Tata Cara Pengelolaan Sertifikat (*Certification Practice Statement*)

Privy

Versi 3.1

19 Desember 2024

Jl. Kemang Raya 15C
Telp: 021-22715509
Email: Policy@privy.id
Website: www.privyca.id

Halaman Persetujuan *Policy Authority*
Policy Authority Approval Page

Dokumen ini disetujui secara elektronik sesuai pada waktu dan lokasi penandatanganannya.
This document is approved electronically according to the time and location of signing.

Menyetujui,
Approved by,

PSrE Induk / *Root CA* (Kementerian Komunikasi dan Informatika / *Ministry of Communication and Information*)	**PSrE Privy / *Privy CA***
Ditandatangani secara elektronik yang diterbitkan BSrE Aries Kusdaryono	
Aries Kusdaryono	Krishna Chandra
Direktur Tata Kelola Aplikasi Informatika/ *Policy Authority* PSrE Induk	Direktur PT Privy Identitas Digital/ *Policy Authority* PSrE Privy

Riwayat Perubahan

Versi	Tanggal	Deskripsi Riwayat dan Perubahan
1.0	-	Versi Perdana
1.1	22 Februari 2019	Penambahan untuk memenuhi persyaratan pengakuan sebagai Penyelenggara Sertifikasi Elektronik berinduk oleh Kominfo.
1.2	12 Januari 2021	Penambahan ketentuan RA Privy dan penyesuaian lainnya.
2.0	16 Juni 2021	Perubahan judul dokumen dan penyesuaian terhadap CP PSrE Induk Indonesia.
2.1	25 November 2021	Penambahan ketentuan tentang Inter-operasi, frekuensi pelatihan ulang, dan perubahan merek PrivyID menjadi Privy serta penyesuaian lainnya.
2.2	31 Januari 2023	Penambahan layanan Segel Elektronik dan identifikasi WNA. Penambahan persyaratan untuk penyesuaian terhadap CP Induk.
3.0	18 Agustus 2023	Penyesuaian terhadap ketentuan CP Induk berupa Perubahan OID, Kelas Sertifikat, Proses Validasi Identitas Awal, Arsip Dokumen, Perubahan Ketentuan Asuransi, Rencana Privasi.
3.1	19 Desember 2024	Penyesuaian terhadap ketentuan OID, penyesuaian ketentuan umur Sertifikat, penyesuaian profil sertifikat dan penyesuaian lainnya.

Change History

Version	Date	History and Change Description
1.0	-	Initial Release
1.1	February 22, 2019	Addition to meet the requirements for recognition as a subordinated Electronic Certification Authority by MCIT.
1.2	January 12, 2021	Addition of RA Privy provisions and other adjustments.
2.0	June 16, 2021	Change of document title and adjustment to the Certificate Practice (CP) of Indonesian Root CA.
2.1	November 25, 2021	Addition of provisions on Inter-operation, retraining frequency, and rebranding PrivyID to Privy as well as other adjustments.
2.2	January 31, 2023	Addition of Electronic Seal service and identification of foreigners. Addition of requirements for adjustments to the Root CP.
3.0	August 18, 2023	Adjusment to the CP Root CA in the form of changes to OID, Certificate Class, Initial Identity Validation Process, Document Archival, Changes to Insurance Provisions, Privacy Plan.
3.1	December 19, 2024	Adjustments to OID, Certificate Operational Periods, Certificate Profile provisions, and other relevant adjustments.

DAFTAR ISI / *TABLE OF CONTENTS*

1. Pengantar / *Introduction*

1.1. Ringkasan / *Overview*

Privy atau PT Privy Identitas Digital merupakan badan hukum yang menjalankan usaha sebagai Penyelenggaraan Sertifikasi Elektronik (“PSrE”) atau disebut juga dengan *Certificate Authority* (“CA”). Berdasarkan peraturan perundang-undangan yang diatur di Indonesia, Privy merupakan PSrE Non-Instansi.

Privy or PT Privy Identitas Digital is a legal entity that engages a business as an Electronic Certification Organization or *Penyelenggaraan Sertifikasi Elektronik* ("PSrE") or also known as Certificate Authority ("CA"). Based on the laws and regulations regulated in Indonesia, Privy is a Non-Government CA.

Tata Cara Pelaksanaan Sertifikat PSrE/*Certificate Practice Statement* (“CPS”) menguraikan persyaratan usaha, hukum, dan teknis yang mengatur mengenai Penyelenggara Sertifikasi Elektronik Privy oleh peserta di dalam Infrastruktur Kunci Publik/*Public Key Infrastructure* (“PKI”) Privy. CPS ini dibuat dengan memenuhi persyaratan formal yaitu konten, tata letak, dan format dari *Request for Comments* (“RFC”) 3647 tentang X.509 *Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework* yang dikeluarkan pada bulan November 2003 oleh *Internet Engineering Task Force* (IETF). CPS menguraikan praktik

The CA Certificate Practice Statement ("CPS") outlines the business, legal, and technical requirements governing the Privy Electronic Certification Authority by participants in the Privy Public Key Infrastructure ("PKI"). This CPS was created in compliance with the formal content, layout, and format requirements of Request for Comments ("RFC") 3647 on X.509 Public Key Infrastructure Certificate Policy and Certification Practices Statement Framework issued in November 2003 by the Internet Engineering Task Force (IETF). The CPS outlines the operational practices and procedures of Privy CA to meet

dan prosedur operasional PSrE Privy untuk memenuhi kriteria yang diatur oleh Kebijakan Sertifikat/*Certificate Policy* (“CP”) dari Penyelenggara Sertifikasi Elektronik Induk Indonesia (“PSrE Induk”).

the criteria set by the Certificate Policy ("CP") of the Indonesian Root Electronic Certification Authority ("Root CA").

Dokumen ini dibuat dengan asumsi bahwa pembaca telah memahami ketentuan yang diatur di dalam CP PSrE Induk, mengenal konsep Tanda Tangan Elektronik, Sertifikat Elektronik/Sertifikat Digital (“Sertifikat”), dan PKI secara umum. Apabila pembaca tidak mengenal konsep PKI, Pembaca dapat mengunduh CP PSrE Induk melalui https://www.rootca.id/.

This document is prepared on the assumption that the reader has understood the provisions set forth in the Root CA CP, is familiar with the concepts of Electronic Signatures, electronic certificates ("Certificates"), and PKIs in general. If the reader is not familiar with the concept of PKI, the reader can download the Root CA CP via https://www.rootca.id/.

Kecuali ditentukan lain, setiap penyebutan PSrE atau CA, adalah mengacu kepada PSrE Privy.

Unless otherwise specified, any reference to PSrE or CA, shall refer to Privy CA.

1.2. Identifikasi dan Nama Dokumen / *Document Name and Identification*

Dokumen ini berjudul “**Tata Cara Pengelolaan Sertifikat (*Certificate Practice Statement*) v.3.1”** yang merupakan CPS dari PSrE Privy.

This document is titled "**Certificate Practice Statement v.3.1"** which is the CPS of Privy CA.

Privy, sesuai kewenangannya, ditetapkan untuk memiliki

Privy, according to its authority, is designated to have Object

Object Identifier (OID) dengan nomor identifikasi joint-iso-itu-t(2) country(16) id(360) gov(1) kominfo(1) psre-induk(1) psre-Indonesia(3) psre-non-Instansi(12) privy(1).

Berikut merupakan OID untuk dokumen yang diterbitkan oleh Privy:

Sertifikat Non-Instansi	2.16.360.1.1.1.3.12
OID Privy	2.16.360.1.1.1.3.12.1
CPS	2.16.360.1.1.1.3.12.1.1

Selain OID untuk dokumen, berikut merupakan OID sesuai dengan ketentuan yang telah ditetapkan oleh Kementerian Komunikasi dan Informatika:

1.2.1. OID untuk Level Verifikasi	
Verification Level	2.16.360.1.1.1.4
OID untuk Level 1	2.16.360.1.1.1.4.1
OID untuk Level 2	2.16.360.1.1.1.4.2
OID untuk Level 3	2.16.360.1.1.1.4.3
OID untuk Level 4	2.16.360.1.1.1.4.4

Identifiers (OIDs) with the identification number joint-iso-it-t(2) country(16) id(360) gov(1) kominfo(1) psre-induk(1) psre-Indonesia(3) psre-non-Instansi(12) privy(1).

Here are the OIDs for documents published by Privy:

Non-Government Certificate	2.16.360.1.1.1.3.12
OID Privy	2.16.360.1.1.1.3.12.1
CPS	2.16.360.1.1.1.3.12.1.1

In addition to OIDs for documents, the following are OIDs in accordance with the provisions set by the Ministry of Communication and Information:

1.2.1. OID for Verification Level	
Verification Level	2.16.360.1.1.1.4
OID for Level 1	2.16.360.1.1.1.4.1
OID for Level 2	2.16.360.1.1.1.4.2
OID for Level 3	2.16.360.1.1.1.4.3

1.2.2. OID untuk SII Type	
SII Type	2.16.360.1.1.1.6
NIK	2.16.360.1.1.1.6.1
1.2.3. OID untuk Perubahan Sertifikat	
Peruntukan Sertifikat	2.16.360.1.1.1.7
Individu	2.16.360.1.1.1.7.1
Badan Usaha/Organisasi	2.16.360.1.1.1.7.2
1.2.4. OID untuk Individu	
Certificate Policies	2.16.360.1.1.1.5
1.2.4.1. OID untuk Individu Warga Negara Indonesia	
Orang Individu Warga Negara Indonesia (WNI)	2.16.360.1.1.1.5.1
Individu non-Instansi Online	2.16.360.1.1.1.5.1.2
Individu non-Instansi Online Level 2	2.16.360.1.1.1.5.1.2.2

OID for Level 4	2.16.360.1.1.1.4.4
1.2.2. OID for SII Type	
SII Type	2.16.360.1.1.1.6
National Identification Number (NIK)	2.16.360.1.1.1.6.1
1.2.3. OID for Certificate Modifications	
Certificate Designation	2.16.360.1.1.1.7
Individual	2.16.360.1.1.1.7.1
Business Entity/Organization	2.16.360.1.1.1.7.2
1.2.4. OID for Individuals	
Certificate Policies	2.16.360.1.1.1.5
1.2.4.1. OID for Indonesian Citizen (WNI) Individuals	
Indonesian Citizen (WNI) Individual	2.16.360.1.1.1.5.1
Non-Government Individual Online	2.16.360.1.1.1.5.1.2

1.2.4.2. OID untuk Individu Warga Negara Asing	
Orang Individu Warga Negara Asing (WNA)	2.16.360.1.1.1.5.2
Individu WNA Online	2.16.360.1.1.1.5.2.2
Individu WNA Online level 2	2.16.360.1.1.1.5.2.2.2
Individu WNA Online level 3	2.16.360.1.1.1.5.2.2.3
1.2.5. OID untuk Badan Usaha	
OID Segel Elektronik	2.16.360.1.1.1.8
Badan Usaha	2.16.360.1.1.1.8.1

Non-Government Individual Online Level 2	2.16.360.1.1.1.5.1.2.2
1.2.4.2. OID for Foreign Citizen (WNA) Individuals	
Foreign Citizen (WNA) Individual	2.16.360.1.1.1.5.2
WNA Individual Online	2.16.360.1.1.1.5.2.2
WNA Individual Online Level 2	2.16.360.1.1.1.5.2.2.2
WNA Individual Online Level 3	2.16.360.1.1.1.5.2.2.3
1.2.5. OID for Business Entity	
Electronic Seal OID	2.16.360.1.1.1.8
Business Entity	2.16.360.1.1.1.8.1

Untuk Sertifikat Elektronik yang diterbitkan sebelum CPS ini dan menggunakan OID sebagaimana disebutkan pada bagian 1.2.1 dan 1.2.3 CPS ini akan tetap berlaku sampai dengan masa

For Electronic Certificates issued prior to this CPS and using the OIDs as mentioned in sections 1.2.1 and 1.2.3 of this CPS, they will remain valid until the expiration of the respective

berlaku Sertifikat tersebut berakhir. Untuk seluruh Sertifikat Elektronik yang diterbitkan setelah CPS ini efektif berlaku akan menggunakan OID sebagaimana diatur dalam CPS ini.

Certificates. All Electronic Certificates issued after the effective date of this CPS will use the OIDs as stipulated in this CPS.

Dokumen CPS tersedia secara umum pada https://repository.privyca.id.

CPS documents are publicly available at https://repository.privyca.id.

1.3. Partisipan PKI / *PKI Participants*

1.3.1. Penyelenggara Sertifikasi Elektronik / *Certification Authorities*

Penyelenggara Sertifikasi Elektronik (PSrE) /*Certificate Authority* (CA) adalah Badan Hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat, sesuai dengan apa yang diatur di dalam CPS ini. PSrE Privy berdasarkan CPS ini merupakan CA yang menjalankan fungsi *Public Key Infrastructure* (PKI) Privy, yang termasuk namun tidak terbatas pada:

a. Operasional Siklus Sertifikat;
b. Pemrosesan Permohonan Sertifikat;
c. Penerbitan Sertifikat;
d. Penerimaan Sertifikat;
e. Penggunaan Sertifikat;

Electronic Certification Authority or Penyelenggara Sertifikasi Elektronik (PSrE)/Certificate Authority (CA) is a Legal Entity that functions as a trusted party, which provides and audits Certificates, in accordance with what is regulated in this CPS. Privy CA based on this CPS is a CA that performs Privy Public Key Infrastructure (PKI) functions, which include but are not limited to:

a. Certificate Cycle Operations;
b. Certificate Application Processing;
c. Certificate Issuance;
d. Certificate Acceptance;

f. Pembaruan dan/atau Perpanjangan Sertifikat; dan
g. Pencabutan Sertifikat;

e. Certificate Usage;
f. Certificate Renewal and/or Extension; and
g. Certificate Revocation;

1.3.1.1. PSrE Induk / *Root CA*

PSrE Induk adalah PSrE yang ditetapkan sebagai induk (*root*) PSrE Indonesia sebagaimana diatur di dalam peraturan perundang-undangan yang mengatur mengenai penyelenggaraan sertifikasi elektronik. PSrE Induk berperan dalam menandatangani dan mencabut Sertifikat PSrE yang berinduk di bawahnya. PSrE Induk dikelola oleh Kominfo. PSrE Induk tidak menerbitkan Sertifikat kepada Pemegang Sertifikat. PSrE Induk bertanggung jawab terhadap penerbitan dan pengelolaan Sertifikat PSrE Indonesia, sebagaimana dirinci dalam CP PSrE Induk, termasuk namun tidak terbatas pada:

1. Pengendalian terhadap proses pendaftaran calon PSrE Indonesia;
2. Proses identifikasi dan autentikasi;
3. Proses penerbitan *self-sign* Sertifikat PSrE Induk;

The Root CA is a CA that is designated as the Root of the Indonesian CA as stipulated in the laws and regulations governing the implementation of Electronic Certification. The Root CA plays a role in signing and revoking subordinated CA Certificates. The Root CA is managed by Kominfo. The Root CA does not issue Certificates to Subscribers. The Root CA is responsible for the issuance and management of Indonesian CA Certificates, as detailed in the Root CA CP, including but not limited to:

1. Control of the registration process for Indonesian CA candidates;
2. Identification and authentication process;
3. The process of self-sign issuance of the Root CA Certificate;
4. The process of issuing an Indonesian CA Certificate;
5. The process of issuing Certificate Revocation Lists

4. Proses penerbitan Sertifikat PSrE Indonesia;
5. Proses penerbitan Daftar Pencabutan Sertifikat (*Certificate Revocation List*/CRLs);
6. Publikasi Sertifikat dan CRLs;
7. Validasi Sertifikat;
8. Pencabutan Sertifikat;
9. Membangun dan memelihara sistem PSrE Induk; dan
10. Memastikan semua aspek layanan, operasional, dan infrastruktur yang terkait dengan PSrE Induk yang diterbitkan sesuai dengan CP dilaksanakan sesuai dengan persyaratan, representasi, dan jaminan dari CP PSrE Induk.

(CRLs);
6. Publication of Certificates and CRLs;
7. Certificate Validation;
8. Certificate Revocation;
9. Establishing and maintaining the Root CA system; and
10. Ensuring all aspects of services, operations and infrastructure associated with the Root CA issued pursuant to the CP are implemented in accordance with the requirements, representations and warranties of the Root CA CP.

1.3.1.2. PSrE Indonesia / *Indonesian CA*

PSrE Indonesia adalah PSrE yang telah mendapatkan pengakuan sebagai PSrE Berinduk dari Kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, yang Sertifikatnya ditandatangani oleh PSrE Induk.

Indonesian CA is a CA that has been recognized as a Root CA from the Ministry that organizes government affairs in the field of communication and informatics, whose Certificate is signed by the Root CA.

PSrE Indonesia tidak boleh menjadi induk bagi PSrE lainnya.

Indonesian CAs are not allowed to root themselves

on other CAs.

1.3.2. Otoritas Pendaftaran / *Registration Authorities*

Otoritas Pendaftaran /*Registration Authorities* (RA) merupakan pihak yang ditunjuk oleh PSrE Privy untuk menjalankan fungsi penerimaan permohonan pendaftaran, identifikasi, autentikasi Pemohon/Pemilik dan/atau menerima permohonan pencabutan Sertifikat Elektronik sesuai dengan ketentuan pada CPS ini.

Registration Authorities (RAs) are parties appointed by Privy CA to carry out the functions of receiving enrollment application, identifying and authenticating Applicants/Subscriber, and/or processing requests for the revocation of Electronic Certificates in accordance with the provisions of this CPS.

Adapun kewajiban RA adalah sebagai berikut:

a. Tunduk terhadap prosedur pendaftaran pemohon Sertifikat;
b. Identifikasi dan autentikasi Pemohon Sertifikat berdasarkan prosedur pendaftaran yang ditetapkan oleh PSrE Privy;
c. Memulai atau meneruskan permohonan untuk pencabutan Sertifikat kepada PSrE Privy; dan
d. Menyetujui permohonan penerbitan ulang atau perpanjangan Pemegang Sertifikat.

The obligations of the RAs are as follows:

a. Subject to Certificate applicant registration procedures;
b. Identification and authentication of the Certificate Applicant based on the enrollment procedure established by Privy CA;
c. Initiate or forward an application for Certificate revocation to Privy CA; and
d. Approve Subscriber re-issuance or renewal applications.

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

In the event that Privy CA acts directly to receive an application for Certificate issuance from the Applicant, then Privy CA shall act as an RA for itself.

Kecuali disebutkan lain, RA yang tercantum dalam ketentuan ini adalah RA yang terikat dengan hubungan kontraktual dengan PSrE Privy. Oleh karena itu, seluruh ketentuan yang secara tegas menjelaskan mengenai peran RA di dalam CPS ini berlaku terhadap seluruh RA. PSrE Privy memiliki hak untuk melakukan audit atau pemeriksaan terhadap kesesuaian fungsi yang dijalankan oleh RA dengan CPS ini dan peraturan perundang-undangan yang berlaku.

Unless otherwise specified, RAs listed in this provision are those bound by a contractual relationship with Privy CA. Therefore, all provisions that expressly describe the role of RAs in this CPS apply to all RAs. Privy CA has the right to conduct an audit or examination of the conformity of the functions carried out by RAs with this CPS and applicable laws and regulations.

1.3.3. Pemilik / *Subscribers*

Pemilik/Pemegang Sertifikat adalah pihak yang identitasnya tertera dalam Sertifikat yang diterbitkan oleh PSrE Privy dan sudah melalui proses verifikasi. Sebelum dilakukan verifikasi identitas dan Sertifikat diterbitkan, Pemilik/Pemegang Sertifikat disebut sebagai Pemohon.

Subscriber is the party whose identity is listed in the Certificate issued by Privy CA and has undergone the verification process. Before the identity is verified and the Certificate is issued, the Subscriber is referred to as the Applicant.

Pemilik/Pemegang Sertifikat adalah pihak yang namanya tertera sebagai subjek pada Sertifikat yang menegaskan bahwa dia menggunakan kunci dan Sertifikat sesuai CPS dan tidak menerbitkan Sertifikat.	Subscriber is the party whose name appears as the subject of the Certificate, confirming that they are using the key and Certificate in accordance with the CPS and are not issuing Certificates.

1.3.4. Pengandal / *Relying Parties*

Pengandal/*Relying Parties* adalah Orang atau Badan Hukum yang mempercayai Sertifikat dan/atau Tanda Tangan Elektronik yang diterbitkan oleh Privy. Pengandal terlebih dahulu memeriksa respon dari CRL atau OCSP yang sesuai sebelum memanfaatkan informasi yang tertera di dalam Sertifikat.	Relying Parties are Persons or Legal Entities that trust the Certificates and/or Electronic Signatures issued by Privy. Relying Parties first check the response from the appropriate CRL or OCSP before utilizing the information contained in the Certificate.
Pengandal mengandalkan keabsahan hubungan antara identitas Pemegang Sertifikat dengan kunci publik yang tercantum dalam Sertifikat. Pengandal bertanggung jawab untuk melakukan pengecekan status informasi di dalam Sertifikat. Pengandal dapat menggunakan informasi di dalam Sertifikat untuk menentukan apakah suatu	The Relying Parties relies on the validity of the relationship between the Subscriber's identity and the public key contained in the Certificate. The Relying Parties are responsible for checking the status of the information in the Certificate. The Relying Parties may use the information in the Certificate to determine whether or not a Certificate is reliable.

Sertifikat dapat diandalkan atau tidak.

Pengandal menggunakan informasi dalam Sertifikat untuk, antara lain:

a. Memeriksa tujuan penggunaan Sertifikat;
b. Melakukan verifikasi Tanda Tangan Elektronik;
c. Melakukan pemeriksaan (apakah Sertifikat ada pada daftar) pencabutan (CRL dan OCSP); dan
d. Penyetujuan atas batas tanggung jawab dan jaminan.

Relying Parties use the information in the Certificate to, among other things:

a. Check the intended use of the Certificate;
b. Perform verification of Electronic Signatures;
c. Conduct a checking (whether the Certificate is on the list) of revocations (CRL and OCSP); and
d. Give an approval of limits of liability and warranties.

Setiap pihak, baik pelanggan maupun bukan pelanggan Privy, dapat mengandalkan Sertifikat yang diterbitkan oleh Privy. Namun siapapun yang mengandalkan Sertifikat yang diterbitkan oleh Privy tunduk pada ketentuan yang diatur dalam CPS ini dan juga Perjanjian Pengandal.

Any party, whether a Privy customer or non-customer, can rely on the Certificate issued by Privy. However, anyone who relies on the Certificate issued by Privy shall be subject to the provisions stipulated in this CPS and also the Relying Parties Agreement.

1.3.5. Partisipan Lain / *Other Participants*

Dalam menjalankan layanannya, PSrE Privy bekerja sama dengan partisipan lain yaitu pihak ketiga yang menyediakan layanan Pusat Data dan Pusat Data Pemulihan.

In running its services, Privy CA collaborates with other participants, namely third parties who provide Data Center and Recovery Data Center services.

1.4. Kegunaan Sertifikat / *Certificate Usage*

Sertifikat memuat Tanda Tangan Elektronik Penerbit Sertifikat dan informasi mengenai identitas dan status subjek hukum Pemegang Sertifikat dalam suatu Transaksi Elektronik.

The Certificate contains the Certificate Issuer's Electronic Signature and information about the identity and status of the legal subject of the Subscriber in an Electronic Transaction.

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

PSrE Privy menetapkan bahwa Layanan Sertifikat yang diterbitkan untuk Pengguna Akhir adalah hanya untuk melakukan **Tanda Tangan Digital dan Segel Elektronik**.

Privy CA stipulates that the Certificate Service issued to End Users is only for performing **Digital Signatures and Electronic Seals**.

Tanda Tangan Digital merupakan jenis Tanda Tangan Elektronik yang digunakan untuk mendukung penandatangan melalui media elektronik dengan menggunakan metode kriptografi asimetris dan menggunakan Sertifikat untuk melakukan verifikasi antara pasangan Kunci Privat yang dikuasai oleh Pemegang Sertifikat dan Kunci Publik yang tertera di dalam Sertifikat.

Digital Signature is a type of Electronic Signature used to support signing through electronic media using asymmetric cryptography methods and using Certificates to verify between the Private Key pair controlled by the Subscriber and the Public Key stated in the Certificate.

Segel Elektronik adalah data elektronik yang dilekatkan, terasosiasi, atau terkait dengan

Electronic Seal is electronic data attached, associated, or related to Electronic

Informasi Elektronik dan/atau Dokumen Elektronik untuk menjamin asal, integritas, dan keutuhan dari Informasi Elektronik dan/atau Dokumen Elektronik yang digunakan oleh Badan Usaha.

Information and/or Electronic Documents to guarantee the origin, integrity, and wholeness of Electronic Information and/or Electronic Documents used by Business Entities.

Sertifikat yang diterbitkan oleh PSrE Privy untuk Pemegang Sertifikat digunakan untuk transaksi dengan menggunakan Tanda Tangan Elektronik sehingga menjadi Tanda Tangan Digital, yang membutuhkan 3 (tiga) faktor berikut yang menjamin:

a. *Non-Repudiation*: Penanda tangan tidak dapat menampik tanda tangan yang telah dibubuhkannya.
b. *Authentication*:
   Kepastian bahwa penanda tangan merupakan pihak yang benar-benar melakukan tanda tangan.
c. *Integrity*:
   Kepastian bahwa suatu informasi atau dokumen elektronik tidak mengalami perubahan.

Certificates issued by Privy CA to Subscribers are used for transactions using Electronic Signatures so that they become Digital Signatures, which require the following 3 (three) factors to guarantee:

a. Non-Repudiation:
   The signatory cannot revoke the signature that has been affixed.
b. Authentication:
   Certainty that the signatory is the legitimate party who executed the signature.
c. Integrity:
   Certainty that electronic information or documents have not been altered.

Berdasarkan penjelasan tersebut, *Key Usage* yang diperbolehkan untuk *Pemegang*

Based on this explanation, the Key Usage allowed for Subscribers is Digital Signature

Sertifikat adalah *Digital Signature* dan *Non-Repudiation*.	and Non-Repudiation.
Sertifikat yang diterbitkan oleh PSrE Privy adalah Sertifikat Elektronik dengan level verifikasi identitas level 2 (Sertifikat Kelas 3) dan level verifikasi identitas level 3 (Sertifikat Kelas 4) sesuai dengan peraturan *perundang*-undangan yang mengatur mengenai penyelenggaraan sertifikasi elektronik.	The certificate issued by Privy CA is an Electronic Certificate with identity verification level 2 (Class 3 Certificate) and identity verification level 3 (Class 4 Certificate) in accordance with the laws and regulations governing the implementation of electronic certification.

1.4.2. Penggunaan Sertifikat yang Dilarang / *Prohibited Use of Certificates*

Sertifikat yang diterbitkan oleh PSrE Privy hanya dapat digunakan untuk hal-hal yang diperbolehkan menurut ketentuan CPS ini dan peraturan perundang-undangan yang berlaku.	Certificates issued by Privy CA can only be used for matters permitted under the provisions of this CPS and applicable laws and regulations.

1.5. Administrasi Kebijakan / *Policy Administration*

Policy Authority (PA) memiliki peran dan tanggung jawab sebagai berikut: 1. Menetapkan CPS PSrE Privy; 2. Memastikan semua layanan, operasional dan infrastruktur PSrE Privy yang didefinisikan dalam CPS telah dilakukan sesuai dengan persyaratan, pernyataan dan jaminan dari CP PSrE Induk; dan	The Policy Authority (PA) has the following roles and responsibilities: 1. Establishing the CPS for Privy CA; 2. Ensuring that all services, operations, and infrastructure of Privy CA, as defined in the CPS, are conducted in accordance with the requirements,

3. Menyetujui terjalinnya hubungan kepercayaan dengan KPI lainnya yang memiliki level verifikasi yang setara.

statements, and assurances from the Root CA; and
3. Approving the establishment of trust relationships with other KPIs that have an equivalent level of verification.

1.5.1. Organisasi Pengelola Dokumen / *Document Management Organization*

CPS ini dikelola oleh *Policy Authority* Privy (PA). CPS diubah sesuai dengan kebijakan yang ditentukan oleh PA. CPS ini juga berubah jika diperlukan penyesuaian dengan *Baseline Requirements* dari *CA Browser Forum, Webtrust Principles & Criteria for Certificate Authority*, *Adobe Approved Trusted List Technical Requirements,* dan/atau CP PSrE Induk.

This CPS is managed by the Privy's Policy Authority (PA). The CPS is amended in accordance with the policies established by the PA. This CPS may also be revised as necessary to align with the Baseline Requirements of the CA Browser Forum, the Webtrust Principles & Criteria for Certificate Authorities, the Adobe Approved Trusted List Technical Requirements, and/or the Root CA CP.

PA terdiri dari *Chief* Executive *Officer* (Direktur Utama) dan/atau pihak yang ditunjuk untuk mengepalai C-Level Unit di Privy.

The PA consists of the Chief Executive Officer and/or appointed individuals heading C-Level Units within Privy.

PA dapat dihubungi melalui:
Policy Authority Privy
Jl. Kemang Raya No. 15C
Telp: 021-22715509

The PA can be contacted at:
Policy Authority Privy
Jl. Kemang Raya No. 15C
Telp: 021-22715509

Email: Policy@privy.id	Email: Policy@privy.id

1.5.2. Narahubung / *Contact Person*

Narahubung dapat menggunakan informasi yang tertera pada bagian 1.5.1.	The contact person can use the information listed in section 1.5.1.

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

PA Privy dibantu oleh Departemen yang mengurusi bagian hukum dan kepatuhan beserta dengan perwakilan yang ditunjuk oleh masing-masing divisi Privy yang terkait dengan PKI Privy dalam menentukan kesesuaian dan penerapan dari CPS ini.	The Privy PA is assisted by the legal and compliance department along with representatives appointed by each Privy division associated with the Privy PKI in determining the suitability and applicability of this CPS.

1.5.4. Prosedur Persetujuan CPS / *CPS Approval Procedures*

Perubahan terhadap CPS melalui persetujuan dari PA dan telah mendapat persetujuan dari PA PSrE Induk.	Changes to the CPS are subject to approval by the PA and have obtained approval from the PA of the Root CA.

1.6. Definisi dan Akronim / *Definitions and Acronyms*

Lihat Lampiran 2.	See Appendix 2.

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

2.1. Repositori / *Repositories*

PSrE Privy menyediakan dan menjaga Repositori yang berisi dokumen yang menunjang penyelenggaraan layanan PKI yaitu:

a. *Public Key Certificate* PSrE;
b. *CRL* dan/atau Status Keaktifan Sertifikat;
c. CPS;
d. Perjanjian Pemegang Sertifikat;
e. Perjanjian Pengandal;
f. Pemberitahuan Privasi;
g. Kebijakan Jaminan; dan
h. OCSP.

Privy CA provides and maintains a Repository that contains documents that support the implementation of PKI services, namely:

a. CA Public Key Certificate;
b. CRL and/or Certificate Activation Status;
c. CPS;
d. Subscriber Agreement;
e. Relying Parties Agreement;
f. Privacy Notice;
g. Warranty Policy; and
h. OCSP

2.2. Publikasi Informasi Sertifikat / *Publication of Certificate Information*

Dokumen elektronik yang disebutkan di bagian 2.1. tersedia dan dapat diakses secara publik melalui URL https://repository.privyca.id. Dokumen tersebut hanya berlaku dan diakui oleh PSrE Privy apabila dokumen tercantum dan dapat diakses melalui Repositori Privy.

The electronic documents mentioned in section 2.1. are publicly available and accessible through the URL https://repository.privyca.id. The document is only valid and recognized by Privy CA if the document is listed and accessible through the Privy Repository.

Dalam pelaksanaannya, PSrE Privy dapat menampilkan dokumen yang tercantum dalam Repositori tersebut dalam beberapa pilihan Bahasa. Khusus terhadap dokumen hukum, jika terdapat ketidaksesuaian antara

In its implementation, Privy CA can display documents listed in the Repository in several language options. Especially for legal documents, if there is a discrepancy between one language and another, the

satu bahasa dengan bahasa yang lain, maka dokumen berbahasa Indonesia yang berlaku.

Indonesian language document shall prevail.

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

Berikut merupakan waktu atau frekuensi publikasi untuk dokumen-dokumen yang tertera di dalam Repositori:

a. *Public Key Certificate/* Sertifikat Kunci Publik PSrE
   Paling lambat 1 x 24 jam setelah pasangan kunci dibangkitkan.
b. CRL dan/atau Status Keaktifan Sertifikat
   Sebagaimana ditentukan pada bagian 4.9.7.
c. CPS

   Dalam kurun waktu 7 (tujuh) hari kerja setelah mendapat persetujuan dari PA dan PA PSrE Induk. CPS akan ditinjau ulang setidaknya sekali dalam waktu satu tahun kalender. Jika tidak ada perubahan terhadap konten dari CPS tersebut, setidaknya akan dilakukan perubahan terhadap versi dan tanggal penerbitan dari CPS yang baru.

The following is the publication time or frequency for the documents listed in the Repository:

a. CA Public Key Certificate
   No later than 1 x 24 hours after the key pair is generated.
b. CRL and/or Certificate Activation Status
   As specified in section 4.9.7.
c. CPS.

   Within 7 (seven) business days after obtaining approval from the PA and the PA of Root CA. The CPS will be reviewed at least once a calendar year. If there are no changes to the content of the CPS, at least a change will be made to the version and publication date of the new CPS.

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

Dokumen yang tercantum dalam Repositori merupakan informasi publik yang dapat diakses oleh siapapun dalam bentuk dokumen *read-only.* PSrE Privy menerapkan kontrol keamanan secara logis dan fisik untuk mencegah pihak yang tidak berwenang untuk menambahkan, menghapus, atau mengubah dokumen di dalam Repositori.	Documents listed in the Repository are public information that can be accessed by anyone in the form of read-only documents. Privy CA applies logical and physical security controls to prevent unauthorized parties from adding, deleting, or changing documents in the Repository.

3. Identifikasi dan Autentikasi / *Identification and Authentication*

Privy sebagai CA dan/atau RA melakukan verifikasi dan autentikasi identitas dan/atau atribut lainnya dari Pemohon Sertifikat untuk menerbitkan Sertifikat.	Privy CA as a CA and/or RA verifies and authenticates the identity and/or other attributes of the Certificate Applicant to issue the Certificate.

3.1. Penamaan / *Naming*

3.1.1. Tipe Nama / *Types of Name*

Sertifikat yang dibangkitkan dan ditandatangani oleh PSrE Privy sesuai dengan standar ITU X.500 *Distinguished Names*. Seluruh Sertifikat mengandung X.501 distinguished *name* dalam kolom *Subject Name*. Sertifikat yang diterbitkan oleh PSrE Privy menggunakan *Distinguished Name* (DN) yang *non-null* untuk	Certificates issued by Privy CA are compliant with the ITU X.500 Distinguished Names standard. All Certificates contain an X.501 distinguished name in the Subject Name field. Certificates issued by Privy CA use a non-null Distinguished Name (DN) to support identification of the Subscriber.

mendukung identifikasi dari Pemegang Sertifikat.

DN yang digunakan oleh PSrE Privy adalah sesuai dengan ketentuan yang diatur di dalam CP PSrE Induk. Adapun pengaturan parameter mengacu pada Standar Interoperabilitas PSrE Induk. PSrE Privy menggunakan DN untuk mengidentifikasi suatu individu dan/atau Badan Hukum/Badan Usaha yang ditampilkan dalam kolom *Subject Name* dan *Issuer Name*. Isi dari DN tersebut dapat berupa atribut sebagai berikut:

The DN used by Privy CA is in accordance with the provisions stipulated in the Root CA CP. The parameter settings refer to the Root CA Interoperability Standard. Privy CA uses the DN to identify an individual and/or Legal Entity/Business Entity that appeared in the Subject Name and Issuer Name field. The contents of the DN can be in the form of the following attributes:

Atribut *Common Name* (CN) yang digunakan pada Sertifikat perorangan/individu adalah nama lengkap Pemegang Sertifikat ditambah dengan *Username* Privy, atau entitas yang mewakili Pemegang Sertifikat beserta *Username* Privy. Sedangkan untuk Badan Usaha/Badan Hukum adalah nama Badan Usaha/Badan Hukum tersebut sesuai pada dokumen legalitas milik Badan Usaha/Badan Hukum tersebut beserta *Username* Privy.

The Common Name (CN) attribute used in individual Certificate represents the full name of the Subscriber, accompanied by its Privy Username, or the name of the entity representing the Subscriber along with the Privy Username. For Business Entity/Legal Entity, the CN attribute reflects the name of the Business Entity/Legal Entity as stated in its legal documentation, along with the Privy Username.

Atribut Organization name (O) untuk Sertifikat perorangan/individu tidak berlaku, sedangkan untuk Badan Hukum/Badan Usaha akan diisi dengan nama entitas RA yang melakukan validasi identitas.

The Organization name (O) attribute for individual Certificate is not applicable (N/A). However, for Legal Entity/Business Entity, this attribute will be filled in with the name of the RA entity that validates the identity.

Atribut *Organization Unit* (OU) untuk Sertifikat perorangan/individu akan diisi Personal dan untuk Badan Hukum/Badan usaha akan diisi dengan Badan Usaha/Badan Hukum.

The Organization Unit (OU) attribute for individual Certificates will be set as "Personal" and Legal Entity/Business Entity Certificates will be set as "Business Entity/Legal Entity".

Atribut *Country* (C) merupakan negara dimana Pemegang Sertifikat menyatakan kedudukannya.

The Country (C) attribute indicates the country where the Subscriber declares its residence.

Ketentuan terkait DN tersebut selengkapnya dapat dilihat pada tabel di bawah ini:

DN	Keterangan	Individu WNI dan WNA	Badan Usaha
CN	Common Name	Nama Lengkap dan	Nama Badan Usaha/ Badan Hukum

The complete provisions related to the DN can be seen in the table below:

DN	Information	WNI and WNA Individuals	Business Entity
CN	Common Name	The Full Name and the	The name of the Business

		User name Privy	dan Username Privy
O	Organization Name	Tidak berlaku	Nama Entitas RA yang melakukan validasi identitas
OU	Organization Unit	Personal	Badan Usaha
C	Country	ID	ID

		Privy Username	Entity/ Legal Entity and the Privy Username
O	Oranization Name	N/A	The name of the RA entity responsible for validating the identity
OU	Organization Unit	Personal	Business Entity
C	Country	ID	ID

PSrE Privy menggabungkan penggunaan Sertifikat Pemilik sebagai perorangan/individu dengan Sertifikat Pemilik yang berafiliasi dengan suatu Badan Hukum/Badan Usaha. Dalam hal Pemilik menggunakan Sertifikat yang berafiliasi dengan suatu Badan Hukum/Badan Usaha,

Privy CA combines the use of the Subscriber's Certificate as an individual with the Subscriber's Certificate affiliated with a Legal Entity/Business Entity. In cases where the Subscriber utilizes a Certificate affiliated with a Legal Entity/Business Entity, the

Pemilik harus memeriksa alasan persetujuan penggunaan Sertifikat agar sesuai dengan tujuan penggunaannya dalam hal sebagai perorangan/individu atau berafiliasi dengan suatu Badan Hukum/Badan Usaha.	Subscriber is required to verify the basis for approving the use of the Certificate to ensure its alignment with the intended purpose, whether for individual use or in affiliation with a Legal Entity/Business Entity.

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

Sertifikat yang diterbitkan oleh PSrE Privy akan memunculkan nama-nama yang dapat dipahami dan digunakan oleh Pengandal. Nama yang digunakan tersebut dapat mengidentifikasi orang atau objek dalam Sertifikat tersebut.	Certificates issued by Privy CA will display names that are clear and understandable for the Relying Party. These names can be used to identify the individuals or objects mentioned in the Certificate.
PSrE Privy menggunakan DN sebagaimana disebutkan pada bagian 3.1.1 untuk mengidentifikasi suatu individu dan/atau Badan Hukum/Badan Usaha yang ditampilkan dalam kolom *Subject Name* dan kolom *Issuer Name.* Dengan menyetujui penerbitan Sertifikat, Pemilik dianggap telah menyetujui isi dari DN yang digunakan oleh Privy pada Sertifikat Pemilik.	Privy CA uses the DN as specified in section 3.1.1 to identify an individual and/or Legal Entity/Business Entity, which is displayed in the Subject Name and Issuer Name fields. By accepting the issuance of the Certificate, the Subscriber is deemed to have agreed to the contents of the DN used by Privy in the Subscriber's Certificate.

3.1.3. Anonimitas atau Pseudonimitas Pemegang Sertifikat / *Anonymity or Pseudonymity of Subscribers*

Privy tidak menerbitkan Sertifikat anonim atau pseudonim.	Privy does not publish anonymous or pseudonymous Certificates.

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

DN dalam Sertifikat diuraikan menggunakan standar X.500.	The DN in the Certificate is described using the X,500 standard.

3.1.5. Keunikan Nama / *Uniqueness of Name*

DN dari setiap Sertifikat yang diterbitkan adalah unik dengan kriteria berdasarkan Kelas atau tipe dari Sertifikat yang diterbitkan. Apabila dibutuhkan, PSrE Privy dapat menambahkan informasi tambahan yang dicantumkan di dalam *Subject Distinguished Name* pada Sertifikat sebagai daya pembeda dalam hal terdapat 2 (dua) atau lebih Sertifikat yang seharusnya memiliki *Subject Name* yang sama.	The DN of each Certificate issued is unique with criteria based on the Class or type of Certificate issued. If needed, Privy CA can add additional information included in the Subject Distinguished Name on the Certificate as a distinguishing factor in the event that there are 2 (two) or more Certificates that should have the same Subject Name.

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

Pemohon tidak diperbolehkan mengajukan permohonan Sertifikat dengan konten yang melanggar hak kekayaan intelektual pihak lain. PSrE Privy	Applicants are not allowed to apply for Certificates with content that violates the intellectual property rights of others. Privy CA will not verify

tidak akan memverifikasi permohonan yang terkait dengan penggunaan merek dagang. Pemohon atau Pemegang Sertifikat berkewajiban dan bertanggung jawab untuk memastikan bahwa permohonan Sertifikat yang diajukan tidak melanggar hak kekayaan intelektual pihak lain.

applications related to the use of trademarks. The Applicant or Subscriber is obliged and responsible for ensuring that the Certificate application submitted does not violate the intellectual property rights of others.

3.2. Validasi Identitas Awal / *Initial Identity Validation*

PSrE Privy akan melakukan identifikasi dan autentikasi Pemohon Sertifikat berdasarkan prosedur pendaftaran yang ditetapkan oleh PSrE Privy yang mengacu kepada Standar Verifikasi Identitas yang diterbitkan oleh PSrE Induk.

Privy CA will identify and authenticate Applicant for Certificate in accordance with the registration procedure established by Privy CA, referencing the Identity Verification Standards Issued by Root CA.

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

Pasangan Kunci yang telah dibangkitkan oleh Privy, Kunci Privatnya akan disimpan dan diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan *Federal Information Protection Standards* (FIPS)-140 level 2. Untuk pembuktian penguasaan Kunci Privat yang terasosiasi dengan Sertifikat Pemohon

The Key Pair that has been generated by Privy, the Private Key will be stored and secured using a cryptographic module that meets the requirements of Federal Information Protection Standards (FIPS)-140 level 2. To prove the possession of the Private Key associated with the Applicant Certificate for the signing process, it uses the

untuk proses penandatanganan menggunakan metode autentikasi yang ditentukan oleh PSrE Privy yang meliputi 2 dari 3 faktor autentikasi yaitu *Something you know, Something you have*, *Something you are*.

authentication method determined by Privy's CA which includes 2 of the 3 authentication factors, namely Something you know, Something you have, Something you are.

3.2.2. Autentikasi Identitas Organisasi / *Authentication of Organization Identity*

Jika suatu Sertifikat digunakan untuk mengidentifikasi suatu Badan Hukum/Badan Usaha maka pengajuan untuk mendapatkan Sertifikat tersebut hanya dapat diajukan oleh pihak yang berwenang untuk mewakili Badan Hukum/Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut.

If a Certificate is used to identify a Legal Entity/Business Entity, the application to obtain the Certificate can only be submitted by the party authorized to represent the Legal Entity/Business Entity, namely the highest leader or President Director of the Business Entity or it can be submitted by a third party representing the Business Entity whose authority can be proven by a power of attorney signed by the highest leader or President Director of the Business Entity.

PSrE Privy dan/atau RA akan memeriksa dokumen-dokumen milik Badan Hukum/Badan Usaha dan identitas pemohon sesuai autentikasi identitas individu

Privy CA and/or RA will check the documents belonging to a Legal Entity/Business Entity and the applicant's identity according to the authentication

yang diatur dalam bagian 3.2.3. Adapun pemeriksaan yang dilakukan meliputi:

a. Formulir pendaftaran Sertifikat yang mencantumkan informasi identitas, nomor ponsel, alamat email, dan akun pribadi Privy milik perwakilan Badan Hukum/Badan Usaha (dalam hal perwakilan Badan Hukum/Badan Usaha belum mempunyai akun Privy, maka perwakilannya tersebut diminta untuk melakukan pembuatan akun Privy);
b. Kartu Nomor Pokok Wajib Pajak ("NPWP") Badan Hukum/Badan Usaha.
c. Akta pendirian dan/atau akta perubahan terakhir Badan Hukum/Badan Usaha beserta Surat Keputusan dari Kementrian Hukum dan HAM atas akta tersebut ("**SK Kemenkumham**");
d. Surat kuasa/surat penunjukan dari pihak yang berwenang untuk mewakili Badan Hukum/Badan Usaha (jika dibutuhkan).

of individual identity stipulated in section 3.2.3. The examinations conducted encompass the following:

a. The Certificate registration form, which includes the representative of the Legal Entity/Business Entity's identity information, mobile phone number, email address, and Privy personal account (if the representative of the Legal Entity/Business Entity does not yet have a Privy account, they will be required to create one);
b. Legal Entity/Business Entity Taxpayer Registration Number ("NPWP") Card;
c. Deed of Establishment and/or last amandement act of Legal Entity/Business Entity, along with the Decree from the Ministry of Law and Human Rights of the Republic of Indonesia regarding the deed ("MOLHR Decree");
d. Power of attorney/letter of appointment from an authorized party to represent the Legal Entity/Business Entity (if required).

PSrE Privy melakukan identifikasi dan autentikasi terhadap dokumen-dokumen yang diberikan oleh Badan Hukum/Badan Usaha untuk penerbitan Sertifikat. Adapun proses identifikasi dan autentikasi yang dilakukan adalah:

a. Pemeriksaan dan validasi data perwakilan Badan Hukum/Badan Usaha meliputi pemeriksaan akun Privy dan sertifikat elektronik Privy yang dimiliki oleh perwakilan Badan Hukum/Badan Usaha, yang telah mencakup pemeriksaan data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection* serta melakukan validasi data KTP perwakilan Badan Hukum/Usaha dengan melakukan pencocokan data dengan basis data kependudukan yang dikelola oleh pemerintah yang menyelenggarakan administrasi kependudukan;
b. Pemeriksaan NPWP dengan akta;

Privy CA will identify and authenticate of documents proviced by Legal Entity/Business Entity for the issuance of Certificates. The identification and authentication process carried out is as follows:

a. The examination and validation of the Legal Entity/Business Entity representative's data include verifying the Privy account and electronic certificate held by the representative, which entails biometric data verification through a self potrait subjected to liveness detection, as well as validating the representative's ID card (KTP) by matching the data with the population database managed by the government responsible for civil registration administration;
b. Examination of the Taxpayer Registration Number with the Deed;
c. Examination of the Deed of Establishment and/or the latest Amendment Deed of

c. Pemeriksaan akta pendirian dan/atau akta perubahan terakhir Badan Hukum/Badan Usaha beserta SK Kemenkumhamnya dengan membandingan informasi pada dokumen tersebut dengan informasi yang diterima dari basis data Instansi berwenang yang memberikan pengesahan Badan Hukum/Badan Usaha sesuai dengan ketentuan perundang-undangan.

the Legal Entity/Business Entity along with the MOLHR Decree, by comparing the information in said documents with the information received from the authorized institution's database that provides validation of Legal Entity/Business Entity in accordance with the provisions of the applicable laws and regulations.

Dalam hal proses identifikasi dan autentikasi permohonan Sertifikat Badan Hukum/Badan Usaha telah berhasil, PSrE Privy akan menerbitkan Sertifikat Level 3/ Kelas 4 bagi Badan Hukum/Badan Usaha tersebut.

In the event that the process of identification and authentication of the application for a Legal Entity/Business Entity has been successfully completed, Privy CA will issue a Level 3/Class 4 Certificate for the Legal Entity/Business Entity.

PSrE Privy menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi bagi organisasi setidaknya selama masa berlaku dari Sertifikat yang diterbitkan. PSrE Privy tidak menerbitkan Sertifikat bagi Pemohon yang tidak dapat diverifikasi.

Privy CA keeps a record of the type and details of the identification, which are used for authentication for the organization at least during the validity period of the Certificates issued. Privy CA does not issue Certificates to Applicants who cannot be verified.

3.2.3. Autentikasi Identitas Individu/Perorangan / *Individual Identity Authentication*

PSrE Privy dan/atau RA akan mengidentifikasi dan mengautentikasi permohonan Sertifikat yang diajukan oleh individu/perorangan berdasarkan kelas Sertifikat. PSrE Privy dapat menerbitkan Sertifikat untuk Pemohon Sertifikat dengan klasifikasi Sertifikat Level 2/ Kelas 3 dan Sertifikat Level 3/Kelas 4.

Privy CA and/or RA will identify and authenticate Certificate applications submitted by individuals based on the Certificate class. Privy CA may issue Certificates to Certificate Applicants with Level 2/Class 3 and Level3/Class 4 Certificate classifications.

Pemohon terdiri dari Warga Negara Indonesia (WNI) atau Warga Negara Asing (WNA). Berdasarkan ketentuan yang diatur oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik, untuk mendapatkan Sertifikat, Pemohon dalam hal ini WNI, diwajibkan untuk menunjukkan, membuktikan, dan memberikan hal-hal berikut:

a. Formulir pendaftaran Sertifikat;
b. Informasi data Nomor Induk Kependudukan (NIK), nama dan tanggal lahir (Data Demografi). Dalam mengumpulkan Data Demografi, PSrE Privy dapat

The Applicant consists of an Indonesian Citizen (WNI) or Foreign Citizen (WNA). Based on the provisions regulated by laws and regulations regarding the implementation of electronic certification, to obtain a Certificate, the Applicant, in this case an Indonesian citizen (WNI), is required to show, prove, and provide the following requirements:

a. Certificate registration form;
b. Information of the National Identification Number (NIK), full name and date of birth (Demographic Data). In collecting Demographic

memintakan secara langsung kepada Pemohon atau dapat memintakan salinan dokumen Kartu Tanda Penduduk (KTP) yang dikeluarkan oleh Pemerintah Indonesia untuk menjadi dasar pengumpulan Data Demografi Pemohon;

c. Nomor *handphone* dan/atau alamat surat elektronik; dan
d. Data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection*.

Data, Privy CA may request it directly from the Applicant or may request a copy of the Population Identity Card (KTP) issued by the Government of Indonesia as the basis for collecting the Applicant's Demographic Data;

c. Mobile phone number and/or email address; and
d. Biometric data in the form of selfies that have been tested for liveness detection using the liveness detection mechanism.

PSrE Privy dan/atau RA berkewajiban untuk memeriksa, melakukan validasi, dan memastikan bahwa informasi yang diberikan oleh Pemohon adalah valid dan autentik. Adapun proses validasi yang dilakukan antara lain dengan melakukan pencocokan Data Demografi dan biometrik berupa swafoto, dengan basis data kependudukan yang dikelola oleh lembaga pemerintah yang menyelenggarakan administrasi kependudukan.

Privy CA and/or RA are obliged to check, validate, and ensure that the information provided by the Applicant is valid and authentic. The validation process includes, among other things, matching the Applicant's Demographic Data and biometric data, such as a selfie, with the population database managed by the government agency responsible for population administration.

Apabila pencocokan data identitas dilakukan oleh PSrE

If identity data matching is carried out by Privy CA and/or

Privy dan/atau RA dengan melakukan pencocokan data pada basis data kependudukan yang ada di kementerian yang berwenang menyelenggarakan administrasi kependudukan secara nasional maka Sertifikat yang diterbitkan adalah Sertifikat Level 2/Kelas 3.

RA by matching data in the population database maintained by the relevant ministry responsible for national population administration, the issued Certificate will be a Level2/Class 3 Certificate.

Sementara untuk WNA, wajib memberikan:

a. Formulir pendaftaran Sertifikat;
b. Foto dokumen Paspor;
c. KTP atau Kartu Izin Tinggal Sementara (KITAS) yang dikeluarkan oleh Lembaga Kementerian Terkait;
d. Surat permohonan dari perusahaan yang ditandatangani oleh penanggung jawab perusahaan dimana Pemohon bekerja atau terafiliasi bagi Pemohon yang tidak memiliki KTP;
e. Data biometrik berupa swafoto yang telah diuji deteksi kehidupan dengan menggunakan mekanisme *liveness detection;*
f. Nomor telepon; dan
g. Alamat surat elektronik.

Meanwhile, for Foreign Citizen (WNA), the following must be provided:

a. Certificate registration form;
b. Photo of Passport document;
c. ID card (KTP) or Temporary Stay Permit Card (KITAS) issued by the relevant Ministry;
d. Application letter from the company signed by the person in charge of the company where the Applicant works or is affiliated for those who do not have an ID card (KTP);
e. Biometric data in the form of selfies that have undergone liveness detection using a liveness detection mechanism;
f. Phone number; and
g. Email address.

Dalam hal proses verifikasi dokumen dan identitas berhasil, PSrE Privy akan menerbitkan Sertifikat Level 2/Kelas 3 bagi WNA yang melampirkan KITAS sebagai dokumen identitas yang digunakan. Bagi WNA yang menggunakan KTP sebagai dokumen identitas yang digunakan, maka dapat diterbitkan Sertifikat Level 3/Kelas 4 oleh PSrE Privy.

In the event that the document and identitity verification process is successful, Privy CA will issue a Level 2/Class 3 Certificate for the Foreign Citizen (WNA) who provide a KITAS as their identification document. For Foreign Citizen (WNA) using an ID card (KTP) as their identification document, a Level 3/Class 4 Certificate may be issued by Privy CA.

PSrE Privy dan/atau RA juga harus memeriksa dan melakukan validasi terhadap informasi lainnya yang telah diterima dari Pemohon untuk mendeteksi kebenaran dan keasliannya serta mencari jika ada perubahan dan/atau pemalsuan terhadap informasi-informasi lainnya tersebut.

Privy CA and/or RA must also check and validate other information that has been received from the Applicant to detect its validity and authenticity and look for any changes and/or falsification of such other information.

PSrE Privy menyimpan catatan tentang jenis dan rincian dari identifikasi yang digunakan untuk autentikasi individu/perorangan setidaknya selama masa berlaku dari Sertifikat yang diterbitkan. PSrE Privy tidak menerbitkan Sertifikat bagi Pemohon yang tidak dapat diverifikasi.

Privy CA keeps a record of the type and details of identification, which are used for authentication for the individual at least during the validity period of the Certificates issued. Privy CA does not issue Certificates to Applicants who cannot be verified.

3.2.4. Informasi Pemegang Sertifikat yang Tidak Terverifikasi / *Non-Verified Subscriber Information*

PSrE Privy tidak menerbitkan Sertifikat untuk Pemohon Sertifikat yang informasinya tidak dapat diverifikasi dan diautentikasi sesuai bagian 3.2.3. diatas.	Privy CA does not issue Certificates to Certificate Applicants whose information cannot be verified and authenticated in accordance with section 3.2.3. above.

3.2.5. Validasi Otoritas / *Validation of Authority*

PSrE Privy dan/atau RA menggunakan upaya yang wajar dan andal untuk memeriksa keautentikan informasi Pemohon terhadap permohonan yang diajukan untuk Sertifikat yang dibuat dengan atas nama Badan Hukum/Badan Usaha.	Privy CA and/or RA use reasonable and reliable efforts to check the authenticity of the Applicant's information against the application submitted for Certificates made on behalf of Legal Entities/Business Entities.

3.2.6. Kriteria Inter-operasi / *Criteria of Interoperation*

Tidak ada ketentuan.	No Stipulation.

3.3. Identifikasi dan Autentikasi untuk Permintaan *Re-key* / *Identification and Authentication for Re-key Requests*

3.3.1. Identifikasi dan Autentikasi untuk *Re-key* Rutin / *Identification and Authentication for Routine Re-key*

Privy akan mengirimkan pemberitahuan untuk perpanjangan masa berlaku Sertifikat kepada Pemegang Sertifikat 40 (empat puluh) hari kalender sebelum masa berlaku berakhir. Sebelum masa berlaku Sertifikat berakhir, Pemegang Sertifikat dapat mengajukan	Privy will send a notification for the extension of the Certificate's validity to the Subscriber 40 (forty) calendar days before the expiration date. Before the Certificate expires, the Subscriber may submit a request for a key replacement (re-key), provided that Privy CA

permohonan pergantian kunci (*re-key*) dengan ketentuan bahwa PSrE Privy akan menerbitkan pasangan kunci baru dan menerbitkan Sertifikat baru, dengan masa validitas baru. PSrE Privy meminta Pemegang Sertifikat untuk melakukan autentikasi Pemegang Sertifikat menggunakan Sertifikat yang masih berlaku.

will issue a new key pair and issue a new Certificate, with a new validity period. Privy CA require the Subscriber to authenticate themselves using the valid Certificate.

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

Dalam hal Sertifikat telah dicabut dan/atau telah kedaluwarsa, Pemegang Sertifikat harus mengulang proses pendaftaran untuk selanjutnya dilakukan verifikasi oleh PSrE Privy sebagaimana diatur pada bagian 3.2 untuk selanjutnya diterbitkan Sertifikat baru dengan kunci dan validitas baru.

In the event that the Certificate has been revoked and/or has expired, the Subscriber must repeat the registration process, which will subsequently be verified by Privy CA as outlined in Section 3.2, in order to issue a new Certificate with a new key and validity period.

3.4. Identifikasi dan Autentikasi untuk Permohonan Pencabutan / *Identification and Authentication for Revocation Requests*

Permohonan untuk mencabut Sertifikat dapat diajukan atas dasar risiko kebocoran kunci maupun alasan lainnya oleh Pemegang Sertifikat dengan menghubungi Privy melalui kontak yang tertera pada Situs

Requests to revoke the Certificate can be submitted on the basis of the risk of key leakage or other reasons by the Subscriber by contacting Privy through the contact listed on the Site and proving the

dan membuktikan penguasaan terhadap informasi data Pemegang Sertifikat yang disimpan oleh Privy. Dalam hal permohonan pencabutan untuk Sertifikat individu WNI dan/atau WNA, maka PSrE Privy meminta data username Privy, alasan pencabutan, dan waktu terakhir kali Pemilik menggunakan akun Privy. Dalam hal permohonan pencabutan dilakukan terhadap Sertifikat Badan Usaha maka PSrE Privy akan memastikan bahwa pihak yang melakukan permohonan adalah pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut. PSrE Privy akan melakukan verifikasi data dengan mengajukan beberapa pertanyaan. PSrE Privy dapat meminta syarat tambahan jika diperlukan untuk melakukan autentikasi permohonan pencabutan Sertifikat.

possesion of the Subscriber's data information stored by Privy. In the case of a revocation request for an Individual Certificate for WNI and/or Foreign Citizen (WNA), Privy CA request the Privy username, reason for revocation, and the last time the Subscriber used their Privy account. In the event that the revocation request is made for the Business Entity Certificate, Privy CA will ensure that the request is made by those who have the authority to represent the Business Entity, namely the highest leader or President Director of the Business Entity or this can be submitted by a third party representing the Business Entity whose authority can be proven by a power of attorney signed by the highest leader or President Director of the Business Entity. Privy CA will verify the data by asking several questions. Privy CA may request additional requirements if necessary to authenticate the Certificate revocation request.

4. Persyaratan Operasional Siklus Sertifikat / *Certificate Life-Cycle Operational Requirements*

4.1. Permohonan Sertifikat / *Certificate Application*

4.1.1. Pihak yang dapat Mengajukan Permohonan Sertifikat / *Parties Eligible to Submit Certificate Applications*

Pihak yang dapat mengajukan permohonan penerbitan Sertifikat adalah orang dan/atau Badan Hukum/Badan Usaha.	Those who can apply for Certificate issuance are persons and/or Legal Entities/Business Entities.
Orang yang dapat mengajukan permohonan penerbitan Sertifikat adalah warga negara Indonesia atau warga negara asing dan hanya dapat dilakukan oleh individu tersebut, sedangkan untuk Badan Hukum atau Badan Usaha harus terdaftar sebagai Badan Hukum atau Badan Usaha yang sah di Indonesia dan dilakukan oleh pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut.	Persons who can apply for the issuance of Certificates are Indonesian citizens or foreign citizens and it can only be carried out by the individual, while for Legal Entities or Business Entities, they must be registered as Legal Entities or Legal Business Entities in Indonesia and it is carried out those who have the authority to represent the Business Entity.

4.1.2. Proses Pendaftaran dan Tanggung jawabnya / *Enrollment Process and Responsibilities*

Berikut merupakan langkah yang dilakukan untuk memperoleh Sertifikat: a. Mengisi formulir pendaftaran yang secara lengkap beserta dengan dokumen lain yang dibutuhkan sesuai dengan ketentuan pada bagian 3.2.	The following are the steps that must be taken to obtain a Certificate: a. Fill the registration form along with other required documents in accordance with the provisions in section 3.2. to Privy CA

kepada PSrE Privy dan/atau RA. Pemohon berkewajiban untuk memberikan data dan informasi yang tepat, benar, dan jelas;

b. Setuju terhadap Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, serta Pemberitahuan Privasi Privy yang berlaku;
c. Membayar biaya Sertifikat dan biaya penggunaannya (apabila berlaku);
d. Menunggu validasi serta verifikasi identitas dari PSrE Privy dan/atau RA; dan
e. Jika validasi dan verifikasi gagal dilakukan, PSrE Privy dan/atau RA dapat meminta data dan informasi tambahan kepada Pemohon.

Validasi dan verifikasi dilakukan berdasarkan permohonan kelas Sertifikat yang diajukan oleh Pemohon. Jika validasi dan verifikasi berhasil, Sertifikat kemudian diterbitkan.

Dalam rangka memproses penerbitan Sertifikat, RA memiliki tanggung jawab sebagai berikut:

and/or RA. The applicant is obliged to provide accurate, correct and clear data and information;

b. Agree to the applicable Subscriber Agreement, Terms and Conditions, and Privy Privacy Notice;
c. Pay the Certificate fee and usage fee (if applicable);
d. Wait for validation and identity verification from Privy CA and/or RA; and
e. If the validation and verification is failed, Privy CA and/or RA may request additional data and information from the Applicant.

Validation and verification are carried out based on the Certificate class application submitted by the Applicant. If validation and verification are successful, the Certificate is then issued.

In order to process the issuance of Certificates, RA has the following responsibilities:

a. To check the registration form along with the

a. Memeriksa formulir pendaftaran beserta dengan dokumen tambahan yang dikirimkan oleh Pemohon adalah benar, jelas dan tepat, berikut dengan data dan informasi pendukungnya;
b. Memastikan bahwa jalur komunikasi yang digunakan antara Pemohon, RA, dan PSrE Privy untuk menghimpun dan menyalurkan informasi yang dibutuhkan untuk memenuhi kebutuhan pendaftaran adalah jalur komunikasi yang aman;
c. Mengirimkan informasi dan/atau dokumen yang dibutuhkan oleh PSrE Privy sebagaimana disebutkan pada bagian 3.2 untuk kebutuhan pemenuhan terhadap peraturan perundang-undangan; dan
d. Menyimpan informasi dan/atau dokumen yang telah diberikan oleh Pemohon dengan aman.

Setelah menerima permohonan penerbitan Sertifikat tersebut, PSrE Privy dan/atau RA akan menjalankan validasi dan verifikasi sebagaimana yang

additional documents submitted by the Applicant are correct, clear and accurate, along with the supporting data and information;
b. To ensure that the communication channel used between the Applicant, RA, and Privy CA to collect and distribute information needed to fulfill the registration requirements is a secure communication channel;
c. To send information and/or documents needed by Privy CA in section 3.2 for the needs of compliance with laws and regulations; and
d. To securely store information and/or documents that have been provided by the Applicant.

Upon receiving the Certificate issuance request, Privy CA and/or RA will carry out validation and verification as set out in section 3.2. above. In the

telah diatur di bagian 3.2. di atas. Dalam hal RA menerima permohonan penerbitan Sertifikat dan telah melakukan validasi dan verifikasi terhadap permohonan tersebut, maka RA akan melanjutkan permohonan penerbitan Sertifikat ke PSrE Privy.

event that RA receives the Certificate issuance application and has performed validation and verification of the application, RA will forward the Certificate issuance application to Privy CA.

Setelah validasi dan verifikasi dinyatakan berhasil oleh RA, maka PSrE Privy bertanggung jawab untuk menerbitkan Sertifikat Pemohon setelah seluruh syarat penerbitan Sertifikat lainnya terpenuhi dan menyimpan informasi terkait dengan proses pendaftaran Pemohon sebagaimana diatur di dalam peraturan perundang-undangan.

After the examination and validation is declared successful by the RA, Privy CA is responsible for issuing the Applicant Certificate after all other Certificate issuance requirements are met and storing information related to the Applicant registration process as stipulated in the laws and regulations.

PSrE Privy dan/atau RA akan melakukan upaya yang wajar untuk memastikan bahwa Pemohon Sertifikat memberikan data dan informasi yang valid dan autentik. Pemohon Sertifikat harus melalui proses registrasi sebagaimana yang dicantumkan di dalam CPS ini sebelum permohonan penerbitan Sertifikat diterima. PSrE Privy dan/atau RA memiliki wewenang

Privy CA and/or RA will make reasonable efforts to ensure that Certificate Applicants provide valid and authentic data and information. The Certificate Applicant must go through the registration process as stated in this CPS before the Certificate issuance application is accepted. Privy CA and/or RA have the authority to reject an application for Certificate

untuk menolak permohonan penerbitan Sertifikat jika ada data dan informasi yang kurang dan/atau tidak benar. Sertifikat hanya dapat diterbitkan jika Pemohon menyetujui Perjanjian Pemegang Sertifikat dan Pemberitahuan Privasi.

issuance if there is missing and/or incorrect data and information. The Certificate can only be issued if the Applicant agrees to the Subscriber Agreement and Privacy Notice.

4.2. Pemrosesan Permohonan Sertifikat / *Certificate Application Processing*

4.2.1. Melaksanakan fungsi Identifikasi dan Autentikasi / *Performing the Identification and Authentication functions*

PSrE Privy dan/atau RA dapat menggunakan data dan informasi yang diajukan oleh Pemohon untuk mengautentikasi dan memeriksa identitas pemohon sebagaimana diatur dalam bagian 3.2 dari CPS ini.

Privy CA and/or RA may use the data and information submitted by the Applicant to authenticate and check the identity of the applicant as stipulated in section 3.2. of this CPS.

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

PSrE Privy dan/atau RA hanya akan memberikan persetujuan terhadap permohonan penerbitan Sertifikat apabila telah memenuhi kriteria yang disebutkan di bagian 4.1.

Privy CA and/or RA will only approve the Certificate issuance application if it meets the criteria mentioned in section 4.1.

Dalam hal Pemohon tidak berhasil memenuhi kriteria tersebut maka Privy dan/atau RA memiliki kewenangan berikut:

In the event that the Applicant fails to meet these criteria, the Privy and/or RA has the following authorities:

a. To reject the application for

a. Menolak permohonan penerbitan Sertifikat Pemohon; dan/atau
b. Meminta informasi tambahan kepada Pemohon agar dapat memenuhi kriteria yang dibutuhkan.

issuance of the Applicant Certificate; and/or
b. To request additional information from the Applicant in order to fulfill the required criteria.

4.2.3. Waktu untuk Memproses Permohonan Sertifikat / *Certificate Application Processing Time*

PSrE Privy memastikan bahwa proses permohonan penerbitan Sertifikat dilakukan selambatnya dalam jangka waktu 3 x 24 jam setelah semua rincian dan dokumen yang diperlukan dari Pemohon diterima oleh PSrE Privy.

Privy CA ensures that the Certificate issuance application process is carried out at the latest within 3 x 24 hours after all the necessary details and documents from the Applicant are received by Privy CA.

4.3. Penerbitan Sertifikat / *Certificate Issuance*

Setelah menerima permohonan penerbitan Sertifikat, PSrE Privy akan menanggapi sesuai dengan persyaratan yang ditetapkan dalam CPS.

Upon receiving a request for Certificate issuance, Privy CA must respond according to the requirements set out in the CPS.

4.3.1. Tindakan PSrE Privy selama Penerbitan Sertifikat / *Privy CA Actions during Certificate Issuance*

Setelah menerima permohonan penerbitan Sertifikat, PSrE Privy melakukan tindakan-tindakan sebagai berikut:
a. Melakukan verifikasi dan validasi atas dokumen dan identitas yang diberikan oleh

After receiving the Cerificate issuance application, Privy CA shall undertake the following action:
a. Conduct verification and validation of the documents and identity provided by

Pemohon atau melalui RA sebagaimana diatur dalam bagian 3.2.2 dan 3.2.3;

b. Dalam hal permohonan diajukan untuk Badan Hukum/Badan Usaha, PSrE Privy memverifikasi otoritas yang melakukan Permohonan sesuai dalam bagian 3.2.5;
c. Melakukan verifikasi sumber permohonan Sertifikat sebelum diterbitkan;
d. Mempersiapkan bahwa Pemegang Sertifikat menerima sertifikat sebagaimana diatur pada bagian 4.4;
e. Membuat Sertifikat tersedia bagi Pemegang Sertifikat setelah Pemegang Sertifikat menyetujui kewajibannya menurut CPS ini.

the Applicant or through the RA, as stipulated in sections 3.2.2 and 3.2.3;

b. In the event an application is submitted for a Legal Entity/Business Entity, Privy CA verifies the authority submitting the Application as stipulated in section 3.2.5;
c. Verify the source of Certificate requests prior to issuance;
d. Ensure that the Subscriber receives the Certificate as stipulated in section 4.4;
e. Make the Certificate available to the Subscriber once the Subscriber has agreed to their obligations under this CPS.

4.3.1.1. Tindakan RA selama Penerbitan Sertifikat / *RA Actions during Certificate Issuance*

Setelah melakukan verifikasi dan validasi sebagaimana diatur dalam bagian 3.2.2, 3.2.3, dan 3.2.5, RA kemudian meneruskan permohonan penerbitan Sertifikat kepada PSrE Privy beserta dengan informasi pendaftaran Pemohon yang wajib disimpan oleh PSrE Privy

After conducting verification and validation as stipulated in sections 3.2.2, 3.2.3, and 3.2.5, RA subsequently forwards the Certificate issuance request to the Privy CA, along with the Applicant's registration information, which is required to be retained by Privy CA as

sebagaimana dijelaskan pada bagian 4.1. RA wajib memastikan bahwa Pemegang Sertifikat menerima Sertifikat sebagaimana diatur dalam bagian 4.4.

elucidated in section 4.1. RA is obligated to ensure that the Subscriber receives the Certificate as prescribed in section 4.4.

4.3.2. Pemberitahuan ke Pemegang Sertifikat oleh PSrE Privy tentang Penerbitan Sertifikat / *Notification to Subscribers by Privy CA on Certificate Issuance*

Segera setelah Sertifikat diterbitkan, maka PSrE Privy memberitahu Pemohon Sertifikat bahwa permohonan Sertifikat telah disetujui melalui email dan/atau nomor telepon Pemohon yang terdaftar, paling lambat dalam jangka waktu 3 (tiga) jam. Privy memberitahukan kepada Pemohon Sertifikat bahwa mereka tidak dapat menggunakan Sertifikat sebelum melakukan pemeriksaan atas semua informasi dalam Sertifikat.

As soon as the Certificate is issued, Privy CA notifies the Certificate Applicant that the Certificate application has been approved via email and/or the Applicant's registered telephone number, no later than within 3 (three) hours. Privy will inform the Certificate Applicant that they cannot use the Certificate until they have verified all information contained in the Certificate.

4.4. Pernyataan Persetujuan / *Certificate Acceptance*

4.4.1. Sikap yang Dianggap sebagai Menyetujui Sertifikat / *Actions Deemed as Certificate Approval*

Pemohon dianggap telah menerima dan menyetujui Sertifikat setelah pemberitahuan kepada Pemohon sesuai bagian 4.3.2.

The Applicant is deemed to have received the Certificate upon notification to the Applicant in accordance with section 4.3.2.

Bentuk penerimaan dan persetujuan dari Pemohon adalah apabila Pemohon telah menggunakan Sertifikat Elektronik yang telah diterbitkan oleh PSrE Privy atau dalam jangka waktu 7 (tujuh) hari kerja Pemegang Sertifikat tidak menyampaikan keluhan terhadap informasi yang tertera pada Sertifikat tersebut (yang mana salah satu dari dua keadaan tersebut terjadi terlebih dahulu), maka Pemegang Sertifikat dianggap telah menerima dan menyetujui semua informasi yang tertera pada Sertifikat.	The acceptance and approval from the Applicant is indicated by the Applicant's use of the Electronic Certificate issued by Privy CA, or if within 7 (seven) working days, the Subscriber does not submit a complaint about the information stated on the Certificate (whichever of these two conditions occurs first), the Subscriber is deemed to have accepted and approved all the information stated on the Certificate.
Apabila Pemegang Sertifikat memiliki keluhan terhadap informasi yang tertera pada Sertifikat, maka Pemegang Sertifikat dapat mengajukan permohonan pencabutan Sertifikat sesuai ketentuan yang diatur pada bagian 4.9. melalui media komunikasi yang disediakan dan ditentukan oleh PSrE Privy.	If the Subscriber has a complaint about the information contained in the Certificate, the Subscriber can submit a Certificate revocation request in accordance with the provisions set out in section 4.9. through the communication media provided and determined by Privy CA.

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

PSrE Privy mempublikasikan Sertifikat PSrE Privy dalam	Privy CA publishes Privy CA Certificates in a Repository which is accessible through the

Repositori yang dapat diakses melalui Situs Privy.	Privy Website.
PSrE Privy tidak mempublikasikan Sertifikat Pengguna Akhir.	Privy CA does not publish end user Certificates.

4.4.3. Pemberitahuan Sertifikat oleh PSrE Privy kepada Pihak Lain / *Notification of Certificate Issuance by CA Privy to Other Parties*

RA dapat menerima pemberitahuan terhadap penerbitan suatu Sertifikat apabila RA terlibat dalam proses penerbitan Sertifikat tersebut.	RA may receive notification of the issuance of a Certificate if RA was involved in the process of the issuance of the Certificate.

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

4.5.1. Penggunaan Kunci Privat dan Sertifikat oleh Pemegang Sertifikat / *Subscriber's Private Key and Certificate Usage*

PSrE Privy melindungi Kunci Privatnya dari penggunaan tanpa izin atau atas pengungkapan oleh pihak lain dengan menggunakan HSM milik PSrE Privy.	Privy CA safeguards its Private Keys against unauthorized use or disclosure by third parties through the use of its Hardware Security Module (HSM).
Pemegang Sertifikat menitipkan Kunci Privatnya kepada PSrE Privy, sesuai dengan persetujuan berdasarkan Perjanjian Pemegang Sertifikat dengan PSrE Privy, maka PSrE Privy akan mengamankan Kunci Privat tersebut menggunakan perangkat dengan spesifikasi minimal FIPS 140-2 Level 2.	The Subscriber entrusts the Private Key to Privy CA, in accordance with the agreement based on the Subscriber Agreement with Privy CA, thus Privy CA will store the Private Key using an equipment with a minimum specification of FIPS 140-2 Level 2.

PSrE Privy melakukan upaya-upaya pengamanan dan penyimpanan dengan penuh kehati-hatian terhadap Kunci Privat Pemegang Sertifikat agar Kunci Privat tersebut hanya dapat digunakan oleh Pemegang Sertifikat. PSrE Privy telah menerapkan 2 faktor autentikasi bagi Pemegang Sertifikat yang akan menggunakan Kunci Privatnya. Pemegang Sertifikat melindungi parameter autentikasi yang digunakan untuk mengaktifkan Kunci Privatnya. Pemegang Sertifikat hanya memakai Kunci Privatnya untuk tujuan yang sudah ditentukan.

Privy CA undertakes diligent security and storage measures for the Subscriber's Private Key to ensure that the Private Key can only be used by the Subscriber. Privy CA has implemented two-factor authentication for the Subscriber who will use their Private Key. The Subscriber is responsible for protecting the authentication parameters used to activate their Private Key. The Subscriber shall only use their Private Key for the specified purposes.

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

Dalam mengandalkan Sertifikat yang diterbitkan oleh PSrE Privy, Pengandal memberikan jaminan dan pernyataan sesuai ketentuan yang diatur pada 9.6.4.

In relying on the Certificate issued by Privy CA, the Relying Party provides warranties and representations in accordance with the provisions set out in 9.6.4.

Pengandal dapat mengakses *Public Key Certificate* Privy melalui Repositori Privy.

The Relying Party can access Privy's Public Key Certificate through the Privy's Repository.

4.6. Pembaruan Sertifikat / *Certificate Renewal*

PSrE Privy tidak melakukan Pembaruan Sertifikat.	Privy CA does not perform Certificate Renewal.

4.6.1. Kondisi untuk Pembaruan Sertifikat / *Circumstances for Certificate Renewal*

Tidak ada ketentuan.	No Stipulation.

4.6.2. Pihak yang Dapat Mengajukan Pembaruan Sertifikat / *Parties Eligible to Submit Certificate Renewal Requests*

Tidak ada ketentuan.	No Stipulation.

4.6.3. Pemrosesan Permohonan Pembaruan Sertifikat / *Processing Certificate Renewal Requests*

Tidak ada ketentuan.	No Stipulation.

4.6.4. Pemberitahuan Penerbitan Sertifikat Baru ke Pemegang Sertifikat / *Notification of New Certificate Issuance to Subscribers*

Tidak ada ketentuan.	No Stipulation.

4.6.5. Sikap yang Dianggap sebagai Penerimaan Pembaruan Sertifikat / *Conduct Constituting Acceptance of a Renewal Certificate*

Tidak ada ketentuan.	No Stipulation.

4.6.6. Publikasi Pembaruan Sertifikat oleh Privy / *Publication of the Renewal Certificate by Privy*

Tidak ada ketentuan.	No Stipulation.

4.6.7. Pemberitahuan Pembaruan Sertifikat oleh Privy kepada Pihak Lain / *Notice of Certificate Renewal by Privy to Other Parties*

Tidak ada ketentuan.	No Stipulation.

4.7. *Re*-key Sertifikat / *Certificate Re-key*

Re-key merupakan proses dimana Pemegang Sertifikat	Re-key is the process by which a Subscriber applies for the

mengajukan penerbitan Sertifikat baru untuk menggantikan Sertifikat lamanya yang akan menghasilkan pasangan kunci yang baru dan masa validitas yang baru.

issuance of a new Certificate to replace its old Certificate which will result in a new key pair and a new validity period.

4.7.1. Kondisi untuk *Re-key* Sertifikat / *Circumstances for Certificate Re-key*

Re-key Sertifikat dapat dilakukan selama:

a. Sertifikat lama yang akan diganti belum dicabut, terkompromi, atau kedaluwarsa;
b. Pemegang Sertifikat telah memberikan persetujuan untuk pembangkitan Pasangan Kunci dan penerbitan Sertifikat baru; atau
c. Semua rincian dalam Sertifikat tetap akurat dan tidak memerlukan validasi baru atau tambahan validasi.

Certificate Re-keying can be carried out under the following conditions:

a. The old certificate to be replaced has never been revoked, compromised, or expired;
b. The Subscriber has provided consent for the generation of a Key Pair and the issuance of a new Certificate; or
c. All details associated with the Certificate are still accurate and do not require any new or additional validation.

Apabila Kunci Privat Pemilik terkompromi, Sertifikat kedaluwarsa atau dicabut dan terdapat perubahan rincian, maka Pemegang Sertifikat dapat mengajukan permohonan penerbitan Sertifikat baru sebagaimana diatur pada bagian 4.1.

If the Private Key of the Subscriber has been compromised, the Certificate has expired or been revoked, or if there are changes to the details, the Subscriber may apply for the issuance of a new Certificate as outlined in section 4.1.

4.7.2. Pihak yang dapat Mengajukan *Re-key* Sertifikat / *Parties Eligible to Submit Certificate Re-key Requests*

Pemegang Sertifikat dapat mengajukan *re-key* Sertifikat. Dalam hal pembaruan Sertifikat yang diajukan adalah untuk Sertifikat Badan Usaha, maka permohonan hanya dapat diajukan pihak yang memiliki wewenang untuk mewakili Badan Usaha tersebut yaitu pimpinan tertinggi atau Direktur Utama dari Badan Usaha tersebut ataupun dapat diajukan oleh pihak ketiga yang mewakili Badan Usaha yang wewenangnya dapat dibuktikan dengan surat kuasa yang ditandatangani oleh pimpinan tertinggi atau Direktur Utama Badan Usaha tersebut dengan menghubungi Privy melalui kontak yang tertera pada Situs, lalu PSrE Privy akan melakukan verifikasi data dengan mengajukan beberapa pertanyaan untuk membuktikan wewenang pihak yang memohon pembaruan Sertifikat Badan Usaha tersebut.	The Subscriber may request for a Certificate re-key. In the event that the proposed Certificate renewal is for a Business Entity Certificate, the application can only be submitted by a party who has the authority to represent the Business Entity, namely the highest leader or President Director of the Business Entity or can be submitted by a third party representing the Business Entity whose authority can be proven by a power of attorney signed by the highest leader or President Director of the Business Entity by contacting Privy through the contact listed on the Website, then Privy CA will verify the data by asking a few questions to prove the authority of the party requesting the renewal of the Business Entity Certificate.

4.7.3. Pemrosesan Permohonan *Re-key* Sertifikat / *Processing Certificate Re-keying Requests*

Prosedur *re-key* Sertifikat adalah sebagaimana ditentukan pada bagian 4.3 dan 3.3.	The Certificate re-keying procedure is as specified in sections 4.3 and 3.3.

Dalam melakukan *re-key*, PSrE Privy menggunakan masa berlaku baru bagi Sertifikat baru yang diterbitkan.	In carrying out the re-key process, Privy CA will assign a new validity period to the newly issued Certificate.

4.7.4. Pemberitahuan Penerbitan *Re-key* Sertifikat ke Pemegang Sertifikat / *Notification of Certificate Re-key Issuance to Subscribers*

Setelah *re-key* Sertifikat berhasil dilakukan, maka PSrE Privy akan memberitahukan Pemohon Sertifikat bahwa penerbitan Sertifikat telah berhasil dilakukan melalui *email* dan/atau nomor telepon Pemohon yang terdaftar, selambatnya dalam jangka waktu 3 (tiga) jam dengan merujuk ke bagian 4.3.2.	After the Certificate re-keying is successfully carried out, Privy CA will notify the Certificate Applicant that the Certificate issuance has been successfully carried out via email and/or the Applicant's registered telephone number, no later than within 3 (three) hours by referring to section 4.3.2.

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

Pemegang Sertifikat dianggap telah menerima Sertifikat hasil *re-key* ketika pemberitahuan sebagaimana ditentukan pada bagian 4.7.4 telah diterima oleh Pemegang Sertifikat dengan merujuk ke bagian 4.4.1.	The Subscriber is deemed to have received the rekeyed Certificate when the notificiation specified in section 4.7.4 has been received by the Subscriber with reference to section 4.4.1.

4.7.6. Publikasi *Re-key* Sertifikat oleh Privy / *Publication of the Re-key Certificate by Privy*

Privy akan melakukan publikasi sertifikat sesuai dengan ketentuan yang diatur pada Bagian 4.4.2.	Privy will publish the re-keyed Certificate in accordance with the provisions outlined in section 4.4.2.

4.7.7. Pemberitahuan Sertifikat *Re-key* oleh Privy / *Notification of Re-key Certificate by Privy*

Tidak ada ketentuan.	No Stipulation.

4.8. Modifikasi Sertifikat / *Certificate Modification*

PSrE Privy tidak melakukan modifikasi Sertifikat. Apabila terjadi kesalahan dalam penerbitan Sertifikat, maka PSrE Privy melakukan pencabutan Sertifikat dan menerbitkan Sertifikat baru yang sesuai dengan ketentuan yang diatur pada CPS ini.	Privy CA does not modify the Certificate. If there is an error in the issuance of the Certificate, Privy CA revokes the Certificate and issues a new Certificate in accordance with the provisions stipulated in this CPS.

4.8.1. Keadaan yang Menyebabkan Modifikasi Sertifikat / *Circumstances of Certificate Modification*

Tidak ada ketentuan.	No Stipulation.

4.8.2. Pihak yang Dapat Mengajukan Permohonan Modifikasi Sertifikat / *Parties Eligible to Submit Certificate Modification Requests*

Tidak ada ketentuan.	No Stipulation.

4.8.3. Pemrosesan Permohonan Modifikasi Sertifikat / *Processing of Certificate Modification Requests*

Tidak ada ketentuan.	No Stipulation.

4.8.4. Pemberitahuan Sertifikat Baru ke Pemegang Sertifikat / *Notification of New Certificate to Subscribers*

Tidak ada ketentuan.	No Stipulation.

4.8.5. Sikap yang dianggap sebagai Penerimaan Modifikasi Sertifikat / *Actions Deemed as Acceptance of Certificate Modification*

Tidak ada ketentuan.	No Stipulation.

4.8.6. Publikasi Sertifikat yang Dimodifikasi oleh PSrE Privy / *Publication of Modified Certificate by Privy CA*

Tidak ada ketentuan.	No Stipulation.

4.8.7. Pemberitahuan Penerbitan Sertifikat oleh PSrE Privy ke Pihak Lain / *Notification of Certificate Issuance by Privy CA to Other Parties*

Tidak ada ketentuan.	No Stipulation.

4.9. Pencabutan dan Pembekuan Sertifikat / *Certificate Revocation and Suspension*

4.9.1. Keadaan yang Menyebabkan Pencabutan Sertifikat / *Circumstances of Certificate Revocation*

PSrE Privy melakukan pencabutan Sertifikat untuk hal-hal berikut ini: a. Ketika Pemegang Sertifikat atau pihak ketiga lainnya yang berwenang mengajukan permohonan pencabutan Sertifikat; b. Ketika Kunci Privat terkompromi, hilang, dan/atau rusak; c. Ketika terjadi perubahan standar industri, kebijakan pemerintah, dan/atau peraturan perundang-undangan yang mempengaruhi keabsahan Sertifikat. d. Ketika informasi yang tertera di dalam Sertifikat tidak akurat atau menyesatkan;	Privy CA revokes the Certificate for the following reasons: a. When the Subscriber or other third parties with authority applies for Certificate revocation; b. When the Private Key is compromised, lost, and/or corrupted; c. When there are changes in industry standards, government policies, and/or laws and regulations that affect the validity of the Certificate; d. When the information contained in the Certificate is inaccurate or misleading; e. When an application for Certificate issuance is made illegally; f. When Certificate issuance is

e. Ketika permohonan penerbitan Sertifikat dilakukan secara secara tidak sah;
f. Ketika penerbitan Sertifikat dilakukan secara tidak sesuai dengan ketentuan yang tercantum di dalam CPS;
g. Ketika Pemegang Sertifikat melanggar ketentuan yang tercantum di dalam CPS atau Perjanjian Pemegang Sertifikat;
h. Ketika Sertifikat Privy mengalami kebocoran;
i. Ketika Privy berhenti beroperasi;
j. Alasan lainnya yang menurut Privy dibenarkan untuk melakukan pencabutan Sertifikat; atau
k. Pemegang Sertifikat sudah tidak bisa lagi menggunakan Sertifikat.

not carried out in accordance with the provisions stated in the CPS;
g. When the Subscriber violates the terms of the CPS or Subscriber Agreement;
h. When the Privy Certificate has a leak;
i. When Privy stops operating;
j. Other reasons that Privy considers justified to revoke the Certificate; or
k. The Subscriber can no longer use the Certificate.

4.9.2. Pihak yang dapat Mengajukan Pencabutan Sertifikat / *Parties Eligible to Submit Certificate Revocation Requests*

Pencabutan Sertifikat hanya dapat dilakukan oleh subjek yang terkait dengan Sertifikat tersebut, dalam hal ini Pemegang Sertifikat, atau kuasanya, dapat mengajukan pencabutan Sertifikat untuk Sertifikatnya.

Certificate Revocation can only be carried out by the subject to whom the Certificate relates, in which case the Subscriber, or his/her proxy, can apply for Certificate Revocation for his/her Certificate.

Pihak ketiga yang berwenang mengajukan permohonan pencabutan harus dapat membuktikan wewenang tersebut berdasarkan kuasa dari Pemegang Sertifikat untuk melakukan pencabutan sertifikat dan/atau wewenangnya berdasarkan peraturan perundang-undangan yang berlaku.	Third parties who can apply for revocation must be able to prove that they are authorized by the Subscriber to revoke the certificate and/or their authority under applicable laws and regulations.
Dalam hal ketentuan yang tercantum pada bagian 4.9.1. terpenuhi, maka PSrE Privy juga dapat melakukan Pencabutan Sertifikat tanpa permintaan pencabutan oleh Pemegang Sertifikat.	In the event that the conditions listed in section 4.9.1. are met, Privy CA can also revoke the Certificate without a revocation request by the Subscriber.

4.9.3. Prosedur Pengajuan Pencabutan Sertifikat / *Procedure for Revocation Request*

PSrE Privy memverifikasi identitas sebelum dilakukan pencabutan Sertifikat sebagaimana bagian 3.4. Sertifikat yang telah dicabut masuk kedalam daftar CRL dan OCSP.	Privy CA verifies identity prior to Certificate revocation in accordance with section 3.4. Revoked certificates shall be listed in the CRL and OCSP lists.
Dalam mengajukan permintaan pencabutan Sertifikat, Pemegang Sertifikat harus menyerahkan bukti yaitu:	In submitting a Certificate revocation request, the Subscriber must obligate to provide evidence, namely: a. The Private Key of the

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Terdapat alasan relevan lain yang diberikan oleh Pemegang Sertifikat.

Certificate has been compromised;
b. The usage of the Certificate is not in accordance with the CPS; or
c. There is another relevant reasons provided by the Subscriber.

Permintaan pencabutan Sertifikat oleh pihak ketiga harus disertai dengan kuasa pencabutan Sertifikat. Pihak ketiga juga menyerahkan bukti yaitu:

a. Kunci Privat Sertifikat telah terungkap;
b. Penggunaan Sertifikat tidak sesuai dengan CPS; atau
c. Pemegang Sertifikat sudah tidak terasosiasi dengan pihak ketiga tersebut.

Requests for Certificate revocation by third parties must be accompanied by a power of attorney for such Certificate revocation. The third party must also submit the following evidence:

a. The Certificate Private Key has been revealed;
b. The usage of the Certificate is not in accordance with the CPS; or
c. The Subscriber is no longer associated with the third party.

Setelah dilakukan pencabutan, Pemegang Sertifikat dapat mengajukan penerbitan Sertifikat Baru. Proses Penerbitan Sertifikat Baru akan mengikuti ketentuan pada bagian 3.2.5 dan 4.1. hingga 4.4.

After revocation, the Subscriber may apply for issuance of a New Certificate. The New Certificate Issuance process will be in accordance with the provisions in sections 3.2.5 and 4.1. to 4.4.

4.9.4. Tenggang Waktu Permohonan Pencabutan / *Revocation Request Grace Period*

PSrE Privy tidak mengatur tenggang waktu untuk permohonan pencabutan Sertifikat yang diajukan oleh Pemegang Sertifikat atau pihak ketiga lainnya. Pihak sebagaimana diatur pada bagian 4.9.2 meminta pencabutan segera setelah teridentifikasi adanya keperluan pencabutan.	Privy CA does not set a grace period for Certificate revocation requests submitted by Subscribers or other third parties. Parties as set out in section 4.9.2 should request revocation as soon as the need for revocation is identified.

4.9.5. Jangka Waktu PSrE Privy untuk Memproses Permohonan Pencabutan / *Timeframe for Privy CA to Process Revocation Requests*

PSrE Privy segera mencabut Sertifikat dalam jangka waktu 1 x 24 jam, setelah persyaratan pengajuan pencabutan Sertifikat sebagaimana tercantum pada bagian 4.9.3 berhasil dipenuhi.	Privy CA immediately revokes the Certificate within 1 x 24 hours, once the requirements for applying for Certificate revocation as listed in section 4.9.3 are successfully met.

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

Pengandal memvalidasi setiap Sertifikat terhadap CRL dan/atau OCSP terbaru yang diterbitkan oleh PSrE Privy sebagaimana dapat diakses melalui Repositori dan/atau URL https://ocsp.privyca.id. Frekuensi validasi Sertifikat terhadap CRL dan/atau OCSP milik PSrE ditentukan oleh Pengandal.	The Relying Parties shall validate each Certificate against the most recent CRL and/or OCSP published by Privy CA as accessible via the Repository and/or URL https://ocsp.privyca.id. The frequency of Certificate validation against the CRL and/or OCSP of Privy CA is determined by the Relying

	Parties.

4.9.7. Frekuensi Penerbitan CRL / *CRL Issuance Frequency*

CRL diperbarui secara berkala dalam jangka waktu maksimal 1 x 24 jam dan dapat diakses melalui Repositori.	CRLs are updated regularly within a maximum time frame of 1x 24 hours and can be accessed through the Repository.

4.9.8. Latensi Maksimum untuk CRL / Maximum Latency for CRLs

CRL dipublikasikan dalam jangka waktu 30 menit setelah CRL diperbarui.	The CRL is published within 30 minutes after the CRL is updated.

4.9.9. Ketersediaan Pemeriksaan Pencabutan/Status secara Daring / *Online Revocation/Status Checking Availability*

PSrE Privy menyediakan layanan pengecekan informasi status Sertifikat/pencabutan Sertifikat melalui CRL yang tersedia pada URL https://ocsp.privyca.id dan/atau OCSP yang selalu tersedia pada URL https://ocsp.privyca.id, diluar waktu pemeliharaan yang ditentukan oleh PSrE Privy. Pengandal menggunakan layanan CRL dan/atau OCSP untuk memeriksa status pencabutan Sertifikat.	Privy CA provides Certificate status/revocation information checking services via the CRL available at the URL https://ocsp.privyca.id and/or the OCSP, which is always available at the URL https://ocsp.privyca.id, except during maintenance periods as determined by Privy CA. Relying parties use the CRL and/or OCSP services to verify the revocation status of Certificates.

4.9.10. Persyaratan Pemeriksaan Pencabutan Secara Daring / *Online Revocation Checking Requirements*

Repositori PSrE Privy berisi dan mempublikasi daftar semua	The Privy CA repository should contain and publish a list of all

responder OCSP yang Privy operasikan yang selalu tersedia pada URL https://ocsp.privyca.id. Jika OCSP diimplementasikan, semua layanan yang digunakan mendukung dengan standar *Internet Engineering Task Force* (IETF) RFC 6960 untuk memenuhi persyaratan keamanan dan interoperabilitas.	OCSP responders that they operate which is always available at the URL https://ocsp.privyca.id. If OCSP is implemented, all services must be compliant with the RFC 6960 Internet Engineering Task Force (IETF) standard to meet security and interoperability requirements.

4.9.11. Bentuk lain dari Pengumuman Pencabutan yang Disediakan / *Other forms of Revocation Announcements Provided*

Tidak ada ketentuan.	No Stipulation.

4.9.12. Persyaratan Khusus Kebocoran Kunci / *Special Requirements for Key Compromise*

Tidak ada ketentuan.	No Stipulation.

4.9.13. Kondisi untuk Pembekuan Sertifikat / *Circumstances for Suspension*

Tidak ada ketentuan.	No Stipulation.

4.9.14. Pihak yang dapat Mengajukan Permohonan Pembekuan / *Parties Eligible to Request Suspension*

Tidak ada ketentuan.	No Stipulation.

4.9.15. Prosedur Permohonan Pembekuan / *Procedure for Suspension Request*

Tidak ada ketentuan.	No Stipulation.

4.9.16. Jangka waktu Masa Pembekuan / *Limits on Suspension Period*

Tidak ada ketentuan.	No Stipulation.

4.10. Layanan Status Sertifikat / *Certificate Status Services*

4.10.1. Karakteristik Operasional / *Operational Characteristics*

PSrE Privy menyediakan layanan pemeriksaan informasi status Sertifikat melalui CRL dan/atau OCSP.	Privy CA provides Certificate information status service through CRL or OCSP.

4.10.2. Ketersediaan Layanan / *Service Availability*

Layanan CRL atau OCSP tersedia sepanjang waktu, diluar waktu pemeliharaan yang ditentukan oleh PSrE Privy.	CRL or OCSP services are available at all time, outside of the maintenance time specified by Privy CA.

4.10.3. Fitur Opsional / *Optional Features*

Tidak ada ketentuan.	No Stipulation.

4.11. Akhir Masa Berlangganan / *End of Subscription*

Pemegang Sertifikat mengakhiri langganan Privy ketika Sertifikat miliknya telah dicabut dan akun Privy miliknya telah ditutup. PSrE Privy memiliki prosedur untuk mengakhiri masa berlangganan.	The Subscriber terminates their Privy's subscription when their Certificate has been revoked and their Privy account has been closed. Privy CA has a procedure in place for subscription termination.

4.12. Pemulihan dan Eskro Kunci / *Key Escrow and Recovery*

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

Tidak ada ketentuan.	No Stipulation.

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

Tidak ada ketentuan.	No Stipulation.

5. Fasilitas, Manajemen, dan Kontrol Operasi / *Facilities, Management, and Operational Controls*

5.1. Kontrol Fisik / *Physical Controls*

PSrE Privy melakukan kontrol terhadap keamanan Pusat Data sebagaimana diatur dalam CPS ini. “Pusat Data” mengacu kepada server yang ditempatkan melalui media penyimpanan yang menjalankan siklus operasi Sertifikat dan diletakan secara fisik dalam suatu lemari penyimpanan khusus.	Privy CA exercises control over Data Center security as set out in this CPS. "Data Center" shall refer to servers placed through storage media that run the Certificate operating cycle and are physically placed in a special storage cabinet.

5.1.1. Lokasi dan Konstruksi / *Site Location and Construction*

Seluruh fasilitas komputasi yang digunakan untuk menjalankan Layanan PSrE Privy ditempatkan dalam Pusat Data dan Pusat Data Pemulihan di dalam wilayah Negara Kesatuan Republik Indonesia. Pusat Data dan Pusat Data Pemulihan tersebut dilengkapi dengan berbagai mekanisme keamanan baik secara logis dan fisik untuk menjaga agar *non-Trusted Personnel Roles* tidak dapat memiliki akses ke Pusat Data. Bangunan Pusat Data dan Pusat Data Pemulihan dibangun dengan kualitas premium. Pusat Data harus berada di lokasi yang ketika terjadi bencana alam baik	All computing facilities used to run Privy CA Services are placed in a Data Center and Recovery Data Center within the territory of the Republic of Indonesia. The Data Center and the Recovery Data Center are equipped with various logical and physical security mechanisms to keep non-Trusted Personnel Roles from having access to the Data Center. The Data Center and the Recovery Data Center building are constructed with premium quality. The Data Center must be located in a location that in the event of a natural disaster, neither the Data Center nor the

pada Pusat Data, Pusat Data Pemulihan tidak ikut terkena dampaknya. Pusat Data Pemulihan PSrE Privy telah ditempatkan dengan mempertimbangkan availability layanan PSrE Privy.

Recovery Data Center is affected. The Recovery Data Center of Privy CA has been established taking into consideration the availability of Privy CA services.

5.1.2. Akses Fisik / *Physical Access*

Untuk mendapatkan akses masuk ke Pusat Data, maka harus dilakukan pendaftaran terlebih dahulu dan melalui penjagaan dengan setidaknya 4 (empat) lapis pengamanan antara lain akses yang dijaga 24 (dua puluh empat) jam oleh sekuriti, kamera pengawas, beberapa lapis pintu keamanan, akses masuk 3 (tiga) faktor autentikasi, dan kunci pengaman pada media penyimpanan. Hanya pihak tertentu yang termasuk pada *Trusted Personnel Roles* yang mendapat akses untuk masuk ke Pusat Data. PSrE Privy melakukan review terhadap akses fisik setiap 1 x 24 jam.

To gain access to the Data Center, registration must be made in advance within a minimum of four layers of protection, including access control and must go through 24 (twenty-four) hour security guard, surveillance cameras, several layers of security doors, 3 (three) authentication factors access, and security locks on storage media. Only certain parties included in the Trusted Personnel Roles have access to the Data Center. Privy CA reviews physical access every 1 x 24 hours.

Privy melakukan pengamanan fisik terhadap pengamanan Pusat Data dengan melakukan:

1. Memastikan tidak ada akses ke Pusat Data tanpa izin;

Privy shall undertake physical security measures to safeguard the Data Center by:

1. Ensure that no access to the Data Center occurs without permission;

2. Menyimpan semua media yang berisi informasi teks yang bernilai tinggi dan sensitif dalam media yang aman;
3. Melakukan monitor terhadap akses ke Pusat Data;
4. Memelihara dan memeriksa log akses secara berkala; dan
5. Memastikan kendali akses ke modul kriptografis dan sistem komputer Privy minimal 2 (dua) orang.

2. Storing all media containing high-value and sensitive textual information in a secure media;
3. Monitoring access to the Data Center;
4. Maintaining and periodically reviewing access logs; and
5. Ensuring access control to Privy's cryptographic modules and computer systems by a minimum of 2 (two) individuals.

Proses pemeriksaan keamanan fasilitas yang menyimpan perangkat Privy dilaksanakan jika fasilitas ditinggalkan. Setidaknya proses pemeriksaan memverifikasi hal-hal sebagai berikut:

1. Semua security container sudah diamankan;
2. Sistem keamanan fisik berfungsi dengan baik; dan
3. Area diamankan dari akses yang tidak berhak;

A security checking of the facility that stores Privy devices is performed when the facility is abandoned. At a minimum, the inspection process verifies the following:

1. All security containers have been secured;
2. Physical security systems are functioning properly; and
3. The area is secured from unauthorized access.

Pemeriksaan dibuktikan dengan log yang dapat dipertanggungjawabkan. Jika fasilitas tidak ditempati setiap waktu, maka orang terakhir yang meninggalkan fasilitas membuat

The inspection is evidenced by an accountable log. If the facility is not occupied at all times, the last person to leave the facility shall create a sign-out sheet indicating the date and time,

lembaran *sign-out* yang menunjukkan tanggal dan waktu, dan menyatakan bahwa semua mekanisme perlindungan fisik telah ada dan aktif.

and certifying that all physical protection mechanisms are in place and active.

5.1.3. Listrik dan Pendingin Ruangan / *Power and Air Conditioning*

Fasilitas dan Pusat Data Privy dilengkapi dengan daya listrik yang tinggi dan didukung dengan cadangan listrik dari *Uninterrupted Power Supply* (UPS) dan generator listrik yang bekerja reaktif terhadap pemadaman listrik yang mampu bekerja selama minimal 6 jam saat tidak adanya daya utama untuk mendukung keberlangsungan operasional.

The facilities and Privy Data Center are equipped with high electrical power and supported by electricity backup from Uninterrupted Power Supply (UPS) and electricity generators that work reactively to power outages that are able to work for minimum 6 hours of power outage to support operational continuity.

Pusat Data juga dilengkapi dengan menara (*tower*) pendingin ruangan yang menyesuaikan agar temperatur dan tingkat kelembaban ruangan terkendali untuk menjaga kinerja mesin dan peralatan Privy.

The Data Center is also equipped with an air-conditioning tower that adjusts the temperature and humidity levels to maintain the performance of Privy's machines and equipment.

5.1.4. Keterpaparan Air / *Water Exposures*

Pusat Data PSrE Privy berada di kawasan bebas banjir dan terletak tinggi diatas permukaan laut. Selain itu Pusat Data juga dilengkapi dengan alat pendeteksi kebocoran air dan

Privy CA Data Center is located in a flood-free area and high above sea level. In addition, the Data Center is also equipped with a water leak detection device and an Environment

Environment Monitoring System yang dapat mendeteksi tinggi kadar kelembapan udara.	Monitoring System that can detect high levels of air humidity.

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

Pusat Data dilengkapi dengan sensor deteksi asap, dan sistem pemadam kebakaran otomatis.	The Data Center is equipped with smoke detection sensors, and an automatic fire extinguishing system.

5.1.6. Media Penyimpanan / *Storage Media*

Media penyimpanan disimpan dan dilindungi dari hal-hal yang dapat menyebabkan kerusakan, pencurian dan akses yang tidak berhak. Salinan yang digunakan sebagai cadangan terhadap media penyimpanan tersebut disimpan dan diamankan di lokasi yang terpisah dari Pusat Data dan Pusat Pemulihan Data.	Storage media is stored and protected from things that can cause damage, theft, and unauthorized access. Copies used as backups of the storage media are stored and secured in a separate location from the Data Center and Recovery Data Center.

5.1.7. Pembuangan Limbah / *Waste Disposal*

Seluruh dokumen dan perangkat keras yang sudah tidak digunakan dihancurkan dan dibuang dengan cara yang aman dan wajar agar perangkat tersebut tidak dapat digunakan lagi.	All document and obsolete hardware is destroyed and disposed of in a safe and reasonable manner so that it can no longer be used.

5.1.8. Cadangan *Off-site* / *Off-site Backup*

PSrE Privy menyiapkan sistem pencadangan yang cukup untuk	Privy CA prepares a backup system that is sufficient to be

digunakan dalam rangka pemulihan dari kegagalan sistem. Sistem pencadangan tersebut dilakukan dengan cara menyalin data yang yang ada pada Pusat Data dan Pusat Pemulihan Data secara manual ke sebuah media penyimpanan, untuk selanjutnya disimpan di lokasi yang aman dan berada di lokasi yang terpisah dengan Pusat Data dan Pusat Pemulihan Data. Hanya sistem pencadangan yang disimpan terakhir yang digunakan untuk pemulihan.

used in order to recover from system failure. This backup system involves manually copying data from the Data Center and the Recovery Data Center to a storage medium, which is then stored in a secure location separate from the Data Center and Recovery Data Center. Only the last stored backup system is used for recovery.

5.1.9. Pusat Data Pemulihan / *Recovery Data Center*

PSrE Privy memiliki Pusat Data Pemulihan di dalam wilayah Negara Kesatuan Republik Indonesia. Pusat Data Pemulihan merupakan fasilitas yang digunakan PSrE Privy untuk memulihkan infrastruktur atau layanan pasca bencana dan memiliki jarak tertentu dengan Pusat Data. Ketentuan pada bagian 5.1.1 – 5.1.8 juga berlaku terhadap Pusat Data Pemulihan.

Privy CA has a Recovery Data Center within the territory of the Republic of Indonesia. The Recovery Data Center is a facility used by Privy CA to restore post-disaster infrastructure or services and has a certain distance from the Data Center. The provisions in sections 5.1.1 - 5.1.8 shall also apply to the Recovery Data Center.

5.2. Kontrol Prosedural / *Procedural Controls*

5.2.1. Trusted Personnel Roles */ Trusted Personnel Roles*

Posisi Peran Terpercaya (*Trusted Personnel Roles*) termasuk namun tidak terbatas pada:

Trusted Personnel Roles positions include but are not limited to:

a. Koordinator: Melakukan penetapan terkait kebutuhan bisnis dan kebijakan internal PSrE Privy.
b. *Policy Authority* (PA): Menetapkan kebijakan PSrE Privy.
c. Staff PA: Membantu PA dalam menetapkan kebijakan PSrE Privy.
d. *Administrator Network:* Melakukan operasional, pemeliharaan sistem dan keamanan *network* PSrE Privy.
e. *Administrator* Aplikasi: Melakukan operasional, pemeliharaan sistem dan keamanan aplikasi PSrE Privy.
f. *Administrator* OS: Melakukan operasional, pemeliharaan sistem dan keamanan *Operating System* PSrE Privy.
g. Security Officer: Mengelola penerapan kebijakan dan praktik keamanan PSrE Privy.
h. *Administrator* HSM: Melakukan operasional, pemeliharaan sistem dan keamanan HSM PSrE Privy.
i. *Registration Authority* (RA): Melakukan dan mengelola proses pendaftaran, perpanjangan dan

a. Coordinator: Establishes business requirements and internal policies for Privy CA.
b. Policy Authority (PA): Defines the policies for Privy CA.
c. PA Staff: Assists the PA in setting Privy CA policies.
d. Network Administrator: Manages the operations, maintenance, and security of Privy CA's network.
e. Application Administrator: Oversees the operations, maintenance, and security of Privy CA's applications.
f. OS Administrator: Manages the operations, maintenance, and security of Privy CA's Operating System.
g. Security Officer: Oversees the implementation of Privy CA's security policies and practices.
h. HSM Administrator: Handles the operations, maintenance, and security of Privy CA's Hardware Security Module (HSM).
i. Registration Authority (RA): Manages the registration, renewal, and revocation processes for Electronic

pencabutan Sertifikat Elektronik.

j. Staff RA: Membantu RA untuk melakukan dan mengelola proses pendaftaran, perpanjangan dan pencabutan Sertifikat Elektronik.
k. Repositori: Bertanggung jawab atas operasional, *troubleshoot* dan pengembangan repositori.
l. *Key Custodian*: Melakukan peran sebagai pemegang (*custodianship*) perlengkapan aktivitas PSrE Privy.
m. Internal Audit: Melakukan audit internal PSrE Privy.

Certificates.

j. RA Staff: Assists the RA in managing the registration, renewal, and revocation of Electronic Certificates.
k. Repository: Responsible for the operations, troubleshooting, and development of the repository.
l. Key Custodian: Acts as the custodian of equipment for Privy CA's activities.
m. Internal Audit: Conducts internal audits for Privy CA.

Peran tersebut secara detail dijelaskan melalui kebijakan internal perusahaan dan merupakan dokumen yang bersifat rahasia.

These roles are detailed in the company's internal policies and are classified as confidential documents.

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

Untuk kegiatan yang memerlukan kendali multipersonel, PSrE Privy hanya melibatkan pihak yang memegang Peran Terpercaya.

For activities that require multi-personnel control, Privy CA only involves individuals holding Trusted Roles.

Adapun tugas berikut yang memerlukan 2 (dua) orang atau lebih antara lain:

1. Pembangkitan kunci PSrE Privy;
2. Penandatanganan Sertifikat PSrE Privy;
3. Pencabutan Sertifikat PSrE Privy; dan
4. Pencadangan Kunci Privat PSrE Privy.

The following tasks require two or more personnel:

1. Generation of Privy CA keys;
2. Signing of Privy CA Certificates;
3. Revocation of Privy CA Certificates; and
4. Backup of Privy CA Private Keys.

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

Sebelum mengisi posisi *Trusted Personnel Roles*, maka individu akan diperiksa latar belakangnya sesuai dengan ketentuan pada bagian 5.3.1 dan 5.3.2 untuk memastikan bahwa *Trusted Personnel Roles* diisi oleh orang yang tepat. Autentikasi *Trusted Personnel Roles* dilakukan melalui kendali akses fisik dan kendali akses tingkat sistem. Autentikasi tersebut dilakukan berdasarkan identifikasi orang yang mengakses ruangan atau sistem dan hak akses yang diatur sesuai dengan peran dan tanggung jawab orang tersebut. Sebelum menjalankan tugas sebagai *Trusted Personnel Roles,* Privy akan menerbitkan surat

Before filling the Trusted Personnel Roles position, the background of the individual will be checked according to the provisions in sections 5.3.1 and 5.3.2 to ensure that Trusted Personnel Roles are filled by appropriate persons. Authentication of Trusted Personnel Roles is carried out through physical access control and system level access control. The authentication is based on the identification of the person accessing the room or system and the access rights set according to the person's roles and responsibilities. Before performing their duties as Trusted Personnel Roles, Privy CA will issue an assignment

penugasan bagi para individu terkait tersebut.

letter for the relevant individuals.

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

PSrE Privy memastikan bahwa 1 (satu) orang hanya dapat mengisi 1 (satu) peran *Trusted* Personnel *Roles* pada saat yang bersamaan untuk peran-peran berikut:

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

Privy CA ensures that 1 (one) person can only fill 1 (one) Trusted Personnel Roles role at the same time for the following roles:

a. Policy Authority and operational administrator;
b. Internal audit and all other roles; and
c. Application developers and all other roles.

5.3. Kontrol Personil / *Personnel Controls*

5.3.1. Persyaratan Kualifikasi, Pengalaman, dan Perizinan / *Qualification, Experience, and Clearance Requirements*

Karyawan Privy tunduk pada pemeriksaan latar belakang dan pemeriksaan catatan kriminal yang dilakukan oleh Privy. Privy berdasarkan kebijaksanaannya memastikan karyawan Privy diisi oleh orang yang berpengalaman, terampil, terpercaya, dan berintegritas. Untuk memastikan hal tersebut maka Privy melakukan pemeriksaan latar belakang, termasuk namun tidak terbatas, terhadap pemeriksaan identitas, latar belakang pendidikan, pekerjaan,

Privy employees shall be subject to background checks and criminal record checks conducted by Privy. Privy at its discretion ensures that Privy employees are filled with persons who are experienced, skilled, trusted, and have integrity. Thus, Privy conducts background checks, including but not limited to identity checks, educational background, employment, qualifications, and experience, and criminal record checks as

kualifikasi, dan pengalaman, pemeriksaan catatan kriminal yang dibuktikan dengan SKCK dari Kepolisian Republik Indonesia dan Informasi finansial dari sistem pengecekan finansial yang dikeluarkan oleh otoritas yang berwenang.

evidenced by Statement of Police Report from the Indonesian National Police.

5.3.2. Prosedur Pemeriksaan Latar Belakang / *Background Check Procedure*

Diatur melalui bagian 5.3.1.

Administered through section 5.3.1.

5.3.3. Persyaratan Pelatihan / *Training Requirements*

Setiap orang yang diterima untuk mengisi posisi *Trusted Personnel* Roles menerima pelatihan yang mencakup, namun tidak terbatas, kepada hal-hal ini:

a. Konsep dasar mengenai PKI;
b. CP/CPS;
c. Internal *Standard Operational Procedure* (SOP) terkait dengan kegiatan operasional PKI;
d. Dokumentasi mengenai tata cara menggunakan sistem PKI;
e. Pemulihan bencana dan keberlangsungan bisnis; dan
f. Pemahaman mengenai pentingnya keamanan siber, terkhusus mengenai taktik *phishing* dan *social engineering*.

Each person hired to fill Trusted Personnel Roles receives training that includes, but is not limited to, the following:

a. Basic concepts about PKI;
b. CP/CPS;
c. Internal Standard Operational Procedure (SOP) related to PKI operational activities;
d. Documentation on how to use the PKI system;
e. Disaster recovery and business continuity; and
f. Understanding the importance of cybersecurity, specifically phishing and social engineering tactics.

Evaluasi terhadap kecukupan kompetensi personil PSrE Privy dilakukan minimal 1 (satu) kali dalam setahun.	Evaluation of the adequacy of the competence of Privy CA personnel is carried out at least once a year.

5.3.4. Frekuensi Pelatihan Ulang dan Persyaratannya / *Retraining Frequency and Requirements*

Karyawan yang mengisi posisi *Trusted Personnel Roles* memiliki keahlian dan kemampuan yang konsisten dengan perkembangan industri PKI. PSrE Privy melakukan pelatihan ulang secara rutin minimal setiap 1 (satu) kali dalam setahun dan/atau disesuaikan berdasarkan kebutuhan karyawan. Dalam hal PSrE Privy mengubah kebijakan operasional PKI, maka PSrE Privy memberikan pelatihan sesuai dengan perubahan kebijakan yang diambil oleh PSrE Privy.	Employees who fill Trusted Personnel Roles positions have skills and abilities that are consistent with developments in the PKI industry. Privy CA conducts regular retraining minimum once a year and/or adjust training based on employee needs. In the event that Privy CA changes the PKI operational policy, Privy CA shall provides training in accordance with the policy changes adopted by the Privy CA.

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

PSrE Privy memastikan bahwa dalam hal terjadi perubahan atau rotasi pegawai, maka hal tersebut tidak berdampak negatif terhadap efektivitas operasional layanan atau keamanan sistem.	Privy CA ensures that in the event of a change or rotation of employees, it does not have a negative impact on the effectiveness of service operations or system security.

5.3.6. Sanksi terhadap Tindakan yang Tidak Sah / *Sanctions for Unauthorized Actions*

Karyawan yang tidak menjalankan perannya sesuai dengan CPS ini, baik secara disengaja maupun tidak, akan menerima sanksi berdasarkan kebijakan PSrE Privy. Untuk karyawan yang berperan *sebagai Trusted Personnel Roles* dan tidak menjalankan perannya sesuai CPS ini, akan dikenakan sanksi berupa pencabutan dari fungsi *Trusted Personnel Roles* sampai ada peninjauan lebih lanjut dari manajemen perusahaan.

Employees who do not perform their roles in accordance with this CPS, whether intentionally or unintentionally, shall be subject sanctions based on Privy CA policy. For employees who serve in Trusted Personnel Roles and fail to perform their roles in accordance with this CPS, subject to a sanction in the form of withdrawal from the Trusted Personnel Roles function until further review by the company management.

5.3.7. Persyaratan Kontraktor Independen / *Independent Contractor Requirements*

Kontraktor independen yang dipekerjakan untuk menjalankan fungsi *Trusted Personnel Roles* juga harus tunduk kepada ketentuan yang diatur di dalam CPS ini.

Independent contractors hired to perform Trusted Personnel Roles shall also be subject to the provisions set out in this CPS.

5.3.8. Dokumentasi yang Disediakan untuk Personil / *Documentation Supplied to Personnel*

Karyawan akan dibekali dengan dokumentasi pendukung yang dibutuhkan untuk menjalankan perannya sesuai dengan CPS ini.

Employees will be provided with the supporting documentation needed to perform their roles in accordance with this CPS.

5.4. Prosedur Log Audit / *Audit Log Procedure*

Log audit dibuat untuk kejadian yang terkait dengan keamanan PSrE, VA dan RA secara otomatis. Semua log audit keamanan akan dijaga dan tersedia. Log audit keamanan untuk setiap kejadian yang dapat diaudit dipelihara sebagaimana disebutkan pada Bagian 5.5.2.

Audit logs are generated automatically for events related to the security of CA, VA, and RA. All security audit logs will be maintained and made available. Security audit logs for each auditable event are preserved as specified in Section 5.5.2.

5.4.1. Jenis Peristiwa yang Direkam / *Types of Events Recorded*

Informasi yang akan disimpan di dalam log termasuk namun tidak terbatas kepada:

a. Jenis kejadian;
b. Nomor seri atau urutan rekaman;
c. Tanggal dan waktu kejadian;
d. Sumber perekaman;
e. Indikator sukses atau gagal yang sesuai; dan
f. Identitas dari entitas dan/atau operator yang menyebabkan kejadian.

Information to be stored in the logs shall include but is not limited to:

a. Types of event;
b. Serial number or record sequence;
c. Date and time of the incident;
d. Source of recording;
e. Appropriate indicators of success or failure; and
f. Identity of entities and/or operators causing the incident.

PSrE Privy mengaktifkan semua fitur audit keamanan dari sistem operasi PSrE dan RA, serta aplikasi PSrE, Validasi Otoritas, dan RA yang dipersyaratkan oleh CPS ini. PSrE Privy memastikan bahwa seluruh kegiatan yang berkaitan dengan siklus Sertifikat

Privy CA enables all security audit features of the CA and RA operating systems, as well as the CA, Validation Authority, and RA applications required by this CPS. Privy CA must ensure that all activities related to the Certificate cycle are recorded in

dicatat dalam log sehingga setiap tindakan *Trusted Personnel Roles* dalam operasional PSrE Privy dapat dilacak. Waktu disinkronkan dengan otoritas sumber waktu dengan ketelitian paling lama 1 (satu) menit.

logs so that every action of Trusted Personnel Roles in Privy CA operations can be traced. Time is synchronized with the time source authority with a maximum accuracy of 1 (one) minute.

5.4.2. Frekuensi Pemrosesan Log / *Frequency of Processing Log*

PSrE Privy secara berkala melakukan pemeriksaan terhadap log yang sudah disimpan. Pemeriksaan tersebut dilakukan untuk memverifikasi bahwa log tersebut tidak dirusak, diacak, dan tidak adanya jenis kehilangan lain terhadap log.

Privy CA checks the logs that have been stored periodically. These checks are performed to verify that the logs have not been tampered with, scrambled, and that there is no other type of corruption to the logs.

Pemeriksaan dilanjutkan dengan penyelidikan yang lebih menyeluruh terhadap peringatan atau penyimpangan yang muncul dalam log.

The check continues with a more thorough investigation into any warnings or irregularities that appear in the logs.

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

PSrE Privy menyimpan log audit dalam jangka waktu 1 (satu) tahun. Jangka waktu ini dapat berubah sewaktu-waktu sesuai dengan hukum yang berlaku.

Privy CA stores audit logs for a period of 1 (one) year. This period may subject to change at any time in accordance with applicable law.

5.4.4. Perlindungan Log Audit / *Protection of Audit Logs*

Log Audit dilindungi untuk mencegah perubahan dan mendeteksi gangguan serta

Audit Logs are protected to prevent changes and detect tampering and to ensure that

untuk memastikan bahwa hanya individu dengan akses terpercaya yang berwenang yang mampu melakukan operasi apa pun tanpa memodifikasi integritasnya.	only individuals with authorized trusted access are able to perform any operations without modifying their integrity.

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

Log audit disalin untuk dicadangkan dengan mekanisme *Hot Backup*. Cadangan log tersebut disimpan secara terpisah dari Pusat Data.	Audit logs are copied to be backed up with a Hot Backup mechanism. Such log backups are stored separately from the Data Center.

5.4.6. Sistem Pengumpulan Audit (Internal atau Eksternal) / *Audit Collection System (Internal or External)*

Proses log untuk audit berjalan secara otomatis sejak sistem dinyalakan dan sebaliknya berhenti jika sistem dimatikan. *Trusted Personnel Roles* dapat membuat log audit secara manual dan terpisah.	The log process for auditing runs automatically from system startup and otherwise stops if the system is shut down. Trusted Personnel Roles can create audit logs manually and separately.

5.4.7. Pemberitahuan ke Subjek yang Menyebabkan Peristiwa / *Notification to Event-Causing Subject*

Tidak ada ketentuan.	No Stipulation.

5.4.8. Penilaian Kerentanan / *Vulnerability Assessments*

PSrE Privy melakukan penilaian kerentanan, yang tidak terbatas hanya kepada *penetration testing, stress test dan load test*, secara berkala untuk memastikan bahwa sistem	Privy CA conducts vulnerability assessments, which are not limited to penetration testing, stress tests and load tests, periodically to ensure that the system is reliable without any

secara andal tanpa adanya ancaman secara internal dan eksternal yang dapat berdampak kepada sistem PSrE Privy. Penilaian kerentanan dilakukan paling tidak sekali setahun.

internal and external threats that can impact the Privy CA system. Vulnerability assessments are carried out at least once a year.

Hasil dari penilaian kerentanan menjadi informasi yang dirahasiakan dan digunakan untuk menjaga dan meningkatkan keamanan sistem PSrE Privy.

The results of the vulnerability assessment shall become confidential information and are used to maintain and improve the security of the Privy CA system.

5.5. Pengarsipan Catatan / *Records Archiving*

5.5.1. Jenis Catatan yang Diarsipkan / *Types of Records Archived*

Berikut merupakan catatan yang disimpan dalam arsip:

a. Siklus hidup operasi Sertifikat termasuk permohonan Sertifikat, penolakan permohonan Sertifikat, dan permintaan pencabutan Sertifikat;
b. Semua Sertifikat dan CRL sebagaimana yang diterbitkan atau dipublikasikan oleh PSrE Privy;
c. Log Audit;
d. Konfigurasi sistem PKI; dan
e. Dokumen yang tersedia di Repositori termasuk amandemen dan perubahannya.

Here are the records kept in the archive:

a. The Certificate operation lifecycle includes Certificate application, rejection of Certificate application, and request of Certificate revocation;
b. All Certificates and CRLs as issued or published by Privy CA;
c. Audit Logs;
d. PKI system configuration; and
e. Documents available in the Repository include amendments and changes.
f. Supporting Data for the Information Security

f. Data pendukung Sistem Manajemen Keamanan Informasi (SMKI):
   i. Penunjukkan dan pencabutan peran dan kewenangan;
   ii. Akses pengunjung ke fasilitas PSrE;
   iii. Perubahan dan pemeliharaan perangkat keras dan perangkat lunak sistem;
   iv. Deteksi dan tindakan terhadap insiden keamanan informasi
   v. Pelatihan keadaan darurat;
   vi. Tindakan dan penilaian risiko terkait keamanan informasi;
   vii. Perubahan aset, prosedur dan tanggung jawab; dan
   viii. Perubahan dokumentasi.

Management System (ISMS):
   i. Appointment and revocation of roles and authorities;
   ii. ii. Visitor access to CA facilities;
   iii. Changes and maintenance of hardware and software systems;
   iv. Detection and actions against security incidents;
   v. Emergency situation drills;
   vi. Risk actions and assessment;
   vii. Changes to assets, procedures, and responsibilities; and
   viii. Documentation changes.

5.5.2. Masa Retensi Arsip / *Retention Period for Archive*

PSrE Privy menyimpan arsip selama 5 (lima) tahun. Perangkat lunak dan perangkat keras yang dibutuhkan untuk membaca arsip dipelihara selama masa retensi.

Privy CA retains archives for 5 (five) years. The software and hardware needed to read the archives are maintained during the retention period.

5.5.3. Perlindungan Arsip / *Protection of Archive*

PSrE Privy menjaga agar arsip dilindungi dari akses, modifikasi, penghapusan, atau gangguan yang tidak sah dan memelihara arsip dan aplikasi yang dibutuhkan untuk memproses catatan yang diarsipkan tersebut.	Privy CA keeps archives protected from unauthorized access, modification, deletion, or tampering and shall maintain the archives and necessary applications for processing the archived records.
Muatan arsip tidak boleh diungkap kecuali berdasarkan ketentuan bagian 9.3 dan 9.4 CPS ini. Catatan dari transaksi individu dapat diungkap berdasarkan permintaan dari pemilik yang terlibat dalam transaksi tersebut atau berdasarkan permintaan agen yang dikenali oleh hukum.	The contents of the archives may not be disclosed except in accordance with the provisions of sections 9.3 and 9.4 of this CPS. Records of individual transactions may be disclosed upon request from the subscriber involved in the transactions or based on requests from agents recognized by law.

5.5.4. Prosedur Pencadangan Arsip / *Archive Backup Procedure*

Tidak ada ketentuan.	No Stipulation.

5.5.5. Persyaratan Stempel Waktu Pencatatan / *Requirements for Time-Stamping of Records*

Seluruh catatan diberikan stempel waktu (*time stamping*) secara otomatis sejak catatan tersebut terekam.	All records are automatically time-stamped from the moment they are recorded.

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

Pengumpulan arsip dilakukan secara internal oleh Privy.	Archive collection is carried out internally by Privy.

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

Permohonan untuk memperoleh informasi di dalam arsip hanya dapat diberikan oleh pihak yang dipercayakan melalui *Trusted Personnel Roles.* Sedikitnya 1 (satu) kali dalam setahun, sampel dari arsip akan diperiksa oleh *Trusted Personnel Roles* yang bertanggung jawab terhadap hal tersebut untuk memeriksa integritas dari informasi yang terekam di dalam arsip.

Requests to obtain information in the archives can only be made by parties entrusted through Trusted Personnel Roles. At least once a year, a sample taken from the archive will be examined by the Trusted Personnel Roles responsible for it to check the integrity of the information recorded therein.

5.6. Pergantian Kunci / *Key Changeover*

Dalam hal terjadi hal yang membahayakan PKI Privy, untuk meminimalisir risiko terhadap bocornya Kunci Privat PSrE Privy, kunci tersebut diganti dengan kunci baru yang digunakan untuk penandatangan Sertifikat. PSrE Privy melakukan pemberitahuan kepada Pemegang Sertifikat dan Pengandal dalam hal terjadi penggantian kunci baru PSrE Privy tersebut.

In the event that something endangers the PKI Privy, to minimize the risk of leakage of the Privy CA's Private Key, the key is replaced with a new key used for Certificate signing. Privy CA notifies Subscribers and Relying Parties in the event of a new Privy CA key changeover.

Sertifikat PSrE Privy yang masih berlaku, akan tersedia untuk memverifikasi tanda tangan yang lama sampai semua Sertifikat yang ditandatangani oleh Kunci

A valid Privy CA Certificate will be available to verify the old signature until all Certificates signed by the corresponding Privy CA Key have also expired.

Privat PSrE Privy yang terkait tersebut juga sudah kedaluwarsa. Jika Kunci Privat PSrE Privy yang lama digunakan untuk menandatangani CRL, kunci yang lama akan disimpan dan dilindungi. Masa berlaku Sertifikat dan Kunci Privat PSrE Privy dijelaskan pada bagian 6.3.2.

If an old Privy CA's Private Key is used to sign a CRL, the old key must be kept and protected. The validity period of the Privy CA Certificate and Private Key is detailed in Section 6.3.2.

Dalam hal PSrE Privy memperbarui Kunci Privat dan menghasilkan Kunci Publik baru, maka PSrE Privy memberitahukan semua Pemegang Sertifikat yang mengandalkan Sertifikat PSrE Privy bahwa telah terjadi perubahan. PSrE Privy tidak menerbitkan Sertifikat Pemilik dengan Pasangan Kunci yang masa berlakunya melebihi masa berlaku Sertifikat PSrE Privy. Pasangan Kunci PSrE Privy dibangkitkan lagi paling lambat pada saat Sertifikat PSrE Privy kedaluwarsa dikurangi masa berlaku Sertifikat Pemilik ("***Grace Period***").

In the event that Privy CA updates the Private Key and generates a new Public Key, Privy CA will notify all Subscribers relying on the Privy CA Certificate that a change has occurred. Privy CA does not issue Subscriber Certificate with Key Pairs that have a validity period exceeding the Privy CA Certificate. Privy CA Key Pairs are re-generated no later than the expiration of the Privy CA Certificate, minus the validity period of the Subscriber Certificate ("**Grace Period**").

Untuk Sertifikat Pemilik yang akan diterbitkan selama *Grace Period*, maka PSrE Privy akan membangkitkan Kunci Privat

For Subscriber Certificate to be issued during the Grace Period, Privy CA will generate a new Private Key before the existing

baru sebelum Kunci Privat yang telah ada kedaluwarsa untuk mengakomodasi masa pakai Sertifikat Pemilik yang dibangkitkan sebelum masa *Grace Period* dimulai. Selama masa *Grace Period* semua Sertifikat akan ditandatangani dengan Kunci Privat terbaru milik PSrE Privy.

Private Key expires to accommodate the lifespan of the Subscriber Certificate generated before the Grace Period begins. During the Grace Period, all Certificates will be signed with the latest Private Key of Privy CA.

5.7. Pemulihan Bencana dan Kondisi Terkompromi / *Compromise and Disaster Recovery*

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

PSrE Privy telah mempunyai rencana penanganan insiden dan rencana pemulihan bencana yang diperbaharui secara berkala.

Dalam hal terjadi hal yang membahayakan pelayanan PKI Privy, PSrE Privy segera melakukan investigasi sesuai prosedur yang telah ditentukan untuk memeriksa dan memperhitungkan dampak dari bahaya tersebut. Jika PKI Privy memang dalam keadaan bahaya atau dalam keadaan terkompromi yang menyebabkan Sertifikat yang diterbitkan oleh PSrE Privy harus dicabut, maka Sertifikat baru harus segera diterbitkan.

Privy CA has an incident handling plan and a disaster recovery plan that are periodically updated. In the event that something endangers the services of PKI Privy, Privy CA immediately conducts an investigation according to predetermined procedures to examine and calculate the impact of the danger. If the Privy PKI is indeed in a state of danger or compromised that causes the Certificate issued by Privy CA to be revoked, a new Certificate must be issued immediately.

PSrE Privy akan menginformasikan kepada PSrE Induk dalam hal:

a. terjadi insiden serangan *Denial of Service* yang berdampak berhentinya pelayanan operasional Privy;
b. sistem PSrE Privy terkompromi;
c. adanya upaya untuk menembus sistem PSrE Privy baik secara fisik maupun elektronik yang berdampak berhentinya pelayanan operasional Privy;
d. Insiden yang mencegah atau menghambat penerbitan CRL dalam waktu 24 jam dari waktu yang ditentukan;
e. CRL dan/atau OCSP *responder* tidak dapat diakses oleh publik dikarenakan adanya insiden serangan seperti *Denial of Service* dan upaya menembus sistem Privy.

Privy CA shall promptly notify the Root CA in the following events:

a. An incident of Denial of Service attack that results in the cessation of Privy's operational services;
b. Indication of compromise to the Privy CA system;
c. Attempt to breach the Privy CA system, whether physically or electronically, that result in the cessation of Privy's operational services;
d. Incidents preventing or impeding CRL issuance within 24 hours of the designated time;
e. Unavailability of CRL and/or OCSP responder for public access due to incidents such as Denial of Service attacks and attempts to breach the Privy system.

PSrE Privy juga memberikan laporan berkala kepada PSrE Induk terkait dengan insiden dan gangguan yang terjadi dalam kegiatan PSrE Privy.

Privy CA also provides periodic reports to the Root CA regarding incidents and disruptions that occur within the operations of Privy CA.

Semua sistem pencadangan/pemulihan diuji minimal setahun sekali.	All backup/recovery systems are tested at least once a year.

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

Jika peralatan PKI Privy mengalami kerusakan atau berhenti berfungsi namun Kunci Privat masih tetap berfungsi dan tidak mengalami kerusakan, maka operasi PKI harus dengan segera dijalankan kembali dengan mengutamakan kemampuan sistem PKI untuk membangkitkan status informasi Sertifikat sesuai dengan rencana pemulihan bencana PSrE Privy.	If the Privy PKI equipment is damaged or stops functioning but the Private Key is still functioning and undamaged, the PKI operation must be immediately restarted by prioritizing the ability of the PKI system to generate Certificate information status in accordance with the Privy CA disaster recovery plan.
Jika Pasangan Kunci PSrE Privy rusak, operasional PSrE Privy harus dilakukan kembali secepat mungkin dengan memberikan prioritas ke pembangkitan Pasangan Kunci Privy baru. PSrE Privy akan membangkitkan Pasangan Kunci PSrE baru sesuai dengan prosedur yang ditetapkan dalam CPS ini. Dalam hal kemampuan untuk membangkitkan status Sertifikat tidak dapat beroperasi atau rusak, PSrE Privy akan secepat mungkin membangkitkan status Sertifikat. Dalam hal PSrE Privy	If the Privy CA Key Pair is damaged, Privy CA operations must be reestablished as soon as possible by giving priority to the generation of a new Privy Key Pair. Privy CA shall generate a new CA Key Pair in accordance with the procedures set out in this CPS. In the event that the ability to generate Certificate status becomes inoperable or is damaged, Privy CA will promptly work to regenerate the Certificate status. If Privy CA is unable to generate the Certificate status information

tidak dapat membangkitkan informasi status Sertifikat dalam jangka waktu yang wajar, PSrE akan berkoordinasi dengan PSrE Induk untuk menentukan apakah diperlukan pencabutan Sertifikat milik PSrE Privy.

within a reasonable timeframe, PrivyCA will coordinate with Root CA to determine whether the revocation of the Privy CA Certificate is necessary.

PSrE Privy melakukan pemberitahuan kepada PA dan PSrE Induk sesegera mungkin apabila ketentuan dalam bagian ini terjadi.

Privy CA notifies the PA and Root CA as soon as possible if the provisions in this section occur.

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

Dalam keadaan dimana Kunci Privat PSrE Privy terkompromi, hilang, hancur, atau dicurigai terkompromi, maka setelah dilakukan investigasi, PSrE Privy akan :

1. Segera memutuskan untuk mencabut seluruh Sertifikat yang telah diterbitkan dan membangkitkan Pasangan Kunci Privy yang baru;
2. Dengan segera akan memberikan pengumuman kepada Pemegang Sertifikat dan Pengandal melalui Situs Privy mengenai pencabutan Sertifikat yang disebabkan karena hal tersebut;

In circumstances where Privy CA's Private Key is compromised, lost, destroyed, or suspected of being compromised, then after investigation, Privy CA must:

1. Immediately decide to revoke all issued Certificates and generate a new Privy Key Pair;
2. Immediately make an announcement to the Subscribers and Relying Parties through the Privy Site regarding the revocation of the Certificate caused by this reason;
3. Investigate the cause of the compromise or loss and

3. Menyelidiki penyebab kompromi atau kerugian dan Kembali yang harus diambil untuk mencegah kompromi tersebut terulang Kembali.
4. Memberitahu PSrE Induk sesegera mungkin agar dapat melakukan pencabutan Sertifikat PSrE Privy;
5. Meminta penerbitan Sertifikat PSrE Privy baru ke PSrE Induk sesuai dengan proses registrasi awal yang disebutkan dalam CP Induk.

Controls to be carried out to prevent the compromise from re-occuring;
4. Notify the Root CA as soon as possible to facilitate the revocation of the Privy CA Certificate;
5. Request the issuance of new Privy CA Certificates from Root CA in accordance with the initial registration process outlined in the Root CA's CP.

PSrE Privy akan menyelidiki penyebab kompromi atau kerugian dan tindakan yang harus diambil untuk mencegah kompromi tersebut terulang kembali. Dalam hal kunci PSrE Induk terkompromi, PSrE Privy akan menghentikan layanan sampai dengan PSrE Privy menerima pasangan kunci baru yang didapat pada saat *key ceremony* baru dan memberitahukan semua Pemegang Sertifikat, Pengandal dan pihak-pihak relevan lainnya agar mengeluarkan Sertifikat PSrE Induk dari rantai kepercayaannya dan dilanjutkan dengan pencabutan semua Sertifikat dan menerbitkan CRL

The Privy CA will investigate the cause of the compromise or loss and the actions needed to prevent future occurrences. In the event that the Root CA key is compromised, the Privy CA will suspend the services until it receives the new key pair obtained during the new key ceremony and will notify all Subscribers, Relying Parties, and other relevant parties to remove the Root CA Certificate from its chain of trust, followed by the revocation of all Certificates and the issuance of the final CRL. The Privy CA will generate the new Privy CA Key Pair in accordance with the procedures established in this

terakhir. PSrE Privy akan membangkitkan Pasangan Kunci PSrE baru sesuai dengan prosedur yang ditetapkan dalam CPS ini.

CPS.

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

PSrE Privy melakukan *mirroring system* sebagai cadangan layanan PKI di tempat yang terpisah dengan Pusat Data sebagai bagian dari rencana pemulihan bencana. Dalam hal layanan Privy terhentikan yang diakibatkan oleh musibah, maka PSrE Privy segera menjalankan layanan PKI-nya melalui cadangan layanan PKI tersebut, hingga Pusat Data pulih dan digunakan seperti semula paling lambat 24 (dua puluh empat) jam setelah terjadi bencana.

Privy CA conducts a mirroring system as a backup for PKI services in a place separate from the Data Center as part of the disaster recovery plan. In the event that the Privy service is stopped due to a disaster, Privy CA immediately runs its PKI service through the backup PKI service, until the Data Center is restored and used as before no later than 24 (twenty-four) hours after the disaster.

Dalam hal terjadi bencana yang mengakibatkan semua fasilitas dan peralatan PSrE Privy rusak secara fisik dan semua salinan Kunci Privat PSrE Privy hancur, PSrE Privy meminta agar Sertifikatnya dicabut. PSrE Privy mengikuti ketentuan sebagaimana diatur pada bagian 5.7.3.

In the event of a disaster that results in all of Privy CA's facilities and equipment being physically damaged and all copies of Privy CA's Private Keys being destroyed, Privy CA must request that its Certificate be revoked. Privy CA follows the provisions as set out in section 5.7.3.

5.8. Pengakhiran CA atau RA / *CA or RA termination*

Dalam hal PSrE Privy mengakhiri layanan-nya, maka:

a. PSrE Privy memberikan pemberitahuan melalui surat elektronik kepada para pihak yang terlibat dalam siklus operasional Sertifikat, termasuk kepada PSrE Induk, Pemegang Sertifikat, Pengandal, dan RA;
b. Memastikan bahwa informasi status Sertifikat tetap dapat diakses untuk jangka waktu 2 (dua) tahun setelah pengakhiran layanan;
c. Menjamin agar proses pencabutan semua Sertifikat pada saat penutupan dilakukan sampai selesai;
d. Memastikan agar segala gangguan yang diakibatkan oleh penutupan Privy dapat diminimalisasi;
e. Mengirimkan informasi CRL terakhir kepada Pemegang Sertifikat,Pengandal yang merupakan pengguna layanan Privy dan pihak lain yang terkait dengan proses pengakhiran layanan PSrE; dan

In the event that Privy CA terminates its services, then:

a. it provides notification via email to parties involved in the Certificate operational cycle, including to the Root CA, Subscribers, Relying Parties, and RA;
b. it ensures that Certificate information status remains accessible for a period of 2 (two) year after termination of service;
c. it ensures that the process of revocation of all Certificates at the time of closure is carried out to completion;
d. it ensures that any disruption caused by Privy's closure can be minimized;
e. it sends the updated CRL information to Subscribers and Relying Parties who are users of Privy services and other parties involved in the termination process of the CA; and
f. it destroys the Privy PKI system that contains the

f.	Menghancurkan sistem PKI Privy yang berisi Kunci Privat PSrE Privy dan Kunci Privat Pemegang Sertifikat.	Privy CA's Private Key and Subscriber's Private Key.
	Selain hal yang dikemukakan diatas lebih lanjut pengakhiran layanan PSrE akan dilakukan sesuai dengan Panduan Penutupan Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia. ketentuan terkait hak dan kewajiban yang berlaku bagi para pihak adalah sesuai dengan kesepakatan, sebagaimana telah disepakati dalam Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan, Pemberitahuan Privasi Privy, dan/ atau perjanjian lainnya.	In addition to the matters stated above, the termination of the CA services will be carried out in accordance with the Electronic Certification Authority (PSrE) Indonesia Closure Guidelines. The provisions related to the rights and obligations applicable to the parties shall be in accordance with the agreement, as agreed in the Subscriber Agreement, Terms and Conditions, Privy's Privacy Notice, and/or any other agreements.

6. Kontrol 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*

Pasangan Kunci PSrE Privy dibangkitkan melalui sistem PKI Privy, dan Kunci Privat PSrE Privy tidak boleh meninggalkan perangkat keras modul kriptografi (yang memenuhi persyaratan *Federal Information Protection Standards* (FIPS)-140-	Privy CA Key Pair is generated through the Privy PKI system, and Privy CA Key must not leave the cryptographic module hardware (which meets the requirements of Federal Information Protection Standards (FIPS)-140-2 Level 3) connected to

2 Level 3) yang terhubung dengan sistem tersebut.	the system.
Untuk Pasangan Kunci Pemegang Sertifikat dibangkitkan dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS-140-2 Level 3. Pasangan Kunci Pemegang Sertifikat yang dibangkitkan disimpan dan diamankan dengan menggunakan modul kriptografi yang memenuhi persyaratan FIPS-140-2 Level 2.	For Subscriber Key Pairs is generated using cryptographic modules that meet the FIPS-140-2 Level 3 requirements. The generated Certificate Holder's Key Pair is stored and secured using cryptographic modules that comply with FIPS-140-2 Level 2 requirements.
Dalam proses pembangkitan kunci, PSrE Privy menerapkan kendali multipersonel dan menyiapkan jejak audit yang menunjukkan bahwa persyaratan kebutuhan keamanan untuk prosedur telah diikuti. 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.	In the key generation process, Privy CA implements multi-personel controls and prepares an audit trail demonstrating that the security requirements for the procedure have been adhered to. An independent third party should validate the implementation of the key generation procedure either by witnessing the key generation or by examining the signed and documented records of the key generation.

6.1.2. Pengiriman Kunci Privat Kepada Pemegang Sertifikat / *Private Key Delivery to Subscriber*

Privy tidak melakukan pengiriman Kunci Privat kepada Pemegang Sertifikat.	Privy does not deliver the Private Key to the Subscriber.

6.1.3. Pengiriman Kunci Publik ke Privy / *Public Key Delivery to Privy*

Pasangan Kunci Pemegang Sertifikat dibangkitkan oleh Privy sehingga Privy secara langsung menyimpan dan melekatkan Kunci Publik Pemegang Sertifikat pada Sertifikat Pemegang Sertifikat setelah penerbitan pasangan kunci Pemegang Sertifikat dilakukan oleh Privy.	The Subscriber Key Pair is generated by Privy so that Privy directly stores and attaches the Subscriber's Public Key to the Subscriber's Certificate after the issuance of the Subscriber's key pair by Privy.

6.1.4. Pengiriman Kunci Publik PSrE Privy ke Pengandal / *Privy CA Public Key Delivery to the Relying Parties*

Kunci Publik PSrE Privy tidak dikirim kepada Pengandal, namun Pengandal dapat mengakses Kunci Publik tersebut melalui Repositori PSrE Privy. Penjelasan tanggung jawab tentang publikasi dan repositori sertifikat mengacu pada bagian 2.1.	Privy CA Public Key is not delivered to the Relying Parties, but the Relying Parties can access the Public Key through the Privy CA Repository. Explanation of responsibilities regarding certificate publication and repository shall refer to section 2.1.

6.1.5. Ukuran Kunci / *Key Sizes*

Sertifikat	*Digest Algorithm*	*Encryption Algorithm*	Panjang Kunci
Privy CA	SHA-256	RSA	4096-bit
End User	SHA-256	ECC	256-bit

Certificate	Digest Algorithm	Encryption Algorithm	Key Length
Privy CA	SHA-256	RSA	4096-bit
End User	SHA-256	ECC	256-bit

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

Privy membangkitkan Pasangan Kunci PSrE Privy dengan menggunakan modul kriptografi sesuai standar FIPS 140-2 level 3 dan menggunakan suatu metode yang wajar untuk memvalidasi kesesuaian Kunci Publik yaitu FIPS 186-4. Privy melakukan pemeriksaan secara berkala untuk menguji ukuran Kunci dan memastikan pemutakhiran berdasarkan standar keamanan industri dan persyaratan regulasi.

Privy generates Privy CA Key Pairs using cryptographic modules according to FIPS 140-2 level 3 standards and uses a reasonable method to validate the suitability of Public Keys, namely FIPS 186-4. Privy performs periodic checks to test the Key size and ensure updates based on industry security standards and regulatory requirements.

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

Kunci Privat PSrE Privy dan Pemegang Sertifikat digunakan sesuai dengan penjelasan yang

Privy CA's Private Keys and Subscriber's Private Keys are used in accordance with the

disampaikan pada Profil Sertifikat sebagaimana dimaksud pada bagian 10.

explanation provided in the Certificate Profile as referred to in section 10.

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

Untuk melindungi Kunci Privat PSrE Privy dari penyalahgunaan atau pengaksesan secara tidak sah, Privy melakukan upaya terbaik untuk:

a. Mengamankan semua akses dan kontrol pasangan kunci.
b. Mengimplementasikan prosedur yang mampu mencegah, menjaga, mengawasi dan melakukan mitigasi terhadap informasi rahasia dari akses tidak sah, perubahan tidak sah, kerusakan data, dan kebocoran informasi rahasia.

To protect Privy CA's Private Keys from any misuse or unauthorized access, Privy makes its best efforts to:

a. Secure all key pair access and control.
b. Implement procedures capable of preventing, safeguarding, monitoring and mitigating confidential information from unauthorized access, unauthorized changes, data corruption and leakage of confidential information.

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

PSrE Privy menjamin semua sistem untuk menandatangani Sertifikat dan CRL atau menerbitkan respon OCPS menggunakan perangkat FIPS 140-2 Level 3 sebagai tingkat minimum perlindungan kriptografis.

PSrE Privy ensures that all systems used for signing Certificates and CRL or issuing OCSP responses utilize FIPS 140-2 Level 3 devices as the minimum level of cryptographic protection.

Kunci Privat PSrE Privy dan Pemegang Sertifikat dibangkitkan oleh perangkat modul kriptografi yang memenuhi standar FIPS 140-2 Level 3. Untuk operasi penandatanganan, Privy juga menggunakan perangkat modul kriptografi dengan standar yang sama.Pemilik mengakses Kunci Privatnya yang telah dibangkitkan oleh Privy dengan menerapkan kombinasi 2 (dua) faktor autentikasi.	Privy CA and Subscriber's Private Keys are generated by a cryptographic module that meets the FIPS 140-2 Level 3 standard. For signing operations, Privy also uses a cryptographic module with the same standard. The end user accesses his Private Key that has been generated by Privy by applying a combination of 2 (two) authentication factors.

6.2.2. Kendali Multipersonel (n dari m) Kunci Privat PSrE / *Multipersonnel Control (n of m) CA Private Key*

Privy menerapkan mekanisme teknis dan prosedur yang mensyaratkan partisipasi dari beberapa (m dari n) *Trusted Personnel Roles* untuk melakukan operasi dan fungsi kriptografi yang sensitif seperti *backup* kunci penandatanganan PSrE Privy dan akses ke kunci penandatanganan PSrE Privy yang di-*backup* untuk pemulihan bencana.	Privy implements technical mechanisms and procedures that require the participation of several (m out of n) Trusted Personel Roles to perform sensitive cryptographic operations and functions such as backup of Privy CA signing keys and access to Privy CA backed-up signing keys for disaster recovery.
Modul Kriptografis yang memuat seluruh kunci penandatanganan PSrE Privy tidak dapat diaktivasi atau diakses hanya oleh 1 (satu) orang.	The Cryptographic Module that contains all c Privy signing keys cannot be activated or accessed by only 1 (one) person.

PSrE Privy mencatat nama-nama pihak yang terlibat dalam kendali multipersonel dalam sebuah daftar yang tersedia untuk pemeriksaan audit.

Privy CA records the names of parties involved in multipersonnel control in a list available for audit checks.

6.2.3. Eskro Kunci Privat / *Private Key Escrow*

Kunci Privat PSrE Privy dan Kunci Privat Pemegang Sertifikat tidak boleh dan tidak akan pernah dititipkan sebagaimana diatur dalam bagian 4.12.1.

Privy CA's Private Key and Subscriber's Private Key must not and will never be escrowed as stipulated in section 4.12.1.

6.2.4. Cadangan (*Backup*) Kunci Privat / *Private Key Backup*

Untuk menjaga keberlangsungan layanan, pasangan Kunci PSrE Privy dicadangkan dan disimpan secara aman dengan kendali multipersonel yang sama dengan Pasangan Kunci asli. Kunci Privat Pemegang Sertifikat tidak dicadangkan oleh PSrE Privy.

To maintain the continuity of services, Privy CA Key pairs are backed up and stored securely with the same multi-personnel control as the original Key Pair. Subscriber's Private Key are not backed up by PSrE Privy.

PSrE Privy tidak menyalin Pasangan Kunci Pemegang Sertifikat. Dalam hal Pasangan Kunci Pemegang Sertifikat akan disalin, semua salinan Pasangan Kunci yang dibangkitkan dilindungi dengan standar dan mekanisme yang sama dengan Pasangan Kunci asli. Salinan Pasangan Kunci tersebut disimpan dalam lokasi fisik yang berbeda dari Pusat Data.

Subscriber Key Pairs are copied and safeguarded by Privy with its best efforts. All copies of the generated Key Pair are protected with the same standards and mechanisms as the original Key Pair. Copies of such Key Pairs are stored in a different physical location from the Data Center.

6.2.5. Pengarsipan Kunci Privat / *Private Key Archival*

Kunci Privat PSrE Privy dan Kunci Privat *Signing* Pemegang Sertifikat tidak diarsipkan.	Privy CA Private Key and the Subscriber's Signing Private Key are not archived.

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

Kunci Privat PSrE Privy dibangkitkan dan disimpan dalam modul kriptografi. Jika ada penyalinan dengan tujuan kelangsungan dan pemulihan layanan, Kunci Privat akan disalin dalam keadaan terenkripsi ke modul kriptografi dengan standar/level keamanan yang sama. Di luar modul kriptografi, Kunci Privat PSrE Privy tidak akan pernah ditemukan dalam bentuk teks sederhana (*plaintext*). Dalam hal PSrE Privy mengetahui bahwa Kunci Privat disampaikan kepada orang atau entitas yang tidak berwenang, maka PSrE Privy akan mencabut semua Sertifikat yang memuat Kunci Publik yang berasosiasi dengan Kunci Privat yang telah disampaikan tersebut.	The Privy CA Key is generated and stored in the cryptographic module. If there is any copying for the purpose of service continuity and restoration, the Private Key will be copied in an encrypted state to the cryptographic module with the same security standard/level. Outside the cryptographic module, the Privy CA Key will never be found in plaintext. In the event that Privy CA becomes aware that the Private Key has been disclosed to unauthorized individuals or entities, the Privy CA will revoke all Certificates containing the Public Key associated with the aforementioned disclosed Private Key.

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

Kunci Privat PSrE Privy disimpan pada modul kriptografi yang	Privy CA's Private Key is stored in a cryptographic module that

memenuhi standar FIPS 140-2 minimum level 3 dalam keadaan terenkripsi dan dilindungi oleh mekanisme teknis yang menjaga kunci dari akses tidak sah. Sedangkan untuk Kunci Privat Pemegang Sertifikat disimpan pada modul kriptografi yang memenuhi standar FIPS 140-2 minimum level 2.

meets the FIPS 140-2 minimum level 3 standard in an encrypted state and is protected by technical mechanisms that guard the key from unauthorized access. Meanwhile, the Subscriber's Private Key is stored in a cryptographic module that meets the minimum FIPS 140-2 standard level 2.

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

Kunci Privat PSrE Privy diaktifkan dengan mekanisme yang telah disediakan oleh penyedia modul kriptografi dan sesuai dengan prosedur dan standar keamanan informasi. Operasi pengaktifan Kunci Privat Privy melalui kendali multipersonel yang telah dinyatakan dalam CPS di bagian 5.2.2.

Privy CA's Private Key is activated by a mechanism provided by the cryptographic module provider and in accordance with information security procedures and standards. Privy Private Key activation operation is carried out through multi-personnel control that has been stated in the CPS in section 5.2.2.

Pengaktifan dan akses Kunci Privat Pemegang Sertifikat dilindungi dengan mekanisme keamanan yang dikendalikan, diawasi, dijaga, dan diatur oleh Privy. Pengaktifan Kunci Privat Pemegang Sertifikat dilakukan dengan cara mengautentikasi Pemegang Sertifikat ke modul kriptografis sebelum melakukan

The activation and access of the Subscriber's Private Key is protected with security mechanisms controlled, supervised, maintained, and regulated by Privy. Activation of the Subscriber's Private Key is done by authenticating the Certificate Holder to the cryptographic module before

aktivasi Kunci Privat terkait dengan menggunakan PIN. Entri data aktivasi harus dilindungi dari pengungkapan (data tidak boleh ditampilkan saat dimasukkan).

activating the associated Private Key using a PIN. Activation data entry must be protected from disclosure (data must not be displayed when entered).

Pemegang Sertifikat bertanggung jawab untuk melindungi Kunci Privat sesuai dengan kewajiban yang diatur dalam Perjanjian Pemegang Sertifikat Privy.

The Subscriber is responsible for protecting the Private Key in accordance with the obligations set forth in the Privy Subscriber Agreement.

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

Privy melakukan pengawasan terhadap modul kriptografis yang sudah diaktivasi dan memastikan modul kriptografis tidak ditinggal tanpa pengawasan dan tidak dapat diakses secara tidak sah. Dalam hal modul kriptografis harus dinonaktifkan, maka akan dilakukan oleh *Trusted Personnel Role(s)* terkait.

Privy CA shall exercise supervision over the activated cryptographic module and ensure that the cryptographic module is not left unattended and cannot be accessed unlawfully. In the event that the cryptographic module must be deactivated, such deactivation shall be carried out by the relevant Trusted Personnel Role(s).

Kunci Privat Pemilik akan dihancurkan ketika Sertifikat atau Kunci Privat tidak lagi diperlukan sesuai dengan ketentuan bagian 6.2.10 CPS ini.

The Subscriber's Private Key will be destroyed when the Certificate or Private Key is no longer required in accordance with the provisions of section 6.2.10 of this CPS.

6.2.10. Metode Menghancurkan Kunci Privat / *Methods of Destroying Private Key*

Trusted Personnel Role(s) menghancurkan Kunci Privat PSrE Privy ketika Kunci Privat tidak lagi diperlukan untuk kelangsungan layanan dengan cara menghapus atau menghancurkan Kunci Privat beserta dengan cadangannya sesuai dengan prosedur yang telah disediakan oleh penyedia modul kriptografi (termasuk diantaranya dengan cara *factory reset*).	Trusted Personnel Role(s) destroys the Privy CA's Private Key when the Private Key is no longer required for service continuity by deleting or destroying the Private Key along with its backup in accordance with the procedures provided by the cryptographic module provider (including by factory reset).
Kunci Privat Pemegang Sertifikat dihancurkan ketika Sertifikat atau Kunci Privat tidak lagi diperlukan. Hal ini dilakukan dengan mekanisme teknis tertentu yang dapat menjamin tidak ada kehilangan, pencurian, atau penggunaan tidak sah dari Kunci Privat maupun Sertifikat terkait.	The Subscriber's Private Key is destroyed when the Certificate or Private Key is no longer needed. This is carried out with certain technical mechanisms that can guarantee no loss, theft, or unauthorized use of the Private Key or associated Certificate.
Penghancuran Kunci Privat Privy dicatat dalam log sesuai ketentuan pencatatan log pada bagian 5.4.	The destruction of the Privy Key is recorded in the log according to the logging provisions in section 5.4.

6.2.11. Peringkat Modul Kriptografi / *Cryptographic Module Rating*

Sesuai dengan yang tercantum pada bagian 6.2.1.	As listed 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*

Privy mengarsipkan setiap Kunci Publik yang dibangkitkan minimal 5 (lima) tahun.

Privy archives every Public Key generated for a minimum of 5 (five) years.

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

Periode operasi pasangan kunci ditentukan oleh periode operasional Sertifikat yang sesuai. Jangka waktu operasional maksimum pasangan kunci ditentukan sebagai berikut:

Jenis Sertifikat	Jangka Waktu Operasional Sertifikat	Jangka Waktu Operasional Kunci Privat
Privy CA Class 3	10 Tahun	10 Tahun
Privy CA Class 4	10 Tahun	10 Tahun
Sertifikat Level 2/Kelas 3	Maksimal 2 Tahun	Maksimal 2 Tahun

The operating period of the key pair is determined by the operating period of the corresponding Certificate. The maximum operational period of a key pair is determined as follows:

Types of Certificate	Certificate Operational Period	Operational Period of Private Key
Privy CA Class 3	10 Years	10 Years
Privy CA Class 4	10 Years	10 Years
Certificate Level 2/Class 3	Maximum 2 Years	Maximum 2 Years
Certificate Level 3/Class 4	Maximum 2 Years	Maximum 2 Years
Time	1 Year	1 Year

Sertifikat Level 3/Kelas 4	Maksimal 2 Tahun	Maksimal 2 Tahun
Time Stamp Authority	1 Tahun	1 Tahun
OCSP Responder	1 Tahun	1 Tahun

Stamp Authority		
OCSP Responder	1 Year	1 Year

6.4. Data Aktivasi / *Activation Data*

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

Pembangkitan dan penggunaan data pengaktifan untuk mengaktifkan Kunci Privat PSrE Privy dilakukan melalui upacara kunci. Data pengaktifan dibangkitkan secara otomatis oleh modul kriptografi dengan menggunakan kartu pintar yang dilindungi oleh kata sandi yang kuat dan harus memenuhi kuorum yang telah ditentukan (n dari m). Kartu pintar diserahkan dan disimpan secara aman kepada *Trusted Personnel Roles* yang telah memenuhi kualifikasi yang telah ditentukan dan melalui pengecekan latar belakang.

The generation and use of activation data to activate the Privy CA Key is carried out through a key ceremony. The activation data is generated automatically by the cryptographic module using a smart card that is protected by a strong password and must meet a predefined quorum (n out of m). The smart cards are handed over and stored securely to Trusted Personnel Roles that have met the predefined qualifications and undergone background checks.

PSrE Privy melindungi data aktivasi untuk mengaktifkan Kunci Privat berdasarkan tingkat keamanan yang sesuai dengan modul kriptografis yang digunakan oleh personil yang ditunjuk untuk melakukan kegiatan security dan sesuai dengan akses kontrol yang telah ditetapkan pada *script key ceremony* di modul kriptografi yang digunakan. Penggunaan data aktivasi Kunci Privat Pemegang Sertifikat harus dimasukkan oleh Pemegang Sertifikat itu sendiri.

Privy CA protects the activation data used to activate the Private Key based on a security level appropriate to the cryptographic module utilized by personnel designated to perform security activities, and in accordance with the access controls established in the key ceremony script of the cryptographic module. The use of the Subscriber's Private Key activation data must be entered by the Subscriber's themselves.

6.4.2. Perlindungan Data Aktivasi / *Activation Data Protection*

Data pengaktifan PSrE Privy dilindungi menggunakan mekanisme kontrol akses fisik dan teknologi kriptografi. Data pengaktifan disimpan dalam kartu pintar yang diserahkan kepada *Trusted Personnel Roles* dan telah memenuhi kualifikasi dan pengecekan latar belakang yang telah ditentukan.

Privy CA activation data is protected using physical access control mechanisms and cryptographic technologies. Activation data is stored in smart cards that are assigned to Trusted Personnel Roles and have met predefined qualifications and background checks.

Pemegang Sertifikat diwajibkan untuk selalu menjaga kerahasiaan data aktivasi. PSrE Privy menyediakan prosedur untuk penguncian akun sementara dalam hal Pemegang

Subscriber's are required to always maintain the confidentiality of activation data. Privy CA provides procedures for temporary account lockout in the event

Sertifikat mengalami kegagalan *login* dengan jumlah yang ditentukan.	that the Subscriber's experiences a specified number of login failures.

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

Data aktivasi Kunci Privat PSrE Privy hanya dikuasakan kepada *Trusted Personnel Roles* yang telah ditentukan.	Privy CA's Private Key activation data is only authorized to the specified Trusted Personnel Roles.

6.5. Kontrol Keamanan Komputer / *Computer Security Control*

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

Privy memastikan premis dan perangkat keras yang menjaga komponen perangkat lunak Privy aman dari akses yang tidak sah. Privy melaksanakan mekanisme teknis dan prosedur yang memastikan keamanan informasi pada sistem Privy. Semua akses terhadap informasi terkait Privy tercatat dan memerlukan autentikasi identitas berdasarkan pembatasan kontrol akses layanan untuk setiap *Trusted Personnel Roles*. Semua akses menjadi catatan audit yang dilindungi untuk tujuan pencegahan dan penanggulangan risiko keamanan informasi.	Privy ensures the availability of premise and hardware that keep Privy software components safe from unauthorized access. Privy implements technical mechanisms and procedures that ensure the security of information on the Privy system. All access to Privy-related information is recorded and it requires identity authentication based on service access control restrictions for each Trusted Personel Roles. All accesses become protected audit logs for the purpose of preventing and mitigating information security risks.
Fungsi keamanan komputer berikut disediakan oleh	The following computer security functions are provided by a

kombinasi sistem operasi, perangkat lunak, dan perlindungan fisik yang mencakup namun tidak terbatas kepada:

a. Akses masuk menggunakan autentikasi identitas.
b. Memberikan akses kontrol berdasarkan dokumen kebijakan *user access matrix*.
c. Menyediakan kemampuan dan sumber daya untuk keperluan audit keamanan.
d. Menyediakan jalur dan mekanisme terpercaya untuk akses sistem dengan menggunakan kriptografi untuk sesi komunikasi dan keamanan basis data.
e. Menyediakan perlindungan mandiri untuk sistem operasi
f. Mewajibkan penggunaan kebijakan kata sandi kuat (*strong password policy*);
g. Mewajibkan penggunaan saluran terpercaya untuk identifikasi dan autentikasi;
h. Menyediakan perlindungan terhadap kode jahat (*malicious code*);
i. Memberikan kemampuan untuk melakukan pemeriksaan terhadap standar dari perangkat lunak dan perangkat keras yang

combination of operating system, software, and physical protection which includes but is not limited to:

a. Login access using identity authentication.
b. Providing access control based on the user access matrix policy document.
c. Providing capabilities and resources for security audit purposes.
d. Providing trusted lines and mechanisms for system access through the utilization of cryptography for communication sessions and database security.
e. Providing standalone protection for the operating system
f. Requiring the use of a strong password policy;
g. Requiring the use of trusted channels for identification and authentication;
h. Providing protection against malicious codes;
i. Providing the ability to check the standards of installed software and hardware against the standards set through internal company policies.
j. Providing the ability to

terpasang dengan standar yang telah ditetapkan melalui kebijakan internal perusahaan.

j. Memberikan kemampuan untuk menerapkan praktik keamanan terbaik industri seperti penggunaan kata sandi yang kuat, penggunaan jalur komunikasi yang terenkripsi, melakukan isolasi terhadap setiap proses domain, dan menyediakan kemampuan melindungi diri sendiri untuk sistem operasi.

implement industry best security practices such as the use of strong passwords, the use of encrypted communication lines, isolating each domain process, and providing self-protection capabilities for the operating system.

Perangkat Privy beroperasi dengan konfigurasi yang telah dievaluasi untuk menjaga standar keamanan komputer.

Privy devices operate with configurations that have been evaluated to maintain computer security standards.

6.5.2. Peringkat Keamanan Komputer / *Computer Security Rating*

Privy memastikan bahwa untuk menjamin tingkat keamanan komputer yang digunakan oleh Privy, semua perangkat komputer telah memenuhi persyaratan keamanan FIPS 140-2 Level 1.

Privy ensures that to guarantee the level of computer security used by Privy, all computer devices have met FIPS 140-2 Level 1 security requirements.

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

6.6.1. Kendali Pengembangan Sistem / *System Development Controls*

Privy melakukan kendali pengembangan sistem sebagai berikut:

Privy exercises control over the development of the system as follows:

1. Menggunakan perangkat lunak yang dirancang dan dikembangkan melalui metodologi yang formal dan terdokumentasi;
2. Pengadaan perangkat keras dan perangkat lunak telah dilakukan dengan upaya-upaya untuk mengurangi kemungkinan komponen yang terdapat dalam perangkat lunak yang dirusak;
3. Pengembangan perangkat keras dan perangkat lunak telah dilakukan dalam sebuah lingkungan yang terkendali dan proses pengembangan didefinisikan dan didokumentasikan;
4. Perangkat keras dan perangkat lunak didedikasikan untuk pelaksanaan aktivitas KPI.
5. Perawatan yang cukup dilakukan untuk mencegah perangkat lunak yang berbahaya untuk dimuat ke perangkat. Privy telah melakukan scan secara berkala terhadap kode-kode berbahaya pada perangkat keras dan perangkat lunak; dan
6. Pembaruan perangkat keras dan perangkat lunak dibeli

1. Utilizing software that is designed and developed through formal and documented methodologies;
2. Hardware and software procurement has been conducted with efforts to minimize the likelihood of components compromised within the software;
3. Development of hardware and software has occurred within a controlled environment, with defined and documented development processes;
4. Hardware and software are dedicated to the execution of KPI activites;
5. Adequate measurer are taken to prevent the loading of harmful software onto the devices. Privy conducts periodic scans for malicious code in both hardware and software; and
6. Hardware and software updates are acquired or developed in the same manner as the original devices and are installed by trusted

atau dikembangkan dengan cara yang sama dengan perangkat aslinya dan diinstal oleh personel yang terpercaya dan terlatih melalui langkah-langkah yang terdokumentasi.	and trained personnel through documented procedures.
Privy melakukan pengujian di lingkungan non-produksi terhadap perangkat lunak siap pakai maupun perangkat lunak yang dikembangkan sendiri yang digunakan untuk manajemen produksi sebelum diterapkan di lingkungan produksi. Setiap perubahan sistem atau komponennya telah melalui proses reviu Kontrol Manajemen Perubahan dan persetujuan pihak-pihak terkait.	Privy conducts testing in a non-production environment on both off-the-shelf software and internally developed software utilized for production management, prior to their implementation in the production environment. Any system or component modifications have undergone the Change Management Control review proves and received approval from relevant parties.

6.6.2. Kendali Manajemen Keamanan / *Security Management Controls*

Segala perubahan pada konfigurasi sistem PKI milik Privy tercatat dan dikontrol oleh prosedur yang telah ditentukan. Prosedur ini mencakup pencegahan akses dan perubahan tidak sah. Semua perangkat yang disediakan oleh pihak ketiga yang terpasang divalidasi bahwa terbebas dari segala perubahan di luar yang telah ditentukan.	Any changes to Privy's PKI system configuration are recorded and controlled by defined procedures. These procedures include the prevention of unauthorized access and changes. All installed devices provided by third parties are validated to be free of any changes beyond those specified.

Metode manajemen konfigurasi resmi harus digunakan untuk instalasi dan pemeliharaan sistem PSrE Privy. PSrE Privy memastikan Perangkat lunak yang akan digunakan pertama kali harus diverifikasi bahwa perangkat lunak tersebut benar berasal dari penyedia, tanpa modifikasi dan benar merupakan versi yang ingin digunakan.	Authorized configuration management methods must be used for installation and maintenance of Privy CA systems. Privy CA ensures that the software to be used for the first time must be verified that the software comes from the provider, without modification and is the correct version to be used.

6.6.3. Kendali Keamanan Siklus Hidup / *Life Cycle Safety Controls*

Privy memastikan dan menjaga tingkat kepercayaan dan keamanan semua komponen perangkat lunak dan perangkat keras PKI secara berkala.	Privy ensures and maintains the trustworthiness and security of all PKI software and hardware components on a regular basis.

6.7. Kendali Keamanan Jaringan / *Network Security Control*

Privy melakukan upaya yang wajar untuk melindungi jaringan semua komponen PKI pada Privy dari serangan seperti namun tidak terbatas pada *Denial of Service* (DoS), *Slowloris*, *Goloris* dan serangan intrusi. Upaya-upaya tersebut termasuk namun tidak terbatas pada penggunaan *firewall*, pembatasan dan penjaringan akses jaringan, dan memasang sistem pengawasan jaringan. Privy juga menggunakan jaringan aman terpercaya yang secara khusus	Privy makes reasonable efforts to protect the network of all PKI components of Privy from attacks such as but not limited to Denial of Service (DoS), Slowloris, Goloris and intrusion attacks. These efforts include but are not limited to using firewalls, restricting and filtering network access, and installing network monitoring systems. Privy also utilizes a trusted secure network that has been specifically provided for remote access of PKI

yang telah disediakan untuk akses *remote* komponen PKI. Hanya perangkat lunak jaringan yang diperlukan untuk mengoperasikan layanan Privy yang diizinkan.

components. Only network software required to operate Privy's services is permitted.

6.8. Stempel Waktu / *Time-Stamps*

Privy melakukan upaya yang wajar mengkonfigurasi dan menjaga sinkronisasi jam sistem internal semua komponen CA menggunakan *Network Time Protocol*.

Privy makes reasonable efforts to configure and maintain synchronization of the internal system clocks of all CA components using Network Time Protocol.

Sistem ini digunakan sebagai stempel waktu untuk:

a. Validasi waktu awal penerbitan Sertifikat Induk CA;
b. Waktu pencabutan Sertifikat;
c. Penjadwalan penerbitan CRL; and
d. Validasi waktu penerbitan Sertifikat Pemegang Sertifikat.
e. Respon OCSP

This system is used as a time-stamp for:

a. Validation of initial time of issuance of the CA Root Certificate;
b. Certificate revocation time;
c. Scheduling of CRL issuance; and
d. Validation of Subscriber Certificate issuance time.
e. OCSP Response

Privy memeriksa dan memastikan bahwa seluruh sistem yang menggunakan stempel waktu tersinkronisasi dengan waktu yang disediakan oleh URL

Privy checks and ensures that all systems that use time-stamps are synchronized with the time provided by the URL https://www.pool.ntp.org/zone/id. Clock matching is an

https://www.pool.ntp.org/zone/id. Pencocokan jam merupakan sebuah aktivitas yang dapat diaudit.	auditable activity.

7. Profil Sertifikat, CRL, dan OCSP / *Certificate, CRL and OCSP Profiles*

7.1. Profil Sertifikat / *Certificate Profile*

Sertifikat dan *Certificate Revocation List* (CRL) yang diterbitkan oleh Privy tunduk terhadap standar dan spesifikasi yang tercantum pada IETF RFC 5280 Internet X.509 *PKI Certificate and Certificate Revocation List* (CRL) *Profile*.	Certificates and Certificate Revocation List (CRL) issued by Privy are subject to the standards and specifications listed in IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.
Semua Sertifikat yang diterbitkan oleh Privy memiliki nomor serial dengan panjang setidaknya 64 bit dengan nilai yang lebih dari nol (0).	All Certificates issued by Privy have a serial number that is at least 64 bits long with a value greater than zero (0).
Lampiran 1 berisi profil Sertifikat untuk masing-masing klasifikasi Sertifikat yang diterbitkan oleh Privy dan telah mengacu ke Standar Interoperabilitas yang diterbitkan oleh PSrE Induk.	Appendix 1 contains Certificate profiles for each of the Certificate classifications issued by Privy and has been referenced to the Interoperability Standard issued by the Root CA.

7.2. Profil CRL / *CRL Profile*

Privy menerbitkan CRL dalam format X.509 versi 2 yang tunduk terhadap standar dan spesifikasi yang tercantum pada Standar Interoperabilitas yang	Privy publishes CRLs in X.509 version 2 format that are subject to the standards and specifications listed in the Interoperability Standards

diterbitkan oleh PSrE Induk dan IETF RFC 5280.

published by PSrE Induk in IETF RFC 5280.

7.3. Profil OCSP / *OCSP Profile*

Online Certificate Status Profile (OCSP) yang diatur oleh Privy patuh terhadap standar yang ada pada Standar Interoperabilitas yang diterbitkan oleh PSrE Induk, IETF RFC 6960 dan IETF RFC 5019.

Online Certificate Status Profile (OCSP) set up by Privy complies with the standards in the Interoperability Standards published by Root CA, IETF RFC 6960 and IETF RFC 5019.

8. Audit Kepatuhan dan Penilaian Kelaikan Lainnya / *Compliance Audits and Other Fitness Assessments*

PSrE Privy melaksanakan Penilaian Kelaikan atau Audit Kepatuhan sebagaimana dipersyaratkan oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikat elektronik dan sesuai dengan standar industri. Privy telah memenuhi audit untuk memastikan semua persyaratan pada CPS ini telah diimplementasikan dan diaudit berdasarkan standar antara lain:

a. WebTrust – Principles and Criteria for Certification Authorities;
b. SNI ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi; dan
c. SNI ISO/IEC 27701:2019 Sistem Manajemen Informasi Privasi.

Privy CA conducts a Feasibility Assessment or Compliance Audit as required by the laws and regulations governing the provision of electronic certificates and in accordance with industry standards. Privy has fulfilled audits to ensure all requirements in this CPS have been implemented and audited based on standards including:

a. WebTrust – Principles and Criteria for Certification Authorities;
b. SNI ISO/IEC 27001:2022 Information Security Management System; and
c. SNI ISO/IEC 27701:2019 Privacy Information Management System.

8.1. Frekuensi atau Lingkup Penilaian / *Frequency or Scope of Assessment*

Implementasi dari CPS ini dijalankan dengan maksud untuk memenuhi kriteria dari standar yang dikeluarkan oleh Kominfo dan juga standar industri internasional.	The implementation of CPS is carried out with the intention of meeting the criteria of the standards issued by the Ministry of Communication and Information Technology (MCIT) and also international industry standards.
Privy diaudit minimal 1 (satu) kali setahun sebagaimana dipersyaratkan oleh peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik dan juga diaudit sesuai kebutuhan standar industri lainnya.	Privy is audited at least 1 (one) year as required by the laws and regulations regarding the implementation of electronic certification and is also audited according to the needs of other industry standards.
Privy juga mengirimkan laporan tahunan kepada Kominfo sesuai dengan ketentuan yang diatur di dalam peraturan perundang-undangan mengenai penyelenggaraan sertifikasi elektronik.	Privy also submits annual reports to the Ministry of Communication and Information in accordance with the provisions stipulated in the laws and regulations regarding the implementation of electronic certification.

8.2. Identitas/kualifikasi Penilai / *Identity/qualification of Auditor*

Audit eksternal dilakukan oleh Penilai Terkualifikasi yang independen, kredibel, memahami dan berpengalaman di bidang keamanan informasi dan PKI, diakui oleh Kominfo untuk	External audits are conducted by Qualified Auditors who are independent, credible, understand and experienced in the field of information security and PKI, recognized by MCIT for

sertifikasi dari Kominfo dan/atau diakui oleh AICPA/CICA sebagai penyelenggara jaminan sertifikasi dari *Webtrust* untuk sertifikasi *Webtrust*.

Secara spesifik, kriteria Penilai Terkualifikasi harus memiliki kualifikasi berikut:

a. Penilai harus memiliki tim asesmen independen yang qualified;
b. tidak memiliki konflik kepentingan terhadap PSrE Privy;
c. Penilai harus memiliki kemampuan untuk melakukan audit berdasarkan standar audit dalam ketentuan peraturan perundang-undangan termasuk pengetahuan terkait pemanfaatan layanan yang menggunakan Sertifikat Elektronik seperti Tanda Tangan Elektronik, Segel Elektronik Sertifikat, X.509 versi 3 *PKI Certificate Policy and Certification Practices Framework*, Undang-Undang tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah

certification from MCIT and/or recognized by AICPA/CICA as a certification guarantee provider from Webtrust for Webtrust certification.

Specifically, the Qualified Auditor criteria must have the following qualifications:

a. The auditor must have a qualified independent assessment team;
b. The auditor has no conflict of interest with Privy CA;
c. The auditor must have the ability to conduct audits based on audit standards in the provisions of laws and regulations including knowledge related to the utilization of services that use Electronic Certificates such as Electronic Signatures, Electronic Seal Certificates, X.509 version 3 PKI Certificate Policy and Certification Practices Framework, Law on Electronic Information and Transactions, Government Regulations on the Implementation of

tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan Peraturan Menteri Kominfo terkait Tata Kelola Penyelenggaraan Sertifikasi Elektronik;

d. Memiliki kecakapan dalam audit keamanan informasi, peralatan dan teknik keamanan informasi, dan teknologi IKP;
e. Penilai harus memiliki bukti bahwa dirinya memenuhi kualifikasi penilai untuk suatu skema audit. Bisa dibuktikan dengan sertifikasi seperti antara lain auditor sistem informasi (CISA) atau *IT Security specialist*, akreditasi, lisensi, atau asesmen lain yang sah;
f. Menguasai beberapa keahlian tertentu, pengujian kompetensi, langkah-langkah jaminan kualitas seperti tinjauan sejawat, standar berkenaan dengan penugasan staf yang tepat, hingga keterlibatan dan persyaratan untuk melanjutkan pendidikan profesional; dan

Electronic Systems and Transactions, and Regulations of the Minister of Communication and Information Technology related to Governance of Electronic Certification Implementation;

d. The auditor must have the proficiency in information security auditing, information security tools and techniques, and IKP technology;
e. The auditor must have the evidence that they meet the auditors qualifications for an audit scheme. This may be evidenced by certification, accreditation, license, or other valid assessments;
f. The auditor must have the certain skills, competency testing, quality assurance measures such as, among others, Certified Information Systems Auditor (CISA) or IT Security Specialist, peer review, standards

g. Patuh terhadap hukum, kebijakan pemerintah, atau kode etik profesional.

regarding appropriate staff assignments, and involvement and requirements for continuing professional education; and

g. The auditor must comply with laws, government policies, or professional codes of conduct.

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

Penilai yang dipilih untuk melakukan audit merupakan penilai independen di luar Privy dan telah memiliki hubungan kontraktual dengan Privy dalam melakukan audit. Penilai harus mempertahankan standar etika yang tinggi yang dirancang untuk memastikan ketidakberpihakan dan pelaksanaan penilaian profesional yang independen, dengan tunduk pada ketentuan perundang-undangan yang berlaku.

The auditors selected to conduct the audit shall be independent auditors outside Privy and has established a contractual relationship with Privy for the purpose of conducting the audit. The auditors must maintain high ethical standards designed to ensure impartiality and the conduct of an independent professional assessment, subject to applicable laws and regulations.

8.4. Topik Penilaian / *Topics Covered by Assessment*

Penilaian Kelaikan bertujuan untuk memverifikasi bahwa PSrE Privy beroperasi sesuai dengan CP PSrE Induk yang berlaku dan ketentuan peraturan perundang-undangan. Penilaian Kelaikan mencakup penilaian CPS Privy

The purpose of the Assessment is to verify that Privy CA is operating in accordance with the applicable Root CA CP and regulatory requirements. The assessment includes the CPS Privy assessment that applies to

yang berlaku terhadap CP PSrE Induk, untuk menentukan bahwa CPS tersebut telah diimplementasikan dan ditegakkan. Penilaian ini paling sedikit mencakup organisasi, operasional, pelatihan personel, dan manajemen Privy.

the Root CA CP, to determine that the CPS has been implemented and enforced. This assessment covers at least Privy's organization, operations, personnel training, and management.

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

Ketika Penilai kepatuhan menemukan adanya ketidaksesuaian antara bagaimana PSrE dirancang atau dioperasikan atau dipelihara terhadap CP PSrE Induk yang berlaku dan CPS ini maka:

a. Mencatat ketidaksesuaian tersebut;
b. Penilai kepatuhan harus secara segera menyampaikan temuan tersebut kepada PA; dan
c. Melaporkan ke PSrE Induk

When the compliance Auditor finds a discrepancy between how the CA is designed or operated or maintained against the applicable Root CA CP and this CPS, then:

a. Record the non-conformity
b. The compliance auditor must promptly communicate the findings to the PA; and
c. Report to the PSrE Induk

PA harus menentukan pemberitahuan atau tindakan perbaikan lebih lanjut mengenai hal-hal yang diperlukan sesuai dengan persyaratan CPS dan kontrak masing-masing, kemudian melanjutkan untuk membuat pemberitahuan tersebut dan melakukan tindakan

The PA shall determine what further notifications or remedial actions regarding such matters are required in accordance with the requirements of the CPS and the respective contract, then proceed to make such notifications and undertake

perbaikan tersebut tanpa penundaan.

such remedial actions without delay.

8.6. Laporan Hasil Penilaian / *Communication of Result*

Laporan hasil penilaian termasuk identifikasi tindakan perbaikan yang dilakukan atau diambil oleh Privy dilaporkan kepada PA paling lambat 7 hari kerja setelah Penilaian selesai dilakukan. Privy meneruskan dan mengkomunikasikan laporan tersebut kepada pihak-pihak lain yang berkepentingan sesuai dengan kesepakatan di dalam perjanjian dan peraturan perundang-undangan yang berlaku serta sesuai ketentuan bagian 8.5.

The assessment report including the identification of corrective actions performed or taken by Privy, must be submitted to the PA no later than 7 working days after the assessment is completed. Privy will forward and communicate the report to other relevant parties in accordance with the agreements within the contract and applicable laws and regulations, as well as the provisions of section 8.5.

8.7. Audit Internal / *Internal Audit*

Audit pada sistem operasional direncanakan dan disepakati untuk meminimalkan risiko gangguan pada proses bisnis PSrE Privy dengan frekuensi 1 (satu) tahun sekali. Audit internal ini juga dilakukan untuk memeriksa kesesuaian dengan peraturan perundang-undangan.

Audits on operational systems are planned and agreed to minimize the risk of disruption to Privy CA's business processes with a frequency of 1 (one) year. This internal audit is also carried out to check compliance with laws and regulations.

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*

Privy dapat mengenakan biaya atas layanan penerbitan, penggunaan, dan/atau pembaruan Sertifikat.	Privy may charge fees based on the issuance, use, and/or renewal of Certificates.

9.1.2. Biaya Pengaksesan Sertifikat / *Certificate Access Fees*

Tidak ada ketentuan.	No Stipulation.

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

Tidak ada ketentuan.	No Stipulation.

9.1.4. Biaya Layanan Lainnya / *Fees of Other Services*

Privy dapat mengenakan biaya untuk biaya lain yang belum diatur di CPS ini.	Privy may charge for other fees that have not been regulated in this CPS.

9.1.5. Kebijakan Pengembalian Biaya / *Refund Policy*

Dalam hal Privy mengenakan biaya atas penerbitan dan/atau pembaruan Sertifikat sebagaimana diatur dalam bagian 9.1.1, Privy akan mengatur ketentuan pengembalian biaya dengan mengutamakan perlindungan yang wajar terhadap Pemohon atau Pemegang Sertifikat.	In the event that Privy charges fees for the issuance and/or renewal of Certificates as stipulated in section 9.1.1, Privy will arrange the fee refund provisions with priority given to reasonable protection for the Applicant or Subscribers.

9.2. Tanggung Jawab Keuangan / *Financial Responsibility*

9.2.1. Cakupan Asuransi / *Insurance Coverage*

Privy menjamin kerugian akibat kesengajaan dan/atau kelalaian dalam Penyelenggaraan Sertifikat Elektronik sebagaimana disebutkan lebih lanjut pada Kebijakan Jaminan. Penggantian	Privy guarantees compensation for losses due to willful misconduct and/or negligence in the Management of Electronic Certificates as further outlined in the Warranty Policy.

yang dilakukan dilakukan terhadap Sertifikat Elektronik yang belum dicabut atau telah kedaluwarsa dengan maksimum penggantian 1 (satu) kali permohonan klaim garansi per satu Sertifikat Elektronik.	Compensation is provided for Electronic Certificates that have not been revoked or have expired, with a maximum of one (1) warranty claim per Electronic Certificate.
Privy memiliki *Cyber Edge Insurance Policy* dengan batas tanggungan sebesar USD 2.500.000 (Dua Juta Lima Ratus dolar Amerika Serikat) *dan Technology Professional Indemnity Insurance* dengan gabungan batas tanggungan sebesar USD 2.000.000 (Dua juta dolar Amerika Serikat).	Privy has Cyber Edge Insurance Policy with a coverage limit of USD 2,500,000 (Two Million Five Hundred United States dollars) and Technology Professional Indemnity Insurance with a combined coverage limit of USD 2,000,000 (Two million United States dollars).

9.2.2. Aset Lainnya / *Other Assets*

Privy menjamin kemampuan keuangan secara wajar dalam menjalankan operasionalnya sebagai PSrE.	Privy assures reasonable financiall capability in conducting its operations as a CA.

9.2.3. Cakupan Asuransi atau Garansi untuk Pemegang Sertifikat / *Insurance or Warranty Coverage for Subscribers*

Privy menyediakan Jaminan atau Garansi untuk para Pemegang Sertifikat yang diatur dalam dokumen Kebijakan Jaminan pada Repositori Privy.	Privy provides an Insurance Guarantee or Warranty for Subscribers which is regulated in the Warranty Policy document in the Privy Repository.

9.3. Kerahasiaan Informasi Bisnis / *Confidentiality of Business Information*

9.3.1. Cakupan Informasi Rahasia / *Scope of Confidential Information*

Hal-hal berikut merupakan informasi rahasia dan mendapatkan perhatian khusus dari Privy:

a. Informasi Pribadi sebagaimana yang diatur dalam bagian 9.4
b. Kunci Privat Pemegang Sertifikat yang disimpan oleh Privy, dan informasi yang dibutuhkan untuk menggunakan Kunci Privat tersebut oleh Pemegang Sertifikat;
c. Rekam jejak audit (audit *logs*) dari sistem PSrE Privy dan RA;
d. Data aktivasi pada saat pengaktifan Kunci Privat PSrE Privy sebagaimana dijabarkan pada bagian 6.4.;
e. Catatan permohonan Sertifikat;
f. Laporan Audit yang dibuat oleh Privy, atau Penilai eksternal maupun internal;
g. Hasil penilaian kerentanan; dan
h. Dokumentasi Proses Bisnis Privy diluar dari yang dipaparkan di CPS ini dan/atau Repositori, seperti *Disaster Recovery Plan* dan *Business Continuity Plans*.

The following information is classified as confidential information and receives special attention from Privy:

a. Private Information as set out in section 9.4
b. The Subscriber's Private Key stored by Privy, and the information required to use that Private Key by the Subscriber;
c. Audit logs of Privy CA and RA systems;
d. Activation data at the time of activating the Privy CA Key as described in section 6.4;
e. Certificate application record;
f. Audit Reports prepared by Privy, or external or internal Assessors;
g. Vulnerability assessment results; and
h. Privy Business Process Documentation other than what is described in this CPS and/or Repository, such as Disaster Recovery Plans and Business Continuity Plans.

Kecuali diwajibkan oleh hukum atau perintah pengadilan, pemilik data harus memberikan persetujuan tertulis kepada Privy sebelum mengungkapkan informasi di atas.	Except as required by law or court order, the data owner must provide written consent to Privy before disclosing the above information.

9.3.2. Informasi yang Tidak Dalam Cakupan Informasi yang Rahasia / *Information not within the scope of confidential information*

Informasi yang tidak dikategorikan rahasia sebagaimana diatur dalam CPS ini merupakan informasi publik. Setiap informasi yang dipublikasikan dalam Sertifikat dianggap tidak bersifat rahasia.	Other information that is not categorized as confidential information regulated above is public information. Any information published in the Certificate is considered non-confidential.
Sertifikat, respon OCSP, CRL beserta informasi pribadi atau perusahaan yang muncul di dalamnya dan di direktori/repositori publik termasuk kategori informasi publik.	Certificates, OCSP responses, CRL, along with personal or company information that appears in them and in the public directory/repository, are classified as public information.

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

Privy melindungi informasi rahasia yang secara jelas ditandai atau diberi label secara rahasia atau diberi label sebagai rahasia atau menurut sifatnya harus dipahami secara wajar sebagai rahasia dan memperlakukan informasi tersebut dengan tingkat	Privy protects confidential information that is clearly marked or labeled as confidential, or that by its nature should reasonably be understood as confidential, and treats such information with the same level of care and security

perhatian dan keamanan yang sama seperti Privy melindungi informasi rahasianya. Bentuk pelaksanaan tanggung jawab dalam hal perlindungan informasi rahasia mencakup namun tidak terbatas pada:

a. Pelatihan dan peningkatan *awareness*;
b. Perjanjian kontrak pegawai; dan
c. NDA (*Non-Disclosure Agreement*) dengan pegawai, pegawai *outsource*, dan rekanan.

as Privy protects its own confidential information. The execution of responsibilities in terms of protecting confidential information includes, but is not limited to:

a. Training and awareness raising;
b. Employee contract agreements; and
c. NDA (Non-Disclosure Agreement) with employees, outsourced employees and partners.

9.4. Privasi Informasi Pribadi / *Privacy of Personal Information*

9.4.1. Rencana Privasi / *Privacy Plan*

Privy melindungi informasi privat sesuai dengan ketentuan yang tercantum di dalam Ketentuan Penggunaan Layanan, Pemberitahuan Privasi, dan/atau Perjanjian Pemegang Sertifikat yang disesuaikan dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi dan informasi dan transaksi elektronik.

Privy protects private information in accordance with the provisions stated in the Terms of Service, Privacy Notice, and/or Subscriber Agreement which are adjusted to the provisions of laws and regulations regarding the protection of personal data and electronic information and transactions.

PSrE Privy memberikan akses dan kemampuan kepada Pemegang Sertifikat dan Pengandal untuk mengoreksi atau mengubah informasi privat atau organisasi

PSrE Privy provides access and the ability for Subscriber and Relying Parties to correct or modify private or organizational information through a

melalui permintaan yang sah kepada PSrE Privy. Informasi tersebut hanya bisa diberikan setelah PSrE Privy melakukan langkah-langkah untuk mengautentikasi identitas dari pihak yang meminta. PSrE Privy hanya mengumpulkan dan menggunakan data yang diperlukan untuk pendaftaran dan sertifikasi untuk tujuan tersebut.

legitimate request to PSrE Privy. Such information will only be provided after PSrE Privy has taken steps to authenticate the identity of the requesting party. PSrE Privy only collects and uses data necessary for registration and certification for that purpose.

9.4.2. Informasi yang diperlakukan sebagai Privat / *Information Treated as Private*

Informasi yang diperlakukan sebagai informasi privat adalah segala informasi tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik. Dalam hal Layanan Privy, semua informasi tentang Pemegang Sertifikat yang tidak tersedia secara umum melalui Sertifikat yang diterbitkan dianggap sebagai informasi privat. Hal ini juga termasuk untuk informasi privat Pemegang Sertifikat yang Sertifikatnya berhasil diterbitkan dan juga bagi yang penerbitan

Information deemed private shall include all information about an individual person that is identified or can be individually identified, either directly or indirectly, through electronic or non-electronic systems, whether in isolation or in combination with other information. In the context of the Privy Service, this provision applies all information about the Subscriber that is not publicly available through the issued Certificate is considered private information. This includes private information for Subscribers whose Certificates are successfully issued as well as those whose Certificate

Sertifikatnya ditolak. Untuk informasi privat bagi calon Pemegang Sertifikat yang penerbitan Sertifikatnya ditolak, Privy akan menghapus informasi privat tersebut paling lambat 30 (tiga puluh) hari kalender dari tanggal diterimanya informasi privat tersebut apabila Pemohon tidak mengajukan kembali terkait dengan penerbitan Sertifikatnya tersebut. Privy hanya menyimpan Nomor Induk Kependudukan (NIK) calon Pemegang Sertifikat yang penerbitan Sertifikatnya ditolak disertai alasan penolakan.

Issuance is denied. For the private information of prospective Subscribers whose certificate issuance has been denied, Privy shall erase the aforementioned private information no later than 30 (thirty) calendar days from the date of receipt of said private information if the Applicant does not reapply in relation to the issuance of their Certificate. Privy shall only retain the identity card number (NIK), of the prospective Subscriber whose certificate issuance has been denied, along with the reasons for the rejection.

Privy melindungi semua informasi privat Pemegang Sertifikat dari pengungkapan yang tidak sah. Informasi privat dapat dirilis atas permintaan Pemegang Sertifikat baik terhadap Privy maupun RA. Arsip yang dikelola oleh Privy tidak boleh dirilis kecuali yang diizinkan pada bagian 9.4.1.

Privy protects all Subscribers' personally identifiable information from unauthorized disclosure. Private information may be released at the request of the Subscriber to either Privy or the RA. Records maintained by Privy may not be released except as permitted in section 9.4.1.

9.4.3. Informasi yang tidak Dianggap Privat / *Information not Deemed Private*

Informasi yang tidak masuk dalam kategori atau definisi informasi yang diperlakukan sebagai informasi privat sebagaimana

Information that does not included within the category or definition of information

dijelaskan pada bagian 9.4.2 dan/atau informasi yang termasuk dalam bagian 7 (Sertifikat, CRL, Profil OCSP) dari CPS ini tidak dikenakan perlindungan sebagaimana dijelaskan pada bagian 9.4.2	deemed as private, as described in section 9.4.2 and/or information included in section 7 (Certificates, CRLs, OCSP Profiles) of this CPS shall not be subject to protection as described in section 9.4.2.

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

Privy bertanggung jawab untuk memproses dan menyimpan informasi privat sesuai dengan Pemberitahuan Privasi dan standar pelindungan yang diwajibkan dalam peraturan perundang-undangan yang berlaku terkait dengan pelindungan data pribadi. Informasi yang disimpan dapat berbentuk digital maupun fisik. *Backup* informasi privat harus dienkripsi setiap akan dipindahkan ke media *backup*.	Privy is responsible for processing and storing private information in accordance with the Privacy Notice and the required standard of protection as mandatet by the applicable statutory regulations concerning the protection of personal data. The information stored can be in digital or physical form. Backup of private information must be encrypted every time it is transferred to backup media.

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

Informasi privat yang diperoleh dari Pemohon pada saat proses pendaftaran diperlakukan sebagai informasi privat sehingga perlu persetujuan tertulis atau terekam dari Pemohon untuk Privy dapat menggunakan informasi tersebut. Privy	Private information obtained from the Applicant during the registration process is treated as private information, requiring written or recorded consent from the Applicant for Privy to utilize the information. Privy accommodates all

mengakomodir semua ketentuan terkait penggunaan informasi privat ke dalam dokumen Pemberitahuan Privasi dan Perjanjian Pemegang Sertifikat sesuai dengan peraturan perundang-undangan yang berlaku terkait dengan pelindungan data pribadi. Penggunaan informasi privat harus didasarkan pada pelaksanaan Perjanjian Pemegang Sertifikat atau Perjanjian Pengandal, atau dasar hukum lainnya, yang mengacu pada Pemberitahuan Privasi dan ketentuan peraturan perundang-undangan yang berlaku.	provisions related to the use of private information into the Privacy Notice document and the Subscriber Agreement based on the laws and regulations in personal data protection. The use of private information must be based on the execution of the Subscriber Agreement or Relying Parties Agreement, or other legal basis, which refers to the Privacy Notice and the applicable provisions of laws and regulations.

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

Privy tidak boleh mengungkapkan informasi privat kepada pihak ketiga manapun kecuali yang diberikan kewenangan oleh kebijakan ini, diwajibkan oleh hukum, aturan dan peraturan pemerintah, atau perintah pengadilan.	Privy shall not disclose private information to any third party except those authorized by this policy, required by law, government rules and regulations, or court orders.

9.4.7. Keadaan Pengungkapan Informasi Lainnya / *Other Information Disclosure Circumstances*

Tidak ada ketentuan.	No Stipulation.

9.5. Hak atas Kekayaan Intelektual / *Intellectual Property Rights*

Privy memiliki dan menguasai hak kekayaan intelektual apapun, termasuk namun tidak terbatas pada paten, hak cipta, merek, rahasia dagang atas Layanan Privy (termasuk namun tidak terbatas pada seluruh informasi, perangkat lunak, informasi, teks, huruf, angka, susunan warna, gambar, logo, nama, video dan audio, fitur, database, pemilihan dan pengaturan desain, Sertifikat dan Pasangan Kunci). Pemegang Sertifikat dan Pengandal tidak dapat menggunakan hak kekayaan intelektual Privy tanpa persetujuan tertulis terlebih dahulu dari Privy. Privy tidak akan melanggar hak kekayaan intelektual pihak lain.

Privy owns and controls any intellectual property rights, including but not limited to patents, copyrights, trademarks, trade secrets, for the Privy Service (including but not limited to all information, software, information, text, letters, numbers, color arrangements, images, logos, names, video and audio, features, databases, selection and design settings). Subscribers and Relying Parties cannot use Privy's intellectual property rights without prior written approval from Privy. Privy will not violate the intellectual property rights of other parties.

9.6. Pernyataan dan Jaminan / *Representations and Warranties*

9.6.1. Pernyataan dan Jaminan PSrE / *CA Representations and Warranties*

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

a. Privy mematuhi ketentuan yang diatur di dalam CP PSrE Induk dan CPS ini;
b. Privy menerbitkan dan memperbarui CRL sesuai ketentuan dalam CPS ini;
c. Seluruh Sertifikat yang diterbitkan akan memenuhi

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

a. Privy complies with the provisions stipulated in the Indonesian Root CA CP and this CPS;
b. Privy publishes and updates CRLs in accordance with the provisions of this CPS;

syarat yang diatur berdasarkan CPS ini dan hanya informasi yang telah diverifikasi yang ditampilkan di Sertifikat;.

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

c. All Certificates issued will be qualified under this CPS and only verified information will appear on the Certificates;.
d. Privy displays publicly accessible information through its Repositories;
e. Privy Private Keys are protected and cannot be accessed by unauthorized parties;
f. All statements made by Privy in all applicable agreements are true and accurate, to the best of its knowledge; and
g. Each Subscriber has been required to represent and warrant that all information provided by the Subscriber relating to or contained in the Certificate is correct.

9.6.2. Pernyataan dan Jaminan RA / *RA Representations and Warranties*

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

a. Tidak ada kekeliruan fakta dalam Sertifikat yang diketahui oleh atau berasal dari entitas yang tidak menyetujui pendaftaran

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

a. There is no error of fact in the Certificate that is known by or originates from an entity that does not approve the

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 oleh RA adalah sesuai dengan CP PSrE Induk, CPS ini dan dituangkan di dalam perjanjian; dan
d. Pemegang Sertifikat dikenakan kewajiban sebagaimana disebutkan dalam bagian 9.6.3. Pemegang Sertifikat mendapat informasi tentang konsekuensi/akibat dari ketidakpatuhan terhadap kewajiban tersebut.

registration of the Certificate or the issuance of the Certificate;

b. No misinformation in the Certificate was made by the entity that approved the Certificate registration as a result of carelessness in the management of the Certificate registration;
c. The registration activities performed by RA are in accordance with the Root CA CP, this CPS and set forth in the agreement; and
d. The Subscriber is subject to the obligations mentioned in section 9.6.3. The Subscriber is informed of the consequences of non-compliance with these obligations.

9.6.3. Pernyataan dan Jaminan Pemegang Sertifikat / *Subscriber Representations and Warranties*

Privy mewajibkan Pemegang Sertifikat dan/atau Pemohon untuk menyetujui dokumen yang berisi persyaratan yang harus dipenuhi terkait perlindungan Kunci Privat dan penggunaan Sertifikat, sebelum Sertifikatnya

Privy requires the Subscriber and/or Applicant to agree to a document containing requirements that must be met regarding the protection of the Private Key and the use of the Certificate, before the

diterbitkan. Pemegang Sertifikat dan/atau Pemohon menyetujui hal-hal sebagai berikut:

a. Setiap Tanda Tangan Digital yang dibuat dengan menggunakan Kunci Privat yang terkait dengan Kunci Publik yang ada di dalam Sertifikat adalah Tanda Tangan Digital dari Pemegang Sertifikat dan Sertifikat sudah diterima dan valid (tidak kadaluarsa atau dicabut) saat tanda tangan dibubuhkan;
b. Kunci Privat Pemegang Sertifikat harus diamankan dan hanya Pemegang Sertifikat yang memiliki akses terhadap Kunci Privat tersebut;
c. Semua pernyataan yang dibuat oleh Pemegang Sertifikat saat proses permohonan pendaftaran adalah benar serta telah melakukan reviu dan verifikasi terhadap informasi yang terdapat pada Sertifikat;
d. Semua informasi yang diberikan oleh Pemegang Sertifikat dan informasi yang berada di dalam Sertifikat adalah benar;
e. Sertifikat digunakan hanya untuk tujuan yang legal dan

Certificate is issued. The Subscriber and/or Applicant agree to the following:

a. Each Digital Signature created using the Private Key associated with the Public Key contained in the Certificate is the Digital Signature of the Subscriber and the Certificate was accepted and valid (not expired or revoked) when the signature was affixed;
b. The Subscriber's Private Key is stored and secured by Privy and only the Subscriber has access to the Private Key;
c. All statements made by the Subscriber during the registration application process are true and have reviewed and verified the information contained in the Certificate;
d. All information provided by the Subscriber and the information contained in the Certificate is correct;
e. Certificates are used only for legal and permissible purposes in accordance with the requirements of this CPS;

diperbolehkan sesuai dengan kebutuhan yang ada dalam CPS ini atau Perjanjian Pemegang Sertifikat;

f. Segera melakukan permohonan untuk melakukan pencabutan dan mengakhiri penggunaan Sertifikat dan Kunci Privat yang terasosiasi, jika terdapat hal mencurigakan dan penyalahgunaan atau kebocoran dari Kunci Privat yang terasosiasi dengan Kunci Publik yang termasuk di dalam Sertifikat;
g. Segera 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;
h. Segera menghentikan penggunaan Kunci Privat yang terasosiasi dengan Kunci Publik yang Sertifikatnya dicabut;
i. Akan menanggapi instruksi Privy terkait keadaan terkompromi atau penyalahgunaan Sertifikat

f. The Subscriber and/or Applicant immediately makes a request to revoke and terminate the use of the Certificate and associated Private Key, if there is suspicion and misuse or leakage of the Private Key associated with the Public Key included in the Certificate;
g. The Subscriber and/or Applicant immediately submits a request to revoke the Certificate, and stop using it, if there is any information that does not conform or becomes inappropriate in the Certificate;
h. The Subscriber and/or Applicant immediately stops using the Private Key associated with the Public Key whose Certificate was revoked;
i. The Subscriber and/or Applicant will respond to Privy's instructions regarding compromised circumstances or misuse of the Certificate within 48 (forty-eight) hours;
j. The Subscriber and/or

dalam kurun waktu 48 (empat puluh delapan) jam;

j. Menyetujui dan menerima bahwa Privy diberikan kewenangan untuk segera melakukan pencabutan Sertifikat jika Pemegang Sertifikat melakukan pelanggaran atas ketentuan yang tercantum dalam Perjanjian Pemegang Sertifikat, Syarat dan Ketentuan serta Pemberitahuan Privasi Privy, atau jika Privy menemukan bahwa Sertifikat tersebut digunakan untuk mempermudah tindakan kriminal seperti *phising* , penipuan atau pendistribusian *malware*;

k. Pemegang Sertifikat merupakan Pengguna Akhir dan bukan merupakan PSrE, dan tidak menggunakan Kunci Privat yang kunci publiknya tercantum dalam Sertifikat untuk tujuan penandatangan Sertifikat PSrE lain.

Applicant agrees and accepts that Privy is authorized to immediately revoke the Certificate if the Subscriber violates the provisions stated in the Subscriber Agreement, Terms and Conditions and Privy Privacy Notice, or if Privy finds that the Certificate is used to facilitate criminal acts such as phishing, fraud or malware distribution;

k. The Subscriber is an End User and not a CA, and does not use the Private Key whose public key is listed in the Certificate for the purpose of signing another CA Certificate.

9.6.4. Pernyataan dan Jaminan Pengandal / *Relying Party Representations and Warranties*

Dalam hal perwakilan dari Pengandal mengandalkan Sertifikat yang diterbitkan oleh

In the event that the representative of the Relying Parties relies on the Certificate

Privy, Pengandal menjamin bahwa Pengandal:

a. Memiliki kemampuan teknis untuk menggunakan Sertifikat;
b. Akan selalu dan 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 PSrE Privy atau RA yang berwenang, jika Pengandal menyadari atau mencurigai bahwa telah terjadi Kunci Privat telah terkompromi;
d. Memiliki informasi yang cukup untuk membuat keputusan berdasarkan informasi sejauh mana Pengandal memilih mempercayai informasi yang tertera pada Sertifikat dan bertanggung jawab untuk memutuskan untuk mempercayai atau tidak informasi tersebut, serta akan menanggung konsekuensi hukum dari kegagalan memenuhi kewajiban Pengandal yang ada pada CPS ini dan Perjanjian Pengandal,
e. Harus mematuhi ketentuan yang ditetapkan di CPS dan perjanjian lain yang terkait.

issued by Privy, the Relying Parties guarantees that the Relying Parties:

a. Have the technical ability to use the Certificate;
b. Will always and properly verify the information contained in the Certificate before use and assume any consequences of failing to do so;
c. Report immediately to Privy CA or the authorized RA, if the Relying Parties realizes or suspects that a Private Key has been compromised;
d. Have sufficient information to make an informed decision as to the extent to which the Relying Parties chooses to believe the information contained in the Certificate and are responsible for deciding whether or not to believe such information, and will bear the legal consequences of failing to fulfill the Relying Parties's obligations hereunder;
e. Must comply with the terms set out in the CPS and other relevant agreements.

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

Tidak ada ketentuan.	No Stipulation.

9.7. Pelepasan Jaminan / *Disclaimers of Warranties*

Privy menyatakan bahwa: a. Kecuali untuk jaminan yang telah tercantum di dalam CPS dan perjanjian lainnya dan sepanjang diizinkan oleh hukum, Privy mengabaikan semua jaminan atau kondisi lainnya, baik secara tersurat, tersirat, lisan atau tertulis, termasuk jaminan apa pun yang dapat diperjualbelikan atau kesesuaian untuk tujuan tertentu; b. Tidak menjamin Sertifikat yang penggunaannya tidak sesuai dengan peruntukannya sebagaimana diatur pada bagian 4.5; dan c. Tidak menjamin keakuratan, keaslian, kelengkapan atau kesesuaian dari setiap informasi yang ada dalam Sertifikat demo atau *testing*.	Privy states that: a. Except for the warranties stated in the CPS and other agreements and to the extent permitted by law, Privy disclaims all other warranties or conditions, whether express, implied, spoken or in writing, including any warranties of merchantability or fitness for a particular purpose; b. Does not warrant the Certificate if it is used for purposes other than those specified in Section 4.5; and c. It does not guarantee the accuracy, authenticity, completeness or suitability of any information contained in the demo or testing certificate.

9.8. Pembatasan Tanggung Jawab / *Limitations of Liability*

9.8.1. Pembatasan Tanggung Jawab Privy / *Privy Limitation of Liability*

Sepanjang Privy telah menjalankan persyaratan operasional siklus Sertifikat sesuai yang tercantum pada bagian 4	As long as Privy has carried out the Certificate cycle operational requirements as stated in section 4 of this CPS, Privy is not

CPS ini, maka Privy tidak bertanggung jawab atas setiap akibat atau kerugian yang timbul akibat penggunaan Sertifikat tersebut, termasuk:

a. Semua kerusakan yang dihasilkan dari penggunaan Sertifikat atau Pasangan Kunci dengan cara lain selain didefinisikan dalam CPS, Perjanjian Pemegang Sertifikat, atau yang diatur dalam Sertifikat itu sendiri;
b. Semua kerusakan yang disebabkan oleh *force majeure*; dan/atau
c. Semua kerusakan yang disebabkan oleh *malware* (seperti *virus* atau *trojans*) di luar perangkat Privy.

responsible for any consequences or losses arising from the use of the Certificate, including:

a. Any damage resulting from the use of the Certificate or Key Pair in a manner other than as defined in the CPS, the Subscriber Agreement, or as set forth in the Certificate itself;
b. Any damage caused by force majeure; and/or
c. Any damage caused by malware (such as viruses or trojans) other than the Privy's devices.

9.8.2. Pembatasan Tanggung Jawab RA / *RA Limitation of Liability*

Pembatasan tanggung jawab RA ditentukan dalam kontrak antara RA dan Privy dan mengacu kepada ketentuan peraturan perundang-undangan. Secara khusus, RA bertanggung jawab atas pendaftaran Pemohon Sertifikat.

The RA limitation of liability is specified in the contract between RA and Privy and refers to the provisions of laws and regulations. In particular, RA is responsible for the registration of Certificate Applicants.

9.8.3. Pembatasan Tanggung Jawab Pemegang Sertifikat / *Subscribers Limitation of Liability*

Tanggung jawab Pemilik Sertifikat dan/atau batasannya diuraikan dalam kontrak berlangganan atau Perjanjian Pemegang Sertifikat, dengan mengacu pada ketentuan peraturan perundang-undangan yang mengatur hubungan kedua belah pihak. Pemilik Sertifikat secara khusus bertanggung jawab atas kerugian yang disebabkan oleh kelalaian, pelanggaran kelaikan (*due diligence*) seperti memindahtangankan atau membuat dapat diaksesnya metode atau faktor autentikasi kepada orang lain ataupun tidak mencabut Sertifikatnya yang telah atau diduga terkompromi.	The Subscriber liability and/or the limitations thereof are outlined in the subscription contract or Subscriber Agreement, with reference to the statutory provisions governing the relationship between the parties. The Subscriber is specifically liable for any losses caused by negligence, breach of due diligence such as transferring or making accessible authentication methods or factors to others or not revoking its Certificates that have been or are suspected of being compromised.

9.9. Ganti Rugi / *Indemnities*

9.9.1. Ganti Rugi oleh Privy / *Indemnification by Privy*

Privy tidak bertanggung jawab atas penggunaan Sertifikat yang tidak tepat.	Privy is not responsible for improper use of the Certificate.
Ketentuan ganti rugi lainnya oleh Privy ditentukan berdasarkan Perjanjian Pengandal atau Perjanjian Pemegang Sertifikat termasuk setiap kewajiban apapun kepada pihak ketiga penerima manfaat.	The provision of other indemnification by Privy is determined based on the Relying Parties Agreement or Subscriber Agreement including any obligation to third party beneficiaries.

9.9.2. Ganti Rugi oleh Pemegang Sertifikat / *Indemnification by Subscriber*

PSrE Privy mengatur persyaratan ganti rugi oleh Pemilik Sertifikat dalam CPS dan Perjanjian Pemegang Sertifikat. Sejauh yang dibolehkan oleh peraturan perundang-undangan, Pemegang Sertifikat sepakat untuk mengganti rugi Privy berikut dengan para pihak terkait terhadap kerugian, kerusakan, dan biaya, yang diakibatkan oleh:

a. pelanggaran yang dilakukan oleh Pemegang Sertifikat terhadap Perjanjian Pemegang Sertifikat, CPS ini, atau hukum yang berlaku, baik yang dilakukan secara sengaja maupun tidak sengaja;
b. penggunaan Kunci Privat Pemegang Sertifikat yang tidak sah karena kelalaian Pemegang Sertifikat;
c. penggunaan Sertifikat oleh Pemegang Sertifikat untuk kegiatan melawan hukum;
d. Kegagalan Pemegang Sertifikat untuk mengungkapkan alat bukti pada permohonan Sertifikat dengan maksud untuk menipu pihak manapun;
e. Kegagalan Pemegang Sertifikat untuk melindungi

Privy CA establishes indemnification requirements for Certificate Holders as outlined in the CPS and the Subscribers Agreement. To the extent permitted by law, the Subscriber agrees to indemnify Privy and its related parties against any losses, damages, and costs, caused by:

a. a violation by the Subscriber of the Subscriber Agreement, this CPS, or applicable law, whether committed intentionally and unintentionally;
b. unauthorized use of the Subscriber's Private Key due to the negligence of the Subscriber;
c. the use of the Certificate by the Subscriber for unlawful activities;
d. failure of the Subscriber to disclose evidence in the Certificate application with the intent to deceive any party;
e. failure of the Subscriber to protect the Private Key, use a reliable electronic system, or take reasonable steps to prevent leakage,

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

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

loss, disclosure, alteration, or unauthorized use of the Private Key; and/or

f. the use of name (including but not limited to a common name, domain name, or email address) by the Subscriber that infringes the Intellectual Property Rights of a third party.

9.9.3. Ganti Rugi oleh Pengandal / *Indemnification by Relying Parties*

PSrE Privy mengatur persyaratan ganti rugi oleh Pengandal dalam CPS dan Perjanjian Pengandal. Sejauh yang dibolehkan oleh ketentuan peraturan perundang-undangan, Pengandal setuju untuk mengganti rugi dan membebaskan Privy 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

Privy CA specifies the indemnification requirements for Relying Parties in the CPS and the Relying Party Agreement. To the extent permitted by the provisions of the laws and regulations, the Relying Parties agrees to indemnify and hold Privy harmless from any act or omission that results in liability, loss, damage, costs and all claims resulting from:

a. The Relying Parties do not perform their obligations as set out in the Relying

Pengandal, CPS ini, atau hukum yang berlaku; dan

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

Parties Agreement, this CPS, or applicable law; and

b. The Relying Parties do not check the status of the Certificate to determine whether it has expired or been revoked.

9.10. Jangka Waktu dan Pengakhiran / *Term and Termination*

9.10.1. Jangka Waktu / *Term*

CPS ini berlaku secara efektif setelah dipublikasikan melalui Repositori Privy dan tetap berlaku hingga pemberitahuan lebih lanjut oleh PSrE Privy melalui Situs Privy/Repositori Privy.

This CPS is effective after being published through the Privy Repository and remains in effect until further notice by Privy CA through the Privy Site/Privy Repository.

9.10.2. Pengakhiran / *Termination*

CPS ini dapat diubah setiap saat dan akan tetap berlaku sampai dengan diterbitkannya versi CPS yang terbaru atau dinyatakan tidak berlaku oleh PA PSrE Privy. Perubahan CPS ditandai dengan perubahan nomor versi yang jelas. Setiap perubahan efektif berlaku 30 (tiga puluh) hari kalender setelah dipublikasikan.

This CPS may be amended at any time and will remain in effect until a new version of the CPS is issued or it is declared invalid by the PA of PSrE Privy. Amendments to the CPS are indicated by a clear version number change. Any changes shall be effective 30 (thirty) days after publication.

Pada saat berakhirnya CPS ini, maka seluruh Sertifikat yang terbit berdasarkan CPS tetap berlaku hingga berakhirnya masa validitas dari Sertifikat terakhir berdasarkan CPS

At the termination of this CPS, all Certificates issued based on the CPS will remain valid until the expiration of the last Certificate based on the CPS. In the event of any changes

tersebut. Dalam hal terdapat perubahan terkait dokumen Hierarki OID dan/atau dokumen-dokumen terkait lainnya yang berdampak pada perubahan OID PSrE Indonesia, maka OID dalam CPS ini tetap berlaku paling lambat 12 (dua belas) bulan atau lebih cepat setelah dilakukan penyesuaian pada CPS ini.

related to the OID Hierarchy document and/or other related documents that affect the changes to the OID of PSrE Indonesia, the OID in this CPS will remain valid for a maximum of 12 (twelve) months or sooner after adjustments are made to this CPS.

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

Privy mengkomunikasikan kondisi akibat dari penghentian CPS dan juga kondisi keberlangsungan dari Sertifikat yang telah terbit melalui laman atau Repositori.

Privy communicates the conditions resulting from the termination of the CPS as well as the continuity of the issued Certificates through the website or Repository.

Dalam hal CPS sudah tidak berlaku lagi, aturan terkait dengan perlindungan data dan arsip informasi akan tetap dipenuhi oleh PSrE Privy.

In the event that the CPS is no longer in effect, the rules related to data protection and information archiving will still be upheld by PSrE Privy.

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

Para pihak yang terlibat dalam CPS ini dapat mengirimkan pemberitahuan terkait dengan CPS ini kepada Privy melalui alamat dan media komunikasi yang dicantumkan pada Situs Privy dan/atau media komunikasi sebagaimana

The parties involved in this CPS can send notifications related to this CPS to Privy through the address and communication media listed on the Privy Site and/or communication media as mentioned in section 1.5.1. The notification is deemed to

disebutkan pada bagian 1.5.1. Pemberitahuan dianggap telah diterima apabila pengirim menerima pernyataan penerimaan atau tanggapan tertulis dari Privy. Privy akan memberikan tanggapan atas permintaan yang diberikan paling lambat 20 (dua puluh) hari kerja dari diterimanya permintaan tersebut.

have been received if the sender receives a statement of receipt or written response from Privy. Privy shall provide a response to the request submitted by no later than 20 (twenty) business days from the receipt of request.

9.12. Perubahan atau Amendemen / *Amendments*

9.12.1. Prosedur untuk Perubahan atau Amendemen / *Procedure for Amendment*

Segala perubahan CPS ditinjau oleh *Policy Authority* Privy dan untuk selanjutnya disetujui oleh PA PSrE Induk. Privy akan menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Amandemen CPS dilakukan sesuai dengan prosedur persetujuan CPS.

All amendments to the CPS are reviewed and approved by Privy's Policy Authority. Privy will publish a notice on the website regarding major or significant changes to this CPS including the time when the CPS is effective. Amendments to the CPS are made in accordance with the CPS approval procedure.

9.12.2. Periode dan Mekanisme Pemberitahuan / *Notification Mechanism and Period*

Privy akan menerbitkan pemberitahuan di website terkait perubahan besar atau signifikan dari CPS ini termasuk juga keterangan waktu ketika CPS efektif berlaku. Ketika

Privy will publish a notice on the website regarding major or significant amendments to this CPS including the time when the CPS becomes effective. When an amendment occurs, the CPS

terjadi perubahan, CPS dipublikasikan paling lama 7 (tujuh) hari kerja sejak tanggal ditandatangani.

is published no later than 7 (seven) working days from the date of signing.

Setiap perubahan terhadap CPS akan dilakukan melalui pengumuman yang dilakukan oleh Privy kepada para pihak yang terkait. Pengumuman tersebut dapat dilakukan melalui informasi elektronik yang dikirim melalui surat elektronik atau pesan singkat melalui telepon genggam, dan juga dicantumkan dalam Situs yang akan menampilkan pengumuman tersebut selama 7x24 jam setelah pengumuman tersebut disampaikan.

Any changes to the CPS will be executed through notifications issued by Privy to the relevant parties. These notifications may be conveyed through electronic means, including email or text messages via mobile phones, and will also be displayed on the Site for a continuous period of 7x24 hours following the dissemination of the notification.

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, Privy akan menginformasikan perubahan OID kepada PA PSrE Induk sebelum melakukan perubahan OID dan melaksanakan kebijakan baru dengan menggunakan OID yang baru.

If the Policy Authority has a view that it is necessary to change the OID numbers involved, Privy will inform modification of OID to RA Indonesia before make the OID changes and implement the new policy using the new OIDs.

9.13. Ketentuan Penyelesaian Perselisihan/Sengketa / *Dispute Resolution Provisions*

Jika ada perselisihan atau kontroversi sehubungan dengan kinerja, eksekusi atau interpretasi dari CPS ini, para pihak akan berusaha untuk mencapai penyelesaian damai. Ketentuan penyelesaian perselisihan merupakan bagian dari kontrak yang disepakati antara Privy dengan Pemegang Sertifikat atau dengan Pengandal.

If there is any dispute or controversy with respect to the performance, execution or interpretation of this CPS, the parties will endeavor to reach an amicable settlement. The dispute resolution provisions are part of the contract agreed between Privy and the Subscriber or with the Relying Party.

9.14. Hukum Yang Mengatur / *Governing Law*

CPS ini diatur, ditafsirkan, dan dipahami sesuai dengan aturan hukum di Indonesia. Pemilihan aturan hukum ini untuk mendapatkan pemahaman yang sama, terlepas dari lokasi domisili atau lokasi penggunaan Sertifikat Privy ataupun produk/ layanan lainnya. Termasuk apabila Sertifikat yang diterbitkan oleh Privy dipakai untuk kebutuhan komersil atau kontrak di negara lain, baik secara tersirat maupun tersurat menggunakan layanan Privy, tetap menerapkan aturan hukum di Indonesia.

This CPS shall be governed, interpreted, and understood in accordance with the laws of Indonesia. The choice of this rule of law is to get the same understanding, regardless of the location of domicile or location of use of the Privy Certificate or other products/services. Including if the Certificate issued by Privy is used for commercial or contractual needs in other countries, either implicitly or explicitly using Privy services, the rule of law in Indonesia still applies.

Para pihak, termasuk *partners* CA, Pemegang Sertifikat, Pengandal, tidak dapat membatalkan acuan hukum yang telah ditentukan diatas.	Parties, including CA partners, Subscribers, Relying Parties, cannot override the legal references specified above.

9.15. Kepatuhan atas Hukum yang Berlaku / *Compliance with Applicable Law*

Privy mematuhi semua persyaratan, hukum, dan ketentuan peraturan perundang-undangan Indonesia untuk penyediaan produk dan layanan yang dijelaskan dalam CPS ini. Kepatuhan mencakup, namun tidak terbatas pada, perangkat keras, perangkat lunak, sistem, informasi bisnis, proses data, dan semua kegiatan sehari-hari terkait operasi praktik bisnis.	Privy complies with all requirements, laws, and provisions of Indonesian laws and regulations for the provision of products and services described in this CPS. Compliance shall include, but is not limited to, hardware, software, systems, business information, data processes, and all daily activities related to the operation of business practices.

9.16. Ketentuan yang Belum Diatur / Miscellaneous Provisions

9.16.1. Seluruh Perjanjian / *Entire Agreement*

Privy secara kontraktual mewajibkan RA untuk mematuhi CPS ini dan semua panduan terkait termasuk namun tidak terbatas pada ketentuan yang terdapat di Repositori.	Privy contractually obligates RA to comply with this CPS and all related guidelines including but not limited to the provisions contained in the Repository.

9.16.2. Pengalihan Hak / *Assignment*

Ketentuan pengalihan hak dilakukan sesuai dengan ketentuan peraturan perundang-undangan yang	The transfers of rights shall be carried out in accordance with the applicable laws and regulations or announcements

berlaku atau pengumuman yang berkaitan dengan PSrE.

related 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. Proses pembaruan CPS dijelaskan pada bagian 9.12.

If any provision of this CPS, including any limitation of coverage clause, is found to be invalid or unenforceable, this section of the CPS shall thereafter be construed in such a manner as to support the original intent of all parties. Any and all provisions of this CPS that describe limitations of liability are intended to be severable and independent of any other provisions and shall be enforced accordingly. The process for updating the CPS is described in section 9.12.

9.16.4. Penegakan Hukum (Biaya Pengacara dan Pelepasan Hak) / *Enforcement (Attorney's Fees and Waiver of Rights)*

Privy dapat meminta ganti rugi dan penggantian biaya pengacara kepada pihak yang terbukti melakukan kerusakan, kehilangan, dan kerugian lain yang disebabkan oleh pihak tersebut. Kegagalan Privy dalam menerapkan klausul ini dalam satu kasus tidak menghilangkan hak Privy untuk tetap menggunakan klausul ini di

Privy can request compensation and reimbursement of attorney fees to the party proven to have caused damage, loss, and other losses caused by that party. Privy's failure to apply this clause in one case does not eliminate Privy's right to continue using this clause in the future or the right to use other clauses in this CPS. All matters

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 Privy.

related to the waiver of rights in court must be submitted in writing and signed by Privy.

9.16.5. Keadaan Memaksa / *Force Majeure*

Privy tidak bertanggung jawab atas kegagalan atau keterlambatan terhadap kinerjanya dalam CPS ini, yang disebabkan oleh hal-hal yang berada diluar kendali yang wajar, termasuk tapi tidak terbatas pada: tindakan otoritas sipil atau militer, bencana alam, kebakaran, epidemi, banjir, gempa bumi, kerusuhan, perang, kegagalan peralatan, listrik dan kegagalan jalur telekomunikasi, kurangnya akses Internet, sabotase, terorisme, dan tindakan pemerintahan atau setiap kejadian atau situasi yang tidak terduga.

Privy is not responsible for any failure or delay in its performance in this CPS, which is caused by matters beyond its reasonable control, including but not limited to: acts of civil or military authorities, natural disasters, fires, epidemics, floods, earthquakes, riots, wars, equipment failures, power and telecommunications line failures, lack of Internet access, sabotage, terrorism, and government actions or any unforeseen events or situations.

Privy menyediakan BCP dan DRP dengan kendali yang wajar sesuai dengan kapabilitas Privy.

Privy provides BCP and DRP with reasonable control according to Privy's capabilities.

Sepanjang diperbolehkan oleh peraturan perundang-undangan, ketentuan mengenai

To the extent permitted by laws and regulations, the provisions regarding force majeure will be

keadaan kahar akan diatur secara lebih spesifik melalui Perjanjian Pemegang Sertifikat dan Perjanjian Pengandal.	regulated more specifically through the Subscriber Agreement and the Relying Parties Agreement.

9.17. Ketentuan Lain / *Other Provisions*

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

Dalam hal CPS ini ditampilkan dalam beragam pilihan bahasa dan terdapat ketidaksesuaian antara satu bahasa dengan bahasa yang lain, maka teks Bahasa Indonesia yang akan berlaku.	In the event that this CPS is presented in multiple language options and there is a discrepancy between one language and another, the Indonesian text shall prevail.

10. LAMPIRAN 1 – Profil Sertifikat / *APPENDIX 1 - Certificate Profile*

10.1. Sertifikat Privy CA Class 3 / Privy CA Class 3 Certificate

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	PrivyCA Class 3 – G2
Subject: OrganizationName	PT Privy Identitas Digital
Subject: CountryName	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=Certificate Authority, Path Length Constraint=None
Public Key	RSA 4096 bits

10.2. Sertifikat Privy CA Class 4 / *Privy CA Class 4 Certificate*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Kementerian Komunikasi dan Informatika
Issuer: C	ID
Subject: CommonName	PrivyCA Class 4 – G2
Subject: OrganizationName	PT Privy Identitas Digital
Subject: CountryName	ID
Subject Alternative Name	N/A
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi 10 (sepuluh) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = http://crl.rootca.id/RootCAIndonesiaDSG1.crl
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=Certificate Authority, Path Length Constraint=None
Public Key	RSA 4096 bits

10.3. Sertifikat Level 2/Kelas 3 (Subscriber Certificate) / *Level 2/Class 3 Certificate (Subscriber Certificate)*

10.3.1. Sertifikat Individu Non-Instansi Verifikasi Level 2 (Online) / *Individual Non- Government Verification Level 2 (Online) Certificate*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	PrivyCA Class 3 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationalUnitName	Personal
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi maksimal 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS3G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id CA Issuer=https://repository.privyca.id/cert/PrivyCAClass3G2.pem
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.5.1.2.2 Notice=”Individu Non-Instansi Online Level 2”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.3.2. Sertifikat Individu Warga Negara Asing Verifikasi Level 2 (Online) / *Individual Foreigners Verification Level 2 (Online) Certificate*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	PrivyCA Class 3 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationalUnitName	Personal
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi maksimal 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS3G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id CA Issuer: CA Issuer=https://repository.privyca.id/cert/PrivyCAClass3G2.pem
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.5.2.2.2 Notice=”Individu WNA Online level 2”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.3.3. Sertifikat Badan Usaha/Segel Elektronik / *Business Entity Certificates*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	PrivyCA Class 3 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Badan Usaha/Badan Hukum (Username Privy)
Subject: OrganizationName	Nama Entitas RA yang melakukan validasi identitas
Subject: OrganizationalUnitName	Badan Usaha
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi maksimal 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id CA Issuer= https://repository.privyca.id/cert/PrivyCAClass3G2.pem
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.8.1 Notice=”Badan Usaha”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.4. Sertifikat Level 3/Kelas 4 (Subscriber Certificate) / *Level 3/Class 4 Certificate (Subscriber Certificate)*

10.4.1. Sertifikat Individu Non-Instansi Verifikasi Level 3 (Offline) / *Individual Non-Government Verification Level 3 (Offline)*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	PrivyCA Class 4 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationalUnitName	Personal
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi maksimal 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id CA Issuer=https://repository.privyca.id/cert/PrivyCAClass4G2.pem
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.5.1.1.3 Notice=”Individu non-Instansi Offline Level 3”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

10.4.2. Sertifikat Individu Warga Negara Asing Verifikasi Level 3 (online) / *Individual Foreigners Verification Level 3 (Online) Certificate*

Basic Certificate Fields	*Value*
Version	V3
Signature Algorithm	SHA-256 dengan RSA Encryption
Issuer: CN	PrivyCA Class 4 – G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Nama Lengkap (sesuai KTP tanpa gelar) (Username Privy)
Subject: OrganizationalUnitName	Personal
Subject: CountryName	ID
Subject Alternative Name	Opsional Critical=FALSE
Serial Number	Diatur secara otomatis melalui perangkat lunak
Valid From	YYYY/MM/DD HH:MM:SS (durasi maksimal 2 (dua) tahun)
Valid To	YYYY/MM/DD HH:MM:SS
Key Usage	Critical=TRUE Digital Signature, Non-Repudiation
Extended Key Usage	Critical=FALSE PDF Signing 1.2.840.113583.1.1.5
Subject Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
CRL Distribution Points	Critical=FALSE CRL HTTP URL = https://crl.privyca.id/PrivyCACLASS4G2.crl
Authority Information access	Critical=FALSE Access Method=OCSP, URL=https://ocsp.privyca.id CA Issuer= https://repository.privyca.id/cert/PrivyCAClass4G2.pem
Certificate Policies	Critical=FALSE Policy OID : 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id OID : 2.16.360.1.1.1.5.2.2.3 Notice=”Individu WNA Online level 3”
Authority Key Identifier	Critical=FALSE 160 bit hash (SHA-1)
Basic Constraints	Critical=TRUE Subject Type=End Entity, Path Length Constraint=None
Public Key	ECC 256 bits

11. Lampiran 2 – Definisi dan Singkatan/Akronim / *Appendix 2 - Definitions and Abbreviations/Acronyms*

11.1. Definisi / *Definitions*

Istilah / *Term*	**Definisi / *Definitions***
Badan Usaha/Badan Hukum *Business Entity/Legal Entity*	Perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum. *Individual companies or partnership companies, both incorporated and unincorporated.*
Data Elektronik *Electronic Data*	Data berbentuk elektronik yang tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi. *Data in electronic form which is not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations.*
Informasi Elektronik *Electronic Information*	Satu atau sekumpulan Data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode Akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya. *One or a set of Electronic Data, including but not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed that have meaning or can be understood by a person capable of understanding them.*

Dokumen Elektronik *Electronic Documents*	Setiap Informasi Elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau Sistem Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya. *Any Electronic Information created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar form, which can be seen, displayed, and/or heard through a computer or Electronic System, including but not limited to writings, sounds, images, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or significance or can be understood by a person capable of understanding them.*
Infrastruktur Kunci Publik/*Public Key Infrastructure* (“PKI”) *Public Key Infrastructure ("PKI")*	Serangkaian perangkat keras, perangkat lunak, orang, prosedur, aturan, kebijakan dan kewajiban yang digunakan untuk memfasilitasi pembuatan, penerbitan, pengelolaan, dan penggunaan Sertifikat dan kunci yang dapat dipercaya berdasarkan kriptografi Kunci Publik. *The set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the creation, issuance, management and use of Certificates and trustworthy keys based on Public Key cryptography.*
Kebijakan Sertifikat	Seperangkat aturan yang menunjukkan penerapan dari Sertifikat yang dinamai untuk komunitas tertentu dan/atau implementasi PKI dengan persyaratan keamanan umum. Kebijakan Sertifikat tersedia pada Repositori dan repositori

Certificate Policy ("CP")	yang dikelola oleh PSrE Induk yang saat ini tersedia pada https://www.rootca.id/. *A set of rules that indicate the applicability of a named Certificate to a specific community and/or PKI implementation with common security requirements. The Certificate Policy is available in the Repository and the repository managed by the Root CA is currently available at https://www.rootca.id/.*
Ketentuan Penggunaan Layanan *Terms of Use of the Service*	Ketentuan mengenai pengamanan dan penggunaan yang sesuai dari Sertifikat yang diterbitkan sesuai dengan dokumen ini (CPS) ini ketika Pemohon/Pemegang Sertifikat adalah PSrE atau afiliasi dari PSrE Privy. Ketentuan Penggunaan Layanan Privy tersedia di https://privy.id/id/ketentuan-penggunaan. *Conditions regarding security and appropriate use of the Certificate issued in accordance with this document (CPS) when the Applicant/Subscriber is a CA or an affiliate of a Privy CA. Terms of Use of Privy Services are available at https://privy.id/id/ketentuan-penggunaan.*
Kunci Privat *Private Key*	Kunci yang dirahasiakan oleh pemegang Pasangan Kunci yang digunakan untuk membuat Tanda Tangan Elektronik dan/atau mendekripsi catatan atau file elektronik yang dienkripsi dengan Kunci Publik yang sesuai. *A key kept secret by the holder of a Key Pair that is used to create an Electronic Signature and/or decrypt electronic records or files encrypted with the corresponding Public Key.*
Kunci Publik	Kunci yang dapat diungkapkan secara publik yang termuat dalam Sertifikat dan bersesuaian dengan Kunci Privat rahasia yang digunakan. Kunci Publik digunakan oleh Pengandal untuk memverifikasi Tanda Tangan Elektronik yang dibuat oleh Kunci Privat dan/atau untuk mengenkripsi pesan

	sehingga Kunci Publik hanya dapat didekripsi dengan menggunakan Kunci Privat yang sesuai. *The publicly disclosable key contained in the Certificate and corresponding to the confidential Private Key used. The Public Key is used by the Relying Parties to verify the Electronic Signature created by the Private Key and/or to encrypt messages so that the Public Key can only be decrypted using the corresponding Private Key.*
Public Key	
Laporan Audit	Laporan dari Penilai Terkualifikasi yang menyatakan pendapat Penilai Terkualifikasi tentang apakah proses dan kontrol entitas memenuhi ketentuan wajib yang diatur pada dokumen ini (CPS). *A report from a Qualified Auditor expressing the Qualified Auditor's opinion on whether the entity's processes and controls meet the mandatory requirements set out in this document (CPS).*
Audit Report	
Online Certificate Status Profile (“OCSP”)	Protocol pengecekan Sertifikat daring yang memungkinkan aplikasi perangkat lunak Pengandal untuk menentukan status Sertifikat yang diidentifikasi. *An online Certificate checking protocol that allows Relying Parties software applications to determine the status of identified Certificates.*
Online Certificate Status Profile ("OCSP")	
Otoritas Pendaftaran	Pihak yang atas nama CA menjalankan fungsi identifikasi dan autentikasi terhadap permohonan Sertifikat, baik memulai dan meneruskan permohonan untuk pencabutan Sertifikat kepada CA, dan meminta untuk dilakukan penerbitan ulang atau perpanjangan Sertifikat. *The party acting on behalf of the CA performing the identification and authentication functions of the Certificate application, both initiates and forwards the request for Certificate revocation to*
Registration Authority ("RA")	

	the CA, and requests for the re-issuance or renewal of the Certificate.
Pasangan Kunci *Key Pair*	Kunci Privat dan Kunci Publik terkait. *Private Key and associated Public Key.*
Pemberitahuan Privasi *Privacy Notice*	Ketentuan mengenai cara PSrE Privy mengumpulkan, menggunakan, membagikan, memproses, dan mengamankan data pribadi pengguna layanan Privy, termasuk Pemegang Sertifikat. Pemberitahuan Privasi Privy tersedia di https://privy.id/id/pemberitahuan-privasi dan/atau pada Repositori. *Provisions regarding how PSrE Privy collects, uses, shares, processes, and secures the personal data of Privy service users, including Subscribers, are outlined in the Privy Privacy Notice, available at https://privy.id/id/pemberitahuan-privasi and/or in the Repository.*
Pemegang Sertifikat *Subscribers*	Orang atau Badan Hukum yang telah berhasil memperoleh Sertifikat baik melalui RA ataupun Privy. *Persons or Legal Entities who have successfully received a Certificate either through RA or Privy.*
Pemohon *Applicants*	Orang atau Badan Hukum yang telah mengajukan permohonan, namun belum mendapatkan Sertifikat. *Persons or legal entities that have submitted an application, but have not yet received a Certificate.*
Penilai Terkualifikasi *Qualified Auditor*	Orang atau Badan Hukum yang memenuhi persyaratan dalam CPS ini. *Persons or Legal Entities that meet the requirements in the CPS.*
Penyelenggara Sertifikasi Elektronik (“PSrE”)	Badan Hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit Sertifikat.

Certification Authority ("CA")	*A legal entity that serves as a trustworthy party, which grants and audits Certificates.*
Penyelenggara Sertifikasi Elektronik Induk ("PSrE Induk") *Root CA*	Penyelenggara Sertifikasi Elektronik tingkat atas yang Sertifikat Induk-nya didistribusikan oleh Aplikasi Perangkat Lunak dan menandatangani Sertifikat CA di bawahnya. *Top-level Electronic Certification Operators whose Root Certificates are distributed by Software Applications and sign subordinate CA Certificates.*
Pengidentifikasian Objek Kebijakan *Object Identifier* ("OID")	Merupakan set nomor yang secara unik menunjuk kepada sebuah objek atau kebijakan yang diatur dalam CPS. *This is a set of numbers that uniquely refers to an object or policy regulated by the CPS.*
Perjanjian Pemegang Sertifikat *Subscriber Agreement*	Perjanjian antara CA dan Pemohon/Pemegang Sertifikat yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pemegang Sertifikat Privy tersedia di Repositori. *An agreement between the CA and the Applicant/Subscriber that defines the rights and responsibilities of the parties. The Privy Subscriber Agreement is available in the Repository.*
Perjanjian Pengandal *Relying Party Agreement*	Perjanjian antara CA dan Pengandal yang menentukan hak dan tanggung jawab para pihak. Perjanjian Pengandal Privy tersedia di Repositori. *An agreement between a CA and a Privy that defines the rights and responsibilities of the parties. The Privy Relying Party Agreement is available in the Repository.*
Pengandal *Relying Party*	Orang atau Badan Hukum yang mempercayai Sertifikat dan/atau Tanda Tangan Digital yang diterbitkan oleh CA. *A person or Legal Entity who entrusts the Certificate and/or Digital Signature issued by the CA.*

Repositori *Repository*	Database online yang berisi dokumen tata kelola PKI yang diungkapkan secara publik (seperti CP/CPS) dan informasi status Sertifikat, baik dalam bentuk respon CRL atau OCSP. Repositori Privy pada tautan https://repository.privyca.id/. *An online database containing publicly disclosed PKI governance documents (such as CP/CPS) and Certificate status information, both in CRL or OCSP response form. Privy repository can be found at https://repository.privyca.id/.*
Sertifikat Elektronik ("Sertifikat") *Electronic Certificate ("Certificate")*	Sertifikat yang bersifat elektronik dan memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik. *An electronic certificate that contains an Electronic Signature and identity showing the status of the legal subject of the parties in an Electronic Transaction issued by a Certification Authority.*
Sertifikat Induk *Root Certificate*	Sertifikat yang diterbitkan dan ditandatangani sendiri oleh Root CA untuk mengidentifikasi dirinya dan untuk memfasilitasi sertifikasi Sertifikat yang dikeluarkan oleh *Subordinate CA*. *A certificate issued and self-signed by a Root CA to identify itself and to facilitate the certification of Certificates issued by Subordinate CAs.*
Situs *Website*	berarti segala URL yang menggunakan domain dengan alamat www.privy.id dan/atau www.privyca.id atau situs lain yang dinyatakan oleh Privy dari waktu ke waktu. *It means any URL that uses the domain with the address www.privy.id and/or www.privyca.id or other sites stated by Privy from time to time.*
Status Keaktifan Sertifikat	Berisi daftar dengan penanda waktu dari Sertifikat yang dicabut yang diperbaharui secara berkala

	yang dibuat dan ditandatangani secara elektronik oleh CA/PSrE yang menerbitkan Sertifikat.
Certificate Revocation List (”CRL”)	*It contains a time-stamped list of periodically renewed revoked Certificates created and electronically signed by the CA/CA that issued the Certificate.*
Subjek	Berarti perseorangan, Badan Hukum/Badan Usaha yang diidentifikasi dalam Sertifikat sebagai Subjek.
Subject	*It means the individual, Legal Entity/Business Entity identified in the Certificate as the Subject.*
Penyelenggara Sertifikasi Elektronik Berinduk (“PSrE Indonesia”)	CA yang Sertifikatnya ditandatangani oleh *Root CA*, atau *Subordinate CA* lainnya.
Subordinate CA (“Sub-CA”)	*A CA whose Certificate is signed by the Root CA, or another Subordinate CA.*
Tanda Tangan Elektronik	Tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
Electronic Signature	*A signature consisting of Electronic Information attached, associated or related to other Electronic Information that is used as a verification and authentication tool.*
Tata Cara Pelaksanaan Sertifikat PsrE	Satu dari beberapa dokumen yang membentuk kerangka kerja tata kelola di mana Sertifikat dibuat, diterbitkan, dikelola dan digunakan.
Certificate Practice Statement (“CPS”)	*One of several documents that form the governance framework within which Certificates are created, issued, managed and used.*
Warm Backup	Metode pencadangan data yang dilakukan dengan menyalin data pada Pusat data ke lokasi cadangan *off-site* secara *real time*.

Warm Backup	*A data backup method that is performed by copying data on the Data center to an off-site backup location in real time.*

11.2. Singkatan/Akronim / *Abbreviations/Accronym*

Akronim	Arti
AICPA	American Institute of Certified Public Accountants
BCP	Business Continuity Planning
C	Country
CA	Certification Authority/Penyelenggara Sertifikasi Elektronik
CICA	Canadian Institute of Chartered Accountants
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
DN	Distinguished Name
DoS	Denial of Services
DRP	Disaster Recovery Planning
EDI	Electronic Data Interchange
FIPS	Federal Information Protection Standards
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IKP	Infrastruktur Kunci Publik
ISO	International Organization for Standardization
Kominfo	Kementerian Komunikasi dan Informatika Republik Indonesia
KTP	Kartu Tanda Penduduk
NIB	Nomor Induk Berusaha
NIK	Nomor Induk Kependudukan
NPWP	Nomor Pokok Wajib Pajak
O	Organization Name
OU	Organization Unit
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PKI	Public Key Infrastructure
PSrE	Penyelenggara Sertifikasi Elektronik
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SIUP	Surat Izin Usaha Perdagangan
SIM	Surat Izin Mengemudi
SK	Surat Keputusan
SOP	Standard Operational Procedure

Sub-CA	Subordinate Certification Authority
RA	Registration Authority / Otoritas Pendaftaran
UPS	Uninterrupted Power Supply (UPS)
URL	Uniform Resource Locator