSrE. Perangkat lunak PSrE, ketika dimuat pertama kali, harus diperiksa kebenarannya bahwa perangkat lunak tersebut benar berasal dari penyedia, tanpa modifikasi, dan benar merupakan versi yang sesuai.

Configuration of the VIDA CA system along with all modifications and its upgrades are documented and managed by VIDA. There is a mechanism to detect unauthorized modifications to the VIDA CA system software and configuration. Configuration management is applied in the installation and maintenance of CA systems. CA software, when first loaded, must be verified that it is coming from the legitimate provider, without modification, and is the correct version to use.

VIDA memiliki prosedur dan jadwal pemeliharaan sistem. Personel PSrE yang bertanggung jawab harus melakukan pemantauan sistem secara rutin. Sebagai tambahan dari pemantauan yang dilakukan secara manual, mekanisme pemantauan otomatis yang menginformasikan Peran Terpercaya ketika ada aktivitas yang tidak wajar pada sistem juga dapat ditambahkan.

VIDA has system maintenance procedures and schedules. Trusted Roles personnel must carry out regular monitoring of the system. In addition to manual monitoring, automatic monitoring mechanisms that can inform Trusted Roles when inappropriate activity is occurring can also be added.

6.6.3. Kendali Keamanan Siklus Hidup / Life Cycle Security Controls

VIDA melakukan pengawasan terhadap skema pemeliharaan untuk mempertahankan tingkat kepercayaan perangkat keras dan perangkat lunak dan secara berkala mengevaluasi keefektifannya melalui audit.

VIDA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware and periodically evaluate the effectiveness through audit.

6.7. Kendali Keamanan Jaringan / Network Security Controls

VIDA menerapkan langkah-langkah keamanan jaringan yang sesuai untuk memastikan bahwa jaringan terjaga dari *denial of service (DoS)* dan serangan intrusi. Langkah-langkah tersebut termasuk pada penggunaan *firewall*. *Port* jaringan dan layanan yang tidak dipakai harus dimatikan. Perangkat lunak jaringan yang dibutuhkan harus tersedia guna keberlangsungan operasional VIDA.

VIDA will employ appropriate network security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of firewalls. Unused network ports and services shall be turned off. Any necessary network software shall be available for the operational continuity of the VIDA.

6.8. Time-Stamping / Stempel Waktu

Semua komponen VIDA secara berkala disinkronisasikan dengan sebuah layanan waktu menggunakan *Network Time Protocol* (NTP). *Timestamp authority (TSA)* juga bisa digunakan jika perlu. Waktu yang didapat dari layanan waktu diatas akan digunakan untuk menentukan waktu pada saat:

a. Validitas waktu permulaan untuk sebuah Sertifikat VIDA;
b. Pencabutan Sertifikat VIDA;
c. Pembaruan CRL; dan
d. Penerbitan Sertifikat Pemilik;
e. Respon OCSP.

Mekanisme elektronik atau manual bisa digunakan untuk tetap mempertahankan akurasi waktu pada sistem. Penyelarasan jam merupakan sebuah aktivitas yang dapat diaudit sebagaimana diatur pada Bagian 5.4.1.

All VIDA components are regularly synchronized with a time service using a Network Time Protocol (NTP) service. A Timestamp Authority (TSA) may be used to provide the trusted time. Time derived from the time service shall be used for establishing the time of:

a. Initial validity time of VIDA certificate;
b. Revocation of VIDA certificate;
c. Posting of CRL updates; and
d. Issuance of Subscriber certificates;
e. OCSP response.

Electronic or manual mechanisms may be used to maintain system time accuracy. Clock synchronization is considered as auditable events as stipulated in Section 5.4.1.

Dalam menyelenggarakan layanan Penanda Waktu Elektronik tersertifikasi yang digunakan pada layanan VIDA, VIDA mengacu pada tanda waktu nasional yang disebarkan oleh lembaga yang menyelenggarakan urusan pemerintahan di bidang meteorologi, klimatologi, dan geofisika.

When providing a certified electronic Timestamp Service, VIDA will refer to the national timestamp provided by the government agency whose authority concerns meteorology, climatology, and geophysics.

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

7.1. Profil Sertifikat / Certificate Profile

Rincian profil Sertifikat VIDA mengikuti standar RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” dan sesuai dengan standar interoperabilitas PSrE Indonesia. VIDA melakukan tinjauan terhadap profil Sertifikat secara berkala minimal setahun sekali.

A certificate profile according to RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile” is used. VIDA shall review certificate profiles periodically at least once a year.

VIDA CERTIFICATE AUTHORITY					
Certificates Extension	**VIDA**		**Pemilik / Subscriber**		**Description**
keyUsage	Critical TRUE	digitalSignature keyCertSign cRLSign	Critical TRUE	digitalSignature nonRepudiation	Ekstensi yang mendefinisikan kegunaan kunci yang terkandung pada Sertifikat
certificatePolicies	Critical TRUE	None	Critical TRUE		mengacu kepada OID yang dirujuk pada bagian 7.1.6
BasicConstraint	Critical TRUE	Subject Type=CA Path Length Constraint=None	Critical FALSE	Subject Type=End Entity Path Length Constraint=None	Ekstensi untuk mengidentifikasi tipe subjek dari Pemilik Sertifikat
Extended Key Usage	Non Critical FALSE		Non Critical FALSE		Ekstensi yang membatasi secara teknis penggunaan Sertifikat yang diterbitkan VIDA
CRLDistribution Points	Critical TRUE	http://crl.rootca.id/RootCAIndonesiaDSG1.crl	Critical TRUE	http://crl.vida.id/crli/vidapsre.crl	Ekstensi yang memuat URL dari CRL agar Pengandal dapat memeriksa status Sertifikat.

Authority Key Identifier	Non Critical TRUE	KeyID=2968f95c56db1a6eabe223df92c26b12d2a9fe8d	Non Critical TRUE		metode penghitungan mengacu pada RFC 5280
Subject Key Identifier	Non Critical TRUE	94823ad6ed7fc3940583cad35dc85e01fc75d1f2	Non Critical TRUE		metode penghitungan mengacu pada RFC 5280

VIDA SIGN CERTIFICATE AUTHORITY					
Certificates Extension	**VIDA**		**Pemilik / Subscriber**		**Description**
keyUsage	Critical TRUE	digitalSignature keyCertSign cRLSign	Critical TRUE	digitalSignature nonRepudiation	Ekstensi yang mendefinisikan kegunaan kunci yang terkandung pada Sertifikat
certificatePolicies	Critical TRUE	None	Critical TRUE		mengacu kepada OID yang dirujuk pada bagian 7.1.6
BasicConstraint	Critical TRUE	Subject Type=CA Path Length Constraint=None	Critical FALSE	Subject Type=End Entity Path Length Constraint=None	Ekstensi untuk mengidentifikasi tipe subjek dari Pemilik Sertifikat
Extended Key Usage	Non Critical FALSE		Non Critical FALSE		Ekstensi yang membatasi secara teknis penggunaan Sertifikat yang diterbitkan VIDA
CRLDistribution Points	Critical TRUE	http://crl.vida.id/crl/VIDARootCA.crl	Critical TRUE	http://crl.vida.id/crli/VIDASignCA.crl	Ekstensi yang memuat URL dari CRL agar Pengandal dapat memeriksa status Sertifikat.
Authority Key Identifier	Non Critical TRUE	KeyID=927d7b2bd04d334686324a9161b00fe26ab6f669	Non Critical TRUE		metode penghitungan mengacu pada RFC 5280

Subject Key Identifier	Non Critical TRUE	3ae7bb2126a75a1192db8f7a4b14bab705e3e030	Non Critical TRUE		metode penghitungan mengacu pada RFC 5280

OID untuk algoritma penandatanganan elektronik adalah sebagai berikut:

a. VIDA atau Pemilik menggunakan enkripsi RSA untuk kunci subjek dan SHA384 dengan enkripsi RSA untuk tanda tangan elektronik;
b. Pemilik menggunakan enkripsi ECDSA untuk kunci subjek dan SHA256 dengan enkripsi ECDSA untuk tanda tangan elektronik.

OID algorithms used for digital signature are the followings:

a. VIDA or Subscriber uses RSA encryption for subject keys and SHA384 with RSA encryption for digital signatures;
b. The Subscriber uses ECDSA encryption for subject keys and SHA256 with ECDSA encryption for digital signatures.

rsaEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}.

sha384withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}.

ecdsa-with-SHA256(2) OBJECT IDENTIFIER := {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)}

7.2. Profil CRL / CRL Profile

Profil CRL VIDA sesuai dengan Standar Interoperabilitas PSrE Indonesia yang menggunakan CRL dengan *entry extension* RFC 5280.

VIDA's CA CRL profile conforms to the Standard Interoperability of PSrE Indonesia which uses CRL with entry extension RFC 5280.

7.3. Profil OCSP / OCSP Profile

VIDA mengoperasikan sebuah responder Online Certificate Status Protocol (OCSP) yang sesuai dengan RFC 6960 atau RFC 5019 dan mengacu kepada standar interoperabilitas PSrE Indonesia.

VIDA operates an Online Certificate Status Protocol (OCSP) responder in compliance with RFC 6960 or RFC 5019 refer to Indonesia CA interoperability standard.

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

VIDA menjalani audit kepatuhan dan menyampaikan laporan berkala yang dipersyaratkan oleh ketentuan peraturan perundang-undangan terkait Penyelenggaraan Sertifikasi Elektronik. Selain itu, VIDA juga menjalani audit kepatuhan dan/atau penilaian terkait persyaratan Webtrust CA, kebutuhan teknis Adobe Approved Trust List 2.0, serta sistem manajemen keamanan informasi ISO 27001.

VIDA undergoes compliance audit and submit reports periodically as required by laws and regulations concerning Certification Authority. VIDA is also audited for compliance to Webtrust CA, Adobe Approved Trust List Technical Requirement 2.0, and information security management system ISO 27001.

8.1. Frekuensi atau Lingkup Penilaian / Frequency or Circumstances of Assessment

VIDA menjalani audit kepatuhan yang diselenggarakan secara berkala oleh

a. auditor internal VIDA;
b. auditor eksternal independen yang ditunjuk oleh VIDA;
c. Lembaga Sertifikasi PSrE atau PSrE Induk untuk penilaian kelaikan PSrE sesuai ketentuan peraturan perundang-undangan terkait PSrE.

terhadap kriteria audit dan lingkup audit yang telah ditetapkan. Lingkup audit meliputi namun tidak terbatas pada kesesuaian CPS dengan pelaksanaan operasional IKP VIDA, layanan VIDA berupa hasil pengembangan produk, maupun hasil kerja sama antara VIDA dengan Partisipan IKP sesuai bagian 1.3.

Audit kepatuhan dilaksanakan minimal sekali setahun dan juga setiap setelah terjadi perubahan yang signifikan terhadap CPS, prosedur dan teknik yang diterapkan oleh VIDA.

VIDA will undergo a compliance audit on a regular basis conducted by

a. VIDA internal auditor;
b. independent external auditor appointed by VIDA;
c. CA Conformity Assessment Body or Root CA Indonsia for compliance audit in accordance to laws and regulation concerning CA.

towards the defined audit criteria and scope. Scope of the audit covers but is not limited to suitability of CPS with the implementation of VIDA PKI operations, VIDA service that may be the result of product development, as well as result of the cooperation between VIDA with other PKI Participants as per section 1.3.

VIDA undergoes compliance audits at least once a year or after significant changes to the established CPS, procedures and techniques implemented by VIDA.

8.2. Identitas atau Kualifikasi Auditor / Identity or Qualifications of Auditor

Audit kepatuhan bagi VIDA dilaksanakan oleh Auditor yang memiliki kompetensi pada

Compliance audit of VIDA CA is performed by Auditors who shall possess sufficient skills on

bidang audit kepatuhan dan benar-benar memahami persyaratan CPS ini.

Auditor kepatuhan harus memiliki kualifikasi sebagai berikut:

a. Auditor merupakan individu atau tim yang independen dan *qualified*.
b. Auditor memiliki pengetahuan yang cukup tentang Sertifikat Elektronik, *X.509 versi 3 PKI Certificate Policy and Certification Practices Framework*, familiar dengan teknologi IKP, pemanfaatan layanan PSrE yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik dan Segel Elektronik, serta ketentuan peraturan perundang-undangan di Indonesia terkait Informasi dan Transaksi Elektronik, Penyelenggaraan Sistem dan Transaksi Elektronik, Tata Kelola Penyelenggaraan Sertifikasi Elektronik;
c. Auditor memiliki kecakapan dalam melaksanakan audit keamanan informasi, audit peralatan dan teknik keamanan informasi, serta memahami *best practices* industri terkait keamanan informasi berikut risiko keamanan;
d. Auditor memenuhi kualifikasi yang cukup untuk menyelenggarakan suatu skema audit tertentu atau memiliki *third-party attestation function*. Bisa dibuktikan dengan kepemilikan sertifikasi (seperti sertifikasi CISA atau sertifikasi *IT Security specialist*), akreditasi, lisensi, atau asesmen lain yang sah lainnya;
e. Auditor menguasai set keahlian tertentu serta menjalani pengujian kompetensi atau jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional.
f. Patuh terhadap hukum dan peraturan yang berlaku, atau kode etik profesional.

compliance audit, and thoroughly understand the requirements in this CPS.

Compliance auditors must possess these qualifications:

a. Auditors can be an individual or a team which is qualified and independent;
b. Auditors shall have a sufficient knowledge on digital certificate, X.509 PKI Certificate Policy and Certificate Practice Framework, familiarity with PKI technology, CA service utilizing digital certificate such as digital signature and e-seal, and knowledge about laws and regulation in Indonesia concerning electronic information and transactions, electronic system and transaction operations, and certification authority governance;
c. Auditors shall have an adequate skills on auditing information security, auditing information security device and technique, and understanding industry best practices about information security and security risk;
d. Auditors have required qualifications that are considered sufficient for conducting a particular audit scheme or *third-party attestation function*. This can be seen by possession of certification (such as CISA or IT security specialist certification), accreditation, license, or other relevant and valid assessment;
e. Auditors shall master a set of certain skills or undergo competency testing or quality assurance such as peer review, standards regarding accurate staff assigning, and involvement and requirements for higher professional education.
f. Bound by applicable law and regulation, or professional code of ethics.

8.3. Hubungan Auditor dengan Entitas yang Dinilai / Auditor's Relationship to Assessed Entity

Auditor eksternal berasal dari organisasi yang terpisah dari VIDA untuk memberikan evaluasi yang tidak memihak, dan independen. Auditor eksternal tidak boleh melayani VIDA dalam mengembangkan maupun memelihara CPS atau fasilitas PSrE. PA VIDA harus memeriksa independensi dan memastikan tidak ada konflik kepentingan dari auditor eksternal sebelum menunjuk auditor tersebut.

Auditor eksternal harus memiliki perjanjian kontrak dengan VIDA dan menjaga standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan penerapan pertimbangan profesional yang independen, sesuai dengan tindakan disipliner yang ditentukan oleh badan perizinannya.

The external auditor comes from an organisation separated from VIDA to provide unbiased and independent evaluation. External auditor must not have served VIDA in developing or maintaining VIDA's CPS or CA facility. VIDA's PA shall check the independence and ensure there is no conflict of interest from the external auditor before appointing the auditor.

External auditor shall have a contractual engagement with VIDA and maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4. Topik Penilaian / Topics Covered by Assessment

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa VIDA beroperasi sesuai dengan ketentuan peraturan perundang-undangan. Penilaian Kelaikan mencakup penilaian CPS untuk menentukan bahwa CPS telah diimplementasikan dan ditegakkan. Cakupan penilaian setidaknya mencakup organisasi, tata kelola dan manajemen operasional, personil, serta infrastruktur dari VIDA. Penilaian dilaksanakan untuk memenuhi persyaratan dari skema audit tertentu. Persyaratan dapat berubah seiring dengan pembaruan skema audit.

The purpose of a Compliance Audit is to verify that VIDA operates in accordance with this laws and regulations. The Compliance Audit must include an assessment of the applicable CPS, to ensure that the requirements of the CPS are being implemented and enforced. The assessment topics at least cover organization, governance and operation management, personnel, and infrastructure of VIDA. The audit must meet the requirements of certain audit schemes. These requirements may be changed along with audit schemes update.

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

Ketika auditor kepatuhan menemukan adanya ketidaksesuaian antara bagaimana VIDA dirancang atau dioperasikan atau dipelihara sesuai dengan persyaratan pada CPS yang berlaku, tindakan berikut yang dilakukan:

a. Auditor memberitahu VIDA tentang catatan ketidaksesuaian;
b. Pihak yang bertanggung jawab di dalam VIDA untuk memperbaiki ketidaksesuaian akan menentukan pemberitahuan atau tindakan lebih lanjut terkait perbaikan atau tanggapan apa yang perlu dilakukan sesuai dengan persyaratan CPS dan kontrak yang sesuai, kemudian melaksanakan tindakan perbaikan tersebut tanpa penundaan.
c. Audit kepatuhan yang dilaksanakan oleh auditor yang ditunjuk oleh PSrE Induk, maka hasil pelaksanaan audit dilaporkan oleh auditor kepada PSrE Induk.

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

a. The auditor notifies VIDA of the discrepancy notes;
b. The party within VIDA who is responsible for correcting the discrepancy will determine what further notifications or further corrective actions or response necessary pursuant to the requirements of this CPS and the respective contracts, and then proceed to make such notifications and take such corrective actions without delay.
c. Compliance audit that is carried out by auditors appointed by the Root CA Indonesia, the results of the audit are reported by the auditor to the Root CA Indonesia.

8.6. Laporan Hasil Penilaian / Communication of Audit Results

Laporan Penilaian Kelaikan, termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil, harus diberikan kepada PA sebagaimana diatur pada bagian 8.1. Selain itu, hasilnya harus dikomunikasikan seperti yang diatur pada bagian 8.5 di atas.

A Compliance Audit Report, including identification of corrective measures taken or being taken, shall be provided to the PA as set forth in section 8.1. Additionally, the results shall be communicated as set forth in 8.5 above.

8.7. Audit Internal / Internal Audit

VIDA memantau kepatuhan terhadap CP induk, CPS ini, dan ketentuan peraturan perundang-undangan dan secara ketat mengontrol kualitas layanannya dengan melakukan audit internal minimal 1 (satu) kali dalam setahun terhadap sistem operasional PSrE agar dapat meminimalkan risiko gangguan pada proses bisnis maupun layanan VIDA.

VIDA reviews its compliance against Root CA Indonesia's CP, this CPS, law and regulation requirements and strictly controls the quality of its service by performing internal audits at least once a year against CA operational systems so that it can minimise the risk of disruptions to business processes and VIDA CA services.

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

9.1. Biaya / Fees

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

VIDA dapat mengenakan biaya layanan dalam menyelenggarakan siklus hidup sertifikat misalnya dalam proses penerbitan, pembaruan, dan *re-key* Sertifikat. Dalam hal ini, ketentuan terkait biaya akan disampaikan secara jelas kepada pelanggan pada saat pengajuan pemanfaatan layanan yang memanfaatkan sertifikat elektronik dengan tunduk pada ketentuan dalam perjanjian pelanggan (*subscriber agreement*).	VIDA may charge service fees for commencing Certificate lifecycle processes such as issuance, renewal and re-key. In this case, the provisions related to fees will be clearly conveyed to the customer at the time the subscriber applies for consuming service that Certificates provided by VIDA and aligned with provisions stipulated in the subscriber agreement.

9.1.2. Biaya Pengaksesan Sertifikat / Certificate Access Fees

VIDA dapat mengenakan biaya layanan dalam memberikan akses terhadap Sertifikat Elektronik serta pemanfaatan layanan berbasis sertifikat elektronik lainnya yang disediakan oleh VIDA kepada pelanggan/Pemilik termasuk namun tidak terbatas pada tanda tangan elektronik tersertifikasi, segel elektronik, dan lainnya.	VIDA may charge service fee for providing access to Certificate or providing service that utilizes Certificate provided by VIDA to the customer/Subscriber including but not limited to digital signature, e-seal, and others.

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

VIDA tidak mengenakan biaya tambahan untuk pencabutan ataupun pengecekan status keabsahan Sertifikat menggunakan CRL maupun OCSP.	VIDA will not charge a fee for a certificate revocation or for checking the validity status of an issued certificate using a CRL or OCSP.

9.1.4. Biaya Layanan Lainnya / Fees for Other Services

VIDA dapat mengenakan biaya lain yang seperti biaya pemasangan, dukungan purna jual, dan sebagainya.	VIDA may charge a fee for other services such as installation, after sales support, etc..

9.1.5. Kebijakan Pengembalian Biaya/ Refund Policy

VIDA akan bertanggung jawab atas kegagalan pemanfaatan layanan berbasis sertifikat elektronik yang sudah dibayar oleh pelanggan atau Pemilik. Ketentuan pengembalian dana akan tunduk pada tanggung jawab kontraktual dengan pelanggan (apabila ada) dan selaras dengan ketentuan kewajiban dan hak dari Pemilik serta batasan pertanggungjawaban VIDA sebagaimana diatur dalam dokumen *subscriber agreement* dan *warranty policy*.

VIDA will be responsible for any failure in consuming services which utilizes Certificates usage that have been paid for by customer or Subscriber. Refund provisions will be subject to contractual obligation with the customer (if applicable) and align with the provisions of the obligations and rights of the Subscriber as well as the limitations of VIDA's CA liability as stipulated in the subscriber agreement and warranty policy document.

9.2. Tanggung Jawab Keuangan / Financial Responsibility

9.2.1. Cakupan Asuransi / Insurance Coverage

VIDA memiliki asuransi dengan cakupan risiko keamanan siber dan internet (*cyber liability and internet risk*). Melalui asuransi ini, VIDA terlindungi secara finansial apabila terdapat kesalahan maupun serangan siber, yang berakibat pada terganggunya operasional maupun teknologi yang berjalan VIDA.

VIDA has insurance with coverage for cyber and internet security risks (cyber liability and internet risk). Through this insurance, VIDA is financially protected if there is an inadvertent or cyber attack, which results in disrupting VIDA CA's operations and technology.

9.2.2. Aset Lainnya / Other Assets

VIDA mempertahankan kemampuan keuangan yang wajar untuk menjalankan operasional PSrE dan memenuhi kewajiban. VIDA memastikan bahwa seluruh aset yang dibutuhkan untuk menjalankan operasi PSrE dapat terpenuhi, diantaranya perangkat keras, perangkat lunak, ruang kantor yang memadai, serta aset sumber daya manusia yang mumpuni.

VIDA maintains reasonable and sufficient financial resources to maintain CA operations and fulfill its duties. VIDA ensures that all assets needed to carry out CA operations can be met, including hardware , software, adequate office space, as well as qualified human resource assets.

9.2.3. Kebijakan Jaminan berupa Asuransi / Insurance or Warranty Coverage for End-Entities

Merujuk pada bagian 9.2.1, VIDA telah memiliki asuransi yang mencakup perlindungan terhadap risiko siber dan/atau internet. Apabila di kemudian hari VIDA mengalami kegagalan akibat gangguan siber sehingga berdampak kepada ketidaktersediaan layanan bagi pelanggan/Pemilik, maka dengan tunduk pada ketentuan klaim asuransi, asuransi tersebut dapat memberikan perbaikan atas situasi yang dialami VIDA dan pertanggungjawaban VIDA kepada pelanggan/Pemilik akan dilakukan sesuai kondisi yang terjadi dengan tetap selaras dengan dokumen *subscriber agreement* dan *warranty policy*.

Referring to section 9.2.1, VIDA has insurance which includes protection against cyber and/or internet risks. If in the future, VIDA CA experiences failure due to cyber interference which resulting to the unavailability of services for customers/Subscriber, subject to the provisions of the insurance claim, the insurance can provide improvements to the situation experienced by VIDA and VIDA's liability fulfilment to the customer/Subscriber will be carried out in accordance with the provisions in subscriber agreement and warranty policy document.

9.3. Kerahasiaan Informasi Bisnis / Confidentiality of Business Information

9.3.1. Cakupan Informasi Rahasia / Scope of Confidential Information

VIDA berhati-hati dalam menangani informasi yang bersifat rahasia termasuk kondisi yang mengharuskan pengungkapan dan bagaimana pengungkapan harus dilaksanakan agar keamanan tetap terjaga. Sehubungan dengan penyelenggaraan PSrE, yang termasuk dalam kategori informasi rahasia antara lain:

a. Informasi pribadi sebagaimana dijabarkan pada Bagian 9.4;
b. Rekam jejak audit (*audit logs*) dari sistem PSrE dan RA milik VIDA;
c. Data aktivasi pada saat pengaktifan Kunci Privat VIDA sebagaimana dijabarkan pada Bagian 6.4;
d. Kunci Privat Pemilik Sertifikat yang disimpan oleh VIDA, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemilik Sertifikat;
e. Catatan permohonan Sertifikat;
f. Hasil penilaian risiko dan hasil penilaian kerentanan;

VIDA is being careful in handling confidential information including conditions requiring disclosure and how disclosure must be carried out in order to maintain security. In relation with the implementation of CA governance, the following items are classified as confidential information:

a. Personal Information as per detailed in Section 9.4;
b. Audit logs from CA and RA systems owned by VIDA;
c. Activation data used to active VIDA Private Keys as detailed in Section 6.4;
d. Subscriber Private Key held by VIDA and all information that Subscriber need for Private Key usage;
e. Certificate application notes;
f. Risk assessment result and vulnerability assessment result;

g. Dokumentasi bisnis proses VIDA termasuk dokumen Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); dan
h. Laporan audit dari auditor eksternal maupun internal sebagaimana dijabarkan pada bagian 8.

VIDA dapat memberikan label kategori rahasia kepada informasi lainnya di luar hal-hal yang disebutkan pada bagian ini seperti untuk informasi bisnis dan sebagainya. Informasi lain yang diberi label sebagai informasi terbatas, rahasia, atau internal, atau menurut sifatnya harus dipahami secara wajar sebagai rahasia, dikelola oleh VIDA dengan memperhatikan keamanan dan dengan penuh kehati-hatian. VIDA memiliki kewenangan dalam menentukan dan menjalankan pengungkapan informasi rahasia sesuai keperluan penyelenggaraan operasional PSrE serta tunduk pada pengungkapan kepada pihak yang berwenang sesuai dengan bagian 9.4.6.

g. VIDA business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and
h. Audit reports from external or internal auditor as per detailed in section 8.

VIDA may assign confidentiality labels to other information outside of the things mentioned in this section such as for business information and so on. Those information that is labeled as restricted, confidential, or internal, or by its nature should be reasonably understood to be confidential, is managed by VIDA with the managed by VIDA with attention to security and with the utmost care.
VIDA has the authority to determine and carry out disclosure of confidential information according to the needs of implementing CA operation and is subject to information disclosure to authorized parties in accordance with section 9.4.6.

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

Informasi yang diberi label sebagai informasi publik serta informasi yang dipublikasikan di repositori VIDA sesuai bagian 2 termasuk ke dalam kategori bukan informasi rahasia. Sertifikat beserta informasi yang dimuat di dalamnya, informasi mengenai status Sertifikat yang terdapat pada CRL maupun respon OCSP, adalah termasuk kategori informasi publik.

Any information that is labelled as public information and information that is published in VIDA repository shall be deemed as not confidential. Certificates including the information inside, information about status of the certificates that can be found in CRL and OCSP response are deemed public.

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

VIDA 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; dan

VIDA will protect 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; and

c. NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

Penyimpan informasi rahasia baik dalam bentuk fisik maupun elektronik dilakukan dengan memperhatikan penanganan informasi tersebut. Misalnya, informasi yang disimpan dalam bentuk terenkripsi tetap terjaga enkripsinya apabila dicadangkan atau dipindahkan ke media lain.

c. NDA with employees, outsourcers and contractors.

Storing confidential information, whether in physical or electronic form, is carried out by careful attention to how the information is handled. For example, information stored in encrypted form is maintained when being backed up or being transferred to other media.

9.4. Kerahasiaan Informasi Pribadi / Privacy of Personal Information

9.4.1. Rencana Privasi / Privacy Plan

VIDA melindungi informasi pribadi sesuai dengan Kebijakan Privasi yang dipublikasikan pada *website* VIDA, https://www.repo.vida.id. Cakupan pada Kebijakan Privasi tersebut selaras dengan ketentuan peraturan perundangan-undangan Indonesia mengenai pelindungan data pribadi dan informasi dan transaksi elektronik.

VIDA protects personal information in accordance with a Privacy Policy published on VIDA's website at https:/www.repo.vida.id The Privacy Policy coverage is aligned with the provisions of Indonesian laws and regulations regarding the protection of personal data and information and electronic transactions.

9.4.2. Informasi yang Dianggap Privat / Information Treated as Private

Sehubungan dengan penyelenggaraan PSrE, yang termasuk dalam kategori informasi pribadi antara lain data Pemilik yang dikumpulkan saat proses pendaftaran sesuai bagian 3.2.3. VIDA melindungi semua informasi identitas pribadi Pemilik dari pengungkapan yang tidak sah. Catatan transaksi yang dapat mengandung informasi pribadi Pemilik dapat diungkapkan atas permintaan/ persetujuan Pemilik kepada pihak lain seperti RA atau Pengandal. Selain itu, pengungkapan dapat dilakukan atas kewenangan VIDA sebagai PSrE untuk keperluan penyelenggaraan PSrE sesuai bagian 9.4.1, misalnya kepada instansi yang mengelola data kependudukan. Pengungkapan informasi pribadi kepada pihak berwenang lainnya mengacu pada bagian 9.4.6.

In relation with the implementation of CA governance, what is included as the personal information category includes Subscriber data collected during the registration process in accordance with section 3.2.3. VIDA will protect all Subscribers personally identifiable information from unauthorized disclosure. Records of transactions that may contain the Subscriber's personal information may be disclosed upon the Subscriber's request/approval to other parties such as RA or Relying Party. In addition, disclosures can be made based on the authority possessed by VIDA as CA for the purposes of governing CA operation in accordance with section 9.4.1, for example to institution who manages population data. Disclosure of personal information to other authorized parties refers to section 9.4.6.

9.4.3. Informasi tidak Dianggap Privat / Information not Deemed Private

Informasi pribadi yang tercantum pada detil Sertifikat tidak termasuk pada informasi pribadi yang diatur di bagian 9.4.2.

Personal information listed in the Certificate detail is not deemed as personal information outlined in section 9.4.2.

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

VIDA bertanggung jawab untuk menyimpan secara aman informasi pribadi baik dalam bentuk fisik maupun elektronik dan mengelolanya secara aman sesuai dengan Kebijakan Privasi.

VIDA is responsible for securely storing personal information in either physical or electronic form and securely governing it in accordance with a published Privacy Policy document.

9.4.5. Pemberitahuan dan Persetujuan untuk menggunakan Informasi Pribadi / Notice and Consent to use Private Information

VIDA dengan cara yang wajar memberitahukan tentang ketentuan pemrosesan informasi pribadi serta meminta persetujuan dari Pemohon atau Pemilik untuk penggunaan informasi pribadi miliknya. Informasi pribadi diproses lebih lanjut apabila Pemohon atau Pemilik memberikan persetujuan terhadap pemrosesan informasi pribadi tersebut. Ketentuan terkait penggunaan informasi pribadi terdapat dalam Perjanjian Kepemilikan termasuk mencakup persetujuan penggunaan informasi lain yang diperoleh dari pihak ketiga yang digunakan dalam proses validasi pada produk atau layanan yang disediakan oleh VIDA.

VIDA in a reasonable way informs about the provisions of personal information processing and asks for consent from the Applicant or Subscriber for the use of his personal information. Personal information is processed if the Applicant or Subscriber gives consent to the processing of the personal information.VIDA incorporates the relevant provisions within 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 VIDA.

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

VIDA tidak mengungkapkan informasi pribadi kepada pihak ketiga manapun kecuali sesuai dengan kewenangan yang dimiliki oleh VIDA sebagai PSrE, diwajibkan oleh hukum, aturan

VIDA will not disclose personal information to any third party unless authorized by this policy, required by law, government rule or

dan peraturan pemerintah, atau perintah pengadilan.
Ketentuan pengungkapan informasi pribadi, termasuk kepada lembaga pemerintahan atau atas perintah pengadilan, akan tunduk pada ketentuan peraturan perundang-undangan yang berlaku, diantaranya Undang-undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.

regulation, or order of a court of competent jurisdiction.
Provisions for disclosing personal information, including to government agencies or upon court orders, will be subject to the provisions of applicable laws and regulations, including Law no. 27 of 2022 concerning Personal Data Protection.

9.4.7. Keadaan Pengungkapan Informasi Lainnya / Other Information Disclosure Circumstances

Tidak ditentukan.

No stipulation.

9.5. Hak atas Kekayaan Intelektual / Intellectual Property Rights

Semua hak kekayaan intelektual VIDA termasuk semua merek dagang dan hak cipta dari semua dokumen tetap menjadi milik tunggal dari VIDA.
VIDA tidak akan dengan sengaja melanggar hak kekayaan intelektual seperti hak cipta, paten, merek dagang, atau rahasia dagang pihak ketiga. Selain itu, VIDA mematuhi pembatasan hukum pada penggunaan materi sehubungan dengan hak kekayaan intelektual, dan penggunaan produk perangkat lunak berbayar.

VIDA's Intellectual Property Rights including trademarks, copyright and all documents remain as sole property of VIDA.

VIDA will not knowingly infringe any intellectual property rights such as copyright, third party patents, trademarks or trade secrets. In addition, VIDA complies with legal restrictions on the use of the material in connection with intellectual property rights, and use of paid software products.

9.6. Pernyataan dan Jaminan / Representations and Warranties

9.6.1. Pernyataan dan Jaminan PSrE / CA Representations and Warranties

VIDA menyatakan dan menjamin, sejauh yang ditentukan dalam CPS ini, bahwa:

a. VIDA mematuhi ketentuan yang diatur dalam CPS ini;
b. VIDA menerbitkan dan memperbarui CRL secara berkala;
c. Seluruh Sertifikat yang diterbitkan akan memenuhi syarat yang diatur

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

a. VIDA complies, in all material aspects, with the CPS;
b. VIDA publishes and updates CRL on a regular basis;
c. All certificates issued will meet the minimum requirements in accordance

berdasarkan CPS ini dan hanya informasi yang dapat diverifikasi yang ditampilkan pada Sertifikat;

d. VIDA menampilkan informasi yang dapat diakses secara publik melalui repositorinya;
e. Kunci Privat PSrE milik VIDA terlindungi dan tidak dapat diakses oleh pihak yang tidak berwenang;
f. Semua pernyataan yang dibuat oleh VIDA dalam semua perjanjian yang diterapkan adalah benar dan akurat, sejauh yang diketahui oleh VIDA; dan
g. Setiap Pemilik telah diwajibkan untuk menyatakan dan menjamin bahwa semua informasi yang disediakan oleh Pemilik yang terkait dengan atau yang dimuat dalam Sertifikat adalah benar.

with this CPS and only verified information that are shown in the Certificate;

d. VIDA publishes information that can be accessed publicly through its repositories;
e. VIDA's CA Private Key is protected and can not be accessed by unauthorized party;
f. All representations made by VIDA in any applicable agreements are true and accurate, to the best knowledge of the CA; and
g. Each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, or contained in the Certificate is true.

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 CPS ini dan perjanjian yang disetujui lainnya.
d. RA menginformasikan kepada Pemilik mengenai kewajiban Pemilik selaras dengan bagian 9.6.3 berikut juga konsekuensi dari ketidakpatuhan terhadap kewajiban tersebut.

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. all registration activities that have been done by RAs comply with this CPS and other agreed agreements.
d. RA informs the Subscriber regarding the Subscriber's obligations aligned with section 9.6.3 as well as the consequences of non-compliance with these obligations.

9.6.3. Pernyataan dan Jaminan Pemilik Sertifikat / Subscriber Representations and Warranties

Pemilik dan/atau Pemohon harus menyetujui dokumen *Subscriber Agreement* yang berisi persyaratan yang harus dipenuhi Pemilik terkait perlindungan Kunci Privat dan penggunaan Sertifikat, sebelum Sertifikatnya diterbitkan.

Pemilik Sertifikat menjamin bahwa:

a. Setiap Sertifikat 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 kedaluwarsa dan telah dicabut) saat tanda tangan digital dibuat;
b. Setiap Kunci Privat harus diamankan dan hanya Pemilik Sertifikat yang memiliki akses terhadap Kunci Privat tersebut;
c. Sudah melakukan peninjauan terhadap informasi dari Sertifikat;
d. Semua informasi yang diberikan oleh Pemilik dan informasi yang berada di dalam Sertifikat adalah benar;
e. Sertifikat digunakan hanya untuk tujuan yang legal dan diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini;
f. segera:
   (i) melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat dan Kunci Privat yang terasosiasi, jika terdapat kecurigaan penyalahgunaan atau kebocoran dari Kunci Privat Pemilik yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat;
   (ii) 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;
   (iii) menghentikan penggunaan Kunci Privat yang Kunci Publiknya tercantum dalam Sertifikat setelah Sertifikat dicabut;

Subscribers and/or Applicants are required to approve the Subscriber Agreement document containing the requirements the Subscriber shall meet regarding protection of the Private Key and use of the Certificate before the Certificate is issued.

Subscribers warrant that:

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. Private Key is protected and that no unauthorized person has ever had access to the Subscriber's Private Key;
c. Have thoroughly reviewed the certificate information;
d. All information supplied by the Subscriber and information 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 :
   (i) request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
   (ii) request revocation of the certificate, and cease using it, if any information in the certificate is or becomes incorrect or inaccurate;
   (iii) stop using the Private Key whose Public Key is listed in a certificate after the certificate is revoked;

g. Akan menanggapi instruksi VIDA terkait *compromise* atau penyalahgunaan Sertifikat dalam kurun waktu 48 (empat puluh delapan) jam;
h. menyetujui dan menerima bahwa VIDA diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemilik melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Kepemilikan atau jika VIDA menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising*, penipuan, atau pendistribusian *malware;* dan
i. Pemilik merupakan pengguna akhir dan bukan merupakan PSrE lain.

g. Will respond to VIDA instructions regarding compromise or certificates misuses within 48 (forty eight) hours;
h. Acknowledges and accepts that VIDA is entitled to revoke the certificate immediately if the Subscriber violates the terms of the Subscriber Agreement or if VIDA 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 another CA.

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 VIDA, 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 VIDA, jika Pengandal menyadari atau mencurigai bahwa telah terjadi *compromise* pada Kunci Privat;
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;

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 VIDA, 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 VIDA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised;
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. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

e. must comply with the provisions of this CPS and related agreements.

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

Tidak ditentukan.

No stipulation.

9.7. Pelepasan Jaminan / Disclaimers of Warranties

VIDA membuat pernyataan dalam CPS bahwa VIDA tidak menjamin:

a. Kecuali untuk jaminan yang telah tercantum dalam CPS dan kontrak perjanjian dan sepanjang diizinkan oleh hukum, VIDA 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;

c. Keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam demo atau pengujian Sertifikat.

VIDA makes statements in their CPS that VIDA does not warrant:

a. Except for the warranties stated herein including related agreements and to the extent permitted by applicable law, VIDA 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

Keseluruhan tanggung jawab yang dibebankan kepada VIDA diatur dalam kebijakan jaminan, CPS VIDA, dan mengacu kepada ketentuan peraturan perundang-undangan.

The total liability of VIDA is regulated in accordance with warranty policy, VIDA's CPS, and government laws and regulations.

9.8.1. Pembatasan Tanggung Jawab PSrE / CA Limitations of Liability

VIDA tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat, termasuk:

a. semua kerusakan yang dihasilkan dari penggunaan Sertifikat atau pasangan kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Kepemilikan, atau yang diatur dalam Sertifikat itu sendiri;

b. semua kerusakan yang disebabkan oleh keadaan kahar;

c. semua kerusakan yang disebabkan oleh *malware* (seperti virus atau trojans) di luar perangkat VIDA.

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

a. all damage caused by the misuse of certificates or key pairs beside the proper use that have been defined in CPS, Subscriber Agreement, or all provision which have been mentioned in the certificate;

b. all damage caused by the force majeure condition;

c. all damage caused by the malware (i.e virus or trojan) outside VIDA devices.

9.8.2. Pembatasan Tanggung Jawab RA / RA Limitation of Liability

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan VIDA. Secara khusus, RA bertanggung jawab atas pendaftaran Pemilik.

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

9.8.3. Pembatasan Tanggung Jawab Pemilik / Subscriber Limitation of Liability

Pembatasan tanggung jawab Pemilik ditentukan dalam dokumen *Subscriber Agreement*. Secara khusus, Pemilik bertanggung jawab atas kerugian akibat kelalaian atau kesengajaan yang menyebabkan pelanggaran, seperti memindahtangankan token dan PIN kepada orang lain.

The cap on Subscriber's liability is specified in the Subscriber Agreement. In particular, the Subscriber is responsible for losses due to negligence or intentional causes of violations, such as transferring tokens and PINs to other people.

9.9. Ganti Rugi / Indemnities

9.9.1. Ganti Rugi oleh PSrE / Indemnification by CA

Kewajiban ganti rugi VIDA ditetapkan Perjanjian Kepemilikan, kebijakan terkait garansi, Perjanjian Pengandal atau perjanjian lainnya yang mengatur mengenai hal tersebut termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat. Kewajiban ganti rugi sesuai dengan ketentuan peraturan perundang-undangan.

VIDA's indemnification obligations will be set forth in its CPS, Subscriber Agreement, policy related with warranty, Relying Party Agreement or other agreement defining for such warranties including any obligation to third party beneficiaries. The indemnities obligations shall conform to the applicable laws and regulations.

9.9.2. Ganti Rugi oleh Pemilik / Indemnification by Subscriber

VIDA menyertakan persyaratan ganti rugi oleh Pemilik maupun untuk Pemilik Sertifikat dalam Perjanjian Kepemilikan.

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

a. pelanggaran yang dilakukan oleh Pemilik terhadap perjanjian kepemilikan, CPS ini, kewajiban kontraktual, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
b. Penggunaan Kunci Privat yang tidak sah karena kelalaian Pemilik;
c. Penggunaan Sertifikat oleh Pemilik di luar penggunaan yang ditentukan oleh CPS ini termasuk apabila untuk melakukan perbuatan melawan hukum;
d. Pemberian informasi yang keliru oleh Pemilik pada saat permohonan pemrosesan Sertifikat atau kegagalan Pemilik dalam mengungkapkan kebenaran dengan maksud untuk menipu pihak manapun;
e. Kegagalan Pemilik untuk melindungi Kunci Privat, menggunakan sistem

VIDA includes its indemnification requirements from or for Subscribers in the Subscriber Agreements.

To the extent permitted by applicable law, Subscriber agrees to indemnify and hold VIDA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that may incur as a result of:

a. violations committed by the Subscriber against the subscriber agreement, this CPS, contractual obligation, or applicable law, whether done intentionally or unintentionally;
b. Fraudulent or unauthorized use of Subscriber's Private Key due to the Subscriber's negligence;
c. Use of the Certificates by Subscribers beyond the prescribed use defined by this CPS including if committing to unlawful acts;
d. Falsehood or providing false information by the Subscriber during Certificate processing request including failure to disclose fact with intent to deceive any any party;
e. The Subscriber's failure to protect the Subscriber's Private Key, to use a

elektronik yang terpercaya, atau mengambil langkah-langkah yang wajar untuk mencegah kebocoran, kehilangan, pengungkapan, perubahan, atau penggunaan tidak sah Kunci Privat; atau

f. Penggunaan nama oleh Pemilik (termasuk namun tidak terbatas pada common name, nama domain, atau alamat email) yang melanggar Hak Kekayaan Intelektual dari pihak ketiga.

trustworthy system, or to otherwise failure in taking the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's Private Key; or

f. The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

9.9.3. Ganti Rugi oleh Pengandal / Indemnification by Relying Parties

VIDA menyertakan persyaratan ganti rugi oleh maupun untuk Pengandal dalam Perjanjian Pengandal.
Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan VIDA dari tindakan atau kelalaian apa pun yang mengakibatkan kewajiban, kerugian, kerusakan, biaya dan segala tuntutan yang diakibatkan oleh:

a. Pengandal tidak melakukan kewajibannya sebagaimana diatur pada Perjanjian Pengandal, CPS ini, atau hukum yang berlaku;

b. Pengandal tidak memeriksa status Sertifikat untuk menentukan apakah Sertifikat tersebut sudah kedaluwarsa atau sudah dicabut.

VIDA will include its indemnification requirements from or for Relying Parties in its Relying Party Agreement.
To the extent permitted by applicable law, and any applicable contractual agreements, Relying Party agrees to indemnify and hold VIDA harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees that may incur as a result of:

a. The Relying Party's failure to perform the obligations of a Relying Party as per Relying Party agreement, this CPS, or applicable laws and regulations;,

b. The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10. Jangka Waktu dan Pengakhiran / Term and Termination

9.10.1. Jangka Waktu / Term

CPS ini dinyatakan berlaku sampai ada pemberitahuan lebih lanjut oleh VIDA atau perubahan yang dipublikasikan melalui laman atau repositorinya.

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

9.10.2. Pengakhiran / Termination

Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan berlaku efektif 30 (tiga puluh) hari kalender setelah dipublikasikan kecuali ditentukan secara khusus.

Pengakhiran terhadap CPS akan dikomunikasikan lebih lanjut oleh VIDA melalui laman atau repositorinya.

OID dalam CPS VIDA dapat tetap berlaku paling lama 12 (dua belas) bulan atau lebih cepat setelah menyesuaikan dengan ketentuan CP PSrE Induk, Hierarki OID untuk IKP Indonesia, dan/atau dokumen kebijakan terkini lainnya.

Notified changes of this CPS are appropriately marked by an version numbering. Following publications, changes become applicable 30 (thirty) calendar days thereafter unless specifically defined. The termination of the CPS will be further communicated by VIDA through its website or repository.

The OID in the VIDA's CPS can remain valid for a maximum of 12 (twelve) months or sooner after conforming to the provisions of the Root CA Indonesia's CP, the OID Hierarchy for Indonesian IKP, and/or other current policy documents.

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

VIDA mengkomunikasikan kondisi, dampak dari pengakhiran CPS, dan juga kondisi keberlangsungan dari Sertifikat yang masih berlaku melalui laman atau repositorinya. Meski CPS sudah tidak berlaku lagi, aturan terkait pelindungan data dan arsip informasi tetap dipatuhi.

VIDA will communicate the conditions and effect of this CPS termination and continuity of the issued certificate on its website or repository. If CPS may no longer be valid, the regulations pertaining to the laws on data protection and on archival of information are still prevailed.

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

VIDA menyediakan media komunikasi bagi para pihak terkait melalui publikasi pada laman, telepon, *email*, dan dokumen baik dalam bentuk elektronik maupun kertas. VIDA harus memberi tanggapan paling lama 20 (dua puluh) hari kerja melalui media komunikasi yang sama. Komunikasi yang dibuat ke VIDA harus dialamatkan sesuai dengan yang tercantum pada bagian 1.5.2 pada CPS.

VIDA provides communication media for related parties through publication in websites, telephone, email, and documents both in digital or in paper form. VIDA must respond for a maximum of 20 (twenty) working days through the same communication media. Communications made to VIDA must be addressed in accordance with those listed in section 1.5.2 of CPS.

9.12. Perubahan atau Amandemen / Amendments

9.12.1. Prosedur untuk Perubahan atau Amandemen / Procedure for Amendment

CPS ini dapat diubah sewaktu-waktu sesuai kebutuhan dan akan berlaku sampai digantikan oleh versi CPS yang lebih baru atau apabila dinyatakan tidak berlaku oleh *Policy Authority* VIDA. Perubahan CPS dilakukan mengikuti prosedur persetujuan CPS sesuai dengan bagian 1.5.4.

This CPS can be changed at any time as needed and will be valid until replaced by a newer version of the CPS or if declared invalid by VIDA Policy Authority. CPS change are carried out by following the CPS approval procedure in accordance with section 1.5.4.

9.12.2. Periode dan Mekanisme Pemberitahuan / Notification Mechanism and Period

VIDA menerbitkan pemberitahuan pada laman terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku sesuai dengan bagian 2.3.

VIDA will post appropriate notice on the websites of any major or significant changes to this CPS as well as the effective date according to section 2.3.

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

Jika Policy Authority memiliki pandangan diperlukannya perubahan nomor-nomor OID yang terlibat, VIDA akan melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru. Apabila perlu, VIDA dapat menginformasikan perubahan OID kepada PSrE Induk sebelum melakukan penambahan atau perubahan OID tersebut. Daftar OID terdapat di bagian 1.2.

In case the PA has the view that it is necessary to change the involved OID numbers, VIDA will change the OID and enforce the new policy using the new OID. Whenever necessary, VIDA may inform the OID change to Root CA Indonesia before making additions or changes to the OID. The list of OIDs is available in section 1.2.

9.13. Ketentuan Penyelesaian Sengketa / Dispute Resolution Provisions

Jika ada perselisihan sehubungan dengan kinerja, eksekusi, atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara VIDA dan Partisipan.

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

9.14. Hukum yang Mengatur / Governing Law

CPS ini menerapkan aturan hukum di Indonesia untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat VIDA ataupun produk dan layanan lainnya.

Hukum Indonesia juga tetap berlaku dalam hal Sertifikat VIDA dipakai atau dirujuk baik secara eksplisit atau implisit untuk kebutuhan komersil atau kontraktual di negara lain terkait dengan produk atau layanan dari VIDA ini.

Para pihak, termasuk rekan VIDA, Pemilik, Pengandal, tunduk pada acuan hukum yang telah ditentukan di atas.

This CPS is governed, construed and interpreted in accordance with the laws of Indonesia to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of VIDA's certificates or other products and services.

The laws of Indonesia also apply to all VIDA's commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to VIDA's products and services.

Each party, including VIDA'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

VIDA mematuhi hukum yang berlaku di Indonesia terkait Penyelenggaraan Sertifikasi Elektronik. Kepatuhan mencakup, namun tidak terbatas pada, pengadaan perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.

VIDA complies with applicable laws in Indonesia regarding the Implementation of Electronic Certification. Compliance includes, but is not limited to, procurement of hardware, software, systems, business information, data processes, and all day-to-day activities related to operating business practices.

9.16. Ketentuan yang belum diatur / Miscellaneous Provisions

9.16.1. Seluruh Perjanjian / Entire Agreement

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

VIDA contractually obligates every RA involved with Certificate issuance to comply with this CP and all related guidelines.

9.16.2. Pengalihan Hak / Assignment

Partisipan yang beroperasi di bawah CPS ini sesuai bagian 1.3 tidak boleh mengalihkan hak atau kewajibannya tanpa persetujuan tertulis dari VIDA. Ketentuan pengalihan hak harus sesuai dengan ketentuan peraturan perundang-undangan atau pengumuman yang berkaitan dengan PSrE.

Any participants operating under this CPS in accordance with Section 1.3 must not assign their rights or obligations without the prior consent of VIDA. Requirements of the assignment must be in accordance with laws, regulations, or announcements relating to CA.

9.16.3. Keterpisahan / Severability

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

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such a 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 Pelepasan Hak) / Enforcement (Attorneys' Fees and Waiver of Rights)

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

VIDA may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. VIDA's failure to enforce a provision of this CPS does not waive VIDA's right to enforce the same provisions later or right to enforce any other provisions of this CPS. To be effective any waivers must be in writing and signed by VIDA.

9.16.5. Keadaan Kahar / Force Majeure

VIDA tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada di luar kendali yang wajar (keadaan kahar), termasuk tapi tidak terbatas pada tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, pemadaman listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintah atau setiap kejadian atau situasi yang tidak terduga.	VIDA shall not be liable for any failure or delay in its performance under this CPS due to causes that are beyond its reasonable control (*force majeure)*, including, but not limited to act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, power failure and failure of telecommunications lines, lack of Internet access, sabotage, terrorism, and governmental action or any unforeseeable events or situations.
VIDA menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas PSrE.	VIDA will be obliged to provide BCP and DRP with reasonable control in line with the capabilities of the CA.

9.17. Ketentuan Lain / Other Provisions

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

APPENDIX A / LAMPIRAN A

Tabel Akronim dan Definisi / Table of Acronyms and Definition

Akronim/Acronym	**Definition / Definisi**
BCP	Business Continuity Plan
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DRP	Disaster Recovery Plan
FIPS	Federal Information Processing Standards (US Government)
IKP PKI	Infrastruktur Kunci Publik Public Key Infrastructure
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PSrE CA	Penyelenggara Sertifikasi Elektronik Certification Authority
RA	Registration Authority
RFC	Request For Comment Request
VA	Validation Authority

Term / Istilah	**Definition / Definisi**
Pemohon Applicant	Individu atau Badan Hukum yang mengajukan permohonan pembuatan (atau pembaruan) Sertifikat. Setelah Sertifikat diterbitkan, Pemohon disebut sebagai Pemilik. The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the certificate issued, the Applicant is referred to as the Subscriber.

Pemilik Subscriber	Individu yang merupakan subjek dari Sertifikat, telah diterbitkan Sertifikatnya. A person who is the Subject of, and has been issued, a certificate.
Sertifikat Digital Certificate	Sertifikat adalah Sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik. Certificate is a digital certificate that contains digital signatures and identities that show the legal status of the related parties in electronic transactions.
Sertifikat VIDA VIDA Certificate	Sertifikat yang ditandatangani sendiri yang dikeluarkan oleh VIDA untuk mengidentifikasi dirinya sendiri dan untuk memfasilitasi verifikasi Sertifikat yang diterbitkan oleh VIDA. The self-signed Certificate issued by VIDA to identify itself and to facilitate verification of Certificates issued to itself.
Sertifikat Pemilik Subscriber's Certificate	Sertifikat yang dikeluarkan oleh VIDA The certificate issued by VIDA
Certificate Policies	Seperangkat aturan yang menerangkan penerapan sebuah Sertifikat dalam implementasi IKP dengan persyaratan keamanan yang umum. A set of rules that indicates the applicability of a named certificate to a PKI implementation with common security requirements.
Certification Practice Statement	Satu dari beberapa dokumen yang membentuk kerangka kerja pengaturan pembuatan, penerbitan, pengelolaan dan penggunaan Sertifikat. One of several documents forming the governance framework in which certificates are created, issued, managed, and used.
Certificate Revocation List	Daftar terkini dari Sertifikat yang dicabut yang dibuat dan ditandatangani secara digital oleh VIDA yang menerbitkan Sertifikat. A regularly updated timestamped list of revoked certificates that is created and digitally signed by VIDA that issued the certificates.

Certificate Signing Request (CSR)	Sebuah pesan yang menyampaikan permintaan untuk penerbitan Sertifikat. A message conveying a request to have a certificate issued.
Permintaan Pemrosesan Sertifikat Certificate Processing Request/ Certificate Application	Permohonan yang diterima oleh VIDA terkait penerbitan, pembaruan, *re-key,* atau pencabutan suatu Sertifikat Request which come to VIDA to issue, renew, re-key, or revoke a certificate
Kompromi Compromise	Pelanggaran terhadap kebijakan keamanan yang menyebabkan hilangnya kontrol atas informasi sensitif A violation of a security policy that results in loss of control over sensitive information.
Extended Validation Certificate	Sertifikat yang berisi informasi yang ditentukan dalam Pedoman EV dan yang telah divalidasi sesuai dengan pedoman tersebut. A certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the guidelines.
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.
Key Generation Ceremony	Sebuah prosedur di mana pasangan kunci dari PSrE atau RA dihasilkan, kunci privatnya ditransfer ke modul kriptografi lalu dicadangkan, dan/atau Kunci Publiknya disertifikasi. A procedure whereby a CA's or RA's key pair is generated, its Private Key is transferred into a cryptographic module and then backed up, and/or its Public Key is certified.
Object Identifier	Sebuah *unique alphanumeric atau numeric identifier* yang terdaftar di bawah 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	Protokol pemeriksaan Sertifikat secara online bagi Pengandal yang berisi informasi mengenai status Sertifikat. An online certificate-checking protocol for providing Relying Parties with real-time certificate status information.
Kunci Privat Private Key	Kunci dari Pasangan Kunci yang dirahasiakan oleh pemegang Pasangan Kunci, dan yang digunakan untuk membuat Tanda Tangan Elektronik dan / atau untuk mendekripsi catatan elektronik atau berkas yang dienkripsi dengan Kunci Publik terkait. 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 Pasangan Kunci dan yang digunakan oleh Pengandal untuk memverifikasi tanda tangan elektronik yang dibuat dengan Kunci Privat yang sesuai dan/atau untuk mengenkripsi pesan sehingga dapat didekripsi hanya dengan Kunci Privat yang sesuai. The key of a Key Pair that may be publicly disclosed by the holder of the Key Pair and that is used by a Relying Party to verify digital signatures created with the corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the corresponding Private Key.
Segel elektronik E-seal	Tanda tangan elektronik untuk merepresentasikan entitas Digital signature to represent the entity
Tanda tangan elektronik tersertifikasi (Tanda Tangan Digital) Digital signature	Tanda tangan yang bersifat digital yang dibuat berdasarkan Sertifikat Elektronik yang diterbitkan oleh PSrE Indonesia lewat Perangkat Pembuat Tanda Tangan Elektronik tersertifikasi sehingga memenuhi keabsahan kekuatan hukum dan akibat hukum Digital signatures which is made based on Digital Certificates issued by Indonesia CA through a certified Electronic Signature Creation Device so that they meet the validity of legal force and legal consequences