Certification Practice Statement

Privy

Version 2.2

January 31st, 2023

Jl. Kemang Raya 34 Lantai 2

Bangka, Kec. Mampang Prapatan,

Kota Jakarta Selatan

Phone: 021-22715509

Email: Policy@privy.id

Website: www.privyca.id

Policy Authority Approval Page

This document is approved electronically according to the time and location of signing.

Approved by,

Chief Executive Officer

Marshall Pribadi

Change History

Version	Date	History and Change Description
1.0	-	Initial Release
1.1	February 22nd, 2019	Addition to meet the requirements for recognition as a subordinated Electronic Certification Authority by MCIT.
1.2	January 12th, 2021	Addition of RA Privy provisions and other adjustments.
2.0	June 16th, 2021	Change of document title and adjustment to the Certificate Practice (CP) of Indonesian Root CA.
2.1	November 25th, 2021	Addition of provisions on Inter-operation, retraining frequency, and rebranding PrivyID to Privy as well as other adjustments.
2.2	January 31st, 2023	Addition of Electronic Seal service and identification of foreigners. Addition of requirements for adjustments to the Root CP.

Table of Contents

1. Introduction

1.1. Overview

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.

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

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/.

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

1.2. Document Name and Identification

This document is titled "**Certificate Practice Statement v.2.2"** which is the CPS of Privy CA.

Privy, according to its authority, is designated to have Object Identifiers (OIDs) with the identification number joint-iso-it-t(2) country(16) id(360)

gov(1) kominfo(1) rootca(1) psre-berinduk(3) non-asn(12) privy(1).

Here are the OIDs for documents published by Privy:

Non-Government Certificate	2.16.360.1.1.1.3.12
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:

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
OID for Level 4	2.16.360.1.1.1.4.4
Compliance	2.16.360.1.1.1.5
AATL	2.16.360.1.1.1.5.1
SII Type	2.16.360.1.1.1.6
NIK	2.16.360.1.1.1.6.1
Certificate Designation	2.16.360.1.1.1.7
Individuals	2.16.360.1.1.1.7.1
Business Entity/Organization	2.16.360.1.1.1.7.2

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

1.3. PKI Participants

1.3.1. Certification Authorities

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

1.3.1.1. Root CA

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 the Ministry of the Republic of Indonesia which is authorized to carry out the functions of the Root CA in accordance with the provisions of the laws and regulations. CA Root 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 (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. Indonesian CA

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.

Indonesian CAs are not allowed to root themselves on other CAs.

1.3.2. Registration Authorities

Registration Authorities (RAs) are parties appointed by Privy CA to carry out the following functions:

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.

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.

Unless otherwise specified, RAs listed in this provision are those are 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. End Users

The end users of the PKI shall consist of:

a. Applicant - A Person or Legal Entity that has submitted an application, but has not yet received a Certificate.
b. Subscriber – A Person or Legal Entity who has successfully obtained a Certificate through application to RA or Privy.

1.3.4. Relying Parties

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.

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.

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 check (whether the Certificate is on the list) of revocations (CRL and OCSP); and
d. Give an approval of limits of liability and warranties;

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. Other Participants

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

Data Recovery Center services.

1.4. Certificate Usage

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. Appropriate Certificate Uses

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

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.

Electronic Seal is electronic data attached, associated, or related to Electronic Information and/or Electronic Documents to guarantee the origin, integrity, and wholeness of Electronic Information and/or Electronic Documents used by Business Entities.

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 actual person.
c. Integrity:

Certainty that electronic information or documents have not been altered.

Based on this explanation, the Key Usage allowed for Subscribers is Digital Signature and Non-Repudiation.

The certificate issued by Privy CA is an Electronic Certificate with identity verification level 3 and 4 in accordance with the laws and regulations governing the implementation of electronic certification with the following description:

a. Class 3 Certificate
   Certificates issued in accordance with identity verification level 3; and
b. Class 4 Certificate
   Certificates issued in accordance with identity verification level 4.

1.4.2. Prohibited Use of Certificates

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. Policy Administration

1.5.1. Organization Administering the Document

This CPS is managed by the Policy Authority Privy (PA). The CPS is changed according to the policy determined by the PA. This CPS is also changed if adjustments are needed to the Baseline Requirements from the CA Browser Forum, Webtrust Principles & Criteria for Certificate Authority, Adobe Approved Trusted List Technical Requirements, and/or the Root CA CP.

The PA consists of the Chief Executive Officer (President Director) and the party appointed to head the C-Level Unit at Privy.

PA can be contacted via:

Policy Authority Privy

Jl. Kemang Raya 34 Lantai 2

Bangka, Kec. Mampang Prapatan.,

Kota Jakarta Selatan Phone: 021-22715509

Email: Policy@privy.id

Website: www.privyca.id

1.5.2. Contact Person

The contact person can use the information listed in section 1.5.1.

1.5.3. Personnel Determining CPS Suitability for the Policy

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. CPS Approval Procedures

Changes to the CPS are subject to approval by the PA.

1.6. Definitions and Acronyms

See Appendix 2.

2. Publication and Repository Responsibilities

2.1. Repositories

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

a. Public Key Certificate;
b. CRL and/or Certificate Activation Status;
c. CPS;
d. Subscriber Agreement; and
e. Relying Parties Agreement.

2.2. Publication of Certificate Information

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.

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 Indonesian language document shall prevail.

2.3. Time or Frequency of Publication

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) calendar days after approval by the PA. 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. Access Controls on Repositories

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. Identification and Authentication

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. Naming

3.1.1. Types of Name

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 Distinguished Name (DN) to support identification of the Subscriber.

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.

3.1.2. Need for Names to be Meaningful

Privy CA uses DN to identify an individual and/or Legal Entity/Business Entity which is displayed in the Subject Name field and Issuer Name field. The content of the DN can be in the form of the following attributes:

The Common Name (CN) attribute used on individual certificates is the full name of the Subscriber plus the Privy Username, or the entity representing the Subscriber along with the Privy Username. Meanwhile, the Business Entity/Legal Entity uses the name of the Business Entity/Legal Entity according to the legality document belonging to the Business Entity/Legal Entity along with the Privy Username.

Organization name (O) attribute is the name of the Legal Entity/Business Entity in which the Certificate Holder is identified as part of such Legal Entity/Business Entity.

Organization Unit (OU) attribute is the name of the division/department/unit of the Legal Entity/Business Entity in which the Certificate Holder is identified as part of such Legal Entity/Business Entity. In the event that it is used in an

Organizational/Business Entity Certificate, it will be filled in as “Business Entity”.

The Country (C) attribute represents the country in which the Subscriber has declared its domicile.

The Organisation name and Organisation unit information is only used as a method of identification on the Certificate and does not represent authority over the Legal Entity/Business Entity.

For Certificates issued to individual Subscribers without information representing any Legal Entity/Business Entity, the Organization name attribute will be filled with the name of RA entity that performs the identification and authentication function of the Certificate Applicant data, and the Organization Unit will be filled as "Individual".

3.1.3. Anonymity or Pseudonymity of Subscribers

Privy does not publish anonymous or pseudonymous Certificates.

3.1.4. Rules for Interpreting Various Name Forms

The DN in the Certificate is described using the X,500 standard.

3.1.5. Uniqueness of Name

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. Recognition, Authentication, and Role of Trademarks

Applicants are not allowed to apply for Certificates with content that violates the intellectual property rights of others. Privy CA will not verify 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. Initial Identity Validation

Privy CA will identify each application for Certificate issuance.

3.2.1. Method to Prove Possesion of Private Key

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 possesion of the Private Key associated with the Applicant Certificate for the signing process, it uses the 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. Authentication of Organization Identity

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.

Privy CA and/or RA will check the applicant's identity according to the authentication of individual identity stipulated in section

3.2.3, position/authority of the Applicant, power of attorney (if required), legality document or legalization of Legal Entity/Business Entity in the form of Taxpayer Identification Number ("TIN") Card.

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.

3.2.3. Individual Identity Authentication

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 Class 3 and Class 4 Certificate classifications.

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, is required to show, prove, and provide the following requirements:

a. A copy of the document in the form of Population Identity Card (KTP) issued by the Government of Indonesia. Driver's License and Passport can be used as substitute or supporting documents if requested by Privy CA and/or RA;
b. Electronic mail address;
c. Phone number (including mobile phone); and
d. Biometric data in the form of selfies that have been tested for liveness detection using the liveness detection mechanism.

A liveness detection mechanism is a mechanism used to detect whether an object is alive or not. For the avoidance of doubt,

some liveness detection mechanisms are as follows:

a. Active liveness detection, where Privy and/or RA ask the Applicant to blink their eyes, shake their head, and or other movements in the verification process;
b. Passive liveness detection, where Privy and/or RA use certain algorithms in the verification process so that the system can detect whether the selfie or facial video provided by the Applicant is the face of a living person or not;
c. Remote Customer Onboarding, where by using video conference media, the Relying Parties will ask questions and/or provide instructions that must be followed by the Applicant; and/or
d. Other liveness detection test methods.

Privy CA and/or RA are obliged to check, validate, and ensure that the information contained in the Identity Card is valid and authentically submitted by the Applicant by matching data, including biometric data in the form of selfies, with population databases managed by government agencies that organize population administration.

If identity data matching is carried out by Privy CA and/or RA by matching data in the population database so that it is not directly carried out by the government that organizes population administration (or parties appointed by it), the Certificate issued is a Class 3 Certificate. If identity data matching is carried out directly by the government that organizes population administration (or parties appointed by it), the Certificate issued is a Class 4 Certificate. The requirements for the issuance of a Class 4 Certificate can also be met if the Applicant's identity data matching is carried out using an E-KTP Reader that has been activated by the government that organizes population administration.

Meanwhile, foreigners are obliged to provide:

a. Certificate registration form;
b. Photo of Passport or ID card documents;
c. 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;
d. Biometric data in the form of selfies that have been tested for liveness detection using a liveness detection mechanism; and
e. Phone number and/or email address;

Privy CA will issue a Class 3 Certificate for foreigners who attach a photo of the Passport document. For foreigners who have an ID card, a class 4 certificate can be issued by Privy CA in accordance with class 4 provisions.

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.

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.

3.2.4. Non-Verified Subscriber Information

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. Validation of Authority

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. Criteria of Interoperation

No Stipulation.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

The Subscriber may apply for a re-key provided that Privy CA will issue a new key pair and issue a new Certificate, with a new validity period. Privy CA will require the Subscriber to authenticate during the re-key request process, in accordance with the conditions mentioned in section 4.7.

3.3.2. Identification and Authentication for Re-key after Revocation

The re-key provisions mentioned in section 3.3.1 shall apply to Certificates that have been revoked or expired.

3.4. Identification and Authentication for Revocation Requests

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 possesion of the Subscriber's data information stored by Privy. In the case of a revocation request for an Individual Certificate, Privy CA will request data in the form of Privy Username (PrivyID) and email address. 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. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who can Submit a Certificate Application

Those who can apply for Certificate issuance are persons and/or Legal Entities/Business Entities.

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. Enrollment Process and Responsibilities

The following are the steps that must be taken to obtain a Certificate:

a. Send the completed registration form along with other required documents in accordance with the provisions in section 3.2. to Privy CA 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 Policy;
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 additional documents submitted by the Applicant which are accurate, correct and clear, 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; and
c. To send information and/or documents needed by Privy CA in the form of copies of ID cards, electronic mail addresses, telephone numbers, and selfies for the needs of compliance with laws and regulations.
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 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.

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.

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 has the authority to reject an application for Certificate 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 Policy.

4.2. Certificate Application Processing

4.2.1. Performing the Identification and Authentication functions

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. Approval or Rejection of Certificate Applications

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

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 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. Time to Process Certificate Applications

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. Certificate Issuance

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

4.3.1. RA Actions during Certificate Issuance

After carrying out verification and validation as set forth in sections 3.2.2, 3.2.3, and 3.2.5, RA then forwards the Certificate issuance request to Privy CA along with the Applicant's registration information that Privy CA is required to retain as described in section 4.1. RA shall ensure that the Subscriber receives the Certificate as set out in section 4.4.

4.3.2. Privy CA's actions during Certificate Issuance

Upon receiving a verified and validated Certificate issuance request, either through the Applicant or through the RA, CA Privy immediately generates the Key Pair associated with the Applicant and issues the Certificate through Privy's PKI system. The entire process of key issuance, key management, Certificate application, and Certificate issuance is performed through the PKI system.

In the event that the request is forwarded by RA, if it is deemed necessary by Privy CA, then Privy CA can verify and revalidate the information that has been forwarded before generating the Key Pair.

Upon Certificate Issuance, the Certificate belonging to the Applicant will become available and will be stored together with the documents electronically signed by the Subscriber.

4.3.2.1. Issuance of Certificates for Certificate Re-keying Request, and Expired and Revoked Certificates

In the event that a Subscriber requests for Certificate re-keying, or a Certificate expires or has been revoked, the issuance of a new Certificate can be carried out without going through the identification and authentication process as set out in section 4.2.1 provided that the Subscriber successfully performs the authentication mechanism specified by Privy CA for the issuance of the new Certificate.

4.3.3. Notification to Subscribers by Privy CA on Certificate Issuance

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.

4.4. Certificate Acceptance

4.4.1. Attitudes Constituting Certificate Acceptance

The Applicant is deemed to have received the Certificate upon notification to the Applicant in accordance with section 4.3.3.

If within 7 (seven) working days, the Subscriber does not submit a complaint about the information stated on the Certificate, the Subscriber is deemed to have accept all the information stated on the Certificate.

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. Publication of Certificate by CA

Privy CA publishes Privy CA Certificates in a Repository accessible through the Privy Website.

Privy CA does not publish End User Certificates.

4.4.3. Notification of Certificate Issuance by CA Privy to Other Entities

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. Key Pair and Certificate Usage

4.5.1. Subscriber's Private Key and Certificate Usage

The Subscriber entrusts the Private Key to Privy CA, in accordance with the agreement based on the Subscriber Agreement with Privy CA, Privy CA will store the Private Key using a Hardware Security Module (HSM) with a minimum specification of FIPS 140-2 Level 2.

Privy CA makes efforts to carefully secure and store the Subscriber's Private Key so that the Private Key can only be used by the Subscriber. The Subscriber must protect the authentication parameters used to activate their Private Key. The Subscriber shall only use their Private Key for the purpose specified.

4.5.2. Relying Party Public Key and Certificate Usage

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

The Relying Parties can access the Privy Public Key Certificate through the Privy Repository.

4.6. Certificate Renewal

Privy CA does not perform Certificate Renewal.

4.6.1. Circumstances for Certificate Renewal

No Stipulation.

4.6.2. Who May Request Renewal

No Stipulation.

4.6.3. Processing Certificate Renewal Requests

No Stipulation.

4.6.4. Notification of New Certificate Issuance to Subscribers

No Stipulation.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

No Stipulation.

4.6.6. Publication of the Renewal Certificate by Privy

No Stipulation.

4.6.7. Notice of Certificate Renewal by Privy to Other Parties

No Stipulation.

4.7. Certificate Re-key

Re-key is the process by which a Subscriber applies for the 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. Circumstances for Certificate Re-key

Certificate Re-keying can be carried out provided that:

a. The certificate has never been revoked;
b. The new Public Key has never been blacklisted;; or
c. All details associated with the Certificate are still accurate and do not require any new or additional validation.

4.7.2. Who Request Certificate Re-key

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. Processing Certificate Re-keying Requests

The Certificate re-keying procedure is as specified in sections 4.3 and 3.3.

4.7.4. Notification of Certificate Re-key Issuance to Subscribers

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 registered Applicant's telephone number, no later than within 3 (three) hours by referring to section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

The Subscriber is deemed to have received the rekeyed Certificate when the notice specified in section 4.7.4 has been received by the Subscriber with reference to section 4.4.1.

4.7.6. Publication of the Rey-keyed Certificate by Privy

Privy does not publish re-keyed Certificates.

4.7.7. Notification of Re-key Certificate by Privy

No Stipulation.

4.8. Circumstances for Modification

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. Circumstances for Modification

No Stipulation.

4.8.2. Who May Apply for Certificate Modification

No Stipulation.

4.8.3. Processing Certificate Modification Applications

No Stipulation.

4.8.4. Notification of New Certificate to Subscribers

No Stipulation.

4.8.5. Conduct Constituting Acceptance of Certificate Modification

No Stipulation.

4.8.6. Publication of Modified Certificate by Privy CA

No Stipulation.

4.8.7. Notification of Certificate Issuance by Privy CA to Other Entities

No Stipulation.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

Privy CA revokes the Certificate for the following reasons:

a. When the Subscriber 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 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. Who can Request Revocation

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.

Third parties who can apply for revocation must be able to prove that they are authorized by the Subscriber to revoke the certificate.

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. Procedure for Revocation Request

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.

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 use of the Certificate is not in accordance with the CPS; or
c. The Subscriber is no longer associated with the third party.

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 4.1. to 4.4.

4.9.4. Revocation Request Grace Period

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. Time Within wich Privy CA must Process Revocation Requests

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. Revocation Checking Requirement for Relying Parties

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.

4.9.7. CRL Issuance Frequency

CRLs are updated regularly within 1x 24 hours and can be accessed through the Repository.

4.9.8. Maximum Latency for CRLs

The CRL is published within 30 minutes after the CRL is updated.

4.9.9. Online Revocation/Status Checking Availability

Privy CA provides the Certificate status information checking service through OCSP which is always available at the URL https://ocsp.privyca.id, outside the maintenance time determined by Privy CA.

4.9.10. Online Revocation Checking Requirements

The Privy CA repository should contain and publish a list of all OCSP responders that they operate. 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. Other forms of Revocation Announcements Available

No Stipulation.

4.9.12. Special Requirements Related to Key Compromise

No Stipulation.

4.9.13. Circumstances for Suspension

Privy CA does not suspend Certificates.

4.9.14. Who can Request Suspension

No Stipulation.

4.9.15. Procedure for Suspension Request

No Stipulation.

4.9.16. Limits on Suspension Period

No Stipulation.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Privy CA provides Certificate status service through CRL or OCSP.

4.10.2. Service Availability

CRL or OCSP services are available at all time, outside of the maintenance time specified by Privy CA.

4.10.3. Optional Features

No Stipulation.

4.11. End of Subscription

The Certificate Period of Ownership shall end when the Certificate is revoked or its validity period expires. Privy CA has a procedure to terminate the subscription period.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

No Stipulation.

4.12.2. Key Encapsulation and Recovery Policy and Practices

No Stipulation.

5. Facilities, Management, and Operational Controls

5.1. Physical Controls

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. Site Location and Construction

All computing facilities used to run Privy CA Services are placed in a Data Center within the territory of the Republic of Indonesia. The Data Center is equipped with various logical and physical security mechanisms to keep non-Trusted Roles from having access to the Data Center. The Data Center building is constructed with premium quality. The Data Center must be located in such a location that in the event of a natural disaster, neither the Data Center nor the Recovery Data Center is affected.

5.1.2. Physical Access

To gain access to the Data Center, registration must be made in advance 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 Roles have access to the Data Center. Privy CA reviews physical access every 1 x 24 hours.

A security check of the facility that stores the privy device is performed when the facility is abandoned. Setidaknya proses pemeriksaan memverifikasi hal-hal sebagai berikut:

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

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

5.1.3. Power and Air Conditioning

Privy Data Center is 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 3 x 24 hours.

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. Water Exposures

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 Monitoring System that can detect high levels of air humidity.

5.1.5. Fire Prevention and Protection

The Data Center is equipped with smoke detection sensors, and an automatic fire extinguishing system.

5.1.6. Storage Media

Storage media is stored and protected from things that can cause damage. Copies used as backups of the storage media are stored and secured in a location separate from the Data Center.

5.1.7. Waste Disposal

All obsolete hardware is destroyed and disposed of in a safe and reasonable manner so that it can no longer be used.

5.1.8. Off-site Backup

Privy CA prepares a backup system that is sufficient to be used in order to recover from system failure. The backup system is performed directly (Hot Backup) and stored in a secure location and is in a separate location from the Data Center. Only the last stored backup system is used for recovery.

5.1.9. Recovery Data Center

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. Procedural Controls

5.2.1. Trusted Roles

Trusted Roles positions include but are not limited to:

a. Coordinator
b. Policy Authority (PA)
c. PA Staff
d. Network Administrator
e. Application Administrator
f. OS Administrator
g. HSM Administrator
h. Registration Authority (RA)
i. RA Staff
j. Registration
k. Key Custodian
l. Internal Audit

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

5.2.2. Number of Persons Required per Task

Privy CA requires at least 2 (two) persons plus 2 (two) backup persons to fill Trusted Roles positions to carry out each Trusted Roles action. As for the Coordinator and PA, it consists of 1 (one) person without backup person. Privy CA will use certain procedures to ensure that Trusted Roles actions cannot be carried out by 1 (one) person only.

5.2.3. Identification and Authentication for Each Role

Before filling the Trusted 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 Roles are filled by appropriate persons. Authentication of Trusted 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.

5.2.4. Roles Requiring Separation of Duties

Privy CA ensures that 1 (one) person can only fill 1 (one) Trusted 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. Personnel Controls

5.3.1. Qualification, Experience, and Clearance Requirements

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

5.3.2. Background Check Procedure

Administered through section 5.3.1.

5.3.3. Training Requirements

Each person hired to fill Trusted 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.

Evaluation of the adequacy of the competence of Privy CA personnel is carried out at least once a year.

5.3.4. Retraining Frequency and Requirements

Employees who fill Trusted Roles positions have skills and abilities that are consistent with developments in the PKI industry. Privy CA conducts regular retraining every quarter. In the event that Privy CA changes the PKI operational policy, Privy CA provides training in accordance with the policy changes adopted by the Privy CA.

5.3.5. Job Rotation Frequency and Sequence

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. Sanctions for Unauthorized Actions

Employees in the role of Trusted Roles who do not perform their roles in accordance with this CPS, whether intentionally or unintentionally, shall be subject sanctions based on Privy CA policy. Employees who are subject to such sanctions will be removed from the Trusted Roles function until further review by company management.

5.3.7. Independent Contractor Requirements

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

5.3.8. Documentation Supplied to Personnel

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

5.4. Audit Log Procedure

5.4.1. Types of Events Recorded

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.

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 logs so that every action of Trusted 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. Frequency of Processing Log

Privy CA checks the logs that have been stored at least once a week. 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.

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

5.4.3. Retention Period for Audit Logs

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. Protection of Audit Logs

Audit Logs are protected to prevent changes and detect tampering and to ensure that only individuals with authorized trusted access are able to perform any operations without modifying their integrity.

5.4.5. Audit Log Backup Procedures

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. Audit Collection System (Internal or External)

The log process for auditing runs automatically from system startup and otherwise stops if the system is shut down. Trusted Roles can create audit logs manually and separately.

5.4.7. Notification to Event-Causing Subject

No Stipulation.

5.4.8. Vulnerability Assessments

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

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. Records Archiving

5.5.1. Types of Records Archived

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.

5.5.2. Retention Period for Archive

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. Protection of Archive

Privy CA keeps archives protected from unauthorized access, modification, deletion, or tampering.

5.5.4. Archive Backup Procedure

Adequate and regular archive backup procedures are in place so that in the event of loss or damage to the main archive, a full set of backup copies is available in a separate location.

Archive backup is carried out by making a backup which is then stored on 2 (two) storage media. Each of these storage media is stored in a separate location.

5.5.5. Requirements for Time-Stamping of Records

All records are automatically time-stamped from the moment they are recorded.

5.5.6. Archive Collection System (Internal or External)

Archive collection is carried out internally by Privy.

5.5.7. Procedures to Obtain and Verify Archival Information

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

5.6. Key Changeover

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.

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. If an old Privy CA's Private Key is used to sign a CRL, the old key must be kept and protected.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

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.

5.7.2. Computing Resources, Software, and/or Data are Corrupted

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.

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.

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

5.7.3. Entity Private Key Compromise Procedure

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 Controls to be carried out to prevent the compromise from re-occuring.

5.7.4. Business Continuity Capabilities after a Disaster

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.

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. CA or RA termination

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 status information remains accessible for a period of 1 (one) 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
f. it destroys the Privy PKI system that contains the Privy CA's Private Key and Subscriber's Private Key.

In addition to the matters stated above, 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 Policy, and/or any other agreements.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

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 the system.

For Subscriber Key Pairs generated by Privy, the Private Key is stored and secured using a cryptographic module that meets FIPS-140-2 Level 2 requirements.

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. Private Key Delivery to Subscriber

Privy does not deliver the Private Key to the Subscriber.

6.1.3. Public Key Delivery to 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. Privy CA Public Key Delivery to the Relying Parties

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. Key Sizes

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

6.1.6. Public Key Parameters Generation and Quality Checking

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. Privy performs

periodic checks to test the Key size and ensure updates based on industry security standards and regulatory requirements.

6.1.7. Key Usage Purposes (as per X509 v3 key usage field)

Privy CA's Private Keys and Subscriber's Private Keys are used in accordance with the explanation provided in the Certificate Profile as referred to in section 10.

6.2. Private Key Controls and Cryptographic Engineering Module Controls

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. Private Key Controls and Cryptographic Module Engineering Controls

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.

6.2.2. Private Key (n out of m) Multi-Person Control

Privy implements technical mechanisms and procedures that require the participation of several (m out of n) Trusted Roles to perform sensitive cryptographic operations and functions such as but not limited to accessing and activating Privy CA's Private Keys.

6.2.3. Private Key Escrow

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

6.2.4. Private Key Backup

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 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. Private Key Archival

Privy CA Key is not archived.

6.2.6. Private Keys Transfer into or from a Cryptographic Module

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.

6.2.7. Private Key Storage on Cryptographic Module

Privy CA's Private Key is stored in a cryptographic module that 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. Method of Activating Private Key

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.

The activation and access of the Subscriber's Private Key is protected with security mechanisms controlled, supervised, maintained, and regulated by 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. Method of Deactivating Private Key

No Stipulation.

6.2.10. Methods of Destroying Private Key

Trusted 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) or by physically destroying the Privy hardware component in a secure physical environment.

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.

The destruction of the Privy Key is recorded in the log according to the logging provisions in section 5.4.

6.2.11. Cryptographic Module Rating

As listed in section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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	Operational Period
Privy CA Class 3	10 Years
Privy CA Class 4	10 Years
Certificate Class 3	1 Year
Certificate Class 4	1 Year

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

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 Roles that have met the predefined qualifications and undergone background checks.

6.4.2. Activation Data Protection

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 Roles and have met predefined qualifications and background checks.

6.4.3. Other Aspects of Activation Data

Privy CA's Private Key activation data is only authorized to the specified Trusted Roles.

6.5. Computer Security Control

6.5.1. Specific Computer Security Technical Requirements

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 Roles. All accesses become protected audit logs for the purpose of preventing and mitigating information security risks.

The following computer security functions are provided by a 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.
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 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.

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

6.5.2. Computer Security Rating

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. Life Cycle Technical Controls

All Privy's PKI components must undergo the following technical control cycle:

a. Procurement of hardware and software that goes through certain procedures to ensure the devices are free from any unauthorized changes.
b. Reasonable efforts are made to prevent and address malicious software access into the Privy device ecosystem.
c. All personnel who have access to the Privy system must undergo qualification and background checks as specified.
d. All aspects related to the management of Privy components are regulated and supervised with mechanisms determined by Privy to ensure information security along with countermeasures against existing risks.

6.6.1. System Development Controls

No Stipulation.

6.6.2. Security Management Controls

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.

6.6.3. Life Cycle Safety Controls

Privy ensures and maintains the trustworthiness and security of all PKI software and hardware components on a regular basis.

6.7. Network Security Control

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

6.8. Time-Stamps

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

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 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 auditable activity.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate 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.

All Certificates issued by Privy have a serial number that is at least 64 bits long with a value greater than zero (0).

Appendix 1 contains Certificate profiles for each of the Certificate classifications issued by Privy.

Privy will review the Certificate profile periodically at least once a year.

7.1.1. Version Number

Privy issues all Certificates with X.509 v3 version (populate the version field with integer "2").

7.1.2. Certificate Extentions

See Appendix 1.

7.1.2.1. Key Usage

See Appendix 1.

7.1.2.2. Certificate Policy Extension

See Appendix 1.

7.1.2.3. Basic Constraint

See Appendix 1.

7.1.2.4. Extended Key Usage

See Appendix 1.

7.1.2.5. CRL Distribution Points

See Appendix 1.

7.1.2.6. Authority Key Identifier

See Appendix 1.

7.1.2.7. Subject Key Identifier

See Appendix 1.

7.1.3. Algorithm Object Identifiers

The certificate issued by Privy uses the following algorithm:

Algorithm	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
prime256v1	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) curves(3) prime(1) 7 }

7.1.4. Name Formats

Each Certificate with this field complies with the naming format listed in section 3.1.

7.1.5. Name restrictions

Each Certificate issued by Privy has naming restrictions as listed in section 3.1.

7.1.6. Certificate Policy Object Identifier

Privy uses the OID for Privy CPS as listed in section 1.2.

7.1.7. Use of Policy Constraint Extensions

No Stipulation.

7.1.8. Qualification of Syntactic and Semantic Policy

No Stipulation.

7.1.9. Semantic Processing for Critical Certificate Policy Extensions

No Stipulation.

7.2. CRL Profile

Privy publishes CRLs in X.509 version 2 format that are subject to the standards and specifications listed in IETF RFC 5280.

7.2.1. Version Number

The published CRLs shall have the following fields:

a. Issuer: Subject of DN from Privy.
b. Version: Version of CRL.
c. Last update: CRL issuance date.
d. Next update: Expected date of the next CRL issuance.
e. Signature algorithm: Algorithm used for CRL tagging.

The list of Certificates that have been revoked by Privy listed on the CRL shall have the following fields:

a. Serial number: Lists the serial number of each revoked Certificate.
b. Revocation date: Revocation date of each Certificate.

7.2.2. CRL Extensions and CRL Notes

Privy issues CRLs with the following extensions:

a. CRL number: CRL serial number.
b. Authority Key Identifier: 160-bit SHA-1 hash of the Privy Public Key
c. Issuing Distribution Point: Link address to download the CRL.

7.3. OCSP Profile

Online Certificate Status Profile (OCSP) set up by Privy complies with the

standards in IETF RFC 6960 and IETF RFC 5019.

7.3.1. Version Number

Privy published the OCSP response version 1.

7.3.2. OCSP Extension

No Stipulation.

8. Compliance Audits and Other Fitness Assessments

8.1. Frequency or Scope of Assessment

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 is audited at least once a 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 such as the Adobe Approved Trust List or Webtrust for Certification Authorities.

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. Identity/qualification of Auditor

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 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 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 peer review, standards 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. Auditor's Relationship to Assessed Entity

The auditors selected to conduct the audit shall be independent auditors outside Privy.

8.4. Topics Covered by Assessment

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 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. Actions Taken as a Result of Discrepancy

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. The auditor must record the non-conformity
b. The compliance auditor must promptly communicate the findings to the PA; and
c. 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 such remedial actions without delay.

8.6. Communication of Results

The assessment report including the identification of corrective actions taken or to be taken by Privy is reported to the PA, and Privy forwards the report to other interested parties in accordance with the agreement and applicable laws and regulations.

8.7. Internal Audit

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

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Privy may charge fees based on the issuance, use, and/or renewal of Certificates.

9.1.2. Certificate Access Fees

No Stipulation.

9.1.3. Revocation or Status Information Access Fees

No Stipulation.

9.1.4. Fees of Other Services

Privy may charge for other fees that have not been regulated in this CPS.

9.1.5. Refund Policy

Privy does not have a return policy.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Privy has Cyber Edge Insurance Policy with a combined coverage limit of USD 2,000,000 (Two Million 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. Other Assets

No Stipulation.

9.2.3. Insurance or Warranty Coverage for Subscribers

Privy provides an Insurance Guarantee or Warranty for Subscribers which is regulated in the Warranty Policy document in the Privy Repository.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

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

a. Personal Data 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.

9.3.2. Information not within the scope of confidential information

Other information that is not categorized as confidential information regulated above is public information.

Certificates and information regarding the status of Certificates are categorized as public information.

9.3.3. Responsibility to Protect Confidential Information

Privy protects confidential information. The form of responsibility implementation 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. Privacy of Personal Information

9.4.1. Privacy Plan

Privy protects personal data in accordance with the provisions stated in the Terms of Service, Privacy Policy, 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.

9.4.2. Information Treated as Private

All information about the Subscriber that is not publicly available through the issued Certificate is considered personal data information. This includes personal data for Subscribers whose Certificates are successfully issued as well as those whose Certificate Issuance is denied.

Privy protects all Subscribers' personally identifiable information from unauthorized disclosure. Personal 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. Information not Deemed Private

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. Responsibility to Protect Private personal Information

Privy is responsible for storing personal information in accordance with the Privacy Policy securely. The information stored can be in digital or paper form. Backup of personal information must be encrypted every time it is transferred to backup media.

9.4.5. Notice and Consent to use Private Information

Personal information obtained from the Applicant during the registration process is treated as personal information so that the consent of the Applicant is required in order to use the information. Privy accommodates all provisions related to the use of personal information into the Privacy Policy document and the Subscriber Agreement. The use of Personal information

must be based on the execution of the Subscriber Agreement or Relying Parties Agreement, or other legal basis, which refers to the Privacy Policy and the provisions of laws and regulations.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Privy shall not disclose personal information to any third party except those authorized by this policy, required by law, government rules and regulations, or court orders.

9.4.7. Other Information Disclosure Circumstances

No Stipulation.

9.5. Intellectual Property Rights

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. Representations and Warranties

9.6.1. CA Representations and Warranties

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;
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. RA Representations and Warranties

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 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. Subscriber Representations and Warranties

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 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;
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;
f. The Subscriber is an end user and not a CA, and does not use the Private Key associated with the Public Key listed in the Digital Certificate for the purpose of digitally signing Certificates (or other formats of certified Public Keys) or CRLs as another CA;
g. 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;
h. 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;
i. The Subscriber and/or Applicant immediately stops using the Private Key associated with the Public Key whose Certificate was revoked;
j. The Subscriber and/or Applicant will respond to Privy's instructions regarding compromised circumstances or misuse of the Certificate within 48 (forty-eight) hours;
k. The Subscriber and/or 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 Policy, or if Privy finds that the Certificate is used to facilitate criminal acts such as phishing, fraud or malware distribution;

l. 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. Relying Party Representations and Warranties

In the event that the representative of the Relying Parties relies on the Certificate 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. Representations and Warranties of other Participants

No Stipulation.

9.7. Disclaimers of Warranties

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. It does not guarantee Certificates whose use is not in accordance with their designation; and
c. It does not guarantee the accuracy, authenticity, completeness or suitability of any information contained in the demo or testing certificate.

9.8. Limitations of Liability

9.8.1. Privy Limitation of Liability

As long as Privy has carried out the Certificate cycle operational requirements as stated in section 4 of this CPS, Privy is not 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. RA Limitation of LIability

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. Subscribers Limitation of Liability

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. Indemnities

9.9.1. Indemnification by Privy

Privy is not responsible for improper use of the Certificate.

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. Indemnification by Subscriber

To the extent permitted by law, the Subscriber agrees to indemnify Privy and its related parties against losses, damages, and costs, caused by:

a. a violation by the Subscriber of the Subscriber Agreement, this CPS, or applicable law, both 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, 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. Indemnification by Relying Parties

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 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. Term and Termination

9.10.1. Term

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. Termination

Upon the expiration of this CPS, all Certificates issued under the CPS shall remain valid until the expiration of the validity period of the last Certificate under the CPS.

9.10.3. Effect of Termination and Survival

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.

9.10.4. Amendments

Amendments to the CPS are indicated by a clear version number change. Any changes shall be effective 30 (thirty) days after publication.

9.11. Individual Notices and Communication with Participants

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. The notification is deemed to have been received if the sender receives a statement of receipt or written response from Privy.

Any amendments to the CPS will be made through an announcement made by Privy to the relevant parties. The announcement can be made through electronic information sent via electronic mail or short message via mobile phone, and also posted on the Site which will display the announcement for 7x24 hours after the announcement is made.

9.12. Amendments

9.12.1. Procedure for Amendment

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. Notification Mechanism and Period

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 is published no later than 7 (seven) working days from the date of signing.

9.12.3. Circumstances under Which OID Must be Changed

If the Policy Authority has a view that it is necessary to change the OID numbers involved, Privy will make the OID changes and implement the new policy using the new OIDs.

9.13. Dispute Resolution Provisions

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. Governing Law

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.

Parties, including CA partners, Subscribers, Relying Parties, cannot override the legal references specified above.

9.15. Compliance with Applicable Law

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. Miscellaneous Provisions

9.16.1. Entire Agreement

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. Assignment

Entities operating under this CPS may not assign their rights or

obligations without Privy's written consent.

9.16.3. Severability

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. Enforcement (Attorney's Fees and Waiver of Rights)

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 related to the waiver of rights in court must be submitted in writing and signed by Privy.

9.16.5. Force Majeure

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 provides BCP and DRP with reasonable control according to Privy's capabilities.

To the extent permitted by laws and regulations, the provisions regarding force majeure will be regulated more specifically through the Subscriber Agreement and the Relying Parties Agreement.

9.17. Other Provisions

9.17.1. Language

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. APPENDIX 1 - Certificate Profile

10.1. Privy CA Class 3 Certificate

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 with RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Ministry of Communication and Information Technology
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	Automatically set via software
Valid From	YYYY/MM/DD HH:MM:SS (10 (ten) years duration)
Valid To	YYYY/MM/D 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. Privy CA Class 4 Certificate

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 with RSA Encryption
Issuer: CN	Root CA Indonesia DS G1
Issuer: O	Ministry of Communication and Information Technology
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	Automatically set via software
Valid From	YYYY/MM/DD HH:MM:SS (10 (ten) years duration)
Valid To	YYYY/MM/D 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. Class 3 Certificate (Subscriber Certificate)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 with RSA Encryption
Issuer: CN	PrivyCA Class 3 - G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Full Name (according to ID card without title) (Privy Username)
Subject: OrganizationName	Name of RA Entity that performs identity validation
Subject: OrganizationalUnitName	Optional (Individual if submitted by an individual)
Subject: CountryName	ID
Subject Alternative Name	Optional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Automatically set via software
Valid From	YYYY/MM/DD HH:MM:SS (1 (one) year duration)
Valid To	YYYY/MM/D 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 (1.3.6.1.5.5.7.48.1), URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID: 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id

	OID: 2.16.360.1.1.1.3.12 Notice="Non-agency certificate" OID: 2.16.360.1.1.1.7.1 Notice="Personal Certificate" OID: 2.16.360.1.1.1.3.12.1 Notice="Digital Identity Privy"
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. Class 4 Certificate (Subscriber Certificate)

Basic Certificate Fields	Value
Version	V3
Signature Algorithm	SHA-256 with RSA Encryption
Issuer: CN	PrivyCA Class 4 - G2
Issuer: O	PT Privy Identitas Digital
Issuer: C	ID
Subject: CommonName	Full Name (according to ID card without title) (Username Privy)
Subject: OrganizationName	Name of RA Entity that performs identity validation
Subject: OrganizationalUnitName	Optional (Individual if submitted by an individual)
Subject: CountryName	ID
Subject Alternative Name	Optional Critical=FALSE RFC822Name = EmailAddress
Serial Number	Automatically set via software
Valid From	YYYY/MM/DD HH:MM:SS (1 (one) year duration)
Valid To	YYYY/MM/D 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 (1.3.6.1.5.5.7.48.1), URL=https://ocsp.privyca.id
Certificate Policies	Critical=FALSE Policy OID: 2.16.360.1.1.1.3.12.1.1 URL: https://repository.privyca.id

	OID: 2.16.360.1.1.1.3.12 Notice="Non-agency certificate" OID: 2.16.360.1.1.1.7.1 Notice="Personal Certificate" OID: 2.16.360.1.1.1.3.12.1 Notice="Digital Identity Privy"
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. Appendix 2 - Definitions and Abbreviations/Acronyms

11.1. Definitions

Term	Definition
Qualified Auditor	Persons or Legal Entities that meet the requirements in this CPS.
Business Entity/Legal Entity	Individual companies or partnership companies, both incorporated and unincorporated.
Electronic Data	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.
Electronic Information	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.
Electronic Documents	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.
Public Key Infrastructure ("PKI")	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.
Privacy Policy	Provisions regarding how Privy CA collects, uses, shares, processes, and secures personal data of Privy service users, including Subscribers. Privy's Privacy Policy is available at https://privy.id/id/kebijakan-privasi and/or in the Repository.
Certificate Policy ("CP")	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/.
Terms of Use of the Service	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.
Private Key	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.
Public Key	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.
Audit Report	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).
Online Certificate Status Profile ("OCSP")	An online Certificate checking protocol that allows Relying Parties software applications to determine the status of identified Certificates.
Registration Authority ("RA")	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 the CA, and requests for the re-issuance or renewal of the Certificate.
Key Pair	Private Key and associated Public Key.
Subscribers	Persons or Legal Entities who have successfully received a Certificate either through RA or Privy.
Applicants	Persons or legal entities that have

	submitted an application, but have not yet received a Certificate.
Certification Authority ("CA")	A legal entity that serves as a trustworthy party, which grants and audits Certificates.
Root CA	Top-level Electronic Certification Operators whose Root Certificates are distributed by Software Applications and sign subordinate CA Certificates.
Object Identifier ("OID")	This is a set of numbers that uniquely refers to an object or policy regulated by the CPS.
Subscriber Agreement	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.
Relying Party Agreement	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.
Relying Party	A person or Legal Entity who entrusts the Certificate and/or Digital Signature issued by the CA.
Repository	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/.
Electronic Certificate ("Certificate")	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.

Root Certificate	A certificate issued and self-signed by a Root CA to identify itself and to facilitate the certification of Certificates issued by Subordinate CAs.
Website	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.
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.
Subject	It means the individual, Legal Entity/Business Entity identified in the Certificate as the Subject.
Subordinate CA ("Sub-CA")	A CA whose Certificate is signed by the Root CA, or another Subordinate CA.
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.
Certificate Practice Statement ("CPS")	One of several documents that form the governance framework within which Certificates are created, issued, managed and used.
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. Abbreviations/Accronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
C	Country
CA	Certification Authority/Electronic Certification Authority
CICA	Canadian Institute of Chartered Accountants
CN	Common Name
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certification Revocation List
DN	Distinguished Name
DoS	Denial of Services
EDI	Electronic Data Interchange
FIPS	Federal Information Protection Standards
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ID CARD	Identity Card
NIB	Business Identification Number
NIK	Population Identification Number
TIN	Taxpayer Identification Number
O	Organization Name
OU	Organization Unit
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PA	Policy Authority
PKI	Public Key Infrastructure
CA	Certification Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SIUP	Trade Business License
SIM	Driver's License
SK	Decree

SOP	Standard Operational Procedure
Sub-CA	Subordinate Certification Authority
RA	Registration Authority
UPS	Uninterrupted Power Supply (UPS)
URL	Uniform Resource Locator