Certificate Policy & Certificate Practice Statement (CP/CPS) NotarisID B.V.

Version	2.4
Date	11.4.2023
Subject	CP/CPS
Reference	-
Appendix	0
Classification	**WHITE**[1]

NOTE **Drafter must not change the headings of the chapters, since this document follows the suggested outline of RFC 3647 exactly.**

.

Version

Version	Changes	Date
0.8	Draft version for review	09/06/2021
0.9	Draft version for review	21/06/2021
1.0	Approval final version	22/06/2021
1.1	Draft version for review	TBD
1.2	Feedback processed	26/07/2021
1.5	Feedback architects processed	05/10/2021
1.7	Various feedback processed	15/03/2022
1.8	Final review comments processed	24/03/2022
1.9	Processed changed role of Registration Officer	31/03/2022
2.0	Approved by management	31/03/2022
2.1	Restructuring in accordance with RFC 3647 and rewriting due to use of USB-tokens.	12/12/2022
2.2	Changes due to PKI design sessions	16/1/2023
2.3	Minor changes after ETSI stage 1 audit	1/2/2023
2.4	Changed paragraph 7.1.4 regarding test certificate. Termination registration process in case an Appointed Notary accepts another identification document than what is stated herein. Changed paragraphs 4.9.1 and paragraph 6.2.1 regarding validity of certifications of QSCD's and HSM's. Changed paragraph 2.2 regarding which documents are part of archive.	11/4/2023

Content

1 Introduction

1.1 Overview

NotarisID B.V. (hereafter: NotarisID) is a Certificate Authority (CA) and a Trust Service Provider (TSP) which provides the issuance, management, and revocation of Certificates. NotarisID operates in the context of national and European legislation on trust services, including the eIDAS Regulation (EU Regulation 910/2014) and Dutch Telecommunications Act[2].

NotarisID follows, inter alia:

- Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;
- ETSI EN 319 401 V2.3.1 (2021-05);
- ETSI EN 319 411-1 V1.3.1 (2021-05);
- ETSI EN 319 411-2 V2.4.1 (2021-11);
- NPR-CEN/TS 419261[3];
- ISO27001:2013 standards.

Regarding ETSI 319 411-1 and 319 411-2 the following certificate policies are followed:

- NCP+: Normalized Certificate Policy requiring a secure cryptographic device;
- QCP-n-qscd: Policy for EU Qualified Certificate issued to a natural person where the private key and the related certificate reside on a QSCD.

NotarisID issues Certificates which can be used by Relying Parties to verify electronic signatures placed by a Subscriber with a Private Key which in its turn is uniquely linked to the Certificate. This Private Key is held under sole control of Subscriber using an USB-token. The Certificate contains, inter alia, the attributes of Subscriber (first name and last name) and the Public Key. The Certificate is signed by NotarisID using its own private key linked to the NotarisID Subscriber CA certificate. The attributes of the Subscriber are validated by NotarisID by using a Notary Deed of an Appointed Notary as proof of the identity of the Subscriber.

This CPS is applicable to all certificates issued within this CA hierarchy:

- NotarisID Root
    - NotarisID Subscriber Issuing
        - NotarisID Subscriber

[2] Telecommunicatiewet 1998

[3] Also known as “Security requirements for trustworthy systems managing certificates and time-stamps”. TWS is the acronym used to refer to that document.

- Non-repudiation (2.5.29.15.1)

The present document is part of the NotarisID collection of documents that is commonly referred to as the 'set of provisions', as originally defined in IETF RFC 3647[4]. This document follows the structure as defined in aforementioned IETF RFC 3647. IETF RFC 3647 suggests that in case a certain topic does not apply, the accompanying chapter is populated with “no stipulation”. This document follows that suggestion, however, it will -where possible- mention between brackets and in italic, why this topic does not apply and/or is unnecessary in NotarisID context.

1.2 Document name and identification

This document is referred to as “Certificate Policy & Certificate Practice Statement (CP/CPS) NotarisID B.V.” (English) or “Praktijkverklaring NotarisID B.V.” (Dutch). For short it is referred to as “CP/CPS” in NotarisID context.

1.3 PKI participants

This chapter describes the PKI participants.

1.3.1 NotarisID.

NotarisID, a Dutch limited liability company, registered at the Chamber of Commerce under number 76121526. NotarisID issues the Certificates. NotarisID is Registration Authority and Certificate Authority (NotarisID Root CA and NotarisID Subscriber Issuing CA).

1.3.2 Registration Authority and Registration Officers

NotarisID is ultimately accountable as the Registration Authority for establishing the identity of Applicants. The task of validating the identity of Applicants is performed ultimately by the Registration Officer with the help of an Appointed Notary. NotarisID has entered into an agreement (Appointment Agreement) with a selected group of Dutch Notaries (Appointed Notaries). The Registration officer supports Applicant in making an appointment with an Appointed Notary for part of the face to face identity proofing process. The appointed notary sends (a copy of) the resulting Notary Deed to the Registration Officer. The Registration Officer performs certain checks regarding the Notary Deed. Once the Registration Officer completes all checks successfully, the application moves to the next stage (provisioning and Certificate dissemination).

[4] WWW <https://www.ietf.org/rfc/rfc3647.txt>

1.3.3 Subscribers

A Subscriber is a natural person who applies for a Certificate, and once the application was successful is able to make use of the Private Key associated to the Certificate, by using a NotarisID issued USB-token.

1.3.4 Relying Parties

A Relying Party is a natural or legal person who relies upon the information contained within the Certificate. The Relying Party is -inter alia- responsible for checking the validity of the Certificate. In NotarisID context any natural or legal person can be a relying party. Also Subscriber or a Dutch Notary can be a relying party.

1.4 Certificate usage

1.4.1 Type of Certificate

NotarisID only issues one type of Certificate, which is the Certificate for nonrepudiation. The Subscriber can use the Private Key linked to the Certificate to sign electronic document. The Relying Party can use the Certificate to validate the signature.

1.4.2 Appropriate Certificate usage

The appropriate use for the Certificate is:

- the Subscriber is invited by an Appointed Notary to sign an electronic obligatory law transactional contract (title), for which later a notary deed is necessary for lawful execution and/or effectuation;
- or the Subscriber is invited by an Appointed Notary to sign a power of attorney in Notary context;
- and the transaction value of the aforementioned agreement or power of attorney is not higher than € 250.000 (two hundred fifty thousand Euros);
- and Subscriber adheres to the General Terms and Conditions and/or Relying Party must adhere to Terms for Relying Parties.

See also PKI Disclosure Statement and General Terms and Conditions.

1.4.3 Prohibited Certificate usage

Prohibited applications include the following:

- any use of a Certificate after it has been revoked;
- any use of a Certificate after it has expired;

- extract the Certificate from a signed electronic document, and disclose it in any way or form (outside the electronic document).

See also PKI Disclosure Statement, General Terms and Conditions and Terms for Relying Parties.

1.5 Policy administration

Information located in this section includes the contact information of the organization responsible for drafting, registering, maintaining, updating, and approving the CP/CPS.

1.5.1 Organization administering the document

NotarisID assesses this CP/CPS and corrects any errors or omissions, at least once a year. Intended major revisions of this document will be established by the management of NotarisID. Minor/administrative revisions will be done without prior announcement. With minor revisions the version number will increase by 0.1, major revisions lead to a new version.

All changes related to major revisions of the CP/CPS shall be communicated in accordance with the communication plan of NotarisID. Subscribers and known Relying Parties (e.g. Appointed Notaries), will be notified actively of these changes within three (3) months before the actual change. An exception is made for security critical changes, which may become effective immediately without prior notice.

1.5.2 Contact person

Please address any enquiries about this CP/CPS per email to: service@notarisid.nl

Or, alternatively per mail, to:
NotarisID B.V.
Hogehilweg 6
1101 CC AMSTERDAM

1.5.3 Determining CP/CPS suitability

Please refer to paragraph 1.5.1 of this CP/CPS.

1.5.4 Subscriber CP/CPS approval procedures

For TSP documents (inter alia functional designs, technical designs, policies, (work) instructions, document for dissemination), including this CP/CPS, NotarisID has a workflow procedure in place. This procedure invites subject matter experts, part of the internal policy authority, to share their opinions with others. After processing those opinions the document is presented to management for approval. In case the document was approved, and is part of the Document Repository family (e.g. this CP/CPS), the document will then be placed within the Document Repository by a Trusted Staff Member of NotarisID.

See paragraph 1.2 of this CP/CPS for documents part of the Document Repository family.

1.6 Definitions and acronyms

Unless otherwise defined in this document, words starting with capitals in this document have the meaning attributed to them in this section, regardless of whether the words are used in singular of plural form.

1.6.1 Definitions

Appointed Notary: A by NotarisID appointed Notary, who is allowed to perform identity proofing tasks and to deliver a Notary Deed regarding the declaration of identity to Registration Officer of NotarisID. The appointment is done through a special agreement between the Notary and NotarisID, called the Notary Appointment Agreement.

Applicant: The natural person who applies for a Certificate. After successful registration the Applicant becomes the Subscriber.

Certificate: A set of data that contains the identity of a Subscriber and the Public Key of said Subscriber. The data is electronically signed by NotarisID.

Certification Authority (CA): An entity that issues Certificates, for this CP/CPS that would be NotarisID.

Document Repository: an online repository of documents as mentioned in paragraph 2.2 of this CP/CPS.

Identity Document Scanner: the Identity Document Scanner that a Notary is obliged to use pursuant to article 19A of the Professional Regulation (“Beroepsverordening”) (https://www.wet-en-regelgeving-notariaat.nl/overige-regelgeving/content/1011).

Middleware Software: Software to be installed by the Subscriber on his or her computer, which allows the Subscriber to use the USB-token to electronically sign electronic documents.

Notary: An official Notary or candidate notary as registered in the official notarial registry (https://registernotariaat.nl/registernotariaat)

Notary Appointment Agreement: the agreement between an Notary and NotarisID regarding the appointment of the Notary.

Notary Deed: The official and certified deed issued by an Appointed Notary stating the identity of the Applicant was determined by him or her. The Notary Deed may also indicate that the identity of an Applicant could not be determined.

Private Key: The key of a key pair that is kept secret by the holder of the key pair. This key can be used to create electronic signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key. This key is used by a Relying Party to verify electronic signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Registration Authority (RA): An individual or (internal) organisation or process responsible for verifying the identity of a Subscriber prior to issuing a Certificate to Subscriber.

Registration Officer (RO): An individual or organisation responsible for verifying, based on the Notary Deed, that identity proofing and registration of the Applicant has rendered successfully, and thereafter allowing the issuance of a Certificate.

Relying Party: An entity that relies upon the information contained within the Certificate and relies on the outcome of the Certificate status services of CA.

Root CA Certificate: The NotarisID certificate generated and self-signed by NotarisID based on its own key pair, This certificate (i.e. the Private Key linked to it) is used to electronically sign the Subscriber Issuing CA Certificate.

Subscriber Issuing CA Certificate: The NotarisID certificate generated and signed by the Private Key linked to the Root CA Certificate. This certificate (i.e. the Private Key linked to it) is used to electronically sign the Subscriber Certificate.

Subscriber: An entity that has been issued a Certificate. If the Certificate has been issued to a natural person, 'subject' and 'Subscriber' refer to the same entity.

Trusted Staff Member: a staff member of NotarisID that is appointed by management of NotarisID for one or more trusted roles, as mentioned in paragraph 5.2.1 of this CP/CPS. The list of trusted roles, as

mentioned in aforementioned paragraph, is not exhaustive.

Trust service provider (TSP): The definition of eIDAS (Article 3 Definitions) is used. In case the provider is a qualified Trust Service Provider, the abbreviation QTSP is used.

USB-token: a Qualified Signature Creation Device (QSCD) as mentioned in Annex II of eIDAS. This device is provisioned by NotarisID for Subscriber, and is after issuance under sole control of Subscriber. The devices contains the Private Key and Certificate of Subscriber. An electronic signature can be placed on an electronic document, by activating the USB-token with a pin that is only known for Subscriber, provided the Middleware Software is used by Subscriber.

WID: Wet op Identificatieplicht. (Dutch) Compulsory Identification Act.

1.6.2 Acronyms

CA: Certificate Authority

CP: Certificate Policy

CPS: Certification Practice Statement

CSR: Certificate Signing Request

CRL: Certificate Revocation List

DN: Distinguished Name

ETSI: European Telecommunications Standards Institute (ETSI)

FQDN: Fully Qualified Domain Name

GDPR: General Data Protection Regulation

HSM: Hardware Security Module

ITU: International Telecommunication Union

OCSP: Online Certificate Status Protocol

PKI: Public Key Infrastructure

PKIX: Public Key Infrastructure (based on X.509 Digital Certificates)

QSCD: Qualified Signature Creation Device

RA: Registration Authority

RO: Registration Officer

SAM: Signature Activation Module

URI: Uniform Resource Identifier

URL: Uniform Resource Locator

2 Publication and repository responsibilities

2.1 Repositories

NotarisID publishes information about the Certificates that it issues in an online Document Repository, which is accessible through https://portal.notarisid.nl. The Document Repository is accessible at any time, at least with an availability of 99,8% on a monthly basis.

The CRL server is available at:

CRL of NotarisID Root CA	https://pub-notarisid.nl/shared/static/7737lx8r5lb0m8n0bjtuhzpu60ff1j7j.crl
CRL of NotarisID Subscriber Issuing CA	https://pub-notarisid.nl/shared/static/mnzoa8wotl29kedhs9lwo0fl1knf2wr3.crl

The CRL server is available at any time, at least with an availability of 99,8% on a monthly basis.

2.2 Publication of certification information

The following information is accessible in the Document Repository:

#	English Name (if any)	Dutch Name (if any)
1	CP/CPS	Praktijkverklaring
2	PKI Disclosure Statement	n/a
3	General Terms and Conditions	Algemene Voorwaarden
4	Terms for Relying Parties	Informatie voor Vertrouwende Partijen
5	Privacy Statement	Privacy Verklaring
6	n/a	Klachtenprocedure
7	Root CA Certificate	n/a
8	Subscriber Issuing CA Certificate	n/a
9	Instructions for use Middleware Software, including hashes regarding binaries.	Instructies voor Middleware Software, inclusief hashes voor uitvoerbare bestanden.

Earlier versions of the CP/CPS, PKI Disclosure Statement, General Terms and Conditions and Terms for Relying Parties are also available at the website of NotarisID.

NotarisID does not make the Certificates available for Subscribers available outside the USB-token. NotarisID deems the Certificate sensitive and/or of personal nature (since verified attributes are bound to

the Certificate). The Certificate however is attached to the electronic document Subscriber signed with the use of the Private Key securely stored in the USB-token.

2.3 Time or frequency of publication

Described hereunder is the frequency of publication into the Document Repository. The second column refers to the document numbers as set out in paragraph 0 of this CP/CPS.

Frequency / When published	**# document**
After revision and approved by management NotarisID	1, 2, 3, 4, 5, 6 and 9
After successful key ceremony and successful registration.	7 and 8

The certificate status services (CRL) are updated immediately after a successful revocation.

2.4 Access controls on repositories

The Document Repository is secured against unauthorized modifications. Only the Trusted Staff Members have writing permissions for the Document Repository.

3 Identification and authentication

This section describes the identification and authentication process during initial registration. NotarisID only has one (1) process, this process is described in this chapter of this CP/CPS.

3.1 Naming

3.1.1 Types of names

The Subscriber is identified in the subject field of the certificate with a distinguished name (DN) as meant in X.501:

serialNumber	The unique serial number of the Certificate, also used to ensure the bind attributes (names) are unique (GUID)
commonName	This field consists of the exact values of the givenName and surname in the next two fields. <givenName> <surname>
givenName	This field accurately reflects the Subscriber's given name(s) as stated on the identification document (WID)
Surname	This field accurately represents the Subscriber's last name(s), including prefixes, as stated on the identification document (WID).

Please refer to the certificate profiles as described in chapter 7 of this CP/CPS for more information.

3.1.2 Need for names to be meaningful

No stipulation.

(Each DN has a meaningful relation to the represented Subscriber)

3.1.3 Anonymity or pseudonymity of Subscribers

No stipulation.

(Pseudonymous or anonymous Certificates are not supported by NotarisID)

3.1.4 Rules for interpreting various name forms

No stipulation.

(Not applicable, the attributes from the scanned identity document are leading and not open for interpretation, the visual part of documents NotarisID accepts are always Latin character based)

3.1.5 Uniqueness of names

The name of the Subscriber is unique. This uniqueness is achieved by adding the unique serial number to the name.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to proof possession of Private Key

The Private Key is generated by NotarisID. NotarisID does not accept private keys generated by Applicants.

3.2.2 Authentication of Organization identity

No stipulation.

(NotarisID does not issue Certificates to organizations, only to natural persons)

3.2.3 Authentication of individual identity

- Applicant applies for Certificate at a designated area, on the website of NotarisID.
- Applicant consents with applicable General Terms and Conditions.
- Registration Officer of NotarisID contacts the Applicant, to make an appointment with an Appointed Notary.
- Notary confirms appointment, and applies his / her own terms and conditions (including any privacy statement(s)) regarding his / her identity proofing / attribute attestation service.

- Applicant goes to Appointed Notary at the agreed upon date and time.
- Appointed Notary scans the identity document with his or her Identity Document Scanner.
- Only the following identity documents are supported:
    - Dutch Passport issued by a Dutch government.
    - Dutch Identity Card issued by a Dutch government.
- In case an Appointed Notary accepts another document, the registration process is terminated by the Registration Officer, despite the end result, the Notary Deed, being valid and legal.
- Appointed Notary checks as described by in the Notaries Act and underlying laws:
    - the result of the Identity Document Scanner;
    - if Applicant is the actual holder of the Identity Document;
    - the BRP (“Basisregistratie Personen”);
    - if the Identity Document is not reported missing, through VIS (“Verificatie Identificatie Systeem”);
- In case the checks were positive, Appointed Notary creates an official Notary Deed, in which Notary Deed he or she states that the identity of the Applicant was determined and the attributes as state in the Notary Deed were validated.
- A copy of the Notary Deed is sent to the Registration Officer of NotarisID.
- Registration officer performs checks regarding the copy of the Notary Deed, including (for example) a check to establish whether the Appointed Notary was registered as a Notary or Candidate Notary at the time he / she signed the Notary Deed and/or was not (temporary) suspended from office.
- In case checks were positive, the Registration Officer passes the application to the Device Provision Service of NotarisID (for dissemination of the Certificate to the USB-token).

3.2.4 Non-verified Subscriber information

NotarisID uses two attributes which are not verified directly (in accordance with paragraph 3.2.3 of this CP/CPS), but are verified indirectly. Those are e-mail address and telephone number. These are used for communication. The Registration Officer verifies those indirectly, by using the given attributes for contacting the Applicant to schedule an appointment with an Appointed Notary.

3.2.5 Validation of authority

No stipulation.

(NotarisID does not determine certain rights, entitlements and/or permissions of the Applicant)

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

(NotarisID does not support re-keying)

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

(NotarisID does not support re-keying. After revocation a Subscriber may apply for a new Certificate.)

3.4 Identification and authentication for revocation requests

In case the revocation is done by Subscriber, the Subscriber must call the Revocation Officer of NotarisID. The Revocation Officer will ask for the revocation code. In case Subscriber does not have the Revocation Code, the Revocation Officer will ask the Subscriber questions, regarding the attributes of Subscriber. In some case the Revocation Officer might initiate a video call, and will ask Subscriber to hold up a valid Dutch Identity Document.

4 Certificate life-cycle operation requirements

4.1 Certificate application

4.1.1 Who can submit a Certificate application

A natural person with Dutch citizenship and a valid identity document as defined in paragraph 3.2.3 of this CP/CPS.

4.1.2 Enrolment process and responsibilities

Since NotarisID generates the Private Key and Public key, there is no special process in place that the Applicant has to follow, save for the process as set out in paragraph 3.2.3 of this CP/CPS.

Applicant is responsible for:

- having a valid identity document as defined in paragraph 3.2.3 of this CP/CPS;
- following up directions and/or communication requests of Registration Officer;
- showing up at the agreed upon date and time at the notary office of the Appointed Notary with the agreed upon identity document.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Please refer to paragraph 3.2.3 of this CP/CPS.

4.2.2 Approval or rejection of Certificate applications

Please refer to paragraph 3.2.3 of this CP/CPS.

4.2.3 Time to process Certificate applications

The time to process the application depends on when Applicant is able to see an Appointed Notary for the necessary identity proofing. The whole process can take up ten (10) working days, or more.

4.3 Certificate issuance

4.3.1 CA actions during Certificate issuance

The CA validates the completion of the process described in section 3.2.3 before issuance of a Certificate.

4.3.2 Time to process Certificate applications

Subscriber receives an e-mail notification after issuance of the Certificates. The e-mail also contains an invitation to contact the Registration Officer for an appointment. Please refer to paragraph 4.4.1 of this CP/CPS.

4.4 Certificate acceptance

4.4.1 Conduct constituting Certificate acceptance

The acceptance of the Certificate coincides with the acceptance of the USB-token. A Trusted Staff Member will hand over the USB-token to the Applicant. Acceptance of Certificate will be deemed to have occurred after handing over of the USB-token. Subscriber must then sign for receipt of the USB-token, which means that the Subscriber accepts integrally this CPS/CPS and the terms and conditions. Please refer to paragraphs 6.1.2 and 6.1.3 of this CP/CPS for the process of Private Key and Public Key / Certificate delivery.

4.4.2 Publication of the Certificate by the CA

No stipulation.

(NotarisID does not make the Certificate available for the public)

4.4.3 Notification of Certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate usage

The agreement entered into by the Subscriber entails the obligations for the use of the USB-token, Private Key and/or Certificate in accordance with this CP/CPS, the General Terms and conditions for Subscribers.

4.5.2 Relying Party Public Key and Certificate usage

The Terms for Relying Parties entail the obligations for the use of the Certificate in accordance with this CP/CPS and the Terms for Relying Parties, and the usage purposes described in the Certificate.

4.6 Certificate renewal

No stipulation.

(NotarisID does not support Certificate renewal, Subscriber should apply for a new Certificate)

4.7 Certificate re-key

No stipulation.

(NotarisID does not support Certificate re-keying, Subscriber should apply for a new Certificate)

4.8 Certificate modification

No stipulation.

(NotarisID does not support Certificate modification, Subscriber should apply for a new Certificate)

4.9 Certificate revocation and suspension

A Certificate can be revoked under certain circumstances (see paragraph 4.9.1 of this CP/CPS). NotarisID will then put the concerning Certificate on a Certificate revocation list (CRL) stating that the Certificate was revoked. Once a Certificate has been revoked, the Certificate cannot be (made) valid again. This section describes under which circumstances, by whom and in which way a Certificate can be revoked.

NotarisID does not support suspension.

4.9.1 Circumstances for revocation

A Certificate can be revoked under the following circumstances:

- The Subscriber requests revocation.
- Confidentiality of the Private Key corresponding to the Certificate's Public Key was presumably compromised. Cases include those: in which the USB-token is lost, or confidentiality of the PIN was compromised.
- The Subscriber fails to comply with his or her obligations based on this CP/CPS and/or the agreement (based on General Terms and Conditions).
- Information in the Certificate is not or no longer correct and up-to-date, or information in the Certificate is misleading.
- There are indications that the Certificate is being misused.
- The Certificate appears not to have been issued following the proper procedures in retrospect.
- NotarisID terminates its activities with no other (Q)TSP taking over the Document Repository and/or CRL services (including bankruptcy of NotarisID).
- NotarisID suspects the CA Private Key used to issue the Certificate to be compromised.
- Other circumstances occur which, that in the view of NotarisID, justify revoking the Certificate to sustain trust in the Public Key infrastructure.
- The Subscriber, who is a natural person, has died.
- Algorithm compromise.
- The Certificate was issued in violation of the then-current version of these requirements.`
- The common criteria certification regarding the QSCD (USB-token) is revoked in the interim.

4.9.2 Who can request revocation?

A Certificate may be revoked at the initiative of:

- NotarisID
- Subscriber

NotarisID can itself initiate Certificate revocation, anyone who is aware of a circumstance that could lead to revocation may inform NotarisID without obligation. With the Appointed Notaries, NotarisID made the agreement, that in case an Appointed Notary is aware of a Subscriber that has passed away (for example,

in case an Appointed Notary is asked for the will of the Subscriber that has passed away), he or she must notify NotarisID. Revocation can then proceed if NotarisID sees a reason for it.

4.9.3 Procedure for revocation request

Please refer to paragraph 3.4 of this CP/CPS.

4.9.4 Revocation request grace period

Subscriber is required to request a revocation request immediately in case one of circumstances mentioned in the CP/CPS and/or General Terms and Conditions occur. No grace period is permitted once a revocation request has been verified. NotarisID will revoke a Certificate as soon as possible following successful verification of a revocation request.

4.9.5 Time within which CA must process the revocation request

The maximum delay, between receipt of a revocation request and the decision to change its status information being available to all Relying Parties ,shall be at most 24 (twenty four) hours.

The maximum delay, between the confirmation of the revocation of a Certificate to become effective and the actual change of the status information of this Certificate being made available to Relying Parties, shall be at most 60 minutes.

4.9.6 Revocation checking requirement for Relying Parties

Before relying on a Certificate a Relying Party is obliged to:

- validate the Certificate;
- validate the complete chain (of signers) of the Certificate;
- check the revocation status of the Certificate through CRL's;
- take notice of the limitations regarding the use of the Certificate.

CRL's are publicly available online. Please refer to section 2.1 of this CP/CPS.

See also PKI Disclosure Statement and Terms for Relying Parties.

4.9.7 CRL issuance frequency

The NotarisID Subcriber Issuing CA certificate CRL is updated every clock hour.

The NotarisID Root CA certificate CRL is updated once a year, or so much sooner after revocation and/or renewal.

4.9.8 Maximum latency for CRLs (if applicable)

No stipulation.

4.9.9 Online revocation/status checking availability

No stipulation.

(NotarisID does not support OSCP)

4.9.10 Online revocation checking requirements

(NotarisID does not support OSCP)

4.9.11 Other forms of revocation advertisements available

No stipulation.

(NotarisID does not support any other forms of revocation advertisements)

4.9.12 Special requirements regarding key compromise

4.9.12.1 Root CA Certificate

Revocation of the Root CA Certificate will be considered if the signing key belonging to the Root CA Certificate is compromised or suspected to be compromised. Indicators of Private Key compromise may include:

- audit findings indicating Private Key compromise;
- incidents reported by third parties which may indicate Private Key compromise.

All indicators are registered, analysed, and followed up accordingly. In case of a Private Key compromise regarding the Root CA Certificate, NotarisID must revoke its Root CA Certificate immediately.

4.9.12.2 Subscriber Issuing CA Certificate

Revocation of the Subscriber Issuing CA Certificate will be considered if the signing key belonging to the Subscriber Issuing CA Certificate is compromised or suspected to be compromised. Indicators of Private Key compromise may include:

- audit findings indicating Private Key compromise;
- incidents reported by third parties which may indicate Private Key compromise.

All indicators are registered, analysed, and followed up accordingly. In case of a Private Key compromise regarding the Subscriber Issuing CA Certificate, NotarisID must revoke its Subscriber Issuing CA Certificate immediately.

4.9.12.3 Subscriber Certificate

Revocation of the Certificate will be considered if the signing key belonging to the Certificate is compromised or suspected to be compromised. Indicators of Private Key compromise may include:

- theft or loss of USB-token holding the Private Key;
- audit findings indicating Private Key compromise;
- incidents reported by third parties which may indicate Private Key compromise.

All indicators are registered, analysed, and followed up accordingly. In case of a Private Key compromise, the Subscriber must revoke his / her Certificate immediately.

In case of a Private Key compromise, the Subscriber must cease using the USB-token and revoke his / her Certificate immediately.

An entity who discovers a key compromise may report it by sending an email or call NotarisID. Please refer to paragraph 1.5.2 of this CP/CPS.

4.9.13 Circumstances for suspension

No stipulation.

(NotarisID does not support suspension)

4.9.14 Who can request suspension?

No stipulation.

(NotarisID does not support suspension)

4.9.15 Procedure for suspension request

No stipulation.

(NotarisID does not support suspension)

4.9.16 Limits on suspension period

No stipulation.

(NotarisID does not support suspension)

4.10 Certificate status service

4.10.1 Operational characteristics

NotarisID offers a Certificate status service allowing to check the validity of Certificates. NotarisID uses only Certificate Revocation Lists (CRL).

4.10.2 Service availability

Please refer to paragraph 2.1 of this CP/CPS.

4.10.3 Optional features

No stipulation.

(There are no additional or optional features)

4.11 End of subscription

A Subscriber's subscription service ends when the Certificate of Subscriber expires, the Certificate is revoked successfully or the Subscriber agreement expires.

See further the General Terms and Conditions for end of subscription.

4.12 Key escrow

No stipulation.

(NotarisID does not support key escrow)

5 Facility, management, and operational controls

This section describes non-technical security controls used by NotarisID to perform the functions of key generation, subject authentication, Certificate issuance, Certificate revocation, audit and archival.

5.1 Physical security controls

5.1.1 Site location and construction

NotarisID has multiple physical sites:

- Office located in Amsterdam, the Netherlands.
- One datacentre in Amsterdam, the Netherlands.
- One datacentre in Enschede, the Netherlands.

NotarisID is based in a shared office building in Amsterdam. This office has a lockable door, the keys of which are kept by NotarisID. Access cards are issued to authorized personnel and contractors. NotarisID does not use safes at the office location, it rented safes from a professional safe provider in Rotterdam.

NotarisID uses two fully-managed datacentres from a leading global datacentre provider. These datacentres are set up in a redundant way and are both located in the Netherlands at a distance of more than 100 kilometres apart. The high secure zones of NotarisID are located in these datacentres. The cages in which the cabinets are placed (in which the equipment of NotarisID is located), are lockable.

5.1.2 Physical access

Access to the office:

- Security badges or physical keys are used to get access to the NotarisID corporate office facilities.
- Any lost or stolen badges or keys must be immediately reported to the security officer of NotarisID, so that security badges can be blocked and/or locks be changed.
- All entry/exit points of the NotarisID corporate office spaces are secured with locks.
- The NotarisID corporate office spaces are only accessible with the specific keys.
- A current list of personnel having a key of the NotarisID corporate office is maintained at all times.
- All individual access is verified before granting access to the office space.
- NotarisID only issues authorized credentials to outside vendors after the outside vendor has been properly screened.

Access to the datacentres:

- Authorization to visit the data centre is only given based on the task the employee has to complete.
- No one is assigned continuous authorization to visit the datacentre.
- Working visits to the datacentre have to be approved by the IDNH COO or IT Infra & Ops manager. The approval is given through the customer portal of datacentre provider. Included in this approval are the specific names of the visitors and a description of predefined task/role.
- Visitors are required to identify themselves using a valid identification mean.
- The physical cage is only opened and closed when authorized by the IDNH COO or IT Infra & Operations manager.
- Visitors must adhere to the rules on access to and behaviour of the datacentre provider at the datacentre.
- Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area.
- Every entry and exit to the datacentre and cage shall be logged.

Physical security datacentres:

- Parking areas are kept at a distance of at least 10 metres from the building and use adequate bollards to maximize the amount of standoff distance to the extent possible.
- Parking under the facility is prohibited.
- All vehicles entering controlled parking areas are registered.
- Security guardhouse is equipped with all necessary equipment to allow monitoring of physical security systems including alarms and CCTV.
- The security displays (CCTV & alarms) cannot be visually monitored from outside the guardhouse.
- Guards in the main guardhouse are provided with external communications. They are also provided with redundant security controls, which ensure the availability at all times regardless of an emergency.
- Access to the security guardhouse is controlled by the electronic access control system and mantrap.
- 24/7 On-site security guards are required for the common areas of all leased facilities when the building is accessible.
- Access to the facility is provided with manned reception area Mon-Fri, 8h00-18h00.
- Access to the facility is provided with manned reception area 24 x 7 x 365.
- A secured area is provided for the secure storing of materials delivered to site.
- Secure delivery and loading areas when not in use and monitor while in use.
- The exterior of the building and building perimeter is monitored including parking areas with CCTV cameras.
- All building and room entrances are monitored with CCTV cameras with sufficient clarity to monitor individuals.
- Recording capability on all CCTV systems is included. At a minimum, record movement for twenty days at 10 fps, 4 CIFs for resolution.
- Evidence/history is provided in case of security incidents in or around the facility.

- A general purpose perimeter fence is installed (according to BS 1722-14:2001 Category 1) with a height of min. two (2) metres above ground level with intrusion detection implemented on the fence
- Adequate lighting (either motion activated or permanent lights) of walking areas, entrances, gates, and parking areas and the perimeter is provided to allow guard monitoring and CCTV recording.
- Emergency lighting and emergency is provided as per local regulations.
- Construct building exterior doors and windows resist forced entry into the building, in accordance with EN 1627 class RC4 or US ASTM F1233 class 4 DOS SD-STD-01.01 (five (5) minutes resistance) or equivalent.
- There are use glass break alarms to monitor building exterior glazing.
- Air intakes are protected from access by unauthorized individuals by locating them high above ground level or in areas not accessible by aggressors.
- Power and telecommunications cabling located in common areas are protected from data interception, data corruption or sabotage.
- Facilities and secure areas are protected with appropriate entry/access controls (a combination of technical, procedural, and physical safeguards ensuring that only authorized personnel are allowed access).
- Intrusion detection is integrated to allow for detection at the earliest opportunity.
- The system is divided into a sufficient number of security zones to allow for quick viewing via CCTV and physical response.
- Security equipment is protected with a UPS system and a backup generator.
- Security equipment is configured to automatically restart after a power interruption, in order to reactivate all default applications
- Electronic access control system is used to access the facility and private areas.
- Electronic access control system with at least one form of dual authentication (pin code, biometric) is used to access to secure areas.
- All visitors verifying their identity using a government-issued identity document and provide visitor badges with limited access to required areas only, are registered, auto-expiring after maximum one (1) day.
- Access to secure areas is restricted to authorized staff and contractors with a legitimate business need.
- Access records and access control system logs are maintained for investigation and audit purposes.
- Computer equipment in secure are installed in private areas only, protected with electronic access control system.
- Secure area walls are built slab-to-slab, continuing above-ceiling and under-floor separating the area from any adjacent occupants.
- All doors leading into secure areas are equipped with automatic door closures and door alarms.
- It is mandatory for every person who enters a secure area cage, to badge at the badge reader to enter and to exit.
- For facilities with physical keys in use, it is ensured that a manual or electronic key control system is in place that includes an audit ability.

5.1.3 Power and air conditioning

The datacentres have:

- an emergency power generator system with an autonomy of at least 24 hours.
- a redundant battery backup system.
- a redundant power distribution system.
- a concurrently maintainable power provisioning system.
- a redundant cooling system.
- a concurrently maintainable cooling system.

5.1.4 Water exposures

The datacentres have:

- an environmental monitoring system.
- a humidity control system.

5.1.5 Fire prevention

The datacentres have:

- a fire protection system.
- a high sensitivity fire detection system (type ‘VESDA’ or equivalent).
- a gas-based fire extinguishing system.
- a redundant network connection (external connection as well as internal distribution).

5.1.6 Media storage

The only media NotarisID possesses, are WORM SD-cards to record important acts and/or ceremonies and non-provisioned (empty) USB-tokens. Those are stored in a safe. Please refer to paragraph 5.1.1 of this CP/CPS.

NotarisID uses external datacenter (business cloud) for storage of information assets (please refer to paragraph 5.1.1). No other information carrying assets are located at the NotarisID enclosed corporate office spaces besides the devices that employees and external bring themselves.

5.1.7 Waste disposal

- NotarisID's information and asset carriers of information is valuable and must be protected accordingly and securely be disposed of or destructed when required in line with applicable laws and regulations.
- Assets containing sensitive information are disposed and destructed in a secure manner in line with its classification to prevent against illegal retention of information and unauthorized access to the information.
- A systematic approach to information security is implemented to identify NotarisID needs. Identified risks are addressed according to the risk assessment methodology to ensure that sufficient mitigating controls are in place considering the nature of the service or product delivered.
- NotarisID designed and implemented secure disposal and destruction controls.
- Disposal of sensitive items are logged to maintain an audit trail.
- Media containing confidential information is disposed of securely e.g., by incineration or shredding. Or the information is destroyed, deleted, or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function, or erasure of data for use by another application.
- Destruction of NotarisID owned media, both digital and non-digital, is carried out by a qualified party.
- For the deletion and disposal of assets that are owned by suppliers, the appropriate contractual provisions concerning end of contract shall be agreed upon between parties and specifically documented.

5.1.8 Off-site backup

Backups are stored off-site via a remote backup service to ensure critical data can be restored in case of a disaster, accidental error or system crash.

5.2 Procedural controls

5.2.1 Trusted roles

NotarisID staff members are assigned various trusted roles with corresponding responsibilities. Their authorizations correspond to their roles. Roles include:

a) Security officers: person overseeing that established security guidelines are implemented and observed.
b) System auditors: person having a supervising role and assessing independently how business processes are arranged/organized and to what extent reliability requirements are met.

c) System administrators: person administering the NotarisID systems, including installation, configuration, and maintenance of the systems.
d) System operators: person responsible for the daily management of the NotarisID-systems.
e) Registration Officer (RO): an individual or organisation responsible for verifying, based on a Notary Deed, that identity proofing and registration of the Applicant has been done allowing for Certificate issuance.
f) Revocation officer: person responsible for operating Certificate status changes (including preparation of revocation requests and revocation of Certificates).
g) Provisioning officer: person responsible for provisioning letter with username/password of USB-token and revocation code to subscriber.
h) Key custodian: manages CA cryptographic key material, together with other key custodians.
i) Crypto manager: manages and determine all cryptographic devices and algorithms.

5.2.2 Number of persons required per task

- There is one (1) security officer, with one (1) back up security officer.
- There is (at least) one (1) system auditor.
- There (at least) two system administrators.
- There (at least) two system operators.
- There is one (1) registration officer, with one (1) backup registration officer.
- There is one (1) revocation officer, with one (1) backup revocation officer.
- There is one (1) provisioning officer, with one (1) backup provisioning officer.
- There are three (3) key custodians.
- There is (at least) one crypto manger.

Remarks regarding compatibility of Trusted Roles:

- NotarisID deems the roles of Registration Officer and revocation officer compatible. Those roles are vested in one (1) Trusted Staff Member.
- The roles of provisioning officer and Registration Officer are not deemed compatible by NotarisID, and are therefore always separated.
- Any Trusted Staff Member can be a key custodian, provided there are at least three (3) key custodians.
- The system auditor serves as backup security officer (in case the first security officer is not or temporary unavailable).

5.2.3 Identification and authentication for each role

No stipulation

5.2.4 Roles requiring separation of duties

Please refer to paragraph 5.2.2 of this CP/CPS.

5.3 Personnel security controls

5.3.1 Qualifications, experience, and clearance requirements

NotarisID ensures that all personnel are competent to perform the required tasks. Personnel are hired or contracted based on skills, competencies, and certifications appropriate to the position, and additional training is provided as needs arise. Training records for employees are maintained by the HR department.

5.3.2 Background check procedures

Personnel is screened before entering service with NotarisID. NotarisID uses two screening levels. One for Trusted Staff Members. And one for other staff members of NotarisID.

	Trusted Staff Member	**Other staff members of NotarisID**
Request and check resumes and degrees.	☑	☑
Request and check references.	☑	☑
General search internet.	☑	☑
Certificate of good conduct. ("VOG")	☑ *(profile legal = 55)*[5]	☑ *(profile legal = 55, or any other profile that fits the function)*
Financial check.	☑	☒
Self-certification ("eigen verklaring") *(including statement regarding impartiality and integrity)*	☑	☒

Please refer to paragraph 5.3.7 for contractors and other vendors, which puts staff at the disposal of NotarisID.

[5] Since the concept of electronic signatures is a legal construct, and since the Registration Officer uses the help of Appointed Notary for Identity Proofing, NotarisID deems the profile "legal" ("Juridisch") the most fitting.

5.3.3 Training requirements

Personnel have sufficient knowledge and expertise to fulfil their tasks within NotarisID. NotarisID ensures that they are trained in company-specific procedures.

5.3.4 Retraining frequency and requirements

Regular retraining is performed. Training records for employees are maintained by Human Resources (HR) of NotarisID.

5.3.5 Job rotation frequency and sequence

No stipulation.

(NotarisID does not have a policy regarding frequency and sequence)

5.3.6 Sanctions for unauthorized actions

Unpermitted actions by organisation members may lead to disciplinary measures by the CEO or COO of NotarisID. Additionally, in case an employee does not adhere to the policies and procedures, the CEO or COO can decide to revoke access rights and/or terminate the appointment as Trusted Staff Member.

5.3.7 Independent contractor requirements

For contractors (“ZZP-ers”) the same applies as stated in paragraphs 5.3.1 to 5.3.6 and 5.3.8 (*mutatis mutandis*) of this CP/CPS. For staff members which are put at the disposal of NotarisID (for example secondment or system administrators as a result of outsourcing system administration), NotarisID relies on the vetting procedure of the vendor, provided that NotarisID has determined that the vetting procedure is adequate, i.e. at least not less restrictive than its own vetting procedure. The adequacy decision is recorded, and the vendor agrees that the aforementioned vetting procedure is followed.

Appointment as a Trusted Staff Member (and termination) is always done by NotarisID, regardless which vetting procedure is used (own or vendor).

5.3.8 Documentation supplied to personnel

All employees are provided with a contract of employment, a defined job role / function, and personnel handbook. Collectively these documents provide necessary information regarding role, rights, laws and procedures pertaining to employment at NotarisID.

5.4 Audit logging procedures

5.4.1 Types of events recorded

NotarisID security logging:

- Authentication and actions of authorized users, system access, access to files, access to data in databases and use of online systems.
- Authentication and actions of system administrators, such as use of technical management functions, changes of configurations or settings, execution of system commands, start and stop, execution of a backup or restore.
- All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.
- Actions in the context of system security, such as entering and removing users, granting and revoking rights, resetting passwords, issuing and revoking cryptographic keys.
- Security incidents such as the presence of malware, vulnerability testing, failed login attempts, authorization violations, denied access attempts, use of non-operational system services, starting and stopping security services.

NotarisID system operations logging:

- Use of functional management functions, such as changes to configurations and settings, release of new functionalities, interventions in data sets (including databases).
- Online sessions. The following is logged: session start, authentication, date and time, calling and sending system and process.
- Check on the storage of the logs: when the storage medium for the log files overflows above a certain limit, it is logged and leads to automatic alerts for the management organization (= see also capacity management). This also applies if it is no longer possible to store log data (for example: a log server that is not available).
- Initiation and stoppage of systems and system processes. For example, when a system component stops running.

NotarisID records the following TSP events:

- All events related to registration including requests for a Certificate shall be logged.
- All registration information including the following shall be recorded:
    - type of document(s) presented by the applicant to support registration;
    - record of unique identification data, numbers, or a combination thereof (e.g. Applicant's identity card or passport) of identification documents, if applicable;
    - storage location of copies of applications and copies of Notary Deeds;
- NotarisID shall log all events relating to the life-cycle of CA keys.
- NotarisID shall log all events relating to the life-cycle of Certificates.
- NotarisID shall log all requests and reports relating to revocation, as well as the resulting action.
- NotarisID shall record all relevant information concerning data issued and received and shall log all events relating to the Certificate registration, generation, USB-token preparation and when applicable, revocation management.

A log line contains at least:

- A username or ID that can be traced back to a natural person.
- The event.
- Where possible, the identity of the workstation or site:
    - Host name.
    - Operating System (OS).
    - Name of the application.
    - IP address(es).
    - Location(s).
    - The object on which the action was performed.
- If relevant, the result of the action.
- The date and time of the event.

5.4.2 Frequency of processing log

Audit logs are processed following previously mentioned events. Logs are provided with a timestamp using a clock that is synchronized at least once a day with a trusted time source.

5.4.3 Retention period for audit log

Type	**Retention**
NotarisID security logging	Two (2) years.
NotarisID system operations logging	Two (2) years.
Logging TSP events	Seven (7) years after any Certificate based on these records ceases to be valid.

5.4.4 Protection of audit log

Audit logs are protected and the integrity is ensured. In case parts of the audit log files must be retrieved, four eyes principle is used.

Please refer to paragraph 9.4.6 of this CP/CPS for demands.

5.4.5 Audit log backup procedures

Incremental backups of audit logs are created daily, in an automated way, complete backups are created on a thirty (30) day basis and are also archived at a remote location.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

(NotarisID does not notify subscriber)

5.4.8 Vulnerability assessments

The audit log and components supporting the audit log are in scope of the NotarisID vulnerability management policy and procedures.

5.5 Records archival

5.5.1 Types of records archived

NotarisID records all relevant registration information, including at least:

- the certificate application form.
- the findings and decision on the application.
- the identity of the Registration Officer who processed or approved the Certificate application.
- proof of identification (copy of Notary Deed).
- information (of third parties) which lead to revocation.

- the signed Notary Appointment Agreements.

5.5.2 Retention period for archive

NotarisID retains all relevant documentation and information, relating to a Certificate during its term of validity and for a period of at least seven (7) years from the date of expiry of the Certificate.

5.5.3 Protection of archive

Archives are secured against unauthorized access and are, as a rule, accessible only for management, Trusted Staff Members and internal and external auditors. These may, however, grant access to (part) of the archives to others, if, and only if, those others need this for their tasks. Trusted Stuff Members only have access to parts of the archives, which are necessary to perform their duties. For instance, the Registration Officer has access to the archive containing information regarding application and identity proofing, and the revocation officer has access to the archive containing revocation information.

Archives are secured against modification and deletion. To this end, both organizational and technical controls are in place. Archives are also protected against storage media deterioration. The archives (in case of NotarisID, i.e. long term storage) are stored on monitored, redundant hard disks with a sufficient RAID configuration.

5.5.4 Archive backup procedures

The entire archive is backed up off-site.

5.5.5 Requirements for timestamping of records

Records are provided with a timestamp using a clock that is synchronized with UTC at least once a day. System clocks are configured to map to centralized and managed time servers. Privileged administrators only have access to configure authoritative time data on any system component.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Upon first request of a Subscriber (parts of) records concerning the operation of services shall be made available, if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings. NotarisID will ensure the identity of the requesting Subscriber, prior to making available the (parts of) records.

5.6 Key changeover

No stipulation.

(NotarisID does not support key changeover)

5.7 Compromise and disaster recovery

NotarisID has a business continuity plan to ensure continuity when a disaster occurs. The aim of the plan is to ensure the orderly recovery of business operations, communication to Subscribers and Relying Parties, and continuity of services for the Subscriber affected. The business continuity plan is a confidential document.

5.7.1 Incident and compromise handling procedures

NotarisID has processes in place for handling (security) incidents. NotarisID has a communication plan in place designed to notify the Dutch Telecom Authority (Rijksinspectie Digitale Infrastructuur), National Cyber Security Centre (if necessary), Dutch Data Protection Authority, suppliers, Subscribers and Relying Parties in the event of a disaster, security compromise, or business failure. NotarisID annually tests, reviews, and updates these procedures.

5.7.2 Computing resources, software, and/or data are corrupted

No stipulation.

5.7.3 Private Key compromise procedures

For NotarisID Private Keys, key generation and dissemination procedures are in place. The Certificate corresponding to the compromised key will be revoked. A new key ceremony is planned and executed.

For Subscriber Private Keys, the enrolment procedure will be used to replace a compromised Private Key. The Certificate corresponding to the compromised key will be revoked.

5.7.4 Business continuity capabilities after a disaster

NotarisID has a Business Continuity Plan in place describing the measures to prevent a disruptive incident or disaster from occurring. Would such an event take place the measures and services to return to the default situation are described.

5.8 CA or RA termination

If NotarisID decides to terminate the certification service delivery. The termination will be done in accordance with a controlled process as further described in its termination plan. The activities that are carried out during the termination depend on whether is voluntary or involuntary.

Parts of the plan upon termination include:

- stop issuing new Certificates immediately.
- maintain the revocation status service (CRL only) for up to six (6) months after the expiry date of the last Certificate issued has expired or has been terminated by revocation.
- destroy or permanently deactivate all Private Keys used for the service provision in question and permanently destroy all Private Keys used for that purpose.
- termination and destruction of systems, procedures and non-relevant data.
- an inventory of the data to be retained, which is necessary in order to provide legal proof of certification.
- Realisation of provisions relating to the transfer of the obligations to other Trust Service Providers, insofar as this is reasonably possible.[6]
- Keep the Document Repository, including the CA certificate, up for at least six (6) months after the expiry date of the last Certificate issued has expired or has been terminated by revocation.
- Use of the communication plan in place designed to notify the Dutch Telecom Authority (Rijksinspectie Digitale Infrastructuur), suppliers, Subscribers and Relying Parties in the event of termination.
- Revocation of all Certificates.
- Revocation of NotarisID Root CA Certificate.
- Revocation of NotarisID Subscriber Issuing CA Certificate.
- Archiving validation files, for seven (7) years.
- Placing a notice in Document Repository regarding (involuntary) termination.
- Placing notices on top of every document part of the Document Repository family regarding (involuntary) termination.

[6] Since the Certificates are valid for one (1) year, a transfer to another (Q)TSP is unlikely.

- Remove Middleware Software from Document Repository.

The termination plan is revised annually for as long as NotarisID remains active.

Prior to termination of the Trust Service, NotarisID undertakes reasonable efforts to transfer obligations and/or documentation to a third party. The following requirements apply for the third party:

#	REQUIREMENT	MUST HAVE OR NICE TO HAVE
1	The third party must be a (Q)TSP	**Should have**
2	The third party is willing to offer Subscribers a new certificate (issued by that third party in case it is a (Q)TSP).	**Nice to have**
3	The third party must host the Document Repository for at least six (6) months after termination. Including Root Certificate.	**Must have**
4	The third party must archive the TSP event log and/or other company documentation for at least seven (7) years after termination.	**Must have**
5	The third party must keep the (frozen) CRL available for at least six (6) months after termination.	**Must have**
6	The third party has a customer service in place for questions of Subscribers or Relying Parties, for at least one (1) year after termination. This includes following up questions regarding evidence for legal proceedings[7].	**Must have**
7	The third party must understand information security and should have an Information Security Management System in accordance with ISO 27001. Since the documents and/or information it receives should be only made accessible to staff members on a need to know basis and/or authorization scheme / matrix.	**Must have**

In case no third party can be found that meets the requirements, obligations and documentation is transferred to the Dutch limited liability company “PWF Diensten B.V.”, hereafter “PWFD”, a subsidiary of the parent company of NotarisID B.V. PWFD is able to comply with requirements 3 to 7 (free of charge – since it fits in its regular course of business).

[7] In the general terms and conditions of NotarisID is stipulated that the statute of limitations regarding claims is limited to one (1) year. That is the minimum that can be agreed upon with a consumer according to the Dutch Civil Code.

However, in case of a scheduled termination, NotarisID will plan termination in such a manner, that in case a termination decision was made by management of NotarisID, it will keep operation going (except for issuing new Certificates) for at least one (1) year, since a Certificate is valid for one (1) year.

5.8.1 Voluntary termination

NotarisID deems the following events, voluntary termination:

- Shareholders terminate NotarisID.
- NotarisID decides to terminate itself, by its own accord.

See paragraph 5.8 of this CP/CPS for termination plan.

5.8.2 Involuntary termination

NotarisID deems the following events, involuntary termination:

- Suspension of payments.
- Bankruptcy.
- Dutch Telecom Authority revokes qualified status.
- Major security incident that leads to not being a trustworthy (Q)TSP (anymore).

See paragraph 5.8 of this CP/CPS for termination plan.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 The CA key pair

The key pair of NotarisID (CA key pair) is generated (once) in a cryptographic module (HSM). The Public Key of NotarisID is transferred to a signing process in the form of a certificate signing request (CSR), the request is self-signed electronically by NotarisID. The HSM is configured in such a way that the root CA key pair can be used only under dual control by authorized, trusted personnel. The process to generate the key pair of NotarisID and the accompanying CA certificate, is called the key ceremony, for which a policy is in place. This process is done twice. Once for the generation of the NotarisID Root CA key pair, and once for the generation of the NotarisID Subscriber Issuing CA key pair.

The process is captured and a report is drawn up, and signed by the security officer of NotarisID and an independent third party, for example an auditor.

6.1.1.2 The Subscriber key pair.

The key pair for the Subscriber is generated by NotarisID within the USB-token (to be issued to Subscriber). The Public Key is transferred to a signing process in the form of a certificate signing request (CSR). The request is signed electronically by NotarisID, with the Private Key that is linked to the NotarisID Subscriber Issuing CA Certificate as described in paragraph 6.1.1.1 of this CP/CPS. This process is called Certificate generation. During this process the private key of Subscriber does not leave the USB-token.

NotarisID does not accept a CSR from Subscriber.

The Subscriber key pair is only generated after the Registration Officer approved the application of Applicant.

6.1.2 Private Key delivery to Subscriber

The Certificate is placed in the USB-token after Certificate Generation. The Registration Officer contacts the Subscriber for an appointment, since the Registration Officer will deliver the USB-token at the address of the Subscriber. Once the Registration Officer is at the agreed upon address of Subscriber, Subscribers must be able to show an official Dutch identity document, as mentioned in paragraph 3.2.3 of this CP/CPS. In addition an official Dutch Driver's license is also allowed. The Registration officer checks the identity

document, and records the type of document and document number. Before handing over the USB-token, Subscriber must sign a statement, stating that Subscriber received the USB-token.
The Registration officer will archive the statement at the office of NotarisID.

The provisioning officer prepares and sends a letter (by snail mail – to the address Registration Officer visited) to Subscriber with the instructions for activation accompanied with the initial pin of the USB-token, which is needed to set a pin desired by Subscriber.

Both the USB-token and the PIN letter are delivered to the address of Subscriber. That is the address that the notary mentioned in the Notary Deed. In case the address on the identity document differs from the address mentioned in the Notary Deed, the address in the Notary Deed prevails (since the address on the identity document, may be an old address).

6.1.3 Public Key delivery to Certificate issuer

No stipulation.

(The Public Key itself is not delivered to Subscriber, since the Public Key resides in the Certificate)

6.1.4 CA Public Key delivery to Relying Parties

No stipulation.

(The Public Key of NotarisID is not delivered, only the CA certificate (in which the Public Key of NotarisID resides) is made available)

6.1.5 Key sizes

NotarisID uses a key size of 2048 for Subscriber Certificates. NotarisID uses a key size of 4096 for NotarisID Root CA Certificates. NotarisID uses a key size of 4096 for NotarisID Subscriber Issuing CA Ccertificates. For all aforementioned certificates SHA-512 with RSA encryption is used for generation of key pairs.

6.1.6 Public Key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Please refer to paragraph 1.4.1 of this CP/CPS.

6.2 Private Key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The key pairs for NotarisID itself are generated within a cryptographic module (HSM).
The HSM's are FIPS 140-2 level 3 certified. The HSM's run in FIPS mode.

The key pair for a Subscriber is safely generated inside the QSCD. The QSCD (in the form and shape of a USB-token) is Common Criteria certified.

The certifications of the HSM's and used QSCD are checked yearly by NotarisID. NotarisID does not issue a Subscriber Certificate in case the validity of the QSCD certification is less than a year.

6.2.2 Private Key (n out of m) multi-person control

All operations performed on the cryptographic module regarding the Private Key of NotarisID are under at least dual control.

All operations performed on the cryptographic module regarding the Private Key of Subscriber are performed by the Registration Officer.

6.2.3 Private Key escrow

No stipulation.

(NotarisID does not support key escrow)

6.2.4 Private Key backup

The Private Key of NotarisID is backed up by authorised personnel within strict procedures onto multiple smart cards, which are stored in a safe.

The Private Key of Subscriber is not stored, since it is placed onto the USB-token.

6.2.5 Private Key archival

No stipulation.

(NotarisID does not support Private Key archival)

6.2.6 Private Key transfer into or from a cryptographic module

Please refer to paragraph 6.2.4 of this CP/CPS.

6.2.7 Private Key storage on cryptographic module

Please refer to paragraph 6.2.8 of this CP/CPS.

6.2.8 Method of activating Private Key

No Stipulation.

(Activation of Private Key of NotarisID is done through key ceremony procedure(s), activation of Private Key of Subscriber, is done by Subscriber using the USB-token)

6.2.9 Method of deactivating Private Key

No stipulation.

6.2.10 Method of destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

Please refer to paragraph 6.2.1 of this CP/CPS.

6.3 Other aspects of key pair management

6.3.1 Public Key archival

Public Keys of NotarisID are archived by the NotarisID and stored in a physically secure environment for at least seven (7) years, following the end of the period of validity of the associated certificates.

6.3.2 Certificate operational periods and key pair usage periods

Certificates can never be valid for a longer time than the Subscriber Issuing CA Certificate. The Subscriber Issuing CA Certificate can never be valid for a longer time than the Root CA Certificate. Therefore, it is NotarisID's policy to renew the Root CA Certificate and/or the Subscriber Issuing CA Certificate as soon as their expiration date is less than two (2) years away, ensuring a minimum validity of one (1) year for Subscriber Certificates.

6.4 Activation data

6.4.1 Activation data generation and installation

Please refer to paragraph 6.1.2 of this CP/CPS.

6.4.2 Activation data protection

The letter including the initial pin as mentioned in paragraph 6.1.2 of this CP/CPS, is created by a provisioning officer. Other staff members of NotarisID do not have access to the letter and pin. After Subscriber received the USB-token and (later) the letter including the pin, it is the obligation of Subscriber to change the pin to a Subscriber desired pin.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

NotarisID has a substantial number of security controls in place, covering, inter alia:

- Access Control.
- Cryptography.
- Physical and Environmental Security.
- Operations Security.
- Change management, capacity management and configuration management.
- Logging and monitoring.
- Vulnerability management and anti-malware protection.
- Communications Security.
- System Acquisition, Development and Maintenance.
- Information Security Incident Management.
- Information Security Aspects of Business Continuity Management.

The information security policy of NotarisID and its Information Security Management System (ISMS) is based on ISO 27001:2013. NotarisID is ISO 27001:2013 certified, and maintains its certification.

The configuration of the NotarisID systems is regularly checked for changes, which can potentially violate the security policy or the ISMS of NotarisID. This is done quarterly. The maximum interval between two (2) checks is therefore half a year.

6.5.2 Computer security rating

NotarisID classifies the resources used based on a risk assessment

6.6 Life cycle technical controls

6.6.1 System development controls

Please refer to paragraph 6.5.1 of this CP/CPS.

6.6.2 Security management controls

Please refer to paragraph 6.5.1 of this CP/CPS.

6.6.3 Life cycle security controls

Please refer to paragraph 6.5.1 of this CP/CPS.

6.7 Network security controls

Please refer to section 6.5.1

6.8 Timestamping

No stipulation

(NotarisID does not issue Certificates which can be used for validating timestamps)

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profiles

7.1.1 Certificate Profile NotarisID Root CA

The NotarisID Root CA certificate has the following profile:

	Attribute	Value	Critical	Coding
tbsCertificate	Version	2 (V3)		Integer
	Serial number	Unique number generated by CA, length 20 octets		Integer
	Signature algorithm	1.2.840.113549.1.1.13 (sha512WithRSA)		OID
	Issuer	2.5.4.3 (CN) = NotarisID Root CA 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL		UTF8String UTF8String PrintableString
	Valid from	yyyy.mm.dd HH:MM:SS (Date and time of creation of Certificate)		UTCTime
	Valid to	yyyy.mm.dd HH:MM:SS (“Valid from: + 15 years)		UTCTime
	Subject	2.5.4.3 (CN) = NotarisID Root CA 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL		UTF8String UTF8String PrintableString
	Subject Public Key Info	1.2.840.113549.1.1.1 (rsaEncryption) Public Key		OID Integer
	Standard Extensions:			
	2.5.29.19 Basic Constraints	True (CA) (pathLenConstraint = none)	Yes	BOOLEAN -
	2.5.29.15 Key Usage	5 (keyCertSign) 6 (crlSign)	Yes	BIT_STRING
	2.5.29.14 Subject Key Identifier	SHA-1 hash of Subscriber’s Public Key		OCTET_STRING
signatureAlgorithm		1.2.840.113549.1.1.13 (sha512RSA)		OID
signatureValue		Electronic signature computed upon the ASN.1 DER encoded tbsCertficate		BIT_STRING

7.1.2 Certificate Profile NotarisID Subscriber CA

The NotarisID Subscriber CA certificate has the following profile:

	Attribute	Value	Crit.	Coding
tbsCertificate	Version	2 (V3)		Integer
	Serial number	Unique number generated by issuing CA, length 160 bits (20 octets)		Integer
	Signature algorithm	1.2.840.113549.1.1.13 (sha512WithRSA)		OID
	Issuer	2.5.4.3 (CN) = NotarisID Root CA 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL		UTF8String UTF8String PrintableString
	Valid from	yyyy.mm.dd HH:MM:SS (Date and time of creation of Certificate)		UTCTime
	Valid to	yyyy.mm.dd HH:MM:SS (“Valid from: + 10 years)		UTCTime
	Subject	2.5.4.3 (CN) = NotarisID Subscriber CA 2.5.4.97 (organizationIdentifier) = NTRNL-76121526 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL		UTF8String UTF8String UTF8String PrintableString
	Subject Public Key Info	1.2.840.113549.1.1.1 (rsaEncryption) Public Key		OID Integer
	Standard Extensions:			
	2.5.29.35 Authority Key Identifier	Value of the “Subject Key Identifier” of de issuer CA		OCTET_STRING
	2.5.29.14 Subject Key Identifier	SHA-1 hash of Subscriber’s Public Key		OCTET_STRING
	2.5.29.1 Key Usage	5 (keyCertSign) 6 (crlSign)	Yes	BIT_STRING

	Attribute	Value	Crit.	Coding
	2.5.29.32 Certificate Policies	2.5.29.32.0 (anyPolicy) 1.3.6.1.5.5.7.2.1 (PolicyQualifierId)=https://pub-notarisid.nl/shared/static/6em0fb8kzojw6q3kkkk5zf9ucrqc3jzi.pdf		OID OID IA5String
	2.5.29.19 Basic Constraints	True (CA) pathLenConstraint = 0	Yes	BOOLEAN INTEGER
	2.5.29.37 Enhanced Key Usage			
	2.5.29.31 CRL Distribution Points	https://pub-notarisid.nl/shared/static/7737lx8r5lb0m8n0bjtuhzpu60ff1j7j.crl		OCTET_STRIN G
	Private Internet Extensions:			
	1.3.6.1.5.5.7.1.1 Authority Information Access	1.3.6.1.5.5.7.48.2 (accessMethod) = https://pub-notarisid.nl/shared/static/s0i2xxy9vvjwwcqfvnwc9howms1w5qgx.cer		OID OCTET_STRIN G
signatureAlgorithm		1.2.840.113549.1.1.13 (sha512RSA)		OID
signatureValue		Electronic signature computed upon the ASN.1 DER encoded tbsCertficate		BIT_STRING

7.1.3 Certificate Profile NotarisID Subscriber Certificate

The NotarisID Subscriber Certificate has the following profile:

	Attribute	Value	Crit.	Coding
tbsCertificate	Version	2 (V3)		Integer
	Serial number	Unique number generated by issuing CA, length 160 bits (20 octets)		Integer
	Signature algorithm	1.2.840.113549.1.1.13 (sha512WithRSA)		OID
	Issuer	2.5.4.3 (CN) = NotarisID Subscriber CA 2.5.4.97 (organizationIdentifier) = NTRNL-76121526 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL		UTF8String UTF8String UTF8String PrintableString

	Attribute	Value	Crit.	Coding
	Valid from	yyyy.mm.dd HH:MM:SS (Date and time of creation of Certificate)		UTCTime
	Valid to	yyyy.mm.dd HH:MM:SS (“Valid from: + 1 years)		UTCTime
	Subject	2.5.4.3 (CN) = <given names> [<prefix>] <surname> 2.5.4.42 (GN) = <given names> 2.5.4.4 (SN) = [<prefix>] <Surname> 2.5.4.5 (SERIALNUMBER) = <UUID> 2.5.4.6 (C) = NL		UTF8String UTF8String PrintableString
	Subject Public Key Info	1.2.840.113549.1.1.1 (rsaEncryption) Public Key		OID Integer
	Standard Extensions:			
	2.5.29.35 Authority Key Identifier	Value of the “Subject Key Identifier” of de issuing CA (NotarisID Subscriber CA)		CONTEXT_SP
	2.5.29.14 Subject Key Identifier	SHA-1 hash of Subscriber’s Public Key		OCTET_STRING
	2.5.29.15 Key Usage	40 (Non-Repudiation)	Yes	BIT_STRING
	2.5.29.32 Certificate Policies	0.4.0.194121.1.2 (qcp-natural-qscd 1.3.6.1.5.5.7.2.1 (CPS) = https://pub-notarisid.nl/shared/static/6em0fb8kzojw6q3kkkk5zf9ucrqc3jzi.pdf 1.3.6.1.5.5.7.2.2 (User Notice) = “Op dit certificaat is het CP/CPS van NotarisID B.V. van toepassing. Deze kan worden geraadpleegd op https://pub-notarisid.nl/shared/static/6em0fb8kzojw6q3kkkk5zf9ucrqc3jzi.pdf”		OID OID IA5String OID UTF8String
	2.5.29.17 Subject Alternative Name			OID CONTEXT_SP
	2.5.29.19 Basic constraints	False (End Entity) pathLenConstraint = None	Yes	BOOLEAN INTEGER
	2.5.29.37 Enhanced Key Usage	1.3.6.1.5.5.7.3.4 (Email Protection) 1.3.6.1.4.1.311.10.3.12 (Document Signing)		OID OID

	Attribute	Value	Crit.	Coding
	2.5.29.31 CRL Distribution Points	https://pub-notarisid.nl/shared/static/mnzoa8wotl29kedhs9lwo0fl1knf2wr3.crl		OCTET_STRING
	1.3.6.1.5.5.7.1.3 Qualified Certificate Statements	0.4.0.1862.1.1 (European Qualified Certificate) 0.4.0.1862.1.2 (limit value) = 250.000 0.4.0.1862.1.4 (Secure Signature Creation Device Qualified Certificate) 0.4.0.1862.1.6 (QcType) 0.4.0.1862.1.6.1 (esign) 0.4.0.1862.1.5 (OcPDS) https://pub-notarisid.nl/shared/static/jbuvuj5yu39m3pjwe6l8edus0iz9dv6q.pdf		OID OID OID OID OID IA5String PrintableString
	Private Internet Extensions:			
	1.3.6.1.5.5.7.1.1 Authority Information Access	1.3.6.1.5.5.7.48.2 (accessMethod=Certification Authority Issuer) = https://pub-notarisid.nl/shared/static/zntt6uz2gt9q1u5a8m1vmj517j5hqpsx.cer		OID CONTEXT_SP
signatureAlgorithm		1.2.840.113549.1.1.13 (sha512RSA)		OID
signatureValue		Electronic signature computed upon the ASN.1 DER encoded tbsCertficate		BIT_STRING

7.1.4 Certificate Profile NotarisID Subscriber Certificate for check or test purposes

There is no profile for test certificates, since NotarisID does not issue test certificates using the production environment. Upon first request of a third party, NotarisID shall provide that third party with a NotarisID Subscriber Certificate for check and test purposes which is issued using a test or an acceptance environment.

In case the aforementioned third party is only able to test with a Certificate issued using the production environment of NotarisID, a Certificate is issued in conformity with all applicable NotarisID policies and procedures. This means that a staff member of NotarisID or a staff member of the aforementioned third party must apply for the registration and undergo the identity proofing procedure as set herein. In case a staff member of NotarisID is the applicant, the staff member should not have a Trusted Role and should not be a Subscriber (already). In case a staff member of NotarisID is the applicant, the Third Party must enter into an NDA regarding the use of the Certificate. The end result is a valid Certificate, and does therefore not bare any markings and/or signs stating it is a test Certificate or specimen Certificate.

7.2 CRL profiles

The NotarisID CRL has the following profile:

	Attribute	Value		Crit.	Coding
tbsCertificate	Version	2 (V3)			Integer
	Signature algorithm	1.2.840.113549.1.1.13 (sha512WithRSA)			OID
	Issuer	2.5.4.3 (CN) = NotarisID Subscriber CA 2.5.4.97 (organizationIdentifier) = NTRNL-76121526 2.5.4.10 (O) = NotarisID B.V. 2.5.4.6 (C) = NL			UTF8String UTF8String UTF8String PrintableString
	thisUpdate	yyyy.mm.dd HH:MM:SS (Date and time of creation of CRL)			UTCTime
	nextUpdate	yyyy.mm.dd HH:MM:SS (Date and time of next creation of CRL)			UTCTime
	Revoked Certificates				
	1…n List of revoked Certificates	Certificate	Serial number of the revoked Certificate		INTEGER
		Revocation time	yyyy.mm.dd HH:MM:SS (Date and time of revocation of Certificate)		UTCTime
	CRL Extensions:				
	2.5.29.35 Authority Key Identifier	Value of the “Subject Key Identifier” of de issuer CA			OID CONTEXT_SPECIFIC
	2.5.29.20 CRL Number	CRL sequence number			OCTET-STRING INTEGER
	2.5.29.60 Expired Certs On CRL	True			BOOLEAN
signatureAlgorithm		1.2.840.113549.1.1.13 (sha512RSA)			OID
signatureValue		Electronic signature computed upon the ASN.1 DER encoded tbsCertficate			BIT_STRING

7.3 OCSP profile

No stipulation.

(NotarisID does not support OCSP, only CRL)

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

NotarisID is a trust service provider as meant in chapter three of the eIDAS Regulation (EU Regulation 910/2014). For this reason, it is subjected to supervision by the Dutch Telecom Authority (Rijksinspectie Digitale Infrastructuur). Compliance certificates have a validity of two years, with annual interim audits. Moreover, internal audits are performed regularly.

8.2 Identity/qualifications of assessor

NotarisID is certified according to ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 and ISO27001:2013 standards by BSI Group The Netherlands B.V., which in turn is certified by the Dutch Accreditation Council (Raad voor Accreditatie).

8.3 Assessor's relationship to assessed entity

The auditor performing the compliance audit has no other relationship whatsoever with NotarisID.

8.4 Topics covered by assessment

The scope of the compliance audit comprises the following services:

- Registration service.
- Certificate generation service.
- Revocation management service.
- Revocation status service.
- Dissemination service.
- Subject device provision service.

8.5 Actions taken as a result of deficiency

With respect to ETSI compliance audits, significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. Dependent of the deficiency, this determination is made by NotarisID with input from the auditor. NotarisID is then responsible for developing and implementing a corrective action plan. If exceptions or deficiencies pose an immediate threat to the security or integrity of the NotarisID, a corrective action plan will be developed within fourteen (14) days and implemented within a three (3) month period. For less serious exceptions or deficiencies, NotarisID will evaluate the significance of such issues and determine the appropriate course of action.

8.6 Communication of results

Compliance audit certificates can be consulted on NotarisID's website: https://notarisid.nl. The underlying audit reports are confidential and are therefore not made public.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Certificates are issued free of charge.

9.1.2 Certificate access fees

The Certificate of Subscriber is not available for public. The Root Certificate of NotarisID can be accessed through the Document Repository by anyone, free of charge.

9.1.3 Revocation or status information access fees

The Document Repository and CRL can be accessed by anyone, free of charge.

9.1.4 Fees for other services

The Appointed Notary charges a fee for the Notary Deed. In the Notary Agreement, NotarisID and Appointed Notary agreed that NotarisID will bear these fee(s).

9.1.5 Refund policy

Please refer to the General Terms and Conditions.

9.2 Financial responsibilities

9.2.1 Insurance coverage

NotarisID is insured. It has an insurance for General Liability (“Bedrijfsaansprakelijkheidsverzekering”) that covers personal injury and property damages. NotarisID has an insurance for Professional Liability (“Beroepsaansprakelijkheidsverzekering”) that covers damages due to (attributable) errors or omissions made by NotarisID.

Insurance	Limits
General Liability	Per year: € 10.000.000,- Per claim: € 5.000.000,-
Professional Liability	Per year: € 5.000.000,- Per claim: € 2.500.000,-

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

(The in paragraph 9.2.1 of this CP/CPS mentioned insurances are not first party insurances and/or named insurances)

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

NotarisID considers all data provided within the framework of the certification service as confidential.

9.3.2 Information not within the scope of confidential information

All data not mentioned in paragraph 9.3.1 of this CP/CPS.

9.3.3 Responsibility to protect confidential information

Any party having confidential information at its disposal is responsible for ensuring its confidentiality.

9.4 Protection of personal data

NotarisID has an Information Security Management System (ISMS) certified according to ISO27001:2013 in place, ensuring confidentiality of all processed personal data processed. As a part of this ISMS, NotarisID has an information security policy which is reviewed periodically. the information security policy identifies the information and data, and measures which are necessary to protect that information and data.

Furthermore, the NotarisID Privacy Statement is applicable to all the provided services.

9.4.1 Privacy plan

Please refer to the NotarisID Privacy Statement, which is made publicly available in the Document Repository.

9.4.2 Information treated as private

Please refer to the NotarisID Privacy Statement, which is made publicly available in the Document Repository.

9.4.3 Information not deemed private

Please refer to the NotarisID Privacy Statement, which is made publicly available in the Document Repository.

9.4.4 Responsibility to protect private information

Please refer to the NotarisID Privacy Statement, which is made publicly available in the Document Repository.

9.4.5 Notice and consent to use private information

Please refer to the NotarisID Privacy Statement, which is made publicly available in the Document Repository.

9.4.6 Disclosure pursuant to judicial or administrative process

NotarisID has a procedure in place in case it needs to adhere to (new) judicial or government demands. This procedure is followed by a Trusted Staff Member in case such a demand arises. Part of this procedure is that NotarisID will always try to invoke its extended notary privilege (“afgeleid verschoningsrecht notaris”), however, it cannot warrant nor guarantee that this will be successful.

The Law of the Netherlands do not give (Q)TSP special rights regarding judicial and/or government demands.

9.4.7 Other information disclosure circumstances

No stipulation.

(There are no other disclosure circumstances)

9.5 Intellectual property rights

All documents, products and services made public by NotarisID are subject to copyright and/or licensees.

9.6 Statements and warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.6.1 CA representations and warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.6.2 RA representations and warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.6.3 Subscriber representations and warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.6.4 Relying party representations and warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.6.5 Representations and warranties of other participants

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.7 Disclaimers of warranties

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.8 Limitations of liability

Please refer to the General Terms and Conditions and the Terms for Relying Parties.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP/CPS is effective immediately after publication in the Document Repository and remains effective until a new version is published.

9.10.2Termination

By publishing a new version of this CP/CPS, the previous version of the CP/CPS is terminated.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communication

NotarisID can be contacted via mail, e-mail, and telephone. NotarisID publishes information on its public website and/or in the Document Repository and contacts individual Subscribers via e-mail or telephone.

9.12 Amendments

9.12.1 Procedure for amendment

NotarisID has the right to amend or supplement this CP/CPS. NotarisID will review and update this CPS/CPS when:

a) the yearly scheduled review is performed;
b) there are changes to the process, procedures or policy described in this document;
c) there are changes to the law, regulations, or requirements;
d) there are changes to the business interests of NotarisID and adjustments are required;
e) any changes which are not noted in the document history are grammatical, typographical or format changes which do not impact the underlying information pertaining to processes, procedures, and policy.

9.12.2 Notification mechanism and period

Please refer to paragraph 9.10.1 of this CP/CPS.

9.12.3 Circumstances under which Object Identifier (OID) must be changed

No stipulation.

9.13 Dispute resolution provisions

NotarisID has a complaint procedure, which is available in the Document Repository.

9.14 Governing law

All activities performed by NotarisID are subject to the Law of the Netherlands.

9.15 Compliance with applicable law

NotarisID complies with the applicable laws and regulations.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

(Force majeure is governed by the Law of the Netherlands)

9.17 Other Provisions

No stipulation.

###